EnCyb

TLP: GREEN

THE INTEL BULLETIN

SEPTEMBER 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
Threat Intelligence Overview 4
Notable Campaigns & Events 5
Major Vulnerability & Exploit Intel 23
MITRE ATT&CK Mapping 25
Recommendations 26
Appendix 27
- Threat Actors Observed 27
- Malware Families Observed 28
- Acronyms 29

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

September 2026 was characterized by a **combination of ransomware activity, exploitation of internet-facing vulnerabilities, supply-chain compromise, data breaches, credential and session abuse, and politically motivated distributed denial-of-service (DDoS) campaigns**. The threat landscape demonstrated continued convergence between **financially motivated cybercrime, hacktivism, and targeted data exploitation, with organizations across government, finance, technology, healthcare, education, and critical infrastructure** remaining exposed.

The Global Threat Overview identified **Government, Finance, Technology, Education, and NGO sectors** among the most targeted sectors during the reporting period. The leading risk categories were Ransomware, Vulnerability Exploitation, Data Breach, Phishing, and Supply-Chain Compromise. The report also **highlighted Qilin, Akira, TheGentlemen, Storm, and Krybit** among the most active malware families observed during the month.

The vulnerability landscape remained equally concerning. September reporting included actively exploited vulnerabilities affecting Check Point **Management Server, Citrix NetScaler, Cisco Secure Email Gateway, FortiMail, GitLab, Microsoft Exchange Server, Node.js ecosystem components**, and other enterprise technologies. Of particular concern were vulnerabilities enabling unauthenticated remote access, arbitrary command execution, privilege escalation, session hijacking, and security-control bypass.

The overall threat assessment for September is therefore HIGH, driven by the combination of active exploitation, ransomware expansion, large-scale data exposure, supply-chain weaknesses, and politically motivated attacks against public-facing infrastructure.

Threat Intelligence Overview

10+
Major Incidents

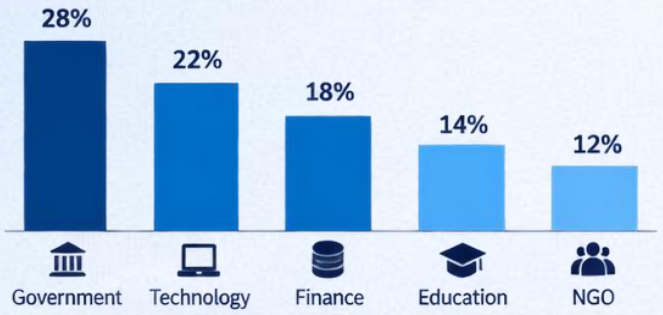
9+
Critical Vulnerabilities

10+
Active Threat Actors

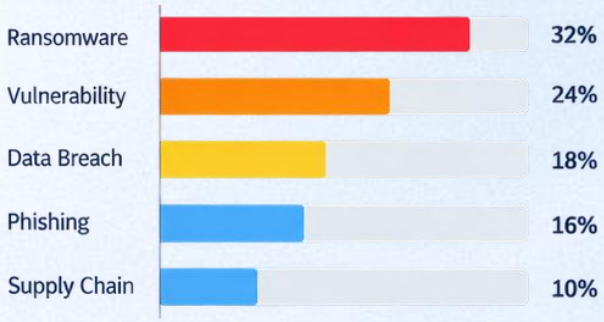
~28M+
Records Exposed

5
Active Malware Families

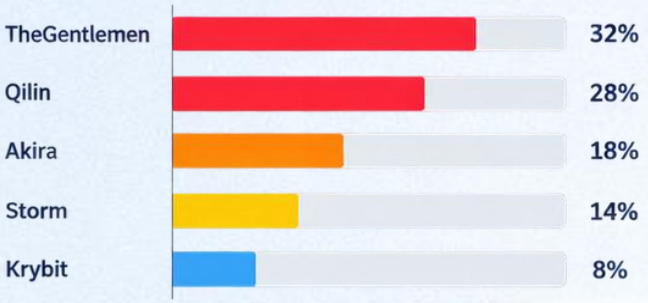
Top 5 Target Sectors



Top 5 Threat Risks



Top 5 Active Malwares



Major Vulnerabilities & Exploits

CVE ID	Product / Component	Risk
CVE-2026-96940	Microsoft Exchange Server	Critical
CVE-2026-104286	FortiMail	Critical
CVE-2025-7775	Citrix NetScaler (CitrixBleed 2)	High
CVE-2025-8971	Check Point Management Server	High
CVE-2025-20352	Cisco Secure Email Gateway	High

September 2026 Threat Highlights

ShinyHunters
FBI compromise claim with alleged access to personnel data and website defacement.

Gyazo
23.62M user records exposed following image-upload server compromise.

Brevo
Supply-chain attack via compromised Cloudflare API key, malicious JavaScript and ClickFix activity.

DragonForce
RaaS activity with data theft, encryption and extortion across multiple sectors.

DMDC
3.05M individuals affected due to file-sharing vulnerability exposing military personnel information.

RipperSec / TheGarudaEye
Layer 7 DDoS attacks targeting public-facing infrastructure in the Middle East region.

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.



Reported a cyber intrusion claim involving **the U.S. Federal Bureau of Investigation (FBI)**, attributed to the cybercrime and extortion group **ShinyHunters**, which claimed to have compromised FBI systems and **accessed sensitive information relating to FBI personnel and job applicants**. The group claimed access to Criminal Justice, Human Resources (HR), and Medlink services and alleged possession of data relating to nearly all FBI agents and job applicants. To support its claims, ShinyHunters reportedly defaced a subdomain of the FBI's jobs website, fbijobs.gov, displaying a message stating that the site had been seized. The group further claimed to have obtained **2-3 TB of information** and provided a sample allegedly containing personal information of **approximately 5,000 FBI employees**, **including names, telephone numbers, and home addresses**. The authenticity and origin of the complete dataset had not been independently confirmed, although reports indicated that portions of the sample appeared authentic.

Threat Actor Profile



Attack Technique: ShinyHunters claimed to have gained unauthorized access to FBI systems by **exploiting a zero-day vulnerability in Oracle PeopleSoft and subsequently accessing multiple FBI services**. The group alleged that it exfiltrated 2-3 TB of information, including sensitive personnel data, and used website defacement as evidence of the claimed compromise. The attackers subsequently used the alleged stolen information as leverage by **threatening disclosure and demanding that the FBI retract or correct an earlier threat report concerning the group.**





Figure: *Official FBI jobs portal was seized by ShinyHunters*

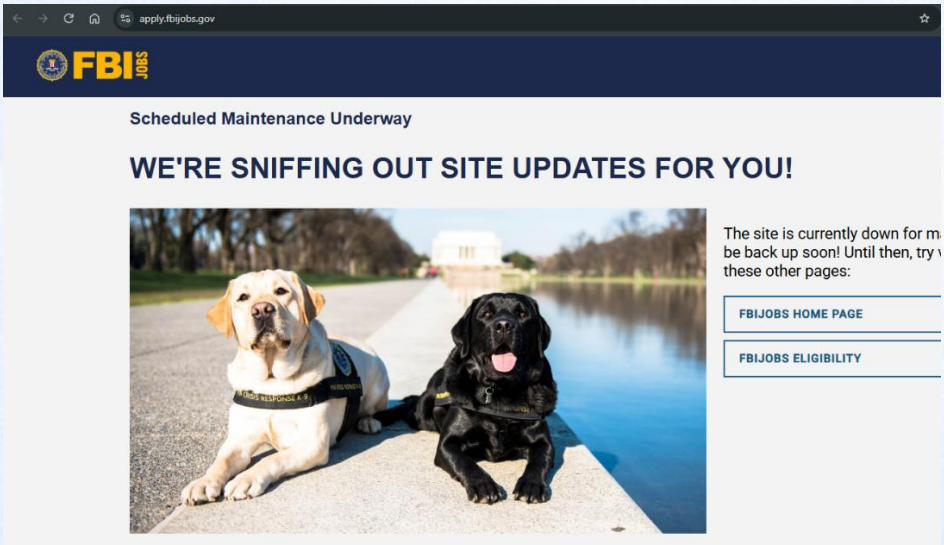
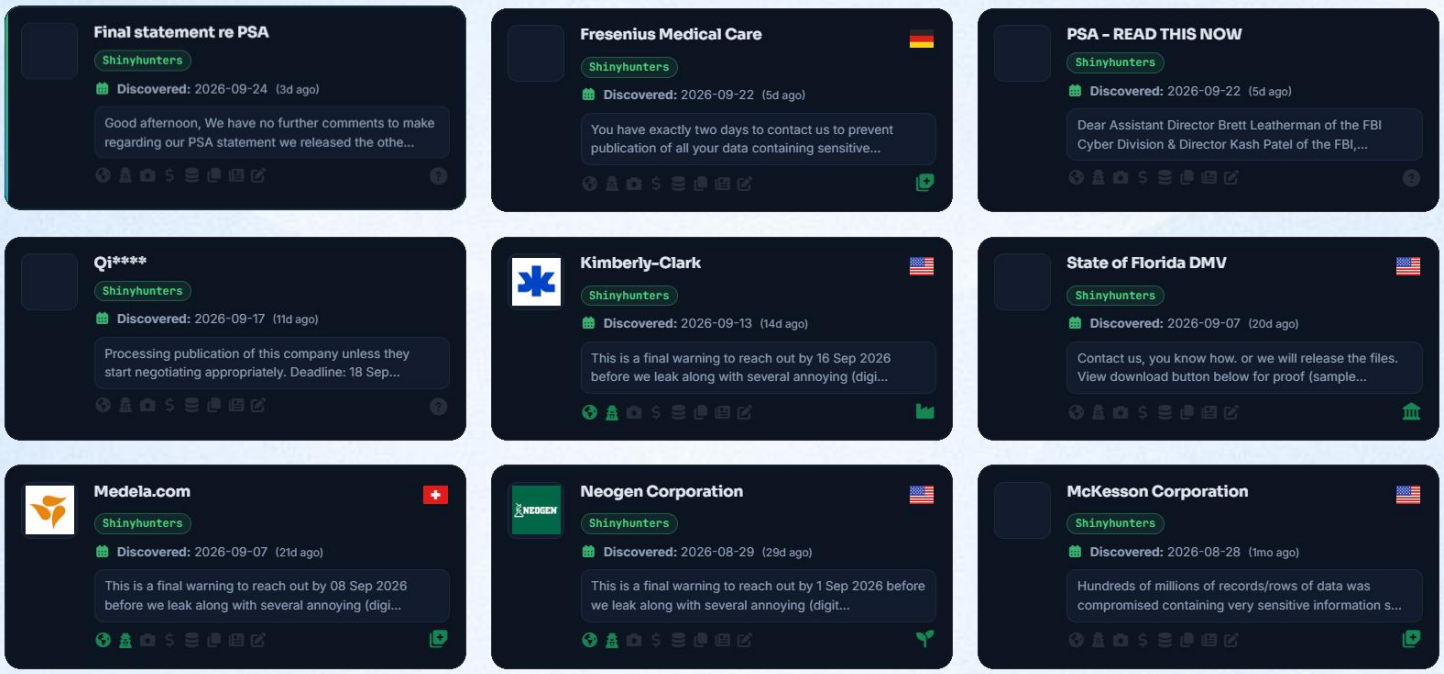


