DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT REPORT

MARCH 2026

Contents

LOTS AND DDOD: THE NEW EMERGING TECHNIQUES

Introduction

Attackers today are no longer trying to break down the front door, they are silently blending into the environment and operating quietly within trusted systems. These strategies are not new, and now they are rapidly getting popular in the threat environment.

These techniques are called “Living off Trusted Sites (LOTS)” The concept is similar to “Living-off-the-Land (LotL)” technique which is used by threat actor groups where they use existing resources and standard services (e.g., PowerShell) for cyber-attacks. This benefits the attacker by hiding large amounts of legitimate network traffic and bypass traditional security measures.

What Is LOTS?

The concept of “Living off Trusted Sites (LOTS)” is to use legitimate services and trusted websites to conduct malicious activities without any detection. Services that are used daily like GitHub, Google Drive, Google Spreadsheet, Azure, AWS, etc. are rarely monitored and are used by the threat actors to conduct malicious activities like:

- Hosting phishing webpages
- Operating botnet commands
- Command and Control (C2) servers
- Drop malwares
- Exfiltrate the system

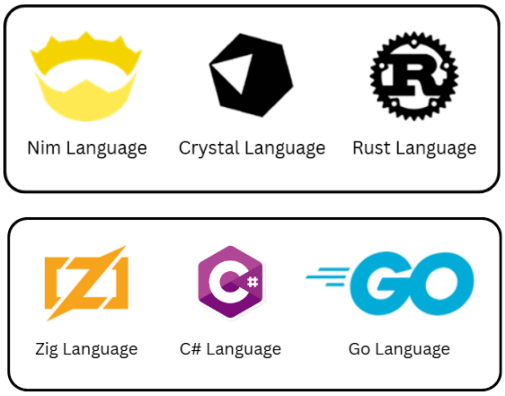
What is DDoD?

The campaign “vibeware” launched by APT36 shows a shift toward a technique described as “Distributed Denial of Detection” in which threat actors create multiple malware variants. These variants are written in different niche languages, but the core logic of these variants is similar to each other. These variants are then deployed simultaneously through a wide range of legitimate platforms including cloud services, messaging applications and productivity tools that create a distributed attack surface.

So, instead of creating a single malware, attackers are creating multiple malware variants to ensure that when one of the paths is detected and blocked, others remain active.

APT36: Vibeware

APT36 introduced a new campaign called as “vibeware” in which they used an AI-driven development model that produces a large number of implants or variants that are written in multiple languages.



This is critical as instead of a critical payload, they generate dozens of variants that are slightly different from one another. Their core logic is same, but languages and structures are different. These are polyglot malwares which can be used to flood target's environment with the disposable polyglot binaries.

So, this campaign can be called as Distributed Denial of Detection (DDoD) as it will exhaust defenders my sending large volumes of variants.

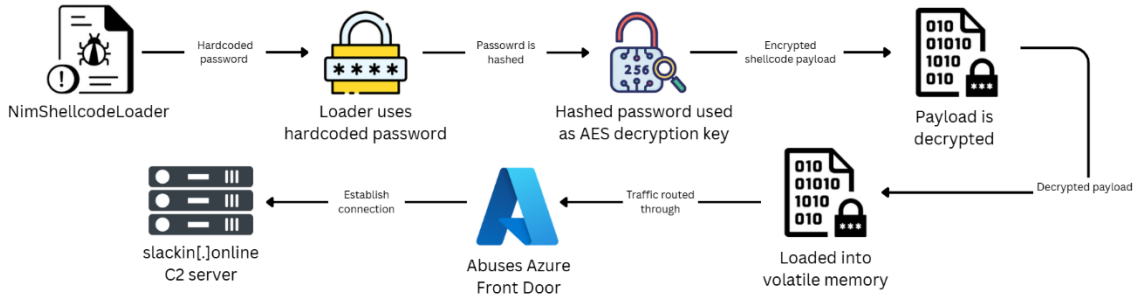
APT36 used a PDF file that tricks the recipient to click on the download button to access the whole PDF.

Trusted Applications Exploited

Microsoft Azure (Azure Front Door)

The **NimShellcodeLoader** is written in Nim language. This variant exploits Azure Front Door which is a trusted Content Delivery Network (CDN). They blend in with legitimate traffic by routing it through Azure Front Door and mask its connection to their C2 server (***slackin[.]online***).

The internal name is ***cobaltdropper.nim*** which is used to deploy a Cobalt Strike beacon and embed it directly in the binary.



1. The NimShellcodeLoader is executed on the victim system. It contains embedded, encrypted shellcode payload (Cobalt Strike beacon).

2. The loader uses a hardcoded password (***Pun7sh3r@123***) which is hashed using SHA-256.

3. The resulting hash is used as AES decryption key.

4. The encrypted payload (encrypted using AES in CBC mode) is decrypted using AES key.

5. The decrypted payload is loaded directly into the memory.

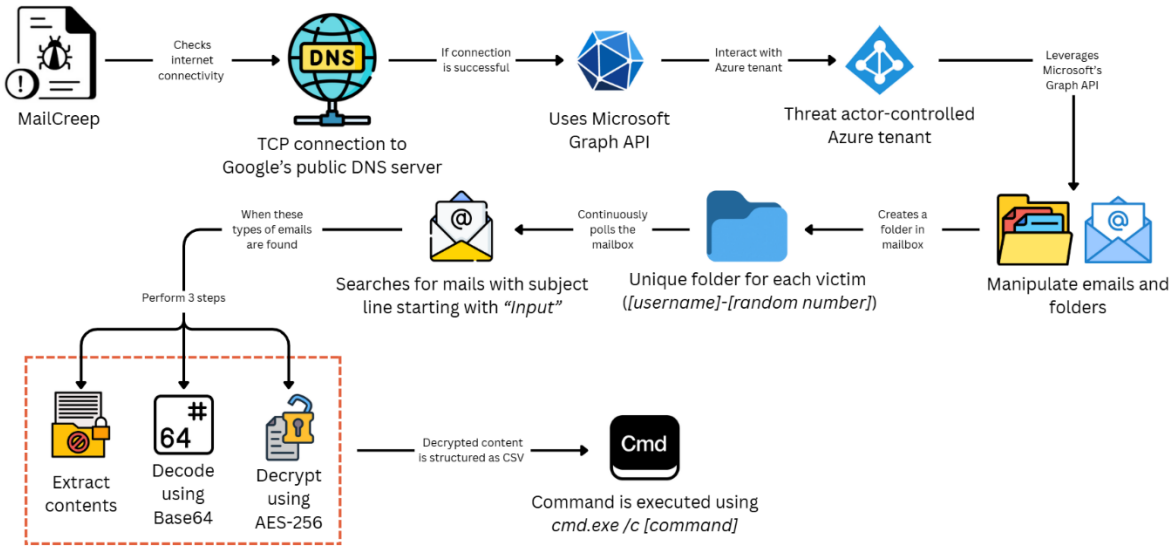
6. The beacon establishes connection with its C2 server: slackin[.]online.

7. Instead of establishing a direct connection, the traffic is routed through Azure Front Door (a trusted CDN) and communication is hidden within legitimate traffic.

Microsoft (Microsoft Graph / Microsoft 365)

The attacker leverages Microsoft's cloud ecosystem through the **MailCreep** module which utilizes the Microsoft Graph API for communication and data operations. It is

written in Go language and attackers blend into normal enterprise traffic by embedding C2 functionality within legitimate API calls.



1. MailCreep initiates a network connectivity check by attempting a TCP Connection to Google Public DNS (8.8.8.8, port 53).

2. If connection is successful, it leverages Microsoft Graph API to interact with threat actor-controlled Azure tenant and manipulate emails and folders.

3. MailCreep creates a unique folder in mailbox for each victim (format – *[username] - [random number]*).

4. Continuously polls the mailbox to search for mails starting with "Input" in subject line.

5. Once a mail is identified, it will extract:
   - Email contents
   - Decode it using Base64
   - Decrypt it using AES-256 in CBC mode

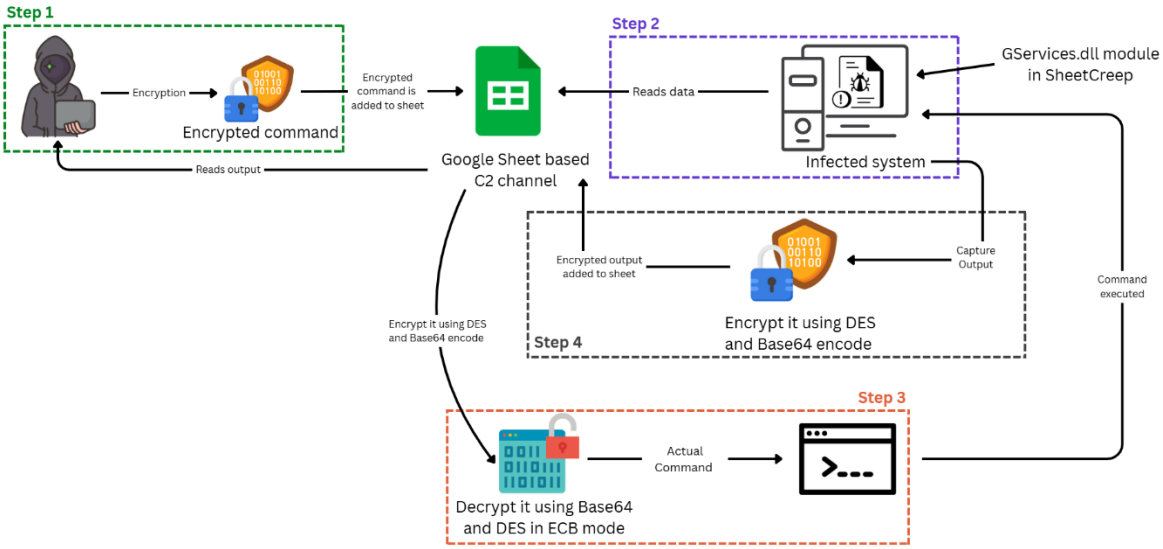
6. The result is parsed as CSV.

7. Parsed commands are executed on victim using *cmd.exe /c [command]*. This allows attackers to run system commands, perform any file operation or execute a payload.

Google Sheets and Google Drive

Google services are heavily abused through multiple components by **SheetCreep** and **LuminousStealer**.

SheetCreep, written in C#, uses Google sheet as a command-and-control channel.



1. The module named GServices.dll uses Google sheet to retrieve commands and upload the output of command making it a bidirectional C2 hub where commands and outputs are exchanged.

2. The attacker encrypts the command and stores encrypted commands in the Google spreadsheet.

3. Gservices.dll module polls specific spreadsheet to enter the data.

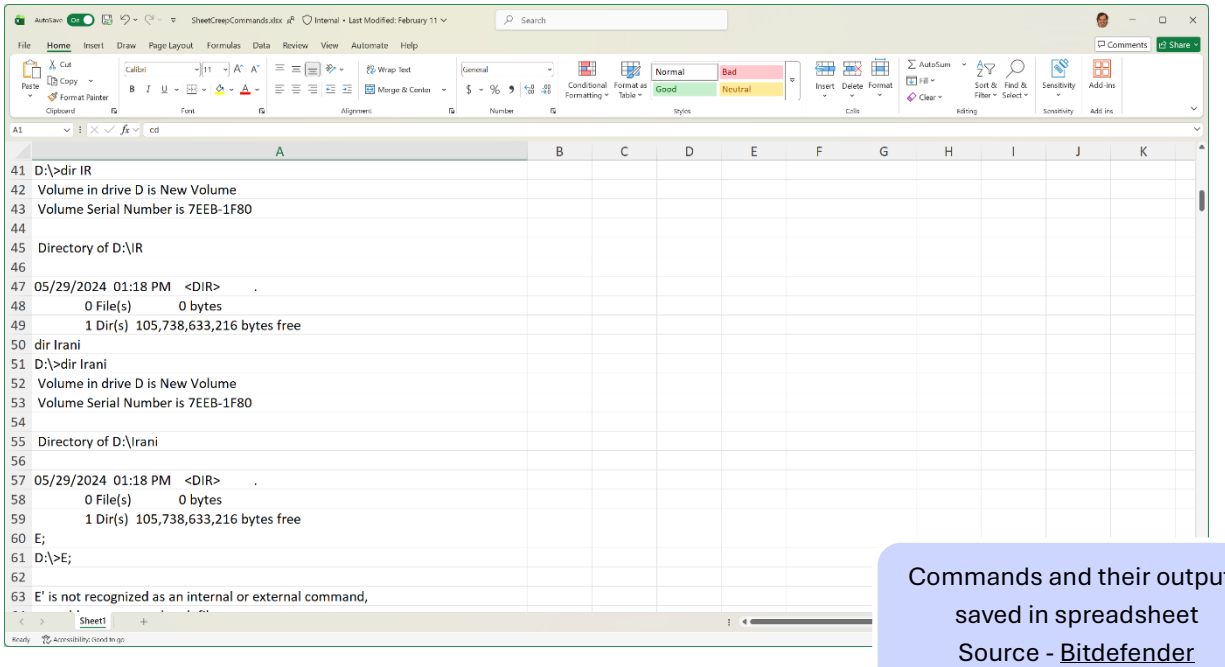
4. Malware fetches the actual command and decrypts it using Base64 and DES in ECB mode.

