

# NetCloud Exchange HMF IDPS Ruleset

v1.374.3380 - May 20, 2026

By the Cradlepoint Threat Research and Analysis (TR&A) team

## Preface:

This document provides a complete listing of all signatures which the Cradlepoint NetCloud Exchange HMF Intrusion Detection and Prevention (IDS/IPS) engine can detect and act upon. It also highlights changes since the last ruleset publication.

## AT A GLANCE:

---

### Changes since last release:

[Added](#): 2

[Removed](#): 20

[Modified](#): 0

[Entire Ruleset](#): 711

## [+] ADDED RULES:

---

**SEVERITY: Major**

*SIGNATURE ID - MESSAGE*

---

• **2068716 - ET MALWARE XorBee RAT CNC Checkin M1**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2026\_04\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1095 Non-Application Layer Protocol](#)

• **2068765 - ET MALWARE ShadowLink IoT Botnet Socks Proxy Registration Attempt**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2026\_04\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

## [-] REMOVED RULES:

---

**SEVERITY: Critical**

*SIGNATURE ID - MESSAGE*

---

• **2049867 - ET MALWARE Suspected FIN7/Carbanak Related Payload C2 Downloader (GET)**

- **Category:** Malware
- **Severity:** Critical
- **Date Added:** 2024\_01\_11
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

**SEVERITY: Major**

*SIGNATURE ID - MESSAGE*

---

• **2010597 - ET MALWARE Potential FakeAV HTTP GET Check-IN (/check)**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_09\_12
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2011588 - ET MALWARE Zeus Bot Connectivity Check**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_09\_12
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2017269 - ET MALWARE CBReplay.P Ransomware**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_04\_18
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0040 Impact](#)
  - **Technique:** [T1486 Data Encrypted for Impact](#)

• **2018295 - ET MALWARE Mal/Ransom-CE Connectivity Check**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_09\_12
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

- **MD5:** 6faa7077de347ee0fa8c991934c2c3a5
- **2018784 - ET MALWARE Win32/Neurevt.A/Betabot Check-in 4**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
  - **MD5:** 5eada3ed47d7557df375d8798d2e0a8b
- **2019341 - ET MALWARE Cryptowall 2.0 DL URI Struct Oct 2 2014**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2019481 - ET MALWARE Orca RAT URI Struct 1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2019482 - ET MALWARE Orca RAT URI Struct 2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2020380 - ET MALWARE Possible Deep Panda User-Agent**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 5acc539355258122f8cdc7f5c13368e1
- **2020826 - ET MALWARE Potential Dridex.Maldoc Minimal Executable Request**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 28208e19a528bfa95e5662e2d6f2e911
- **2021245 - ET MALWARE Possible Dridex Download URI Struct with no referer**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2021995 - ET MALWARE Win32/Necurs Common POST Header Structure**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** d11a453d4de6e6fd991967d67947c0d7
- **2022939 - ET MALWARE Possible Pony DLL Download**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_18
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 62e7a146079f99ded1a6b8f2db08ad18
- **2022940 - ET MALWARE Possible Malicious Macro DL EXE Jul 01 2016 (userdir dotted quad)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_18
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** a27bb6ac49f890bbdb97d939ccaa5956
- **2024508 - ET MALWARE Nemucod JS Downloader Aug 01 2017**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_08\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
  - **MD5:** cb558b04216e0e7a9c936945ebee6611
- **2051981 - ET MALWARE Win32/Powershell Loader Related Activity (GET)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_18
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** b1fd11164cec63f26a8b08ca2ab81b84

• **2051982 - ET MALWARE Suspected Trojan-Proxy Web Socket Connection Activity**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_04\_18
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 063d956b55da0d18f3f732c2bbd4bc28

• **2052168 - ET MALWARE Win32/SSLoad Tasking Result**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_04\_22
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** d6b0726de53f8a3da67a6e693485ca7a

• **2052192 - ET MALWARE Possible SSload Interactive Shell whoami Output**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_04\_22
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **MD5:** 67bb8840ab72dc31713751adccbbf6a1

## ENTIRE RULESET:

---

**Total rules: 711**

**SEVERITY: Critical**

SIGNATURE ID - MESSAGE

---

- **2024194 - ET EXPLOIT Cisco Catalyst Remote Code Execution (CVE-2017-3881)**
  - **Category:** Exploit
  - **Severity:** Critical
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024980 - ET EXPLOIT Actiontec C1000A backdoor account M2**
  - **Category:** Exploit
  - **Severity:** Critical
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2025785 - ET EXPLOIT ADB Broadband Authorization Bypass**
  - **Category:** Exploit
  - **Severity:** Critical
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1212 Exploitation for Credential Access](#)
  - **CVE:** [2018-13109](#)
- **2031459 - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (web.config) (CVE-2020-10148)**
  - **Category:** Exploit
  - **Severity:** Critical
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)

- CVE: [2020-10148](#)
- **2031460 - ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (SWNetPerfMon.db) (CVE-2020-10148)**
  - **Category:** Exploit
  - **Severity:** Critical
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- CVE: [2020-10148](#)
- **2021641 - ET MALWARE LokiBot User-Agent (Charon/Inferno)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_12\_03
- **2024312 - ET MALWARE LokiBot Application/Credential Data Exfiltration Detected M1**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_12\_03
- **2051140 - ET MALWARE DuckTail APT CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_03\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 3ab0d663608d0fded925fd01c44e7c63
- **2052248 - ET MALWARE Arechclient2 Backdoor/SecTopRAT Related Activity M2 (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_04\_29
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** a2c80aed8f6721a1e4bd66dded415eab
- **2052444 - ET MALWARE DuckTail APT Payload Request**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_10
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 6b18c0bff7be3ea36fa03eb0d52bd088
- **2052457 - ET MALWARE GhostRat CnC Checkin**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_10
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** f126ebba071ecab70a832ca04aa06765
- **2052602 - ET MALWARE AMOS CnC Exfiltration - /joinsystem (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2052604 - ET MALWARE AMOS CnC Exfiltration - /p2p (POST) M1**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0010 Exfiltration](#)
- **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2052605 - ET MALWARE AMOS CnC Exfiltration - /p2p (POST) M2**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2052619 - ET MALWARE JS/Unknown RAT Activity (GET) M1**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2b1aad3c4eebdd8b4bbd4cbb1fb2468
- **2052621 - ET MALWARE JS/Unknown RAT Activity (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2b1aad3c4eebdd8b4bbd4cbb1fb2468
- **2052638 - ET MALWARE Horabot CnC Host Details Exfil**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 1484c908cc1819798beed27c9531f24a
- **2052804 - ET MALWARE Winnti CnC Activity (Outbound)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_23
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **2052908 - ET MALWARE CrimsonRAT Host Details Exfil**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** da2331ac3e073164d54bcc5323cf0250
- **2052949 - ET MALWARE Suspected Smokeloader Payload Related Activity (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_31
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** bcb2c402c896b5477e1f94a1c7278682
- **2054350 - ET MALWARE Win32/Cryptbotv2 CnC Activity (POST) M4**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_09
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2054414 - ET MALWARE ZharkBot CnC Exfil in HTTP URI**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_10
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2054425 - ET MALWARE Imposter Interpol Stealer CnC Checkin**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_12
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** fd4308bfa31bb22965a5d3e729c3e37b
- **2054616 - ET MALWARE Win32/saolei CnC Host Checkin**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** c8e6cd1fb6f5dfe1ab548024a7f67043
- **2054665 - ET MALWARE Win32/Rhadamanthys CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)

- **MD5:** 6ca89843cc5ffa1af85636dea4019a1a
- **2054667 - ET MALWARE JaskaGO CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 5dcba1aedb36bd8ccc7c70466dbd4cff
- **2054711 - ET MALWARE PrivateLoader CnC Activity (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_07\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 164a9c52deb23309bf904a7c8f475ffd
- **2054750 - ET MALWARE PshellBkdr C2 Traffic Known Authorization Bearer in HTTP Request (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2054783 - ET MALWARE CHM Stealer CnC Host Profile Exfil (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** fee9d2b13985879ba348080a9bf4e6f1
- **2054812 - ET MALWARE Crimson RAT CnC Victim Details Exfil**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** f5380e7a6e15a0ef27e6f31fcc29ed4d
- **2055379 - ET MALWARE Cobalt Strike Malleable C2 (MSNBC Video Profile)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
- **2055382 - ET MALWARE Cobalt Strike Malleable C2 (Pandora Profile)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
- **2055467 - ET MALWARE ELF/crond CnC Request (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)

- **MD5:** d13254b450e9c45b86f0972eb3a10608
- **2055497 - ET MALWARE SystemBC CnC Beacon**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_08\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** ed44877077716103973cbbabd531f38e
- **2057741 - ET MALWARE TA582 CnC Checkin**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_12\_03
- **2057743 - ET MALWARE TA582 CnC Checkin**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2024\_12\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e8da759e748db6eab355cf87d1f2db6c
- **2059633 - ET MALWARE Lazarus APT Electron CnC Activity (GET) M1**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_01\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2a8e4281213e4aaa485612f9ded261a2
- **2061118 - ET MALWARE Arechclient2 Backdoor/SecTopRAT Related Activity M3 (GET)**
  - **Category:** Malware

- **Severity:** Critical
- **Date Added:** 2025\_04\_14
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1102 Web Service](#)
- **MD5:** 8f6d5a6f20fbcc87e2d2032652b02de6
- **2061376 - ET MALWARE Generic Malware CnC Activity - (Unix Timestamp In HTTP URI)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_04\_21
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
  - **MD5:** f4ee2d49e1a99151ad151078779e9cc5
- **2062720 - ET MALWARE Common Stealer Behavior - Source IP Associated with Hosting Provider Check via ip.api .com**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1596 Search Open Technical Databases](#)
- **2062829 - ET MALWARE SVCStealer 4.4 CnC Task Checkin (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 804abee66ca7c07365c191a87532e137
- **2063399 - ET MALWARE Agent Tesla CnC Exfil via TCP**

- **Category:** Malware
- **Severity:** Critical
- **Date Added:** 2025\_07\_24
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **MD5:** f1b1fdd112b02733cd8e5d8ed62acec1
- **2063441 - ET MALWARE Numinon CnC Activity via WebSockets**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2063453 - ET MALWARE Voldemort System Info Exfil**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2064237 - ET MALWARE GCleaner Loader CnC Checkin (/info)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e627cad277450feb0685a9b2abd981f8
- **2064241 - ET MALWARE GCleaner Loader CnC Checkin (/update)**
  - **Category:** Malware

- **Severity:** Critical
- **Date Added:** 2025\_11\_04
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** e627cad277450feb0685a9b2abd981f8
- **2064261 - ET MALWARE GCleaner Loader CnC Checkin (GET)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e627cad277450feb0685a9b2abd981f8
- **2064262 - ET MALWARE GCleaner Loader CnC Checkin (/ycl)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e627cad277450feb0685a9b2abd981f8
- **2064271 - ET MALWARE GCleaner CnC Checkin (/service)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e627cad277450feb0685a9b2abd981f8
- **2065099 - ET MALWARE Bad PDF Editor Tamperedchef Process Initiation**