Figure: *FBI has now changed the page into maintenance notification*

Recent Victims of ShinyHunters





A major data breach affecting **Gyazo, the image-sharing service operated by Japanese software company Helpfeel**, after attackers exploited a **vulnerability in the service's image upload server** to gain unauthorized access and execute malicious commands. The intrusion, identified on **September 11, 2026**, allowed the attacker to access a database containing approximately **23.62 million Gyazo user records** before access was blocked the following day. The exposed information reportedly includes **names or nicknames, email addresses, password hashes, user IDs, device IDs, login session IDs, X integration tokens, Google SSO email addresses, profile information, subscription and billing status, registration and last-login information, and usage statistics**. In addition, approximately **490 million image metadata records were exposed**, primarily associated with images uploaded in or before January 2019, while metadata from a further 2.4 million images was accessed through specific searches. The exposed image metadata may include image IDs, upload IP addresses, User-Agent information, EXIF location data, OCR text, image titles, source URLs, and hashed passphrases associated with private images. Some of this information could potentially be used to reconstruct Gyazo image URLs and access images without authorization.

Helpfeel stated that payment card information was not exposed and that it had blocked the access routes used in the incident and remediated the exploited vulnerability. The investigation remained ongoing, and users were advised to change their passwords, particularly where the same or similar passwords were reused on other services, and to remain vigilant against phishing and other suspicious communications.

Incident Metric

User records exposed	~23.62 million
Image metadata records exposed	~490 million
Date of intrusion	September 11, 2026
Attacker access cut off	September 12, 2026
Public disclosure date	September 16, 2026
Disclosure delay	~5 days (attack to notice)
Data types exposed	Emails, password hashes, user/device/session IDs, image IDs, OCR text, EXIF data, X and Google SSO tokens
Payment card data exposed	None, per Helpfeel
Regulator notified	Japan's Personal Information Protection Commission
Bulk of exposed images date to	January 2019 or earlier

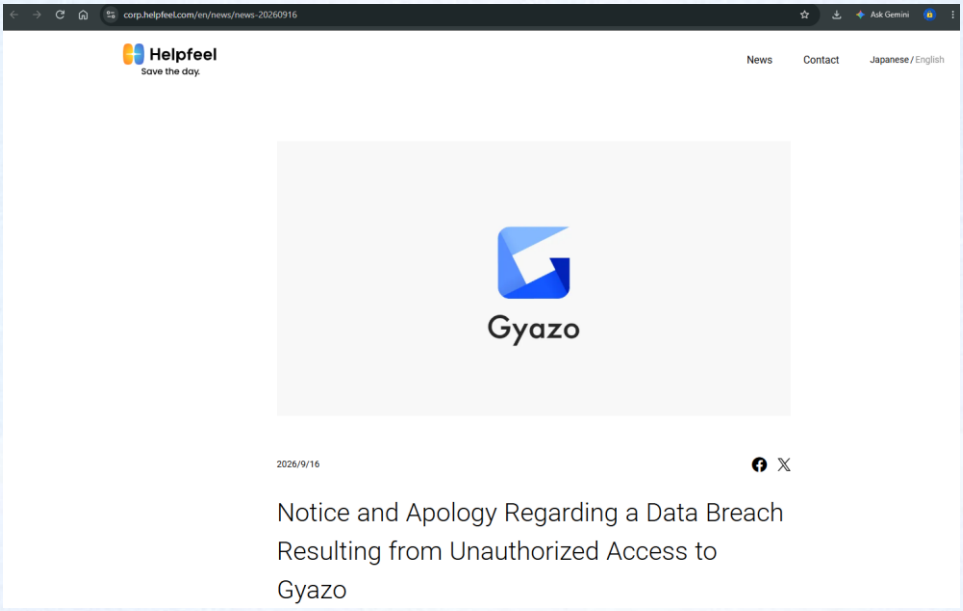
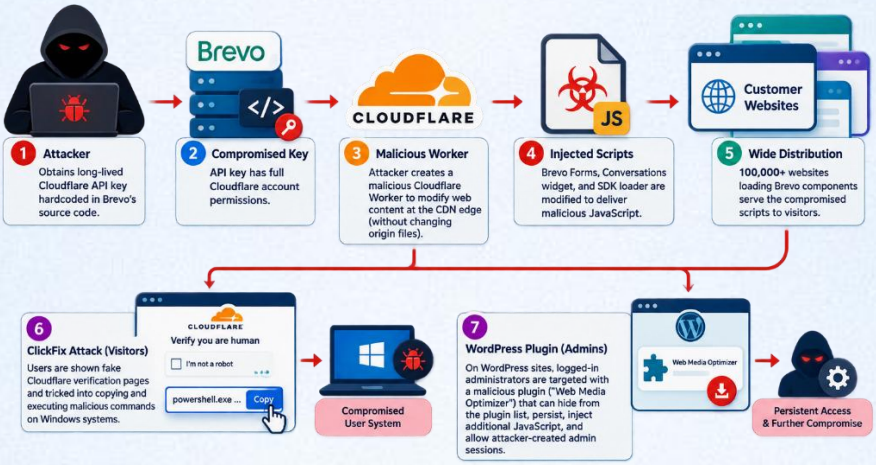


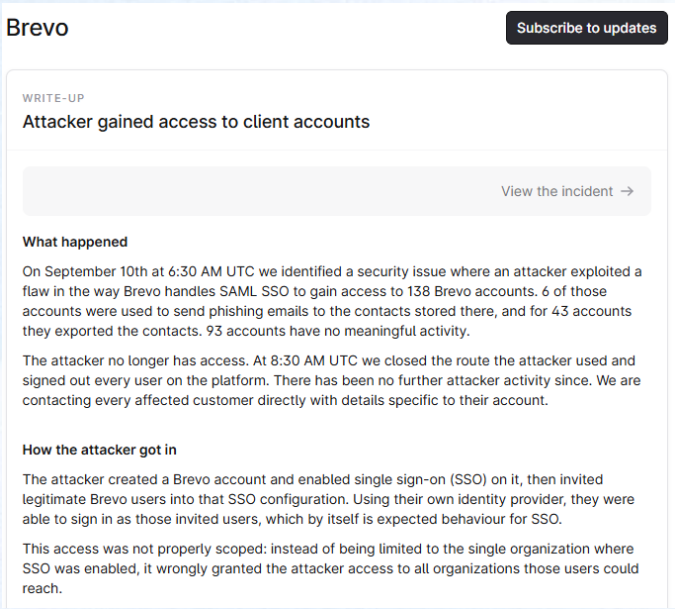
Figure: *Helpfeel (formerly Nota) disclosed breach affecting Gyazo, its cloud-based screenshot and screen-recording sharing service* ***(Source:*** *https://corp.helpfeel.com/en/news/news-20260916**)***

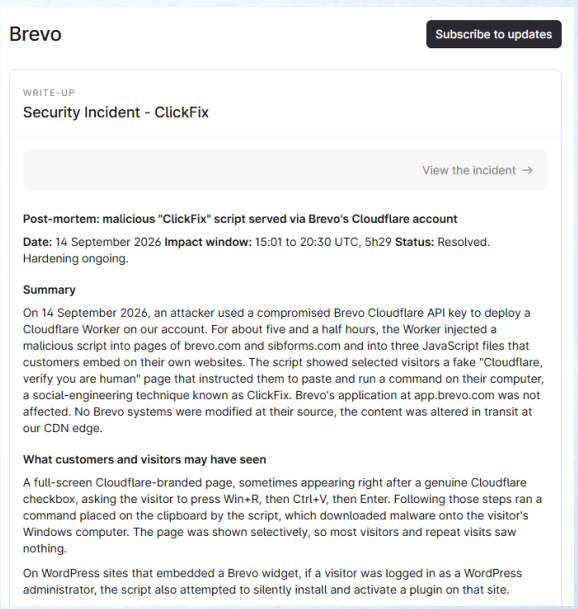


Supply chain attack targeting Brevo, a customer engagement and digital marketing platform, in which attackers **compromised a long-lived Cloudflare API key that had been hardcoded in Brevo's application source code**. The Cloudflare API key were owning the full account privileges. The attackers created a malicious Cloudflare Worker that modified Brevo-hosted JavaScript, including Forms, Conversations, and SDK components, potentially **affecting 100,000+ websites**.

Visitors were redirected to fake Cloudflare verification pages using the **ClickFix technique** to execute malicious commands. On WordPress sites, the **attack also attempted to install a disguised "Web Media Optimizer" plugin capable of persistence**, JavaScript injection, and administrator session generation. Brevo stated that its core application, APIs, email infrastructure, and customer data were unaffected.







