EnCyb

TLP: GREEN

THE INTEL BULLETIN

AUGUST 2026

A Monthly Threat Intelligence Overview

www.encyb.com | cti.hunt@encyb.com

Social: LinkedIn | X | Facebook |

PCI QSA | CERT-IN Empaneled | ISO 27001 & ISO 9001 Certified|

Prepared By

EnCyb CTI Team

CONTENTS

Executive Summary 3
Global Threat Overview 4
Top 5 Target Sectors 4
Top 5 Risks Breakdown 4
Top 5 Active Malwares 4
Notable Campaigns & Events 5
Major Vulnerability & Exploit Intel 33
MITRE ATT&CK Mapping 35
Recommendations 36
Appendix 37
Threat Actors Observed 37
Malware Families Observed 38
Acronyms 38

Disclaimer:

- *This report is intended solely for cybersecurity awareness and defensive purposes.*
- *The screenshot figures are being exposed by threat actors or victims.*
- *The report is strictly for intended audience only.*
- *Do not expose it outside the organization.*
- *Some threat actor claims and dark web listings referenced may remain unverified at the time of publication.*
- *EnCyb is not responsible for any harmful actions taken based on the information presented in this report.*

Executive Summary

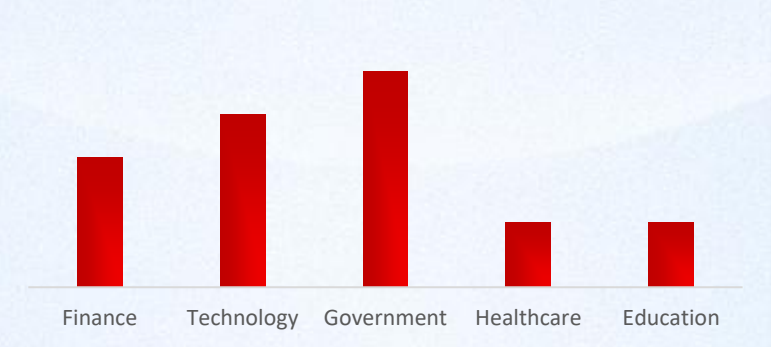
August 2026 was characterized by continued growth in **ransomware, cloud and identity-focused attacks, exploitation of internet-facing infrastructure, data extortion, and increasingly AI-assisted cyber operations**. Threat actors demonstrated a strong preference for abusing trusted services, exposed remote-access infrastructure, cloud identities, and legitimate administrative tools rather than relying solely on conventional malware. Ransomware operations such as **Gunra and Medusa continued to combine initial-access exploitation, credential theft, data exfiltration, and encryption**, while emerging extortion groups such as ExfilSquad increasingly relied on data theft and public disclosure without traditional ransomware deployment.

The vulnerability landscape remained equally significant. August reporting included actively exploited and critical vulnerabilities affecting **Fortinet products, macOS Screen Sharing, PostgreSQL, GitLab AI Gateway, Metabase, ServiceNow AI Platform, and other enterprise technologies**. The combination of rapidly weaponized vulnerabilities and exposed internet-facing infrastructure reinforces the requirement for continuous asset discovery, risk-based vulnerability management, identity hardening, and threat-informed detection.

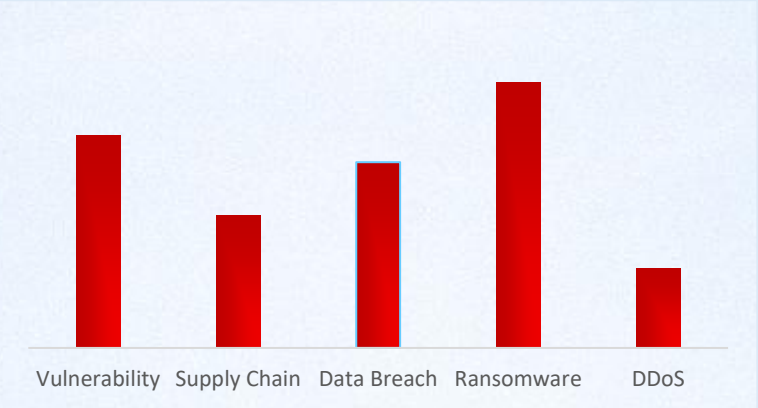
In overall, August's threat landscape highlights a shift toward identity-centric, cloud-enabled, and automation-assisted attacks. Organizations should prioritize phishing-resistant MFA, cloud identity protection, rapid vulnerability remediation, endpoint monitoring, and detection of data exfiltration and legitimate-tool abuse.

Global Threat Overview

Top 5 Target Sectors



Top 5 Risks Breakdown



Top 5 Active Malwares



Notable Campaigns & Events

A summary of significant cyber incidents, threat actor activities, and major cybersecurity developments observed during the reporting period, with focus on events linked to ongoing geopolitical tensions and emerging cyber threats.

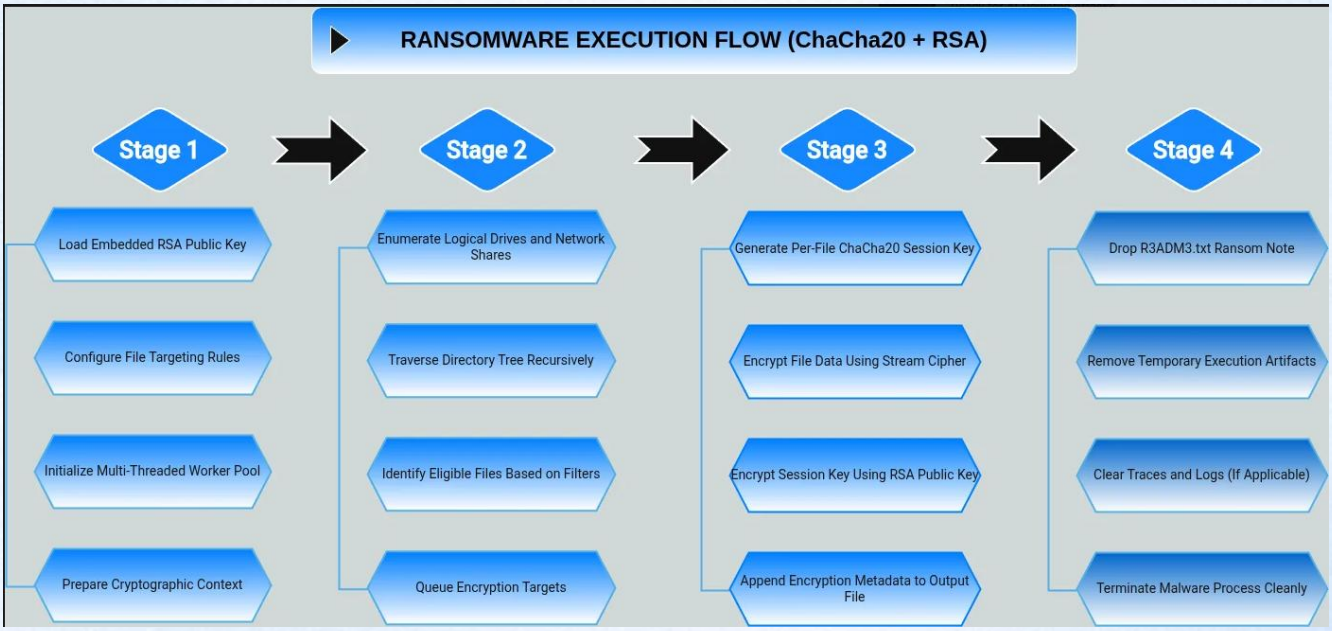
➢ Gunra Ransomware Exploits Fortinet Flaws and Bypasses MFA

Discovered in August 2026, a joint advisory from U.S. and South Korean cybersecurity agencies warned of **Gunra ransomware** attacks targeting critical infrastructure and organizations globally. Gunra operates as a **ransomware-as-a-service (RaaS)** operation and is derived from leaked **Conti ransomware source code**. The group has been observed exploiting known vulnerabilities in internet-facing **Fortinet FortiOS and FortiProxy** appliances to gain initial access, followed by credential theft, lateral movement, data exfiltration, MFA bypass, and ransomware deployment. The attacks employ a **double-extortion** model, where sensitive data is stolen before systems are encrypted and victims are threatened with publication of the stolen information.

Threat Actor : Gunra Ransomware Group / Gunra RaaS

Target Verticals : Critical Infrastructure, Healthcare, Financial Services, Government Services, Manufacturing, Transportation, and Professional/Nonprofit Services

Attack Technique : The threat actors exploit known authentication-bypass vulnerabilities in internet-facing Fortinet FortiOS and FortiProxy appliances, specifically CVE-2024-55591 and CVE-2025-24472, to obtain initial access. After compromising an SSL-VPN appliance, the actors intercept credentials and session cookies and use the stolen session information for session hijacking and internal access. Gunra has also been observed modifying VDI authentication-processing files to allow a designated OTP value to bypass MFA. The attackers subsequently use tools such as Impacket for lateral movement and credential dumping, exfiltrate sensitive data from Microsoft OneDrive, SharePoint, and MEGA, delete backups, and deploy ransomware to encrypt critical systems.



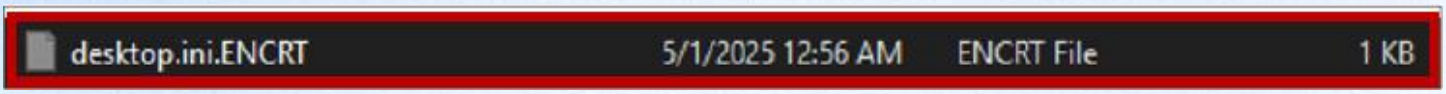
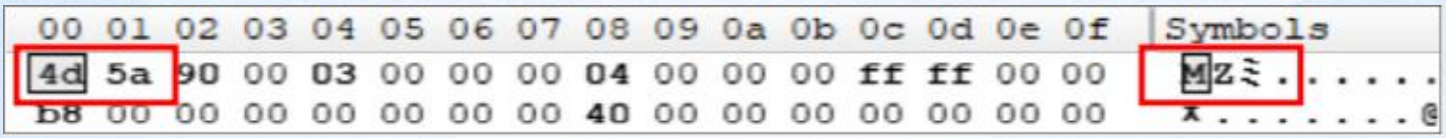


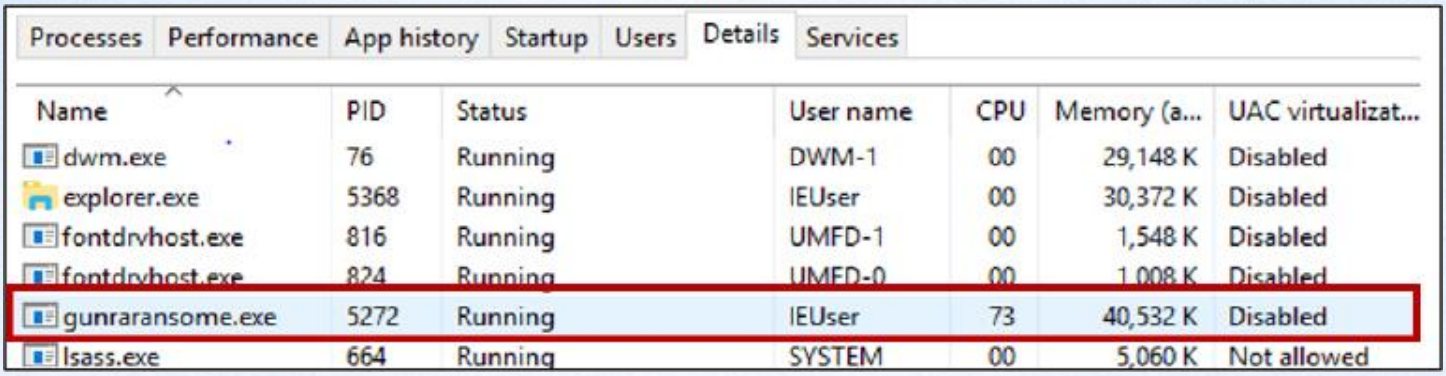
Figure: *Screenshots of files encrypted by Gunra Ransomware*

File Format: MZ Header- begins with the ASCII characters "MZ" (0x4D 0x5A). The signature is an executable file.



Behavior of Gunra Ransomware

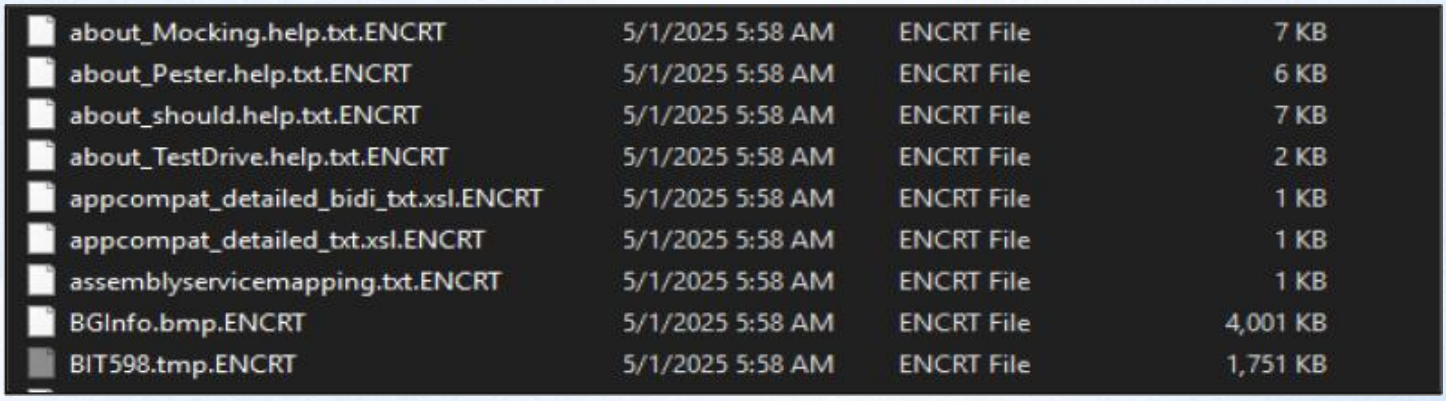
It creates a process with the name 'gunraransome.exe' in 'taskmgr'.



Deletes available shadow copies using the Windows Management Instrumentation (WMI) utility.

