Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

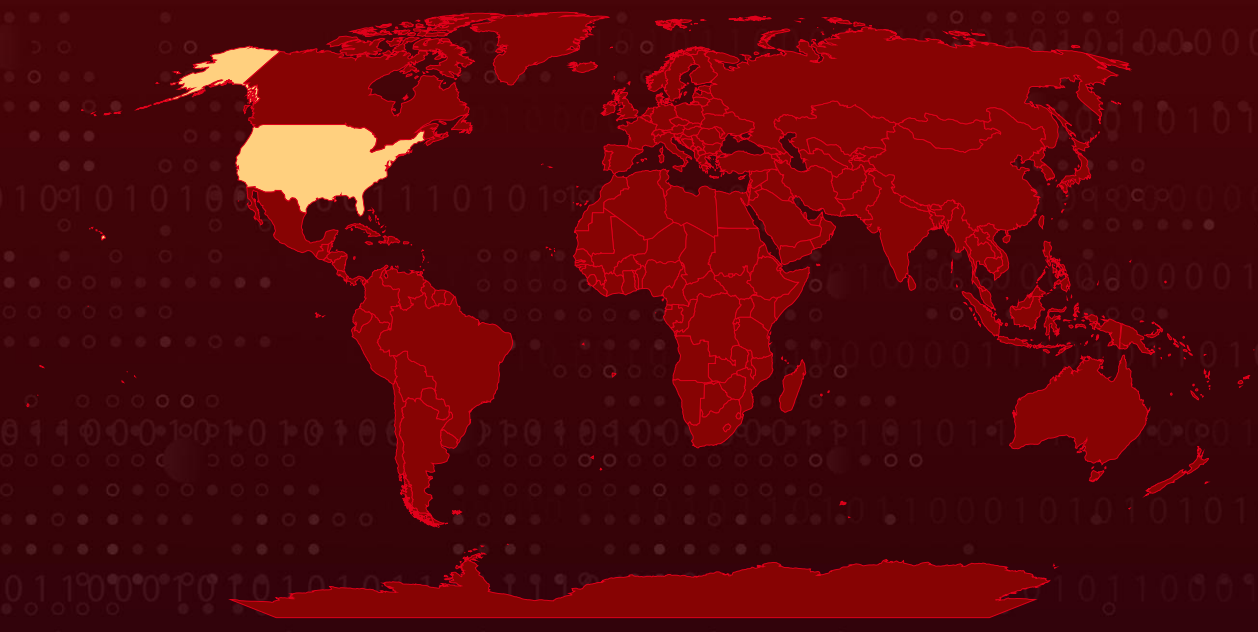
Factory Reset: How Attackers Are Halting U.S. Production Floors

Date of Publication	Last Update Date	Admiralty Code	TA Number
July 28, 2026	August 18, 2026	A1	TA2026213

Summary

Targeted Region: United States
Targeted Sector: Manufacturing
Targeted Platforms: Windows, Linux, VMware ESXi, network appliances
Dominant Ransomware: Akira, Qilin, Play, Clop, Dragon Force, INC
Total CVEs in Scope: 37 unique - 14 zero-days (37.8%), 36 on CISA KEV (97.3%)
Attack: The U.S. Manufacturing sector sat at the sharp end of the ransomware curve across the reporting window, with 45 distinct campaigns converging on a single reality: the network perimeter is the front door, and it is unlocked. Akira dominated the leaderboard while emerging brands scaled fastest beneath it, and a synchronised late-2025 pileup pointed to a shared upstream trigger the sector should expect to see repeat. Weaponised CVEs clustered on VPNs, firewalls and remote-support tooling, with backup infrastructure specifically targeted for destruction before encryption. Behind the ransomware volume sat a quieter nation-state espionage layer aimed at long-dwell access, a reminder that for manufacturers with defense, aerospace or semiconductor exposure, the intellectual-property threat is as serious as the extortion one.

Attack Regions



Targeted Non-Targeted

By the Numbers

37

Exploited CVEs tracked

58

Malware families observed

88

Ransomware Groups Tracked

14

Exploited as zero-days

Reading the numbers

Nearly all weaponised CVEs (36 of 37) are already CISA KEV-listed, and 36 of 37 have a vendor patch; the exposure is overwhelmingly from known, patchable flaws left unpatched rather than novel zero-days.

Most Recurring Threats

The CVE, ransomware, and malware are seen most often against the U.S. manufacturing sector.