Figures: *Brevo official incident writeup on their portal.(**Sources :** https://status.brevo.com/incidents/01M266V1CZKJQNGZRNEGFD5CQE/write-up, https://status.brevo.com/incidents/01M2QBC4EZ24ZACW6SWQYVW8N3/write-up)*

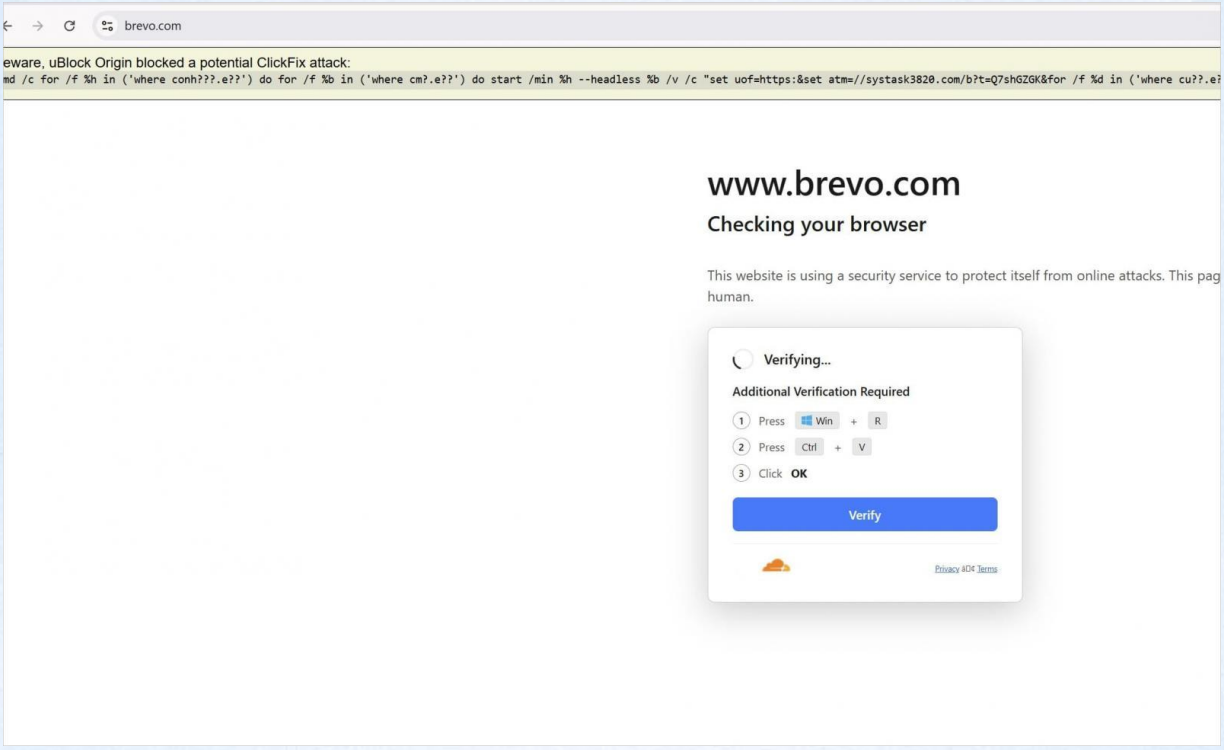


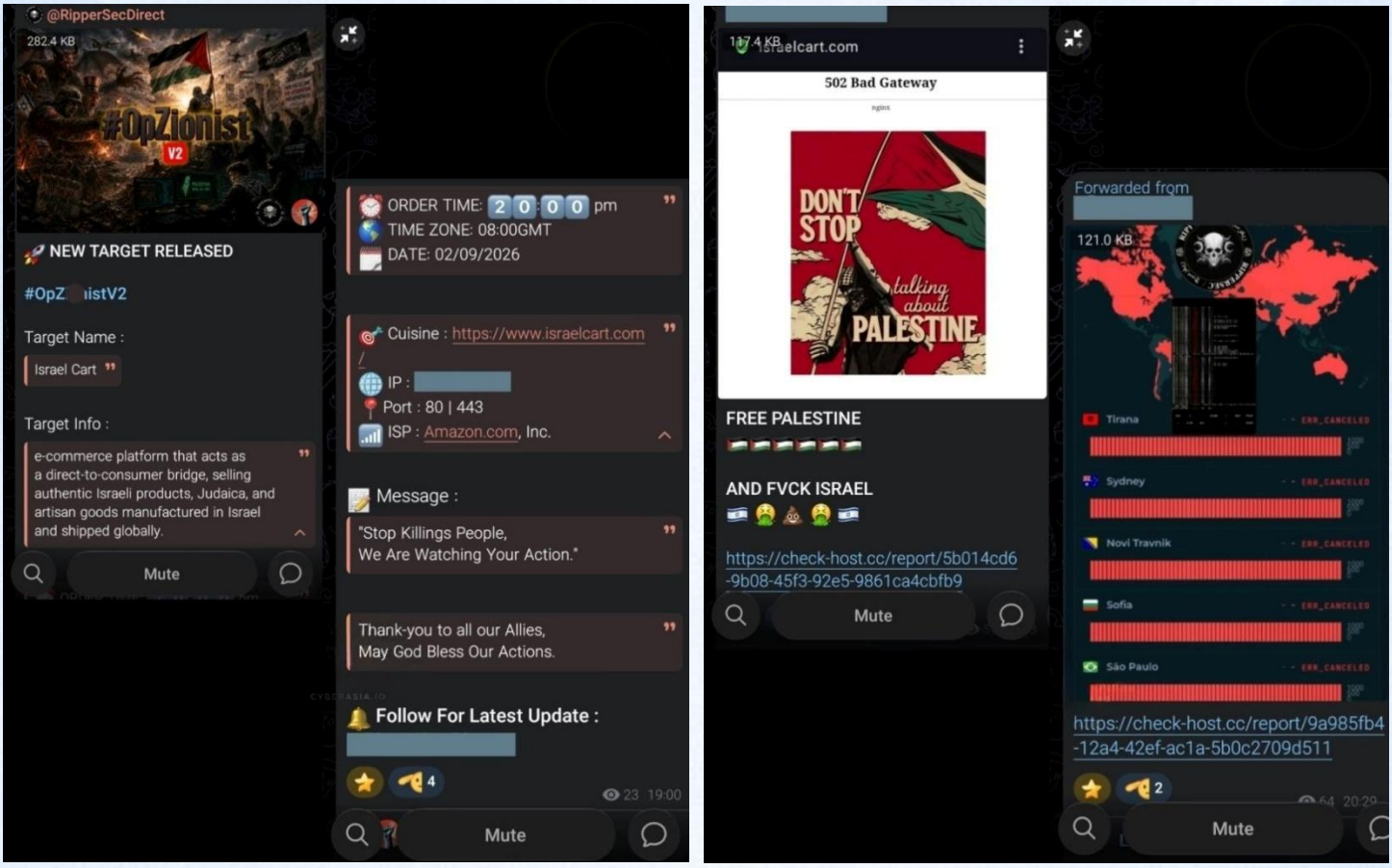
Figure*: ClickFix lure on the Brevo website*

The injected payload used ClickFix social engineering to trick visitors into manually executing attacker-supplied commands. Logged-in WordPress administrators were separately targeted through an attempted silent installation of a persistent malicious plugin, enabling further malicious JavaScript injection and potential administrator-session abuse.



Reported a coordinated distributed **denial-of-service** (DDoS) campaign targeting **Israel Cart, an Israeli e-commerce platform**, attributed to the Southeast Asian hacktivist collective **RipperSec** under the #OpZionistV2 campaign. The attack, first reported on **September 2, 2026**, subjected the platform's web infrastructure to sustained application-layer request floods targeting HTTP and HTTPS services hosted on Amazon Web Services (AWS). During the campaign, israelcart.com became intermittently or completely inaccessible across multiple independent monitoring locations, with monitoring nodes recording persistent connection timeouts, severe packet loss, socket exhaustion, and **repeated 502 Bad Gateway and 504 Gateway Timeout responses**.

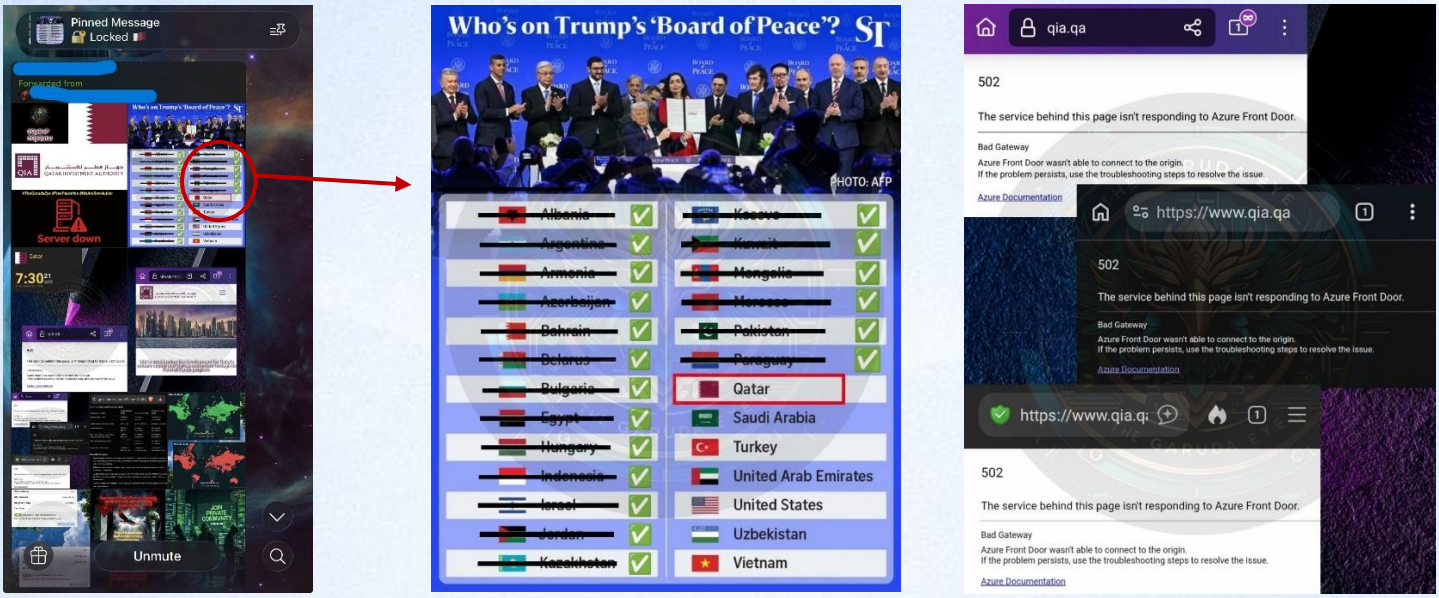
The campaign was amplified through allied hacktivist channels, with RBL Leviathan Ghost reportedly directing the DDOSTEAMRBL bot cluster against the target, while The Comrade's Group contributed additional traffic using the MegaMedusa stress-testing framework. The disruption affected the availability of the e-commerce storefront and potentially impacted customer transactions and service reliability.