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe sha
dowcopy where "ID='{1E6BB20E-B7BC-40A3-A07A-C888
D9CFAB41}'" delete
```

Encrypts the victim's files and appends them with the extension ". ENCRT".



Drops a ransom note file named “R3ADM3.txt” in every directory where files are encrypted by the ransomware.

YOUR ALL DATA HAVE BEEN ENCRYPTED!

We have dumped your sensitive business data and then encrypted your side entire data.

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program, you must contact us.

We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free when you contact us.

You Only Have 5 Days To Contact Us!

How to contact us

Ñ. Download "Tor Browser" and install it.
O. In the "Tor Browser" open this site here :

http:/

Ó. After signup and login to this site and contact Manger

You need to contact "Manager" to recover all your data successfully.

!!!DANGER !!!
ÝO NOT MODIFY or try to RECOVER any files yourself.We WILL NOT be able to RESTORE them.
Und also we will publish your data on the dark web if there is no reply from you within 5 days.

Publish URL: http://gu

!!!DANGER !!!

External Threat Landscape Management

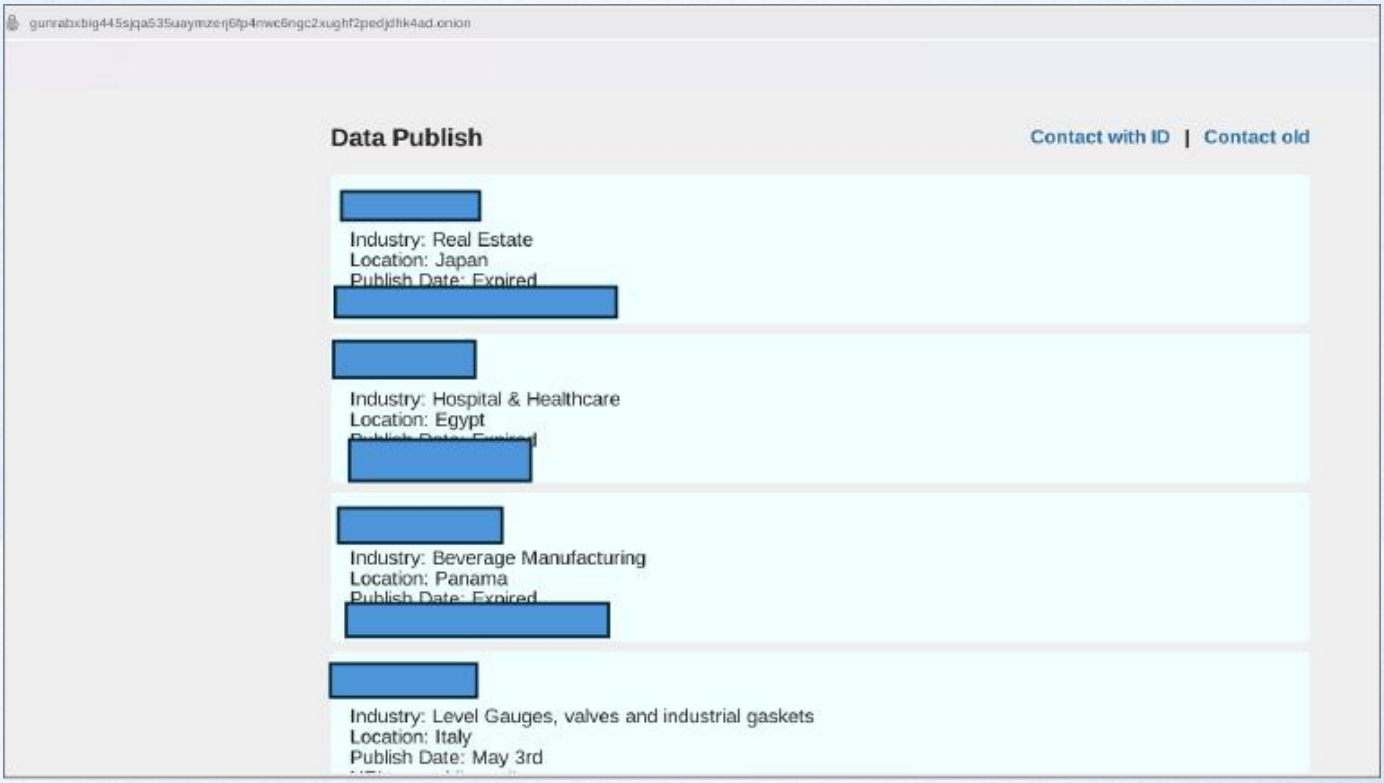
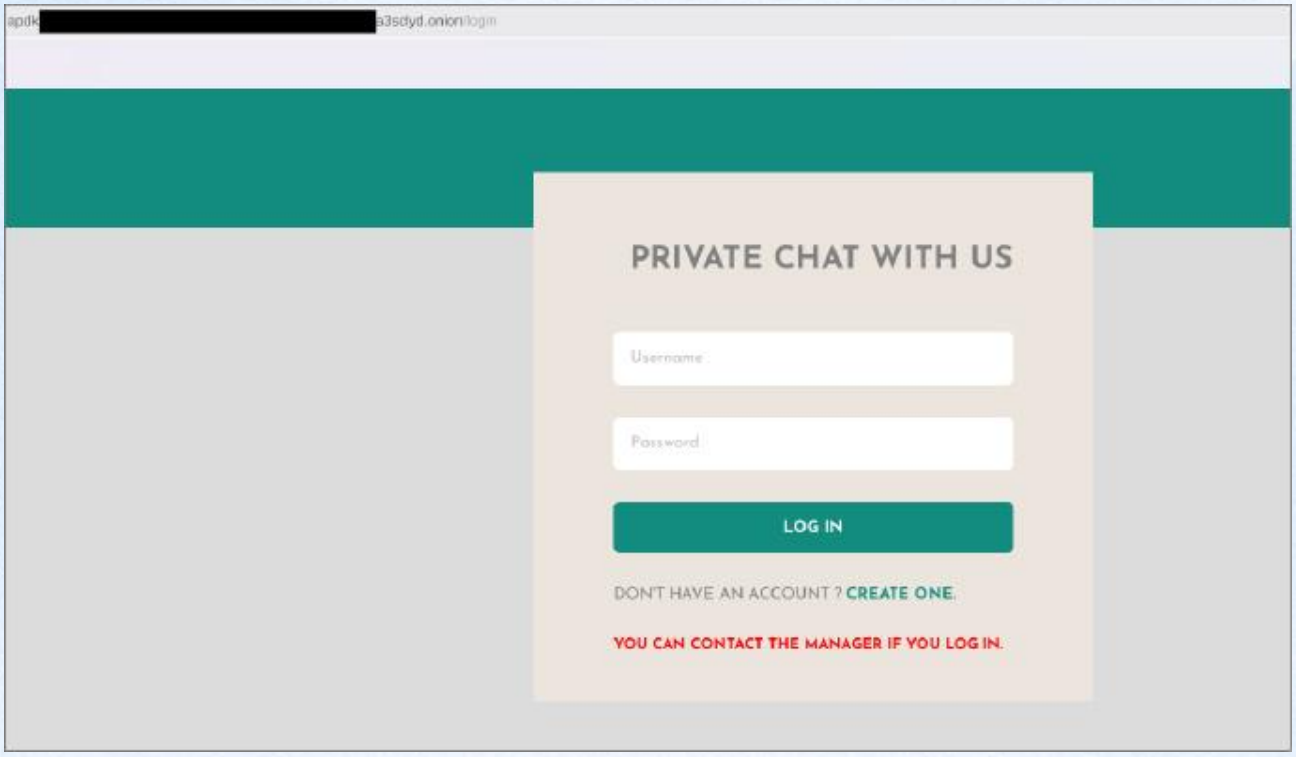


Figure: *Gunra ransomware data publish forum in DarkWeb*

Victims are typically given a five-day deadline, and the group conducts negotiations via Tor-based portals styled similarly to messaging apps like WhatsApp, complete with assigned roles such as “Manager.”



Indicators Of Compromise:

TYPE	INDICATOR
IP Addresses/Domain	23.239.119[.]2
	23.239.119[.]3
	23.239.119[.]4
	23.239.119[.]5
	23.239.119[.]6
	86.54.28[.]216
	103.125.234[.]14
	70.36.99[.]82
	211.21.210[.]181
	123.184.143[.]105
	182.204.21[.]240
	182.204.16[.]112
	123.244.187[.]144
	182.204.39[.]118

	67.43.53[.]10
	123.246.37[.]108
	91.201.66[.]146
	Datapub[.]news
	gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion
	lgiil72vkmdtbc3qv4tyq6wedyjxqr2qd4ze7xl2cxgerdnymxj7soqd[.]onion
	nsnhzysbntsqdwpys6mhml33muccsvterxewh5rkbmcab7bg2ttevjqd[.]onion
Email Addresses	a00f105546345756@proton[.]me
	4569f6322bc3b22e9@proton[.]me
	ilovemycubscout@gmail[.]com
	6449a3c1e612168526@proton[.]me
Hash(SHA 256)	2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751
	834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1
	91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0
	a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
File Accounts	forticloud-sync

➢ ExfilSquad Targets New Victims and Distributes Stolen Data via Torrents

Identified in mid-2026, ExfilSquad is an emerging financially motivated cybercriminal group conducting large-scale data breaches and extortion campaigns. Unlike conventional ransomware operators, the group generally does not encrypt systems; instead, it steals sensitive information and threatens to publish the data on its Tor-based Data Leak Site (DLS) unless a ransom is paid. In August 2026, ExfilSquad announced multiple victims across the U.S., UK, and Sweden, including organizations in government, education, aviation, technology, and other sectors.

Threat Actor : ExfilSquad – financially motivated cybercriminal/extortion group

Target Verticals : Government, Education, Financial Services, Aviation, Technology, Manufacturing, Retail, and Public Sector organizations

Attack Technique : The threat actors target misconfigured cloud/SaaS portals, CRM platforms, employee portals, and consumer-facing systems to obtain and exfiltrate large volumes of sensitive information. Following successful compromise, ExfilSquad uses data theft and extortion rather than traditional ransomware encryption. Stolen information is advertised through a Tor-based Data Leak Site, with victims given deadlines to negotiate ransom payments. The group has also adopted torrent-based distribution, assigning victims unique torrent trackers and web seeds to make stolen data widely accessible through peer-to-peer networks. This approach makes the leaked information difficult to remove once distributed and increases the potential reputational and privacy impact on affected organizations.

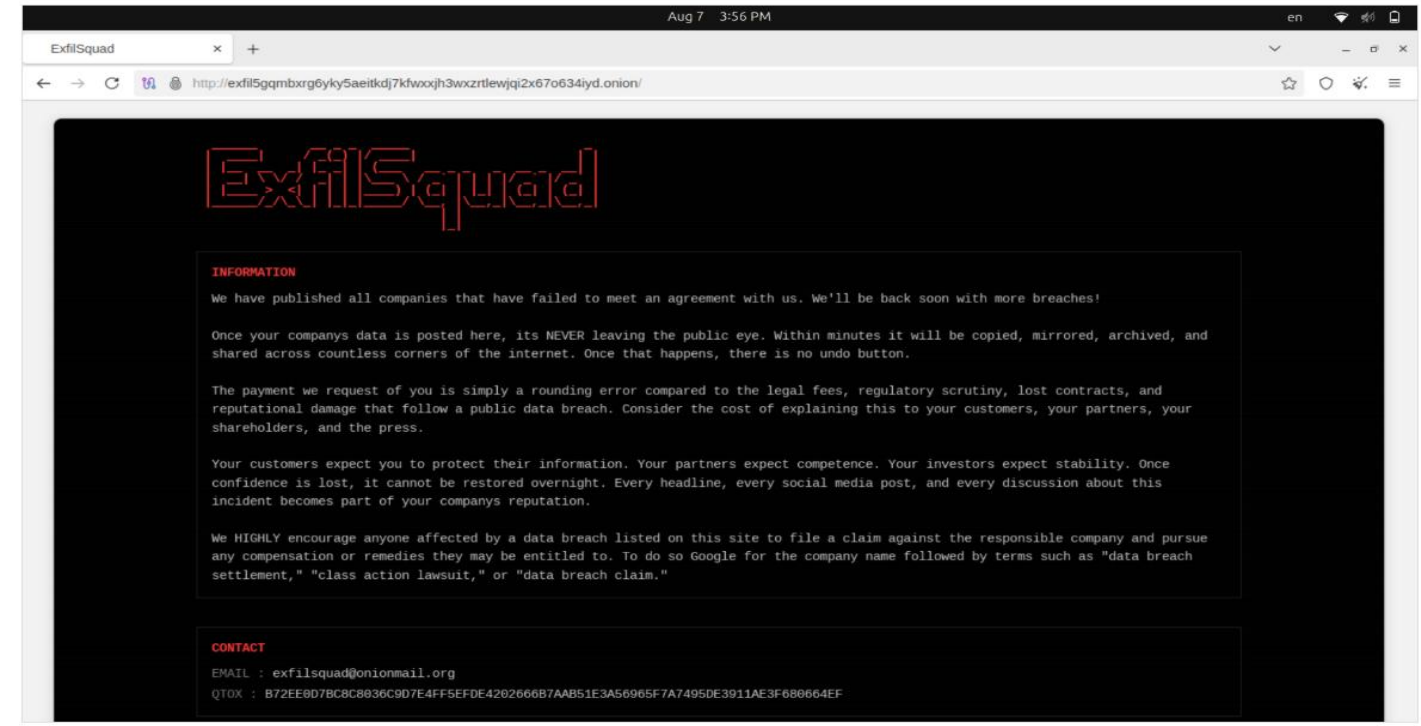


Figure: *ExfilSquad announced new victims this week and set a firm deadline -* ***August 5, 2026*** *- to complete all required negotiations. Otherwise, the stolen data will be released.*

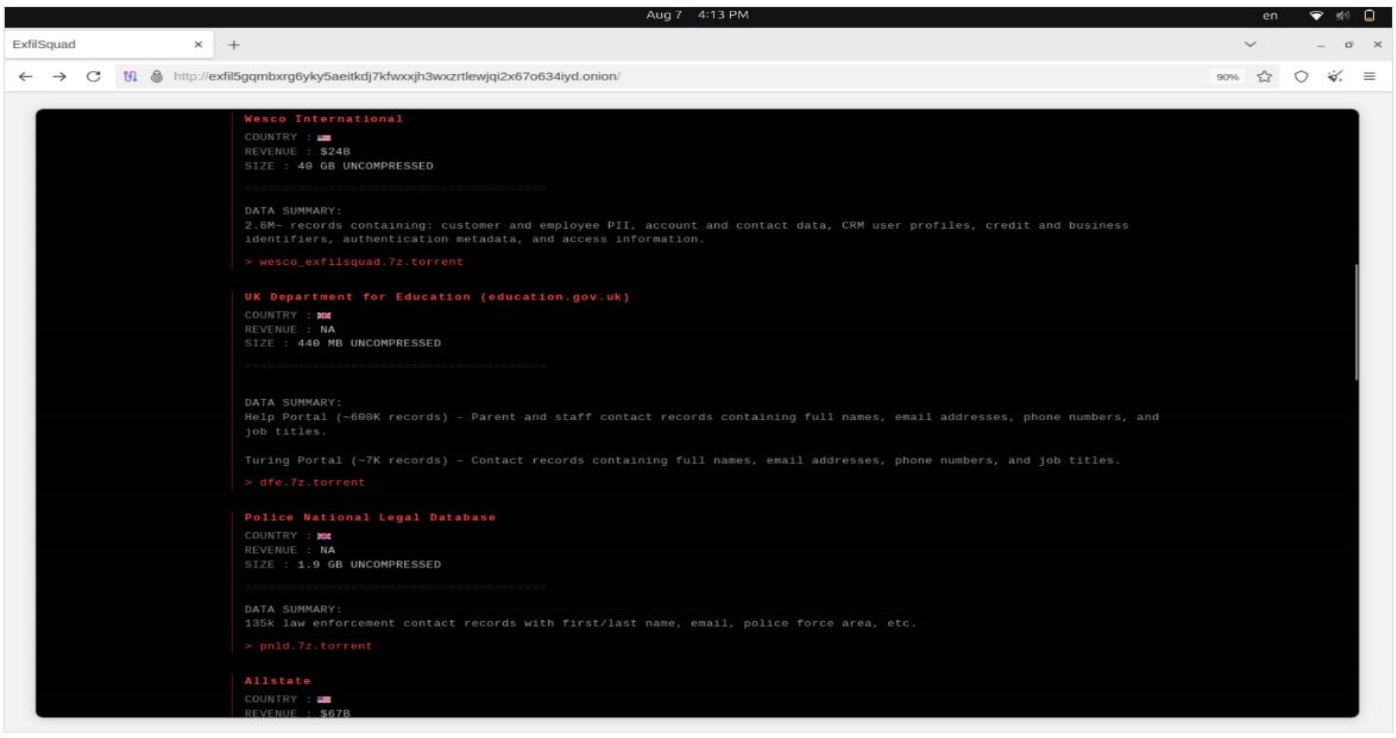


Figure: Data Leak Site (DLS) *in TOR*

Indicators Of Compromise:

TYPE	INDICATOR
Data Leak Site (DLS)	exfil5gqmbxrg6yky5aeitkdj7kfwxxjh3wxzrtlewjqi2x67o634iyd.onion
Contact Email	exfilsquad@onionmail.org
qTox Identifier	B72EE0D7BC8C8036C9D7E4FF5EFDE4202666B7AAB51E3A56965F7A7495DE3911AE3F680664EF

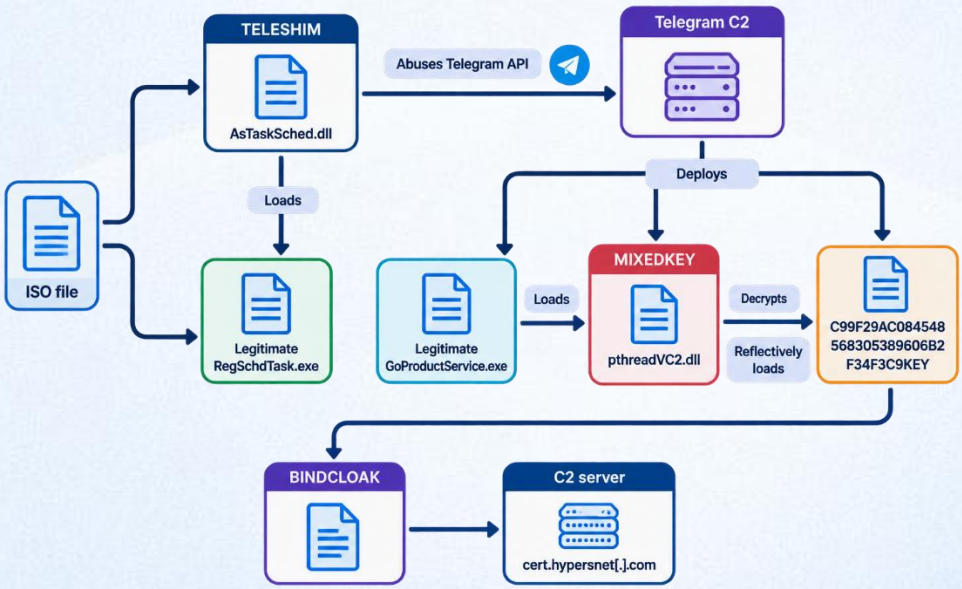
➢ OctLurk-Linked BINDCLOAK Targets Government Entities in the Middle East

A suspected threat group known as OctLurk has been linked to the modular backdoor BINDCLOAK through shared infrastructure and code similarities. OctLurk has been observed using BINDCLOAK for post-compromise activity against government entities in the Middle East, representing an expansion from its earlier targeting of organizations in Central Asia, with recent activity focusing on the energy sector. BINDCLOAK incorporates multiple evasion mechanisms, including techniques designed to prevent detection of API calls originating from unbacked executable memory regions. The malware also generates unique host identifiers using victim hostnames and volume serial numbers. Zscaler reported that BINDCLOAK supports core and plugin modules delivered from its command-and-control (C2) infrastructure, with C2 communication conducted through encrypted and structured messages over TLS via TCP.

Threat Actor : OctLurk – suspected cyber-espionage threat group

Target Verticals : Government organizations and Energy sector in the Middle East.

Attack Technique : The threat actors uses the modular BINDCLOAK backdoor for post-compromise activity. BINDCLOAK employs evasion techniques to conceal API calls originating from unbacked executable memory regions and generates unique host identifiers from hostnames and volume serial numbers. The malware supports core and plugin modules delivered through its C2 infrastructure, while command-and-control communication uses encrypted, structured messages over TLS via TCP.



Indicators Of Compromise:

TYPE	INDICATOR
Hashes	97124a93766be732e8fef5a56a5346a2
	C1f16e31ae71372ee45fa6fd6927c7b887a4e3f2
	789fd11285642861190dc074c1e9a5957073f1a2afebd5160f9cc907f7f320bd
	68926e6c958562deaae35de3d9f59de3
	Ccb2002fe8f5cc1f511d52309625b52d1c507421
	c84542ac30cbe9bb8bd648bad323c37801023bf9451c1c0990452466e084340f
	087499849115eb28c4364581d2b28d09
	86ee99f293a30720bcc898a4a8e391f93fb9be95
	32529043d15e9111ba284f1d8a9e4b3f58e071c6b69c8f271d4d02feacd44e66
	B776eb638fbb535708fb92b12fcc1731
	2377c47cfde148c2140faa7105628174f9c4d56d
	db11ff3f37a8b2aa25c480871504b886a6364167ecb501eacf7345f6bbf9582b
	7cbc51ada1a4aec88660ec32c408114b
	F46c01a5be2e08e36d4ec3302a8650a6ed25ec14
	5c2fe953da53da66fbcbb3be0fd6b63907c10714c337f287b2fc258857bbff6d
	3f60d53a2b5737d77e058d9e33cbe9eb
	1099bf51e53bd5fb32401edb4e0be841d8486b19
	cac1f37beaa814461f7709a073aeec468c74e5d70f7d693a9e367ece4a3a78be
	28b47bdf16d7af6f8ec21218eac9145a
	Fee6806c96f87bf1e240a2eb6fd7e045101d58d3
	0637069c7052118fd5c0f1113541bdd35e5f71cd9689f2516045da152c6fa8d9
	78a4f8574830bf7fbaf63d7da09be2b8
	Ee287d6a09295502ab2407aec336f9f0d8477d68
	3b3eaea783fd6dab90f0408274bf8a9c49adbdc70c0efd70658d65b0e1684a3f