MOST ACTIVE RANSOMWARE

Akira

361 leak-site victim posts

MOST RECURRING IN CAMPAIGNS

Qilin

Tracked in multiple campaigns

MOST RECURRING MALWARE

StealC

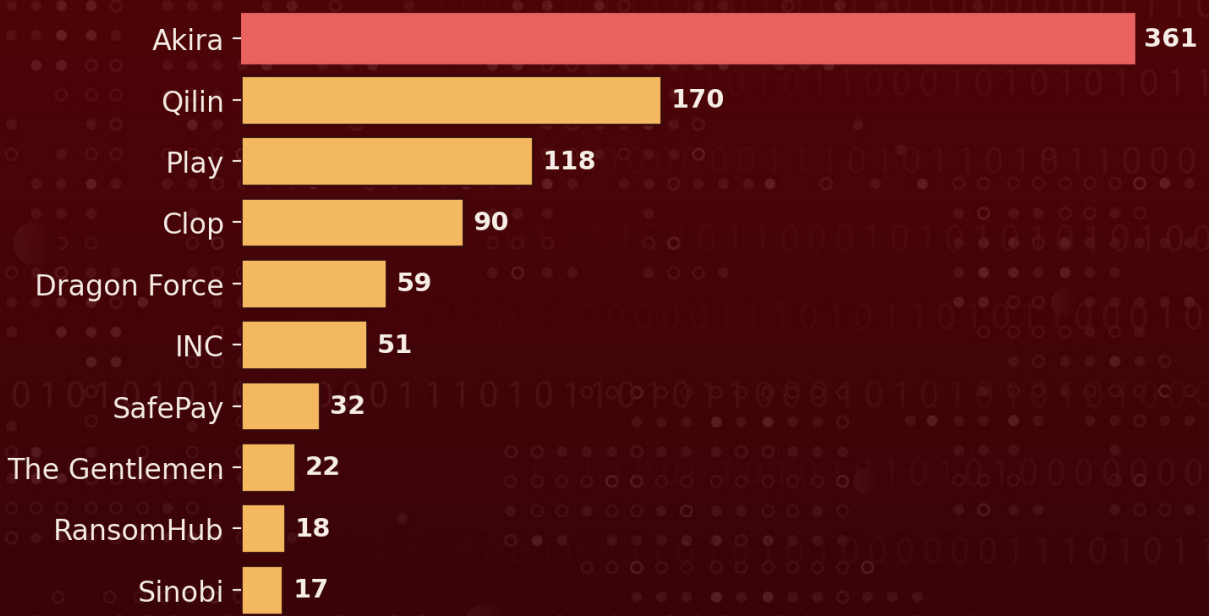
Tied across multiple stealer campaigns

MOST RECURRING CVE

CVE-2024-55591

Fortinet FortiOS auth-bypass

Top ransomware brands by leak-site victim posts

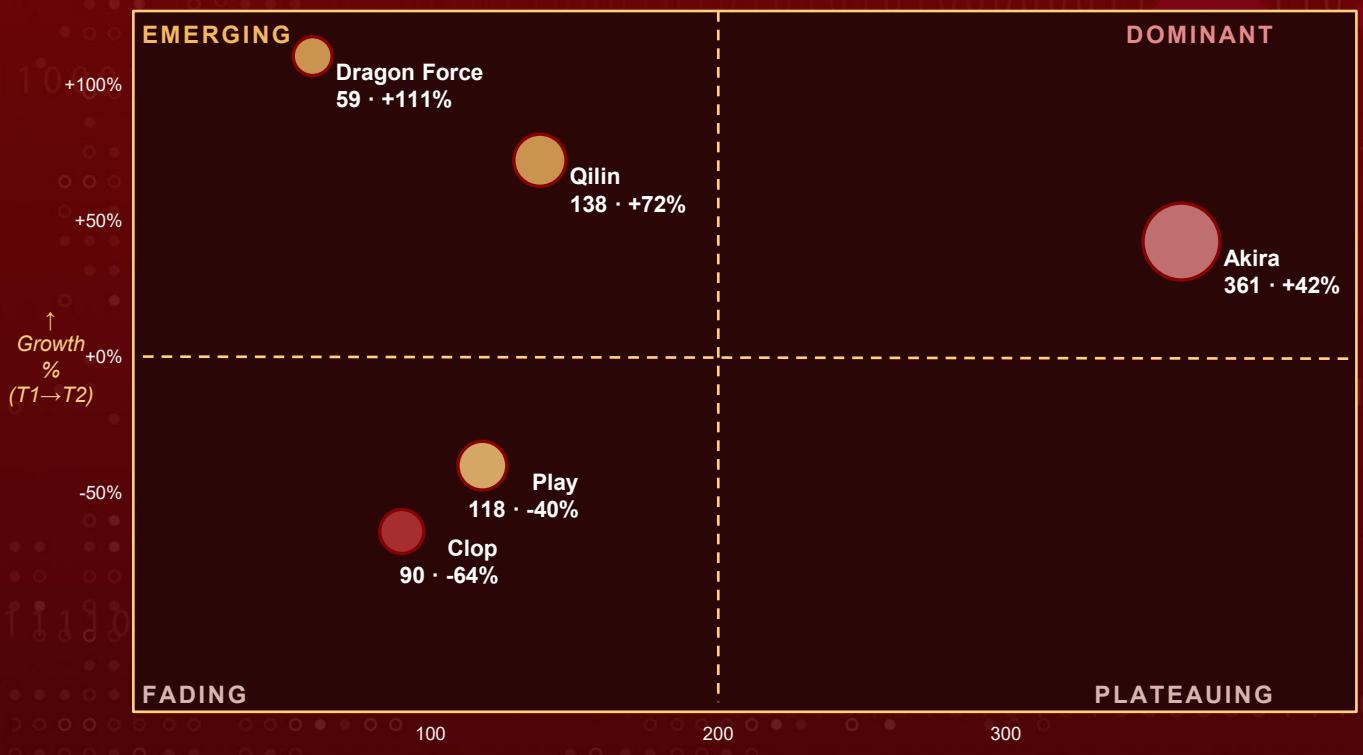


Akira dominates manufacturing leak-site postings, roughly double the next brand (Qilin). Together, the top five - Akira, Qilin, Play, Clop, and DragonForce account for the bulk of publicly claimed victims.

Note: Leak-site victim-post counts reflect publicly claimed victims on each group's data-leak site

Ransomware Momentum Quadrant

Volume × Trajectory, which crews will define next quarter?



Quadrant classification:

- **DOMINANT** - total ≥ 200 posts AND growth ≥ +30%
- **PLATEAUING** - total ≥ 200 posts AND growth < +30%
- **EMERGING** - total < 200 posts AND growth ≥ +30%
- **FADING** - total < 200 posts AND growth < +30% (typically declining)

LEADERBOARD RANK ≠ FUTURE RISK

Akira is dominant and still growing. Akira sits alone in the top-right quadrant: 361 posts (>2× the runner-up) AND +42% T1→T2 growth. It is both today's problem and tomorrow's.

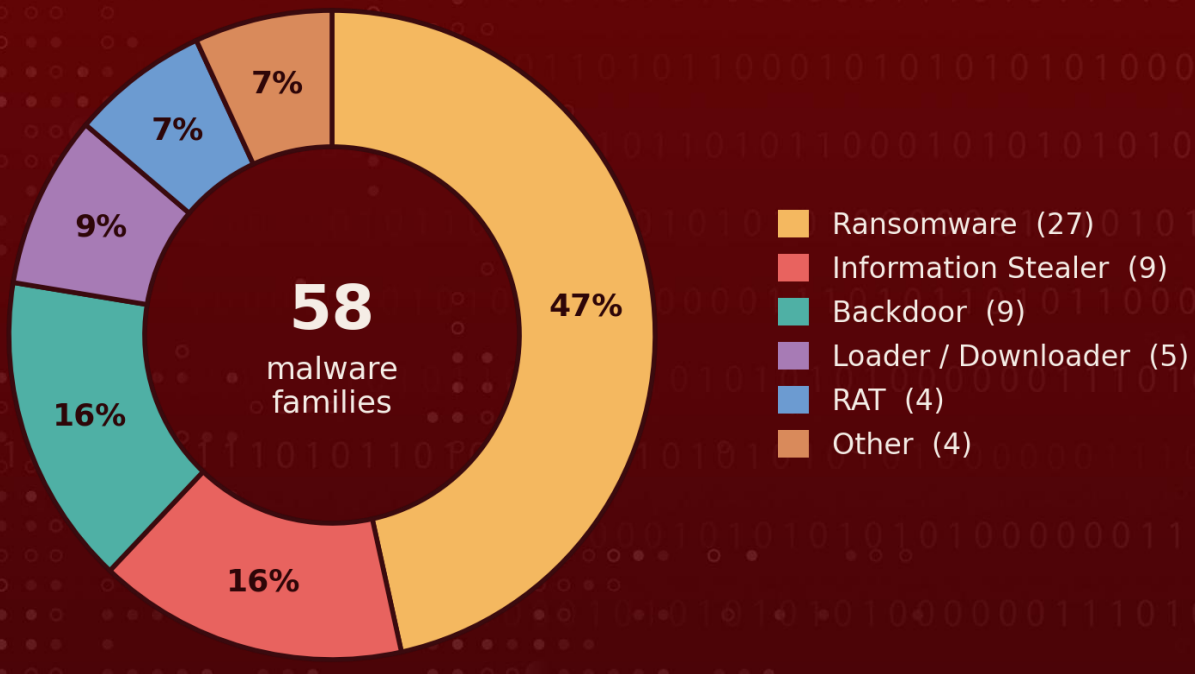
Qilin and Dragon Force are the emerging threats. Qilin (+72%) and Dragon Force (+111%) sit in the top-left EMERGING quadrant. They have lower absolute volume today but are scaling fastest. These are the crews to add to hunt-package priorities NOW.

Play and Clop are fading - reallocate hunt effort. Play (-40%) shows a genuine cooling trend; Clop (-64%) is between burst campaigns (its historical pattern is periods of dormancy punctuated by mass-exploitation events like MOVEit and Cleo). For both, reduce the cadence of dedicated named-actor hunt queries and shift those analyst-hours toward Qilin and Dragon Force, whose monthly activity is rising fastest. Retain a dormant-watch IOA package on Clop to catch the next burst cycle.

Note: Split the 18-month window into T1 (Jan-Sept 2025, 9 months) and T2 (Oct 2025 - Jun 2026, 9 months).