5. After decryption, the actual command is executed on the victim machine.

6. Malware captures the output and re-encrypts it in DES and Base64.

7. Encrypted output is saved to Google spreadsheet using Google Drive API.

8. Attackers read the output from Google spreadsheet.

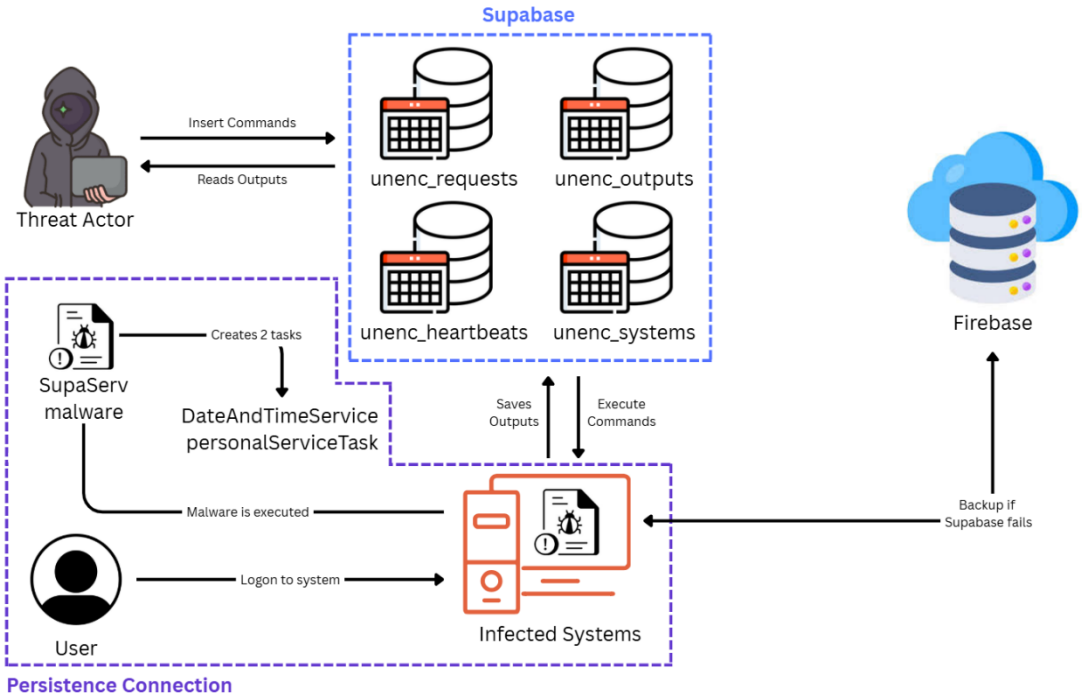


	A
41	D:\>dir IR
42	Volume in drive D is New Volume
43	Volume Serial Number is 7EEB-1F80
44	
45	Directory of D:\IR
46	
47	05/29/2024 01:18 PM <DIR> .
48	0 File(s) 0 bytes
49	1 Dir(s) 105,738,633,216 bytes free
50	dir Irani
51	D:\>dir Irani
52	Volume in drive D is New Volume
53	Volume Serial Number is 7EEB-1F80
54	
55	Directory of D:\Irani
56	
57	05/29/2024 01:18 PM <DIR> .
58	0 File(s) 0 bytes
59	1 Dir(s) 105,738,633,216 bytes free
60	E;
61	D:\>E;
62	
63	E' is not recognized as an internal or external command,

Commands and their outputs saved in spreadsheet
Source - Bitdefender

Supabase

The **SupaServ** malware, written in Rust, uses Supabase as its primary command-and-control infrastructure. It is used to remotely connect to compromised systems.



1. For persistent connection, it uses ITaskService COM interface which creates scheduled tasks triggered at user login.

2. User login to their system.

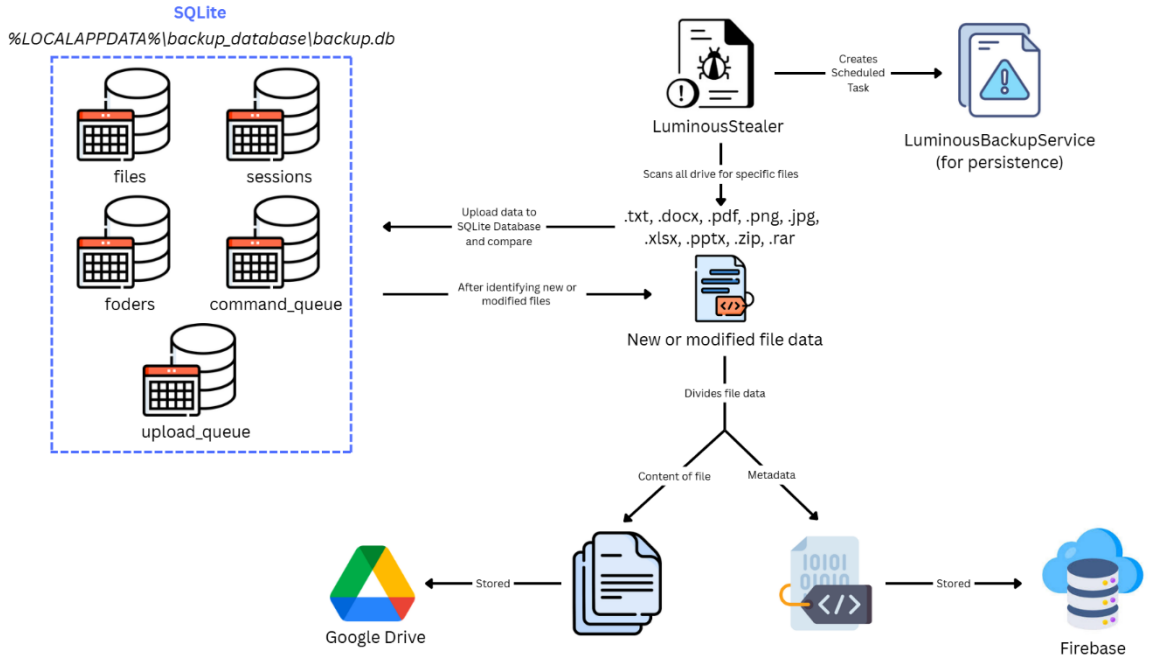
3. SupaServ malware is executed creating two tasks:
    - DateAndTimeService
    - personalServiceTask

4. The malware uses Supabase platform as a primary communication channel. It also uses Firebase cloud platform as a backup C2 infrastructure.

5. Supabase contains four different tables:
    - unenc_requests – Used for polling incoming tasks/commands
    - unenc_outputs – Contains command results
    - unenc_systems – Used to exfiltrate system fingerprint data
    - unenc_heartbeats – Used for session tracking
6. Threat actor inserts commands/tasks in unenc_requests in their Supabase platform.
7. The malware retrieves command and executes it on victim's machine. Then it captures the result and uploads it to unenc_outputs.
8. Attack reads the outputs by accessing the database.

SQLite

The **LuminousStealer** malware, written in Rust, uses SQLite database as its primary command-and-control infrastructure. It scans specific files in the system and uploads data on Google Drive and Firebase.



1. It creates a scheduled task named LuminousBackupService for persistence connection.

2. LuminousStealer uses a local SQLite database (%LOCALAPPDATA%\backup_database\backup.db) on infected host machine.

3. This SQLite database has five tables:
    - files – Catalog of all identified files
    - sessions – Tracks active exfiltrate sessions
    - folders – Directory structure metadata
    - command_queue – Tasks received from C2
    - upload_queue – Files waiting for cloud exfiltration

4. The malware performs recursive scan across all drives to search for files with following extensions - .txt, .docx, .pdf, .png, .jpg, .xlsx, .pptx, .zip, .rar, .doc, and .xls.

5. Stores metadata in SQLite database and compares it with existing records. Only data of new or modified files is sent further.

6. The following data is divided into metadata and content of file.
    - Metadata (names, hashes, etc.) is stored in Firebase.
    - File content (Browser profiles, wallets, etc.) is stored in Google Drive.

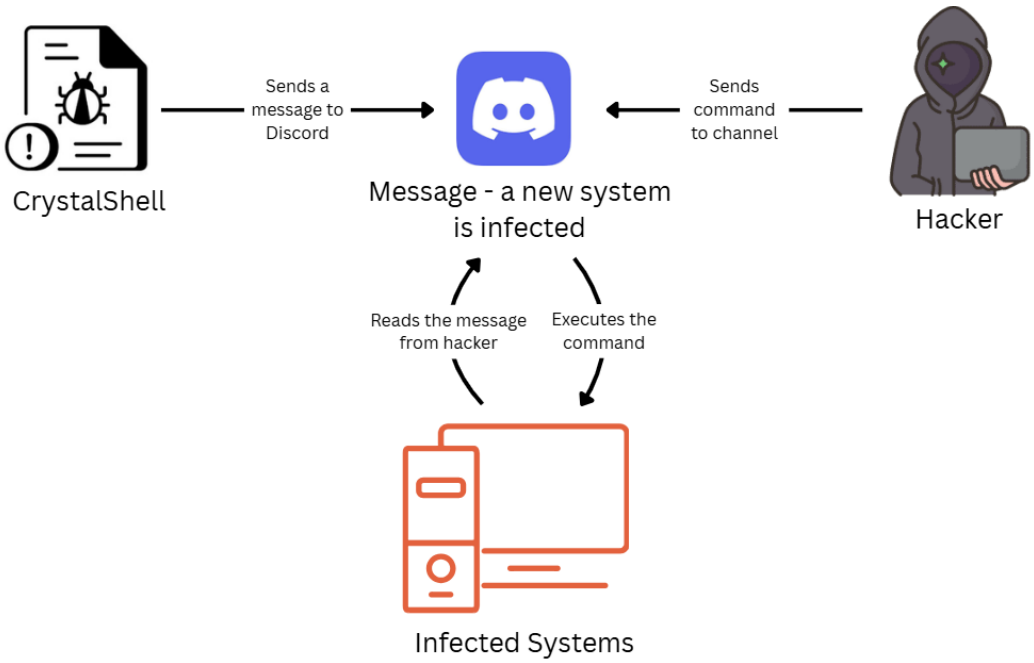
Firebase

Firebase is utilized as both a backup C2 channel and a data exfiltration platform. In the case of **SupaServ**, Firebase acts as a fallback mechanism if primary C2 (Supabase) is not available, ensuring continuity of operation.

Additionally, **LuminousStealer** stores actual content of files in Firebase, distributing exfiltrated data across services to avoid centralized detection.

Discord

The **CrystalShell** backdoor, developed in Crystal language, primarily leverages Discord as its command-and-control (C2) channel and is used for cross-platform deployment. This sample was identified between late December 2025 and late January 2026.



1. Once CrystalShell is executed on victim machine, it initializes its Discord communication module.

2. It connects to a hardcoded Discord channel ID which is controlled by attacker. Malware announces that a new system is infected using format - ***Users:/***

3. The attacker will send commands to the discord channel. CrystalShell verifies if it is from attacker or not by validating discord ID.
    - Authorized user – Accept and execute the command
    - Unauthorized user – Bot responds “You are not authorized”

4. The commands sent by the attacker are Base64-encoded. After decoding, malware processes command in two categories:
    - Built-in Commands
        - These are managed internally by malware:
            - **Format:** *! en (command)*
    - System Commands
        - Other commands not recognized as a built-in command are executed via:
            - **Linux:** */bin/sh -c [command]*
            - **Windows:** *cmd.exe /c > %TEMP%\<8-random-chars>cr_shell_output 2>&1*

5. After executing commands, results are captured and encoded in Base64 format and are sent back to discord.
    - Results from built-in commands are returned as **base64()**.
    - Results from system commands are returned as **!base64()**.