***Figures**: Threat actor telegram channel posts on publish and proof of attack on israelcart.com*

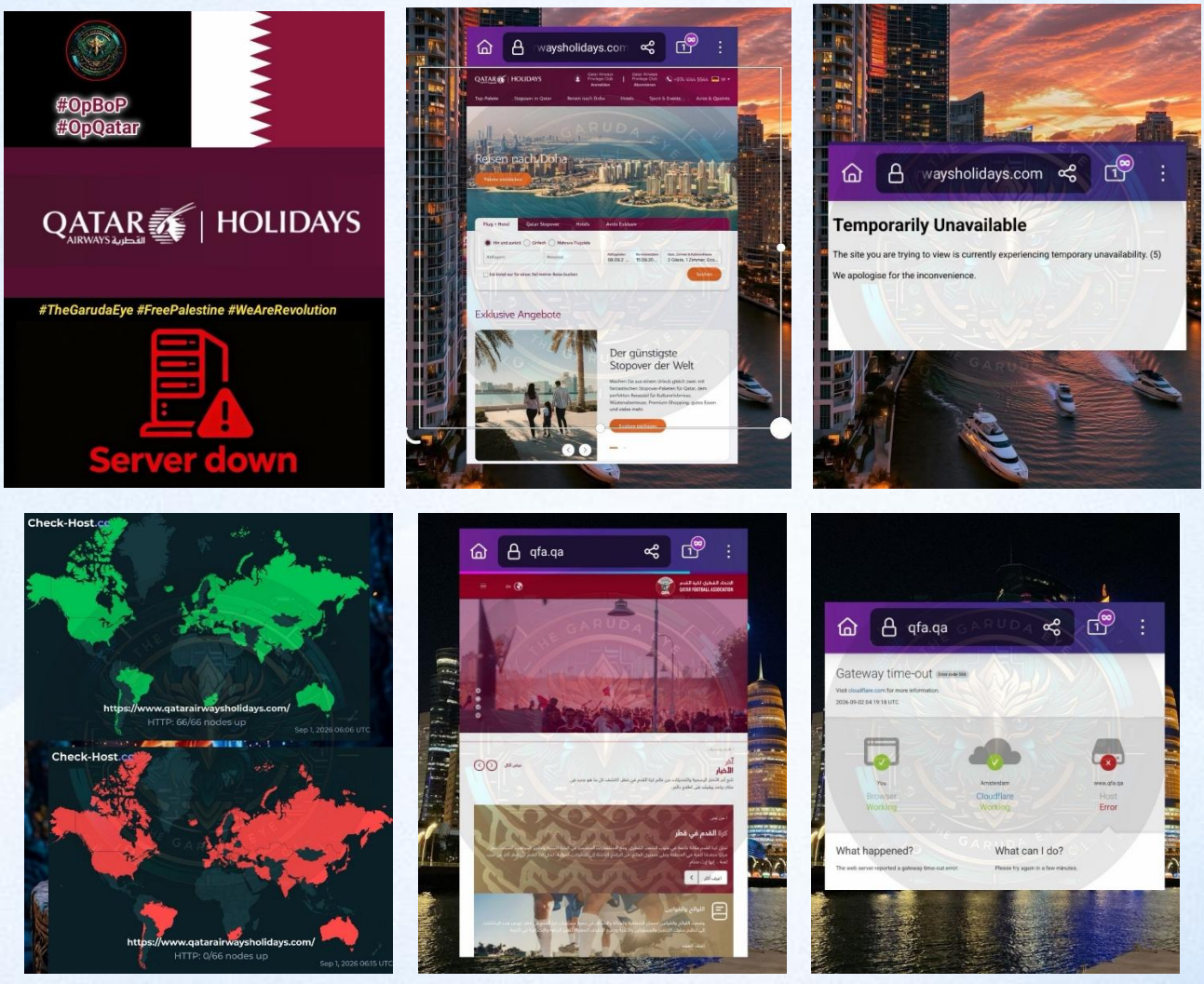


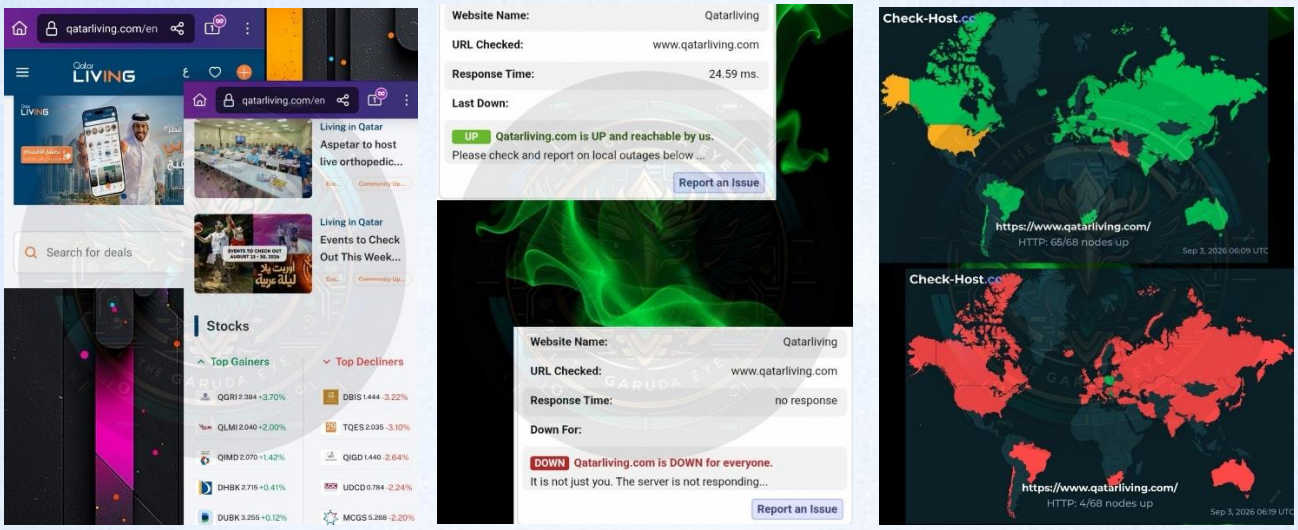
Distributed attack targeting **established public infrastructure of Qatar**. Qatar Football Association (QFA) website, attributed to the hacktivist collective TheGarudaEye. The attack disrupted the QFA public website for more than three hours through coordinated Layer 7 HTTP flood waves, with visitors encountering HTTP 504 Gateway Timeout and Cloudflare Error 525 responses. Reported that multi-region network diagnostics recorded connection timeouts across international testing nodes, with subsequent probes showing a combination of HTTP 403, HTTP 504, and Cloudflare 525 errors.



***Figures**: Telegram post by GarudaEye with theirs target lists and proof of take downs.*

Actor's Post on Current Victims





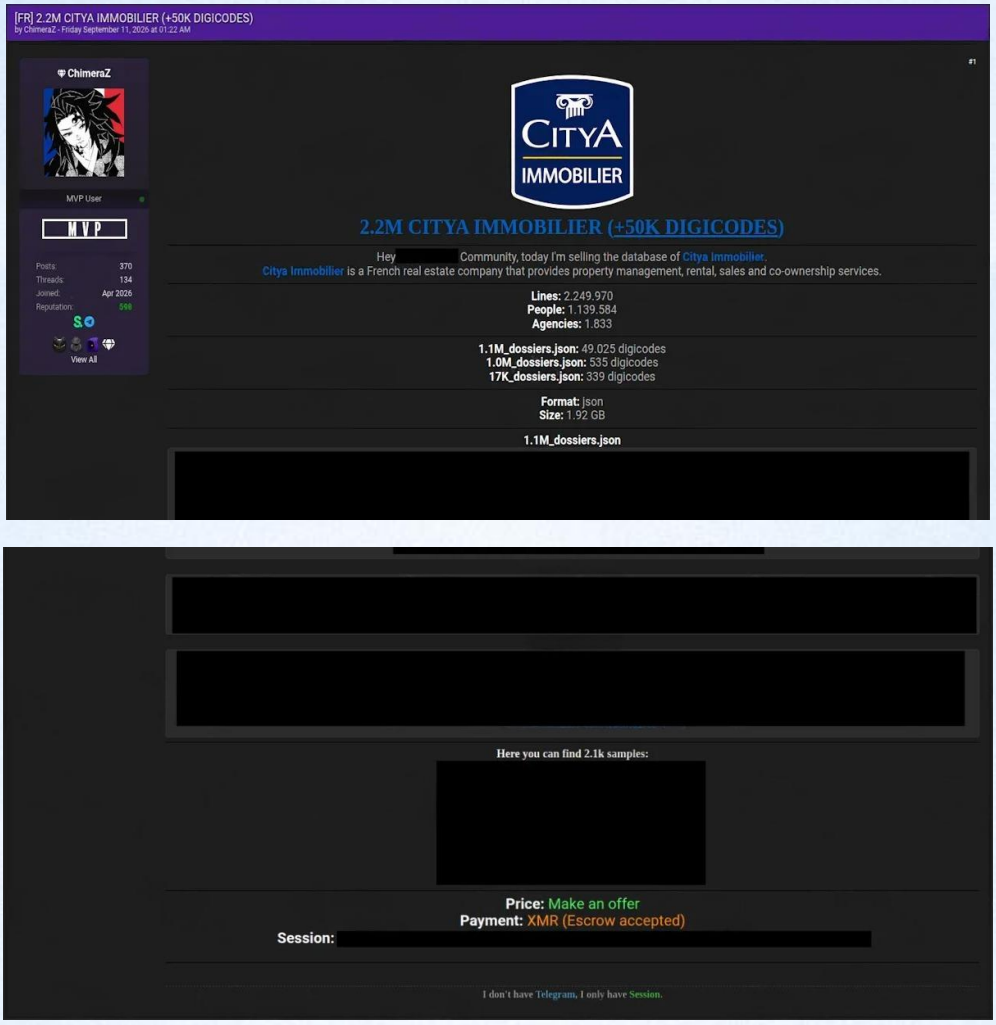
The attack was claimed through **Telegram channels associated with TheGarudaEye** under the campaign designation "**GLOBAL CYBER ATTACK #0131**," with the group initially announcing a three-hour attack duration and later extending the claimed disruption window to 15 hours. As the attack continued, QFA administrators reportedly implemented an emergency defensive measure by stopping the public-facing web application to limit further service degradation and protect backend systems. The incident was assessed as an external Layer 7 DDoS attack, with the report stating that no organizational data was exfiltrated, databases were not breached, and administrative credentials were not leaked. The activity forms part of TheGarudaEye's broader ideologically motivated hacktivist campaigns targeting Gulf-region digital infrastructure.