Malware Analysis

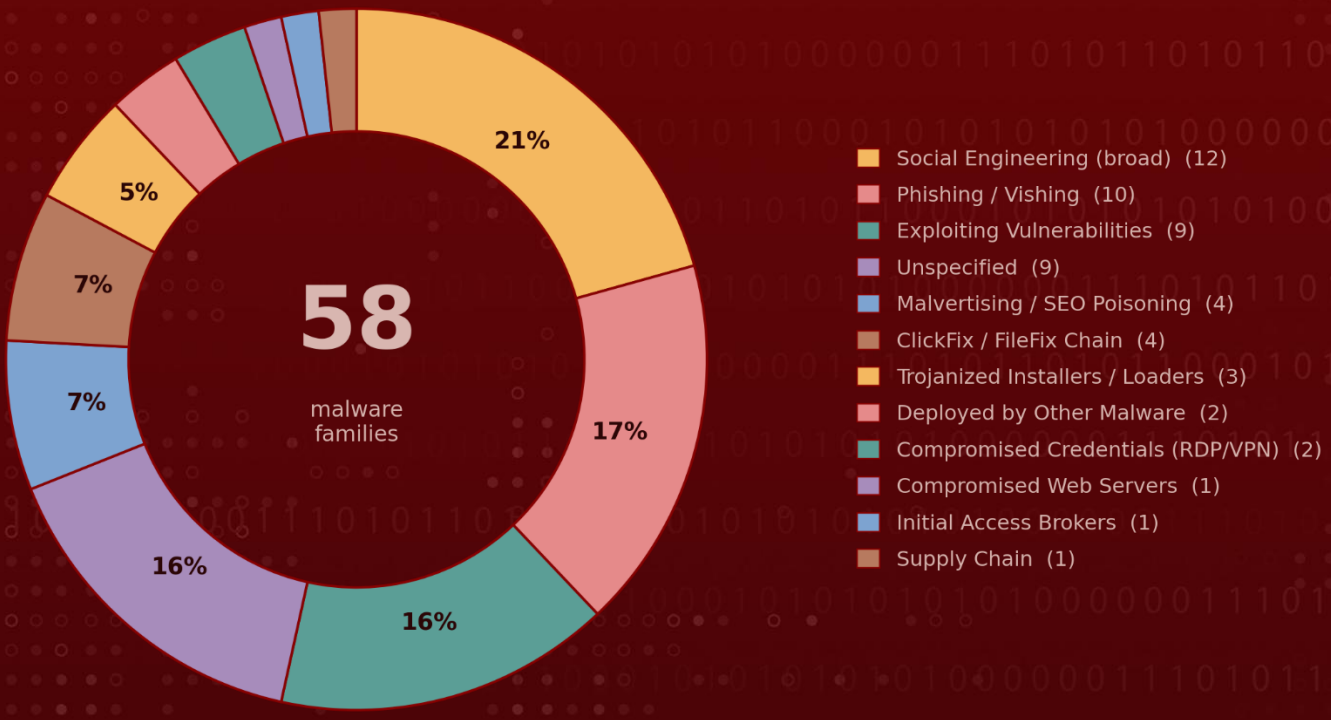
58 tracked malware families grouped by type.



Ransomware leads at 47% (27 of 58 families), confirming extortion as the primary end goal targeting U.S. manufacturing. **Information stealers and backdoors follow at 16% each** - stealers harvest the credentials that open the door, while backdoors give the persistent, quiet access espionage crews and ransomware affiliates rely on. Loaders/downloaders (9%) and RATs (7%) round out the delivery-and-control toolkit. Read together, the mix describes a full intrusion lifecycle: steal access, establish persistence, then encrypt or exfiltrate for extortion.

Delivery-Method Analysis

How do the observed malware families reach victim environments?



TWO CATEGORIES OWN MOST DELIVERY

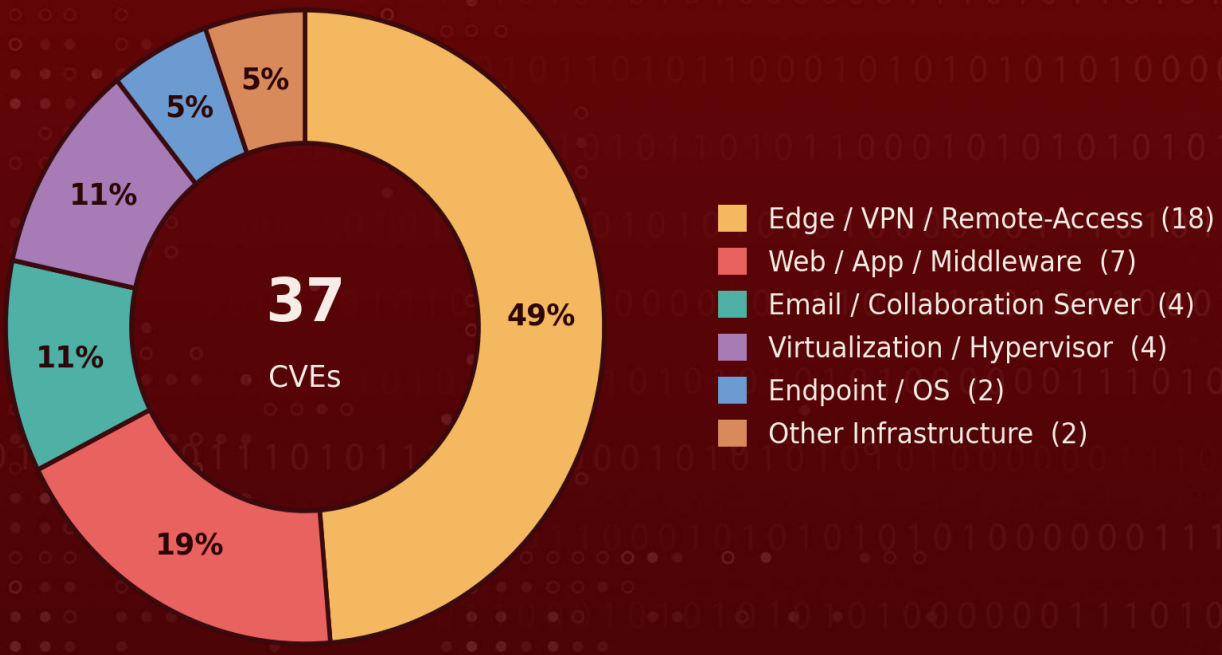
The user is the attack surface. User-focused delivery (phishing, social engineering, malvertising, ClickFix) accounts for 50% of all in-scope malware families - a larger share than any other category. Vulnerability exploitation is 19%.

Email + patching = two-thirds of coverage. Together, user-focused delivery and vulnerability exploitation account for roughly two-thirds of observed malware entry points. Any CISO budget that under-invests in either of these categories leaves outsized exposure.

The sleeper category is credential compromise. Only 3/48 families are attributed to compromised credentials, but this vector is disproportionately consequential (e.g., the Sinobi flagship intrusion cascade started here).

Affected Products

37 exploited CVEs grouped by the type of product targeted.