It also has a transition layer that converts Linux command to Windows commands:

- ls – dir
- pwd – cd
- mv - move

Slack

The **ZigShell** backdoor, developed in Zig language, is believed to be the counterpart of CrystalShell which uses slack as its command-and-control (C2) infrastructure. Communication protocol remains same as Crystal Shell, only platform changes from Discord to Slack.

Command prefix format:

- **CrystalShell:** ! en [command]
- **ZigShell:** ! [command]

Commands in ZigShell:

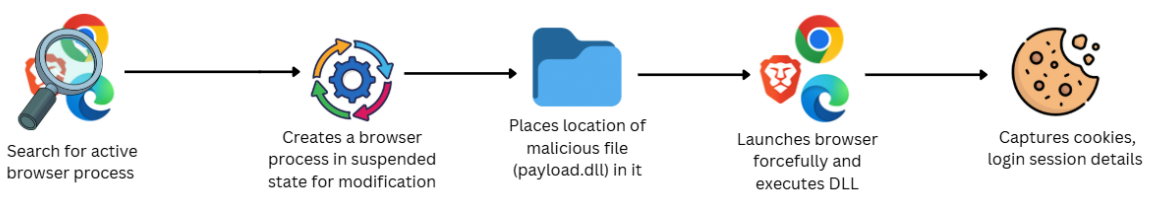
send – Upload files or move them to Slack channel. Command - *Usage: send*.

drop – Download files or pull from slack to user machine. Command - *Usage: drop*.

get – Command that supports both uploading and downloading of files from Slack and user machine. Command - *Usage: get*.

Chromium-Based Browsers

The **LuminousCookies** module, written in Rust, targets Chromium-Based browsers to extract sensitive data such as cookies and other credentials. It aims to bypass App-Bound Encryption (ABE) which is a security mechanism designed to protect browser-stored secrets.



1. Direct access to protected cookies is initially blocked by operating system. To overcome this, the malware performs DLL injection.

2. The injector scans for active Chromium-based browser processes
    - Google Chrome
    - Microsoft Edge
    - Brave

3. Once target is identified, the injector prepares for DLL injection. It launches a new browser process in suspended state.

4. It uses:
    - **VirtualAllocEx** to allocate memory inside target browser.
    - **WriteProcessMemory** to write path of payload.dll into allocated memory.

5. Then it triggers DLL Injection that resolves the address of **LoadLibrary** from kernel32.dll.

6. Executes **CreateRemoteThread** which forces target browser process to load payload.dll.

7. The malicious DLL is now running inside browser process. The injector then creates a named pipe for communication. It then extracts and decrypts the captured data and sends it back through the pipe.

This is how LuminousCookies shows highly effective process injection techniques.

Windows Shortcuts and Persistence Mechanism

The Gate Sentinel Beacon is a customized variant of GateSentinel project that contains a Go-based server and C-based client. In this campaign, attackers weaponize legitimate Windows shortcuts (.lnk) files to achieve stealthy execution.

Shortcuts modified were:

- **Google Chrome**: Desktop\Google Chrome.lnk
- **Microsoft Edge (Public)**: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Edge.lnk
- **Microsoft Edge:** C:\Users\%USERNAME%\AppData\Roaming\Microsoft\
    - **User**: Windows\Start Menu\Programs\Microsoft Edge.lnk

- **User-Pinned Taskbar**: Internet Explorer\Quick Launch\User Pinned\TaskBar\Microsoft Edge.lnk
- **OS-Pinned Taskbar**: Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts*\Microsoft Edge.lnk

File indicators

LuminousCookies

MD5	0fbb0143272c325f4b540819a84826b5
SHA256	194e3059c90e1790748e8a855f328bc28f4ff450e48bc24719f729ada0c8a816
Malware	LuminousCookies
Filename	7ulswlt.exe
File Type	Win32 EXE
Description	LuminousCookies Injector

MD5	2e75e109184a7f6473258bf00440bfd0
SHA256	20308d881eaaef3cfe9672fe98aebda22a7eb520da298a1aaab89111bd9ee526
Malware	LuminousCookies
Filename	di06pt.exe
File Type	Win32 EXE
Description	LuminousCookies Injector

SheetCreep

MD5	32277138366754f6e8514bb89ed74741
SHA256	af1c7f1e0a88b0f1650ccb3909be37a91b76427975ded321f419edd97642a1b0
Malware	SheetCreep
Filename	GServices.exe
	2q48onmqo.exe
File Type	Win32 EXE
Description	Malware that uses Google Sheet as C2 hub

MD5	6bed5e271eddf5cb86a5964b8c2f51b6
SHA256	59abb997927e471472a1c487dea0180d11e9c99774bb138ace46771acba9c3d8
Malware	SheetCreep
Filename	Document.zip
Description	Archive containing SheetCreep payload

MD5	87c7d69c6131406afdd0a08e89329d0a
SHA256	b56062033df06738b66c38b3fa2f82a7e8c558336a4790c83c7faad595172167
Filename	details.png
Description	SheetCreep

MD5	556a567a2c5c27a6aa5660e2e6bcce7b
SHA256	bb11bea463ab1b976c3716591f93eccc71c1a2d1c389a371416b140cd8faa6f0
Filename	details.png
Description	SheetCreep

MD5	0729db72ab4ad9b2ac7a82918c744388
SHA256	71794df37a107472e8d0829387741953f9e6c7778519b11f061c79ff6fb0f386
Filename	Proof.png
Description	SheetCreep

MD5	f9a2da8f12179414663a230f11edca20
SHA256	9eebbf8899a1cf4156a872e9b8cde2a8f6ab364b8089550510938405c622cc58
Filename	edge.exe
Description	SheetCreep

MD5	7269779e3fe07b1d96564117461ec75b
SHA256	eea5cb7795d86e4612edcc6f0085d151e1b7a7351646caf26955c2ac35158971
Filename	chrome.exe
Description	SheetCreep dropper launcher

MailCreep

MD5	ed4dd29c57a38f2bb1934acbaeadeeba
SHA256	a97cc81a2f7c05bfc498b71999176c2aeb6e3ad273e48eb1f5c1c5647419c642
Malware	MailCreep
Filename	ds.png
	4hs9mfac.exe
	a97cc81a2f7c05bfc498b71999176c2aeb6e3ad273e48eb1f5c1c5647419c642-dropped.bin
File Type	Win32 DLL
Description	Malware that uses Microsoft Graph API for communication

MD5	5001c32b386cc8346079db7b2629d777
SHA256	61b2b6b61474398a966e26d3b909542450fcab9b6670558cecd6fabc1015bbce
Filename	d.exe
Description	SheetCreep and MailCreep launcher

.NET Dropper

MD5	03141afe5c20d37620c085cdbeb4058b
SHA256	43fb05d9fc179f791b1a2814f7116ee577b6e48f62eee63af039350260d7fe2b
Filename	details.png
File Type	Portable Executable (PE) file
Description	A dropper .NET binary

LNK Files Dropper

MD5	21dacb6cf6da872f1f3c7b6c876a8a92
SHA256	bec00fa5a87195f182511ecc5292a716c79bc74e17bd1138c8fb2f2285df1b46
Filename	AttachmentLetter.LNK
Description	A dropper LNK launcher

Other Hashes

Hash	**Malware**
f465416476bb3838e982da81aa4aee5b	Gate Sentinel Beacon
7804b006084b6f582f2f74ff758d8cee	Gate Sentinel Beacon
ca2edac970d8afed99db4b5cda72a13e	SupaServ
bea885be7d43627211504dc51685db0e	SupaServ
569bb4899de5759c32ea6df661c35d4c	SupaServ
a5f8e394f7098294b2983f7cd7e750c3	CrystalShell Slack
3cf6bc05a246ddb7bf875381a9bdf7d4	CrystalShell Discord
8a1f290595e459cbfb55fa4c3a58ee0b	CrystalShell Discord
41e952209f149525e4be1eea7961b00b	CrystalShell Discord
83d3def856a88bad32d683ead6cf540b	CrystalShell Discord
c9423c4cb3f520ae60fdd1bf4b9e64b4	CrystalShell Discord
f916e6cc69a4e6a2fcbbcc7fe046f383	CrystalShell Discord
913199ea8343ac030f4fe8dcb215a2eb	ZigShell
54380dfde28bb96e5a3a0dadbf9c4cb0	ZigShell

Domain and IPs

hcisupport[.]in	45.56.162[.]192	Payload hosting domain and IP
hcidoc[.]in	193.29.56[.]122	Payload hosting domain and IP
coadelhi[.]in	104.238.61[.]237	Payload hosting domain and IP

23.152.0[.]81	Havoc C2	Used as CobaltStrike and Mythic C2
45.56.162[.]170:8000	Havoc C2	Used as CobaltStrike C2 to download malicious files

Tactic, Technique and Procedures (TTPs)

Tactic	Technique (ID)	Technique (Name)	Procedure/Description
Resource Development	T1583.001	Acquire Infrastructure - Domains	*hciaccounts[.]in* serves initial payload
	T1583.006	Acquire Infrastructure – Web Services	Google Sheet is used as C2 channel, and Firebase URL and Google cloud storage used to host backup
	T1585.003	Establish Accounts – Cloud Accounts	Google Accounts were created to use Google Sheet, Firebase and cloud storage
	T1587.001	Development Capabilities - Malware	Threat actor created multiple malwares
	T1588.007	Obtain Capabilities – Artificial Intelligence	AI was used to code in niche languages
	T1608.001	Stage Capabilities – Upload Malware	ZIP archive was used to deliver malware
Initial Access	T1566.002	Phishing – Spear phishing Link	Phishing PDFs contain download button linked to ZIP archive
Execution	T1059.001	Command and Scripting Interpreter - PowerShell	PowerShell commands were executed using LNK file
	T1059.003	Command and Scripting Interpreter – Windows Command Shell	Malware executes commands using *cmd.exe* process
Execution	T1204.001	User Execution – Malicious Link	User needs to click on download button

	T1204.002	User Execution – Malicious File	User needs to execute an LNK file to start infection chain
Persistence	T1053.005	Scheduled Task / Job – Scheduled Task	A scheduled task was created to execute malware
Defense Evasion	T1140	De-obfuscate / Decode files or Information	LNK file reverses bytes to load a .NET assembly
	T1564.003	Hide Artifacts – Hidden Window	PowerShell command was used to execute payload without visible window
	T1036.008	Masquerading – Masquerade File Type	Initial payload is .NET binary disguised as PNG extension
	T1027.013	Obfuscated Files or Information – Encrypted / Encoded File	Malwares encrypted its configurations
	T1027.015	Obfuscated Files or Information – Compression	Initial payload was delivered as ZIP archive
Collection	T1530	Data from Cloud Storage	Malwares used Firebase and Google Cloud Storage URL to retrieve backup configurations
Command and Control	T1071.001	Application Layer Protocol – Web Protocols	Google Sheet API was used over HTTPS for C2
	T1102.001	Web Services – Dead Drop Resolver	Backup were hosted on legitimate web services such as Firebase and Google Cloud Storage
	T1102.002	Web Services – Bidirectional Communication	Google Sheet was used as a bidirectional C2 channel
	T1573.001	Encrypted Channel – Symmetric Cryptography	Commands that were sent and received from C2 were encrypted
	T1132.001	Data Encoding – Standard Encoding	Malwares encoded the output in Base64
	T1008	Fallback Channels	Firebase was used as backup if primary C2 fails

RANSOMWARE FRAGMENTATION

Overview

March 2026 has been defined by a convergence of geopolitical conflict, accelerating ransomware fragmentation, and mass exploitation of critical infrastructure.

The armed conflict between the United States, Israel, and Iran — initiated on February 28, 2026 — has triggered the most significant surge of retaliatory cyber operations since the Russia-Ukraine conflict that began in 2022. Over **60 hacktivist and state-aligned groups** have conducted operations ranging from DDoS and website defacement to destructive wiper attacks against healthcare, energy, and defense targets across the Middle East and allied nations. The **Stryker Corporation wiper attack**, which is claimed by Iran-linked **Handala Hack,** is affecting 200,000+ devices across 79 offices globally, and stands as the month's most consequential single incident that has prompted a joint CISA/FBI investigation.

Simultaneously, the ransomware ecosystem continues its post-takedown fragmentation: **NightSpire** has emerged as March's most prolific ransomware group, **DragonForce** continues expanding its "cartel" model absorbing displaced affiliates, and **Tengu/Shisa** has launched a formal affiliate program. Ransomware volume is up by **30%+ Year-over-Year**, with over 57 new groups observed since 2025. The **Tycoon 2FA** phishing-as-a-service platform was seized by Europol on March 4 but recovered operational capacity within days, while **LeakBase** — a major stolen credential forum — was permanently dismantled in a 14-country operation.