A reported data breach claim involving **Citya Immobilier**, a French real estate management company, has raised concerns over the alleged **exposure of approximately 2.2 million records and 50,000 building access codes** (digicodes). The reported dataset presents potential cybersecurity and physical security risks, particularly where compromised access codes could enable unauthorized entry into residential or commercial properties.

Depending on the information contained in the records, the alleged exposure could also facilitate targeted phishing, identity fraud and social engineering against residents and property owners. The incident highlights the convergence of cyber and physical security threats in the real estate sector and the importance of protecting sensitive tenant information and building access credentials.

The full article could not be retrieved, so the dataset figures are based on its headline. The breach's authenticity, the identity of the threat actor and the method of initial compromise remain unverified.



Figures: *Forum post offering an alleged Citya Immobilier dataset containing personal, property and building-access information, observed on 11 September 2026.*

If authentic, the dataset presents a significant privacy and physical-security concern because it appears to **combine identity and contact information with detailed property records and building access information. Names, phone numbers, email addresses and addresses could support phishing, impersonation and fraud, while appointment and property-management records** provide additional context for highly targeted social engineering. The claimed exposure of roughly 50,000 digicodes, together with intercom, residence, floor, door, parking and garage information, could also create risks extending beyond online abuse to unauthorized physical access if any of those codes remain valid.

The forum post provides detailed record counts, file names, sample JSON records and multiple sample-download locations. It also breaks out the number of claimed digicodes contained in each file and states that the full archive is **1.92 GB**. However, the listing does not explain how the data was obtained, when any unauthorized access occurred or whether the exposed access codes remain active.



In a darkweb forum, an actor posting as Marx reportedly advertised **11.8 million payment-related SMS records associated with Transfast (Mastercard's own payment systems), alongside access to a portal**. The alleged exposure raises concerns about the potential compromise of sensitive financial communications and the misuse of payment-related information for fraud, phishing and social engineering. If the advertised records contain identifiable customer or transaction information, they could **enable attackers to craft convincing financial impersonation campaigns**. The additional offer of portal access raises concerns about possible unauthorized access to payment-related systems. However, the authenticity of the advertised dataset, the nature of the portal access and the extent of any compromise require independent verification.

Potential Impact

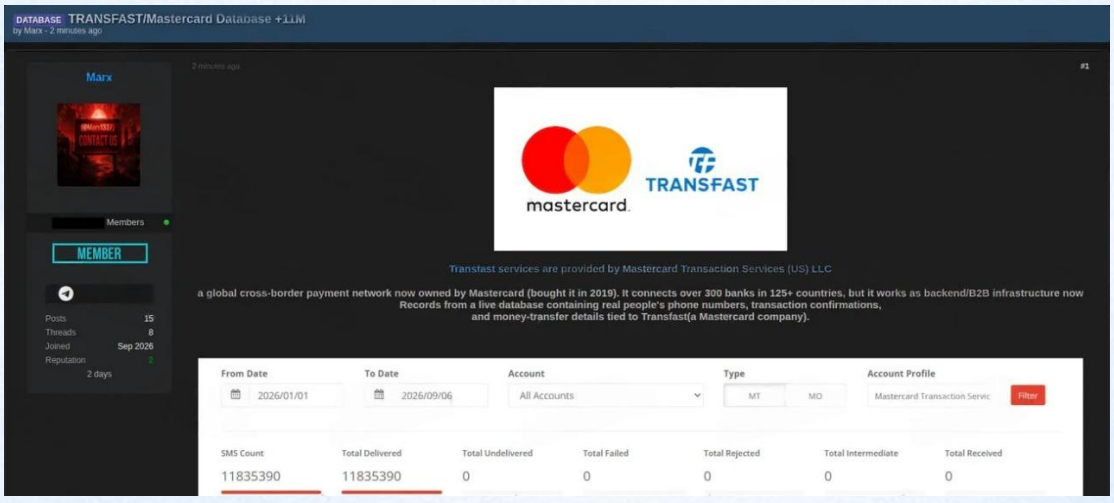
Sensitive Data Exposure: Potential disclosure of payment-related SMS records, which may contain sensitive transaction or customer information.

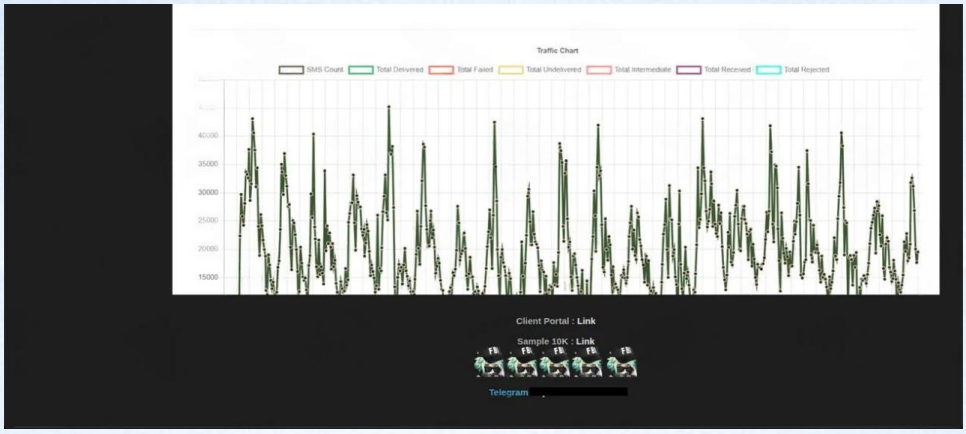
Financial Fraud: Exposed payment information could be exploited to facilitate fraudulent transactions, payment scams and financial impersonation.

Targeted Smishing Attacks: Attackers could use leaked SMS records to craft convincing phishing messages impersonating legitimate payment or remittance services.

Unauthorized Portal Access: If the advertised portal access is functional, attackers may be able to access additional sensitive information or misuse payment-related services, depending on the permissions available.

Customer Privacy and Regulatory Risks: Exposure of identifiable financial information could create privacy concerns and potential regulatory obligations for affected organizations.





Figures: *Forum post advertising Transfast messaging records, observed 7 September 2026.*

Framing matters here more than usual: what is shown is **a messaging provider's portal serving the payment company**, and nothing in the post indicates a compromise of Mastercard's own payment systems. The dashboard is internally coherent, with delivery counts matching the traffic chart across the stated period, but **a screenshot demonstrates a session rather than access that persists**, and no acquisition route is given. The account is **days old with almost no standing**. Dark Web Informer has **not retrieved the sample, is not linking the portal or contact addresses**, and neither company has publicly addressed the claim.



A threat actor operating under the alias **0cx00iq** has allegedly offered for sale a dataset containing sensitive personal information belonging to employees of Kuwait's National Security Agency. According to the actor, the dataset includes employees' full names, national identification numbers, phone numbers, mothers' full names, dates of birth, residential addresses, marital status, military status, and blood types.



The actor claims the information is current as of June 2026 and has advertised the dataset for approximately $3,500 (negotiable), providing a heavily watermarked spreadsheet sample as purported evidence. However, the authenticity, accuracy, and **full scope of the alleged data breach remain unverified** till this reporting date.

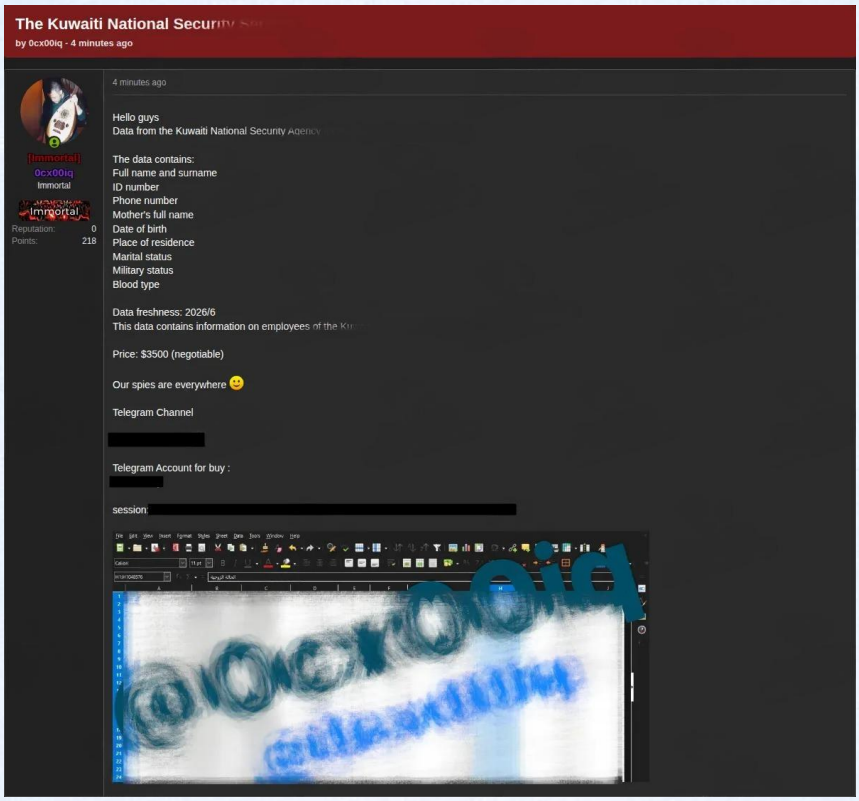


Figure: *Forum post advertising the leaked data*

Impact & Status

The alleged exposure of sensitive personal **information belonging to employees of a national intelligence agency** raises significant security and counterintelligence concerns. If verified, the compromised data could expose affected individuals to **physical targeting, surveillance, coercion, blackmail, identity theft, and impersonation**. Additionally, personal information such as mothers' full names and dates of birth could be exploited for **identity-verification fraud**. Beyond individual risks, the alleged breach could pose broader national security threats by enabling adversaries to identify intelligence personnel, exploit personal vulnerabilities, and conduct targeted intelligence-gathering operations.