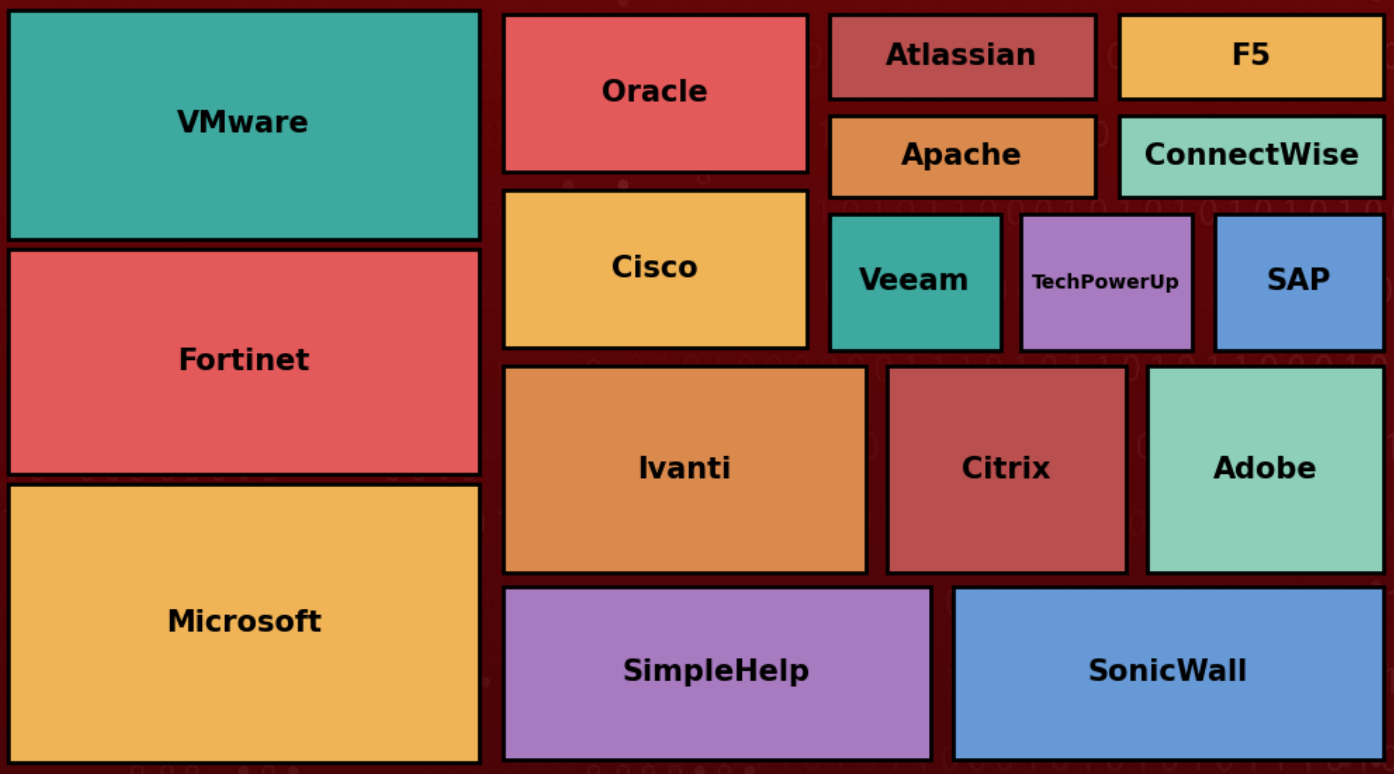


Edge, VPN & remote-access appliances dominate (18 of 37 CVEs). Fortinet, Ivanti, Citrix, SonicWall, SimpleHelp, and ConnectWise devices are the principal doorway into manufacturing networks: internet-facing, often under-patched, and sitting directly on the perimeter. **Web/application/middleware (7)** SAP NetWeaver, Oracle, Log4j, Confluence, ColdFusion, and **virtualization/hypervisor and email/collaboration servers (4 each)** round out the attack surface. The pattern is clear: the exposure is concentrated at the network edge and in the shared enterprise software beneath production systems.

Half of all exploited CVEs target the perimeter itself, the appliances that face the internet before any production system is reached. Segmenting OT/production networks behind these devices and patching the edge first delivers the largest reduction in blast radius.

Affected Vendors

Exploited CVEs by vendor area are proportional to the number of weaponised vulnerabilities.



Microsoft, Fortinet and VMware carry the largest weaponised footprint, followed closely by SimpleHelp, SonicWall and Ivanti. Two themes emerge. **First, security and remote-access vendors** (Fortinet, SonicWall, Ivanti, Citrix, SimpleHelp, ConnectWise, F5), the very products bought to protect the network, are the most-exploited class of appliance. **Second, core enterprise platforms** (Microsoft, VMware, Oracle, SAP, Adobe, Atlassian, Apache) underpin production and back-office systems, so a single vendor flaw cascades widely. Concentrating patch and monitoring effort on this short vendor list covers the majority of the sector's exploited exposure.

Attack Details

#1

The USA Manufacturing sector has absorbed sustained pressure from a professionalized ransomware-as-a-service ecosystem throughout 2025 and into 2026, layered over persistent espionage activity from state-nexus operators. Across 51 discrete campaigns aggregated for this landscape, ransomware families account for 27 of the 58 malware strains observed, with the balance made up of backdoors, infostealers, remote access trojans, loaders, and a cluster of dual-use tooling.

#2

The genealogical thread running through the leading ransomware brands is unmistakable: INC's source code, sold on Russian-speaking forums in May 2024 for $300,000, subsequently propagated into Lynx and then into Sinobi, which listed Manufacturing as its top 2025 vertical. Qilin held the top global ranking for three consecutive quarters through Q1 2026 with over 330 leak-site victims and a cumulative count exceeding 1,800 by late May 2026, expanding from double- to triple-extortion using DDoS pressure and a "Call Lawyer" negotiation feature. The Gentlemen, spun out from Qilin following the hastalamuerte departure in July 2025, scaled from 30 to over 320 publicly listed victims between autumn 2025 and April 2026, with Manufacturing among its most impacted sectors.

#3

Initial access into USA Manufacturing environments is dominated by exploitation of internet-facing edge infrastructure. Fortinet FortiGate appliances have been repeatedly abused via CVE-2024-55591, with one operator maintaining a curated inventory of roughly 14,700 pre-compromised devices, alongside 969 validated brute-forced VPN credentials, thereby reducing the reconnaissance phase to zero for downstream affiliates.

#4

Citrix NetScaler exposures (CVE-2023-3519 and the more recent CVE-2025-5777 "Citrix Bleed 2"), Fortinet FortiClient EMS SQL injection (CVE-2023-48788), SimpleHelp remote support flaws, and SonicWall SSL VPN weaknesses have all been chained by multiple families. Legacy vulnerabilities remain highly exploitable: Ghost ransomware has compromised organizations in more than 70 countries by weaponizing the ProxyShell chain, along with Fortinet, Adobe, and SharePoint flaws dating back to 2009. Of the 37 unique CVEs aggregated, 97.3% already sit on the CISA KEV catalog with vendor patches available.

#5

Post-exploitation tradecraft across the campaign set converges on a small set of durable techniques. Credential harvesting relies on Mimikatz and modified Veeam credential dumpers upgraded for salted-DPAPI; lateral movement uses RDP, PsExec, WMI, WinRM, and Impacket-style atexec and smbexec; and command-and-control traverses Cobalt Strike beacons, SystemBC SOCKS5 proxies, AnyDesk fallback channels, and DNS-over-HTTPS covert tunnels.

#6

Defense evasion has advanced sharply: The Gentlemen exploits CVE-2025-7771 in ThrottleStop.sys via a bring-your-own-vulnerable-driver technique to gain kernel-level code execution and terminate EDR, while Sinobi has been observed uninstalling Carbon Black from a compromised file server. Windows Subsystem for Linux is now used by Qilin to run components from a Linux runtime context on Windows hosts, deliberately evading endpoint tools that lack WSL visibility. Exfiltration overwhelmingly moves through RClone and WinSCP to cloud storage - AWS, BackBlaze, or attacker-controlled buckets.

#7

Beyond financially motivated crime, USA Manufacturing has been squarely inside the targeting map of state-nexus espionage. The People's Republic of China-nexus WARP PANDA deployed the BRICKSTORM Go-based ELF backdoor against VMware vCenter environments at U.S. organizations in 2025, creating unregistered malicious virtual machines that are powered down after use to evade forensic recovery.

#8

Static Tundra, a Russian FSB Center 16 sub-cluster of Energetic Bear active since 2015, continues to weaponize a 2018-era Cisco Smart Install flaw to embed the SYNful Knock firmware implant into network devices for long-term intelligence collection. ShinyHunters has claimed access to CVE-2025-31324 in SAP NetWeaver and CVE-2025-61882 in Oracle E-Business Suite, with stolen datasets priced at up to $1 million. Impact tradecraft has trended toward speed and irreversibility: hybrid Curve25519/AES-128-CTR schemes with per-file keys, configurable partial-file encryption (1-9% on large files), shadow-copy destruction via low-level DeviceIoControl resize, and free-disk-space wiping with double and triple-extortion negotiations through Tor portals, Tox, and Session messengers.

Recommendations

Enforce a hard patch SLA on internet-facing appliances: VPN gateways, firewalls, ADCs, and remote-support tooling from Fortinet, SonicWall, Citrix, Ivanti, F5, ConnectWise ScreenConnect, and SimpleHelp are the single highest-risk technology category in this advisory. 14 of 37 tracked CVEs sit on this tier, and 97% are already on the CISA KEV catalogue. Establish a written 72-hour patch SLA from KEV inclusion, with executive escalation if breached, and maintain an authoritative inventory of every internet-facing appliance, including those managed by third parties.

Harden backup and recovery infrastructure as a targeted asset: Ransomware tradecraft across Qilin, INC, The Gentlemen, DragonForce and Sinobi specifically destroys backup services, shadow copies and ESXi hypervisors before encryption begins recovery capability itself is the target. The 3-2-1 rule is no longer sufficient. Deploy immutable, off-network backups on a separate identity plane from the primary Active Directory forest, and test full-restore quarterly against a scenario in which AD and the hypervisor are lost together.

Segment the hypervisor and identity-management planes: vCenter, ESXi management, and Domain Controllers must live on separate administrative networks with dedicated privileged access workstations. A compromised helpdesk workstation should not be able to authenticate to vCenter or a Domain Controller. This segmentation directly counters the WARP PANDA / BRICKSTORM and Static Tundra / SYNful Knock intrusion patterns documented in this advisory, both of which pivot through the management plane for multi-year dwell.

