EnCyb

TLP:GREEN

The Intel Bulletin

June 2026

A Monthly Threat Intelligence Overview

Prepared By
EnCyb TI Team

www.encyb.com | threatintelligence@encyb.com
Social: LinkedIn | X | Facebook |
PCI QSA | CERT-IN Empaneled | ISO 27001 & ISO 9001 Certified|
SWIFT - Cyber Security Partner
India| Middle East | USA | UK

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
Cyber Incidents Amid Iran-Israel, US Context 22
Vulnerability & Exploit Intel 25
MITRE ATT&CK Mapping 29
Recommendations 30
Appendix 31
Threat Actors Observed 31
Malware Families Observed 31
Acronyms 32

Note:

- *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.*

Executive Summary

June 2026 witnessed a continued shift in the global cyber threat landscape from disruptive ransomware toward data theft, cyber extortion, identity compromise, and software supply chain attacks. Threat actors increasingly prioritized **stealing sensitive data, cloud credentials, source code, intellectual property, and authentication tokens** while leveraging extortion to monetize intrusions without deploying encryption payloads.

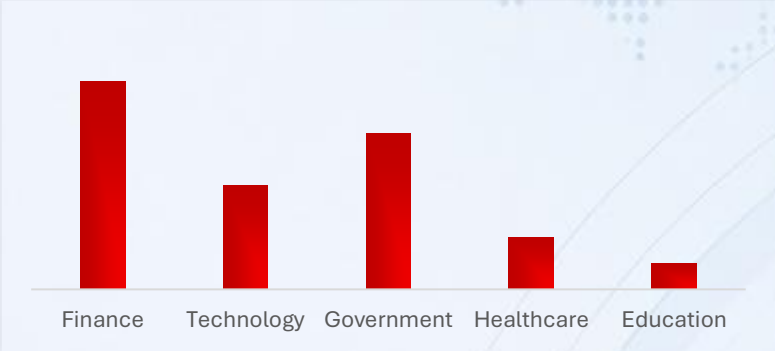
Several financially motivated groups, including World Leaks, **ShinyHunters, FulcrumSec, and TeamPCP, demonstrated increasingly sophisticated attack chains** targeting enterprise identity platforms, cloud services, developer ecosystems, and critical business applications. Supply chain compromises affecting **GitHub, npm, PyPI, CI/CD pipelines**, and enterprise software vendors highlighted the growing risk posed by trusted third-party ecosystems.

Organizations also faced an elevated vulnerability landscape, with multiple actively exploited zero-day vulnerabilities affecting **enterprise VPNs, Windows, Cisco SD-WAN, Linux Kernel, cloud platforms, Microsoft Exchange, Chrome, and widely deployed open-source software**. The increasing speed between vulnerability disclosure and exploitation reinforces the need for rapid patch management and continuous exposure monitoring.

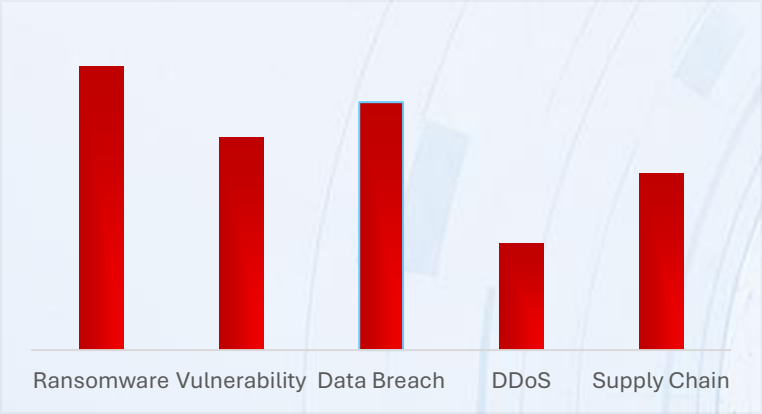
Overall, the June threat landscape demonstrates that modern adversaries are increasingly exploiting trusted identities, cloud infrastructure, and software supply chains rather than relying solely on endpoint malware, requiring organizations to strengthen identity security, secure software development practices, and proactive threat detection capabilities.

Global Threat Overview

Top 5 Target Sectors



Top 5 Risks Breakdown



Top 5 Active Malwares



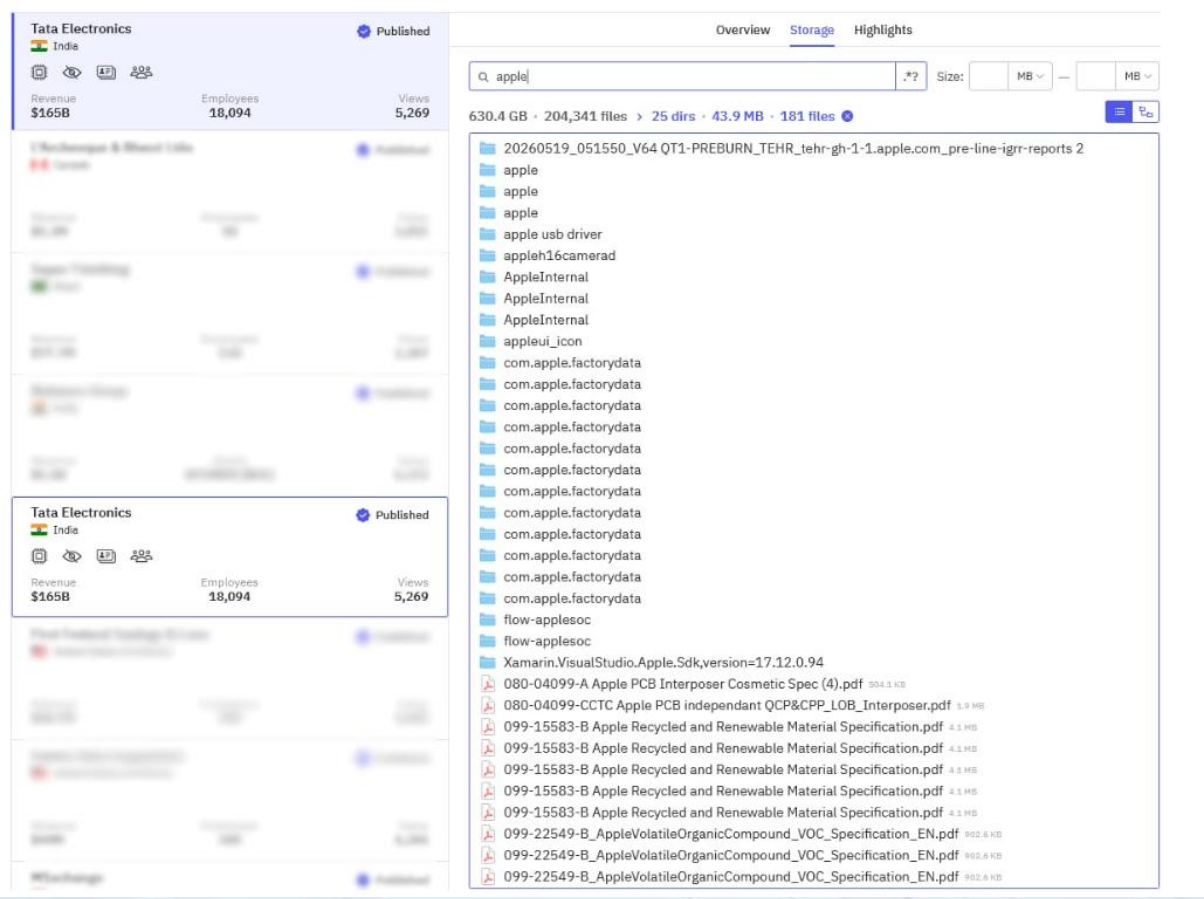
Notable Campaigns & Events

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.

World Leaks Data Extortion Campaign

Security researchers observed the continued expansion of World Leaks, a cybercriminal operation that emerged in early 2025 following the rebranding of the Hunters International ransomware group. Operating as an Extortion-as-a-Service (EaaS) platform, the group focuses on large-scale data theft and extortion rather than traditional file encryption. In **June 2026**, Tata Electronics confirmed a cybersecurity incident after World Leaks claimed responsibility for stealing and publishing more than **200,000 files** (**approximately 630 GB**) containing confidential engineering documents, manufacturing specifications, customer information, emails, and other proprietary data allegedly related to Tata Electronics and its customers, including Apple and Tesla. The incident highlights the growing trend of extortion-only attacks targeting global manufacturing and critical supply chain organizations.