- **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065100 - ET MALWARE Bad PDF Editor Tamperedchef Payload Request**
- **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065101 - ET MALWARE Bad PDF Editor Tamperedchef Install Confirmation M1**
- **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065102 - ET MALWARE Bad PDF Editor Tamperedchef Install Confirmation M2**
- **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065229 - ET MALWARE Cobalt Strike Get Mission Request (POST)**
- **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2065230 - ET MALWARE Cobalt Strike CnC Checkin (Submit Result)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065231 - ET MALWARE Cobalt Strike ScreenShot Exfil (POST)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2067298 - ET MALWARE Malicious Notepad++ Update Deployment URL (update.exe)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2067299 - ET MALWARE Malicious Notepad++ Update Deployment URL (AutoUpdater.exe)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)

- **2067300 - ET MALWARE Malicious Notepad++ Update Deployment URL (install.exe)**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2068527 - ET MALWARE UNK\_MonkeyWrench Exfil via SMTP**
  - **Category:** Malware
  - **Severity:** Critical
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1048 Exfiltration Over Alternative Protocol](#)
  - **MD5:** 664a7f2d21f20f4a9747981145cb1332
- **2051955 - ET WEB\_SPECIFIC\_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt (CVE-2024-3273)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0008 Lateral Movement](#)
    - **Technique:** [T1210 Exploitation Of Remote Services](#)
  - **CVE:** [2024-3273](#)
- **2051955 - ET WEB\_SPECIFIC\_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt (CVE-2024-3273)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Critical
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0008 Lateral Movement](#)
    - **Technique:** [T1210 Exploitation Of Remote Services](#)

- CVE: [2024-3273](#)

**SEVERITY: Major**

*SIGNATURE ID - MESSAGE*

---

**• 8800019 - CP EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (Outbound) (CVE-2021-44228)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2024\_02\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1659 Content Injection](#)
- CVE: [2021-44228](#)

**• 8800020 - CP MISC Microsoft Extensible Storage Engine database detected**

- **Category:** Misc
- **Severity:** Major
- **Date Added:** 2024\_05\_16
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0007 Discovery](#)
  - **Technique:** [T1083 File and Directory Discovery](#)

**• 8800021 - CP MISC Microsoft Windows ntds.dit file Exfiltration Attempt**

- **Category:** Misc
- **Severity:** Major
- **Date Added:** 2024\_05\_16
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0006 Credential Access](#)
  - **Technique:** [T1003 OS Credential Dumping](#)

**• 2018392 - ET ATTACK\_RESPONSE Possible MS CMD Shell opened on local system 2**

- **Category:** Attack\_Response
- **Severity:** Major
- **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0002 Execution](#)
  - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2033916 - ET ATTACK\_RESPONSE Muhstik Botnet Download Activity (GET)**
  - **Category:** Attack\_Response
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
  - **MD5:** 898b3dc58bc5d05d3034a1c259b5a915
- **2038604 - ET ATTACK\_RESPONSE net user Command Output via HTTP POST**
  - **Category:** Attack\_Response
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
  - **MD5:** 91dc943c9e8fd0d4de54228823f9f26b
- **2044751 - ET ATTACK\_RESPONSE Interactive Reverse Shell Without TTY (Outbound)**
  - **Category:** Attack\_Response
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2018977 - ET DOS HOIC with booster outbound**
  - **Category:** DOS
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0040 Impact](#)
- **Technique:** [T1496 Resource Hijacking](#)
- **MD5:** 23fc64a5cac4406d7143ea26e8c4c7ab
- **2027063 - ET EXPLOIT Outbound GPON Authentication Bypass Attempt (CVE-2018-10561)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
- **2027339 - ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027450 - ET EXPLOIT Attempted Remote Command Injection Outbound (CVE-2019-3929)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2027452 - ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)

- **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **CVE:** [CVE-2017-14135](#)
- **2027456 - ET EXPLOIT Dell KACE Attempted Remote Command Injection Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [CVE-2018-11138](#)
- **2027458 - ET EXPLOIT Geutebruck Attempted Remote Command Injection Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [CVE-2017-5173](#)
- **2027460 - ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [CVE-2018-20841](#)
- **2027487 - ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Outbound (CVE-2019-12780)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [CVE-2019-12780](#)
- **MD5:** d6ebabf44849951d754ee2de15a24b92
- **2027488 - ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Outbound (CVE-2016-6255)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [CVE-2019-12780](#)
  - **MD5:** d6ebabf44849951d754ee2de15a24b92
- **2029154 - ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2019-18396](#)
- **2029156 - ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)

- **2029158 - ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2019-16072](#)
- **2029160 - ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2029162 - ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2017-16602](#)
- **2029164 - ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)

- CVE: [2017-6316](#)
- **2029166 - ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- CVE: [2013-5192](#)
- **2029168 - ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2029170 - ET EXPLOIT 3Com Office Connect Remote Code Execution (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2029172 - ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)

- CVE: [2006-4000](#)
- **2029174 - ET EXPLOIT CCBill Online Payment Systems RCE (Outbound)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2029213 - ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Outbound (CVE-2019-7256)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - CVE: [2019-7256](#)
- **2029215 - ET EXPLOIT Netgear DGN1000/DGN2200 Unauthenticated Command Execution Outbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2031938 - ET EXPLOIT Possible NSDP (Netgear) Unauthenticated Buffer Overflow (CVE-2020-35232)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0005 Defense Evasion](#)

- **Technique:** [T1211 Exploitation for Defense Evasion](#)
- **CVE:** [2020-35232](#)
- **2034480 - ET EXPLOIT Attempted IDSVSE IP Camera RCE**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2034750 - ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (udp) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034751 - ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (tcp) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034758 - ET EXPLOIT Apache log4j RCE Attempt (http rmi) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)
- **2034759 - ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034760 - ET EXPLOIT Apache log4j RCE Attempt (tcp rmi) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034761 - ET EXPLOIT Apache log4j RCE Attempt (udp ldap) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034762 - ET EXPLOIT Apache log4j RCE Attempt (udp rmi) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)
- **2034763 - ET EXPLOIT Apache log4j RCE Attempt (udp dns) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034764 - ET EXPLOIT Apache log4j RCE Attempt (tcp dns) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034765 - ET EXPLOIT Apache log4j RCE Attempt (http dns) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034766 - ET EXPLOIT Apache log4j RCE Attempt (udp ldaps) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major

- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)
- **2034767 - ET EXPLOIT Apache log4j RCE Attempt (tcp ldaps) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034768 - ET EXPLOIT Apache log4j RCE Attempt (http ldaps) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034781 - ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M1 (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034782 - ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M1 (Outbound) (CVE-2021-44228)**

- **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034786 - ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (tcp) (Outbound) (CVE-2021-44228)**
- **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034787 - ET EXPLOIT Apache log4j RCE Attempt (tcp iiop) (Outbound) (CVE-2021-44228)**
- **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034788 - ET EXPLOIT Apache log4j RCE Attempt (udp iiop) (Outbound) (CVE-2021-44228)**
- **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)

- CVE: [2021-44228](#)
- **2034789 - ET EXPLOIT Possible Apache log4j RCE Attempt (udp corba) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - CVE: [2021-44228](#)
- **2034790 - ET EXPLOIT Possible Apache log4j RCE Attempt (tcp corba) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - CVE: [2021-44228](#)
- **2034791 - ET EXPLOIT Possible Apache log4j RCE Attempt (udp nds) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - CVE: [2021-44228](#)
- **2034792 - ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nds) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major

- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)
- **2034793 - ET EXPLOIT Possible Apache log4j RCE Attempt (udp nis) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034794 - ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nis) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034795 - ET EXPLOIT Apache log4j RCE Attempt - Nested upper (udp) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)

• **2034796 - ET EXPLOIT Apache log4j RCE Attempt - Nested upper (tcp) (Outbound)**  
(CVE-2021-44228)

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)

• **2034797 - ET EXPLOIT Apache log4j RCE Attempt - Nested lower (udp) (Outbound)**  
(CVE-2021-44228)

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)

• **2034798 - ET EXPLOIT Apache log4j RCE Attempt - Nested lower (tcp) (Outbound)**  
(CVE-2021-44228)

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)

• **2034799 - ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M2 (Outbound)**  
(CVE-2021-44228)

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)
- **2034800 - ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034805 - ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2034806 - ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)

• **2034807 - ET EXPLOIT Apache log4j RCE Attempt - AWS Access Key Disclosure (Outbound) (CVE-2021-44228)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)

• **2034850 - ET EXPLOIT Possible Joomla RCE (CVE-2011-5148)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2011-5148](#)

• **2037047 - ET EXPLOIT Possible Apache log4j RCE Attempt - HTTP URI Obfuscation (CVE-2021-44228) (Outbound)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **CVE:** [2021-44228](#)

• **2042956 - ET EXPLOIT Observed Mirai/Gafgyt Post Brute Force Activity (GET)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_07\_28
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0006 Credential Access](#)

- **Technique:** [T1110 Brute Force](#)
- **MD5:** 512d5c2ba6b14f732061fc2f28a72f72
- **2044002 - ET EXPLOIT Lexmark Malicious File Upload Detected**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2044201 - ET EXPLOIT GitLab Pre-Auth RCE Detected (CVE-2021-22205)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2045125 - ET EXPLOIT Apache log4j RCE Attempt (http) (Outbound) (CVE-2021-44228)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2021-44228](#)
- **2045636 - ET EXPLOIT Possible Command Injection via User-Agent (PwnAgent) - CVE-2023-24749, CVE-2022-47208**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **CVE:** [2023-24749](#)
- **2048213 - ET EXPLOIT Potential Adobe Experience Manager (AEM) Dispatcher Bypass Attempt**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2021572 - ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M1**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_01\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1499 Endpoint Denial of Service](#)
  - **CVE:** [2015-5477](#)
- **2021573 - ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M2**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_01\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1499 Endpoint Denial of Service](#)
  - **CVE:** [2015-5477](#)
- **2021574 - ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M3**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_01\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)

- **Technique:** [T1499 Endpoint Denial of Service](#)
- **CVE:** [2015-5477](#)
- **2021575 - ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M4**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_01\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1499 Endpoint Denial of Service](#)
  - **CVE:** [2015-5477](#)
- **2024548 - ET EXPLOIT Ubiquiti Networks UniFi Cloud Key Firm v0.6.1 Host Remote Command Execution attempt**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024914 - ET EXPLOIT Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [CVE-2017-18377](#)
- **2024915 - ET EXPLOIT Possible Vacron NVR Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0004 Privilege Escalation](#)
- **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024916 - ET EXPLOIT Netgear DGN Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024917 - ET EXPLOIT AVTECH Unauthenticated Command Injection in DVR Devices**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024918 - ET EXPLOIT AVTECH Authenticated Command Injection in CloudSetup.cgi**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024919 - ET EXPLOIT AVTECH Authenticated Command Injection in adcommand.cgi**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2024920 - ET EXPLOIT AVTECH Authenticated Command Injection in PwdGrp.cgi**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0004 Privilege Escalation](#)
  - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2025080 - ET EXPLOIT Actiontec C1000A backdoor account M1**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_01\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2025132 - ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [CVE-2014-8361](#)
- **2025222 - ET EXPLOIT Generic ADSL Router DNS Change Request**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2025223 - ET EXPLOIT Possible Belkin N600DB Wireless Router Request Forgery Attempt**
  - **Category:** Exploit
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0002 Execution](#)
  - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2025576 - ET EXPLOIT HackingTrio UA (Hello, World)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **CVE:** [2018-10561](#)
- **2025735 - ET EXPLOIT TP-Link Technologies TL-WA850RE Wi-Fi Range Extender - Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2025756 - ET EXPLOIT D-Link DSL-2750B - OS Command Injection**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2025769 - ET EXPLOIT Geutebruck Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0004 Privilege Escalation](#)
  - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **CVE:** [2018-7520](#)
- **2025821 - ET EXPLOIT HID VertX and Edge door controllers command\_blink\_on Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2025823 - ET EXPLOIT D-Link DIR601 2.02 Credential Disclosure**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1082 System Information Discovery](#)
- **2025883 - ET EXPLOIT MVPower DVR Shell UCE**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027089 - ET EXPLOIT Possible LG SuperSign EZ CMS 2.5 RCE (CVE-2018-17173)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0002 Execution](#)
- **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2018-17173](#)
- **2027090 - ET EXPLOIT Possible WePresent WIPG1000 OS Command Injection**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027091 - ET EXPLOIT Possible WePresent WIPG1000 File Inclusion**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027092 - ET EXPLOIT Possible ZyXEL P660HN-T v1 RCE (CVE-2017-18368)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2017-18368](#)
- **2027093 - ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6077)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)