Establish continuous external attack-surface discovery: Most intrusions in this advisory began with an internet-exposed asset the victim did not know it owned, inherited through a subsidiary, an acquisition, or an MSP handoff. Run a monthly outside-in scan of your public footprint (DNS, ASN ranges, subsidiary domains, third-party-hosted services) and reconcile the delta with the authoritative inventory. Every unknown asset is a candidate initial-access vector. This is a distinct discipline from vulnerability management: it answers what is exposed before asking what is vulnerable.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.004: Spearphishing Voice
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1569: System Services	T1569.002: Service Execution
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1542: Pre-OS Boot	T1542.001: System Firmware
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1211: Exploitation for Defense Evasion	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools

Tactic	Technique	Sub-technique
Defense Evasion	T1027: Obfuscated Files or Information	
Discovery	T1018: Remote System Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB / Windows Admin Shares
	T1570: Lateral Tool Transfer	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1105: Ingress Tool Transfer	
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1498: Network Denial of Service	

Vulnerability Posture

How dangerous and how actionable the exploited CVEs are.

36 / 37

listed in CISA KEV

14 / 37

exploited as zero-days

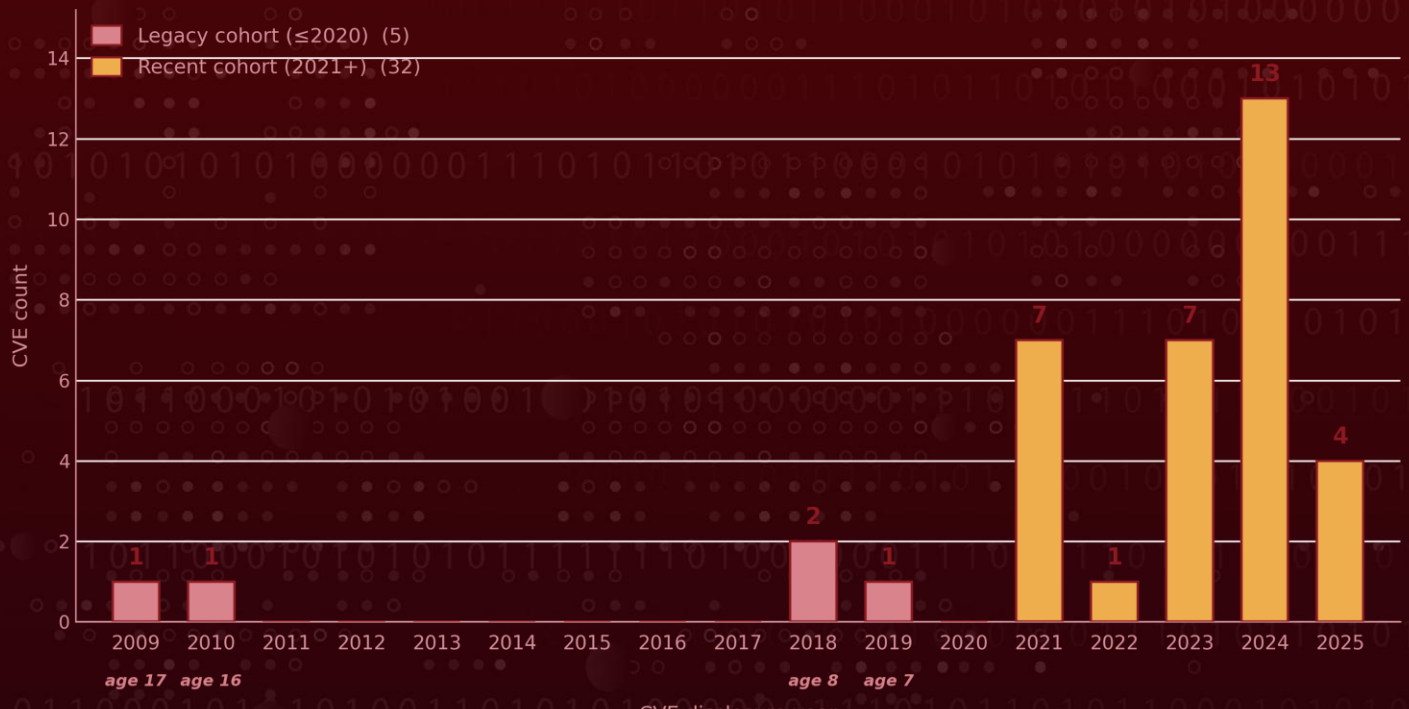
5 / 37

LEGACY CVEs (2009-2020); All patched, all on KEV

36 / 37

have a vendor patch

97% of weaponised CVEs are already in CISA's Known Exploited Vulnerabilities catalogue, and 97% have a patch available, meaning the vast majority of manufacturing's exposure is remediable today and is being exploited because patch lag, not novel zero-days, is the gap. The 14 zero-days that do appear cluster in edge appliances (Fortinet, Citrix, Ivanti, Oracle), underscoring why perimeter devices demand the fastest possible patch SLAs.



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS	✗	✓	✓
CVE-2024-57727	SimpleHelp Path Traversal Vulnerability	SimpleHelp Remote Support Software	✗	✓	✓
CVE-2025-5777	Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	SonicWall SMA 100 Appliances	✗	✓	✓
CVE-2009-3960	Adobe BlazeDS Information Disclosure Vulnerability	Adobe BlazeDS 3.2 and earlier	✗	✓	✓
CVE-2010-2861	Adobe ColdFusion Directory Traversal Vulnerability	Adobe ColdFusion 9.0.1 and earlier	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS, FortiProxy	✗	✓	✓
CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✓	✓
CVE-2021-31207	Proxyshell - Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34473	Proxy Shell - Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	Proxy Shell - Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	SonicWall SonicOS SOHO (Gen 5)	✗	✓	✓
CVE-2024-53704	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability	SonicWALL Gen7 NSv	✗	✓	✓
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	✗	✓	✓
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop	✓	✗	✗
CVE-2024-21762	Fortinet FortiOS SSL-VPN Out-of-Bounds Write Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver Visual Composer	✓	✓	✓
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓
CVE-2021-44228	Log4Shell - Apache Log4j Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server	✓	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21412	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows Internet Shortcut Files	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	✓	✓	✓
CVE-2024-57726	SimpleHelp Missing Authorization Vulnerability	SimpleHelp remote support software	✗	✓	✓
CVE-2024-57728	SimpleHelp Path Traversal Vulnerability	SimpleHelp remote support software	✗	✓	✓
CVE-2023-20118	Cisco Small Business RV Series Routers Command Injection Vulnerability	Cisco Small Business RV Series Routers	✗	✓	✓
CVE-2021-35587	Oracle Fusion Middleware Unspecified Vulnerability	Oracle Access Manager product of Oracle Fusion Middleware	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	✓	✓	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2021-22005	VMware vCenter Server File Upload Vulnerability	VMware vCenter Server	✗	✓	✓
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	✓	✓	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✗	✓	✓
CVE-2024-38812	VMware vCenter Server Heap-Overflow Vulnerability	VMware vCenter Server, VMware Cloud Foundation	✗	✓	✓

Note: The CVEs have patch links hyperlinked to the corresponding tick marks.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Abyss Locker	SHA256	72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462, 3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69522a0a3c34c96b6d, 9243bdcbe30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc, 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64, dee2af08e1f5bb89e7bad79fae5c39c71ff089083d65da1c03c7a4c051fabae0, e6537d30d66727c5a306dc291f02ceb9d2b48bffe89dd5eff7aa2d22e28b6d7c, 1d04d9a8eeed0e1371afed06dcc7300c7b8ca341fe2d4d777191a26dabac3596, 1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eacbefe4120, 25ce2fec4cd164a93dee5d00ab547ebe47a4b713cced567ab9aca4a7080afcb7, b524773160f3cb3bfb96e7704ef31a986a179395d40a578edce8257862cafe5f, 362a16c5e86f13700bdf2d58f6c0ab26e289b6a5c10ad2769f3412ec0b2da711, e5417c7a24aa6f952170e9dfcfdf044c2a7259a03a7683c3ddb72512ad0cd5c7, 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da, 877c8a1c391e21727b2cdb2f87c7b0b37fb7be1d8dd2d941f5c20b30eb65ee97, 2e42b9ded573e97c095e45dad0bdd2a2d6a0a99e4f7242695054217e2bba6829
Anubis	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
AsyncRAT	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ececf197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e,