Threat Actor : World Leaks (Formerly Hunters International)
Target Verticals: Manufacturing, Technology, Healthcare, Financial Services, Critical Infrastructure, Government



WorldLeaks extortion and data leak site

Indicators of Compromise

IOC Type	Details
File hash	OVERSTEP Rootkit (World Leaks-linked UNC6148 Campaign): Hash unavailable - Google GTIG provided YARA detection rule
	Malicious library: libsamba-errors.so.6 (specific hash not publicly disclosed)
	World Leaks Exfiltration Tooling: No public file hashes available for Storage Software
IP Addresses	193.149.180.50 (BitLaunch BLNWX VPS used for SSL VPN sessions in UNC6148 campaign linked to World Leaks victim)
Domains/URLs	World Leaks Main Leak Site: worldleaksartrjm3c6vasllvgacbi5u3mgzkluehrzhk2jz4taufuid[.]onion (TOR hidden service)
	World Leaks Negotiation Portal: vw6vklsuotptwdbiwqfvd7y4b57wdbfm6ypxduzzgbt62snti6jm76yd[.]onion (TOR hidden service)
	World Leaks Insider Journalist Platform: 3jguvp6xhyypdjgxhxweu4zklse66v3awjj2zljpftcjyeoimepnwtyd[.]onion (TOR hidden service)
File Paths	/cf/libsamba-errors.so.6 (staging location)
	/usr/lib/libsamba-errors.so.6 (final deployment)
	/etc/ld.so.preload (persistence configuration - abnormally enlarged from normal 2 bytes)
	/cf/firmware/current/INITRD.GZ (modified boot files)
	/tmp/temp.db (exfiltrated credential database)
	/etc/EasyAccess/var/conf/persist.db (exfiltrated credential database)
	/usr/src/EasyAccess/www/htdocs/ (TAR archive placement for attacker download)

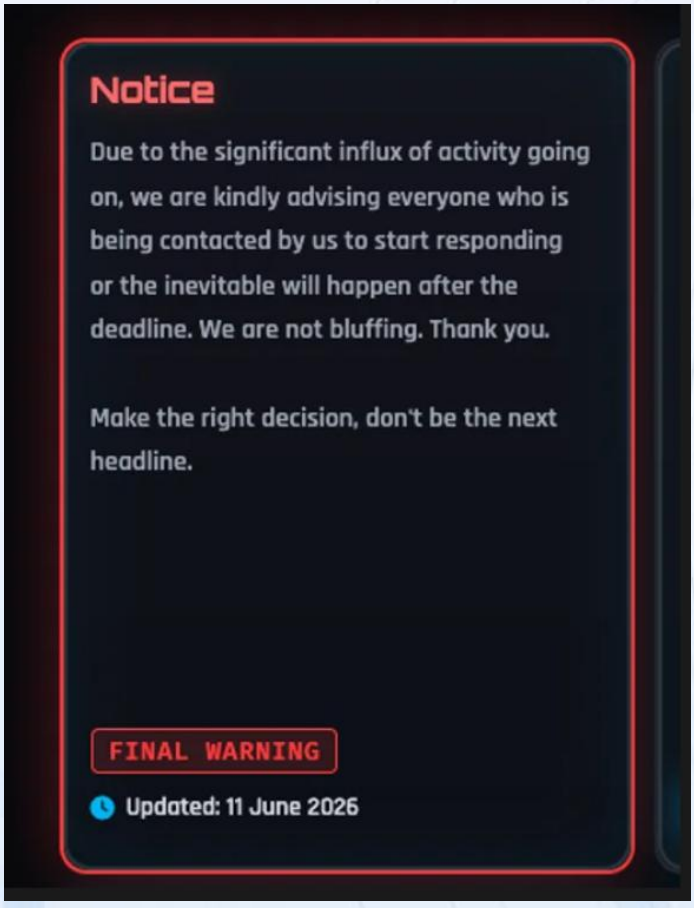
ShinyHunters Oracle PeopleSoft Supply Chain Campaign

Observed a large-scale cyber campaign attributed to the ShinyHunters extortion group targeting organizations through the exploitation of a critical Oracle PeopleSoft zero-day vulnerability. Active between late May and early June 2026, the campaign reportedly compromised more than 100 organizations across approximately 300 PeopleSoft instances, enabling attackers to gain **unauthorized access, steal sensitive data, and conduct extortion operations**. One notable victim, the National Association of Insurance Commissioners (NAIC), confirmed unauthorized access to its Oracle PeopleSoft environment after attackers allegedly exfiltrated **approximately 3.1 TB of data**, including regulatory filings, technical documentation, cloud configuration files, and other internal information. The campaign demonstrates the widespread downstream impact of supply chain compromises affecting enterprise ERP platforms.

Threat Actor : ShinyHunters (UNC6240)
Target Verticals : Government, Insurance, Higher Education, Financial Services, Healthcare, Enterprise Organizations using Oracle PeopleSoft



The actor dumps the leaked NAIC data in Darkweb



Warning on ShinyHunter's DarkWeb blog

Indicators of Compromise

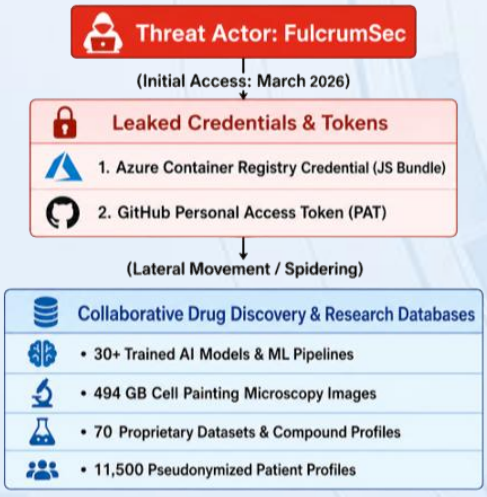
IP Address	Notes
142.11.200[.]186	TLS cert: azurenetfiles[.]net (ShinyHunters-linked)
142.11.200[.]187	TLS cert: azurenetfiles[.]net (ShinyHunters-linked)
142.11.200[.]188	TLS cert: azurenetfiles[.]net (ShinyHunters-linked)
142.11.200[.]189	TLS cert: azurenetfiles[.]net (ShinyHunters-linked)
142.11.200[.]190	TLS cert: azurenetfiles[.]net (ShinyHunters-linked)
108.174.202[.]99	Attack infrastructure
176.120.22[.]24	Attack infrastructure

Novo Nordisk Cyber Extortion Campaign

Reported a cyber extortion campaign targeting **Novo Nordisk**, attributed to the threat actor **FulcrumSec**, which gained initial access through exposed Azure Container Registry (ACR) credentials embedded in a JavaScript bundle and a leaked GitHub Personal Access Token (PAT). The attackers leveraged the compromised credentials to conduct lateral movement across collaborative drug discovery and research environments, **exfiltrating sensitive corporate assets, including more than 30 AI/ML models, 494 GB of cell microscopy images, 70 proprietary datasets and compound profiles**, and approximately **11,500 pseudonymized patient records**. The attackers subsequently demanded a **USD 25 million ransom**, threatening to publicly release the stolen information. The incident highlights the growing risk of credential exposure, supply chain compromise, and cyber extortion targeting organizations within the healthcare and pharmaceutical sectors.

Threat Actor : FulcrumSec
Target Verticals: Healthcare, Pharmaceutical, Biotechnology, Life Sciences, Research Organizations

Attack Technique: The attackers gained initial access using exposed cloud credentials and GitHub Personal Access Tokens (PATs) to access Azure resources. They moved laterally to identify and exfiltrate valuable intellectual property, research data, AI/ML assets, and sensitive information before attempting extortion by threatening to publicly disclose the stolen data instead of deploying ransomware.



Indicators of Compromise

Note: The following IOCs are compiled from verified public researcher tracking of known FulcrumSec infrastructure active during the May/June 2026 campaign window.

Verified malicious IP infrastructure:
- 185.220.101[.]5 (Exfiltration egress point / Tor exit node)
- 93.115.26[.]144 (Command and Control / Repo scraping origin)
- 45.227.254[.]12 (FulcrumSec dark web proxy gateway)

Targeted Cloud/DevOps Telemetry Elements:
- User-Agent String: Mozilla/5.0 (Compatible; GitScraper/2.4; +hx://fulcrumsec[.]info)

Identified Registry Script Hash (SHA-256):
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
(Sample malicious artifact associated with automated container credential testing)

QR Code Phishing (Quishing) Campaign Surge

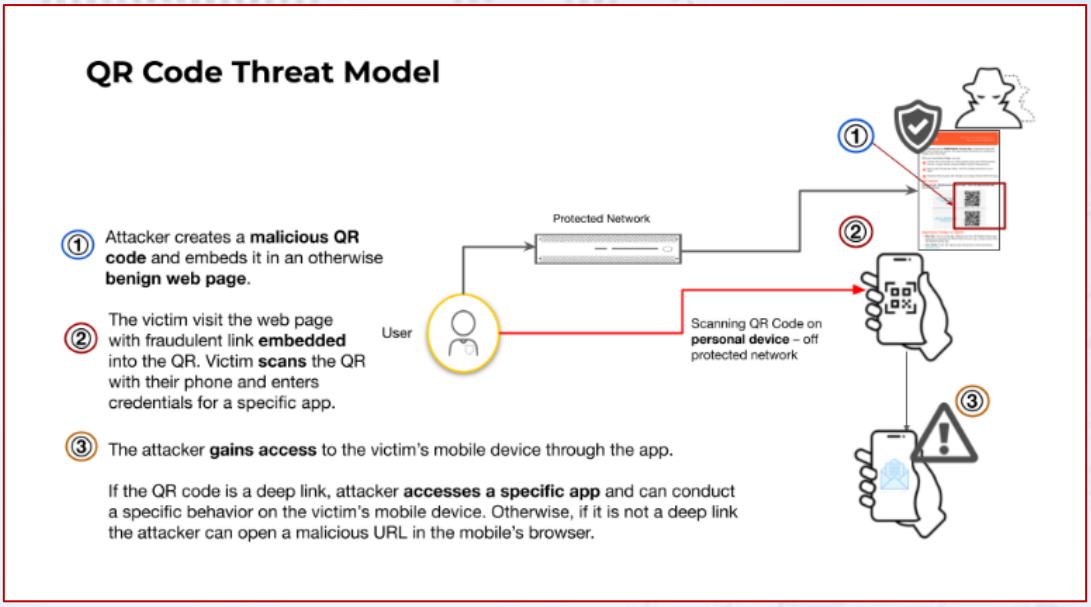
QR code phishing (Quishing) attacks surged in Q1 2026, with Microsoft reporting a 146% increase while blocking approximately **8.3 billion phishing emails**. Attackers increasingly use QR codes in emails, PDFs, invoices, and collaboration platforms to redirect users to credential harvesting pages that bypass traditional email security. Researchers also identified a campaign targeting the hospitality sector, where attackers impersonated Booking.com and used the **ClickFix** technique to trick users into running malicious PowerShell commands, leading to credential theft and malware deployment.