A for-sale listing accompanied by a watermarked spreadsheet sample was published on an underground forum. The sample records, threat actor's contact details, and purchasing information have been excluded from this report. **The authenticity of the alleged data breach remains independently unverified, and Kuwaiti authorities have not issued any public statement regarding the incident.**



A significant data breach involving the **U.S. Department of Defense's Defense Manpower Data Center (DMDC)** reportedly exposed sensitive personal and employment information belonging to **approximately 3.05 million individuals**, including **2.76 million living people** and **294,000 deceased individuals**. The incident originated from a security **vulnerability in a file-sharing system that allowed unauthorized users to access files containing unencrypted personally identifiable information (PII) between October 2025 and July 16, 2026**. The compromised information included Social Security numbers, names, dates of birth, contact details, and military occupational information. The vulnerability was discovered on July 16, 2026, and affected individuals began receiving breach notifications in **September**. Although officials reported no evidence of data misuse at the time of disclosure, the incident raises substantial concerns regarding identity theft, targeted social engineering, and the potential exploitation of military personnel information for intelligence-gathering purposes.

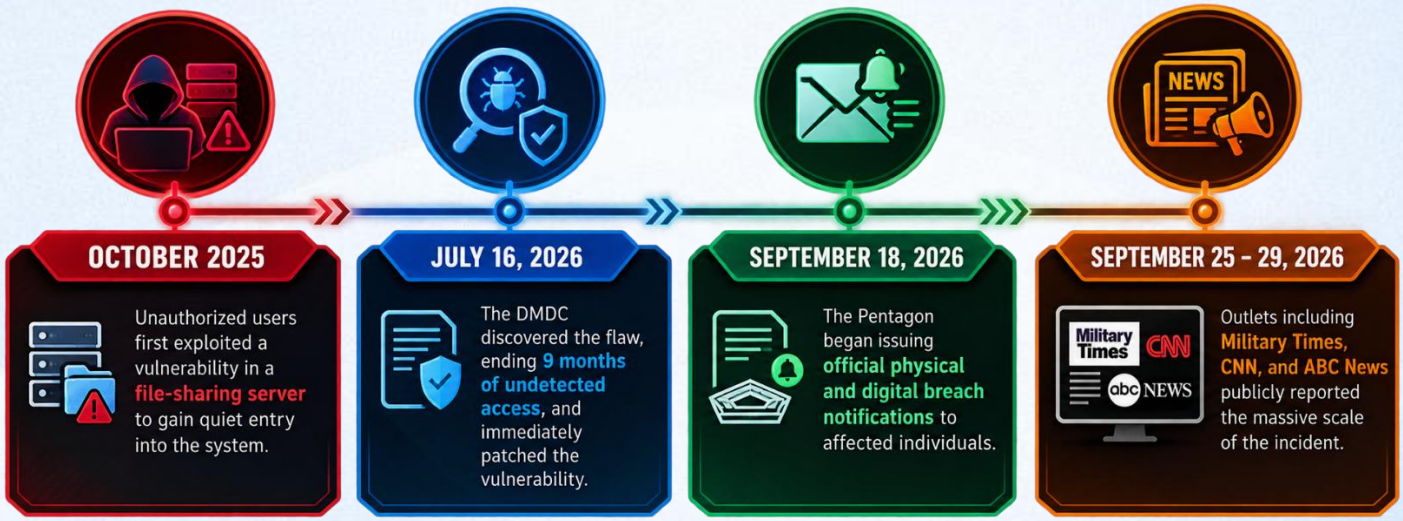
Threat Actor and Targeted Verticals

Threat Actor : *Unidentified*; no confirmed attribution at the time.

Targeted Organization : U.S. Department of Defense (DoD) - Defense Manpower Data Center (DMDC)

Target Verticals : Government, Defense, Military, Public Sector, Federal Personnel Administration

Breach Timeline



Attack Technique

The attackers exploited a security **vulnerability in DMDC's file-sharing system to gain unauthorized access** to files containing unencrypted personnel records. According to the breach notification, unauthorized access occurred over approximately **nine months, from October 2025 until July 16, 2026**. The exposed information included **Social Security numbers and additional personal identifiers, such as names, dates of birth, contact information and military occupational specialties**. Following the discovery, DMDC patched the vulnerability and restored the affected system. The initial intrusion method, identities of the attackers and extent of any data exfiltration remain undisclosed.



The DragonForce ransomware cartel has evolved into a centralized Ransomware-as-a-Service operation, driving a significant surge in global attacks through an aggressive white-label affiliate model. The group utilizes modified legacy source codes and advanced evasion tactics to target high-value organizations across multiple critical sectors. The group maintains an aggressive average attack velocity of 65 victims per month alongside updated VMware ESXi locker capabilities targeting versions 5 through 8.

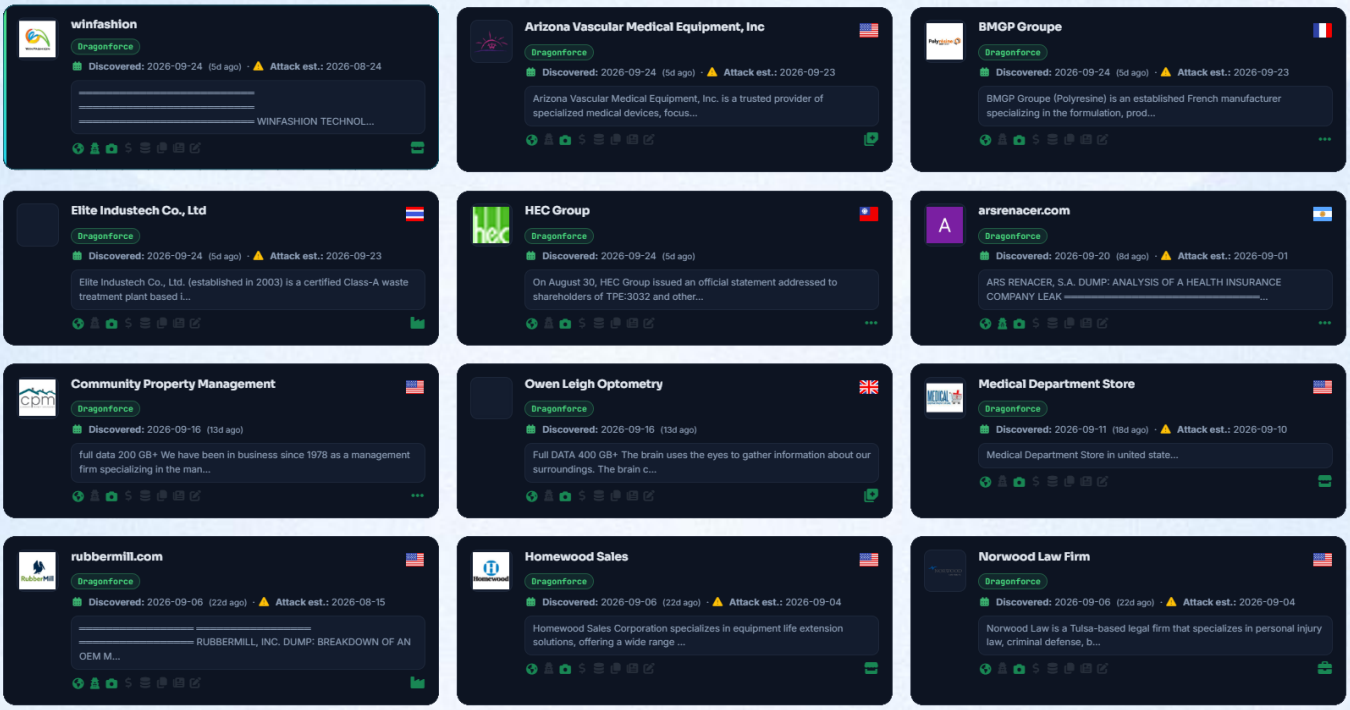
Threat Actor Profile

DragonForce is a financially motivated ransomware operation that emerged in **2023** and developed from a conventional **RaaS** model into a broader ransomware cartel structure. The operation **provides ransomware infrastructure and services to affiliates, allowing multiple operators to conduct intrusions under the DragonForce brand**. Public reporting describes the group as active across multiple industries and countries.

Threat Actor : DragonForce
Type : Ransomware-as-a-Service / ransomware cartel
Motivation : Financially motivated
First observed : 2023
Status : Active
Known aliases : DragonForce, DragonForce Ransomware Cartel, RansomBay
Operation : Data theft + ransomware encryption + extortion
Geographic : Global
Targeting Profile: Professional Services, Manufacturing, Technology, Retail & E-Commerce, Healthcare

The actor's dataset currently lists Professional Services and Manufacturing as the two largest sectors, followed by Technology. The United States accounts for the largest number of tracked victims, followed by the UK, Germany, Canada and Italy.