	7a14a99d70d42d3f7bf72f843185fc07
	577b1cc894636f4ac5ad670b0079b9b7ade137c3
	3b0c658ebaa2bae80af97f390b9b2bb20a2f815eb584b2251255e84da4fa669d
C2 domain	cert.hypersnet[.]com

➢ AI-Fueled Attackers Shrink Patching Windows

AI is increasingly accelerating adversary operations and shortening vulnerability patching windows. CrowdStrike reported an **89% year-over-year increase in AI-enabled adversary activity**, with threat actors using AI for reconnaissance, credential theft, and evasion, while also targeting AI infrastructure through **LLMjacking and cost-harvesting**. During the first half of 2026, **88% of exploitation involving vulnerabilities with public PoC code occurred within 48 hours of release**, while **VAULT PANDA and GENESIS PANDA** exploited vulnerabilities within 24 hours. **Famous Chollima** leveraged AI-generated personas, while **Altered Spider** compromised over 300 software dependencies in a single day. The growing vulnerability landscape, with **48,200 CVEs in 2025 and around 43,000 by late July 2026**, further increases organizational exposure.

Threat Actor : Famous Chollima, Altered Spider, VAULT PANDA, and GENESIS PANDA

Target Verticals : Organizations operating AI workloads, cloud environments, software development infrastructure, and enterprise applications.

Attack Technique : The threat actors leverage AI to accelerate reconnaissance, credential theft, social engineering, and other attack activities while increasingly targeting AI infrastructure and APIs. Techniques include LLMjacking, cost harvesting, software supply-chain compromise, and rapid exploitation of newly disclosed vulnerabilities. CrowdStrike observed 88% of exploitation involving vulnerabilities with public PoC code within 48 hours of PoC release, highlighting the need for organizations to reduce vulnerability remediation windows from days or weeks to hours.

➢ DriveSurge Hijacks Legitimate Websites to Deliver Malware

DriveSurge is a newly identified threat actor conducting large-scale malware delivery campaigns through thousands of compromised legitimate websites. The campaign uses the **zTDS Traffic Distribution System** to profile visitors and redirect selected users to **FakeUpdates or ClickFix** lures. The activity targets both **Windows and macOS** users, with ClickFix campaigns using fake CAPTCHA or browser-error prompts to trick victims into executing commands through PowerShell or Terminal. DriveSurge employs **obfuscated JavaScript, visitor fingerprinting, and TDS failover infrastructure** to evade detection and selectively deliver payloads. Nopal Cyber assesses DriveSurge as an **Initial Access Broker (IAB) operating under a Pay-Per-Install (PPI) model**, with compromised endpoints potentially being sold to downstream threat actors.

Threat Actor : DriveSurge

Target Verticals : Organizations and users across Windows and macOS environments.

Attack Technique : DriveSurge compromises legitimate, high-reputation websites and injects obfuscated JavaScript that loads zTDS infrastructure. The TDS profiles visitors using IP, ASN, user-agent, and referrer information before selectively delivering FakeUpdates or ClickFix payloads. ClickFix campaigns instruct users to paste malicious commands into PowerShell or Terminal, while FakeUpdates delivers browser-themed malware. The actor also uses TDS failover servers, JavaScript obfuscation, and other evasion techniques to maintain payload delivery and avoid detection.

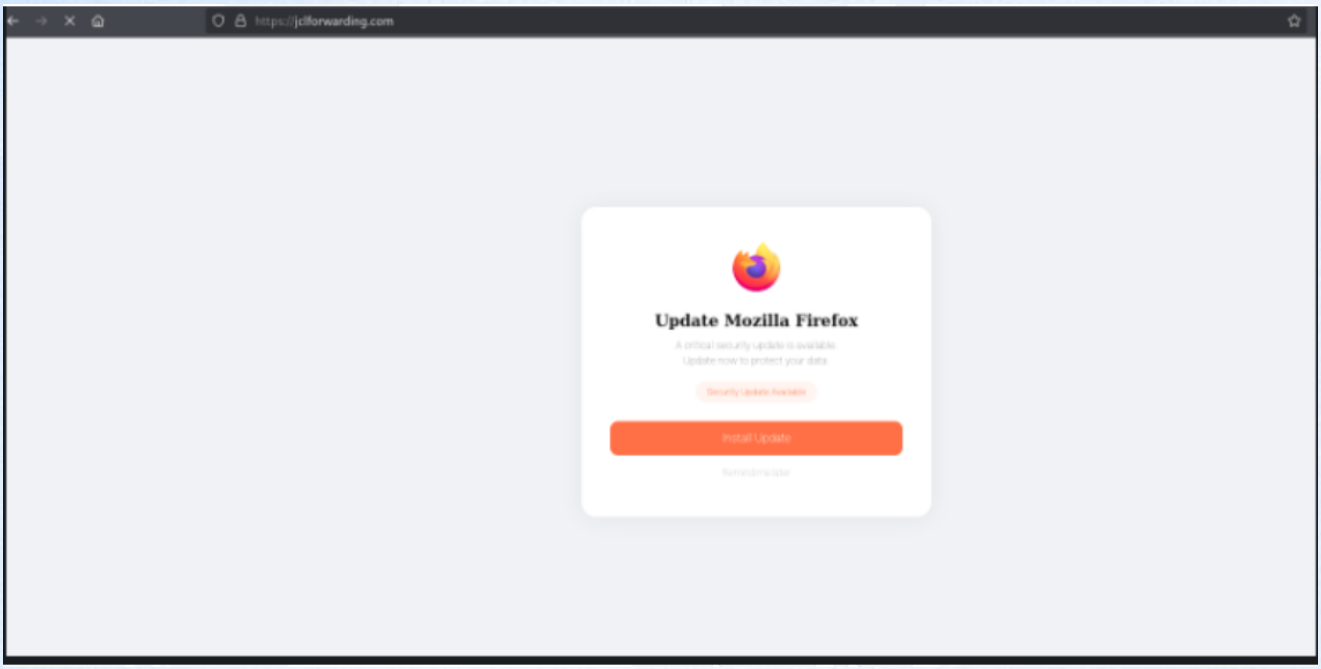


Figure: *Mozilla Firefox update page displayed on the compromised website*

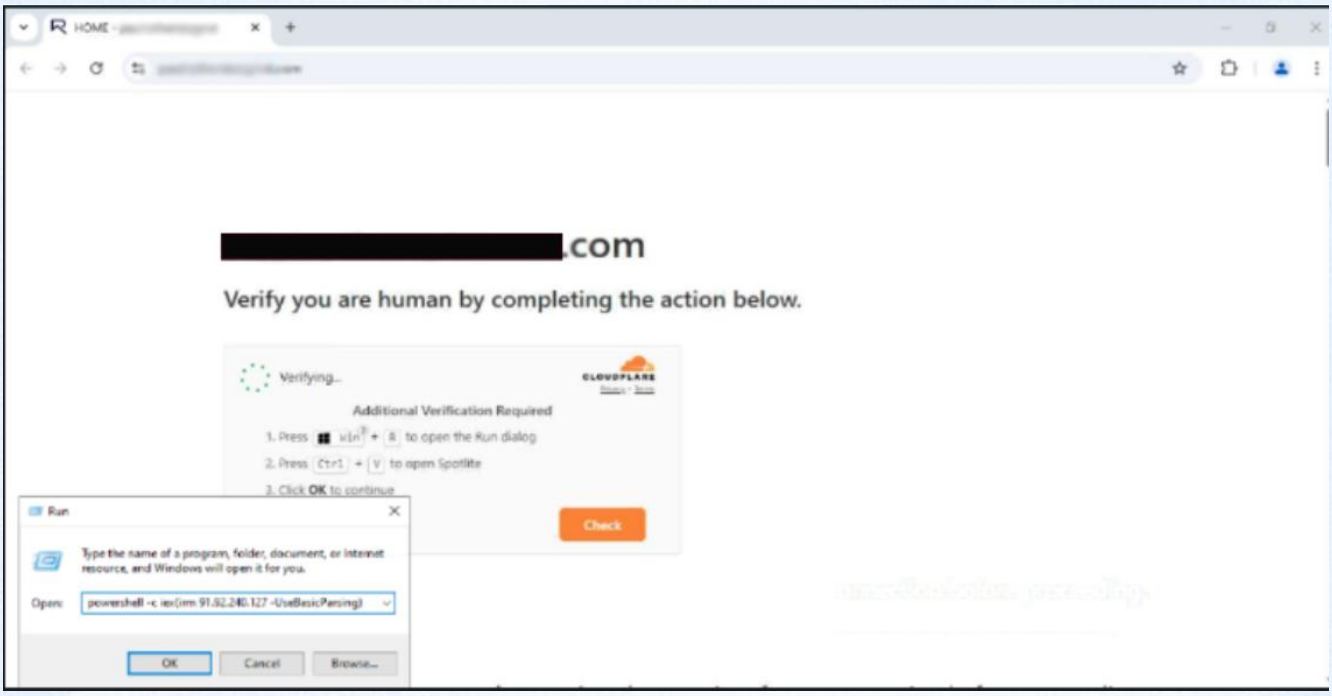


Figure: *ClickFix instance and Malicious Code*

Indicators Of Compromise:

TYPE	INDICATOR
Domain	beacontrace[.]bond
	jclforwarding[.]com
	check[.]first-node[.]rocks

	cptoptious[.]com
	newtdsone[.]shop
	captioto[.]com
	banerpanel[.]live
	testio[.]ecartdev[.]com
	ycyfugihih[.]cfd
	brightson[.]icu
	coverlink[.]icu
	datumprobe[.]icu
	eraggifts[.]icu
	keyview[.]icu
	traceglimpse[.]icu
	tracekey[.]icu
	webgleam[.]info
	cptoptions[.]com
Email	thiagorivera197151[@]ycyfugihih[.]cfd
	samuel_jordan16[@]flixtrend[.]net
IP Address	46[.]226[.]166[.]57
	147[.]45[.]42[.]200
	147[.]45[.]42[.]205
SHA-256	90aecb370dfb1a99a1f7de0a9c6842ab1b664521fddea16b0ec9a91f322646fc
	7aa15de93cf85729ddf970e8d7897f69ece3ca29608f73e784a9ba40c9cea18d
	8ecc7108cd679316bf5900e84f19b256dc399902cdede646493f502ac872cc1a
	e1ce4e6222396a58d13dddfe64c1dd21f1632bcbe11d1867d44bab4fc646883a
	29ac78c51bcdfe68c64830bdeb6e41437dd55e2691149741c9b78be03b6c82ea
	a84b032b49773c2318b11b1164d1aada69e940229aedbf8185c33fc7dd1d2cdf
	428bd0b0ac36dfdd223b3953dbe61c0baf227f893310b03e7afe3111462019c6
File Name	t.js
	Browser Update.exe
	script.js
	banner-js[.]php
	changelog.txt
URL	hxxps[://]newtdsone[.]shop/jsrepo?rnd=
	hxxps[://]cptoptious[.]com/jsrepo?rnd=

	hxxps[://]captioto[.]com/jsrepo?rnd=
	hxxp://46[.]226[.]166[.]57/ce3cbfc887?force=1

➢ Kimsuky (APT43) Scales AI-Driven Espionage

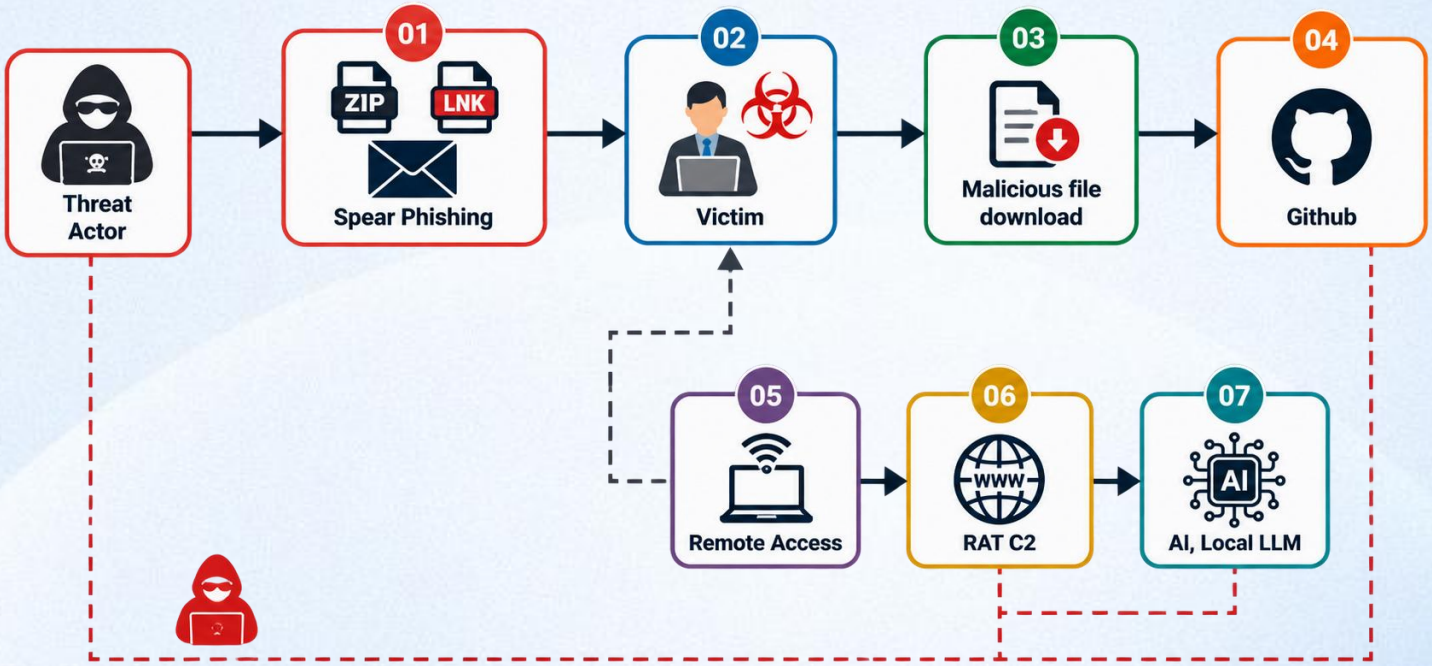
Kimsuky, a North Korean state-sponsored cyber-espionage group, has expanded **Operation GitPower** by integrating artificial intelligence capabilities into its established attack infrastructure. Researchers identified continued use of **spear-phishing emails, malicious LNK files, obfuscated PowerShell loaders, scheduled-task persistence, and GitHub-based C2**, while also uncovering local AI environments using **Ollama, GPT4All, and Msty**, alongside RAG, AI-agent frameworks, Semantic Kernel, LangChain, and Whisper. The campaign also uses **AI-generated decoy documents** to create more convincing phishing lures, while encrypted payloads disguised as image files are retrieved from GitHub repositories. The activity indicates that Kimsuky is building an AI-enabled operational ecosystem to improve phishing, malware development, intelligence analysis, and automation.

Threat Actor : Kimsuky (APT43)

Target Verticals : Policy Organizations, Academia, International Cooperation Organizations, Diplomatic Missions, Military, Security, Security Research, and Virtual Assets

Attack Technique

The group leverages spear phishing, AI-generated decoy documents, malicious LNK files, obfuscated PowerShell execution, scheduled-task persistence, GitHub-hosted C2, encrypted payloads disguised as image files, and local AI/LLM environments for malware development, document analysis, intelligence processing, and operational automation.



Indicators Of Compromise:

TYPE	INDICATOR
Hashes	981dadc1a7ab50d6ff600a69c904a350fcc2d2050ac94589321f51ac5527c78d
	18fa10ff013cf82974f00875e23dae48d4d2dc0993a348f8069dd32845de39a1
	a4f72ce8b5736fe3ca2083cfe21bd51697f12e900e307c357cb8523b8f86e3ec
	9be8f2be7ad882e8423c269a0540b7c73d6470311ddfcfcd318ff9d1983e2935
	2df24d850d6a50410e6503bc449a61778e5e88722ea4e20e198ea61e45a6903e
	d185c71b58b1ebed730feb8bbb6568d80542d2b8228b2777d280a7a4b114fdd0
	018c31af135a0bc5e068df26d866440b28164aa4a659ea7df47bcbaab4a898cd
	a40a61e54be9cc1671ea6832fef8139ce811a7d759058bb8b4ca86863f4cc1bd
	4d37b4ccd6e4c0c9de82e66e40dfb6412b92ea33bcf10442a290b0732eeadae0
	863f1405a190e2d87f06c5a9383b91b660bf4a0cd1b7c1c4987a071ee1c7dbb1
	24dd215bb0946dde131f8fd0a3cc4d9ab6c095c31f8b57fb62462105e9e57cc0
	456ed6926b706c203ac65b5174ac2ce78a5dad2ef0f083ae1f0aedd75d811ca2
	4453b9e985f452365995c399f5292c92764570f03e6a066d7845320dd4ad09a1
	b50422ec3a98d098bb3f7d728012da7e1795221c8b0624562568dff87ab5de2a
	9d50b542ddc7f46aba4c621c503495ed7992d84f92fd89cbb240963636ae19d3