Threat Actor : Multiple Cybercriminal Groups
Target Verticals : Hospitality, Financial Services, Government, Healthcare, Education, Enterprise Organizations

Attack Technique: Threat actors use phishing emails with malicious QR codes to redirect victims to fake login pages for credential theft. They also employ ClickFix social engineering, impersonating trusted brands and tricking users into running malicious PowerShell commands. These techniques enable credential theft, malware installation, and unauthorized access while bypassing traditional email security controls.



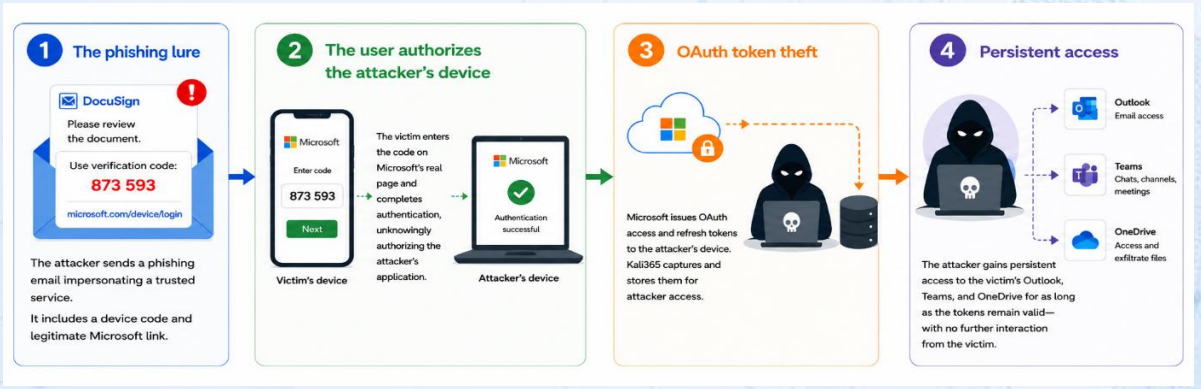
Trends of Quishing attacks by weekly volume



Kali365 Device Code Phishing Campaign

Security researchers identified Kali365, a **Phishing-as-a-Service (PhaaS) toolkit** that abuses the Microsoft OAuth Device Code Authentication flow to compromise **Microsoft 365 accounts without requiring passwords**. Victims are tricked into authenticating through legitimate Microsoft login pages, allowing attackers to obtain access and refresh tokens for persistent account access while bypassing traditional password-based security controls and, in some cases, MFA.

Threat Actor : Multiple Cybercriminal Groups (Kali365 Phishing-as-a-Service Operators)
Target Verticals: Government, Financial Services, Healthcare, Education, Manufacturing, Enterprise Organizations using Microsoft 365.



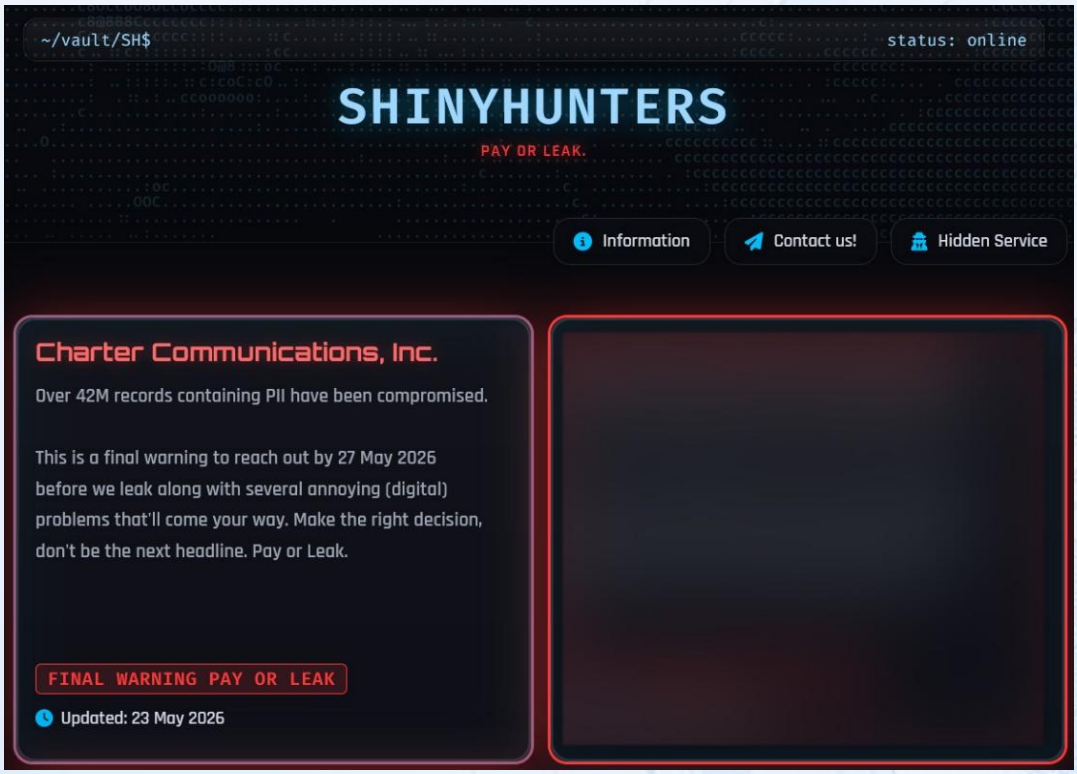
Attack Technique: Kali365 abuses Microsoft's OAuth Device Code Authentication flow by tricking victims into authorizing attacker-generated device codes through the legitimate Microsoft login portal. Attackers then steal OAuth access and refresh tokens, enabling unauthorized access to Microsoft 365 services such as Outlook, SharePoint, OneDrive, and Teams. This token-based technique bypasses password protections, evades traditional phishing detection, and provides persistent access until the tokens are revoked or expire.

Charter Communications confirm data breach

A cyber extortion incident targeting **Charter Communications** was attributed to the threat actor **ShinyHunters**. The attackers reportedly gained initial access through a **voice phishing (vishing)** attack that compromised an employee's **Microsoft Entra account**, enabling unauthorized access to Salesforce. They claimed to have exfiltrated customer data for extortion, while Charter confirmed the incident but stated that no sensitive personal information or CPNI was stolen. The attack highlights the continued effectiveness of social engineering against enterprise identity and SaaS environments.

Breach Overview

Threat Actor : ShinyHunters
Affected Accounts : 4.9 million
Compromised Data : Email addresses, Names, Job titles, Physical addresses, Phone numbers



Charter listing on the ShinyHunters data leak site

Attack Technique: The attackers reportedly gained initial access through a voice phishing (vishing) attack that compromised an employee's Microsoft Entra account. Using the compromised identity, they accessed the organization's Salesforce instance and exported customer data for extortion purposes. The campaign aligns with ShinyHunters' ongoing strategy of targeting enterprise Single Sign-On (SSO) accounts through social engineering to obtain access to SaaS platforms, exfiltrate sensitive business data, and threaten public disclosure unless a ransom is paid.

TeamPCP executes supply chain campaign

TeamPCP (aka UNC6780 (GTIG), PCPcat, Persy_PCP, ShellForce, CipherForce, DeadCatx3) supply chain campaign is a highly coordinated, financially motivated cyber operation that actively weaponizes trusted developer tools to harvest credentials and distribute malware. Initiated in early 2026, the threat actor pivots across five major ecosystems including GitHub, PyPI, and npm to compromise CI/CD pipelines. The actor initially targets widely used, implicitly trusted security tools, allowing them to steal publishing tokens and poison downstream consumers.

Threat Actor Timeline - June



A multi-week, multi-ecosystem attack chain spanning GitHub Actions, Docker Hub, npm, PyPI, OpenVSX, VS Code Marketplace, and Jenkins. Impacted so far: Aqua's Trivy, Checkmarx KICS, LiteLLM, Bitwarden, TanStack, Mistral AI, AntV (323 packages), Microsoft DurableTask, GitHub (~3,800 internal repos), Red Hat Cloud Services (32 packages), +more.