- **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2017-6077](#)
- **2027094 - ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6334)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2017-6334](#)
- **2027097 - ET EXPLOIT Possible Linksys WRT100/110 RCE Attempt (CVE-2013-3568)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2013-3568](#)
- **2027098 - ET EXPLOIT Possible ZTE ZXV10 H108L Router Root RCE Attempt**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027099 - ET EXPLOIT Possible Linksys E1500/E2500 apply.cgi RCE Attempt**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)

- **Technique:** [T1203 Exploitation for Client Execution](#)
- **2027451 - ET EXPLOIT Attempted Remote Command Injection Inbound (CVE-2019-3929)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2027453 - ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Inbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [CVE-2017-14135](#)
- **2027457 - ET EXPLOIT Dell KACE Attempted Remote Command Injection Inbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [CVE-2018-11138](#)
- **2027459 - ET EXPLOIT Geutebruck Attempted Remote Command Injection Inbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)

- CVE: [CVE-2017-5173](#)
- **2027461 - ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Inbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - CVE: [CVE-2018-20841](#)
- **2027486 - ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Inbound (CVE-2019-12780)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - CVE: [CVE-2019-12780](#)
  - **MD5:** d6ebabf44849951d754ee2de15a24b92
- **2027489 - ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Inbound (CVE-2016-6255)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - CVE: [CVE-2019-12780](#)
  - **MD5:** d6ebabf44849951d754ee2de15a24b92
- **2027513 - ET EXPLOIT FCM-MB40 Attempted Remote Command Execution as Root**
  - **Category:** Exploit
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0004 Privilege Escalation](#)
  - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027881 - ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Inbound (CVE-2019-6277)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [CVE-2016-6277](#)
- **2027882 - ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Outbound (CVE-2019-6277)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [CVE-2016-6277](#)
- **2027971 - ET EXPLOIT HiSilicon DVR - Application Credential Disclosure (CVE-2018-9995)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1082 System Information Discovery](#)
  - **CVE:** [2018-9995](#)
- **2027972 - ET EXPLOIT HiSilicon DVR - Buffer Overflow in Builtin Web Server**
  - **Category:** Exploit
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0004 Privilege Escalation](#)
  - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027973 - ET EXPLOIT HiSilicon DVR - Default Telnet Root Password Inbound**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2027974 - ET EXPLOIT HiSilicon DVR - Default Application Backdoor Password**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1082 System Information Discovery](#)
- **2030258 - ET EXPLOIT OpenMRS Deserialization Vulnerability CVE-2018-19276**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [2018-19276](#)
- **2030259 - ET EXPLOIT Multiple Router RCE Routersploit**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0004 Privilege Escalation](#)
- **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2030260 - ET EXPLOIT Edimax Technology EW-7438RPn-v3 Mini 1.27 - Remote Code Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2030261 - ET EXPLOIT Technicolor TD5130.2 - Remote Command Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2030262 - ET EXPLOIT Xfinity Gateway - Remote Code Execution**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2031507 - ET EXPLOIT Microsoft Exchange Server Exploitation (CVE-2020-17141)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
- **2032095 - ET EXPLOIT Yealink RCE Attempt (CVE-2021-27561)**

- **Category:** Exploit
- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0002 Execution](#)
  - **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2021-27561](#)
- **2035013 - ET EXPLOIT Oracle WebLogic IOP JNDI Injection (CVE-2020-14841)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2020-14841](#)
- **2035014 - ET EXPLOIT Sangoma Asterisk Originate AMI RCE (CVE-2019-18610) (PoC Based)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - **CVE:** [2019-18610](#)
- **2036749 - ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M1**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_06\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2014-9118](#)

- **2036750 - ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M2**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_06\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2014-9118](#)
- **2038665 - ET EXPLOIT Attempted Schneider Electric SpaceLogic C-Bus Home Controller 5200WHC2 Remote Code Execution (CVE-2022-34753)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2039129 - ET EXPLOIT ZKBioSecurity SQL Injection Attempt (CVE-2022-36635)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2022-36635](#)
- **2041650 - ET EXPLOIT Xiongmai/HiSilicon DVR - RTSP Buffer Overflow Attempt - CVE-2022-26259**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)

- CVE: [2022-26259](#)
- **2048548 - ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2023\_11\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
  - CVE: [2023-26801](#)
- **2051785 - ET EXPLOIT Possible Uniview IPC2322Ib updatecpld Restricted Shell Bypass Attempt**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_04\_18
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063368 - ET EXPLOIT GTPDoor Trigger Packet Response**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2025\_11\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0008 Lateral Movement](#)
    - **Technique:** [T1210 Exploitation Of Remote Services](#)
- **2016210 - ET EXPLOIT\_KIT Redkit Exploit Kit Three Numerical Character Naming Convention PDF Request**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)

- CVE: [2010-0188](#)
- **2016499 - ET EXPLOIT\_KIT Styx Exploit Kit Payload Download**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
- **2016839 - ET EXPLOIT\_KIT FlimKit hex.zip Java Downloading Jar**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
- **2016869 - ET EXPLOIT\_KIT FlimKit Post Exploit Payload Download**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
- **2027145 - ET EXPLOIT\_KIT Spelevo EK Flash Exploit Attempt**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
- **2044908 - ET EXPLOIT\_KIT TDS checkResult Request - Observed Leading to CryptoClipper**
  - **Category:** Exploit\_Kit

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1189 Drive-by Compromise](#)
- **2068160 - ET EXPLOIT\_KIT Coruna Stage 2 Implant Activity**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2026\_03\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2068161 - ET EXPLOIT\_KIT Coruna Stage 3 Implant Activity M1**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2026\_03\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2068162 - ET EXPLOIT\_KIT Coruna Stage 3 Implant Activity M2**
  - **Category:** Exploit\_Kit
  - **Severity:** Major
  - **Date Added:** 2026\_03\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029009 - ET HUNTING Generic IOT Downloader Malware in POST (Outbound)**
  - **Category:** Hunting
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1566 Phishing](#)
- **2029010 - ET HUNTING Generic IOT Downloader Malware in GET (Outbound)**
  - **Category:** Hunting
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
- **2029589 - ET HUNTING Generic IOT Downloader Malware in GET (Outbound)**
  - **Category:** Hunting
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
- **2013361 - ET MALWARE HTran/SensLiceld.A response to infected host - Inbound Connection Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_02\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1090 Proxy](#)
- **2014226 - ET MALWARE IP2B Trojan Communication Protocol detected**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)

- **2014227 - ET MALWARE BB Trojan Communication Protocol detected**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_13
- **2022270 - ET MALWARE Possible Evil Macro Downloading Trojan Dec 16 2015 Post to EXE**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2022550 - ET MALWARE Possible Malicious Macro DL EXE Feb 2016**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2022622 - ET MALWARE Likely Evil Macro EXE DL mar 15 2016**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2024243 - ET MALWARE ARM Binary Requested via WGET to Known IoT Malware Domain**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2024380 - ET MALWARE Nemucod JS Downloader June 12 2017**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_31
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027119 - ET MALWARE ELF/Mirai Variant UA Outbound (Rift)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027121 - ET MALWARE ELF/Mirai Variant UA Outbound (Tsunami)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027123 - ET MALWARE ELF/Mirai Variant UA Outbound (Yowai)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027125 - ET MALWARE ELF/Mirai Variant UA Outbound (Yakuza)**
  - **Category:** Malware

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2027127 - ET MALWARE ELF/Mirai Variant UA Outbound (Hentai)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027129 - ET MALWARE ELF/Mirai Variant UA Outbound (lessie)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027131 - ET MALWARE ELF/Mirai Variant UA Outbound (Cakle)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027133 - ET MALWARE ELF/Mirai Variant UA Outbound (Damien)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **2027137 - ET MALWARE ELF/Mirai Variant UA Outbound (muhstik)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027139 - ET MALWARE ELF/Mirai Variant UA Outbound (Shaolin)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027701 - ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Started**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027702 - ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Done**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027914 - ET MALWARE Win32/Nemty Ransomware Style Geo IP Check M2**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_08\_30
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0040 Impact](#)
  - **Technique:** [T1486 Data Encrypted for Impact](#)
- **MD5:** 0e0b7b238a06a2a37a4de06a5ab5e615
- **2029027 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029028 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029029 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029030 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029031 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029033 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029034 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029035 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2029036 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029037 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029038 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029209 - ET MALWARE Dark Nexus IoT Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029472 - ET MALWARE ELF/Mirai User-Agent Observed (Outbound)**
  - **Category:** Malware

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029578 - ET MALWARE Polaris Botnet User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029646 - ET MALWARE Polaris Botnet User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029760 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029764 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **2029770 - ET MALWARE Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029791 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029793 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029809 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029930 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2030049 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030123 - ET MALWARE W32/Agent.XXZBEN Downloader Activity**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_03\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 113a0256fa05ece2a56b88e6285aff7a
- **2030199 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030274 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2030374 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030376 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030471 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030584 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- Technique: [T1071 Application Layer Protocol](#)
- **2030677 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030690 - ET MALWARE Possible KONNI URI Path Observed**
  - Category: Malware
  - Severity: Major
  - Date Added: 2024\_05\_31
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1566 Phishing](#)
- **2030693 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030910 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030965 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - Category: Malware

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2030996 - ET MALWARE ELF/Mirai Variant User-Agent (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2033158 - ET MALWARE Cobalt Strike Malleable C2 Profile wordpress\_ Cookie Test**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
- **2033906 - ET MALWARE Win32/Unk.Coinminer Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1496 Resource Hijacking](#)
  - **MD5:** a98df471bde22b7b2d25aae974237363
- **2034840 - ET MALWARE Kimsuky Related Maldoc Retrieving Template (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_29