	4b0358c7e4afa54bc489a6199cca132b5f4a330892eb15bf06c0c4da9e020df2
	70a7f0aeda59f8563031b5ab4554b52f32118a96d197871181aca4ba91168cff
	22180919f562fb9f6e50d7f20b2eb3f94eb009c212b74b45cf77659fe8274d5b
	e49399502d455dbd38f1140bffa761701608526aefb7174646c2f8ffe881ae73
	216ef271db7a1fe301bc4ca8cafb3849e4db57ff05a4bc6c146c13a026c6aa9c
	0432ae814945633b605c77d137bef96c7f84934c682aada69baa326dce781286
	7bc61d1bbc90d66d9988fd3baacd7834b1d2dfefe6d4ac999a194bccb9ba7dfc
	531aacc5cfe1abb14aaf55a2128940db30c63cbc8d5f9846ff8608e566fecb88
	5b1f75205cb79a8c8a3d8083f34b552852dfd567dd65763183b7536a29f55f5b
	e34d73a1da492c9a79a9729f2f7d9d4b5a2448f44934bd5552bd0bbbe1586767
	5daf3d123d58bc15e7b3130bc7c33d29b422b6aa485c67f69fbe0ed0ea95d27f

➢ Lazarus Group Exploits Windows Zero-Day in Operation Dream Job

Lazarus Group, a North Korea-linked threat actor, has been observed exploiting **CVE-2026-68820**, a previously undisclosed Windows **AFD.sys local privilege-escalation zero-day**, as part of its long-running **Operation Dream Job** campaign. The attacks begin with sophisticated fake job offers and impersonation of recruiters from organizations including **Lockheed Martin and Enveil**, followed by malicious PDFs or trojanized PDF viewers. Researchers identified two infection chains: one using **DLL sideloading to deploy MISTPEN and ForestTiger**, and another using a trojanized **SecurityPDF** viewer to deliver the **Troy** backdoor. After gaining SYSTEM-level privileges, Lazarus deploys the **FudModule rootkit** and uses compromised webmail, WordPress, and other legitimate infrastructure for command-and-control. The campaign has targeted **defense, aerospace, and aviation organizations in France, Germany, Brazil, and India**.

Threat Actor : Lazarus Group (Operation Dream Job)

Target Verticals : Defense, Aerospace, Aviation, and Defense-Related Technology Organizations

Attack Technique

The group leverages **spear phishing, fake job offers, recruiter impersonation, weaponized PDFs, SEO-optimized impersonation websites, trojanized PDF viewers, DLL sideloading, privilege escalation through CVE-2026-68820, FudModule rootkit deployment, in-memory execution, and compromised webmail/CMS infrastructure for C2**. The campaign uses MISTPEN, ForestTiger, and Troy to perform reconnaissance, file operations, process management, and remote access.

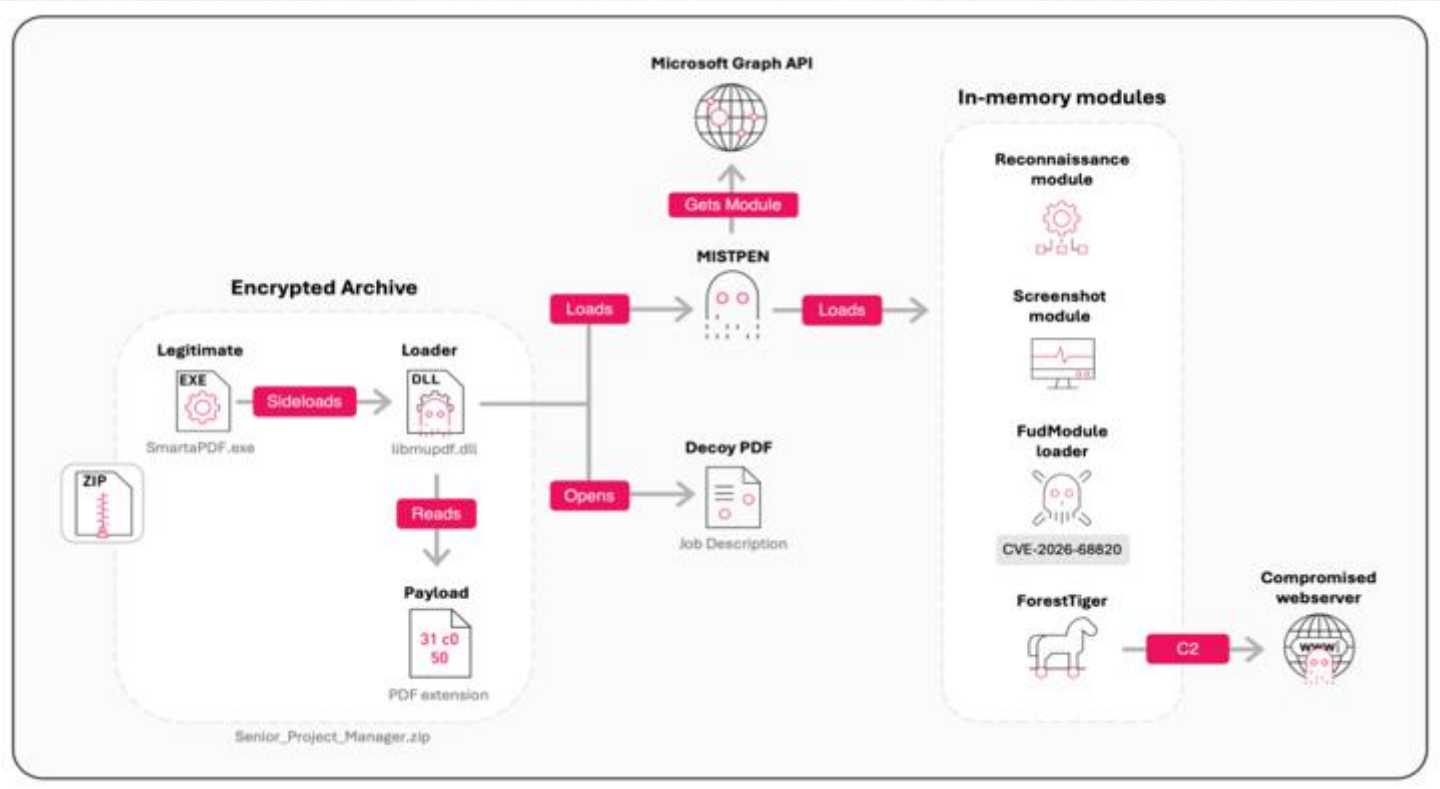


Figure: *High-level overview of the DLL sideloading infection chain*

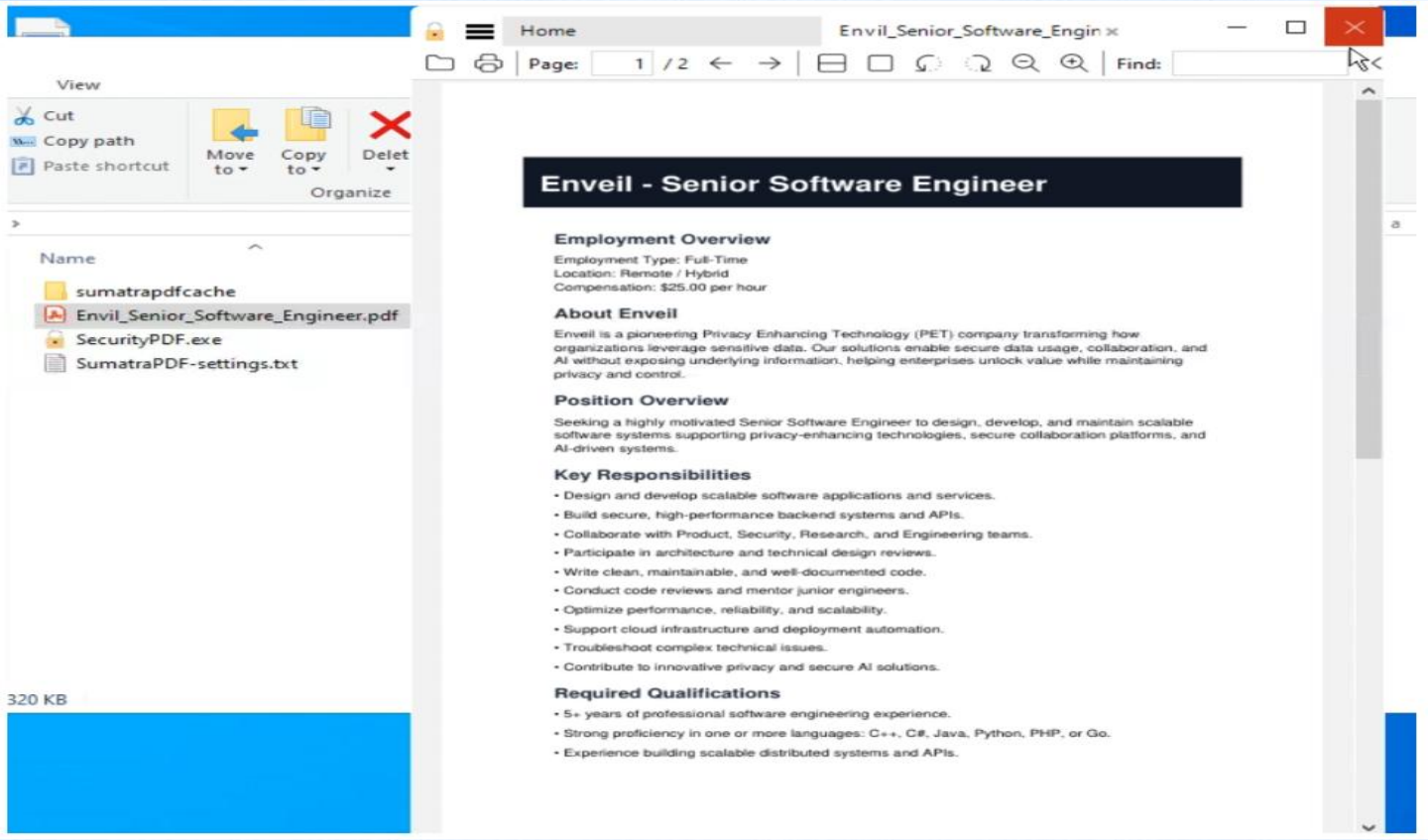


Figure: *Crafted PDF opened by SecurityPDF*

➢ ShinyHunters Claims Metabase Breach Through SQL Injection

ShinyHunters, a financially motivated cybercriminal group, **claimed responsibility for the compromise of Metabase** following the exploitation of a previously unknown vulnerability in Metabase instances. Metabase confirmed that attackers abused a chained vulnerability beginning at the **password-reset endpoint**, enabling SQL injection to create an authenticated session and subsequently generate an API key for bulk data access. Metabase stated that **under 3% of its cloud customers were compromised** before remediation, with some self-hosted and open-source installations also affected. Metabase released security fixes on August 6 and urged customers to upgrade immediately. The ShinyHunters attribution remains a **claim by the group and has not been independently confirmed by Metabase**.

Threat Actor : ShinyHunters

Target Verticals : Organizations Using Metabase for Business Intelligence, Data Analytics, and Cloud-Based Data Services

Attack Technique

The attackers exploited a **chained SQL injection vulnerability** through the Metabase password-reset functionality to create unauthorized sessions, obtain administrative access, generate API keys, and enable bulk data retrieval. ShinyHunters subsequently listed Metabase on its leak site as part of an extortion claim.

➢ LiteLLM Supply-Chain Attack Exposes Developer and Cloud Secrets

In August 2026, researchers reported that the **LiteLLM supply-chain compromise** was part of the wider **TeamPCP** campaign that began with the compromise of Aqua Security's **Trivy** vulnerability scanner. LiteLLM's CI/CD pipeline automatically installed a compromised Trivy release, allowing attackers to publish malicious LiteLLM versions **1.82.7 and 1.82.8** to PyPI. The malicious package executed automatically through a Python .pth file and harvested **Git credentials, CI/CD tokens, AWS/GCP/Azure credentials, Kubernetes secrets, SSH keys, API keys, environment variables and cryptocurrency credentials**. CloudSEK estimated exposure across **more than 2,500 organizations and approximately 434,000 CI/CD pipelines**, although these figures represent **reconstructed exposure rather than confirmed compromise of every organization**. Later analysis found that more than **95% of the identified organizations were exposed before the malicious LiteLLM packages were published**, indicating that the broader Trivy compromise accounted for most of the exposure.

Threat Actor : TeamPCP

Target Verticals : Software Development, Cloud Services, AI/ML Infrastructure, Technology, Financial Services, Healthcare, Government, and Organizations Using CI/CD Pipelines

Attack Technique

The threat actor leveraged software supply-chain compromise, malicious Trivy releases, stolen developer credentials, compromised CI/CD pipelines, poisoned PyPI packages, Python .pth auto-execution, credential harvesting, cloud and Kubernetes secret theft, and downstream propagation through automated build environments.

➢ Jewelbug Breaches Government Webmail While Running Parallel Crypto Fraud

Jewelbug, also tracked as **Earth Alux and REF7707**, has been linked to a campaign combining **government espionage with cryptocurrency fraud**. Researchers observed the group compromising a shared webmail platform used by more than **15 government tenants**, injecting malicious JavaScript into common templates to steal browser cookies and identify targeted government accounts. The campaign collected **more than 580,000 browser cookies, several thousand credentials, and over 2,300 email bodies**, while Jewelbug also used **Antino, ClientKing, and the XG-Web framework** against Windows, Linux, ARM64 systems, and ASUS routers. The group further used **public Google Docs to host obfuscated payloads**, allowing malicious traffic to blend with legitimate cloud services.

Threat Actor : Jewelbug (Earth Alux / REF7707)

Target Verticals : Government, Military, Telecommunications, Defense, Education, Aviation, and Critical Infrastructure

Attack Technique

The group leverages **watering-hole attacks, webmail template injection, browser-cookie theft, malicious JavaScript, fake software-update lures, Antino and ClientKing implants, DNS/Web-based C2, compromised infrastructure, and public Google Docs for payload delivery**. Jewelbug also conducts SEO poisoning and click-fraud operations to direct cryptocurrency users to fraudulent exchange websites.

Indicators Of Compromise:

TYPE	INDICATOR
Hashes	e6ff096a0562c0042b09d250bd60272ffcd8d72bd95c563842acf765a8dc8bcf
	01b5c6acb20e41799a0e96d9d1d6e1c44791883706b6285e874fcb15cc93b31a
	e809da86bd81463347fa7f922d3e088755a94a331889d32acb55aa8f57778a34
	f1ef5fe4c0cdcff13cc750c867728b89719f81437bdc49041edd1ae1f3edb4e8
	e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530
	b09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff
	c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc
	0c39264337a1186b2e765e24073399cbdcba118306614eb411e315887af578bd