Indicators of Compromise

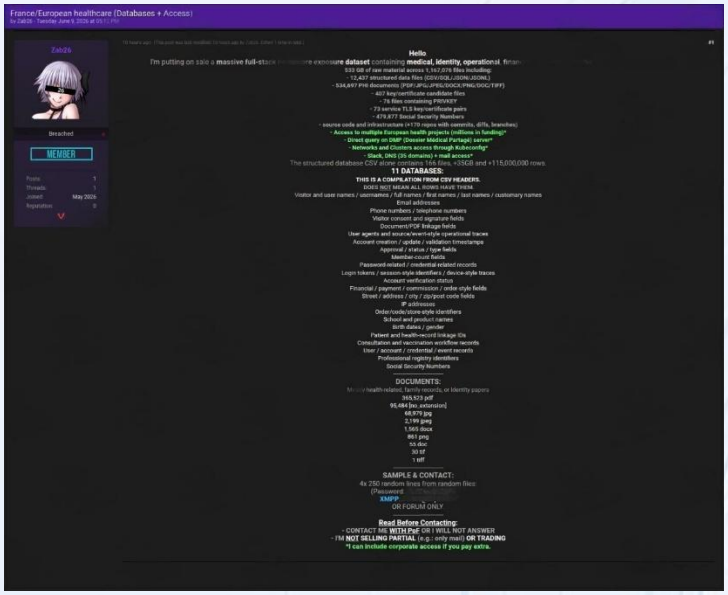
IOC Value	Type	Note
45.148.10[.]212	IP	Havoc C2 TeamServer — TECHOFF SRV, Netherlands
plug-tab-protective-relay[.]trycloudflare[.]com	DOMAIN	exfil
souls-entire-defined-routes[.]trycloudflare[.]com	DOMAIN	kamikaze v1
investigation-launches-hearings-copying[.]trycloudflare[.]com	DOMAIN	kamikaze v2
championships-peoples-point-cassette[.]trycloudflare[.]com	DOMAIN	kamikaze v3/v3.1
create-sensitivity-grad-sequence[.]trycloudflare[.]com	DOMAIN	kamikaze v3.2/v3.3
telemetry.api-monitor[.]com	DOMAIN	secondary webhook exfil
83.142.209[.]11	IP	AdaptixC2 TeamServer — AS205759 Ghosty Networks
46.151.182[.]203	IP	Exfil/backup C2 — AS205759 Ghosty Networks
83.142.209[.]203	IP	Telnyx exfil (port 8080) — AS205759 Ghosty Networks
170.62.100[.]245	IP	Primary operator — Kali Linux, Boto3 S3 enum
209.159.147[.]239	IP	TruffleHog validation — hosts nsa.cat, MinIO
154.47.29[.]12	IP	Org recon — Windows 11, Datacamp VPN Croatia
103.75.11[.]59	IP	Re-check — macOS ARM, Host Universal VPN NZ
nsa[.]cat	DOMAIN	Attacker VPS — nginx, MinIO, open directory
105.245.181[.]120	IP	TruffleHog validation — Vodacom
138.199.15[.]172	IP	GitHub exfil, AWS recon — Mullvad VPN
163.245.223[.]12	IP	GitHub exfil — Interserver
185.77.218[.]4	IP	TruffleHog validation — Crea Nova
193.32.126[.]157	IP	GitHub exfil — Mullvad VPN
23.234.107[.]104	IP	TruffleHog validation — Tzulo
34.205.27[.]48	IP	TruffleHog validation — Amazon AWS
43.228.157[.]123	IP	Open directory malware staging — AS205759 Ghosty Networks SG
43.228.157[.]123/MidwestGrey.exe	URL	Windows PE dropper (Mar 25)
43.228.157[.]123/kfhogts	URL	Python trojan bundle (Mar 13)

43.228.157[.]123/oqqqqoa.mp3	URL	Audio steganography payload
94.154.172[.]43	IP	audit.checkmarx.cx — shared KICS/Bitwarden C2
audit.checkmarx[.]cx	DOMAIN	KICS telemetry exfil endpoint
whereisitat.lucyatemysuperbox[.]space	DOMAIN	xinference exfil (disputed)
zero.masscan[.]cloud	DOMAIN	Mini Shai Hulud primary exfil
Checkmarx[.]cx	DOMAIN	exfil domain (May 9)
91.195.240[.]123	IP	checkmarx.cx resolved IP
updates.checkmarx[.]cx	DOMAIN	update/C2 domain
94.154.172[.]183	IP	updates.checkmarx.cx resolved IP
git-tanstack[.]com	DOMAIN	typosquat C2
83.142.209[.]194	IP	TanStack/Cemu C2 / payload host
83.142.209[.]194/transformers[.]pyz	URL	PyPI mistralai payload download
api.masscan[.]cloud	DOMAIN	C2 (Mistral advisory)
seed1[.]getsession[.]org	DOMAIN	Session network node
seed2[.]getsession[.]org	DOMAIN	Session network node
seed3[.]getsession[.]org	DOMAIN	Session network node
filev2[.]getsession[.]org	DOMAIN	Session network node
check.git-service[.]com	DOMAIN	primary C2
t.m-kosche[.]com	DOMAIN	shared TeamPCP C2
83.142.209[.]194	IP	legacy payload host
t.m-kosche[.]com	DOMAIN	primary exfil C2
185.95.159[.]32	IP	t.m-kosche.com resolved IP
t.m-kosche.com:443/api/public/otel/v1/traces	URL	exfil endpoint (disguised as OpenTelemetry)
api.github.com/search/commits?q=fireda lazer	URL	dead-drop C2 trigger
fulcio.sigstore.dev/api/v2/signingCert	URL	Sigstore abuse for OIDC token forging
rekor.sigstore.dev/api/v1/log/entries	URL	Sigstore abuse
01ff1e56fd59a8fa525d97e670f7f297a1a2 04331b89b2cd4e36a9abc6419203	SHA256	checkmarx-ast-scanner-2026.5.09.hpi (malicious)
f50a96d26a5b0beb29de4127e82b2bf350 c21511e5a43d286e43f798dc6cd53f	SHA256	checkmarx-ast-scanner-2026.5.09.jar (injected)
3ddb8967919a801b3c383e58cddceab211 38134c6a26560d99e2672e86f36f2a	SHA256	checkmarx-ast-scanner-2026.5.09.pom
85487e68fc46fe3faec2617ac4f2ee5d	MD5	checkmarx-ast-scanner.hpi v2026.5.09 (malicious)
1ac56ecda9a255c23eabd70c276905a0	MD5	checkmarx-ast-scanner.jar (injected)
9f9f83795fc162b7e44bc6859fc80535	MD5	cli.js credential stealer
83.142.209.194/v1/weights	URL	C2 exfil endpoint
783b4019fc5b942a29846132d28441c8fc 31bed8	SHA1	~/.local/share/kitty/cat.py
b06b126b9e26af03a7ef2f8b8e90d446	MD5	~/.local/share/kitty/cat.py
169.254.169[.]254	IP	AWS IMDS credential harvest

169.254.170[.]2	IP	ECS container metadata harvest
127.0.0[.]1:8200	URL	Vault token harvest
registry.npmjs.org/-/npm/v1/oidc/token/exchange/package/	URL	npm OIDC token exchange abuse

Zab26 leaks 533GB of French and European Healthcare Data and Access

A threat actor using the alias **Zab26** is advertising for sale what they describe as a **533 GB "full-stack"** healthcare dataset spanning French and European health systems. The listing claims **1.16 million files**, including over 534,000 protected-health-information documents, 479,877 Social Security numbers, more than 115 million database rows, source code, private keys and TLS certificates, and, most alarmingly, claimed live access to health systems, including a query interface to France's DMP (Dossier Medical Partage) shared **medical-record platform, Kubernetes clusters, Slack, and mail**. The claim is unverified.



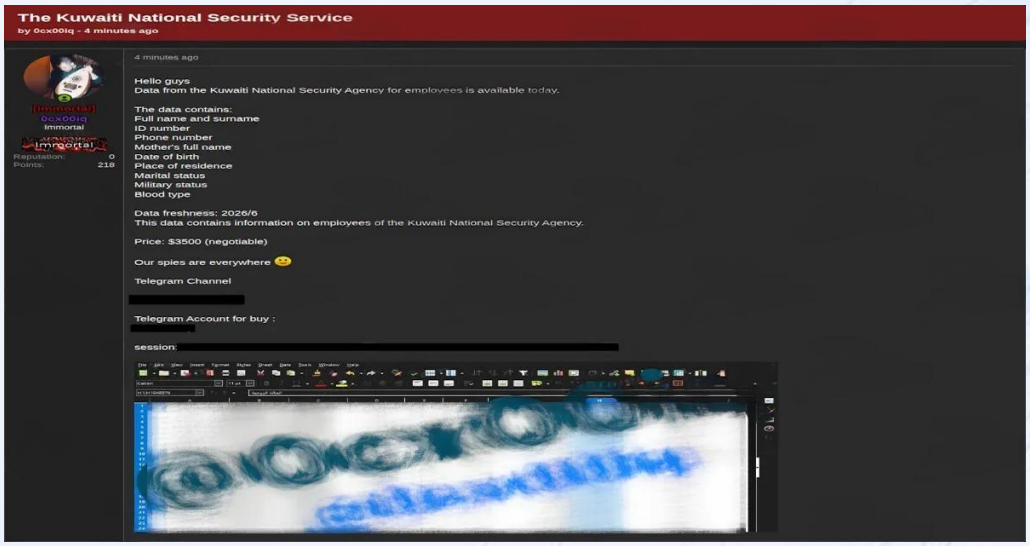
Actor post in darkweb forum

Allegedly Exposed Data:

533 GB / 1.16M files (claimed)
534,697 PHI / medical documents
Patient & health-record identifiers
Private keys & TLS certificates
115M+ database rows
479,877 Social Security numbers
Credentials, tokens & password data
Claimed live system & DMP access

Kuwaiti National Security Agency employee database listed for sale

A threat actor using the alias **0cx00iq** has listed for sale what they describe as a **dataset of employees** of Kuwait's National Security Agency, the country's domestic intelligence service. The actor claims each record contains an **employee's full name, national ID number, phone number, mother's full name, date of birth, place of residence, marital status, military status, and blood type,** with data freshness stated as June 2026. The listing is advertised at around **$3,500** (negotiable), accompanied by a heavily watermarked spreadsheet sample. The dataset's authenticity and scope are unverified.



Actor post in darkweb forum for selling the data

Lazarus Group (DPRK) – Continued Global Cyber Operations

During June 2026, multiple threat intelligence reports highlighted the continued evolution of the Lazarus Group. The North Korean threat actor expanded beyond financial theft into **software supply chain compromises, developer ecosystem abuse, cryptocurrency theft, and enterprise infiltration through phishing, trojanized software, malicious open-source packages, and credential theft**. The group remained highly active against cryptocurrency platforms, software vendors, financial institutions, and defense organizations, reinforcing its status as one of the world's most capable nation-state cyber threats.

Threat Actor: Lazarus Group (Hidden Cobra, Diamond Sleet, Zinc, APT38)

Attack Technique: Lazarus uses spear-phishing, social engineering, supply chain attacks, malicious software packages, credential theft, malware, living-off-the-land techniques, cloud service abuse, and cryptocurrency theft. Recent campaigns increasingly target developer ecosystems, software repositories, and trusted third-party platforms to infiltrate organizations, steal sensitive data, and support DPRK financial objectives.