Major Victims in September



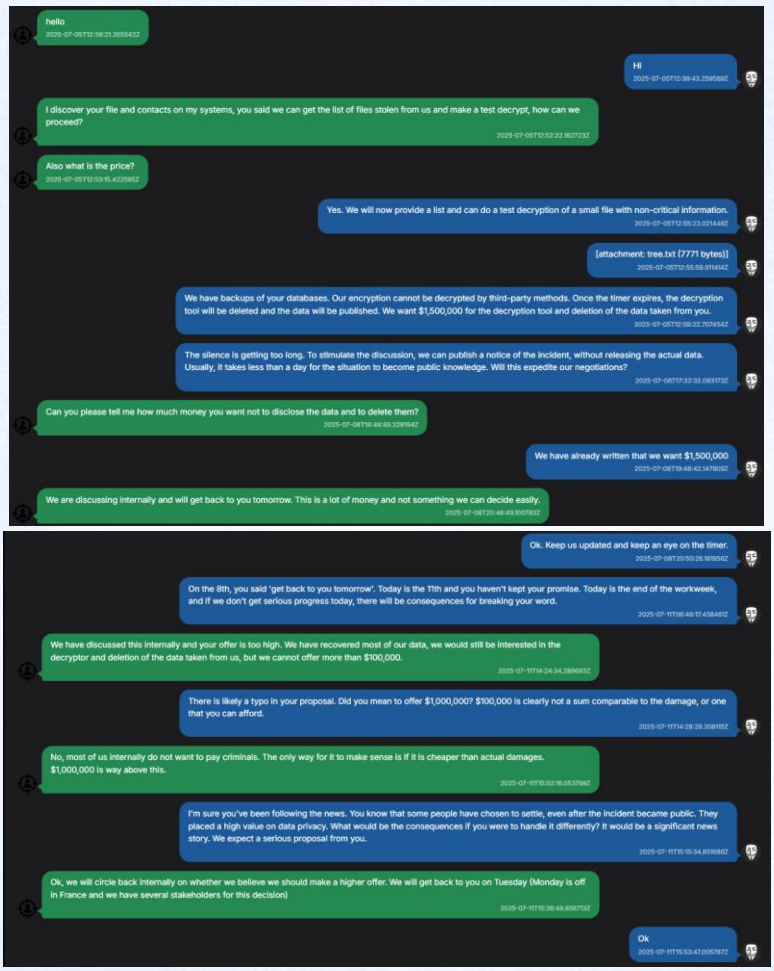


Figure: *Negotiation chat with threat actor*

Widely Exploited Vulnerabilities

VENDOR	PRODUCT	CVE
Apache	Log4j	CVE-2021-44228
Fortinet	FortiOS & FortiProxy	CVE-2024-21762
Fortinet	FortiOS & FortiProxy	CVE-2024-55591
SonicWall	SonicOS SSL-VPN	CVE-2024-40766
Ivanti	ICS	CVE-2024-21887
Pulse Secure / Ivanti	Ivanti Connect Secure	CVE-2024-21893
Pulse Secure / Ivanti	Ivanti Connect Secure	CVE-2023-46805
Windows	SmartScreen	CVE-2024-21412
SimpleHelp	SimpleHelp RMM	CVE-2024-57727
SimpleHelp	SimpleHelp RMM	CVE-2024-57728

TTPs Matrix

Execution : User Execution

Defense Evasion: Indicator Removal: File Deletion, Impair Defenses: Disable or Modify Tools

Discovery : File and Directory Discovery

Impact : Data Encrypted for Impact

DragonForce represents a mature RaaS ecosystem whose risk comes not only from its ransomware payload but from the scale of its affiliate model. The publicly tracked victim population spans numerous industries and jurisdictions, while the operation has continued adapting its infrastructure and attack methods.



A threat actor operating under the handle "**UWAYS**", claiming affiliation with Uways Qarani, alleges unauthorized access to systems associated with Prince Sultan Military Medical City (PSMMC), also referenced in the post as Riyadh Military Hospital. The actor claims to have obtained data belonging to **thousands of Saudi military personnel, along with patient and staff records, treatment information, and identity documents**.

Six screenshots accompanying the claim purportedly show samples of the alleged data, including a patient referral table, hospital and laboratory listings, a staff roster, identity document thumbnails, and hospital administrative interfaces. One displayed dashboard reference Prince Sultan Armed Forces Hospital Madinah, which differs from the Riyadh-based facility named in the original claim. The alleged intrusion, source, authenticity, completeness, and overall **scope of the data have not been independently verified till the reporting date**.

A technically precise description of how the compromise was allegedly achieved, including the initial access vector, systems/data accessed, and how the stolen information was subsequently exposed or offered.

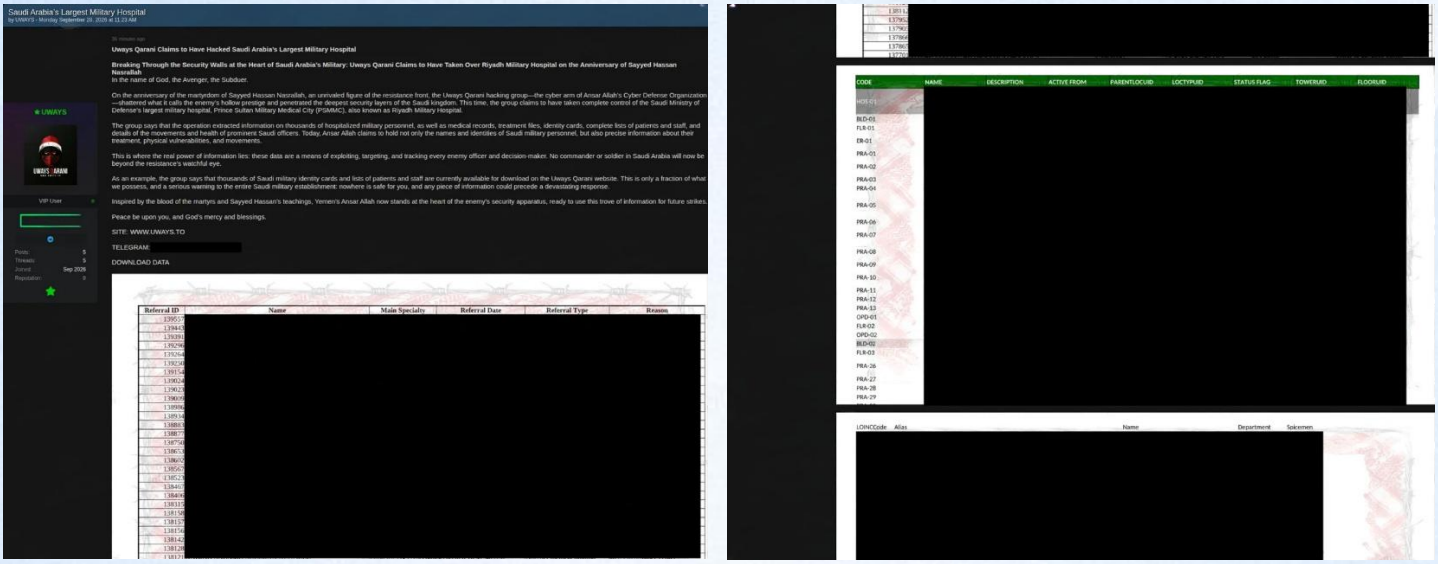


Figure: *Group post in darkweb forum, **t**he visible samples include personal and medical information; individual names, patient identifiers, contact details and document numbers are not repeated in this report.*

Post Claims

- Complete control of the named military hospital claimed
- Information on thousands of military personnel claimed extracted
- Medical records and treatment files claimed
- Patient and staff lists claimed available
- Military identity cards claimed available
- Patient referral table shown
- Staff roster with roles and contact fields shown
- Hospital location and department metadata shown
- Laboratory test catalog shown

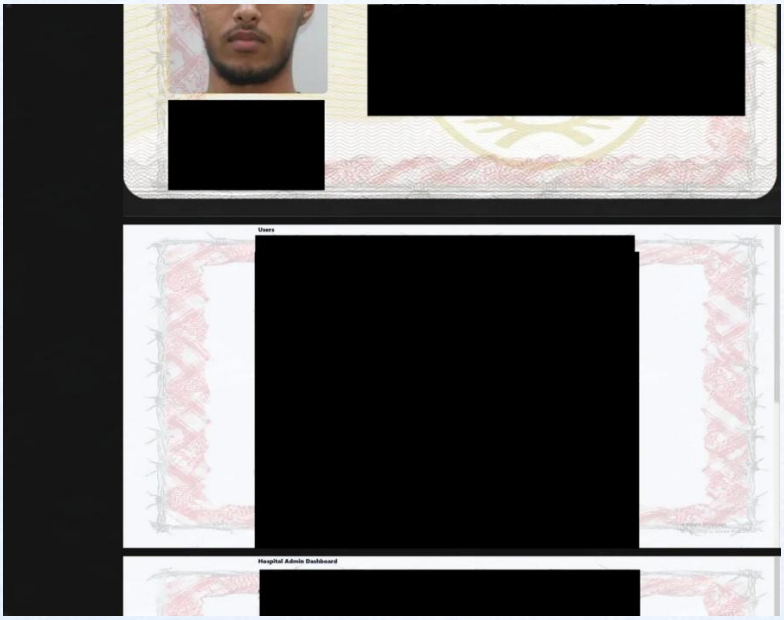


Figure: *Patient identity information sample post.*

Major Vulnerability & Exploit Intel

Open Source & Enterprise Applications

GitLab (CVE-2026-19478) - Unauthenticated Code Injection

A critical flaw in GitLab's GraphQL directives allowed remote, unauthenticated attackers to silently inject malicious code, modify public repositories, and manipulate internal enterprise user data. GitLab has **remediated** an issue in GitLab **CE/EE affecting all versions from 18.2 before 18.11.11, 19.0 before 19.0.8, 19.1 before 19.1.6, and 19.2 before 19.2.4** that under certain conditions could allow an unauthenticated user to remotely modify or delete public projects and user data via a GraphQL directive.

References: *https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-4-released/*

https://nvd.nist.gov/vuln/detail/cve-2026-19478

Node.js & Ecosystem Vulnerabilities

Software supply chain failures remained a massive threat, with over 72% of organizations discovering high-risk vulnerabilities rooted deep within transitive open-source dependencies (such as ecosystem libraries like Node.js).

Undici (HTTP/1.1 Client for Node.js) - CVE-2026-85152: A severe regression vulnerability was introduced in *undici* versions 8.10.0 and 8.10.1. The library omitted the destination origin from its internal cache and request-deduplication keys when components were composed onto a Client or Pool.

Node.js HTTP Request Smuggling - CVE-2026-58044: The internal HTTP parser omitted headers exceeding maxHeadersCount boundaries from application-facing objects (req.headers) but continued using them internally for message framing.

Next.js Ecosystem Patches: On September 30, 2026, the Next.js Security Team rolled out delayed emergency security patches fixing a critical flaw and a high-severity vulnerability originating from upstream dependencies. **Fix:** Update frameworks immediately to v16.3.8 (Active LTS) or v15.5.27 (Maintenance LTS)

Reference: *https://nodejs.org/en/blog/vulnerability/july-2026-security-releases*

CVE-2026-96940 - Microsoft Exchange Server Elevation of Privilege Vulnerability

A weakness in the authorization logic of Microsoft Exchange Server can allow an attacker that has authenticated network access to gain higher privileges than intended. The flaw is recognized as CWE-1390 and could enable the attacker to perform actions as a system administrator or other privileged user, compromising confidentiality, integrity, and availability of mail services. Microsoft Exchange Server 2016 Cumulative Update 23, Microsoft Exchange Server 2019 Cumulative Update 14, Microsoft Exchange Server 2019 Cumulative Update 15, Microsoft Exchange Server Subscription Edition RTM are affected. Users of these versions should verify which cumulative update applies to their installation.