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 51fa8bf006d80f5e140d84df313c650f
- **2034883 - ET MALWARE TA453 ClumsyCover Maldoc Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2035939 - ET MALWARE Fodcha Bot CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2036940 - ET MALWARE ELF/Mirai Variant Activity (Outbound)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
  - **MD5:** d9c25c9dd17e1ef2f5b65f9f9723d301
- **2045229 - ET MALWARE Win32/Phorpiex Template 9 Active - Outbound Malicious Email Spam**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_29
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1566 Phishing](#)
- **2045872 - ET MALWARE Suspected Gamaredon APT Related Activity**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** de9a87a8dc9eb67b3e54c452f63b2579
- **2047646 - ET MALWARE JanelaRAT CnC Checkin Observed**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_06\_12
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2048564 - ET MALWARE Possible Win32/DarkWatchMan User Agent M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_11\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 1706c64156d873ebbd0c6ecac95fec39
- **2052235 - ET MALWARE APT Related CR4T Backdoor Activity**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2052261 - ET MALWARE Win32/ProcessKiller Payload Retrieval Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 1bea43ae6680c0925e6ac5909888a6d4
- **2052262 - ET MALWARE Win32/ProcessKiller CnC Initialization**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_04\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 1bea43ae6680c0925e6ac5909888a6d4
- **2052280 - ET MALWARE Win32/Neshta Variant Related Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 6767f8292814a48db7fa79e8572a324f
- **2052285 - ET MALWARE Possible Royal Road Payload Retrieval Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** b85316f68d9f1dbac481e3f397ebf1b0
- **2052312 - ET MALWARE Cobalt Strike CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
- **2052361 - ET MALWARE Suspected TA401/AridViper APT Micropsia Variant Related Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 36e291abe37fff7868c5ca7d4105c86b
- **2052394 - ET MALWARE Goldoon Botnet Payload Retrieval Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2052412 - ET MALWARE Suspected APT42/TA453 TAMECAT Loader Related Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_10
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)

- **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **MD5:** d7bf138d1aa2b70d6204a2f3c3bc72a7
- **2052557 - ET MALWARE BadSpace/WarmCookie CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2052558 - ET MALWARE W32/Badspace.Backdoor CnC Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2052603 - ET MALWARE AMOS CnC Exfiltration - /sendlog (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2052620 - ET MALWARE JS/Unknown RAT Activity (GET) M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2b1aad3c4eebdd8b4bbd4cbb1fb2468

- **2052789 - ET MALWARE Private Loader Related Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 362697c95a1c9964af1ab23ddfc29b04
- **2052812 - ET MALWARE AnonymousRAT Payload Retrieval Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_23
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 0bbe7daf7e104bf0091f4be771fe2133
- **2052848 - ET MALWARE pcTattletale Software Installer Request (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
- **2052876 - ET MALWARE Unknown RAT CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** db9fd417244157770e31fb4b39e0e97a

- **2052911 - ET MALWARE Suspected TA450 Activity**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 513e8e3ede4f821dad0e3ba3448aca42
- **2052950 - ET MALWARE Async RAT CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_05\_31
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2053040 - ET MALWARE Justice AV Solutions Viewer Backdoor CnC Checkin (CVE-2024-4978)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_06\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **CVE:** [2024-4978](#)
- **2053207 - ET MALWARE Allasenha/CarnavalHeist RAT CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_06\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **2053269 - ET MALWARE Spyder Loader CnC Checkin**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2053279 - ET MALWARE Silverfox Payload Retrieval Attempt**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 07b0577363ee95f35a86913dcbfa0904
- **2053319 - ET MALWARE HTTP Request to URL Ending in Payload .bin**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_06\_10
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 0de8355fa0dae02193976464d64d45b3
- **2053694 - ET MALWARE Win64/TrojanDownloader.Agent.AUO User Agent**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_06\_18
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2053749 - ET MALWARE Win32/ProcessKiller CnC Initialization M2**
- **Category:** Malware

- **Severity:** Major
- **Date Added:** 2024\_06\_26
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **MD5:** 50ebb1dbea9bf98e789af1431e5bc4a6
- **2054070 - ET MALWARE Possible Sniffthem/Tnaket User-Agent Observed M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** bace58b7211332b033975559fc7859b8
- **2054071 - ET MALWARE Possible Sniffthem/Tnaket User-Agent Observed M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** bace58b7211332b033975559fc7859b8
- **2054072 - ET MALWARE Possible Sniffthem/Tnaket Payload Retrieval Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** bace58b7211332b033975559fc7859b8
- **2054073 - ET MALWARE Possible Sniffthem/Tnaket CnC Checkin**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** bace58b7211332b033975559fc7859b8
- **2054173 - ET MALWARE Poseidon Stealer Data Exfiltration Attempt**
    - **Category:** Malware
    - **Severity:** Major
    - **Date Added:** 2024\_07\_04
    - **MITRE ATT&CK®:**
      - **Tactic:** [TA0010 Exfiltration](#)
      - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2054404 - ET MALWARE [ANY.RUN] MetaStealer v.5 CnC Activity (MC-NMF TLS SNI)**
    - **Category:** Malware
    - **Severity:** Major
    - **Date Added:** 2024\_07\_10
    - **MITRE ATT&CK®:**
      - **Tactic:** [TA0011 Command And Control](#)
      - **Technique:** [T1071 Application Layer Protocol](#)
- **2054413 - ET MALWARE ZharkBot User-Agent Observed**
    - **Category:** Malware
    - **Severity:** Major
    - **Date Added:** 2024\_07\_10
    - **MITRE ATT&CK®:**
      - **Tactic:** [TA0011 Command And Control](#)
      - **Technique:** [T1071 Application Layer Protocol](#)
- **2054495 - ET MALWARE Vidar Stealer Form Exfil**
    - **Category:** Malware
    - **Severity:** Major

- **Date Added:** 2024\_07\_17
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **MD5:** 8bea4ed23c54744533c32994e6c88deb
- **2054652 - ET MALWARE Daolpu Stealer Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_07\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2054729 - ET MALWARE 9002 RAT CnC Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 19aff0a43f80919a6113020d3ff38300
- **2054781 - ET MALWARE Specula Framework CnC Activity (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2054782 - ET MALWARE Specula Framework CnC Activity (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_01

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2054939 - ET MALWARE MOONSTONE SLEET APT Payload Delivery Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_08
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1195 Supply Chain Compromise](#)
- **2055399 - ET MALWARE Possible RAZR Ransomware User-Agent Observed**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** a1160fa83f4b7247a10c6476449a2719
- **2055401 - ET MALWARE RAZR Ransomware CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** a1160fa83f4b7247a10c6476449a2719
- **2055496 - ET MALWARE Possible Cthulu Stealer URI Struct M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_29
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0010 Exfiltration](#)
- **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2055498 - ET MALWARE Possible Cthulu Stealer URI Struct M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2055531 - ET MALWARE Rodmacer Stealer Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_08\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 14a50273e7c37a994c687cbce8eb4703
- **2055586 - ET MALWARE TA452 Trojan CnC Checkin M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_02
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0037 Command And Control](#)
    - **Technique:** [T1041 exfiltration over C2 channel](#)
- **2055587 - ET MALWARE TA452 Trojan CnC Checkin M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_09\_02
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0037 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)

• **2055760 - ET MALWARE VBS/Clipboard Stealer Related Activity (GET)**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_09\_09
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0009 Collection](#)
  - **Technique:** [T1115 Clipboard Data](#)
- **MD5:** 0dfe8302e05cb61657b91d412b608042

• **2055906 - ET MALWARE Win32/Mesquito Loader Related Activity (GET)**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_09\_19
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 6d3d9667fce811c895b005dbce80cf24

• **2057246 - ET MALWARE [NCSC] Pygmy Goat SSH Banner**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_11\_28

• **2057247 - ET MALWARE [NCSC] Pygmy Goat SSH ed25519 Key**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_11\_28

• **2057283 - ET MALWARE HTTP Request to Remcos Payload M1**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2024\_11\_28
- **MD5:** 813b231054a869cf29bfe9396731e47f

• **2057292 - ET MALWARE HTTP Request to Remcos Payload M2**

- **Category:** Malware

- **Severity:** Major
- **Date Added:** 2024\_11\_28
- **MD5:** 813b231054a869cf29bfe9396731e47f
- **2058145 - ET MALWARE Retdoor CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_16
- **2058173 - ET MALWARE QuickResponseC2 Default Tasking Struct**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0037 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2058174 - ET MALWARE QuickResponseC2 Default Response Struct**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2024\_12\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0037 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2058670 - ET MALWARE Observed Malicious User-Agent (UNK\_FlappyBird)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_01\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
- **2059018 - ET MALWARE CryptBot CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_01\_16
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** e52da29ca9214e322ba939105a9d6bb8
- **2059019 - ET MALWARE CryptBot Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_01\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** e52da29ca9214e322ba939105a9d6bb8
- **2059634 - ET MALWARE Lazarus APT Electron CnC Activity (GET) M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_01\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2a8e4281213e4aaa485612f9ded261a2
- **2059635 - ET MALWARE Lazarus APT Electron CnC Activity (GET) M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_01\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2a8e4281213e4aaa485612f9ded261a2
- **2060585 - ET MALWARE Win32/SocGholish GhostWeaver Backdoor Activity (PowerShell BOINC Download Request)**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_03\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2060673 - ET MALWARE Observed POST to ClickFix Style URI M1**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_03\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2060675 - ET MALWARE Observed GET to ClickFix Style URI M1**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_03\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2061021 - ET MALWARE SvcStealer CNC Tasking Checkin**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 06635111468af8497979f05ccd5bc2ea
- **2061022 - ET MALWARE SvcStealer Data Exfiltration Attempt**
- **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_04\_14
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1567 Exfiltration Over Web Service](#)
- **MD5:** 06635111468af8497979f05ccd5bc2ea
- **2061025 - ET MALWARE Specter Insight Beacon CnC Checkin M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1567 Exfiltration Over Web Service](#)
  - **MD5:** 612e27b5df944f1591bfc5d1bc17a153
- **2061200 - ET MALWARE Aurotun Stealer CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 73e43654e9f3df0d07d25051b2d3cfeb
- **2061460 - ET MALWARE Trox Stealer System Profiling Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_21
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2061542 - ET MALWARE DuvetStealer C2 (send-zip) Traffic Outbound**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_04\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2061543 - ET MALWARE DuvetStealer C2 (send-token) Traffic Outbound**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2061600 - ET MALWARE DeerStealer Websocket Initial Request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2061601 - ET MALWARE PureLogs GZIP Exfiltration Outbound**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1048 Exfiltration Over Alternative Protocol](#)
- **2061614 - ET MALWARE SNOWLIGHT C2 HTTP Requests**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2062154 - ET MALWARE VKeylogger CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 5787ea8e8245606f5058f20179a82683
- **2062246 - ET MALWARE RedExt C2 Agent Register**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2062247 - ET MALWARE RedExt C2 Agent Exfiltration**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2062248 - ET MALWARE RedExt C2 Agent Beacon**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_05\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2062540 - ET MALWARE APT28 Russia Macro Loader HTTP POST**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_06\_12
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1018 Remote System Discovery](#)
  - **MD5:** 919d1c4abd151525ec71d431f781306c
- **2062548 - ET MALWARE HATVIBE.loader Russia APT28 HTTP PUT Request**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_06\_12
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1018 Remote System Discovery](#)
- **2062713 - ET MALWARE JanelaRAT Staging URL**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_06\_12
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2062775 - ET MALWARE Diamotrix Clipper POST Request M1**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** e18aa4df483848a5d072b14bc00eeb45
- **2062776 - ET MALWARE Diamotrix Clipper POST Request M2**
- **Category:** Malware