Indicators of Compromise

IOC Type	Indicator	Confidence	Description / Associated Campaign
C2 IP	95[.]169[.]180[.]140[:]8080	High	Active Command & Control (C2) infrastructure
C2 IP	144[.]172[.]104[.]117[:]5918	High	Contagious Interview C2
C2 IP	147[.]93[.]40[.]224[:]3000	High	BeaverTail / InvisibleFerret C2
C2 IP	23[.]227[.]202[.]52[:]1245	Elevated	Stealer malware C2
C2 IP	23[.]227[.]202[.]51[:]1224	High	Stealer malware C2
C2 IP	185[.]164[.]111[.]104[:]3000	Elevated	Interview campaign infrastructure
C2 IP	72[.]60[.]174[.]178[:]3000	Elevated	Active C2 server
C2 IP	31[.]220[.]48[.]106[:]3000	Elevated	Interview campaign C2
C2 IP	195[.]50[.]242[.]110	Elevated	Shared with Andariel subgroup
C2 IP	86[.]104[.]72[.]247	High	Multi-malware C2 (Tropidoor, LightlessCan)
C2 IP	45[.]8[.]146[.]93	High	Proxy infrastructure
C2 IP	103[.]35[.]190[.]170	High	Proxy infrastructure
Domain	zoom[.]callapp[.]us	Elevated	Zoom impersonation C2
Domain	zoomsdk[.]us	High	Zoom impersonation C2
Domain	zoom-sdk[.]us	High	Zoom impersonation C2
Domain	zoomwebapi[.]com	Moderate	Zoom impersonation C2
Domain	zoommeetspace[.]com	High	Zoom impersonation C2
Domain	zoombackend[.]xyz	High	Zoom impersonation C2
Domain	zoomfiledrop[.]pages[.]dev	High	Zoom phishing domain
Domain	zooommeeting[.]pages[.]dev	Moderate	Zoom phishing domain
Domain	zmwebsdk[.]com	High	Zoom impersonation C2
Domain	tetrismic[.]vercel[.]app	High	Zoom impersonation C2
Domain	answerpart[.]com	High	Recruitment campaign C2
Domain	app[.]compassidea[.]org	High	Recruitment campaign C2
Domain	sloneek[.]us	High	Recruitment campaign C2
Domain	limesurvey[.]us	High	Recruitment campaign C2
Domain	app[.]qwary[.]org	High	Recruitment campaign C2
Domain	carrerlilla[.]com	High	Recruitment campaign C2
Domain	pathsummitx[.]pages[.]dev	High	Recruitment phishing domain
Domain	wtalents[.]us	Elevated	Recruitment campaign C2
Domain	ziprecruiters[.]org	Elevated	Recruitment phishing domain
Domain	superstate-team[.]xyz	High	Recruitment campaign C2
MD5 Hash	b29ddcc9affdd56a520f23a61b670134	High	Tropidoor malware
MD5 Hash	94ef379e332f3a120ab16154a7ee7a00	High	LightlessCan malware

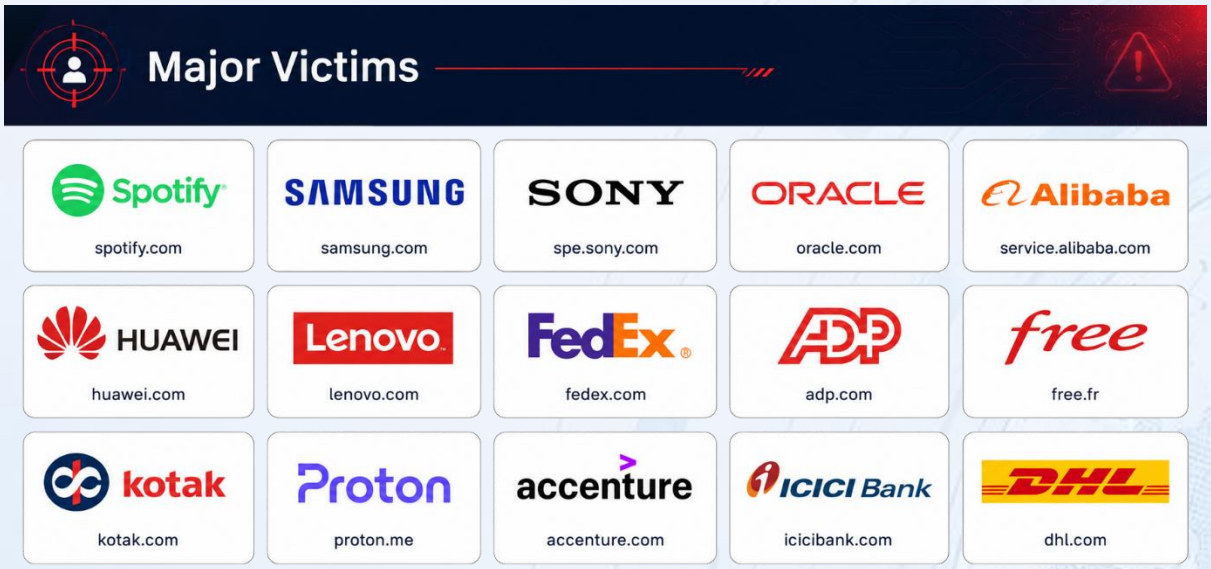
MD5 Hash	84d25292717671610c936bca7f0626f5	High	Multi-malware sample
MD5 Hash	3aed5502118eb9b8c9f8a779d4b09e11	High	InvisibleFerret malware
URL	hxxps[:]//mocki[.]io/v1/32f16c80-602a-4c80-80af-32a9b8220a6b	High	Payload delivery endpoint
URL	hxxp[:]//m21gk[.]wiremockapi[.]cloud/g/api/880	High	Command & Control endpoint
URL	hxxps[:]//86[.]104[.]72[.]247/proxy/Proxy[.]php	High	Proxy infrastructure
URL	hxxps[:]//45[.]8[.]146[.]93/proxy/Proxy[.]php	High	Proxy infrastructure
URL	hxxp[:]//103[.]35[.]190[.]170/Proxy[.]php	High	Proxy infrastructure

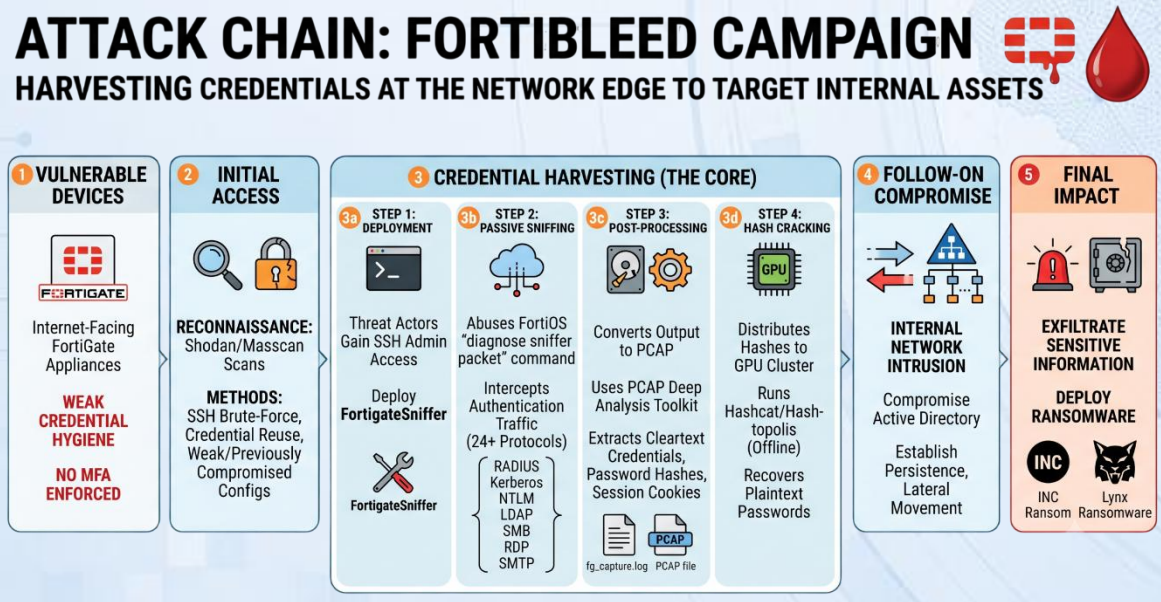


FortiBleed Campaign – Mass Fortinet Credential Harvesting

Uncovered FortiBleed, a large-scale credential harvesting campaign targeting **internet-facing Fortinet FortiGate firewalls and SSL VPNs**. Attackers harvested over **110 million credentials** from **approximately 430,000 devices, with 73,000–75,000 confirmed to have exposed or valid credentials**. Stolen access has been linked to **INC Ransom and Lynx ransomware operations**, enabling unauthorized access, data theft, and ransomware deployment. The campaign primarily exploited previously compromised credentials, credential reuse, brute-force attacks, and weak passwords rather than a new FortiOS vulnerability.

Target Verticals: Government, Critical Infrastructure, Financial Services, Healthcare, Manufacturing, Telecommunications, Energy, Defense, Education, and Enterprise Organizations using Fortinet FortiGate firewalls or SSL VPN gateways.