On the vulnerability front, the **PolyShell** vulnerability in Magento/Adobe Commerce entered mass exploitation on March 19, targeting 56% of vulnerable e-commerce stores globally. **Ivanti EPMM zero-days** (CVE-2026-1281/1340) continue to be chained for unauthenticated RCE against enterprise MDM infrastructure. Google patched **two Chrome zero-days** (CVE-2026-3909/3910) that were exploited in the wild, and CISA issued **Emergency Directive 26-03** for Cisco SD-WAN vulnerabilities.

- **Key Findings:**

  Iran-US-Israel cyber conflict generating 60+ active threat groups; wiper attacks on critical infrastructure of the United States.

  NightSpire, DragonForce cartel, and Tengu/Shisa are leading ransomware landscape shifts.

  PolyShell mass exploitation has affected 56% of vulnerable Magento stores.

  Ivanti EPMM zero-days (CVE-2026-1281/1340) under widespread exploitation.

  Tycoon 2FA takedown by Europol was recovered within days; LeakBase permanently dismantled.

  Bearlyfy deployed custom GenieLocker ransomware against 70+ Russian firms.

  Microsoft March Patch Tuesday: 84 flaws, two publicly disclosed zero-days.

- **Sectors Most Impacted:** Healthcare, Government, E-Commerce, Financial Services, Manufacturing, Energy, Education

Geopolitical Cyber Conflict: The Iran-Israel-US Theater

Conflict Background

On **28 February 2026**, the United States launched **Operation Epic Fury** and Israel launched **Operation Roaring Lion** against Iranian targets. By March 2, Iran's internet connectivity had collapsed to **1-4% availability**, and by March 26 the country had endured **27 consecutive days** of near-total internet blackout. This kinetic-to-cyber spillover has produced the largest coordinated hacktivist mobilization since the early months of the Russia-Ukraine war.

Active Threat Groups

By early March, as the conflict escalated, **60+ individual threat groups** had become active, primarily conducting low-to-medium sophistication operations. The following groups have been attributed to notable activity:

Group	Affiliation	Primary Operations
Handala Hack	MOIS-affiliated (Iran)	Wiper attacks, data exfiltration, death threats targeting diaspora
APT Iran	Pro-Iranian collective	Hack-and-leak operations against Israeli/US entities
Cyber Islamic Resistance	Umbrella collective	DDoS, data wiping, payment system disruption
Dark Storm Team	Pro-Palestinian/Iranian	Large-scale DDoS, ransomware deployment
FAD Team / Fatimiyoun Cyber	Pro-regime (Iran)	Wiper malware, SCADA/PLC targeting
NoName057(16)	Pro-Russian	Israeli infrastructure DDoS
Cardinal	Pro-Russian	IDF network infiltration claims
DieNet	Pro-Iran	Regional DDoS against Gulf state infrastructure
313 Team	Iraqi pro-Iranian	DDoS against Kuwait Armed Forces, MOD
Tarnished Scorpius / INC Ransomware	Criminal RaaS	Opportunistic ransomware during conflict

The Stryker Corporation Attack — Incident of the Month

The Stryker attack represents a significant escalation, an Iran-aligned group successfully deploying a wiper across the global infrastructure of a Fortune 500 healthcare company by compromising a cloud-based device management platform (Microsoft Intune). This attack vector, MDM/UEM compromise enabling mass device wiping, is likely to be replicated by other state-aligned groups and merits urgent attention from organizations relying on centralized endpoint management. CISA subsequently issued guidance flagging rising threats to endpoint management systems across US organizations.

Attribute	Detail
Victim	Stryker Corporation (US medical technology, $18B+ revenue)
Date	March 11, 2026
Threat Actor	Handala Hack (MOIS-affiliated)
Attack Type	Destructive wiper via compromised Microsoft Intune administrative account
Impact	200,000+ devices wiped across 79 global offices; order processing, manufacturing, and shipments disrupted
Data Exfiltrated	50TB claimed by threat actor
Investigation	Joint CISA, FBI, White House NCD, DHA, HHS, and H-ISAC engagement
Motivation	Retaliation for US-Israel strikes; specifically cited Minab school attack

Stryker Corporation Hacked

2026-03-11

We announce to the world that, in retaliation for the brutal attack on the Minab school and in response to ongoing cyber assaults against the infrastructure of the Axis of Resistance, our major cyber operation has been executed with complete success.

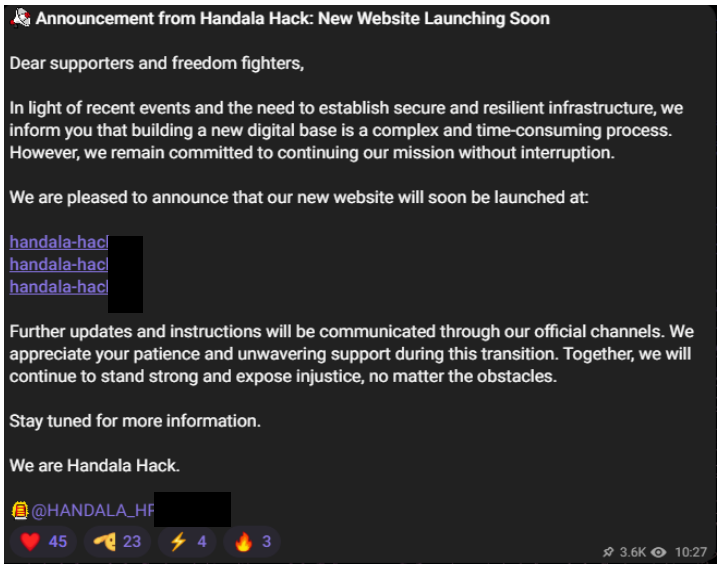
The Zionist-rooted corporation, Stryker, one of the key arms of the global Zionist lobby and a central ring in the 'New Epstein' chain, has been struck with an unprecedented blow. In this operation, over 200,000 systems, servers, and mobile devices have been wiped and 50 terabytes of critical data have been extracted.

Stryker's offices in 79 countries have been forced to shut down. All the acquired data is now in the hands of the free people of the world, ready to be used for the true advancement of humanity and the exposure of injustice and corruption.

A clear warning to all Zionist leaders and their lobbies who hide behind concrete walls and closed windows:
The era of the 'Epstein' rings and the demons of our time is over. 'Nimrod of this era,' even if you close your windows, we will build our nests everywhere. Get ready for the mosquito...

This is only the beginning of a new chapter in cyber warfare. To all those plotting attacks on the infrastructure of the Axis of Resistance:
The era of hit-and-run is over!

PoC soon



Announcement from Handala Hack: New Website Launching Soon

Dear supporters and freedom fighters,

In light of recent events and the need to establish secure and resilient infrastructure, we inform you that building a new digital base is a complex and time-consuming process. However, we remain committed to continuing our mission without interruption.

We are pleased to announce that our new website will soon be launched at:

handala-hacl
handala-hacl
handala-hacl

Further updates and instructions will be communicated through our official channels. We appreciate your patience and unwavering support during this transition. Together, we will continue to stand strong and expose injustice, no matter the obstacles.

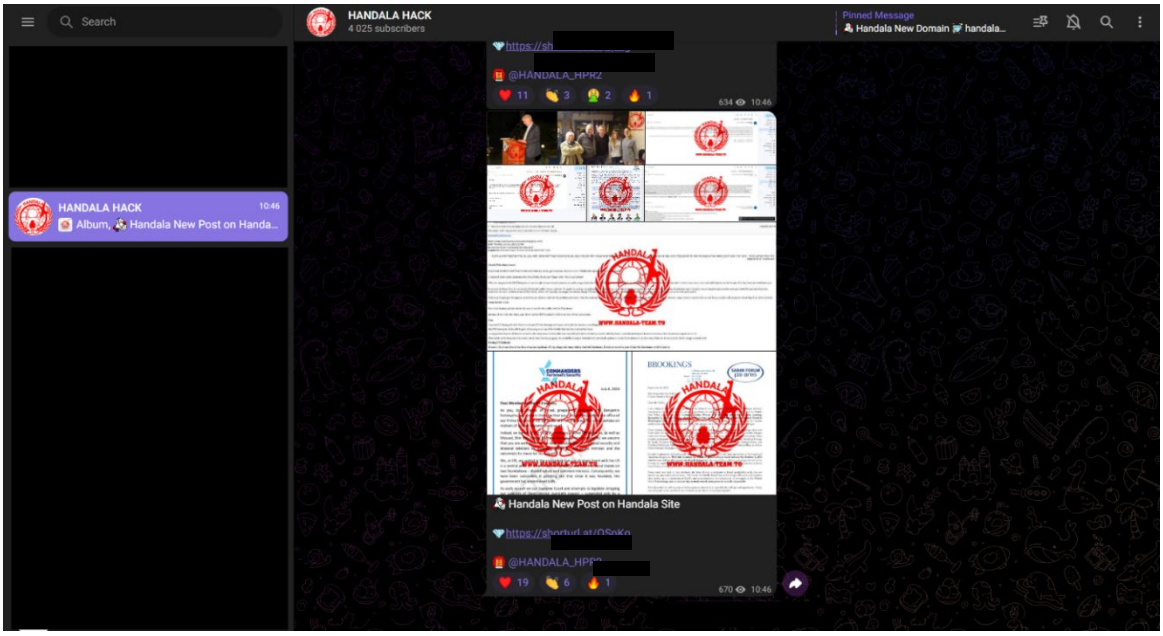
Stay tuned for more information.

We are Handala Hack.

@HANDALA_HP

45 23 4 3

3.6K 10:27



Search

HANDALA HACK
4 025 subscribers

Pinned Message
Handala New Domain handala...

HANDALA HACK 10:46
Album, Handala New Post on Handa...

Handala New Post on Handala Site

Operational Tradecraft Observed

Phishing infrastructure: 7,381 conflict-themed phishing URLs identified from the open-source feeds and Threat Hunting, exploiting humanitarian concern and geopolitical anxiety.

Mobile malware: Malicious RedAlert APK delivering surveillance and data exfiltration capabilities.

Infostealer campaigns: StealC deployed via password-protected ZIPs and JavaScript redirects.

Domain infrastructure: Numbered-increment domain patterns, subdomain chaining, CDN-CGI path exploitation to bypass email security.

Financial fraud: Cryptocurrency donation scams, fake humanitarian aid schemes, fake e-commerce storefronts.

Wiper deployment: Cloud MDM compromise (Intune) enabling mass device destruction without traditional lateral movement.

Impact Assessment

The sustained internet blackout in Iran has **likely degraded** the coordination capacity of Iran's most sophisticated state-sponsored threat actors, but geographically dispersed operatives and proxy groups continue to escalate. As also discovered by Unit 42's recent assessment, Wiper attacks remain the most concerning capability in Iran's offensive toolkit, given a history dating to the 2012 Shamoon campaign. The formation of an "Electronic Operations Room" on February 28 to coordinate cyber retaliation represents formalized operational structure.

Ransomware Landscape — March 2026

Impact Assessment

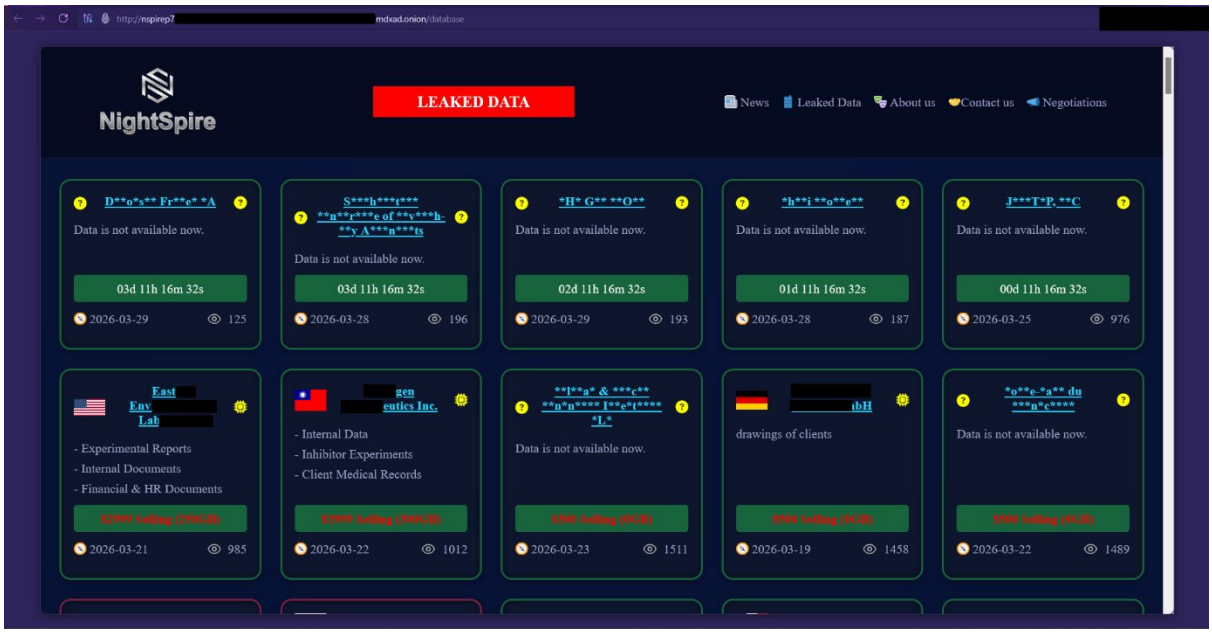
Ransomware attacks have surged **30%+ Year-over-Year** as of Q1 2026 (mentioned in weekly report which contains the investigation on Qilin Ransomware group), projecting total incidents could exceed **12,000 globally** if current momentum continues. The landscape is defined by **fragmentation** — the successful takedowns of LockBit, Hive, and ALPHV/BlackCat in 2024-2025 did not reduce overall volume but instead accelerated the proliferation of smaller, more agile groups.