- **Severity:** Major
- **Date Added:** 2025\_07\_01
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **MD5:** 855e10df6346634ba680ecef86e68ae8
- **2062807 - ET MALWARE Observed GET Request to ClickFix Style URI**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2062808 - ET MALWARE Observed GET Request to ClickFix Style URI**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2063121 - ET MALWARE Diamotrix POST Request M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 0e439843e068d7f1055ec05e03483d27
- **2063162 - ET MALWARE KimJongRAT Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_07\_01
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2063163 - ET MALWARE KimJongRAT CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_01
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2063215 - ET MALWARE PureLogs C2 Server Connection M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** d2c7a610447b218577c31acdf008070b
- **2063239 - ET MALWARE BitterAPT Kiwi2.0 Data Exfiltration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2063264 - ET MALWARE Myth Stealer Data Exfiltration Attempt M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_07\_16
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0010 Exfiltration](#)
- **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2063580 - ET MALWARE Rainbow Hyena Backdoor PhantomRemote (poll) C2 Traffic**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_08\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2063581 - ET MALWARE Rainbow Hyena Backdoor PhantomRemote (result) C2 Traffic**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_08\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2063872 - ET MALWARE Storm-2603 AK47C2 HTTP Backdoor CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2064003 - ET MALWARE CastleLoader User-Agent Observed**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 835ab1cf597812b0e6464c2e8f100678

- **2064004 - ET MALWARE CastleBot CnC Checkin (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 835ab1cf597812b0e6464c2e8f100678
- **2064005 - ET MALWARE CastleLoader CnC Exfil (POST)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 835ab1cf597812b0e6464c2e8f100678
- **2064006 - ET MALWARE CastleLoader Payload Request (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive by Compromise](#)
  - **MD5:** 835ab1cf597812b0e6464c2e8f100678
- **2064007 - ET MALWARE CastleLoader Task Complete in URI (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)

- **MD5:** 835ab1cf597812b0e6464c2e8f100678
- **2064010 - ET MALWARE Vidar Stealer User-Agent Observed**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2064143 - ET MALWARE KoiStealer Payload Request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2064234 - ET MALWARE FakeBooking Payload CnC Activity (upd)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2c29c8685f422db066601de0a8e55ee7
- **2064235 - ET MALWARE FakeBooking Payload CnC Activity (dllstart)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2c29c8685f422db066601de0a8e55ee7

- **2064236 - ET MALWARE FakeBooking Payload CnC Activity (apif)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 2c29c8685f422db066601de0a8e55ee7
- **2064288 - ET MALWARE Quad7 Botnet UPDTAE Backdoor CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2064292 - ET MALWARE Quad7 Botnet - Outbound rlogin Telnet Prompt from Compromised Endpoint**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2064293 - ET MALWARE Quad7 Botnet - Outbound alogin Telnet Prompt from Compromised Endpoint**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)

• **2064294 - ET MALWARE Quad7 Botnet - Outbound zylogin Telnet Prompt from Compromised Endpoint**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2025\_11\_04
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)

• **2064452 - ET MALWARE Kimsuky/TA406 Payload Request (GET)**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2025\_11\_04
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1105 Ingress Tool Transfer](#)
- **MD5:** 6d18166da354efacd541bcac622a6e43

• **2064539 - ET MALWARE TinyNuke Checkin via Telegram**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2025\_11\_17
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2064627 - ET MALWARE Oyster Backdoor CnC Checkin M2**

- **Category:** Malware
- **Severity:** Major
- **Date Added:** 2025\_11\_17
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2064628 - ET MALWARE Oyster Backdoor CnC Checkin M3**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2064629 - ET MALWARE Oyster Backdoor CnC Checkin M4**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2064802 - ET MALWARE Filch Stealer CnC Checkin**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 5e13fd50160acfc9c40de6c3b0f43c11
- **2064816 - ET MALWARE Prince Ransomware GET Wallpaper M1**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1486 Data Encrypted for Impact](#)
- **2064817 - ET MALWARE Prince Ransomware GET Wallpaper M2**
- **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_11\_17
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0040 Impact](#)
  - **Technique:** [T1486 Data Encrypted for Impact](#)
- **2064818 - ET MALWARE Prince Ransomware GET Wallpaper M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1486 Data Encrypted for Impact](#)
- **2065044 - ET MALWARE JS/FatturaPDF CnC Checkin (GET)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** a69f4744a2247f2b0a61f488407d36c1
- **2065234 - ET MALWARE UNK\_MysteriousElephant CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 43073b67b9c6c091bf0d0240df05ed04
- **2065380 - ET MALWARE Valkyrie Stealer Data Exfiltration Attempt M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **MD5:** 7592ee0bba0c9cae1e26de5e3a9675ef
- **2065384 - ET MALWARE Shark Stealer CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8ec92ce467117d0616d9728c3141004c
- **2065385 - ET MALWARE Valkyrie Stealer Data Exfiltration Attempt M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 7592ee0bba0c9cae1e26de5e3a9675ef
- **2065564 - ET MALWARE SearchLoader CnC Beacon**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_17
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065649 - ET MALWARE TA398 CurlBack\_RAT CnC Activity - Fetch Commands M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2065650 - ET MALWARE TA398 CurlBack\_RAT CnC Activity - Upload Results**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2065803 - ET MALWARE SilentSync-RAT CNC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065804 - ET MALWARE SilentSync-RAT Tasking request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2065805 - ET MALWARE SilentSync-RAT CnC Tasking response**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)

- **2065806 - ET MALWARE SilentSync-RAT CnC file tasking request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_11\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2065863 - ET MALWARE OtterCookie File Exfiltration M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_12\_02
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2065905 - ET MALWARE WallStealer Data Exfiltration Attempt over Telegram**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_12\_02
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1567 Exfiltration Over Web Service](#)
  - **MD5:** cb6e677a00a47c9274ceb774acced905
- **2066251 - ET MALWARE PeerBlight BitTorrent DHT CnC Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_12\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **2066336 - ET MALWARE SantaStealer Data Exfiltration Attempt**
  - **Category:** Malware

- **Severity:** Major
- **Date Added:** 2025\_12\_22
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0010 Exfiltration](#)
  - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2066361 - ET MALWARE ZeitLoader Payload Retrieval attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_12\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
  - **MD5:** eb5bd49b6eef60ff85892ef7c8015b01
- **2066365 - ET MALWARE ZeitLoader IP Address Check User-Agent (TimeClient/1.0)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_12\_30
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** eb5bd49b6eef60ff85892ef7c8015b01
- **2066686 - ET MALWARE GhostPenguin C2 Beacon Observed**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_01\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0037 Command And Control](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
  - **MD5:** 7d3bd0d04d3625322459dd9f11cc2ea3
- **2067267 - ET MALWARE PulsarRAT CnC Traffic Observed**
  - **Category:** Malware

- **Severity:** Major
- **Date Added:** 2026\_02\_19
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0037 Command And Control](#)
  - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **MD5:** 69392e0d2b877cb932ab709ebe758975
- **2067339 - ET MALWARE DesckVB RAT DetectaAV Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8f2f2b1a5666036ef7be2cd4d42eb281
- **2067340 - ET MALWARE DesckVB RAT Ping Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8f2f2b1a5666036ef7be2cd4d42eb281
- **2067341 - ET MALWARE DesckVB RAT BlugPass Checkin**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8f2f2b1a5666036ef7be2cd4d42eb281
- **2067343 - ET MALWARE DesckVB RAT BlugPass Checkin - Webcam Enumeration**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8f2f2b1a5666036ef7be2cd4d42eb281
- **2067345 - ET MALWARE DesckVB RAT D ping request/response**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **MD5:** 8f2f2b1a5666036ef7be2cd4d42eb281
- **2067367 - ET MALWARE Marco Stealer Data Exfiltration Attempt**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_02\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)
    - **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **2068452 - ET MALWARE Observed Python Stealer User-Agent (WhatsAppBackup/1.0) Outbound**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2068503 - ET MALWARE Crpx0 Ransomware Payload Request M1**
- **Category:** Malware

- **Severity:** Major
- **Date Added:** 2026\_04\_20
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2068504 - ET MALWARE Crpx0 Ransomware Payload Request M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2068505 - ET MALWARE Crpx0 Ransomware Payload Request M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2068506 - ET MALWARE Crpx0 Ransomware Payload Request M4**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2068518 - ET MALWARE plain-crypto-js RAT Stage 2 C2 Outbound Request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 9663665850cdd8fe12e30a671e5c4e6f
- **2068519 - ET MALWARE plain-crypto-js RAT Stage 1 C2 Outbound Request**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 089e2872016f75a5223b5e02c184dfec
- **2068716 - ET MALWARE XorBee RAT CNC Checkin M1**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **2068765 - ET MALWARE ShadowLink IoT Botnet Socks Proxy Registration Attempt**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2026\_04\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2023333 - ET MALWARE Linux.Mirai Login Attempt (xc3511)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- Technique: [T1573 Encrypted Channel](#)
- **2023430 - ET MALWARE Possible Linux.Mirai Login Attempt (1111111)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1573 Encrypted Channel](#)
- **2023431 - ET MALWARE Possible Linux.Mirai Login Attempt (54321)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0006 Credential Access](#)
    - Technique: [T1110 Brute Force](#)
- **2023432 - ET MALWARE Possible Linux.Mirai Login Attempt (666666)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0006 Credential Access](#)
    - Technique: [T1110 Brute Force](#)
- **2023433 - ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0admin)**
  - Category: Malware
  - Severity: Major
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0006 Credential Access](#)
    - Technique: [T1110 Brute Force](#)
- **2023434 - ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0vizxv)**
  - Category: Malware

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0006 Credential Access](#)
  - **Technique:** [T1110 Brute Force](#)
- **2023435 - ET MALWARE Possible Linux.Mirai Login Attempt (888888)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023436 - ET MALWARE Possible Linux.Mirai Login Attempt (anko)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023437 - ET MALWARE Possible Linux.Mirai Login Attempt (dreambox)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023438 - ET MALWARE Possible Linux.Mirai Login Attempt (fucker)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0006 Credential Access](#)
- **Technique:** [T1110 Brute Force](#)
- **2023439 - ET MALWARE Possible Linux.Mirai Login Attempt (hi3518)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023440 - ET MALWARE Possible Linux.Mirai Login Attempt (ikwb)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023441 - ET MALWARE Possible Linux.Mirai Login Attempt (juantech)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023442 - ET MALWARE Possible Linux.Mirai Login Attempt (jvbzd)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023443 - ET MALWARE Possible Linux.Mirai Login Attempt (klv123)**

- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023444 - ET MALWARE Possible Linux.Mirai Login Attempt (klv1234)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023445 - ET MALWARE Possible Linux.Mirai Login Attempt (meinsm)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023446 - ET MALWARE Possible Linux.Mirai Login Attempt (realtek)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023447 - ET MALWARE Possible Linux.Mirai Login Attempt (service)**
- **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0006 Credential Access](#)
  - **Technique:** [T1110 Brute Force](#)
- **2023448 - ET MALWARE Possible Linux.Mirai Login Attempt (ubnt)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023449 - ET MALWARE Possible Linux.Mirai Login Attempt (vizxv)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023450 - ET MALWARE Possible Linux.Mirai Login Attempt (xmhdipc)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023451 - ET MALWARE Possible Linux.Mirai Login Attempt (zlxx)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)