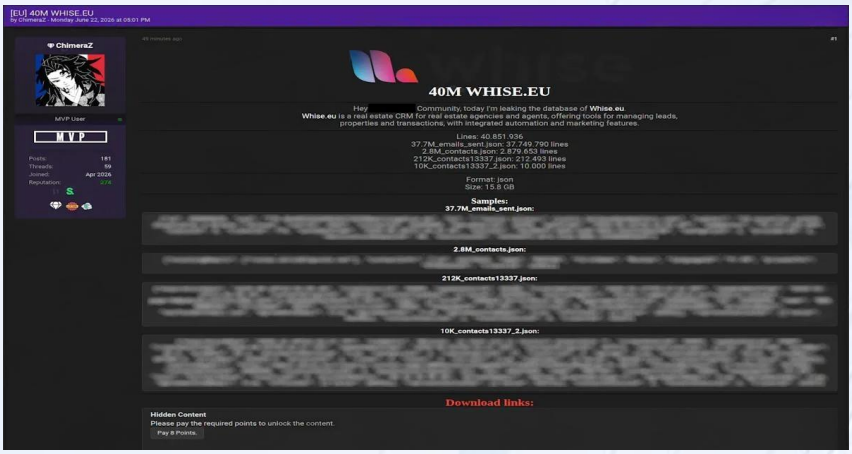




CRM Whise Allegedly Breached, Over 40 million Records Leaked

A threat actor using the alias **ChimeraZ** has posted what they describe as the database of Whise.eu, a European real-estate CRM used by agencies and agents to manage leads, properties, and transactions. The leak is a **~15.8 GB JSON dataset of about 40.85 million** lines, dominated by roughly 37.7 million email-sending logs alongside several million contact records (a 2.8M-contact file plus smaller contact files).

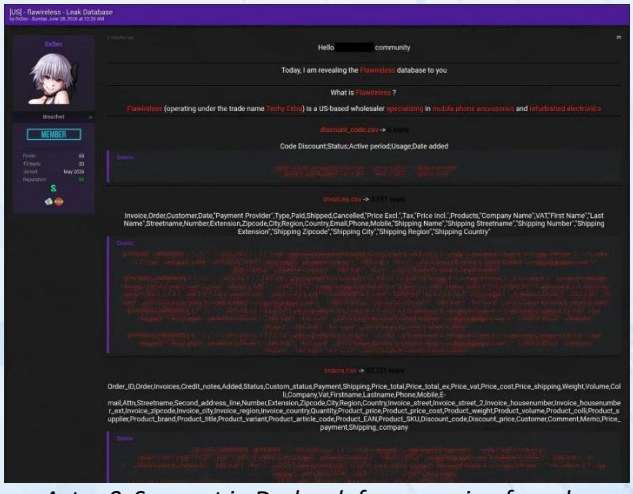
Per the samples, the email logs include recipient names, email addresses, IP addresses, and timestamps, while the contact records include names, email addresses, phone and mobile numbers, marketing-consent flags, and property search criteria. The .be mailing domain and EU focus indicate the data spans individuals across multiple European countries. The dataset's authenticity and scope are unverified.



Actor post in Darkweb forum saying for sale.

US Electronics Wholesaler Flawireless Allegedly Breached by 0xSec

Threat actor **0xSec** claims to have leaked the database of Flawireless (Techy Extra), a US-based mobile accessories and refurbished electronics wholesaler. The dataset reportedly includes over **57,000 order records, invoices, shipments, product catalog data, and customer information** such as names, addresses, email addresses, phone numbers, and payment metadata. No passwords or full payment card details were observed in the shared samples.



Actor 0xSec post in Darkweb forum saying for sale.

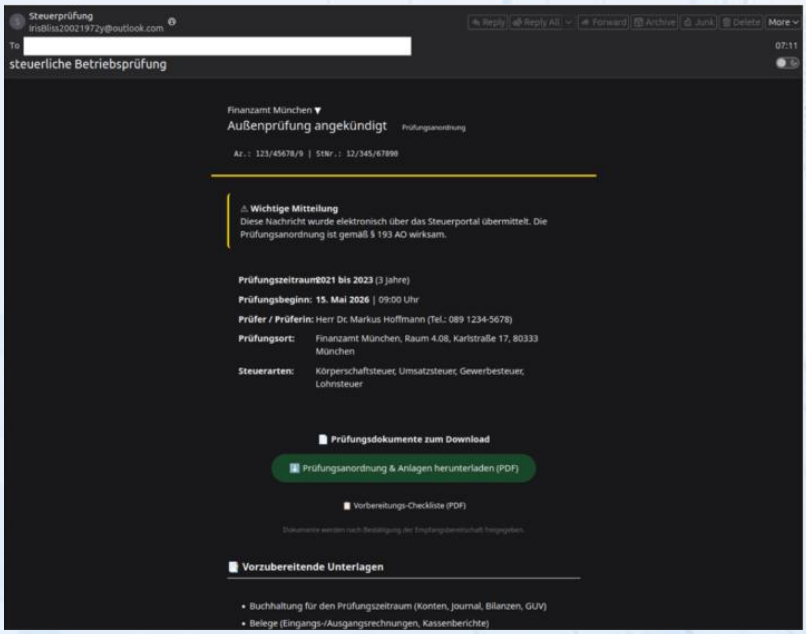
TA4922 Expands Global Financially Motivated Phishing Operations

In June 2026, researchers reported that **TA4922**, a suspected Chinese-speaking financially motivated threat group, expanded its operations beyond East Asia to target organizations across Europe, Africa, and other regions. The group conducted localized phishing campaigns **impersonating tax, payroll, HR, invoicing, and regulatory services, while deploying malware such as Atlas RAT, RomulusLoader, SilentRunLoader, and ValleyRAT (Winos4.0)**. The actors also abused legitimate platforms including LINE, WhatsApp, and Microsoft Teams to evade email security and compromise enterprise environments.

Threat Actor : TA4922 (Suspected Chinese-speaking Financially Motivated Cybercrime Group)
Target Verticals : Government, Financial Services, Manufacturing, Technology, Telecommunications, Healthcare, Retail, Professional Services, and Enterprise Organizations.



Social engineering email instructing recipients to create new LINE messaging group



Tax audit-themed email to lure recipients into downloading audit documentation

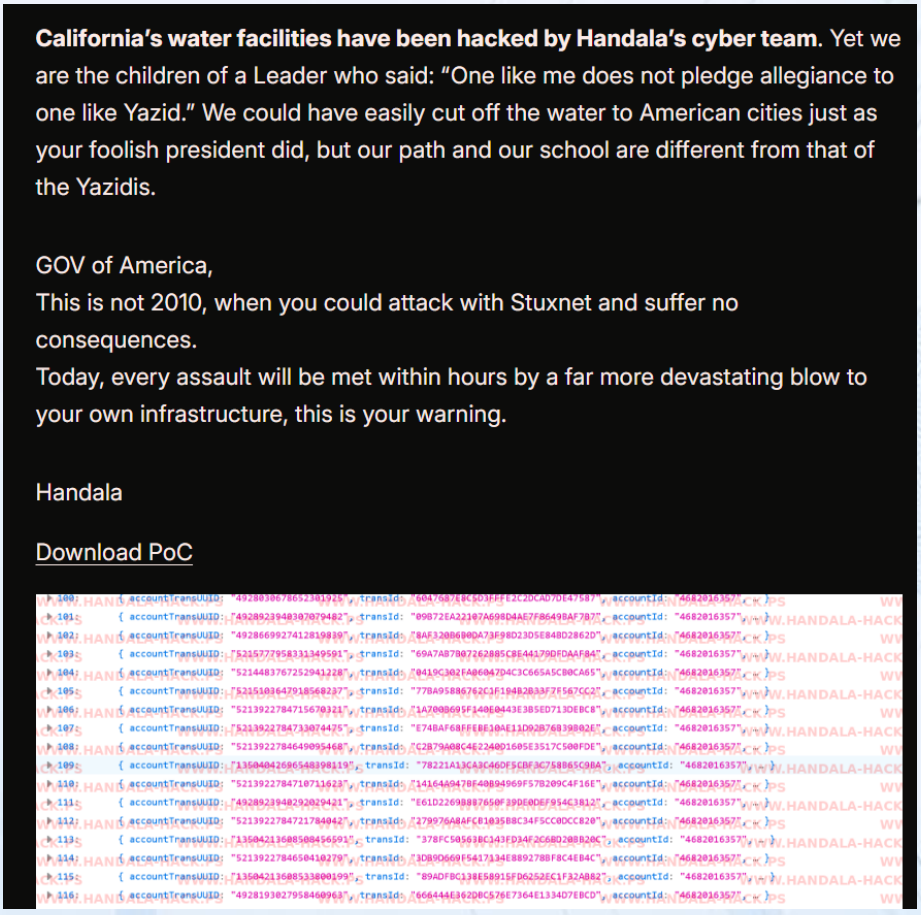
Cyber Incidents Amid Iran-Israel, US Context

Handala Hacked California Water Service

The hacking group said the intrusion was retaliation for recent US actions in Iran and claimed they had the ability to disrupt water access but chose not to. While the level of access Handala had has not been confirmed, actor's official blog says the threat actor likely hacked into Cal Water's RTKBase instance, a GNSS base station platform, and then moved laterally to a billing system.

Cal Water is one of the largest investor-owned water utilities in the US, with roughly two million customers across 100 communities in California. Cal Water's Chico District has been confirmed as the victim of the attack. Data leaked by Handala shows it likely accessed a customer billing database and Cal Water's internal RTKBase application.

"The billing system and RTKBase platform represent distinct infrastructure. The RTKBase network is assessed as a probable initial access vector or lateral pivot point that enabled the actor to reach the billing environment," the company says.



Post in Handala Hack Group official website

LA Metro Cyberattack Linked to Iranian State-Sponsored Hackers

The Los Angeles County Metropolitan Transportation Authority (LACMTA), widely known as LA Metro, discovered a breach in mid-March. The cybersecurity incident led to internal operational disruptions at LA Metro.