Attack Name	TYPE	VALUE
AsyncRAT	SHA256	346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878fefc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0
Beast Ransomware	SHA256	6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0, 479d0947816467d562bf6d24b295bf50512176a2d3d955b8f4d932aea2378227, cc0680de960f3e1b727b61a42e59f9c282bd8e41fe20146ed191c7f4bf9283a7, cf5c45be416d1b18dd67ffa95c6434691f1f9ba9c30754fa6fc9978c1f975750, 2ce62601491549ab91c9517e0accf3286ed29976f6ec359d31ddc060a8d99eb3, 812df0efea089b956d08352ff0a7e8789d43862dc3764f4441d4e1c1d1fb7957, 5bd8f9cbd108abc53fb1c44b8d10239a2a0a9dd20c698fd2fb5dc1938ae7ba96
	IPv4	5[.]78[.]84[.]144
BerserkStealer	SHA256	eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692, a5623b6a6f289bb328e4007385bdb1659407a9e825990a0faaef3625a2e782cf
BlackNevas Ransomware	TOR	Hxxp[://]ctyfftrjgtwdjzlgqh4avbd35sqrs6tde4oyam2ufbjch6oqpqtkdtid[.]onion
	Email	amsomar[@]consultant[.]com, avalonsupp[@]consultant[.]com, biosannetsuabvg[@]mail[.]com, black4over[@]newlookst[.]com, compsupp[@]techie[.]com, corubete[@]dr[.]com, milford[@]usa[.]com, murrock[@]consultant[.]com, ovtaitonine[@]usa[.]com, suppcarter[@]uymail[.]com, toxicavalon[@]toke[.]com, varentsujikyuke[@]mail[.]com, widemoucerpco[@]mail[.]com, paymeuk[@]consultant[.]com , Serina5Murrock[@]email[.]com

Attack Name	TYPE	VALUE
BlackNevas Ransomware	SHA1	203f81cbe35c64071f52f34afbbbfc7d61b3e702, 2a79c999e20c5d8102e0b728733cc8eba2b4d8ac, 3226ebfc23dbe1a6cc44c3255d1a0e12f0dd153c, 3ff7aedacf36f96fef42391aaadb2c63820bef7f, 49551cb0bbc2da3f6d36523a005af5ee1f5ad1a8, 499cd23b37a00b9a8ad212f879501705baad1781, 4d5605008bd0619a5980c4633889d7c253093360, 4db3b2876ef5c8e5ea977d8ffedef428b93408a4, 61c56c25f5ca4bee336aa30e89123eb2daf5166a, 646533556a16a9d17bd7ad2265873bc8f1ccb4f4, 67750b2b0b90572ade6ef760bcded1ef5fc09982, 781a8e52c2399c07ca4853def924d79be5182b32, 7b3cbd60020c1d155b12271881d69c968fcde04f, 7bf79cc58fb8f3d0ec774cb8b9e8ce311cbc27d2, 7c4f10d85607e65386fb504446b45419901c5276, 812d65b67ce28905f5e07ac1f82b827ebd36470a, 88aee839de69ce1602ef2bb401a6cabb6b376e19, 8cbbcbe187ff66c44908a205236d4230931f7d73, 923be026c79e7b5b5d29461420887fe2e8875b01, 92b0ce569d838cd9b773cc13b6b6ea5609e85fd7, B00897AE5B116680CCDD2E43A3A9599D8C3E166E, b8c85fa5a81b3d70a21835fbea394e0611461bf8, c1c9008b4be855583df0f04204443262a3fbc8ab, cd2f25a8ab74bdc17d7c8170f2c4135537ece3c4, cdb07718787743ceb488b5bd184d9a4939c12dbf, d026954e6f646b84943f8514be606650be8c18bb, dc6d4f0a88ea0458926ff8f57dbd8239ed140824, ebf63e7a27c91f96d84b66d7ba435ddc3a153b71, 2d8e9ea39b9853d5676957a51f09f14d3703d1bd, d6e1a47a0cf9bc94a816149f6e1f1a04c53f99d1, 1b14a60d50622a7c846f9e81d9668b4962fc356b, 70e9b61e0a8e708e8512c54f96b90b32bac38984, a35b2be3167b72c73b2f8f9ac058576cf080f752, 1c0620a81f8cfb3c2a8b073b7e5a5c2329b511a5, f7d2d8fd75a62a9ce4533196b13f9ba55e985b62, 3b8185e491bbfe4ba0583f3a5810674aeaff26ad, 1ad51a365293269da14fd6914c3014fb3556f69f, a61aaf88253bfb4bd80e0ca7bbaf4a78e6bb2591, 67a078a7d703308e3c0eb2af7ea0c288453cd705, 80ad69638820c264552e5f73ed696f88614fa3bd, cbe2b0cfa599fe7477ebbe92feaadb54b5b25deb, ad63f0652ce21b0dac5284158cf301410f57d0f9, f7ac2604e6e186a647318544c36ba5758cdcb85a, 97fa0c24f75164940717672f22643ba31161c638, f18b501eca2a7390705967a24f67b808b43d2212,

Attack Name	TYPE	VALUE
BlackNevas Ransomware	SHA1	8dfd14d230d93ff6eea3dd09934ebf9c9e860a0f, 93ba61e1b7d12277e0bcee27ec7f37a74d8f1c97, 119388459d68d2781b843e1db71be8f5e01e965a, 0a33ed85842cf189f96ae9ea804a2e0789200430, 3bcf26bb616c57330da226f5db4e89bb609147e8, 827c01503a92b1e202939ae5a0e3e4d5ff02f4ae, 2e2046d5e8fb4ccc18f7fdf1a4dd076bf2333417, 18af0b641e456ed5df3908f2e2fc16ea01fef0f2, 1881f7bd1867e7d625e2ef2f0dc856437a376112, 1b87e342d2fdd5cf5db3a8280bac92f90f099516, 6b22150c7eeafd74dca41b749bf33f391401d094, a7da9e83c69a9deb6aa4de1fb0ec7d0badb4a426, 67c0338c0a58493befc6c77c9f7fb16d753eb155, 0b02e7c36714e9af519fd24bca893172afd2562d, aa10da9d601482262b87cb1e0748acca7a91c2a5
	MD5	2374998cffb71f3714da2075461a884b, 4a1864a95643b0211fa7ad81b676fe2e, 9f877949b8cbbb3adfe07fd4411b9f26, f2547a80dd64dcd5cba164fe4558c2b6
	SHA256	23642a78addcffd124db133a2dd2fcd2d1bdb060dd1e41da33cb18eec7a88867, 2b9fe8a2629727470be1c928f7c9be7e2ea6cc22fb12f971902bf9cea8b16afb, 360758c296310ba428d0d52c90e31c05fc43d5889282fa840283cf468f2378e8, 3d09e930305cb3aa4ca54a39b0e3749f083d432f202606c8adac8455014b47fc, 43f145fccec00f1e100ec3377eaf0ab60df3b9c5291b8011e05141cc04704be1, 49fcbd606ff10d4661e222b8910ab7829d1668e3c97f1bab7eb51e8ec7d799a5, 501821a19ccf59830789849beff94238736adb4b213870a511890c5c8efab2a6, 623f3e98908962669e48edd414dbb67e9d4e204f677998fdcc9c2d790816a67f, 713392f009bc133f24b3271379a4ac147e1a7782b6a1ac957c1fda69d676b550, 840b1c580bfd15ca3eb1cc94cf479f63b93285d2599bc2e3cd361e3f5a340f19, 8a2d6d27ffcc66400a640d3c9c9e6becb90c04c5bab452cac56f999c48a04d63, 910cc03d64bf09f53cdf3b83068cc46368c23a061c2e1ed5df0e3a35d6c9e084, 95e744ddcc2e8f89f6c6e25503eff2eb5e70e98f6989bb4a4e93f17b09448e78,