- **2023452 - ET MALWARE Possible Linux.Mirai Login Attempt (Zte521)**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023674 - ET MALWARE Possible Linux.Mirai DaHua Default Credentials Login**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2027366 - ET MALWARE Mirai Variant Checkin Response**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2035940 - ET MALWARE Fodcha Bot CnC Client Heartbeat**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2060436 - ET MALWARE Observed Malicious SSL Cert Associated with PolarEdge Botnet M1**
  - **Category:** Malware
  - **Severity:** Major

- **Date Added:** 2025\_04\_14
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1573 Encrypted Channel](#)
- **2060437 - ET MALWARE Observed Malicious SSL Cert Associated with PolarEdge Botnet M2**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2060438 - ET MALWARE Observed Malicious SSL Cert Associated with PolarEdge Botnet M3**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2060439 - ET MALWARE Observed Malicious SSL Cert Associated with PolarEdge Botnet M4**
  - **Category:** Malware
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1573 Encrypted Channel](#)
- **2045753 - ET RETIRED Camaro Dragon APT - Horse Shell CnC Checkin**
  - **Category:** Retired
  - **Severity:** Major
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2051806 - ET RETIRED TheMoon CnC Checkin**
  - **Category:** Retired
  - **Severity:** Major
  - **Date Added:** 2025\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2008542 - ET SCADA CitectSCADA ODBC Overflow Attempt**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2008-2639](#)
- **2011976 - ET SCADA RealWin SCADA System Buffer Overflow**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2012096 - ET SCADA DATAC RealWin SCADA Server Buffer Overflow**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2008-4322](#)

- **2012787 - ET SCADA ICONICS WebHMI ActiveX Stack Overflow**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013074 - ET SCADA DATAC RealWin SCADA Server 2 On\_FC\_CONNECT\_FCS\_a\_FILE Buffer Overflow Vulnerability**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013120 - ET SCADA Siemens FactoryLink 8 CSService Logging Buffer Overflow Vulnerability**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013235 - ET SCADA Golden FTP Server PASS Command Remote Buffer Overflow Attempt**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013730 - ET SCADA PcVue Activex Control Insecure method (AddPage)**
  - **Category:** SCADA

- **Severity:** Major
- **Date Added:** 2024\_02\_07
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1659 Content Injection](#)
- **2013731 - ET SCADA PcVue Activex Control Insecure method (DeletePage)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013732 - ET SCADA PcVue Activex Control Insecure method (SaveObject)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013733 - ET SCADA PcVue Activex Control Insecure method (LoadObject)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013734 - ET SCADA PcVue Activex Control Insecure method (GetExtendedColor)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1659 Content Injection](#)
- **2013735 - ET SCADA Sunway ForceControl Activex Control Vulnerability**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013736 - ET SCADA Sunway ForceControl Activex Control Remote Code Execution Vulnerability 2**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013878 - ET SCADA PROMOTIC ActiveX Control Insecure method (SaveCfg)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2013879 - ET SCADA PROMOTIC ActiveX Control Insecure method (AddTrend)**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)

- **2026003 - ET SCADA SEIG SYSTEM 9 - Remote Code Execution**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2013-0657](#)
- **2026005 - ET SCADA SEIG Modbus 3.4 - Remote Code Execution**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2013-0662](#)
- **2049795 - ET SCADA Rockwell RNA Message Large Header Length - 8Kb**
  - **Category:** SCADA
  - **Severity:** Major
  - **Date Added:** 2024\_02\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2026008 - ET SCAN Geutebrueck re\_reporter 7.8.974.20 Information Disclosure**
  - **Category:** SCAN
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1082 System Information Discovery](#)
  - **CVE:** [2018-15534](#)

- **2026015 - ET SCAN Hikvision IP Camera 5.4.0 Information Disclosure**
  - **Category:** SCAN
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0007 Discovery](#)
    - **Technique:** [T1082 System Information Discovery](#)
- **2021024 - ET SCAN Nmap NSE Heartbleed Response**
  - **Category:** SCAN
  - **Severity:** Major
  - **Date Added:** 2023\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1595 Active Scanning](#)
- **2023102 - ET SCAN OpenVASVT RCE Test String in HTTP Request Outbound**
  - **Category:** SCAN
  - **Severity:** Major
  - **Date Added:** 2023\_07\_24
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1595 Active Scanning](#)
- **2001891 - ET USER\_AGENTS Suspicious User Agent (agent)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2005320 - ET USER\_AGENTS Suspicious User-Agent (MyAgent)**
  - **Category:** User\_Agents
  - **Severity:** Major

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2006388 - ET USER\_AGENTS Suspicious User-Agent (006)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2008460 - ET USER\_AGENTS Suspicious User-Agent (hacker)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2012611 - ET USER\_AGENTS Suspicious User-Agent Sample**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2012619 - ET USER\_AGENTS Suspicious User-Agent Mozilla/3.0**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- **Technique:** [T1071 Application Layer Protocol](#)
- **2012751 - ET USER\_AGENTS suspicious user agent string (changhuatong)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2012757 - ET USER\_AGENTS suspicious user agent string (ChoITBAgent)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2013967 - ET USER\_AGENTS Suspicious User-Agent (adlib)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2017067 - ET USER\_AGENTS Suspicious user agent (Google page)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2033269 - ET USER\_AGENTS WaterDropX PRISM UA Observed**
  - **Category:** User\_Agents

- **Severity:** Major
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2033314 - ET USER\_AGENTS Observed Malicious User-Agent (Brute Force Attacks)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2033315 - ET USER\_AGENTS Observed Malicious User-Agent (Brute Force Attacks)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2033665 - ET USER\_AGENTS sysWeb User-Agent**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 3f295401fa59a32ff7a11551551ec607
- **2034244 - ET USER\_AGENTS Suspicious User-Agent (Embarcadero URI Client/1.0)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** c0e620ed4e96aa1fe8452a3f8b7e2e8d
- **2035537 - ET USER\_AGENTS Observed Malicious User-Agent (CobaltStrike)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1001 Data Obfuscation](#)
  - **MD5:** b8b7a10dcc0dad157191620b5d4e5312
- **2037737 - ET USER\_AGENTS DanaBot Specific UA Observed**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2037828 - ET USER\_AGENTS Suspicious User-Agent (56)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** c9ee1d6a90be7524b01814f48b39b232
- **2038482 - ET USER\_AGENTS ErbiumStealer UA Observed**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2038702 - ET USER\_AGENTS Suspicious User-Agent (RestoroMainExe)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 39fef85fe114d96dde745b8ce0659b2e
- **2038726 - ET USER\_AGENTS Suspicious User-Agent (Testing)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2038731 - ET USER\_AGENTS Suspicious User-Agent (xfilesreborn)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** ba542a8d1d21e2016ade340fdc08d1a4
- **2039832 - ET USER\_AGENTS Observed Malicious VBS Related UA**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **MD5:** 2a90a42a4f379fb4a28bb32a96f8fc0f
- **2044168 - ET USER\_AGENTS Observed DonotGroup Related UA (Chrome Edge)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 79cff3bc3cbe51e1b3fec131b949930
- **2045158 - ET USER\_AGENTS Win32/FakeAV InternetSecurityGuard User-Agent**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 054139bbb3748d0b8d393ab438e3a050
- **2046057 - ET USER\_AGENTS Suspicious User Agent (Zadanie)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2046893 - ET USER\_AGENTS Kimsuky CnC Checkin User-Agent**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **2066620 - ET USER\_AGENTS Installer Analytics User Agent (AdvinstAnalytics)**
  - **Category:** User\_Agents
  - **Severity:** Major
  - **Date Added:** 2026\_01\_20
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1496 Resource Hijacking](#)
- **2066511 - ET WEB\_SPECIFIC\_APPS GeoVision GV-ASWeb <=v6.1.2.0 RCE (CVE-2025-26264)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2026\_01\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2025-26264](#)
- **2026009 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 1**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
  - **CVE:** [2018-15533](#)
- **2026010 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 2**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)

- **Technique:** [T1189 Drive-by Compromise](#)
- **CVE:** [2018-15533](#)
- **2026011 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 3**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
  - **CVE:** [2018-15533](#)
- **2026012 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 4**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
  - **CVE:** [2018-15533](#)
- **2026013 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 5**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive-by Compromise](#)
  - **CVE:** [2018-15533](#)
- **2026014 - ET WEB\_SPECIFIC\_APPS Geutebrueck re\_porter 16 - Cross-Site Scripting 6**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1189 Drive-by Compromise](#)
- **CVE:** [2018-15533](#)
- **2049214 - ET WEB\_SPECIFIC\_APPS Zoneminder Create Snapshot Command Injection Attempt (CVE-2023-26035)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2023\_12\_11
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2023-26035](#)
- **2059683 - ET WEB\_SPECIFIC\_APPS Reolink RLC Series IP Camera TestEmail Authenticated Command Injection Attempt (CVE-2019-11001)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2019-11001](#)
- **2059709 - ET WEB\_SPECIFIC\_APPS Reolink RLC Series IP Camera SetDdns Authenticated Command Injection Attempt (CVE-2021-40407, CVE-2021-40408, CVE-2021-40409)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2021-40407](#)
- **2059712 - ET WEB\_SPECIFIC\_APPS Reolink RLC Series IP Camera SetLocalLink Authenticated Command Injection Attempt (CVE-2021-40410, CVE-2021-40411)**

- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2021-40410](#)
- **2059717 - ET WEB\_SPECIFIC\_APPS Reolink RLC Series IP Camera SetDevName Authenticated Command Injection Attempt (CVE-2021-40412)**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2021-40412](#)
- **2061111 - ET WEB\_SPECIFIC\_APPS TBK DVR-4104/4216 Command Injection Attempt (CVE-2024-3721)**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_04\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-3721](#)
- **2061774 - ET WEB\_SPECIFIC\_APPS Yi IOT XY-3820 Daemon Service Directory Traversal Attempt**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_05\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0010 Exfiltration](#)

- **Technique:** [T1041 Exfiltration Over C2 Channel](#)
- **CVE:** [2025-29660](#)
- **2061775 - ET WEB\_SPECIFIC\_APPS Yi IOT XY-3820 cmd Service Unauthenticated Remote Code Execution Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_05\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1095 Non-Application Layer Protocol](#)
  - **CVE:** [2025-29659](#)
- **2062137 - ET WEB\_SPECIFIC\_APPS DigiEver DS-2105 Pro time\_tzsetup.cgi ntp Parameter Command Injection Attempt (CVE-2023-52163)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_05\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2023-52163](#)
- **2062140 - ET WEB\_SPECIFIC\_APPS GeoVision DateSetting.cgi szSrvIpAddr Parameter Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_05\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2024-6047](#)
- **2063891 - ET WEB\_SPECIFIC\_APPS Ilevia EVE X1 Server Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major