	9b7df409c9a89f7536d3ba7b6d43fb6dbac618c8bb52615ba34cc971ad71bbf3
Domain	fonts[.]tarotfree101[.]top
	fonts[.]chrorne[.]com
	robot[.]avbliud[.]com
	microsoft-flash[.]com
	www[.]wps-cn[.]com
	www[.]f1ash[.]org[.]cn
	browser-update[.]pages[.]dev
	eastus2[.]wac-azure[.]com
	mailbycloud[.]com
	www[.]jkskhei[.]com
	ns1[.]jkskhei[.]com
	dns[.]wizkidblogger[.]com
IP Address	103[.]87[.]9[.]62
	152[.]42[.]174[.]15
	143[.]246[.]208[.]236
	43[.]246[.]208[.]179
	47[.]84[.]37[.]113
	47[.]84[.]51[.]173
	167[.]71[.]195[.]255
	38[.]12[.]1[.]47
	129[.]212[.]237[.]224
	47[.]87[.]71[.]167
	47[.]250[.]208[.]35
	219[.]76[.]254[.]184

➢ TheHatman Raids Fortune 500 Azure Directories

TheHatman, a financially motivated threat actor, has claimed access to **Microsoft Azure/Entra environments** belonging to multiple major organizations and the sale of internal employee-directory data. The exposed datasets reportedly contain **employee names, corporate email addresses, job titles, departments, reporting relationships, group memberships, service accounts, and privileged account information**, providing valuable reconnaissance for subsequent spear-phishing, business email compromise, and social-engineering activity. Reported datasets include **more than 1.7 million records from McDonald's, approximately 800,000 from TCS, 425,000 from Vodafone, 250,000 from HCL Technologies, and 185,000 from IHG**, with additional organizations also listed. Hudson Rock identified infostealer-compromised Microsoft credentials associated with several organizations, but the **exact initial access method has not been conclusively established**, and some affected organizations have disputed or questioned the recency of the data.

Threat Actor **:** TheHatman

Activity window : August 1, 2026 (campaign start) – August 12, 2026 (most recent observed activity)

Target Verticals **:** Retail, IT Services, Telecommunications, Hospitality, Logistics, and Large Enterprises

Total claimed exposure : 3.6M+ records across 9 organizations

Attack Technique **:** The actor reportedly leveraged **compromised credentials to access Azure/Entra directories and enumerate employee identities, organizational relationships, group memberships, service accounts, and privileged accounts**, followed by large-scale directory data exfiltration. The resulting intelligence can facilitate **targeted spear-phishing, business email compromise, credential attacks, impersonation, and privilege escalation**. Hudson Rock linked credentials associated with affected organizations to **infostealer infections**, although this does not by itself prove that infostealers were the direct entry mechanism.

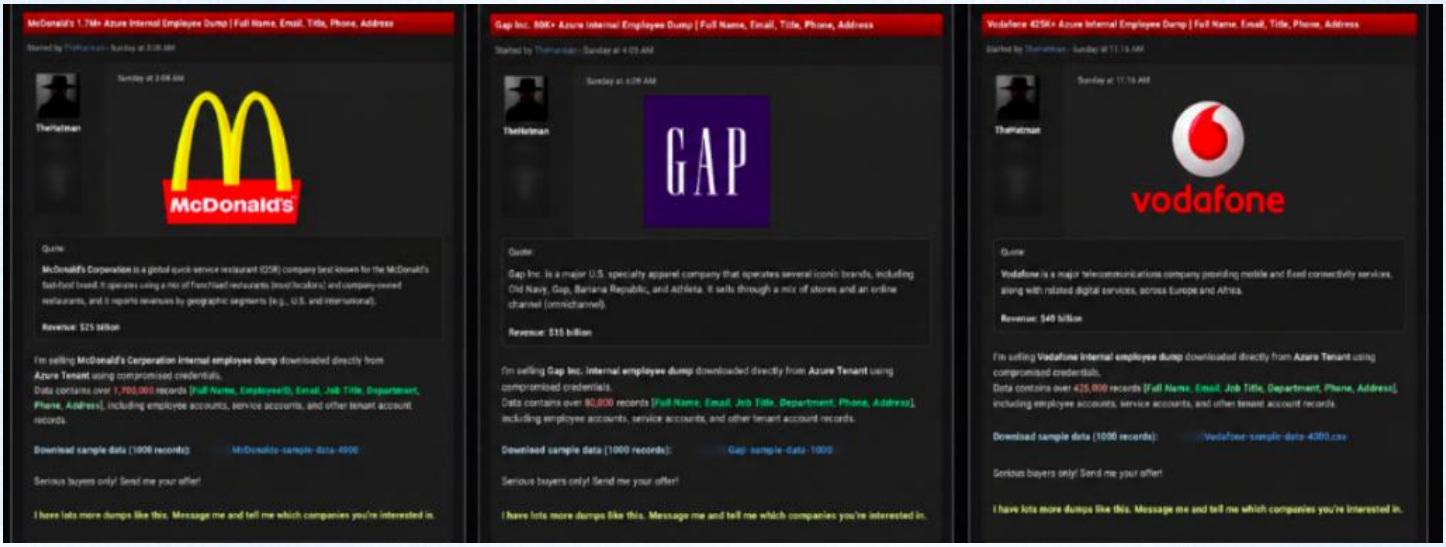


Figure: *TheHatman's alleged Azure-related data claims involving McDonald's, Gap and Vodafone including claimed record volumes and data types. Based on TheHatman darkweb leaksite forum claims and infostealer evidence.*

Major Victims

Organization	Record Claim	Reported Status
McDonald's	Claimed 1.7M+ records	Reported
Vodafone	Claimed 42K+ records	Reported
Gap Inc.	Claimed 30K+ records	Reported
Tata Consultancy Services (TCS)	Claimed 180K+ records	Reported
Hyundai	Claimed 170K+ records	Reported
HCL Technologies	Claimed 230K+ records	Reported
Marriott Hotels	Claimed 90K+ records	Reported
Hexaware	Claimed 20K+ records	Reported
InterContinental Hotels Group (IHG)	Claimed 150K+ records	Reported

➢ Medusa Ransomware Expands Attacks on Critical Sectors

Medusa ransomware has impacted **more than 500 victims as of April 2026**, according to an updated joint advisory issued by **CISA, FBI, and HHS on August 18, 2026**. Operating as a **Ransomware-as-a-Service (RaaS)** operation, Medusa uses a double-extortion model by exfiltrating sensitive information before encrypting systems and threatening to publish the stolen data. The group has primarily affected **Healthcare and Public Health**, while also targeting the Defense Industrial Base, Critical Manufacturing, Government Services and Facilities, Information Technology, and Financial Services sectors. Medusa affiliates gain initial access through **phishing and exploitation of vulnerabilities in ScreenConnect, Fortinet EMS, Fortra GoAnywhere, and BeyondTrust**, and abuse legitimate remote-access tools such as **AnyDesk, Atera, ConnectWise, eHorus, N-able, SimpleHelp, and Splashtop** to maintain access and blend with normal administrative activity.

Threat Actor : Medusa Ransomware (RaaS)

Target Verticals : Healthcare and Public Health, Defense Industrial Base, Critical Manufacturing, Government Services and Facilities, Information Technology, Financial Services, Education, Legal, Insurance, and Manufacturing

Attack Technique : The Medusa leverages **phishing, exploitation of remote-access and internet-facing vulnerabilities, credential theft, data exfiltration followed by encryption, double extortion, and legitimate remote-access tools for persistence and defense evasion**. The updated advisory also notes rapid exploitation of newly disclosed vulnerabilities, with affiliates reportedly able to exploit vulnerabilities within **24 hours of public disclosure**.

Dark Web Presence

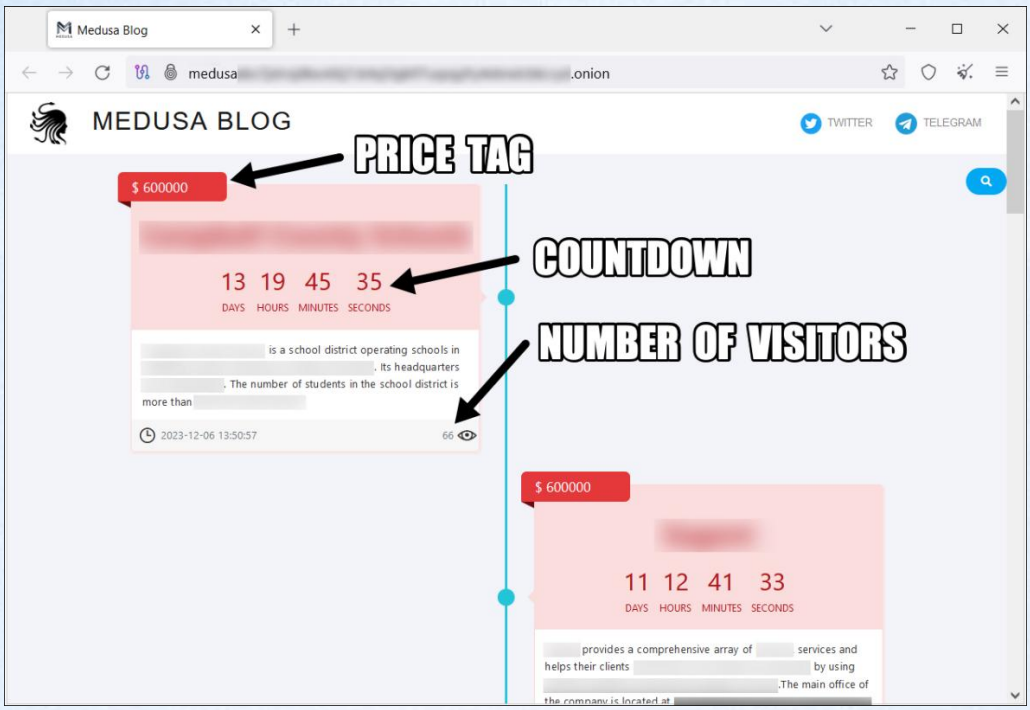


Figure: *Medusa Blog dedicated leak site.*

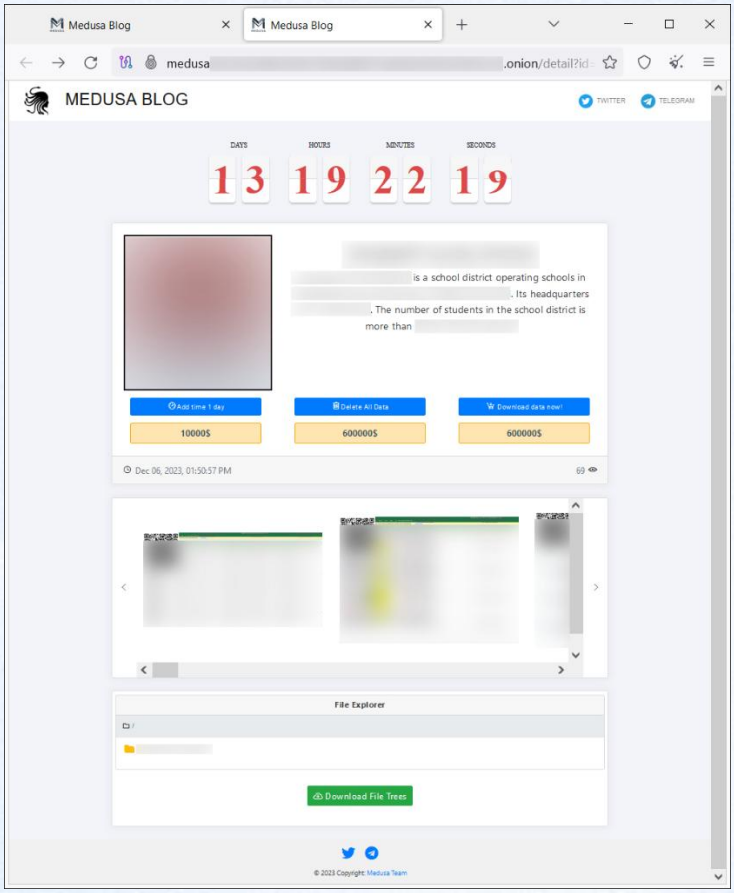


Figure: *Post on the Medusa Blog to a victim.*

A recent post on the Medusa Blog included a video displaying files allegedly belonging to a compromised organization. The video carried the title caption "**Medusa Media Team,**" which may indicate a dedicated branch responsible for managing the group's public image and branding. While similar videos have not accompanied every victim post observed on the site, it remains unclear whether this represents an emerging tactic or an isolated instance. Nevertheless, ransomware groups such as Medusa rely heavily on **reputation and perceived credibility**. Publishing curated videos of victim data can strengthen the group's brand, demonstrate its claimed impact, and reinforce its image as a capable and credible threat actor.

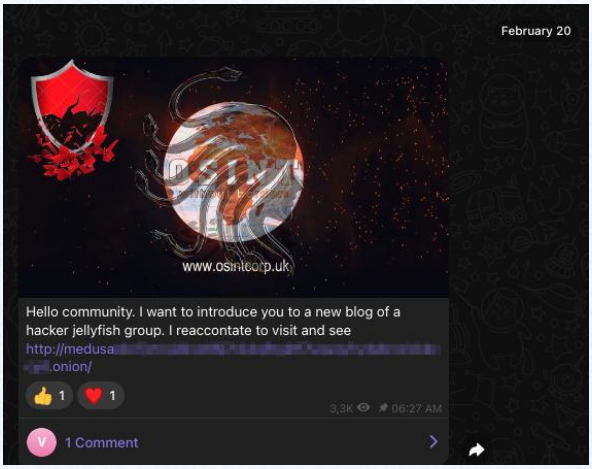
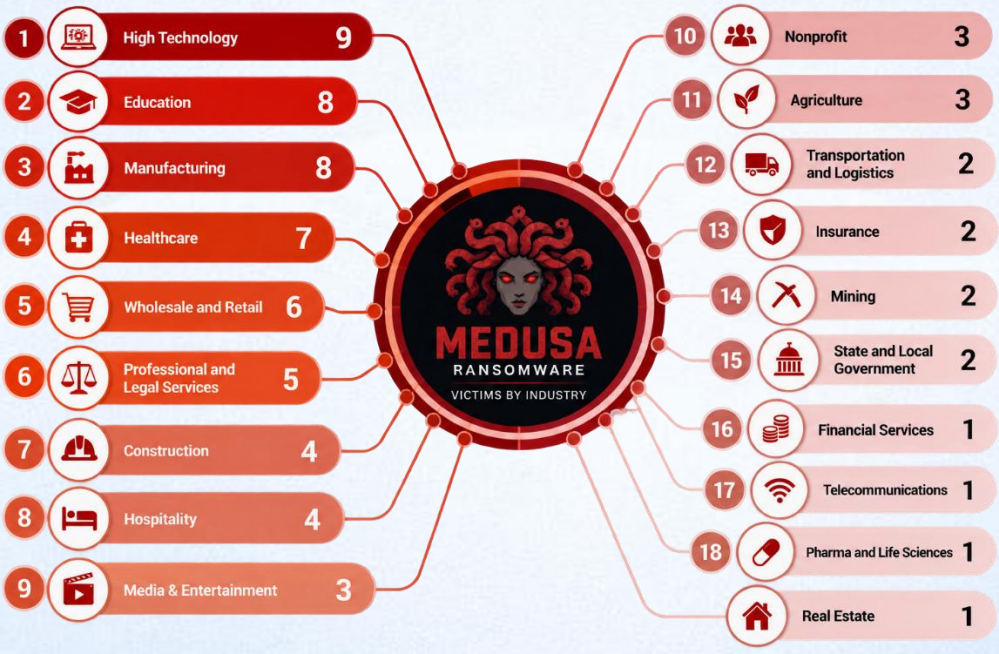


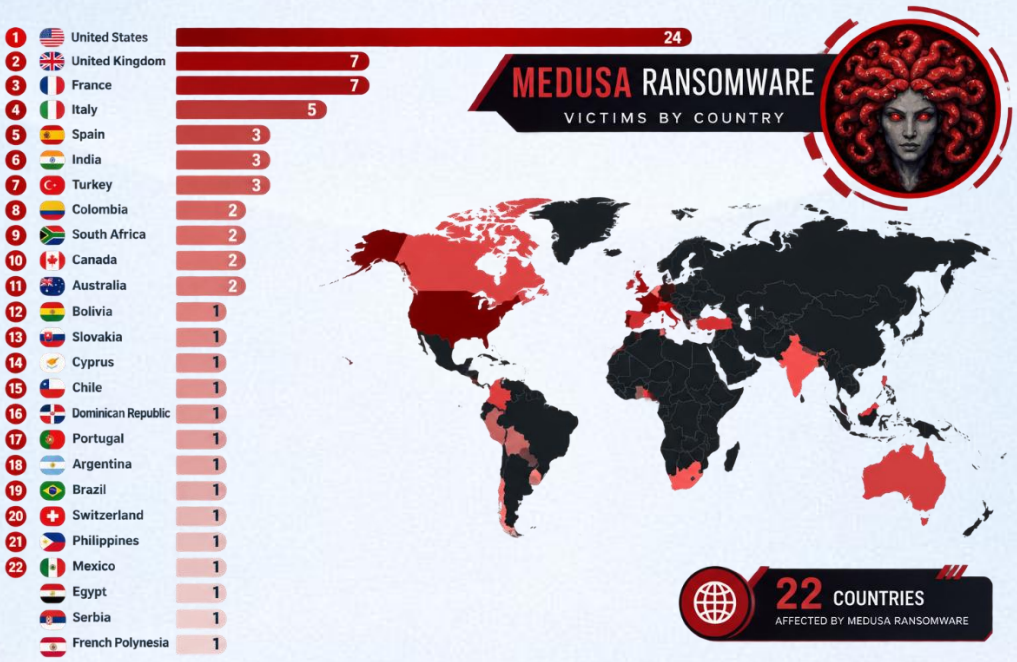
Figure: *Information support admin Telegram message announcing Medusa blog site.*

Understanding Victimology

Based on its leak site, the Medusa ransomware group reportedly impacted approximately **74 organizations** worldwide in 2023. High technology, education, and manufacturing were among the most affected sectors. However, the broad distribution of victims across multiple industries demonstrates the group's opportunistic targeting approach, a characteristic commonly observed among ransomware operations. Medusa does not appear to limit its activities to a specific sector, highlighting the wide-ranging impact of its campaigns.



Medusa ransomware has a broad global footprint, with the United States recording the highest number of reported incidents (24), followed by Europe. Although fewer cases were reported in Africa, South America, and Asia, the overall distribution highlights the group's geographically diverse and international targeting.



➢ Saudi Automotive Marketplace Speero Allegedly Leaked