Metric	Status
YoY attack increase	30%+ (sustained over 4 consecutive months)
New groups (2025)	57 ransomware groups + 27 extortion-only groups
Projected 2026 total	12,000+ incidents if same pace continues
Most active group (March)	NightSpire
2nd most active group (March)	Qilin
Cartel model leader	DragonForce

Notable Groups — March 2026

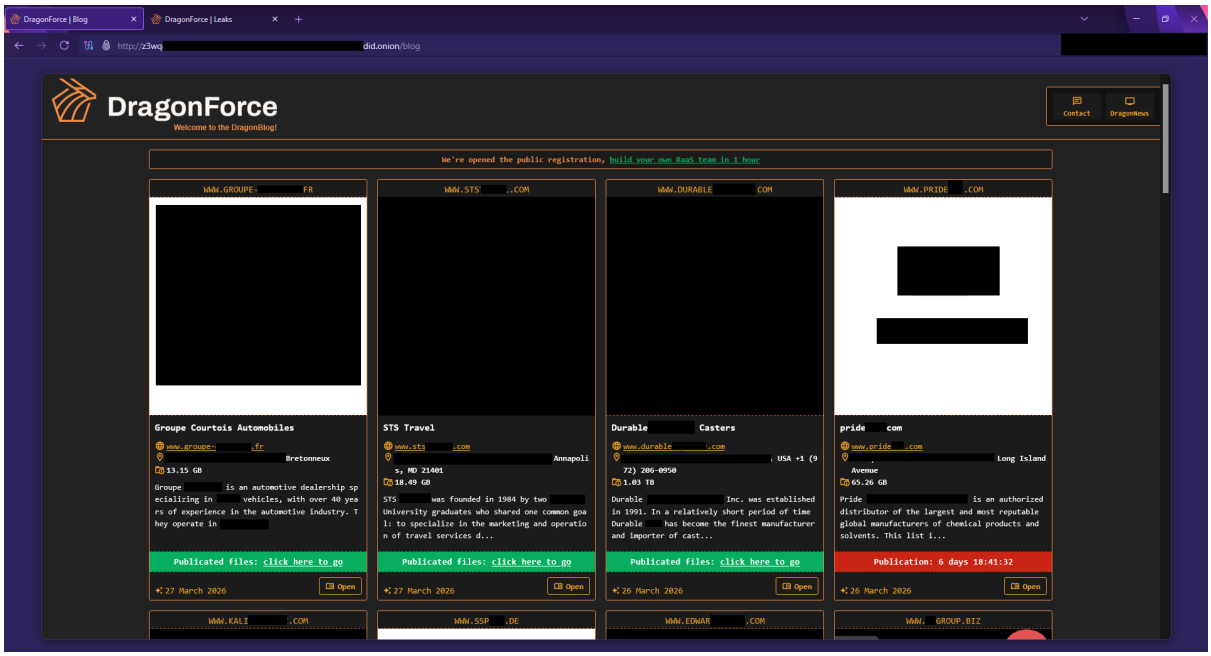
NightSpire — Most Active Group

NightSpire has emerged as March 2026's most prolific ransomware operator, surpassing Qilin and DragonForce in victim volume. Originally operating as an exfiltration-only extortion group since March 2025, NightSpire evolved to full double extortion (encryption + data theft) in late 2025. Primarily targeting, professional services and healthcare, concentrated in the United States and France.



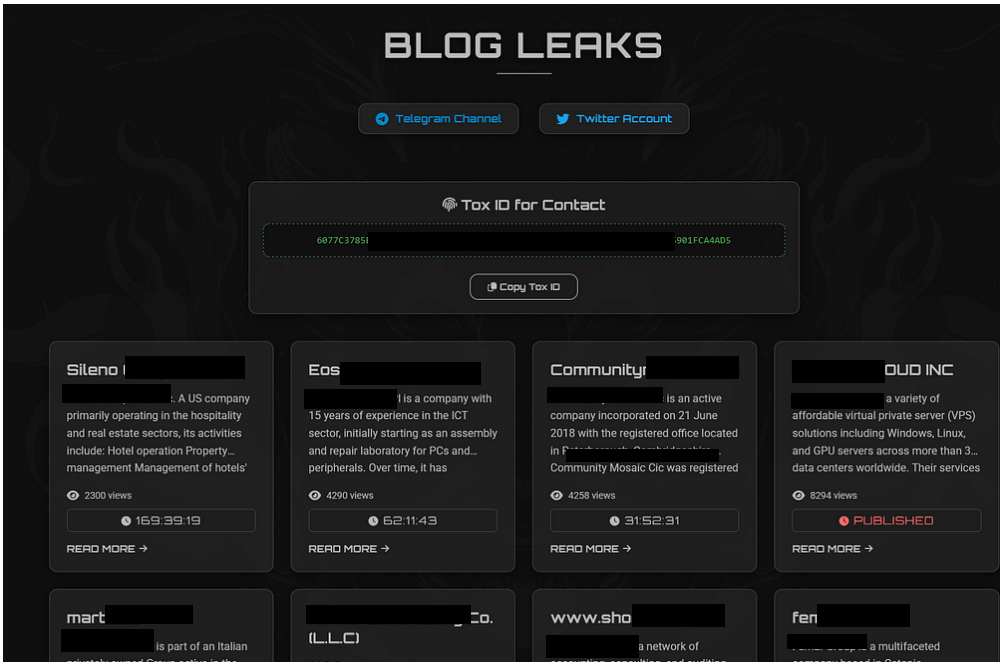
DragonForce — Cartel Model Expansion

DragonForce continues to consolidate its position as the ransomware ecosystem's most ambitious organizational model. Operating as a "cartel" since March 2025, the group allows affiliates to white-label payloads and create branded variants (Devman, Mamona/Global). Following the collapse of RansomHub in April 2025, DragonForce actively recruited displaced affiliates and now offers petabytes of storage, 24/7 server monitoring, and dry-run testing support. The 80/20 revenue split mirrors emerging industry standard.



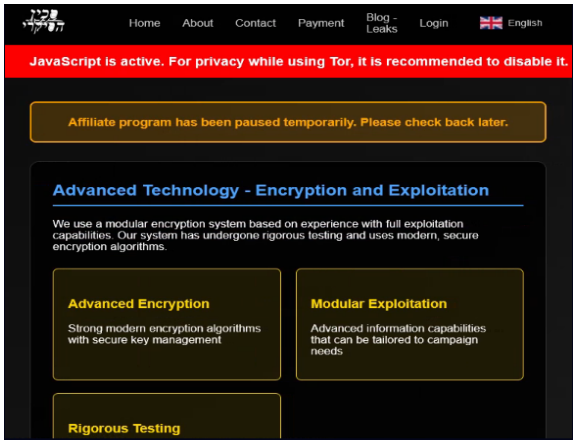
Tengu/Shisa — Formal RaaS Launch

Tengu formally launched its affiliate program in March 2026 with an 80/20 split, concurrent with a partial rebranding to "Shisa Ransomware." Internal affiliate panel documentation (in English and Russian) revealed a 4-tier encryption strategy system and a dedicated ESXi locker with VMware security bypass capabilities. A total of over 52 victims, to date across 20+ countries have been identified.



Sicarii — The Ransomware That Cannot Decrypt

Sicarii, which surfaced in December 2025, carries a critical flaw: its encryption process discards decryption keys, making data recovery **permanently impossible** regardless of ransom payment. Despite limited victim numbers to date, the group has publicly signaled intent to dramatically expand targeting volume — making Sicarii a uniquely destructive threat where payment provides zero recovery guarantee. Check Point Research has published a detailed analysis confirming the irrecoverable nature of the encryption.



Sicarii DLS

Logo of Sicarii group

Bearlyfy / Labubu — Pro-Ukraine GenieLocker Campaign

The pro-Ukrainian threat group Bearlyfy (also tracked as Labubu) has escalated from low-sophistication attacks on small Russian businesses to deploying a custom ransomware family called **GenieLocker** against 70+ Russian firms since January 2025. The shift to proprietary ransomware (with encryption inspired by the Venus/Trinity families) and ransom demands now reaching hundreds of thousands of dollars represent significant operational maturation. The infrastructure also overlaps with PhantomCore, another pro-Ukraine group targeting Russian and Belarusian entities.

Ransomware Trends Assessment

Post-takedown fragmentation is permanent. The disruption of major brands (LockBit, ALPHV, Hive) has been offset by dozens of smaller operations inheriting proven playbooks and affiliate talent.

Cartel models are ascending. DragonForce's white-label approach, enabling affiliates to operate under their own branding while leveraging shared infrastructure, is likely to become the dominant organizational paradigm.

Geopolitically motivated ransomware is growing. Bearlyfy (pro-Ukraine) and Tarnished Scorpius/INC (Iran-aligned opportunism) illustrate the blurring of ideological and financial motivations.

Destructive variants pose existential data risk. Sicarii's key-destruction flaw — whether intentional or accidental — means victims face permanent data loss regardless of payment.

Critical Vulnerabilities & Mass Exploitation

Actively Exploited Vulnerabilities — March 2026

CVE	Product	Type	CVSS	Exploitation Status	Impact
PolyShell (APSB25-94)	Magento/ Adobe Commerce	Unauthenticated file upload → RCE	Critical	Mass exploitation since March 19; 56% of vulnerable stores compromised	Web shell deployment, payment skimming, full server compromise
CVE-2026-1281	Ivanti EPMM	Code injection → RCE	9.8	Widespread; CISA KEV listed	Unauthenticated RCE against MDM infrastructure
CVE-2026-1340	Ivanti EPMM	Code injection → RCE	9.8	Chained with CVE-2026-1281	Full enterprise mobile fleet compromise
CVE-2026-3909	Google Chrome (Skia)	OOB Write	8.8	In the wild (March 10)	Browser-based RCE
CVE-2026-3910	Google Chrome (V8)	Inappropriate implementation	8.8	In the wild (March 10)	JavaScript engine exploitation
CVE-2026-2441	Google Chrome / Chromium	RCE via malicious web content	High	In the wild (pre-patch)	Arbitrary code execution
CVE-2026-1731	BeyondTrust Remote Support	Pre-auth OS command injection	Critical	Active in ransomware campaigns (Feb 13+)	Unauthenticated RCE; CISA 3-day federal mandate
CVE-2026-22719	VMware Aria Operations	Command injection	8.1	Unauthenticated RCE during migration	CISA remediation deadline: March 24
CVE-2026-21262	Microsoft SQL Server	Privilege escalation	—	Publicly disclosed (zero-day)	Local privilege escalation to sysadmin
CVE-2026-26127	Microsoft .NET	Denial of Service	—	Publicly disclosed (zero-day)	Remote application crash
CVE-2026-20127	Cisco SD-WAN	Admin access bypass	Critical	Exploited since 2023; CISA ED 26-03	Administrative access to SD-WAN controllers

PolyShell — Mass Exploitation Event of the Month

The PolyShell vulnerability in Magento Open Source and Adobe Commerce represents March 2026's most significant mass exploitation event. The flaw enables unauthenticated attackers to upload polyglot files, valid images that embed executable PHP code, to Magento servers via the REST API's cart item file upload feature. Once uploaded, these payloads function as web shells enabling arbitrary code execution.