- **Date Added:** 2025\_11\_04
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public Facing Application](#)
- **2063894 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect Unauthenticated DeploymentServlet Request Type DeploySource Directory Traversal and Arbitrary File Upload Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063903 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect Guest login Privilege Escalation M1**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1078 Valid Accounts](#)
- **2063904 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect Guest login Privilege Escalation M2**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1078 Valid Accounts](#)
- **2063906 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect logYumLookup logfile Parameter Authenticated Directory Traversal Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0009 Collection](#)
- **Technique:** [T1005 Data from Local System](#)
- **2063908 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect ProjectUpdateBSXFileProcess.php Authenticated Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063909 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect logMixDownload instance Parameter Authenticated Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063919 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect productRemovalUpdate instance Parameter Authenticated Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063936 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect Unauthenticated IPConfigServlet Manipulation Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1659 Content Injection](#)
- **2063937 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect Unauthenticated NTPServlet Manipulation Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **2063938 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect HTTPDownloadServlet Unauthenticated Arbitrary File Deletion Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1485 Data Destruction](#)
- **2063939 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect DeploymentServlet DeployJars/DeployRuntimeJars Parameter Unauthenticated Directory Traversal and Arbitrary File Upload Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
- **2063944 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect HTTPDownloadServlet Unauthenticated Arbitrary Directory Traversal and File Upload Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1190 Exploit Public Facing Application](#)
- **2063945 - ET WEB\_SPECIFIC\_APPS ABB Cylon FLXeon Capture.js Authenticated Arbitrary File Read and Deletion Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
- **2063949 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon siteGuide.js filename/originalname Parameter Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2063950 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon users.js oldPassword/newPassword Parameter Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1555 Credentials from Password Stores](#)
- **2063951 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon cert.js Multiple Parameters Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0003 Persistence](#)
- **Technique:** [T1505 Server Software Component](#)
- **2063952 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon timeConfig.js Multiple Parameters Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0005 Defense Evasion](#)
    - **Technique:** [T1070 Indicator Removal](#)
- **2063953 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon upload.js Multiple Parameters Command Injection Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2063964 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon siteGuide.js filename Parameter Directory Traversal Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_04
- **2064684 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect multiple caldav URI endpoints skipChecksum Parameter Arbitrary File Upload Attempt**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0003 Persistence](#)
    - **Technique:** [T1105 Ingress Tool Transfer](#)
- **2064685 - ET WEB\_SPECIFIC\_APPS ABB Cylon Fixeon factorySaved.php title Parameter Cross Site Scripting Attempt**

- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1189 Drive by Compromise](#)
- **2064711 - ET WEB\_SPECIFIC\_APPS LG WebOS getFile path Parameter Directory Traversal Attempt**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2026\_01\_13
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
- **2065002 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect 3.08.02 Arbitrary Heap Memory Configuration (CVE-2024-51544)**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0005 Defense Evasion](#)
    - **Technique:** [T1562 Impair Defenses](#)
  - **CVE:** [2024-51544](#)
- **2065034 - ET WEB\_SPECIFIC\_APPS ABB Cylon Aspect 3.07.00 Remote Code Execution**
- **Category:** Web\_Specific\_Apps
  - **Severity:** Major
  - **Date Added:** 2025\_11\_25
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2065916 - ET WEB\_SPECIFIC\_APPS Shenzhen TVT NVMS-9000 Information Disclosure Attempt (CVE-2024-14007)**

- **Category:** Web\_Specific\_Apps
- **Severity:** Major
- **Date Added:** 2025\_12\_02
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1190 Exploit Public Facing Application](#)
- **CVE:** [2024-14007](#)
- **2010643 - ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt**
  - **Category:** Scan
  - **Severity:** Major
  - **Date Added:** 2023\_12\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023016 - ET HUNTING SUSPICIOUS Path to BusyBox**
  - **Category:** Hunting
  - **Severity:** Major
  - **Date Added:** 2023\_12\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2023019 - ET TELNET busybox MIRAI hackers - Possible Brute Force Attack**
  - **Category:** Telnet
  - **Severity:** Major
  - **Date Added:** 2023\_12\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0006 Credential Access](#)
    - **Technique:** [T1110 Brute Force](#)
- **2030919 - ET MALWARE Mozi Botnet DHT Config Sent**
  - **Category:** Malware

- **Severity:** Major
- **Date Added:** 2024\_01\_30
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command and Control](#)
  - **Technique:** [T1095 Non-Application Layer Protocol](#)
- **MD5:** 5616a3471565d34d779b5b3d0520bb70
- **2035718 - ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M1**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2022-0543](#)
- **2035719 - ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M2**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public Facing Application](#)
  - **CVE:** [2022-0543](#)
- **2035720 - ET EXPLOIT Possible Redis RCE Attempt - Dynamic Importing of liblua (CVE-2022-0543)**
  - **Category:** Exploit
  - **Severity:** Major
  - **Date Added:** 2024\_02\_07
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2022-0543](#)

• **2047954 - ET WEB\_SPECIFIC\_APPS Apache RocketMQ 5.1.0 Arbitrary Code Injection in Broker Config (CVE-2023-33246)**

- **Category:** Web\_Specific\_Apps
- **Severity:** Major
- **Date Added:** 2023\_12\_11
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1659 Content Injection](#)
- **CVE:** [2023-33246](#)

**SEVERITY: Minor**

*SIGNATURE ID - MESSAGE*

---

• **8800001 - CP EXPLOIT Possible Malicious Binary File (EICAR)**

- **Category:** Exploit
- **Severity:** Minor
- **Date Added:** 2023\_08\_22
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Initial Access](#)
  - **Technique:** [T1566 Phishing](#)

• **8800002 - CP ATTACK\_RESPONSE id check returned root -1**

- **Category:** Attack\_Response
- **Severity:** Minor
- **Date Added:** 2023\_09\_29
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0043 Reconnaissance](#)
  - **Technique:** [T1592 Gather Victim Host Information](#)

• **8800003 - CP ATTACK\_RESPONSE id check returned root -2**

- **Category:** Attack\_Response
- **Severity:** Minor
- **Date Added:** 2023\_09\_29
- **MITRE ATT&CK®:**

- **Tactic:** [TA0043 Reconnaissance](#)
- **Technique:** [T1592 Gather Victim Host Information](#)
- **8800004 - CP ATTACK\_RESPONSE id check returned root -3**
  - **Category:** Attack\_Response
  - **Severity:** Minor
  - **Date Added:** 2023\_11\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1592 Gather Victim Host Information](#)
- **8800013 - CP MALWARE Lilin Scanner Remote Code Execution Attempt**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_01\_11
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1659 Content Injection](#)
- **8800018 - CP MALWARE NoaBot Botnet Scanner**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_02\_23
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **8800001 - CP EXPLOIT Possible Malicious Binary File (EICAR)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_08\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
- **8800002 - CP ATTACK\_RESPONSE id check returned root -1**

- **Category:** Attack\_Response
- **Severity:** Minor
- **Date Added:** 2023\_09\_29
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0043 Reconnaissance](#)
  - **Technique:** [T1592 Gather Victim Host Information](#)
- **8800003 - CP ATTACK\_RESPONSE id check returned root -2**
  - **Category:** Attack\_Response
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_29
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1592 Gather Victim Host Information](#)
- **8800004 - CP ATTACK\_RESPONSE id check returned root -3**
  - **Category:** Attack\_Response
  - **Severity:** Minor
  - **Date Added:** 2023\_11\_16
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1592 Gather Victim Host Information](#)
- **8800010 - CP EXPLOIT InfectedSlurs 0day Exploit Attempt #1**
  - **Category:** EXPLOIT
  - **Severity:** Minor
  - **Date Added:** 2024\_01\_11
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2023-49897](#)
- **8800011 - CP EXPLOIT InfectedSlurs 0day Exploit Attempt #2**
  - **Category:** EXPLOIT
  - **Severity:** Minor

- **Date Added:** 2024\_01\_11
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command and Control](#)
  - **Technique:** [T1659 Content Injection](#)
- **8800012 - CP EXPLOIT QNAP VioStor InfectedSlurs Exploitation Attempt #3**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2024\_01\_11
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command and Control](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2023-47565](#)
- **2020084 - ET ATTACK\_RESPONSE Microsoft Powershell Banner Outbound**
  - **Category:** Attack\_Response
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2038605 - ET ATTACK\_RESPONSE Nishang Invoke-PowerShellTcp Shell Prompt Outbound**
  - **Category:** Attack\_Response
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
- **2024913 - ET EXPLOIT D-Link 850L Password Extract Attempt**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0007 Discovery](#)
- **Technique:** [T1082 System Information Discovery](#)
- **2025882 - ET EXPLOIT MVPower DVR Shell UCE MSF Check**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2025884 - ET EXPLOIT Multiple CCTV-DVR Vendors RCE**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2029155 - ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2019-18396](#)
- **2029157 - ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)

- **Technique:** [T1203 Exploitation for Client Execution](#)
- **2029159 - ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2019-16072](#)
- **2029161 - ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2029163 - ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2017-16602](#)
- **2029165 - ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)

- **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2017-6316](#)
- **2029167 - ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2013-5192](#)
- **2029169 - ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2029171 - ET EXPLOIT 3Com Office Connect Remote Code Execution (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2029173 - ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)

- **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2006-4000](#)
- **2029175 - ET EXPLOIT CCBill Online Payment Systems RCE (Inbound)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2029207 - ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Inbound (CVE-2019-7256)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2019-7256](#)
- **2030276 - ET EXPLOIT Fastweb Fastgate 0.00.81 - Remote Code Execution**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2030277 - ET EXPLOIT Multiple DLink Routers Remote Code Execution CVE-2019-16920**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)

- **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **CVE:** [2019-16920](#)
- **2030278 - ET EXPLOIT Netis WF2419 2.2.36123 - Remote Code Execution CVE-2019-19356**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - **CVE:** [2019-19356](#)
- **2030309 - ET EXPLOIT Wireless IP Camera (P2) WIFICAM Remote Code Execution**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
- **2030310 - ET EXPLOIT ASUS RT-N56U/RT-AC66U Remote Code Execution**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
- **2030311 - ET EXPLOIT Mi Router 3 Remote Code Execution CVE-2018-13023**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)

- CVE: [2018-13023](#)
- **2030312 - ET EXPLOIT Mi TV Integration Remote Code Execution CVE-2018-16130**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - CVE: [2018-16130](#)
- **2030317 - ET EXPLOIT LG SuperSign EZ CMS 2.5 Remote Code Execution CVE-2018-17173**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0004 Privilege Escalation](#)
    - **Technique:** [T1068 Exploitation for Privilege Escalation](#)
  - CVE: [2018-17173](#)
- **2032077 - ET EXPLOIT ZTE Cable Modem RCE Attempt (CVE-2014-2321)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1190 Exploit Public-Facing Application](#)
  - CVE: [2014-2321](#)
- **2041450 - ET EXPLOIT Xiongmai/HiSilicon DVR - Request for Product Details Possible CVE-2017-7577 Exploit Attempt**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0002 Execution](#)
- **Technique:** [T1203 Exploitation for Client Execution](#)
- **CVE:** [2017-7577](#)
- **2041451 - ET EXPLOIT Xiongmai/HiSilicon DVR - Request for User Details - Possible CVE-2017-7577 Exploit Attempt**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1203 Exploitation for Client Execution](#)
  - **CVE:** [2017-7577](#)
- **2048547 - ET EXPLOIT Tenda G103 Command Injection Attempt (CVE-2023-27076)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_11\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
  - **CVE:** [2023-27076](#)
- **2048549 - ET EXPLOIT DCN DCBI-Netlog-LAB Remote Code Execution Vulnerability Attempt (CVE-2023-26802)**
  - **Category:** Exploit
  - **Severity:** Minor
  - **Date Added:** 2023\_11\_03
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0002 Execution](#)
    - **Technique:** [T1059 Command and Scripting Interpreter](#)
  - **CVE:** [2023-26802](#)
- **2015675 - ET EXPLOIT\_KIT SimpleTDS go.php (sid)**
  - **Category:** Exploit\_Kit
  - **Severity:** Minor