Attack Name	TYPE	VALUE
BlackNevas Ransomware	SHA256	9d9c146910f294b3e2a755f76e8066cd2edfac057ff54f00f405e2f9e8b9e51a, a0630e2a81775e8334ea9f8cac73cebf1b9a70507ea3347c0c2eba82c80219a6, a331504acf589be5d11202232a7a93eeb4fe6b053beea231d9a0a661bcaf3fd6, b0dfaf509de38749c49afcb3cd34d27126044bb77cc16896b02ebced6f95db02, b2353fce403b079735a606294c4ffc20a71f1c6b16ec15e94f554beafcddd1ea, bad3c2f72ef2be522a554a9615dc93027416a3d4048f77519fca5104fabba1f9, bf4adad2eb1163369c133ae61c181a3f91ef8640a457e9c4e72d77a60fbfa7ab, c08a752138a6f0b332dfec981f20ec414ad367b7384389e0c59466b8e10655ec, c0fc61631a20c373ce17e939e09cfb4f5179c9e0788e80079b4ee8986afe89bd, d953bce4d87f5837ce318481e3a1b6617cf64af976043d3b4b4866475bb31972, def75a41435dc28430097a7e116b2d17526ce2b0172995618f2749b0d732f7ea, e7706a633f24679c7550a31b96088dda8f772c98f64daee7cfbf0dc17a4a8338, eb8cbc4a0eae33bfdc4ecb99d033c81224b005e55588ceb86346f2b2d3fd790f, f25f76a85ded0d4d285d9ae5482d8fe07dade3e241853d00b17642d7873733e8
BRICKSTORM	SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759, 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830, 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830
CHROMEPUSH	Domain	cmailer[.]pro
	SHA256	603848f37ab932dccef98ee27e3c5af9221d3b6ccfe457ccf93cb572495ac325

Attack Name	TYPE	VALUE
CMD Organization Ransomware	SHA1	07c14b82f673ba5caa8c1188f052ea31583f0af7
	Email	Cmd2official[@]onionmail[.]org, Cmdhtmnjksgkuhilrtrh[@]onionmail[.]org, MitsueWhite[@]onionmail[.]org, JedAdams[@]onionmail[.]org
	Domain	cmdofficial[.]com
	Onion address	cmdnkiqjije2tllr3biee2sjgj3i4robg2cbtilbnytdhh2wy3syrlyd[.]onion
Crypto24 Ransomware	SHA256	10c3317566f52eaeb45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b, 0e36b1837e5a2cbd14fac2c3b709a5470b7b488bd15898d30840ec60448e83e0, 3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac, 686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac, 24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73
Daixin Team Ransomware	SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238, 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD, 54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939, EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF, 475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28
	File Path	rclone-v1.59.2-windows-amd64\git-log.txt, rclone-v1.59.2-windows-amd64\rclone.1, rclone-v1.59.2-windows-amd64\rclone.exe, rclone-v1.59.2-windows-amd64\README.html, rclone-v1.59.2-windows-amd64\README.txt
	Tor Address	7ukmkdtyxdkdivtjad57klqnd3kdsmq6tp45rrsxqnu76zzv3jvitlqd[.]onion, 232fwh5cea3ub6qguz3pynijxfzl2uj3c73nbrayipf3gq25vtq2r4qd[.]onion

Attack Name	TYPE	VALUE
DarkCloud	SHA256	bd8c0b0503741c17d75ce560a10eeeaa0cdd21dff323d9f1644c62b7b8eb43d9, 9588c9a754574246d179c9fb05fea9dc5762c855a3a2a4823b402217f82a71c1, 6b8a4c3d4a4a0a3aea50037744c5fec26a38d3fb6a596d006457f1c51bbc75c7, f6d9198bd707c49454b83687af926ccb8d13c7e43514f59eac1507467e8fb140, 24552408d849799b2cac983d499b1f32c88c10f88319339d0eec00fb01bb19b4, ce3a3e46ca65d779d687c7e58fb4a2eb784e5b1b4cebe33dbb2bf37cccb6f194, 381aa445e173341f39e464e4f79b89c9ed058631bcbbb2792d9ecbdf9ffe027d, 82ba4340be2e07bb74347ade0b7b43f12cf8503a8fa535f154d2e228efbef69c, e013fb82188cb7ea231183197e12c189b4637e7d92e277793d607405e16da1e2, 6a3b4e62a8262a0bf527ad8ea27eb19a0fcb48a76d6fc2868785362e40491432
DEEPBREATH	SHA256	b452C2da7c012eda25a1403b3313444b5eb7C2c3e25eee489f1bd256f8434735
Deno	Domain	okobojirent[.]com, mshealthmetrics[.]com, verify-safeguard[.]top, neremedysoft[.]com, ndibstersoft[.]com, windowallclean[.]com, cnoocim[.]com, delhedghogeggs[.]com, serialmenot[.]com, crahdhduf[.]com, weaplink[.]com
	IPv4	194[.]31[.]223[.]42, 144[.]31[.]2[.]161, 87[.]121[.]79[.]6, 87[.]121[.]79[.]25, 144[.]31[.]54[.]243, 144[.]31[.]224[.]98
DEVMAN	SHA256	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403
	SHA1	4a34bbad85312ef34b60818a47f7b5bb8e9a7e26
	MD5	e84270afa3030b48dc9e0c53a35c65aa
	Filename	e47qfsnz2trbkhnt.devman
	Mutex	hsfjuukjzloqu28oajh727190

Attack Name	TYPE	VALUE
DEVMAN	Tox ID	9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
	TOR Address	qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd[.]onion
Dire Wolf Ransomware	SHA256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3, 8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
	SHA1	Ed7c9fbd42605c790660df86b7ec325490f6d827, 4a5852e9f9e20b243d8430b229e41b92949e4d69
	MD5	A71dbf2e20c04da134f8be86ca93a619, aa62b3905be9b49551a07bc16eaad2ff
	TOX ID	B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2
	TOR Address	Hxxp[://]direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd[.]onion
	File Name	data345.exe
DragonForce	MD5	d54bae930b038950c2947f5397c13f84
	SHA1	343220b0e37841dc002407860057eb10dbeea94d, e164bbaf848fa5d46fa42f62402a1c55330ef562, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c, 229e073dbcbb72bdfee2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4, 577b110a8bfa6526b21bb728e14bd6494dc67f71, 7db52047c72529d27a39f2e1a9ffb8f1f0ddc774, 81185dd73f2e042a947a1bf77f429de08778b6e9, a4bdd6cef0ed43a4d08f373edc8e146bb15ca0f9, b571e60a6d2d9ab78da1c14327c0d26f34117daa, e1c0482b43fe57c93535119d085596cd2d90560a, eada05f4bfd4876c57c24cd4b41f7a40ea97274c, fc75a3800d8c2fa49b27b632dc9d7fb611b65201
	SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b
	Tor Address	Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion, 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion
EvilAI	SHA256	8ecd3c8c126be7128bf654456d171284f03e4f212c27e1b33f875b8907a7bc65

Attack Name	TYPE	VALUE
FunkSec Ransomware	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
Ghost Ransomware	MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982, 29e44e8994197bdb0c2be6fc5dfc15c2, c9e35b5c1dc8856da25965b385a26ec4, d1c5e7b8e937625891707f8b4b594314, ef6a213f59f3fbee2894bd6734bbaed2, ac58a214ce7deb3a578c10b97f93d9c3, c3b8f6d102393b4542e9f951c9435255, 0a5c4ad3ec240fbfd00bdc1d36bd54eb, ff52fdf84448277b1bc121f592f753c5, a2fd181f57548c215ac6891d000ec6b9, 625bd7275e1892eac50a22f8b4a6355d, db38ef2e3d4d8cb785df48f458b35090
Ghost RAT	MD5	1244b7d19c37baab18348fc2bdb30383
	SHA1	365888661b41cbe827c630fd5eea05c5ddc2480d
	SHA256	1e5c37df2ace720e79e396bbb4816d7f7e226d8bd3ffc3cf8846c4cf49ab1740, 7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958
	IPv4:Port	104[.]234[.]15[.]90[:]19999
	File Path	C:\Windows\Cursors\x.exe
GlassWorm	SHA256	ad6d0679b5b9d2b2458047d4a9adc2d9920abbcf71f9b987b917f07d325ec3f3, 9707200067f6903f70c65721338dc1de18f1cab687a85c868d632cf12bb2f278, b62acc93eb77a4ffb88cf49a8bcef574e6216e10714433a9cb1230bdb2c90546,