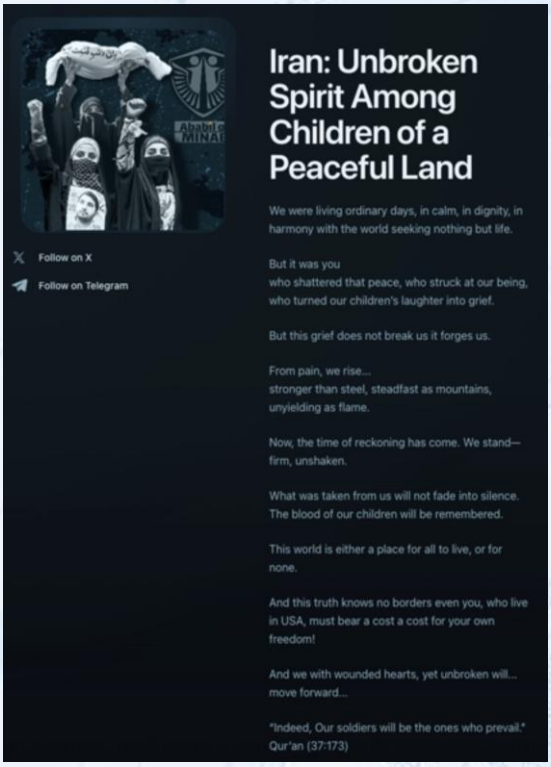
Threat Actor: Ababil of Minab





Screenshots shared from Ababil of Minab after targeting LA Metro

Threat Actor Motivation



Technical Details:

- **VMware vCenter Server**
  Administrative access to LACMTA's virtualization platform managing ~1,421 VMs, 28 hosts, 7.79 TB RAM, and 45 TB storage. Compromise could enable mass VM disruption, ransomware deployment, and persistent infrastructure-wide access.
- **Microsoft IIS Web Server**
  Administrator access to IIS servers hosting multiple internal and public-facing applications, including SSO services. This level of access could facilitate web defacement, credential theft, and lateral movement into backend systems.
- **Rail Yard Management / Train Control System**
  Access to a live Operational Technology (OT) system displaying real-time rail yard operations. Compromise could impact operational safety and trigger critical infrastructure reporting requirements.

The pro-Iranian hacking group **Ababil of Minab** claimed responsibility for a cyberattack targeting the Los Angeles County Metropolitan Transportation Authority (LACMTA). The group published claims via their Telegram channel (t[.]me/ababilofminab/7) and their threat actor website (ababilofminab[.]io/metro-net-is-hacked/), including a video and multiple screenshots purporting to demonstrate access to live LACMTA internal systems. The group's website displays explicitly pro-Iranian messaging. LACMTA has not publicly confirmed or denied the breach at time of writing.

UAE Cyber Security Council Foils Sophisticated Cyberattacks Targeting Financial Sector

The **UAE Cyber Security Council** announced that the national cybersecurity system successfully detected and thwarted a series of sophisticated cyberattacks targeting multiple organizations operating within the UAE financial sector. According to the Council, the attacks were identified and contained in accordance with national cybersecurity protocols, preventing disruption to financial services and preserving the stability of the country's digital ecosystem. While no threat actor attribution or specific victim organizations were disclosed, the activity highlights the continued targeting of critical financial infrastructure by advanced cyber adversaries.

Technical Details

The UAE Cyber Security Council reported that the attack campaign involved **multiple attack vectors** commonly associated with advanced persistent threat (APT) and financially motivated intrusion operations, including:

- **Critical Infrastructure Targeting**
  - Attempts to compromise **digital systems** and **critical technology infrastructure** supporting financial institutions.
  - The attacks were successfully detected and contained before affecting service availability.
- **Advanced Phishing Campaigns**
  - Adversaries conducted sophisticated phishing operations designed to harvest credentials and establish initial access into targeted environments.
  - The campaign leveraged modern social engineering techniques to increase the likelihood of credential compromise.
- **Exploitation of Security Vulnerabilities**
  - Attackers attempted to exploit known security vulnerabilities in exposed systems and services to gain unauthorized access or elevate privileges.
  - No specific CVEs or affected products were disclosed by the UAE authorities.
- **Malware Deployment Attempts**
  - The campaign included attempts to deploy malicious software following successful intrusion attempts, indicating objectives consistent with establishing persistence, credential theft, or disruption of financial operations.
- **AI-Assisted Attack Techniques**
  - The Cyber Security Council highlighted that the attackers employed **Artificial Intelligence (AI)** to develop more sophisticated attack methods, automate elements of phishing campaigns, and increase the complexity of their operations, reflecting the evolving cyber threat landscape facing the financial sector.

Although the UAE Cyber Security Council did not attribute the campaign to a specific threat actor or disclose technical indicators of compromise (IOCs), the reported use of **advanced phishing**, **vulnerability exploitation**, **malware deployment**, and **AI-assisted attack techniques** demonstrates an increasingly sophisticated threat environment targeting the financial sector. The incident reinforces the importance of maintaining robust preventive controls, timely vulnerability management, continuous monitoring, and threat intelligence capabilities to defend against evolving attacks targeting critical financial infrastructure.

Vulnerability & Exploit Intel

Enterprise Network & Infrastructure

CVE-2026-50751 | CheckPoint Remote Access VPN Authentication Bypass (Zero-Day)

Severity & Metrics : Critical | Actively Exploited Zero-Day
The Vulnerability : An authentication bypass vulnerability affecting Check Point Remote Access VPN and Mobile Access gateways allows unauthenticated attackers to bypass authentication controls and gain unauthorized administrative access to internet-facing appliances.
Operational Impact : Successful exploitation may result in unauthorized VPN access, credential theft, lateral movement, ransomware deployment, and complete compromise of enterprise networks.
Threat Context : Actively exploited by the **Qilin ransomware group** and added to the CISA Known Exploited Vulnerabilities (KEV) catalog during June 2026.

CVE-2026-20245 | Cisco Catalyst SD-WAN Manager Command Injection (Zero-Day)

Severity & Metrics : High (CVSS 7.8) | Actively Exploited Zero-Day
The Vulnerability : An authenticated command injection vulnerability enables attackers with prior access to execute arbitrary commands as the root user on Cisco Catalyst SD-WAN Manager appliances.
Operational Impact : Exploitation provides complete administrative control of the SD-WAN management plane, enabling persistence, configuration tampering, and compromise of managed network infrastructure.
Threat Context : Cisco confirmed active exploitation during June 2026. Attackers chained this flaw with CVE-2026-20127 and CVE-2026-20182.

CVE-2026-43503 | Linux Kernel "DirtyClone" Local Privilege Escalation

Severity & Metrics : High (CVSS 8.8) | Public Proof-of-Concept (PoC) Available
The Vulnerability : A flaw in the Linux kernel's XFRM/IPsec subsystem allows local attackers to overwrite cached kernel memory and escalate privileges to root.
Operational Impact : Enables complete system compromise, arbitrary code execution with root privileges, persistence, and defense evasion.
Threat Context : High risk for **Linux servers, Kubernetes clusters, NAS devices, cloud workloads, and enterprise infrastructure.**

Identity & Cloud Platforms

CVE-2026-42824 | Microsoft 365 Copilot "SearchLeak"

Severity & Metrics : Medium (CVSS 6.5)
The Vulnerability : A chained vulnerability in Microsoft 365 Copilot Enterprise Search could

expose emails, documents, SharePoint, OneDrive, and other sensitive organizational data.

Operational Impact : Unauthorized disclosure of enterprise information without requiring malware or elevated privileges.

Threat Context : Organizations adopting Microsoft 365 Copilot should review Microsoft's security recommendations.

CVE-2026-48567 | Azure HorizonDB Elevation of Privilege

Severity & Metrics : Critical (CVSS 10.0)

The Vulnerability : Elevation of privilege vulnerability affecting Azure HorizonDB.

Operational Impact : Unauthorized disclosure of enterprise information without requiring malware or elevated privileges.

Threat Context : Organizations adopting Microsoft 365 Copilot should review Microsoft's security recommendations.

CVE-2026-48579 | Microsoft Exchange Online Information Disclosure

Severity & Metrics : Critical

The Vulnerability : Information disclosure vulnerability affecting Exchange Online.

Operational Impact : Unauthorized access to enterprise email and business communications.

Threat Context : Microsoft 365 tenants should apply Microsoft's latest security updates.

CVE-2026-48579 | Microsoft Exchange Online Information Disclosure

Severity & Metrics : Critical

The Vulnerability : Information disclosure vulnerability affecting Microsoft Graph APIs.

Operational Impact : Exposure of enterprise data accessible through Microsoft Graph integrations.

Threat Context : Organizations should prioritize Microsoft's June security updates.

Microsoft Windows Zero-Day Vulnerabilities (June 2026)

CVE-2026-45586 | Windows CTFMON Privilege Escalation

Severity & Metrics : High (CVSS 7.8) | Publicly Disclosed Zero-Day

The Vulnerability : Improper link resolution allows attackers to obtain SYSTEM privileges.

Operational Impact : Full compromise of Windows systems following initial access.

CVE-2026-50507 | Windows BitLocker Security Feature Bypass

Severity & Metrics : High (CVSS 6.8) | Publicly Disclosed Zero-Day

The Vulnerability : Allows physical attackers to bypass BitLocker encryption.

Operational Impact : Exposure of sensitive enterprise data stored on encrypted devices.

CVE-2026-49160 | Windows HTTP.sys Denial-of-Service ("HTTP/2 Bomb")

Severity & Metrics : High (CVSS 7.5) | Publicly Disclosed Zero-Day

The Vulnerability : A flaw in the Windows HTTP.sys kernel-mode HTTP protocol stack allows specially crafted HTTP/2 requests to exhaust system resources, resulting in a denial-of-service condition. Successful exploitation can cause affected web servers to become unresponsive or crash, disrupting HTTP/2 services without requiring authentication.