Reference: *https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96940*

Microsoft September 2026 Security Updates

Microsoft's September 2026 Security Updates address a broad range of vulnerabilities across Windows and other Microsoft products. The release includes security fixes and cumulative updates, with additional out-of-band updates issued to address issues affecting Remote Desktop Services and other Windows components. Microsoft also expanded VEX reporting to all Microsoft-assigned CVEs, helping organizations better assess vulnerability exposure and prioritize remediation.

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

Enterprise Network & Infrastructure

Check Point Patches Exploited Management Server Zero-Day

Check Point patches a directory traversal and file upload vulnerability allows an unauthenticated attacker to upload and execute arbitrary scripts on Check Point Management Server. This vulnerability is exploited in the Wild. Check Point is aware of a handful of customers who have been attacked. This issue received the ID **CVE-2026-93616** and a CVSS score of 9.8. Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent are the affected products.

Reference: https://support.checkpoint.com/results/sk/sk1000171/

CitrixBleed 2: Critical NetScaler Flaw Enables Session Hijacking and MFA Bypass

CVE-2025-5777 (CitrixBleed 2) is a critical memory exposure vulnerability affecting NetScaler ADC and Gateway deployments configured with Gateway or AAA virtual servers. Attackers can exploit malformed login requests to leak sensitive memory, including session tokens, enabling session hijacking and MFA bypass. The flaw is actively exploited and has been added to CISA's Known Exploited Vulnerabilities catalog. Organizations should immediately apply Citrix's recommended security patches. Over 400 NetScaler instances remain exposed, while the related CVE-2025-6543 affects approximately 500 additional deployments.

Reference: https://www.netscaler.com/blogs/2025-06/netscaler-critical-security-updates-for-cve-2025-6543-and-cve-2025-5777

CVE-2026-76461 actively exploited in Cisco Secure Email Gateway

CVE-2026-76461 is a critical, actively exploited vulnerability in Cisco Secure Email Gateway that allows unauthenticated remote attackers to execute arbitrary commands with root privileges, potentially causing full system compromise. CISA has added it to the KEV catalog and mandated remediation by September 17, 2026. No patch or workaround is currently available; organizations should monitor mail logs for suspicious activity and contact Cisco for guidance.

Reference: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX

CVE-2026-104286 actively exploited in FortiMail via path traversal and null byte injection

CVE-2026-104286 is a critical FortiMail path traversal and null byte injection vulnerability (**CVSS 9.8**) enabling unauthorized code or command execution and potential system compromise. It is actively exploited as a zero-day, with identified IOCs including modified files and suspicious IPs. CISA has mandated mitigation by October 4, 2026. Organizations should disable IBE, restrict management access, apply security updates, and monitor for the reported IOCs.

Reference: https://fortiguard.fortinet.com/psirt/FG-IR-26-175

MITRE ATT&CK Mapping

ATT&CK Tactic	Techniques	Observed in September 2026
Initial Access	**T1190 Exploit Public-Facing Application, T1078 Valid Accounts, T1566 Phishing**	**ShinyHunters** alleged Oracle PeopleSoft exploitation; **Gyazo** image-upload server compromise; **DMDC** file-sharing vulnerability exploitation; **Brevo** supply-chain compromise and ClickFix activity.
Execution	**T1059 Command and Scripting Interpreter, T1204 User Execution, T1203 Exploitation for Client Execution**	**Brevo ClickFix** campaigns tricked users into executing malicious commands; compromised infrastructure delivered malicious JavaScript and attempted WordPress plugin execution.
Persistence	**T1505 Server Software Component, T1098 Account Manipulation**	**Brevo** attackers attempted to install a malicious WordPress plugin for persistence; compromised credentials and sessions enabled continued access.
Privilege Escalation	**T1068 Exploitation for Privilege Escalation**	**Microsoft Exchange CVE-2026-96940** enabled privilege escalation; **Check Point, FortiMail and other enterprise vulnerabilities** provided opportunities for elevated access.
Defense Evasion	**T1562.001 Impair Defenses, T1070.004 File Deletion**	**DragonForce** employed security-tool disabling and file deletion; ransomware operations used evasion techniques to hinder detection and response.
Credential Access	**T1539 Steal Web Session Cookie, T1552.001 Unsecured Credentials**	**CitrixBleed 2** exposed session tokens enabling session hijacking and MFA bypass; **Brevo** involved a highly privileged Cloudflare API key embedded in application source code.
Discovery	**T1083 File and Directory Discovery**	**DragonForce** ransomware activity included file and directory discovery during compromised-environment operations.
Lateral Movement	**T1005 Data from Local System, T1213 Data from Information Repositories**	**ShinyHunters** claimed FBI personnel data theft; **Gyazo** exposed user and image metadata; **DMDC** data included military personnel PII; **UWAYS** claimed access to Saudi military hospital records.

Collection / Exfiltration	**T1486 Data Encrypted for Impact, T1498 Network Denial of Service, T1491.002 External Defacement**	**DragonForce** conducted ransomware encryption and extortion; **RipperSec/TheGarudaEye** launched DDoS campaigns; **ShinyHunters** allegedly defaced the FBI jobs portal.
Impact	**T1190 Exploit Public-Facing Application, T1078 Valid Accounts, T1566 Phishing**	**ShinyHunters** alleged Oracle PeopleSoft exploitation; **Gyazo** image-upload server compromise; **DMDC** file-sharing vulnerability exploitation; **Brevo** supply-chain compromise and ClickFix activity.

Recommendations

Cloud & Identity Security

- Enforce phishing-resistant MFA for privileged, VPN, cloud and externally accessible accounts.
- Rotate and secure API keys using centralized secrets management and periodic credential rotation.
- Apply least-privilege access across cloud IAM, service accounts, APIs and third-party integrations.
- Restrict cloud/SaaS administration to trusted networks or approved access paths where possible.
- Audit third-party integrations by maintaining an inventory of OAuth apps, API integrations and service principals.
- Centralize cloud audit logging for authentication, IAM changes, API activity, administrative actions and data access.

Infrastructure & Vulnerability Management

- Prioritize actively exploited vulnerabilities affecting Check Point, Citrix NetScaler, Cisco Secure Email Gateway, FortiMail and other products.
- Maintain an accurate internet-facing asset inventory covering VPNs, firewalls, email gateways, applications, APIs and remote-access infrastructure and establish periodical audit on them.
- Adopt risk-based vulnerability prioritization using exploitation status, CISA KEV, CVSS, exposure, exploit availability and business criticality.
- Establish emergency zero-day patching with predefined remediation, compensating controls, isolation and validation procedures.
- Restrict management interfaces to authorized administrative networks and secure access paths.
- Strengthening software supply-chain security
- Harden web applications and APIs with secure coding, WAF, input validation, strong authentication and regular penetration testing.

Email & Endpoint Protection

- Strengthen phishing and ClickFix protection through targeted awareness on fake CAPTCHA, browser verification and malicious command prompts.
- Monitor suspicious command execution involving PowerShell, CMD, scripting engines and LOLBins launched from browsers, Office or downloaded files.
- Enable behavioral ransomware detection for mass file changes, encryption, shadow-copy deletion and security-tool tampering.
- Protect EDR controls against unauthorized disabling, modification or service termination.
- Strengthen email authentication with SPF, DKIM and enforced DMARC policies.
- Maintain endpoint isolation procedures for rapid containment of ransomware, credential theft and malware incidents.
- Conduct modern phishing simulations incorporating ClickFix and other current social-engineering techniques.

Appendix

Threat Actors Observed

Threat Actor	Motivation	Primary Activity
ShinyHunters	Financial / Extortion	Alleged data theft, unauthorized access, website defacement and extortion
DragonForce	Financial	Ransomware-as-a-Service, data theft, encryption and extortion
RipperSec	Ideological / Hacktivism	DDoS campaigns targeting Israeli organizations and infrastructure
TheGarudaEye	Ideological / Hacktivism	Layer 7 DDoS campaigns against Gulf-region infrastructure
RBL Leviathan Ghost	Ideological / Hacktivism	DDoS participation against Israel Cart
The Comrade's Group	Ideological / Hacktivism	Additional DDoS traffic against Israel Cart
UWAYS / Uways Qarani	Unknown	Alleged unauthorized access and data theft involving Saudi military healthcare infrastructure
0cx00iq	Financial / Data Sale	Alleged sale of sensitive employee information belonging to Kuwait's National Security Agency
Marx	Financial / Data Sale	Alleged sale of Transfast-related payment SMS records and portal access
Unidentified Actor(s)	Unknown	Alleged compromise of the U.S. DoD Defense Manpower Data Center

Malware Families Observed

Malware	Category	Relevance
Qilin	Ransomware	Identified among the top active malware families during September
Akira	Ransomware	Active ransomware family observed during the reporting period
TheGentlemen	Ransomware	Identified among the top active malware families
Storm	Malware / Threat Campaign	Identified among the top active malware entries
Krybit	Ransomware / Malware	Identified among the top active malware entries
DragonForce	Ransomware / RaaS	Ransomware operation employing encryption, data theft and extortion
Qilin	Ransomware	Identified among the top active malware families during September
Akira	Ransomware	Active ransomware family observed during the reporting period
TheGentlemen	Ransomware	Identified among the top active malware families
Storm	Malware / Threat Campaign	Identified among the top active malware entries
Krybit	Ransomware / Malware	Identified among the top active malware entries
DragonForce	Ransomware / RaaS	Ransomware operation employing encryption, data theft and extortion

Acronyms

Acronym	Meaning
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CISA	Cybersecurity and Infrastructure Security Agency
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
KEV	Known Exploited Vulnerabilities
NGO	Non-Governmental Organization
PII	Personally Identifiable Information
PSMMC	Prince Sultan Military Medical City
QFA	Qatar Football Association
RaaS	Ransomware-as-a-Service
SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
SSO	Single Sign-On
TLP	Traffic Light Protocol
TTP	Tactics, Techniques and Procedures
URL	Uniform Resource Locator