Attack Name	TYPE	VALUE
GlassWorm	SHA256	6beaf047e948c366cb21d16818e1d0bb0ebbd928f40fe22c521344ad9c38f32e, e46ab145387e8ae996a202520f73088ae735f88f18fab1ed60469334d58d727d, 4210121526cb985d0026469de0dc5f3767ce792149164df8fd0b43b4d6f30959, c8c523ff27a7fc4bef39dce97261c97bf724556cf32d0030090c168f82b20c7a, da4aefbcda028808dc892ad5a10bb528f129883ab9c29bb6800d298d3c26f848, d84cbd286724fe8c38f4e389ce9f582df93cac37172823f4eecacdcef0a5975d, 6f698f6983fc7ece0cade5f0c1bc7a66f7400229e0e99271ea9df6bece9473cf, ca2a7d82456036d905b5ea0e25678d8e6af165dc5d2a850450f22e2e63cb2767, 130d1f487072e512611489c4cd725bdfb59c31327d056bdbd22bea4f8fab576b, a3e5d8643dffb775a32fe73b08319dd6b201ec0f0215a048a22f0c47b9a08066
GLOBAL Ransomware	SHA256	a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73
	TOR Address	vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id[.]onion, gdbkvfe6g3whrzkdlbytksygk45zwgmnzh5i2xmqyo3mrpipysjagqyd[.]onion
Hellcat Ransomware	SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599
HYPERCALL	Domain	supportzm[.]com, zmsupport[.]com
	SHA256	c8f7608d4e19f6cb03680941bbd09fe969668bcb09c7ca985048a22e014dffcd, 03f00a143b8929585c122d490b6a3895d639c17d92C2223917e3a9ca1b8d30f9
INC Ransomware	SHA256	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

Attack Name	TYPE	VALUE
Interlock ransomware	SHA256	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f
Interlock RAT	SHA256	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3, 8afd6c0636c5d70ac0622396268786190a428635e9cf28ab23add939377727b0
	IPv4	64[.]95[.]12[.]71, 184[.]95[.]51[.]165
	Domains	existed-bunch-balance-councils[.]trycloudflare[.]com, ferrari-rolling-facilities-lounge[.]trycloudflare[.]com, galleries-physicians-psp-wv[.]trycloudflare[.]com, evidence-deleted-procedure-bringing[.]trycloudflare[.]com, nowhere-locked-manor-hs[.]trycloudflare[.]com, ranked-accordingly-ab-hired[.]trycloudflare[.]com
Lumma Stealer	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f, 65e1a8e550df1000eb91a7b679cf586efab0f24385b810f50349d50eb80ae806, 5ecafa1ecbc54d9a7b0e2e5c646578057215a246aeec2132fe7605a078aa43ec, d0e7a341fe199dbabb5f0798dba0564e9b60e4736a405c46eafc7232cc10dc40, 8a80210b1f6382cdbff2afc0c9a30092fc13687a33f293e36a9dbc0263a45101, a90294b602b51fff7b04e72deeb3e88fb200272321c939f00e13bde1d49ff1a3, 257bcb2bac99fe5e876857ec4511cada759e7f515de629e43cbb0f839575e7fc, 8bfdd127054e1ee93f58148677961929bb9265bb6ba9648f517118c1dfca6504,

Attack Name	TYPE	VALUE
Lumma Stealer	SHA256	6d07ace8512cb823f910bbb8cc9d16e54c04289c142b4b687815805e4ed0c52e, e60f84b8061804f4dfd5115dfb8a56b50b670a9a8650878160a45f22487d077c, e45f7df294a5bd06a40140e1f89788ac86fcbbebe7627a6b21c5819024369959, 82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b, f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc
Lynx Ransomware	Domain	hxxp[:]//lynxblog[.]net
	Email	martina[.]lestariid1898[@]proton[.]me
	SHA256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b, eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc, 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441, 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e, 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0, 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
Medusa Ransomware	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, 6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8cab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4,

Attack Name	TYPE	VALUE
Meduza	SHA256	643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2, d278aa079205cf4bb605de28bc6d6eca5a63b4cdd9d0c7488c40945d2b90b0a0, 44e715e3d9b5434c099452cc2cd991b1f02d4aba25114341a37dc142efd089ff, 9f2c70239fe518552ee44423564b075a85e0fc1e7bd80dc233bcc1f882ffceb9, b14af38c4230de20c7c4fefc1e3c5fffb1562bacedfebc56a508f55182a6fe88, 85b317bb4463a93ecc4d25af872401984d61e9ddcee4c275ea1f1d9875b5fa61, 2aa321a93bfa09139831e510e3cf9a869ece3d2e00889c846be169963cbb3b34, e29fa10b148be279c203e1f9079e7245b834f7912534c1bf4180af37686f621e, 73171634ceb5c5007cf78a6f32d6633590830f39f4e5311a4f323a4d44975ca7
Mesh Agent	SHA256	07f7ce55e75afda05241c70710d5c6769909d94193e41b370a29b5dca3ef1f3d, 12155ad4d117ea2b13131df52de4045e635e100d45bac057d6f5674e894dec99
MixShell	SHA256	d39e177261ce9a354b4712f820ada3ee8cd84a277f173ecfbd1bf6b100ddb713
Nitrogen Ransomware	SHA256	5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac7a71d321, 9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdafbede83051692e63, ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d8507ffe2c, c94b70dff50e69639b0ef1e828621c5fddcf144fea93e27520f48264ddd33273, 0db5c55ef52e89401a668f59bf4f69391f4632447c51483bb64749d7f2123916, 779576719a9c400a7a4abed0386e2111eb331160572c91a2fd8eaa1a7d6e6c63, e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85bda2bff6, 55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be, fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5d2afa2, ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281

Attack Name	TYPE	VALUE
Akira	MD5	7a647af3c112ad805296a22b2a276e7c
	SHA256	8a2d54e3230a4e7656ca760b512a879e0cacbe912a519a1be6916449bd6b5628, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218, d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50, ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5, 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2, 8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439, 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0, 68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a, 566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739, 51e250342faa954d28f46517a83a6ff81cce89c30dc86a9fb3c5fd50d095d850, 462505ad0fd657e7b031b0a3706fdcd04a20402c185b82caec91e29c2ff1e2d9, 43b0ac119ff957bb209d86ec206ea1ec3c51dd87bebf7b4a649c7e6c7f3756e7
Clop	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e
Dragon Force	SHA1	343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c, 229e073dbcbb72bdfee2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4
	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9

Attack Name	TYPE	VALUE
Play	SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30
	IPv4	108[.]61[.]142[.]190 , 45[.]76[.]165[.]129, 149[.]248[.]2[.]42
	URLs	hxxp://108.61.142[.]190/FX300.rar, hxxp://108.61.142[.]190/1.dll.sa, hxxp://108.61.142[.]190/64.zip, hxxp://108.61.142[.]190/winrar-x64-611.exe, hxxp://108.61.142[.]190/PsExec.exe, hxxp://108.61.142[.]190/host1.sa,
Qilin	Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
	IPv4	184[.]174[.]96[.]70, 180[.]131[.]145[.]73
	SHA1	c150e4ab20d59affc62b916c2c90686f43040a9f
	SHA256	cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f, d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6, 516927b55038c1702bc8a6a0262a39d5fe45f4b07527fdc42415533a9665264a, 43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c, 73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38
StealC	SHA256	e6e1106fec7137b46da15bdd0853b1b9a6104bce649a24145793e4d451261c6b, d63a83fb534fd92df1de5373ce6fa7febf6ca715c7528a2a806de49da2889078, a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c, 725df91a9db2e077203d78b8bef95b8cf093e7d0ee2e7a4f55a30fe200c3bf8f, 0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

References

https://www.cisa.gov/news-events/cybersecurity-advisories

https://research.checkpoint.com

https://www.rapid7.com/blog

https://any.run/cybersecurity-blog

https://www.ransomware.live

https://attack.mitre.org/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 28, 2026 • 3:30 AM

More at www.hivepro.com