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0001 Execution](#)
  - **Technique:** [T1189 Drive-by Compromise](#)
- **2048464 - ET FTP Vulnerable WS\_FTP Version in FTP Banner Response (CVE-2023-40044)**
  - **Category:** FTP
  - **Severity:** Minor
  - **Date Added:** 2023\_11\_06
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1592 Gather Victim Host Information](#)
  - **CVE:** [2023-40044](#)
- **2029011 - ET HUNTING Generic IOT Downloader Malware in POST (Inbound)**
  - **Category:** Hunting
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
- **2029012 - ET HUNTING Generic IOT Downloader Malware in GET (Inbound)**
  - **Category:** Hunting
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1566 Phishing](#)
- **2029590 - ET HUNTING Generic IOT Downloader Malware in GET (Inbound)**
  - **Category:** Hunting
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0001 Initial Access](#)
- **Technique:** [T1566 Phishing](#)
- **2027120 - ET MALWARE ELF/Mirai Variant UA Inbound (Rift)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027122 - ET MALWARE ELF/Mirai Variant UA Inbound (Tsunami)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027124 - ET MALWARE ELF/Mirai Variant UA Inbound (Yowai)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027126 - ET MALWARE ELF/Mirai Variant UA Inbound (Yakuza)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027128 - ET MALWARE ELF/Mirai Variant UA Inbound (Hentai)**

- **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027130 - ET MALWARE ELF/Mirai Variant UA Inbound (lessie)**
- **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027132 - ET MALWARE ELF/Mirai Variant UA Inbound (Cakle)**
- **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027134 - ET MALWARE ELF/Mirai Variant UA Inbound (Damien)**
- **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027136 - ET MALWARE ELF/Mirai Variant UA Inbound (Solar)**
- **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2027138 - ET MALWARE ELF/Mirai Variant UA Inbound (muhstik)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2027140 - ET MALWARE ELF/Mirai Variant UA Inbound (Shaolin)**
  - **Category:** Malware
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2048624 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - TCP Statistics**
  - **Category:** SCADA
  - **Severity:** Minor
  - **Date Added:** 2024\_02\_23
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1592 Gather Victim Host Information](#)
- **2048625 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - UDP Statistics**
  - **Category:** SCADA
  - **Severity:** Minor
  - **Date Added:** 2024\_02\_23
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)

- Technique: [T1590 Gather Victim Host Information](#)
- **2048626 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation System Data Details Information Disclosure Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048627 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IP Routing Data**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048628 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - General Memory Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048629 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - General Heap Memory Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)

- Technique: [T1590 Gather Victim Host Information](#)
- **2048630 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - ICMP Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048631 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IGMP Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048632 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - ARP Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048633 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - Interface Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)

- Technique: [T1590 Gather Victim Host Information](#)
- **2048634 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IP Statistics**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048635 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Possible Unauthorized Access Attempt - Request for radevice.css**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048636 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - System List**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048637 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Browse Chasis**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)

- Technique: [T1590 Gather Victim Host Information](#)
- **2048638 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Chassis Detail Request**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048639 - ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Crashdump Display**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048640 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access - Request for home.sel**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1590 Gather Victim Host Information](#)
- **2048641 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access Attempt - Request for err401.sel**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1659 Content Injection](#)
- **2048642 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access - Request for default.sel**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048643 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Possible Unauthorized Access Attempt - Request for /scripts/dScripts.sel**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048644 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Possible Unauthorized Access Attempt - Request for /css/sel.css**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048645 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Dropbear SSH Banner - Possible SSH Login attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1078 Valid Accounts](#)
- **2048646 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-3530-RTAC AcSELeRator Firmware Activity**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1078 Valid Accounts](#)
- **2048667 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL 2032 Processor Telnet Banner**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0043 Reconnaissance](#)
    - Technique: [T1595 Active Scanning](#)
- **2048668 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL Calibration Access Level Login Success**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0004 Privilege Escalation](#)
    - Technique: [T1078 Valid Accounts](#)
- **2048669 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Access Change**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_23
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1659 Content Injection](#)
- **2048670 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Change working directory 2701**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048671 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Current directory /SEL-2701**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048672 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - DNPMPA.TXT File Download Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048673 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - STOR SET\_DNP1.TXT File Upload Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1659 Content Injection](#)
- **2048674 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET\_ File Upload Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048675 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - User ACC Login Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048676 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default Password otter**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048677 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - DNPMPA.TXT File Upload Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1659 Content Injection](#)
- **2048678 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - ERR.TXT File Download Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048679 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET\_DNP1.TXT File Download Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048680 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET\_ File Download Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048681 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default User Account FTPUSER Login Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- Technique: [T1659 Content Injection](#)
- **2048682 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default User Account Password TAIL Login Attempt**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048683 - ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SEL-751A FTP Banner Observed**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048684 - ET SCADA [nsacyber/ELITEWOLF] Possible Siemens S7-1200 Unauthorized Access Attempt - Request for /Images/CPU1200/**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)
    - Technique: [T1659 Content Injection](#)
- **2048685 - ET SCADA [nsacyber/ELITEWOLF] Possible Siemens S7-1200 Unauthorized Access Attempt - Request for /CSS/S7Web.css**
  - Category: SCADA
  - Severity: Minor
  - Date Added: 2024\_02\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0001 Initial Access](#)

- **Technique:** [T1659 Content Injection](#)
- **2048689 - ET SCADA [nsacyber/ELITEWOLF] Siemens S7 Redpoint NSE Request CPU Function Read SZL attempt**
  - **Category:** SCADA
  - **Severity:** Minor
  - **Date Added:** 2024\_02\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
- **2029015 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029016 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029017 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029018 - ET SCAN Mirai Variant User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029019 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029020 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029021 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029022 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029023 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029024 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029025 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029026 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)

• **2029208 - ET SCAN Dark Nexus IoT Variant User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2029473 - ET SCAN ELF/Mirai User-Agent Observed (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2029577 - ET SCAN Polaris Botnet User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2029645 - ET SCAN Polaris Botnet User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)

• **2029759 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor

- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029763 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029769 - ET SCAN Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029790 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029792 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)

- Technique: [T1071 Application Layer Protocol](#)
- **2029808 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - Category: SCAN
  - Severity: Minor
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2029929 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - Category: SCAN
  - Severity: Minor
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030048 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - Category: SCAN
  - Severity: Minor
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030198 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - Category: SCAN
  - Severity: Minor
  - Date Added: 2023\_09\_27
  - MITRE ATT&CK®:
    - Tactic: [TA0011 Command And Control](#)
    - Technique: [T1071 Application Layer Protocol](#)
- **2030273 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - Category: SCAN

- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2030373 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030375 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030470 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030583 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**

- **Tactic:** [TA0011 Command And Control](#)
- **Technique:** [T1071 Application Layer Protocol](#)
- **2030676 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030692 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030909 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030964 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2030995 - ET SCAN ELF/Mirai Variant User-Agent (Inbound)**

- **Category:** SCAN
- **Severity:** Minor
- **Date Added:** 2023\_09\_27
- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2036252 - ET SCAN RDP Connection Attempt from Nmap**
  - **Category:** SCAN
  - **Severity:** Minor
  - **Date Added:** 2023\_07\_28
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0043 Reconnaissance](#)
    - **Technique:** [T1595 Active Scanning](#)
- **2003337 - ET USER\_AGENTS Suspicious User Agent (Autoupdate)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2024\_09\_19
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2010677 - ET USER\_AGENTS Suspicious User-Agent (My Session)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2025\_12\_22
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2026520 - ET USER\_AGENTS Suspicious User-Agent (Windows 8)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27

- **MITRE ATT&CK®:**
  - **Tactic:** [TA0011 Command And Control](#)
  - **Technique:** [T1071 Application Layer Protocol](#)
- **2029423 - ET USER\_AGENTS ABCCoin Activity Observed**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1496 Resource Hijacking](#)
  - **MD5:** 77ec579347955cfa32f219386337f5bb
- **2029554 - ET USER\_AGENTS Observed Suspicious UA (\xa4)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2029771 - ET USER\_AGENTS Shadowcoin Cryptocurrency UA Observed**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)
    - **Technique:** [T1496 Resource Hijacking](#)
- **2029772 - ET USER\_AGENTS Willowcoin Cryptocurrency UA Observed**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0040 Impact](#)

- **Technique:** [T1496 Resource Hijacking](#)
- **2030050 - ET USER\_AGENTS BeeMovie Related Activity**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2034021 - ET USER\_AGENTS Suspicious User-Agent (REBOL)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2034298 - ET USER\_AGENTS Suspicious User-Agent (urlRequest)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 988fbcfeebf2a49af4072030dead68f9
- **2034948 - ET USER\_AGENTS Suspicious User-Agent (dBrowser CallGetResponse)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** e09ad59bff10bd4b730ee643809ec9a7

- **2035032 - ET USER\_AGENTS Suspicious User-Agent (example/1.0)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
- **2035452 - ET USER\_AGENTS Suspicious User-Agent (HTTP-Test-Program)**
  - **Category:** User\_Agents
  - **Severity:** Minor
  - **Date Added:** 2023\_09\_27
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0011 Command And Control](#)
    - **Technique:** [T1071 Application Layer Protocol](#)
  - **MD5:** 6e69e15ae55aee85ace66bb99e6ba885
- **2056210 - ET INFO Observed UDP cups-browsed Add Printer Packet Inbound (HTTP)**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-47176](#)
- **2056211 - ET INFO Observed UDP cups-browsed Add Printer Packet Inbound (IPP)**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-47176](#)

- **2056213 - ET INFO Observed Server Responding with PDD File With Known Dangerous/Exploitable Parameter**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-47177](#)
- **2025574 - ET WEB\_SPECIFIC\_APPS Apache ActiveMQ File Upload RCE (CVE-2016-3088)**
  - **Category:** Web\_Specific\_Apps
  - **Severity:** Minor
  - **Date Added:** 2023\_12\_11
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2016-3088](#)
- **2056210 - ET INFO Observed UDP cups-browsed Add Printer Packet Inbound (HTTP)**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-47176](#)
- **2056211 - ET INFO Observed UDP cups-browsed Add Printer Packet Inbound (IPP)**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)

- **Technique:** [T1659 Content Injection](#)
- **CVE:** [2024-47176](#)
- **2056213 - ET INFO Observed Server Responding with PDD File With Known Dangerous/Exploitable Parameter**
  - **Category:** INFO
  - **Severity:** Minor
  - **Date Added:** 2024\_10\_14
  - **MITRE ATT&CK®:**
    - **Tactic:** [TA0001 Initial Access](#)
    - **Technique:** [T1659 Content Injection](#)
  - **CVE:** [2024-47177](#)