Exploitation Timeline:

- **March 10:** Adobe released a fix in Magento 2.4.9-beta1 (pre-release only — no stable branch patch)
- **March 16:** First observed exploitation in the wild
- **March 19:** Automated mass scanning began; 50+ IP addresses participating
- **March 25:** 56.7% of all vulnerable stores confirmed compromised

Analyst Assessment: The gap between the pre-release patch (March 10) and mass exploitation (March 19), with no stable-branch patch available, created a critical window where defenders had awareness but no viable remediation path for production systems. This pattern of pre-release-only fixes is likely to be exploited by threat actors monitoring vendor pre-release channels. Organizations running Magento should treat this as an emergency.

Microsoft March Patch Tuesday

Microsoft's March 2026 Patch Tuesday addressed **84 vulnerabilities** including two publicly disclosed zero-days (CVE-2026-21262 and CVE-2026-26127) and three critical-rated flaws. Notably, **no vulnerabilities were confirmed as actively exploited** at time of release, the first month without in-the-wild exploitation in six months, a welcome reprieve from February's six actively exploited zero-days.

CISA Emergency Directive 26-03

CISA issued **Emergency Directive 26-03** requiring federal agencies to inventory Cisco SD-WAN systems, apply mitigations, and assess for compromise related to CVE-2026-20127 (exploited since 2023) and CVE-2022-20775. Additionally, CISA published a **Cyber Vulnerability Insights Estimate (CVIE)** cataloguing **136 CVEs** that Iranian government-sponsored actors have targeted, with over **3,100 US critical infrastructure entities** confirmed exposed.

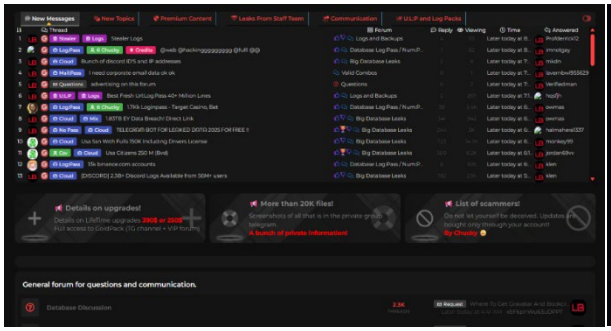
Law Enforcement & Disruption Operations

Operation Leak — LeakBase Takedown (March 3-4, 2026)

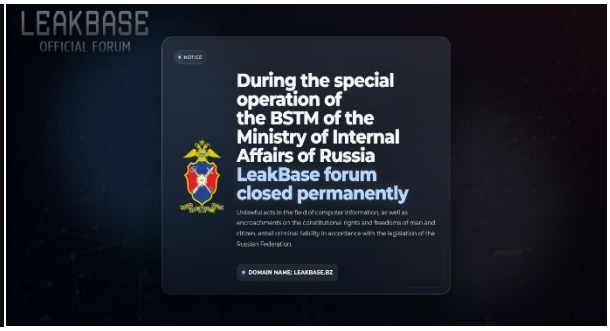
Attribute	Detail
Operation Name	Operation Leak
Target	LeakBase — open-web cybercrime forum for stolen credentials and stealer logs
Date	March 3-4, 2026 (two-phase operation)
Lead Agencies	FBI, Europol, BSTM
Countries Involved	14 (US, Australia, Belgium, Poland, Portugal, Romania, Spain, UK, and 6 others)
Forum Statistics	142,000+ registered users, 32,000+ posts, 215,000+ private messages
Actions	37 most active users targeted; ~100 enforcement actions; full forum data seized
Outcome	Forum permanently shut down; all user accounts, private messages, IP logs, and credit card details preserved for prosecution

Phase 1 (March 3): **Coordinated arrests, house searches, and doorstep interviews across multiple jurisdictions targeting the platform's most active users.** Phase 2 (March 4): Technical disruption — domain seizure and infrastructure takedown.

Russia subsequently arrested the suspected owner and administrator of LeakBase, representing notable cross-jurisdictional cooperation.



Before Seizure

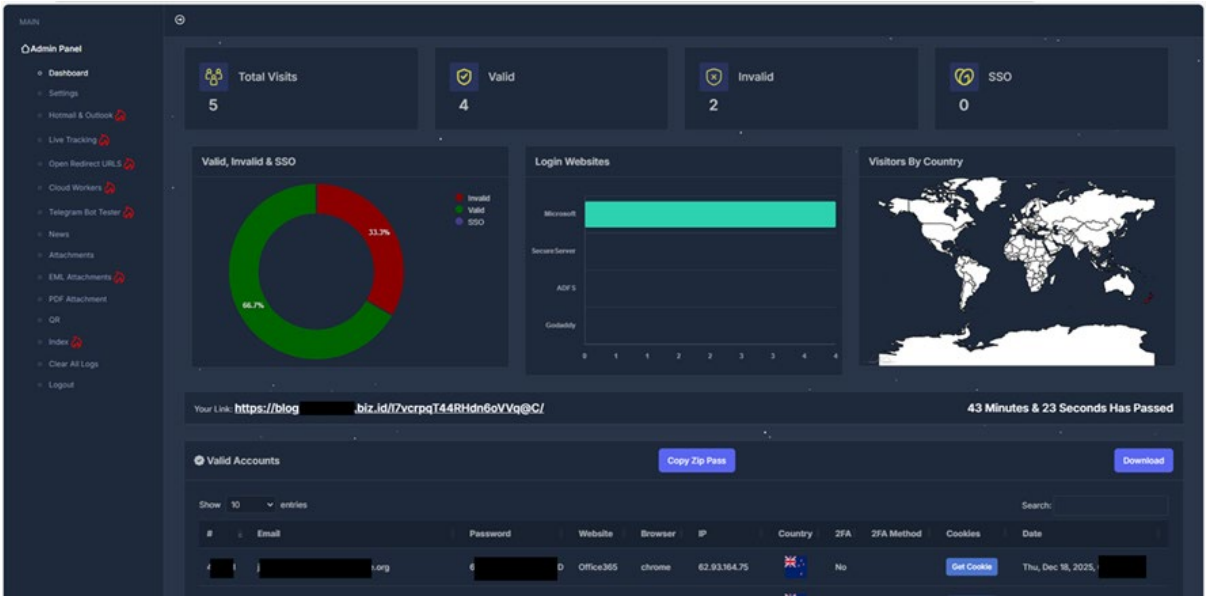


Post Seizure

Tycoon 2FA Disruption (March 4, 2026)

Attribute	Detail
Target	Tycoon 2FA — phishing-as-a-service (PhaaS) platform

Date	March 4, 2026
Lead Agency	Europol, with Microsoft, Trend Micro, and industry partners
Countries	6 (Latvia, Lithuania, Portugal, Poland, Spain, UK)
Infrastructure Seized	330 control panel domains
Platform Statistics	62% of all phishing attempts blocked by Microsoft; 3M+ messages/month; 96,000+ victims; 55,000+ Microsoft customers compromised
MFA Bypass Rate	59% of compromised accounts had MFA enabled
Recovery	Platform returned to pre-disruption activity levels within days



Tycoon's Custom Admin Dashboard

The Tycoon 2FA takedown, while operationally impressive in scale (330 domains), proved **tactically ephemeral**. CrowdStrike observed activity drop to 25% of baseline on March 4-5 before recovering fully within a week, with no meaningful changes in TTPs. This outcome illustrates the fundamental resilience of PhaaS infrastructure and the challenge of permanently disrupting cloud-native criminal platforms. The 59% MFA bypass rate is a critical statistic: it demonstrates that traditional MFA alone is no longer a sufficient defense against adversary-in-the-middle (AiTM) phishing.

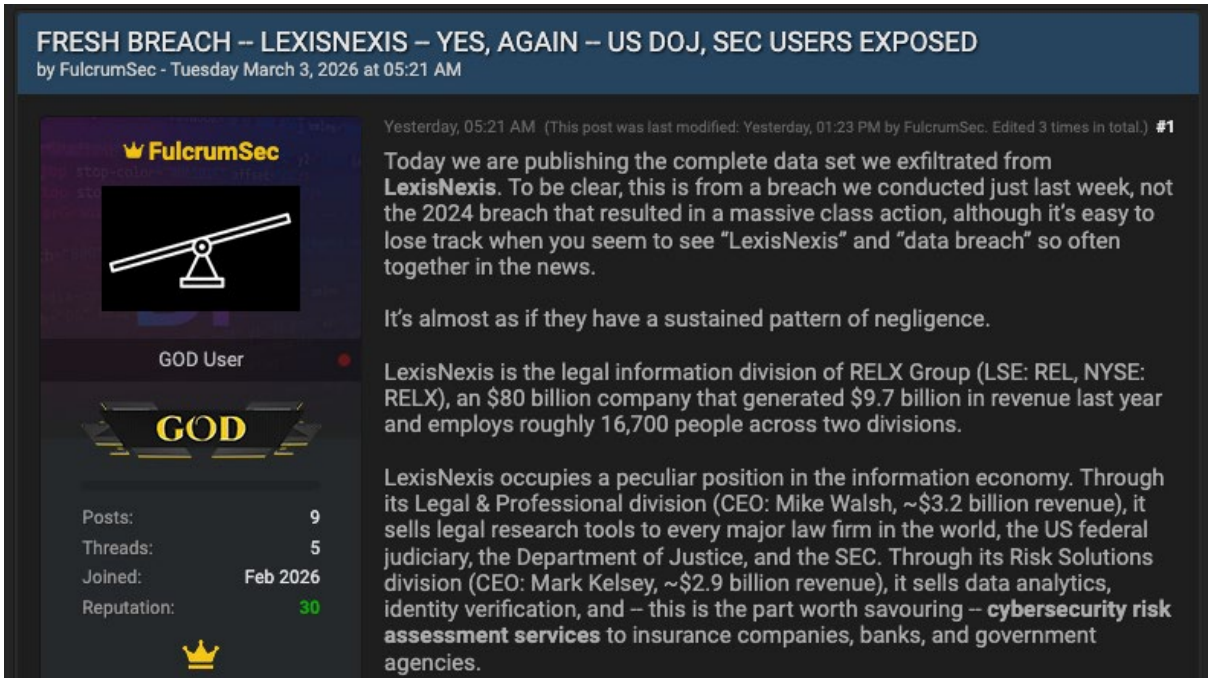
Assessment

March 2026 saw two of the most significant law enforcement operations in recent months targeting different layers of the cybercrime stack — credential markets (LeakBase) and phishing infrastructure (Tycoon 2FA). While LeakBase appears permanently disrupted with arrests and data seizure, Tycoon 2FA's rapid recovery underscores the persistent challenge of disrupting service-based criminal platforms that can reconstitute infrastructure faster than law enforcement can take down.

Supply Chain & Cloud Infrastructure Threats

LexisNexis AWS Breach (Disclosed March 3-4, 2026)

A threat actor tracked as **FulcrumSec** exploited the React2Shell vulnerability (CVE-2025-55182) in an unpatched React frontend application to compromise LexisNexis Legal & Professional's AWS infrastructure on approximately 24 February 2026. The breach was publicly disclosed on March 3-4.



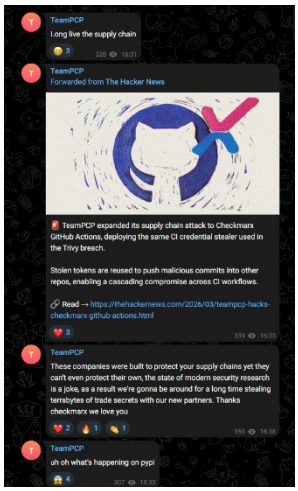
Data Exfiltrated:

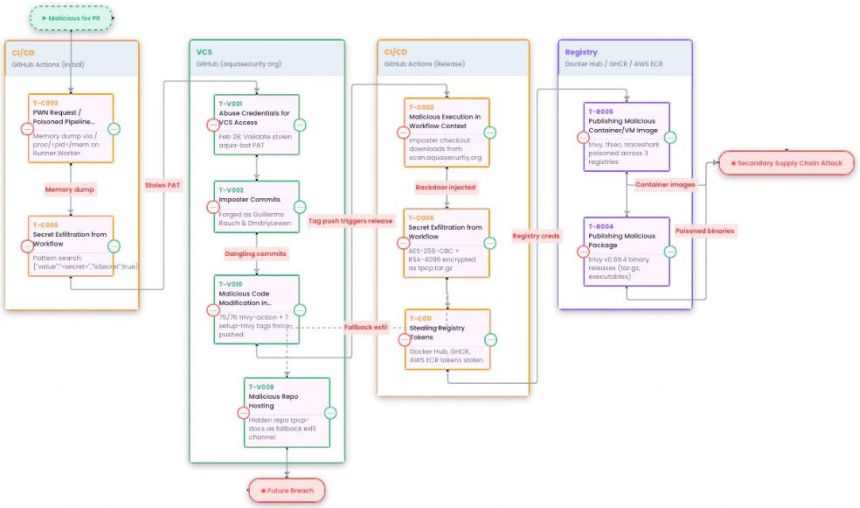
- 2.04 GB of structured data
- 536 Redshift tables, 430+ VPC database tables
- 53 plaintext AWS Secrets Manager secrets
- 3.9 million database records
- 21,042 customer accounts
- 118 users with .gov email addresses (federal judges, DOJ attorneys, SEC staff)
- Complete VPC infrastructure map

The LexisNexis breach is significant for three reasons: (1) it demonstrates continued exploitation of React2Shell (CVE-2025-55182) against major enterprise targets, months after patch availability; (2) the exfiltration of AWS Secrets Manager secrets in plaintext indicates poor secrets management hygiene in a Fortune 500 environment; (3) the exposure of US government employee data from a legal research platform creates potential downstream intelligence value for state actors.