A newly registered threat actor using the alias **UNC2030** is allegedly offering a complete data dump from **speero.net**, a Riyadh-based automotive marketplace for car parts and maintenance services. The claimed dataset reportedly contains **83 tables and approximately 11 GB of CSV data**, with the user table alone comprising **1,000,034 records**. The exposed fields allegedly include **passwords, email verification tokens, password reset codes, and one-time account restoration tokens**. Additional datasets reportedly contain customer addresses, wallet balances and transactions, invoices, payment records, and messaging logs. The actor has also shared a **free sample of the user table** and is offering lookups upon request.

Threat Actor : UNC2030

Target : speero.net

Country : Saudi Arabia

Volume : 11GB, 83 CSV tables

Potential impact

The token fields are the most concerning, as email verification, password reset, and account restoration tokens could enable account takeover without passwords if still valid. Nearly one million customers are reportedly exposed, including names, emails, mobile numbers, and delivery addresses, increasing fraud risks. Wallet balances, transaction history, lifetime spend, and margin data could also enable targeted attacks and financial profiling. However, the small card-table counts suggest mass payment-card exposure is unlikely.

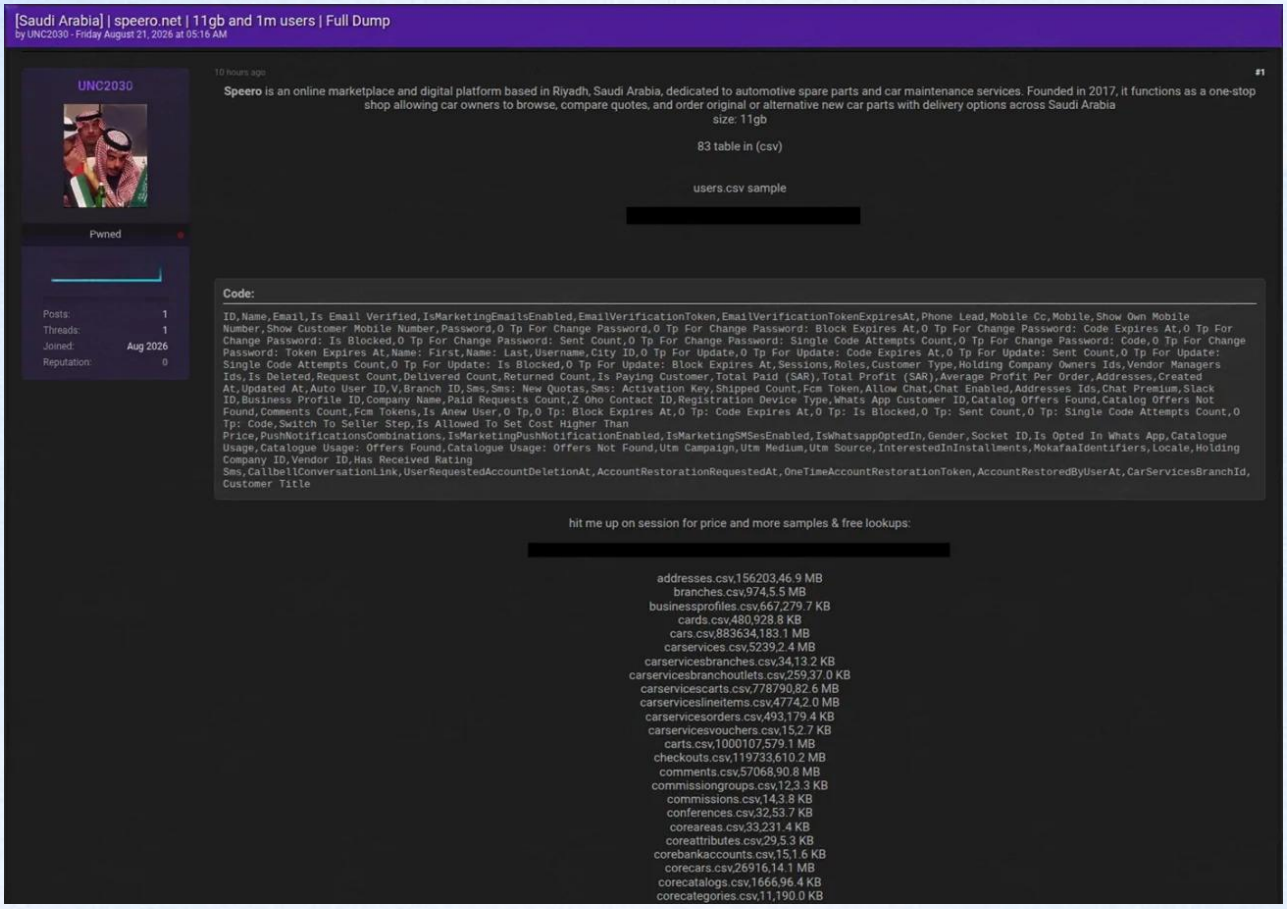


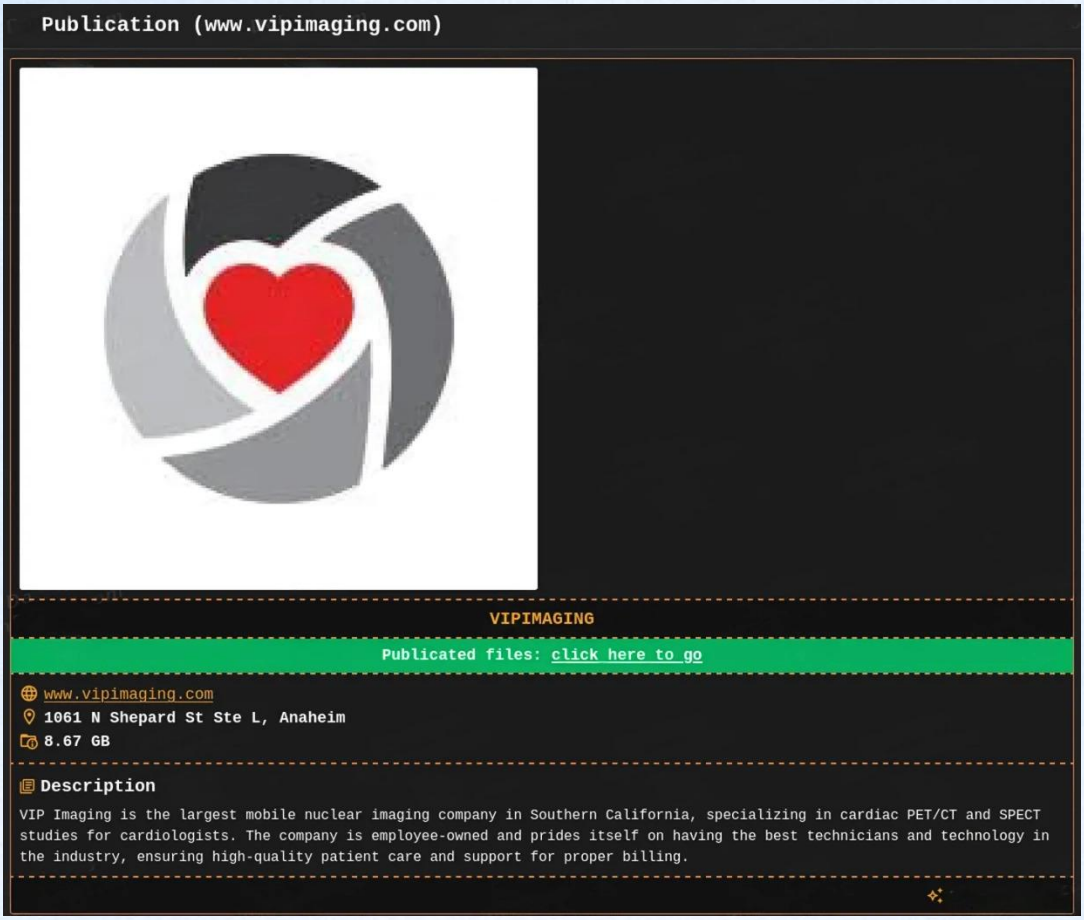
Figure: *Darkweb forum post showing data is on sale*

➢ DragonForce Ransomware Leaks Alleged VIP Imaging Data

The DragonForce ransomware group publicly claimed responsibility for a cyberattack against **VIP Imaging**, a major **mobile nuclear imaging company based in Southern California, USA**. The group reportedly threatened to leak sensitive data unless negotiations were initiated, where the actor has published roughly **8.67 GB of data allegedly stolen** from the company. Authenticity and scope are unverified.

According to the report, VIP Imaging specializes in cardiac PET/CT and SPECT imaging services for cardiologists. The incident highlights the continued targeting of healthcare organizations by ransomware groups, where the potential exposure of sensitive organizational and patient-related information can significantly increase operational and regulatory risks.

Appearance on an active leak site indicates the actor has published data it claims to have exfiltrated, so exposure has likely already occurred rather than being a future threat. As a healthcare provider **handling cardiac imaging (PET/CT and SPECT),** VIP Imaging holds sensitive patient health information, and any authentic exposure would carry risks of medical identity theft, insurance and billing fraud, and serious privacy harm that cannot be undone by changing a password. DragonForce operates a double-extortion, affiliate-driven model, and the data is listed as already published.



Assessment

The available information is based on a DragonForce threat actor claim; the source does not provide independent confirmation of the breach or details regarding the volume and specific types of data allegedly exfiltrated. No data, samples, or actor contact channels are reproduced here, and the authenticity, scope, and contents remain unverified. VIP Imaging has not publicly addressed the claim as of this post.

➢ Khilafah Hackers Deface Five Israeli Websites

According to forums and reports, the hacktivist group **Khilafah Hackers** claimed responsibility for defacing **five Israeli .co.il websites**, reportedly in association with an umbrella group referred to as the Cyber Ummah Alliance. The affected domains were **cafefainberg.co.il, sitemaker.co.il, snapstyle.co.il, glamframe.co.il, and bumpart.co.il.** The sites reportedly displayed an identical "**HACKED**" page featuring religious and political messaging.

The operation appears primarily focused on website defacement and ideological messaging, with no evidence presented in the source confirming data theft despite "Data Exposed" claims displayed on the defacement pages. Noted that the uniform design across all five sites could indicate a shared access vector, such as compromised administrative credentials, a common hosting panel, or vulnerabilities in shared CMS components.

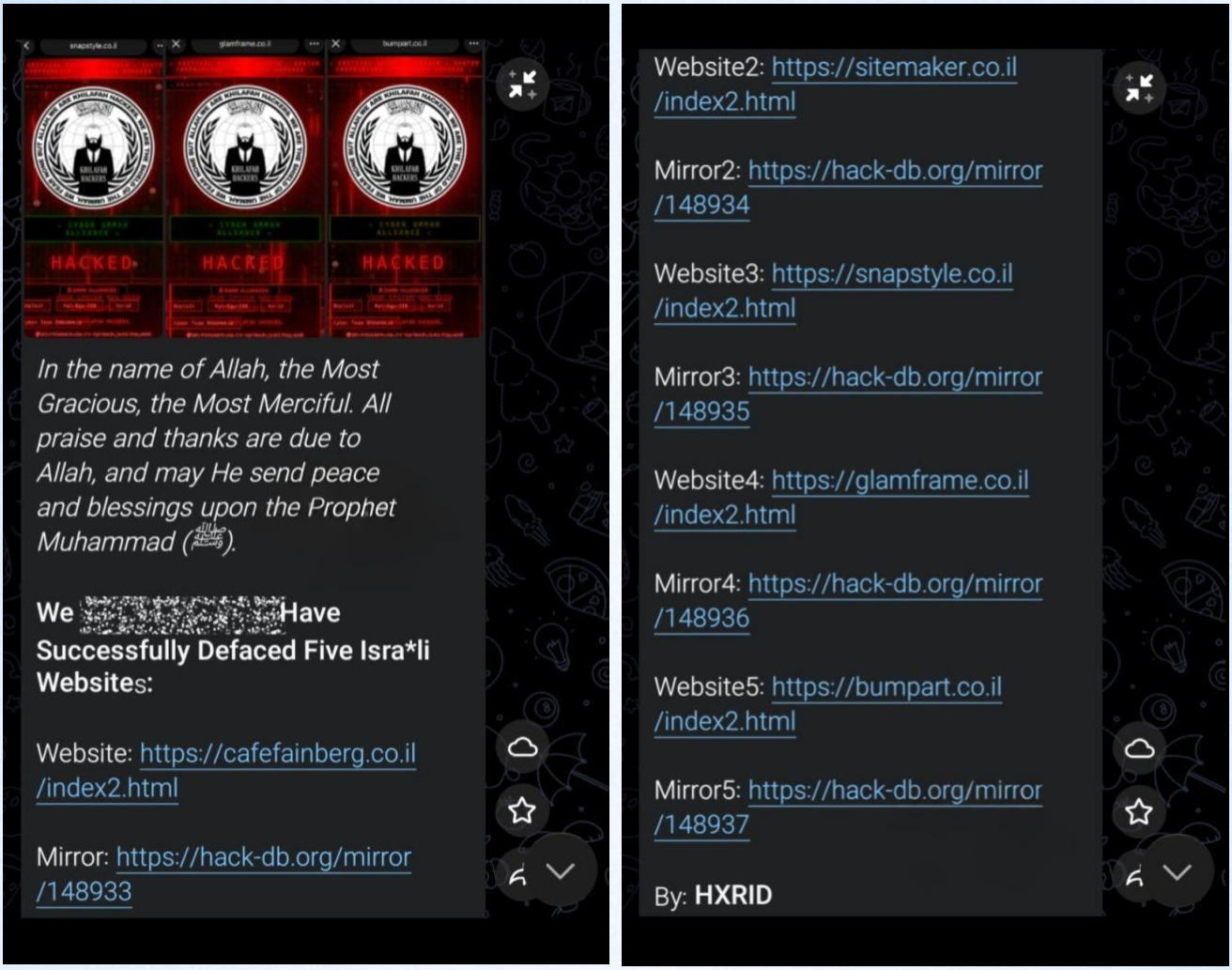


Figure: *Announcement in Khilafah hackers Telegram channel*

➢ Indonesia Tax Data Breach: 100,000 NPWP Records Leaked By K3LLLEAKERS

An alleged Indonesian tax data breach has emerged on cyber underground channels, with the hacktivist group **K3LLLEAKERS** reportedly publishing a database containing **more than 100,000 records attributed to Indonesia's Directorate General of Taxes (Direktorat Jenderal Pajak / pajak.go.id)**. The dataset allegedly includes highly sensitive personal and financial information, such as NPWP tax identification numbers, full names, residential addresses, phone numbers, email addresses, occupations, and tax compliance status covering individuals across Indonesia.

Compromised Data Records

- **Tax Identification Numbers (NPWP):** Unique 15-16-digit national taxpayer identification numbers used for banking, corporate, and civil transactions in Indonesia.
- **Full Legal Names (NAMA_WAJIB_PAJAK):** Complete names of individual taxpayers, business owners, and corporate representatives.
- **Direct Contact Information (EMAIL & TELEPON):** Personal email addresses and mobile phone numbers associated with taxpayer records.
- **Residential Addresses (ALAMAT):** Detailed home addresses, including street numbers, RT/RW codes, sub-districts, and postal zones.

- **Geographic Information (KOTA & PROVINSI):** Records reportedly covering multiple regions, including DKI Jakarta, Gowa, Waingapu, Timika, Balikpapan, Sukabumi, Bengkulu, Papua Pegunungan, and Riau.
- **Demographic & Classification Data:** Gender, taxpayer type (Badan / Orang Pribadi), and taxpayer activity status (Aktif / Tidak Aktif).
- **Professional Occupation (PEKERJAAN):** Occupations such as teachers, technicians, business owners, traders, consultants, private-sector employees, and programmers.
- **Tax Filing Status (STATUS_PAJAK):** Indicators showing whether taxpayers are registered, have filed their returns, or have not yet filed.



Figure: *Hackers post on their official Telegram channel*



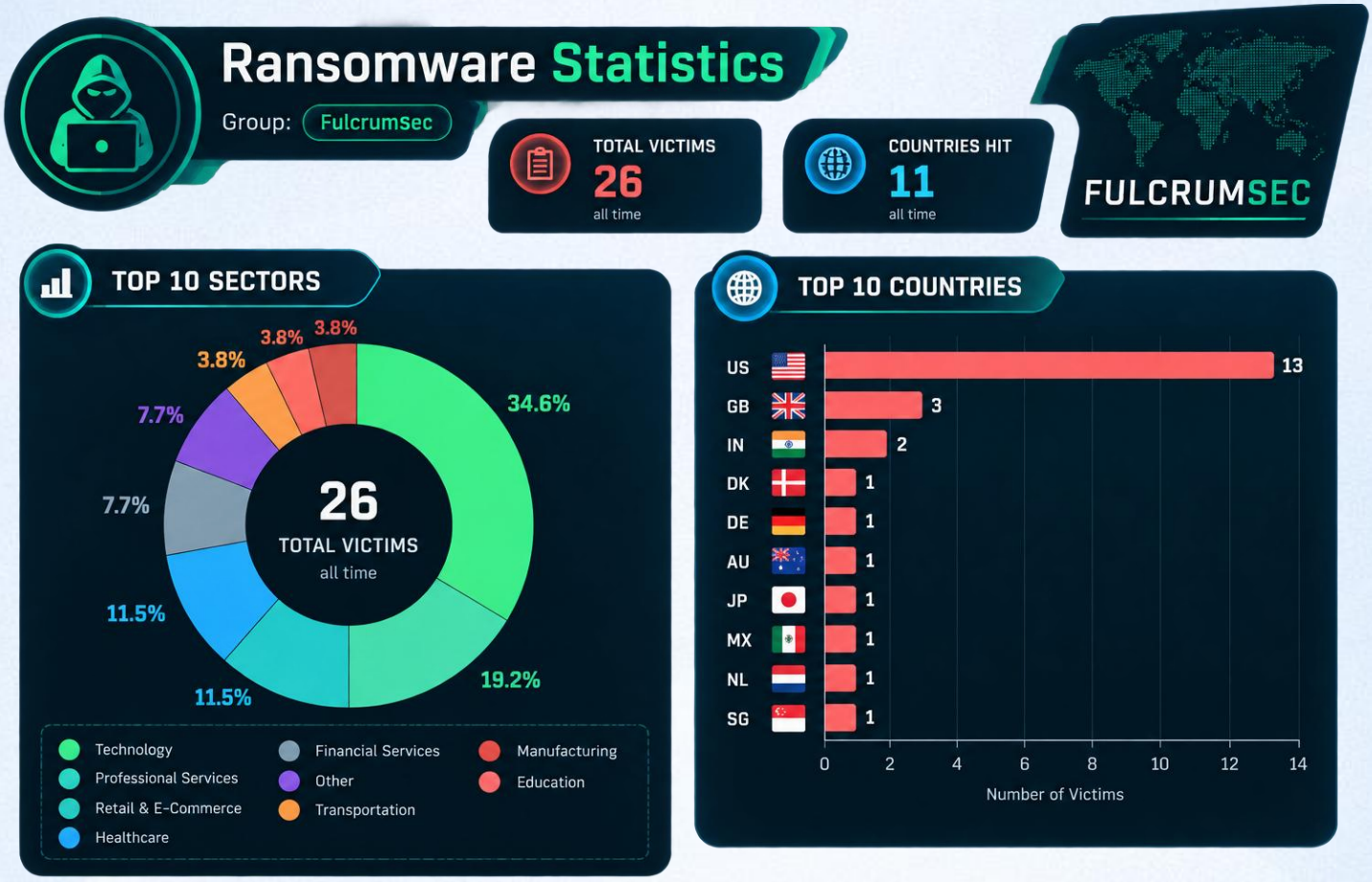
Figure: *Forensic review of a 100,002-line CSV database detailing national demographics and taxpayer records.*

➢ Manchester Airports Group Cyberattack Exposes Data of 8.7 Million Customers

Manchester Airports Group (MAG), which operates Manchester, London Stansted, and East Midlands airports, disclosed a cyberattack in **August 2026** that resulted in the exposure of customer information associated with **airport Wi-Fi registrations and parking, lounge, and Fast Track bookings**. Approximately **8.7 million customers** were affected. The exposed information included **names, email addresses, telephone numbers, postcodes, vehicle registration numbers, residential IP addresses, browser information, and booking-related data**. MAG stated that banking and payment information was not compromised, and airport operations, passenger safety, and aviation security were not affected.

Threat Actor: FulcrumSec

FulcrumSec is a data extortion group active since approximately September 2025, **specializing in high-speed exfiltration of cloud-hosted databases by exploiting unrotated API keys and misconfigured cloud permissions** rather than deploying encryption, with known victims including Australian fintech youX and LexisNexis.