Operational Impact : Exploitation can interrupt the availability of IIS and other Windows applications relying on HTTP.sys, leading to service outages, business disruption, and increased risk for internet-facing environments.

CVE-2026-47291 | Windows HTTP.sys Remote Code Execution

Severity & Metrics : Critical (CVSS 9.8)

The Vulnerability : A critical memory-handling vulnerability in Windows HTTP.sys enables unauthenticated attackers to send specially crafted HTTP requests that can trigger remote code execution in the kernel context. Successful exploitation could provide attackers with full control over vulnerable systems without user interaction.

Operational Impact : Complete compromise of internet-facing Windows web servers.

CVE-2026-44815 | Windows DHCP Client Service Remote Code Execution

Severity & Metrics : Critical (CVSS 9.8)

The Vulnerability : Specially crafted DHCP responses enable remote code execution.

Operational Impact : Remote compromise of Windows endpoints.

CVE-2026-45648 | Active Directory Domain Services Remote Code Execution

Severity & Metrics : Critical

The Vulnerability : Remote code execution affecting Active Directory Domain Services.

Operational Impact : Complete compromise of enterprise identity infrastructure.

CVE-2026-45607, CVE-2026-45641, CVE-2026-47652 | Microsoft Hyper-V Remote Code Execution

Severity & Metrics : Critical

The Vulnerability : Multiple remote code execution vulnerabilities affecting Microsoft Hyper-V.

Operational Impact : Guest-to-host escape and compromise of virtualization infrastructure.

CVE-2026-47288 | Windows Kerberos KDC Remote Code Execution

Severity & Metrics : Critical

The Vulnerability : Remote code execution affecting Windows Kerberos authentication.

Operational Impact : Compromise of enterprise authentication infrastructure.

Open Source & Enterprise Applications

CVE-2026-44789 & CVE-2026-44790 | n8n Workflow Automation

Severity & Metrics : Critical

The Vulnerability : Prototype Pollution and Sandbox Escape vulnerabilities allowing

authenticated attackers to execute arbitrary code on the host.

Operational Impact : Complete compromise of workflow automation servers, credential theft, and lateral movement.

Threat Context : Organizations using self-hosted n8n instances should immediately upgrade to patched versions.

CVE-2026-6722 | PHP SOAP Extension

Severity & Metrics : Critical (CVSS 9.5)

The Vulnerability : Memory corruption vulnerability affecting the PHP SOAP extension.

Operational Impact : May lead to remote code execution or denial-of-service in vulnerable PHP applications.

Threat Context : Organizations hosting PHP-based web applications should deploy updated PHP releases.

curl Multiple Vulnerabilities

Severity & Metrics : Multiple (High to Medium)

The Vulnerability : The latest curl release resolves **18 security vulnerabilities**, including memory safety flaws, certificate validation weaknesses, credential exposure, and protocol handling issues.

Operational Impact : Attackers may trigger denial-of-service, disclose sensitive information, or manipulate application communications.

Threat Context : As curl is embedded in Linux distributions, cloud platforms, DevOps pipelines, and enterprise software, organizations should prioritize vendor security updates.

CVE-2026-11645 | Google Chrome V8 Zero-Day

Severity & Metrics : High | Emergency Security Update

The Vulnerability : Type confusion vulnerability in the V8 JavaScript engine allowing remote code execution via malicious web content.

Operational Impact : Browser compromise, credential theft, arbitrary code execution, and endpoint takeover.

Threat Context : Organizations should immediately update Chrome to the latest stable release to mitigate active exploitation.

CVE-2026-11645 | Google Chrome V8 Zero-Day

Severity & Metrics : Medium

The Vulnerability : Open WebUI versions prior to 0.6.27 are vulnerable to Server-Side Request Forgery (SSRF) in the /api/v1/retrieval/process/web endpoint, allowing authenticated attackers to bypass SSRF protections and access internal services.

Operational Impact : Successful exploitation could expose internal network resources and potentially enable command execution using instance secrets, leading to further compromise.

Threat Context : The vulnerability affects Open WebUI < 0.6.27, requires low-privileged authenticated access, no user interaction, and has partial technical impact.

MITRE ATT&CK Mapping

ATT&CK Tactic	Techniques Observed	Observed in June 2026
Initial Access	T1566 Phishing, T1078 Valid Accounts, T1190 Exploit Public-Facing Application, T1195 Supply Chain Compromise	Kali365, Quishing, FortiBleed, ShinyHunters, TeamPCP
Execution	T1059 Command and Scripting Interpreter, T1204 User Execution	ClickFix PowerShell, malicious npm/PyPI packages, GitHub Actions abuse
Persistence	T1098 Account Manipulation, T1136 Create Account, T1505 Server Components	OAuth refresh tokens, compromised cloud identities, malicious libraries
Privilege Escalation	T1068 Exploitation for Privilege Escalation, T1548 Abuse Elevation Control Mechanism	DirtyClone Linux LPE, Windows Privilege Escalation vulnerabilities
Defense Evasion	T1036 Masquerading, T1027 Obfuscated Files, T1218 Signed Binary Proxy Execution	Legitimate Microsoft authentication flows, trusted developer tools, code signing abuse
Credential Access	T1110 Brute Force, T1555 Credentials from Password Stores, T1556 Modify Authentication Process	FortiBleed credential harvesting, OAuth token theft, GitHub PAT theft
Discovery	T1082 System Information Discovery, T1018 Remote System Discovery, T1046 Network Service Discovery	Enterprise reconnaissance after cloud compromise, infrastructure enumeration
Lateral Movement	T1021 Remote Services, T1550 Use Alternate Authentication Material	Azure identities, VPN credentials, Active Directory movement
Collection	T1005 Data from Local System, T1213 Data from Information Repositories	Customer databases, research data, ERP systems, cloud repositories
Command & Control	T1071 Application Layer Protocol, T1105 Ingress Tool Transfer	HTTPS C2, GitHub infrastructure, Cloudflare tunnels, Tor services
Exfiltration	T1041 Exfiltration over C2 Channel, T1567 Exfiltration to Cloud Storage	World Leaks, FulcrumSec, TeamPCP, ShinyHunters
Impact	T1486 Data Encrypted for Impact, T1499 Endpoint DoS, T1531 Account Access Removal	Extortion campaigns, service disruption, infrastructure compromise

Recommendations

Cloud & Identity Security

- Enforce phishing-resistant Multi-Factor Authentication across all privileged and remote access accounts.
- Apply Privileged Access Management (PAM) with just-in-time administrative access.
- Rotate exposed API keys, GitHub Personal Access Tokens, service accounts, and cloud credentials immediately upon exposure.
- Enforce least-privilege access across CI/CD pipelines and software repositories.
- Check package repositories for typo-squatting and dependency confusion attacks.

Ransomware Readiness

- Implement application allowlisting and Endpoint Detection and Response (EDR) solutions to detect and block ransomware execution, privilege escalation, and lateral movement.
- Segment critical systems and backup infrastructure from user networks to limit lateral movement following an initial compromise.
- Test recovery procedures periodically.

Email & User Protection

- Deploy advanced email security solutions capable of detecting phishing, malicious attachments, and impersonation attacks.
- Block execution of unsigned PowerShell scripts and restrict Office macros where possible.
- Conduct recurring security awareness training covering phishing, vishing, QR-code scams, device code phishing, and ClickFix social engineering techniques.

Vulnerability Management

- Prioritize remediation of internet-facing assets affected by actively exploited vulnerabilities.
- Continuously scan external attack surfaces for exposed VPNs, firewalls, cloud applications, and management interfaces.
- Implement risk-based vulnerability prioritization focusing on Known Exploited Vulnerabilities (KEVs).

Appendix

Threat Actors Observed

Threat Actor	Motivation	Primary Activity
World Leaks	Financial	Data extortion and large-scale data theft
ShinyHunters (UNC6240)	Financial	Data theft, ERP compromise, extortion
FulcrumSec	Financial	Cloud credential theft and extortion
Lazarus Group	Nation State (DPRK)	Supply chain compromise, espionage, cryptocurrency theft
TeamPCP (UNC6780)	Financial	Software supply chain compromise
TA4922	Financial	Regional phishing and malware delivery
Handala	Hacktivist	Critical infrastructure targeting
Ababil of Minab	Pro-Iranian	Critical infrastructure disruption
ChimeraZ	Financial	Data leak marketplace activity
0xSec	Financial	Database theft and underground sales

Malware Families Observed

Malware	Category
SharkLoader	Loader
SharpGPOAbuse	Post-Exploitation Tool
EKZ Infostealer	Information Stealer
ModeloRAT	Remote Access Trojan
Searchall	Credential Stealer
Atlas RAT	Remote Access Trojan
RomulusLoader	Loader
ValleyRAT (Winos 4.0)	Remote Access Trojan
SilentRunLoader	Loader
BeaverTail	Information Stealer
InvisibleFerret	Backdoor
Tropidoor	Backdoor
LightlessCan	Remote Access Trojan

Acronyms

Acronym	Meaning
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
ACR	Azure Container Registry
AD	Active Directory
API	Application Programming Interface
C2	Command and Control
CI/CD	Continuous Integration / Continuous Deployment
CVE	Common Vulnerabilities and Exposures
DLP	Data Loss Prevention
EaaS	Extortion-as-a-Service
EDR	Endpoint Detection and Response
IAM	Identity and Access Management
IOC	Indicator of Compromise
KEV	Known Exploited Vulnerabilities
MFA	Multi-Factor Authentication
OAuth	Open Authorization Framework
PAM	Privileged Access Management
PhaaS	Phishing-as-a-Service
SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
TTP	Tactics, Techniques, and Procedures
VPN	Virtual Private Network
Zero-Day	Previously unknown vulnerability actively exploitable