Trivy Security Scanner Supply Chain Compromise

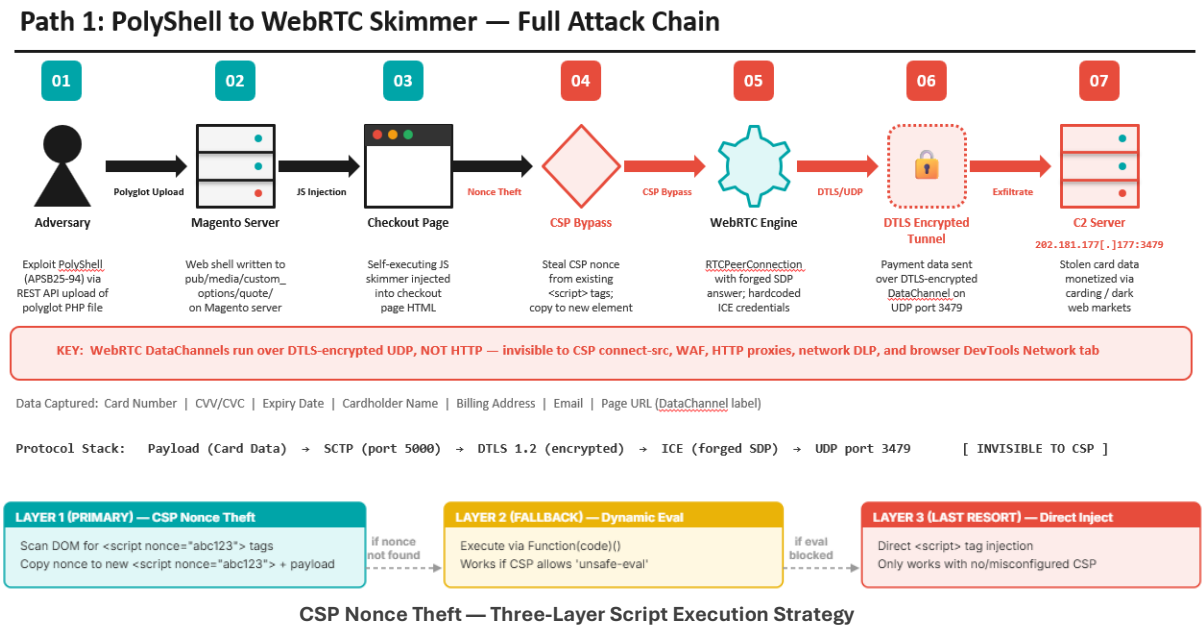
Trivy, a widely used open-source vulnerability scanner maintained by Aqua Security, was compromised for the **second time within a month** in March 2026 by a Threat Actor named '**Team PCP**'. The malware injected into the compromised scanner was capable of stealing sensitive CI/CD pipeline secrets. This double compromise of a security tool is particularly insidious as organizations relying on Trivy to detect vulnerabilities were instead introducing malware into their own built pipelines. Here you can know more about the security incident.





WebRTC Skimmer — CSP Bypass for Payment Theft

A novel e-commerce attack technique was identified in March 2026 in which threat actors abuse the WebRTC protocol to exfiltrate stolen payment card data, bypassing Content Security Policy (CSP) restrictions that would normally block unauthorized outbound connections. This represents a meaningful evolution in e-commerce skimming TTPs.



CSP Nonce Theft — Three-Layer Script Execution Strategy

Emerging TTPs & Tooling Trends

Email Fuzzing/Dynamic Text Randomization

A significant evolution in phishing evasion was documented in March. Threat actors are now employing **dynamic text randomization** across all email fields including sender aliases, display names, subject lines, and body content and fragmenting campaigns into thousands of low-volume variants that individually fall below detection thresholds. This technique directly undermines clustering-based detection and complaint-based feedback loops that email security platforms rely on.

AiTM Phishing Goes Mainstream

Adversary-in-the-middle phishing, where transparent reverse proxies intercept authenticated sessions in real-time, has moved from a specialized technique to a **commodity service**. Tycoon 2FA's 62% market share of Microsoft-blocked phishing and its 59% success rate against MFA-protected accounts signal that AiTM is now the default approach for credential theft operations on scale.

MDM/UEM as an Attack Vector

The Stryker attack introduced a new operational pattern: compromising a cloud-based Mobile Device Management (MDM) or Unified Endpoint Management (UEM) platform to deploy wipers at scale, bypassing traditional network-based lateral movement entirely. By controlling the MDM administrative console, attackers can push destructive payloads to every enrolled device simultaneously, regardless of geographic location or network segmentation. This TTP is highly likely to be adopted by additional threat groups.

Polyglot File Upload Exploitation

PolyShell's exploitation technique of uploading files that are simultaneously valid images and executable PHP code, represents a resurgence in polyglot file attacks against web applications. The technique exploits server-side trust in file MIME types and extensions while embedding executable payloads that survive content validation checks.

ESXi Targeting Continues to Mature

Multiple ransomware groups (Tengu, NightSpire, DragonForce affiliates) now maintain dedicated ESXi locker variants. Tengu's documented ESXi 8.0 execInstalledOnly bypass (as detailed in CTI-2026-002) demonstrates that operators are actively testing against VMware's latest security hardening controls. The trend toward multi-platform encryptors (Windows + ESXi + Linux) as a standard RaaS feature is now firmly established.

Geopolitically Motivated Ransomware

The Bearlyfy/GenieLocker campaign (pro-Ukraine targeting Russia) and Tarnished Scorpius/INC operations (Iran-aligned targeting Israel) illustrate a growing convergence of ideological motivation and ransomware-as-extortion. These hybrid-motivation groups add unpredictability to the threat landscape as their targeting decisions are influenced by geopolitical events rather than being purely financial optimization.

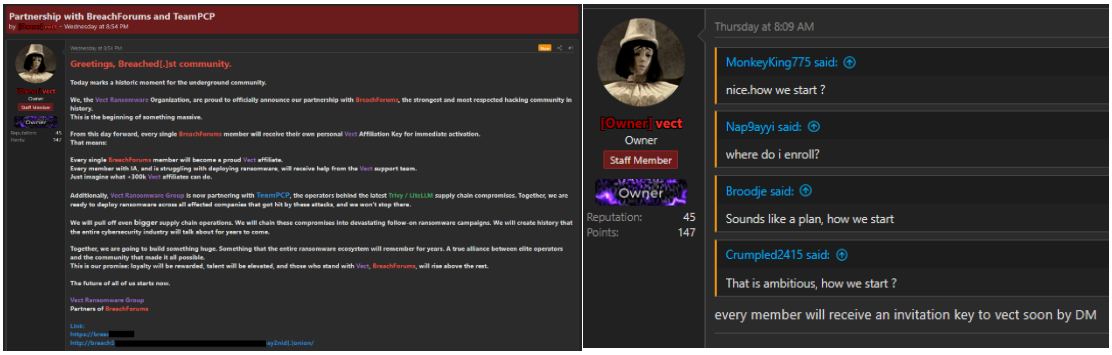
Sector-Specific Threat Assessment

Sector	Threat Level	Key Threats	Notable Incidents
Healthcare	**CRITICAL**	State-sponsored wipers, ransomware, supply chain	Stryker wiper attack (Handala); NightSpire targeting; Israeli healthcare network claimed
Government	**HIGH**	Espionage, credential theft, DDoS, retaliatory ops	LexisNexis .gov data exposure; CISA 136-CVE CVIE for Iranian targeting; Kuwait/Saudi govt DDoS
E-Commerce	**HIGH**	PolyShell mass exploitation, WebRTC skimming	56% of vulnerable Magento stores compromised; payment data theft
Financial Services	**HIGH**	DDoS, phishing, credential theft	Israeli payment infrastructure disrupted; Gulf banking portals targeted
Energy/Critical Infrastructure	**HIGH**	State-aligned sabotage, ICS targeting	Israeli energy exploration; Jordan fuel systems; Saudi critical infra
Technology/SaaS	**ELEVATED**	Supply chain, cloud infrastructure compromise	Trivy scanner double-compromise; LexisNexis AWS breach
Manufacturing	**ELEVATED**	Ransomware, operational disruption	Tengu and NightSpire targeting; Stryker supply chain impact
Education	**ELEVATED**	Phishing, ransomware, credential theft	Tycoon 2FA targeting schools; ransomware incidents
Defence / Military	**ELEVATED**	Espionage, DDoS, hacktivism	IDF network infiltration claims; Iron Dome targeting claims; drone system targeting

Threat Forecast — April 2026

Based on the intelligence acknowledged, the following developments are assessed as **likely to happen or escalate** in the coming weeks:

1. **Iran-aligned cyber retaliation will intensify** as conflict continues and Iranian internet connectivity is gradually restored. More sophisticated operations (beyond DDoS) are probable once state-aligned actors regain coordination capacity.
2. **PolyShell exploitation will escalate** until Adobe releases a stable-branch patch. Magecart-style payment skimming overlays are the most probable monetization path for compromised stores.
3. **Tycoon 2FA and successor PhaaS platforms will continue to proliferate.** The failed disruption demonstrates that AiTM phishing is structurally resilient. Organizations should assume that MFA bypass is now a commodity capability and implement phishing-resistant authentication (FIDO2/passkeys).
4. **Ransomware volume will remain elevated or increase** through Q2 2026. The cartel model (DragonForce) and affiliate model (Tengu/Shisa) lower barriers to entry and accelerate group maturation cycles. Also, Team PCP has collaborated with Breachforums and claims to open access to the affiliate panels of Vect 2.0 Ransomware to all the members of Breachforums as Team PCP has partnership with Vect as well, this would significantly result in increased number of Ransomware attacks in the upcoming time if executed properly.



5. **MDM/UEM-based attacks are likely to be replicated** following the Stryker playbook. Organizations with cloud-managed endpoint fleets should audit administrative access controls, implement break-glass procedures, and segment MDM administrative networks.
6. **ESXi-targeting will become a standard ransomware capability.** Groups without ESXi lockers will be at a competitive disadvantage in the affiliate market, driving rapid adoption.
7. **Supply chain attacks on security tooling** (e.g., Trivy double-compromise) will continue as high-value targets, a single compromised security tool provides access to thousands of downstream environments.

Defensive Recommendations

Immediate Priorities:

- **Magento/Adobe Commerce:** If running any production version up to 2.4.9-alpha2, treat PolyShell as an active compromise. Apply virtual patching (WAF rules blocking polyglot uploads via /rest/V1/carts/*/items), audit pub/media/custom_options/quote/ for unauthorized PHP files, and monitor for web shell activity.
- **Ivanti EPMM:** Apply RPM patches for CVE-2026-1281 and CVE-2026-1340 immediately. Audit EPMM access logs for unauthorized code execution artifacts.
- **Google Chrome:** Ensure all enterprise Chrome installations are updated to the latest stable channel addressing CVE-2026-3909/3910/2441.
- **Cisco SD-WAN:** Comply with CISA Emergency Directive 26-03 — inventory SD-WAN systems, apply mitigations for CVE-2026-20127.
- **Endpoint management (Intune/UEM):** Audit all administrative accounts for cloud-based MDM/UEM platforms. Implement conditional access, privileged access workstations, and break-glass account procedures. The Stryker attack vector is replicable.
- **Iran-related threat hunting:** Review CISA's 136-CVE CVIE catalog for Iranian targeting. Prioritize patching for listed CVEs, particularly in healthcare, energy, and government sectors.