The incident subsequently escalated into an extortion and data-leak operation. The FulcrumSec extortion group claimed responsibility and **published approximately 550 GB of allegedly stolen data after MAG reportedly refused to pay a ransom**. Reported that the leaked dataset contained **approximately 8.8 million email addresses and phone numbers, along with names, browser-agent information, purchases, and vehicle registration records**. The group also claimed to have obtained MAG platform configuration data; however, noted that this claim had not been independently verified.

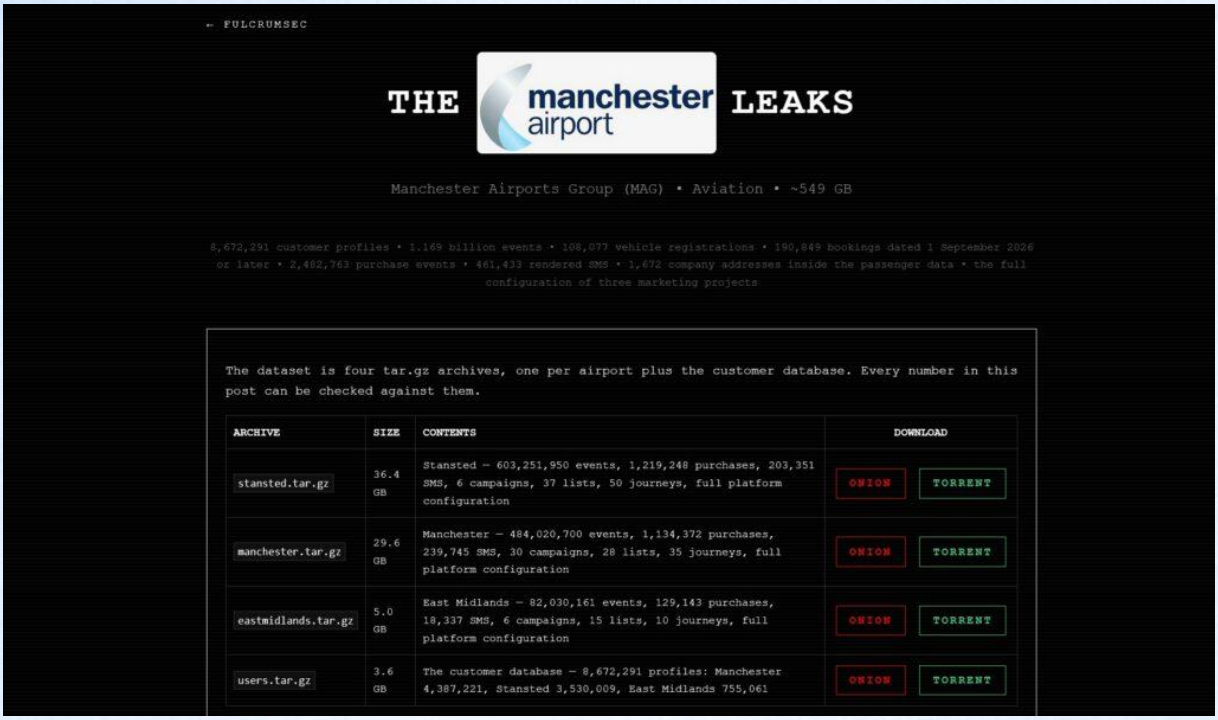
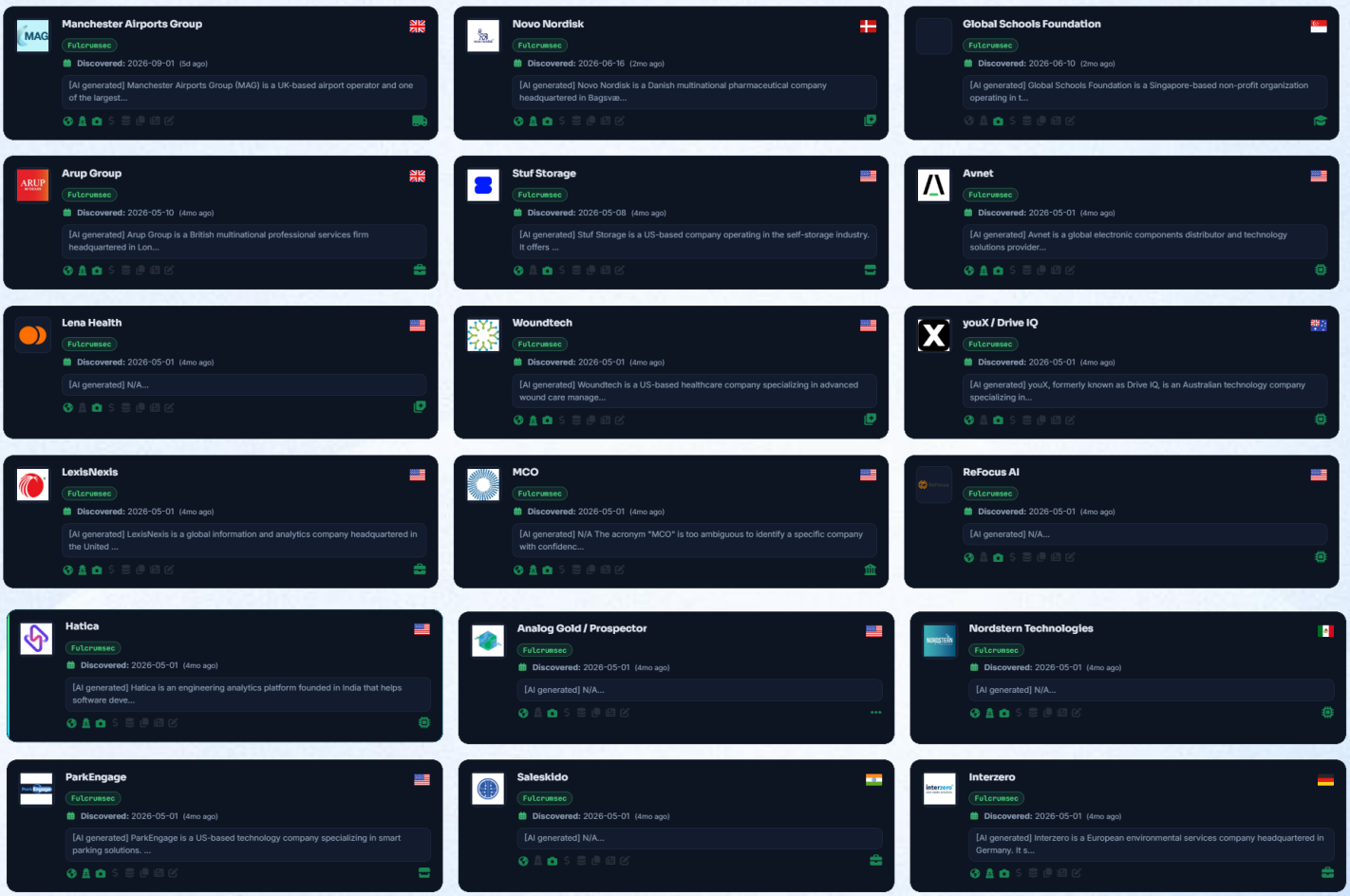


Figure: *Manchester Airport Data exposed via darkweb forum, after the victim refused to pay the ransom*

Major Victims



Major Vulnerability & Exploit Intel

Open Source & Enterprise Applications

Zoom Patches Zero-Click Code Execution Vulnerability

The Zoom patched a zero-click remote code execution (RCE) vulnerability, **CVE-2026-53413**, affecting Zoom's annotation functionality. A malicious meeting participant could exploit a memory-corruption issue by sending specially crafted messages, potentially executing attacker-controlled code on another participant's machine without any action or visible indication from the victim.

It also mentions two additional annotation vulnerabilities:

- **CVE-2026-53414** - missing bounds check enabling a buffer to overread and potential denial-of-service (DoS).
- **CVE-2026-53415** - a use-after-free vulnerability in the annotation function.

Reference: https://www.zoom.com/en/trust/security-bulletin/zsb-26015/

Critical macOS Screen Sharing Authentication Bypass - Under Active Exploitation

CVE-2026-65400 is a pre-authentication vulnerability in the macOS Screen Sharing daemon (screensharingd) that lets a network attacker authenticate without valid credentials and gain root-level remote code execution. Apple patched the flaw on August 6, 2026, in macOS Tahoe 26.6.1, Sequoia 15.7.9, and Sonoma 14.8.9, but after reports of active exploitation, CISA rescored it from 7.1 to 9.8 (Critical) on August 14 and added it to the Known Exploited Vulnerabilities (KEV) catalog on August 18, giving federal agencies until August 21, 2026 to remediate.

Reference: https://www.cve.org/CVERecord?id=CVE-2026-65400

Critical Vulnerabilities Patched with Chrome 151 Update

Google released a Chrome 151 security update addressing **41 critical- and high-severity vulnerabilities**. More than two dozen of the flaws are memory-safety issues that could potentially result in data corruption, crashes, or arbitrary code execution. Among them 6 critical-severity vulnerabilities were fixed. The patched Chrome versions are as follows,

- Windows: 151.0.7922.108 / 151.0.7922.109
- macOS: 151.0.7922.108 / 151.0.7922.109
- Linux: 151.0.7922.108

Reference: https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html

12-Year-Old PostgreSQL Vulnerability Enables Database, Server Takeover

A 12-year-old vulnerability in PostgreSQL, tracked as **CVE-2026-6471** and dubbed PostGREShell which has **CVSS 7.2**, can allow attackers with Replication privileges to achieve remote code execution, escalate to PostgreSQL superuser privileges, and establish a persistent backdoor. The vulnerability stems from missing authorization in PostgreSQL's logical decoding functionality.

Reference: https://www.postgresql.org/support/security/CVE-2026-6471/

Server-Side Request Forgery (SSRF) in GitLab AI Gateway

GitLab has addressed a vulnerability in its AI Gateway component affecting **versions 18.10 through 19.0.12, 19.1 through 19.1.7, and 19.2 through 19.2.2.** The flaw could have enabled an authenticated user with Duo Agent Platform access to redirect outbound AI model requests to an attacker-controlled endpoint by using a specially crafted inline flow configuration to manipulate the HTTP Host header. Successful exploitation could expose Google Cloud Vertex service credentials and private signing keys.

Reference: https://www.cve.org/CVERecord?id=CVE-2026-75871

Latest Metabase vulnerability: CVE-2026-72898

Metabase disclosed that certain versions of Metabase On-Premises are affected by a SQL injection vulnerability exploitable via a password reset API endpoint. Successful exploitation allows a remote, unauthenticated attacker with HTTP(S) access to inject arbitrary SQL into the Metabase application database, which can give them administrator access to the instance. The vulnerability has been designated **CVE-2026-72898** and has been rated critical with a **CVSS score of 10.0**.

Reference: https://www.metabase.com/blog/security-update-6-aug-2026

Enterprise Network & Infrastructure

Fortinet Patches Authentication Flaws in FortiWeb and FortiManager

Fortinet has released patches for multiple vulnerabilities across its product portfolio, including two significant authentication flaws affecting FortiWeb and FortiManager. The vulnerabilities could enable unauthorized access to security infrastructure or allow attackers to impersonate trusted Fortinet devices.

CVE-2026-26035 - FortiWeb Improper Authentication: Improper authentication flaw that can be remotely exploited without authentication when a specific, non-default administrator configuration is enabled. The issue is associated with the wildcard option for administrator accounts, which is disabled by default.

Fortinet addressed the vulnerability in **FortiWeb 8.0.3, 7.6.7, 7.4.12, and 7.2.13.** As a temporary mitigation, Fortinet recommends disabling the wildcard administrator setting.

CVE-2026-70468 - FortiManager Authentication Bypass: The FortiManager vulnerability is an authentication bypass that could allow a remote attacker to impersonate any FortiGate appliance managed by FortiManager. Exploitation requires a particular CLI option to be enabled and the attacker to possess a valid certificate.

Reference: https://fortiguard.fortinet.com/psirt/FG-IR-26-158

ServiceNow Has Addressed Three Critical Vulnerabilities

ServiceNow has addressed three critical vulnerabilities in its AI Platform, **CVE-2026-18885, CVE-2026-18886**, and **CVE-2026-74820**, all rated CVSS 10.0. The flaws involve code injection, access control,and SQL injection and can allow unauthenticated attackers to execute code, escalate privileges, or access and modify instance data.

Reference: https://www.bleepingcomputer.com/news/security/servicenow-warns-of-three-max-severity-security-vulnerabilities/

MITRE ATT&CK Mapping

ATT&CK Tactic	Techniques Observed	Observed in August 2026
Initial Access	T1566 Phishing, T1190 Exploit Public-Facing Application, T1133 External Remote Services, T1078 Valid Accounts	Gunra Fortinet exploitation, Medusa phishing and vulnerability exploitation, Lazarus spear-phishing, TheHatman compromised credentials, DriveSurge ClickFix/FakeUpdates delivery
Execution	T1059 Command and Scripting Interpreter, T1204 User Execution, T1203 Exploitation for Client Execution	ClickFix PowerShell/Terminal execution, malicious PDF execution, scripting activity following infrastructure compromise
Persistence	T1053 Scheduled Task/Job, T1505 Server Software Component, T1098 Account Manipulation	Ransomware persistence mechanisms, compromised cloud accounts, malicious server-side components and continued access following infrastructure compromise
Privilege Escalation	T1068 Exploitation for Privilege Escalation, T1548 Abuse Elevation Control Mechanism	Lazarus exploitation of Windows privilege-escalation vulnerability, exploitation of compromised infrastructure for elevated access
Defense Evasion	T1027 Obfuscated/Compressed Files, T1070 Indicator Removal, T1218 System Binary Proxy Execution	Obfuscated JavaScript used by DriveSurge, anti-analysis techniques, legitimate remote-access tools abused by Medusa, deletion of backups by Gunra
Credential Access	T1555 Credentials from Password Stores, T1110 Brute Force, T1556 Modify Authentication Process, T1539 Steal Web Session Cookie	Browser credential theft, stolen session cookies in Gunra activity, MFA bypass through authentication-process modification, compromised cloud credentials
Discovery	T1087 Account Discovery, T1018 Remote System Discovery, T1046 Network Service Discovery, T1526 Cloud Service Dashboard	TheHatman Azure/Entra directory enumeration, cloud asset discovery, network reconnaissance following VPN and infrastructure compromise
Lateral Movement	T1021 Remote Services, T1570 Lateral Tool Transfer, T1550 Use Alternate Authentication Material	Gunra lateral movement using stolen sessions and Impacket, remote administration tools abused by ransomware operators, internal movement after VPN compromise
Collection / Exfiltration	T1005 Data from Local System, T1530 Data from Cloud Storage, T1567 Exfiltration Over Web Service, T1041 Exfiltration Over C2 Channel	Azure/Entra directory harvesting, OneDrive / SharePoint / MEGA data theft, large-scale cloud and SaaS data exfiltration, ExfilSquad data theft

Impact	**T1486 Data Encrypted for Impact, T1490 Inhibit System Recovery, T1499 Endpoint Denial of Service, T1531 Account Access Removal**	Gunra and Medusa ransomware encryption, shadow-copy deletion, DDoS/disruptive activity, data extortion and public leak operations

Recommendations

Cloud & Identity Security

- Enforce phishing-resistant MFA using FIDO2/passkeys for privileged, remote-access, and cloud identities, particularly for Microsoft Entra ID, VPN, administrative, and service accounts.
- Restrict cloud directory and API permissions using least privilege, Privileged Identity Management, conditional access, and regular entitlement reviews.
- Monitor OAuth applications, refresh tokens, session cookies, and third-party integrations for unauthorized persistence and token abuse.
- Protect service accounts and cloud workload identities by eliminating unnecessary privileges, enforcing short-lived credentials, and preventing interactive logins where not required.
- Delete cloud resources if not in use.

Infrastructure & Vulnerability Management

- Prioritize remediation of internet-facing vulnerabilities, particularly Fortinet FortiOS/FortiProxy, FortiWeb /FortiManager, macOS Screen Sharing, PostgreSQL, GitLab AI Gateway, Metabase, and other externally accessible enterprise applications.
- Treat actively exploited and KEV-listed vulnerabilities as emergency remediation items, with remediation timelines measured in hours or days rather than normal patch cycles.
- Maintain a continuously updated inventory of internet-facing assets, including VPN gateways, firewalls, cloud portals, SaaS applications, databases, APIs, and remote-management infrastructure.
- Monitor for exploitation of public-facing applications through WAF, firewall, IDS/IPS, EDR, and application logs, with particular attention to authentication bypass and RCE attempts.
- Disable unnecessary services and insecure protocols, including exposed management interfaces and legacy network-management mechanisms.
- Remove resources if not in use.
- Implement network segmentation between internet-facing infrastructure, identity services, production systems, databases, and backup environments.
- Continuously assess AI infrastructure and APIs for unauthorized access, excessive permissions, exposed credentials, SSRF, and cloud-resource abuse.
- Accelerate vulnerability remediation based on exploitability, prioritizing vulnerabilities with active exploitation, public PoCs, exposed attack surfaces, or ransomware-associated exploitation.

Email & Endpoint Protection

- Strengthen email security controls against spear-phishing, fake recruitment campaigns, malicious PDFs, credential harvesting, vishing, and AI-generated social-engineering content.
- Deploy and tune EDR detections for PowerShell, Python, Terminal, DLL sideloading, suspicious PDF-reader execution, credential theft, reverse SSH tunnels, and ransomware behavior.
- Detect ClickFix-style attacks by monitoring suspicious PowerShell/Terminal execution originating from browsers, fake CAPTCHA pages, browser error pages, and clipboard-based command execution.
- Block or restrict unauthorized remote-management tools such as AnyDesk, Atera, ConnectWise, eHorus, N-able, SimpleHelp, and Splashtop unless explicitly approved and monitored.
- Conduct recurring phishing simulations and awareness training covering fake job offers, device-code phishing, vishing, ClickFix, malicious documents, and AI-generated lures.

Appendix

Threat Actors Observed

Threat Actor	Motivation	Primary Activity
Gunra Ransomware Group	Financial	Fortinet exploitation, credential theft, MFA bypass, data exfiltration and ransomware
Medusa Ransomware	Financial	Phishing, vulnerability exploitation, data theft, ransomware and double extortion
TheHatman	Financial	Azure/Entra compromise, directory enumeration and large-scale data theft
ExfilSquad	Financial	Cloud/SaaS compromise, data theft, extortion and torrent-based data distribution
Lazarus Group	Nation State (North Korea)	Spear phishing, fake job campaigns, DLL sideloading, zero-day exploitation and espionage
DriveSurge	Financial / Cybercrime	Compromised websites, TDS-based malware delivery, ClickFix and FakeUpdates
Famous Chollima	Nation State / Espionage	AI-generated personas and AI-assisted offensive operations
Altered Spider	Cybercrime	Software supply-chain compromise and large-scale dependency compromise
VAULT PANDA	Cybercrime	Rapid exploitation of newly disclosed vulnerabilities
GENESIS PANDA	Cybercrime	Rapid vulnerability exploitation and AI-assisted attack activity

Malware Families Observed

Malware	Category
Gunra Ransomware	Ransomware
Medusa Ransomware	Ransomware
BusySnake Stealer	Information Stealer
MISTPEN	Backdoor / Remote Access Malware
ForestTiger	Backdoor / Malware
Troy	Backdoor / Remote Access Malware
FudModule	Rootkit
FakeUpdates	Malware Delivery / Loader
Orova	Ransomware / Malware
TheGentlemen	Ransomware
Clop	Ransomware / Data Extortion
Incransom	Ransomware

Acronyms

Acronym	Meaning
ADFS	Active Directory Federation Services
AITM	Adversary-in-the-Middle
API	Application Programming Interface
AMSI	Antimalware Scan Interface
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Commonwealth of Independent States
CKYC	Central Know Your Customer
CMS	Content Management System
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DLS	Data Leak Site
DLL	Dynamic Link Library

DoS	Denial of Service
EoP	Elevation of Privilege
FIDO	Fast Identity Online
IAB	Initial Access Broker
KEV	Known Exploited Vulnerabilities
KVM	Kernel-based Virtual Machine
MSSP	Managed Security Service Provider
OIDC	OpenID Connect
OAuth	Open Authorization Framework
OS	Operating System
PAN-OS	Palo Alto Networks Operating System
PDF	Portable Document Format
PoC	Proof of Concept
PPI	Pay-Per-Install
PyPI	Python Package Index
RaaS	Ransomware-as-a-Service
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
RMM	Remote Monitoring and Management
SaaS	Software as a Service
SSRF	Server-Side Request Forgery
SSO	Single Sign-On
TDS	Traffic Distribution System
TLS	Transport Layer Security
TOR	The Onion Router
TTP	Tactics, Techniques, and Procedures
WMI	Windows Management Instrumentation
XDR	Extended Detection and Response
XML	Extensible Markup Language