Short-term Priorities:

- **Deploy phishing-resistant MFA (FIDO2/passkeys):** Traditional MFA is bypassed by Tycoon 2FA and similar AiTM platforms at a 59% success rate. Password + OTP is no longer sufficient.
- **Monitor for credential exposure:** Following the LeakBase takedown, seized data may be used in new investigations — but also risk secondary leaks. Reset credentials for any services that may have been exposed on the platform.
- **ESXi hardening:** Verify execInstalledOnly=1 on all ESXi 8.0 hosts. Enable Lockdown Mode. Restrict shell and SSH access. Maintain VM-level backups independent of hypervisor snapshots.
- **E-commerce monitoring:** Deploy content integrity monitoring for Magento storefronts. Watch for WebRTC-based data exfiltration that bypasses CSP.

Long-term Priorities:

- **MDM/UEM zero-trust architecture:** Implement tiered administrative access for endpoint management platforms. No single administrative account should be able to push wipers to an entire device fleet.

- **Supply chain security:** Implement SLSA framework compliance for CI/CD pipelines. Verify integrity of security scanning tools (Trivy, etc.) against known good checksums before execution.

- **Ransomware resilience testing:** Conduct tabletop exercises incorporating March 2026 scenarios — MDM wiper, ESXi encryption, PolyShell web shell compromise.

- **Geopolitical threat briefings:** Establish regular cadence of threat briefings for executive leadership covering the Iran-US-Israel cyber dimension and its implications for organizational risk.

CVE-2026-33017

Overview

This report provides a detailed analysis of CVE-2026-33017, a critical unauthenticated Remote Code Execution (RCE) vulnerability affecting the Langflow open-source framework. The vulnerability, with a CVSS v3.1 score of 9.8 (Critical), allows unauthenticated attackers to execute arbitrary code on a target server, leading to potential full system compromise.

Key findings indicate that the flaw resides in an API endpoint intended for building public flows, which insecurely processes an attacker-controlled data parameter, executing embedded Python code via the exec() function. The vulnerability impacts all Langflow versions prior to 1.9.0.

This vulnerability is being actively exploited in the wild, with attacks observed within 20 hours of its public disclosure on March 17, 2026. Consequently, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have added it to its Known Exploited Vulnerabilities (KEV) catalog. The primary remediation is to upgrade immediately to Langflow version 1.9.0 or later. If patching is not feasible, mitigation strategies, including network access restrictions and enhanced monitoring, are strongly recommended.

Introduction

The purpose of this report is to fulfill the research request concerning CVE-2026-33017. It synthesizes intelligence from multiple security sources to provide a comprehensive overview of the vulnerability. The scope of this analysis covers the technical details of the flaw, its severity, current exploitation status, threat intelligence context, and actionable recommendations for remediation and mitigation.

Vulnerability Analysis

Technical Details

CVE-2026-33017 is a code injection vulnerability classified under CWE-94 (Improper Control of Generation of Code). The flaw exists in the POST /api/v1/build_public_tmp/{flow_id}/flow endpoint, which is designed to allow unauthenticated users to build public flows. The vulnerability arises because this endpoint insecurely accepts an optional data parameter. An attacker can supply a specially crafted JSON payload in this parameter containing arbitrary Python code within node definitions. The server-side code then executes this malicious input directly using Python's exec() function without proper sandboxing or input validation, resulting in unauthenticated RCE.

Affected Products and Versions Product:

Langflow Affected Versions: All versions prior to 1.9.0. Specifically, versions 1.8.1 and earlier are confirmed vulnerable. Initial reports suggested version 1.8.2 might be patched, but subsequent analysis by security researchers confirmed it remains exploitable.

Severity Assessment (CVSS)

The National Vulnerability Database (NVD) has assigned this vulnerability a critical severity rating.

CVSS v3.1 Base Score: 9.8 (Critical)

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

This vector indicates the vulnerability is network-exploitable with low complexity, requires no privileges or user interaction, and has a high impact on confidentiality, integrity, and availability.

Exploitation Status and Threat Intelligence

Active Exploitation

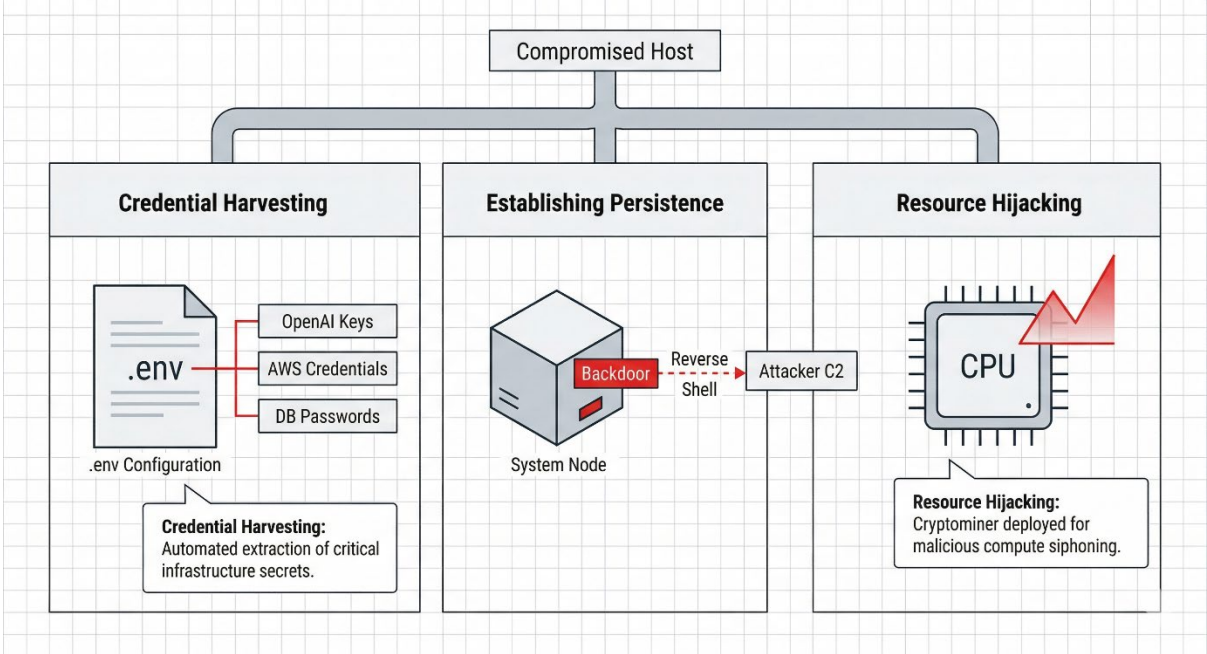
CVE-2026-33017 was weaponized with remarkable speed. Threat actors began actively exploiting the vulnerability in the wild within 20-24 hours of its public disclosure on March 17, 2026. This exploitation occurred even before any public Proof-of-Concept (PoC) code was widely available, indicating that attackers were able to develop exploits directly from the detailed advisory information. Due to its active exploitation, CISA added CVE-2026-33017 to its KEV catalog on March 26, 2026, mandating federal agencies to patch by April 8, 2026.

Public Proof-of-Concept (PoC)

At least one public PoC exploit has been identified on GitHub in the SimoesCTT/Sovereign-Echo-33017 repository. This and other PoCs simplify the exploitation process for a wider audience. No specific entries were found for this CVE on Exploit-DB.

Attacker Tactics and Objectives

Threat intelligence reports from firms like Sysdig indicate that attackers are engaged in automated scanning to identify vulnerable Langflow instances. Observed post-exploitation activities include:



Remediation and Mitigation Strategies

Given the critical nature and active exploitation of this vulnerability, immediate action is required.

Primary Remediation: Upgrade

The definitive solution is to upgrade Langflow to version 1.9.0 or later. This patched version completely removes the vulnerable data parameter from the build_public_tmp endpoint, eliminating the attack vector.

Mitigation and Workarounds

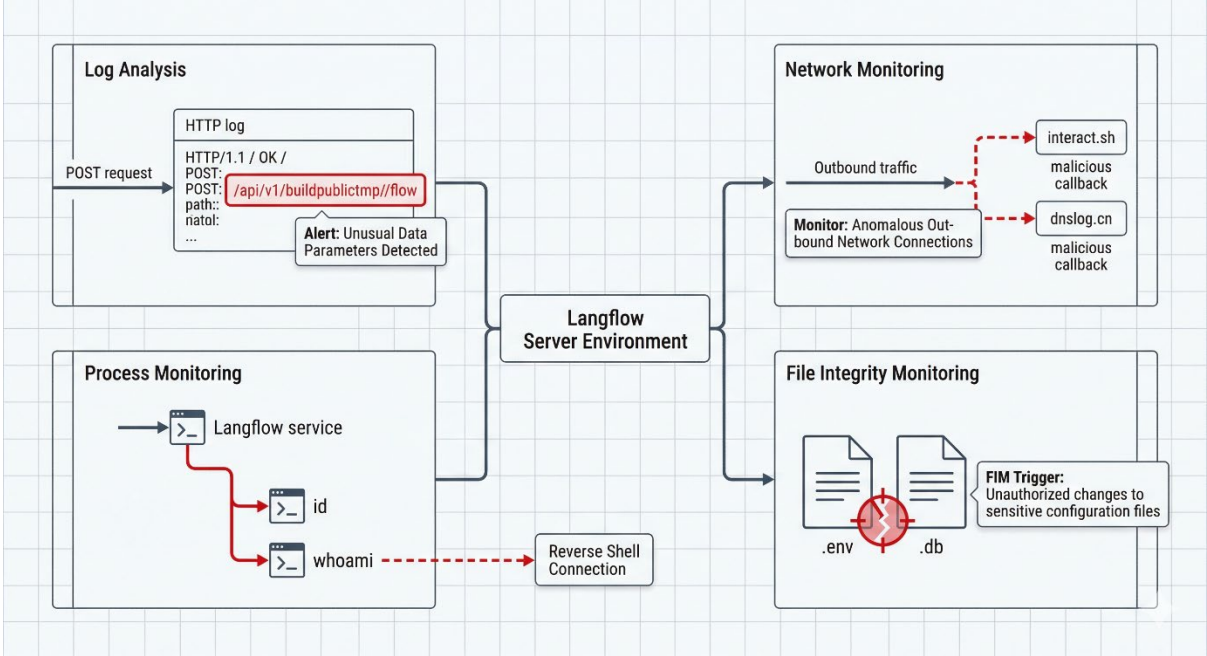
If an immediate upgrade is not possible, the following multi-layered mitigation strategies should be implemented:

Strategy Category	Recommended Action
Network Controls	1. Implement firewall rules to restrict external access to the /api/v1/build_public_tmp endpoint. 2. Deploy a reverse proxy with mandatory authentication in front of Langflow instances.
Configuration Hardening	1. If the functionality is not essential, disable public flow building entirely. 2. Set AUTO_LOGIN=false as a compensating control for exposed instances.

Security Hygiene	1. Assume compromise for any publicly exposed instance. 2. Immediately audit and rotate all credentials, API keys, and secrets accessible to the Langflow server.

Detection and Monitoring

Organizations should actively monitor for signs of compromise:



Conclusion

CVE-2026-33017 is a critical, easily exploitable, and actively exploited remote code execution vulnerability in Langflow that poses a significant threat to organizations utilizing the framework. The speed at which it was weaponized highlights a shrinking gap between vulnerability disclosure and real-world attacks.

The highest priority for all administrators of Langflow instances is to upgrade to version 1.9.0 or later. For systems that cannot be immediately patched, a combination of network segmentation, configuration hardening, credential rotation, and vigilant monitoring is crucial to mitigate risk and detect potential compromise.

Threat Intelligence Sharing Initiative

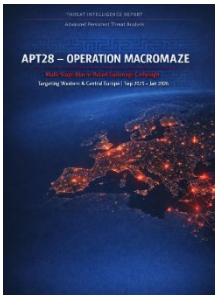
As part of the continuous threat intelligence efforts, a dedicated initiative has been launched to publish weekly Threat Intelligence (TI) reports within the LinkedIn group of the Data Security Council of India (DSCI).

These reports cover focused topics including:

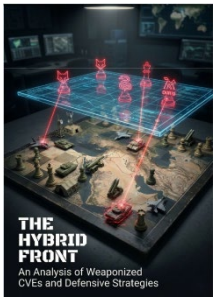
- Dark Web Intelligence & Monitoring
- Cyber Threat Intelligence
- Vulnerability Assessment Insights

We invite you to join the DSCI LinkedIn group and stay updated with research-driven intelligence reports shared by the team.

Qilin Ransomware DW Analysis



APT28: Operation MacroMaze



Analysis of Weaponized CVEs

Medusa Raas DW Analysis

Omnibar: Malicious AI browser

China-based espionage operation

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips