DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT REPORT

FEBRUARY 2026

Table of Contents

Vect 2.0 Ransomware Activity & Dark Web Analysis 3

StarKiller 12

Threat Intelligence Sharing Initiative 19

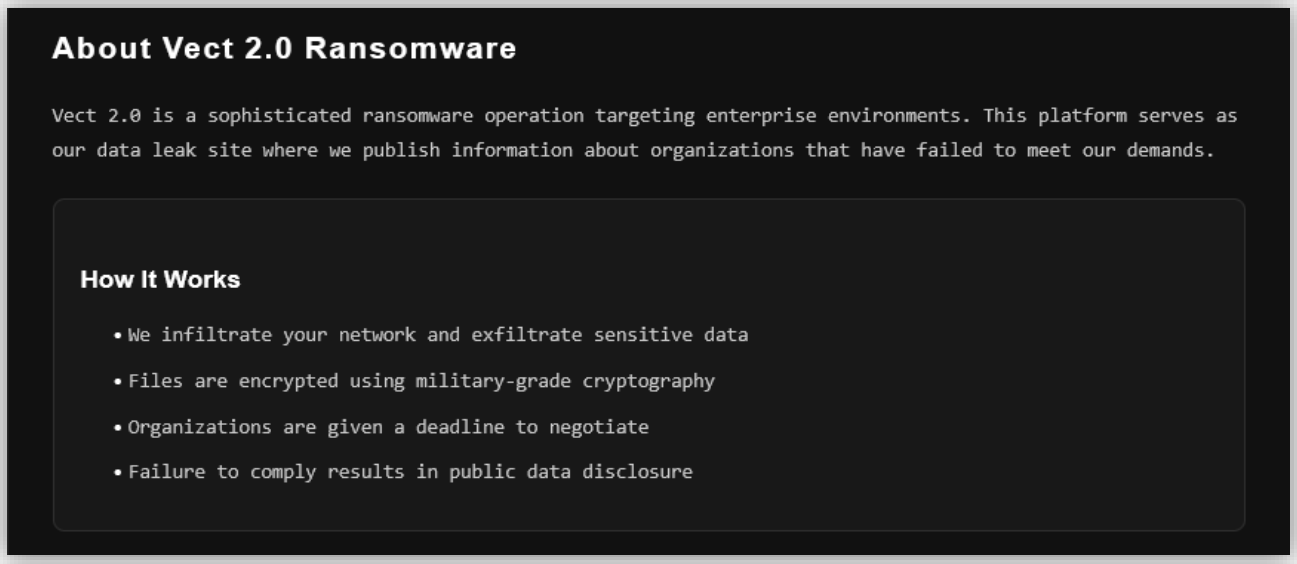
SILENTLY & SLOWLY: VECT 2.0'S EMERGENCE IN FEBRUARY LANDSCAPE

A COMPREHENSIVE ANALYSIS

Vect 2.0 Ransomware Activity & Dark Web Analysis

Vect, now officially rebranded as Vect 2.0, is an emerging and sophisticated Ransomware-as-a-Service (RaaS) group that rapidly escalated its operations through February 2026. Originating in December 2025, Vect 2.0 has distinguished itself with a custom-built C++ codebase and advanced operational tactics, explicitly adopting an "Exfiltration / Encryption / Extortion" model to maximize disruption and financial gain.

During February 2026, Vect 2.0's activity surged, with its Data Leak Site (DLS) dashboard showing total of 20 victims (6 with data published and 14 in progress/negotiating). While external aggregators reported 18 claimed victims, the DLS provides the most current operational status. The group continues to target critical sectors globally, primarily in Brazil and the United States, utilizing highly effective evasion techniques including Safe Mode execution. Its robust operational security posture, Monero-only payments, and exclusive TOR infrastructure signify a professional and dangerous adversary.



*"YOUR DATA HAS BEEN ENCRYPTED BY VECT. DO NOT MODIFY FILES. DO NOT RESTART. TO RECOVER YOUR DATA, ACCESS OUR CHAT PORTAL: bu7zr6foth[redacted]wkbdtgtjuid.onion/chat USE THIS ID TO LOGIN: **[UUID-FORMAT-CHAT-ID]**"*

Ransom note typically follows the structure as shown in the image.

Threat Profile & Attribution

- **Rebranding:** The group has officially rebranded to **"Vect 2.0"**, as observed on its login and registration pages, indicating an evolution in its public-facing identity.
- **Origin:** Analysis of recruitment tactics, specifically the waiver of entry fees for applicants from Commonwealth of Independent States (CIS) countries, strongly suggests that Vect 2.0's operators or primary affiliates are based in this region (e.g., Russia or Belarus).
- **Classification:** Vect 2.0 operates as a Ransomware-as-a-Service (RaaS) model, providing its malware and infrastructure to affiliates in exchange for a share of the ransoms paid. This model allows for rapid expansion and broad targeting.
- **Market Position:** As an emerging threat, Vect 2.0 is quickly establishing itself within the ransomware landscape. It currently represents approximately 1.6% of observed incidents based on the internal analysis of the overall February ransomware incident landscape. However, the group's tooling, infrastructure, and operational model

suggest a trajectory toward capabilities typically associated with established mid-tier operations such as Nova and Tengu.

Vect 2.0 Dashboard Insights

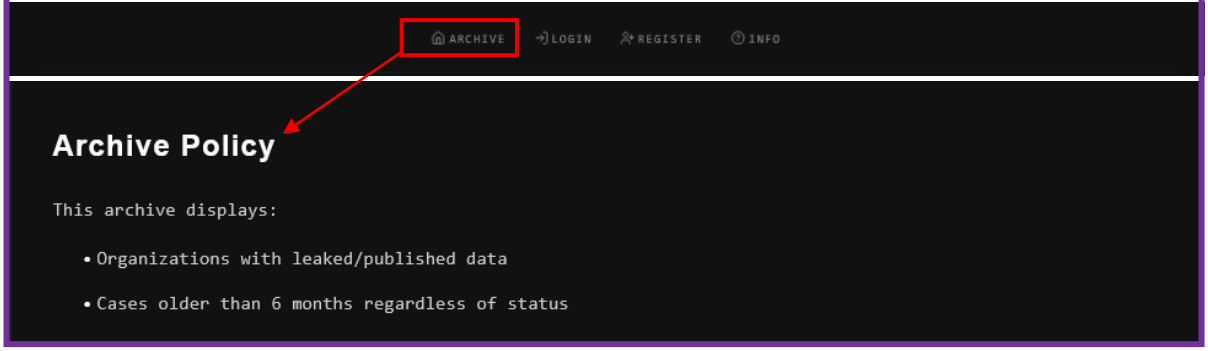
Insights directly from the Vect 2.0 Data Leak Site (DLS) dashboard provides a real-time view of their operational status:

Operational Statistics: As of February 28, 2026, the DLS dashboard reported **20 active cases**.

- **Data Published:** 6 victims had their data publicly leaked on the DLS & prominent platforms like BreachForums.
- **In Progress/Negotiating:** 14 victims were actively under negotiation or in the process of having their data leaked.
- **Note:** The DLS data currently reflects 20 affected companies. Historical or resolved claims dated prior to 13 February 2026 have been removed from the DLS, and therefore the dataset includes only victims listed from 13 February 2026 onward. The threat actor continues to publish data regularly as of now.

Motto/Tagline: The group prominently displays "Exfiltration / Encryption / Extortion", clearly outlining their triple-threat business model.

Archive Policy: Vect 2.0 states an "Archive Policy" where "Cases older than 6 months regardless of status" will be displayed on their DLS, indicating a persistent public shaming tactic.



Technical Analysis

Vect 2.0 employs a highly advanced and multi-platform approach, demonstrating a sophisticated understanding of modern enterprise environments.

Malware Architecture

Custom-Built Encryptor: Developed in C++ from scratch, demonstrating a high level of expertise and avoiding reliance on leaked code from other groups.

Encryption

Algorithm: Uses ChaCha20-Poly1305 AEAD, which is approximately 2.5 times faster than AES-256-GCM on systems without hardware acceleration. This choice allows for rapid encryption and minimal detection windows.

Method: Employs intermittent encryption, scrambling only blocks of data within files. This technique further improves encryption speed and reduces the overall system footprint, making detection more challenging.

Platform Targeting

Vect 2.0 is designed for broad impact across various operating environments:

Windows: Utilizes standard executables, multi-threading, and leverages built-in Windows functionalities.
Linux/VMware ESXi: Specifically targets these environments using ELF binaries (e.g., enc_esxi.elf) designed to encrypt virtual machine disk images (.vmdk, .vmx, VMEM, VMSD, VMSN files), ensuring the compromise of virtualized infrastructures.

Defence Evasion

Safe Mode Execution: A critical evasion technique involves rebooting the compromised system into Safe Mode with networking enabled (bcdedit /set {default} safeboot network). This bypasses many Endpoint Detection and Response (EDR) solutions and other security tools that do not operate in Safe Mode.

Process Termination: Aggressively terminates processes related to security software (AV/EDR), backup solutions (Veeam, BackupExec, Acronis), and database services (SQL, Oracle) to minimize interference during encryption.

Crypter/Packer: Employs a built-in VM Crypter/Packer toggle to obfuscate its binaries and protect them from signature-based detection.

Lateral Movement

Vect 2.0 relies on "Living off the Land" (LotL) techniques to propagate across networks, including:

SMB (Server Message Block): Exploiting admin shares for network propagation.
WinRM (Windows Remote Management): Leveraging remote management protocols.
PowerShell: Utilizing PowerShell for execution and lateral movement.
Group Policy Objects (GPO): The ransomware's payload builder can directly accept Domain Admin credentials, allowing for propagation via Group Policy.

Impact

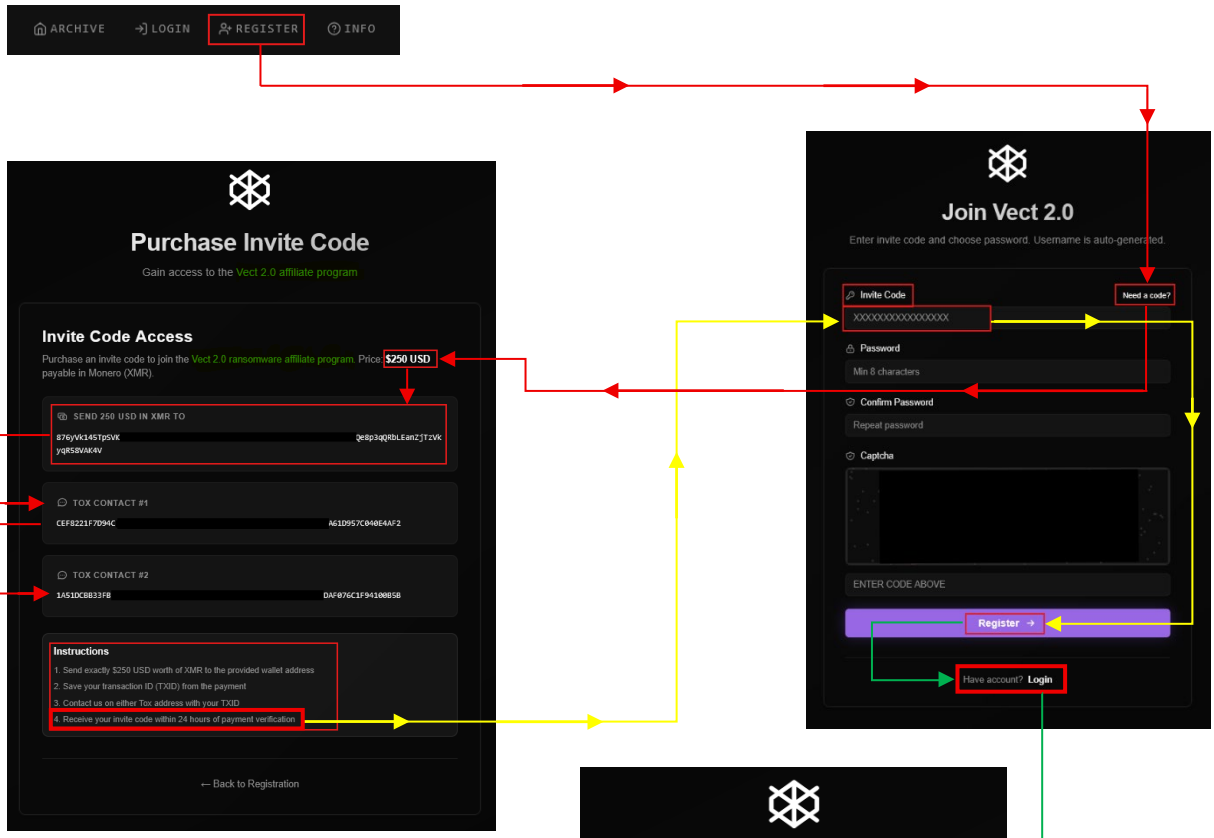
Beyond encryption, Vect 2.0 takes steps to ensure data irretrievability:

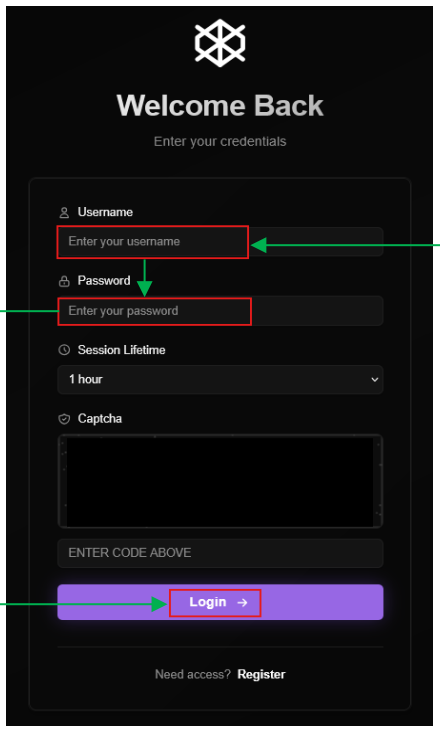
Shadow Copy Deletion: Deletes Volume Shadow Copies (vssadmin Delete Shadows /all /quiet) and disables Windows Backup features (wbadmin delete catalog -quiet) to prevent system recovery from local backups.
Data Exfiltration: Data is staged and exfiltrated prior to encryption, likely using tools like Rclone or proprietary methods, facilitating a double-extortion scheme.

Dark Web Operations & Infrastructure

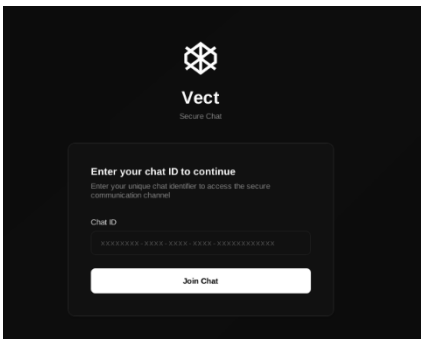
Vect 2.0's operations demonstrate a robust focus on operational security and anonymity, characteristic of a professional RaaS group.

Recruitment: The group actively recruits affiliates, offering a "generous" revenue-sharing model. A **$250 USD entry fee, payable in Monero (XMR)**, is required for new affiliates but is **waived for applicants from CIS countries/operators**, indicating a strategic recruitment drive within this region specially from Russian speaking people.



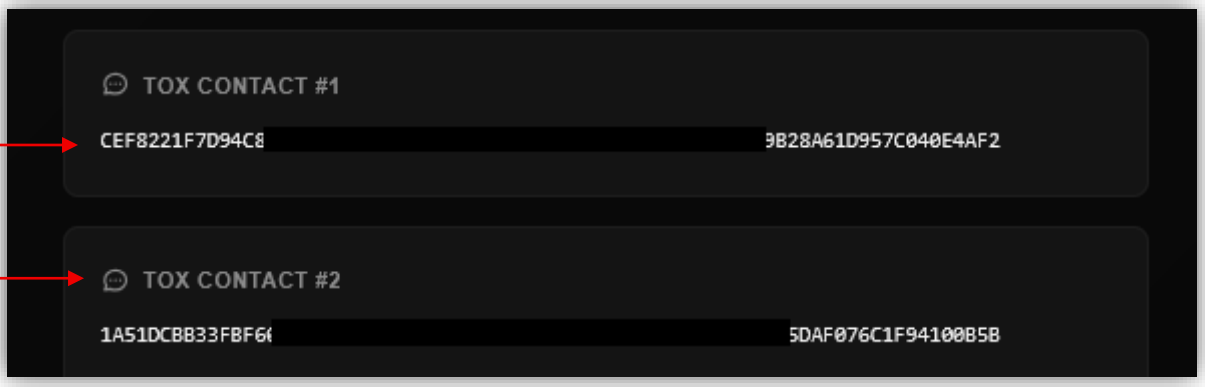


Additionally:

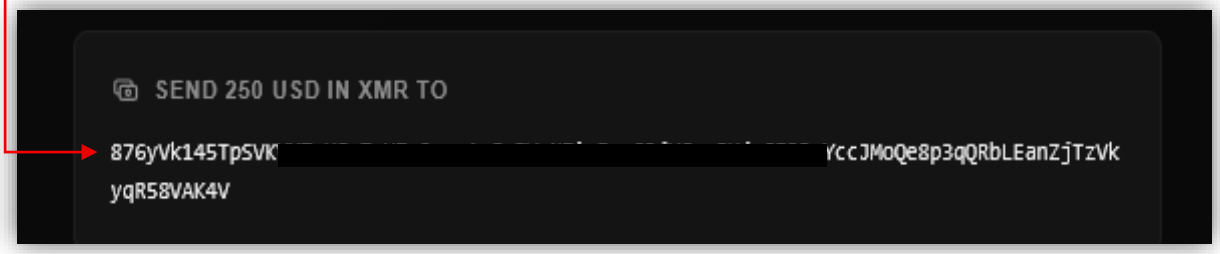


Apart from tox, they also have their own **Chat Portal Branding** "Vect Secure Chat". Which works on specific Chat IDs.

Communication: All communications are facilitated through the **TOX protocol**, ensuring encrypted peer-to-peer messaging and minimizing communication interception risks.



Payment: Vect 2.0 strictly enforces the use of **Monero (XMR)** for all ransom payments, providing enhanced financial anonymity for both the operators and affiliates.



Infrastructure: The group's entire infrastructure, including its Data Leak Site (DLS) and negotiation chat portals, operates exclusively via **TOR hidden services**, maintaining a strict no clear-net presence policy for its public-facing operations.

Observed Clearnet IP: While their public-facing infrastructure is TOR-only, in early stage of their operations security researchers had identified an **observed Clearnet IP: 158.94.210.11 [Port 8000]**, which may be associated with C2 infrastructure or affiliate panel components.

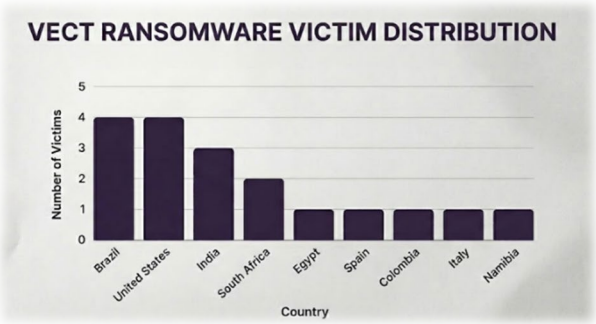
Victimology & Statistics (February 2026)

February 2026 saw a significant revamp & increase in Vect 2.0's victim claims, illustrating its growing threat.

Total Victims: As of February 28, 2026, Vect 2.0's DLS dashboard reported **20 active cases** (excluding initial activity in January 2026 & previously). The last discovered victim in February 2026 was on the 28th of the month.

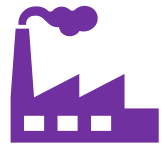
Geographical Statistics:

Brazil: 4 victims
United States: 4 victims
India: 3 victims
South Africa: 2 victims
Egypt: 1 victim
Spain: 1 victim
Columbia: 1 victim
Italy: 1 victim
Namibia: 1 victim



Key Sectors:

Most affected sectors by Vect 2.0 Ransomware group includes Manufacturing, Education, Healthcare, Technology.


Manufacturing sector


Education sector


Healthcare sector


Technology

Attack-to-Leak Delay: The average delay observed between an attack and the public claim by Vect 2.0 on its Data Leak Site was reported to be **8 days**.

Indicators of Compromise (IOCs)

IOC	Type of IOC
158.94.210.11 (Port 8000 observed)	IP Address
svc_host_update.exe	Windows executable file
enc_esxi.elf	Linux/ESXi executable)
VECT_RECOVERY_GUIDE.txt	Ransom Note Filename
README_VECT.html	Ransom Note Filename
Qilin[@]exploit[.]im	Email address
.vect	File extension of encrypted files

More IOCs can be found on DSCI Threat Intel Portal, offered exclusively to our members for in-depth analysis and continuous monitoring of Cyber Threat Landscape, feel free to contact our membership team at membership@dsci.in to get started.

MITRE ATT&CK Mapping

The table below summarises Vect's tactics and techniques mapped to the MITRE ATT&CK framework:

ATT&CK ID	Tactic	Technique
T1078	Initial Access	Valid Accounts: Stolen/weak credentials
T1133	Initial Access	External Remote Services: RDP/VPN
T1566	Initial Access	Phishing
T1059	Execution	Command and Scripting Interpreter
T1053	Persistence	Scheduled Task/Job (inferred)
T1134	Privilege Escalation	Access Token Manipulation (inferred)
T1562.009	Defence Evasion	Safe Mode Boot
T1562.001	Defence Evasion	Impair Defences: Disable Tools
T1003	Credential Access	OS Credential Dumping (inferred)
T1046	Discovery	Network Service Discovery: DFS/SMB
T1082	Discovery	System Information Discovery
T1083	Discovery	File and Directory Discovery
T1021.002	Lateral Movement	Remote Services: SMB/Admin Shares
T1021.006	Lateral Movement	Remote Services: WinRM
T1005	Collection	Data from Local System
T1039	Collection	Data from Network Shared Drive
T1071.001	Command-and-Control	Application Layer Protocol: Web
T1573	Command-and-Control	Encrypted Channel: TOR
T1041	Exfiltration	Exfiltration Over C2 Channel
T1486	Impact	Data Encrypted for Impact
T1490	Impact	Inhibit System Recovery
T1489	Impact	Service Stop

Mitigation Strategies

Organizations can implement the following strategies to reduce their risk exposure to Vect 2.0 Ransomware:

- **Network Perimeter Security:**
  - **Block Known IOCs:** Implement blocks for all known Vect 2.0-related Onion URLs, IP addresses, and communication channels at the perimeter.
  - **TOR Blocking:** Consider blocking access to TOR nodes from the organizational network, especially for outbound connections, unless explicitly required for business purposes.

- **Endpoint and System Hardening:**
  - **Monitor `bcdedit` and Safe Mode Events:** Implement continuous monitoring for `bcdedit` modifications, particularly those related to `safeboot` network, and for system reboots into Safe Mode. This can indicate an active attempt at defence evasion.
  - **Process Monitoring:** Monitor for and block the aggressive termination of critical processes, security software, and backup solutions.
  - **Patch Management:** Ensure all operating systems (Windows, Linux) and applications, especially VMware ESXi environments, are regularly patched and updated to remediate known vulnerabilities that Vect 2.0 or its affiliates might exploit for initial access or lateral movement.
  - **Multi-Factor Authentication (MFA):** Enforce MFA across all services, particularly for remote access, privileged accounts, and critical systems like ESXi.
  - **Network Segmentation:** Implement robust network segmentation, isolating critical assets (e.g., VMware ESXi hosts, domain controllers, backup servers) to limit lateral movement.

- **Data Protection and Recovery:**
  - **Offline Backups:** Adhere to the 3-2-1 backup rule (3 copies of data, 2 different media, 1 offsite/offline). Ensure backups are immutable and stored offline or in an air-gapped environment to prevent ransomware encryption or deletion.
  - **Regular Backup Testing:** Periodically test backup and disaster recovery procedures to ensure data recoverability.

- **User Training and Awareness:**
  - Educate employees on phishing, social engineering tactics, and the importance of strong, unique passwords.


STARKILLER

StarKiller

Introduction

Unlike traditional phishing kits that use static HTML replicas of login pages, Starkiller, a new *commercial-grade phishing framework* dynamically **proxies real login pages** from legitimate services through attacker-controlled infrastructure. This makes it extremely convincing and difficult for conventional detection mechanisms to identify. It is sold by a threat actor group calling itself **Jinkusu** who market the product as a commercial-grade cybercrime platform.

It is distributed like a **Software-as-a-Service (SaaS)** platform, complete with a polished control panel, documentation, community forum, and ongoing updates — significantly lowering the technical barrier for cybercriminals to conduct advanced phishing campaigns.

Tactics, Techniques, and Procedures (TTPs)

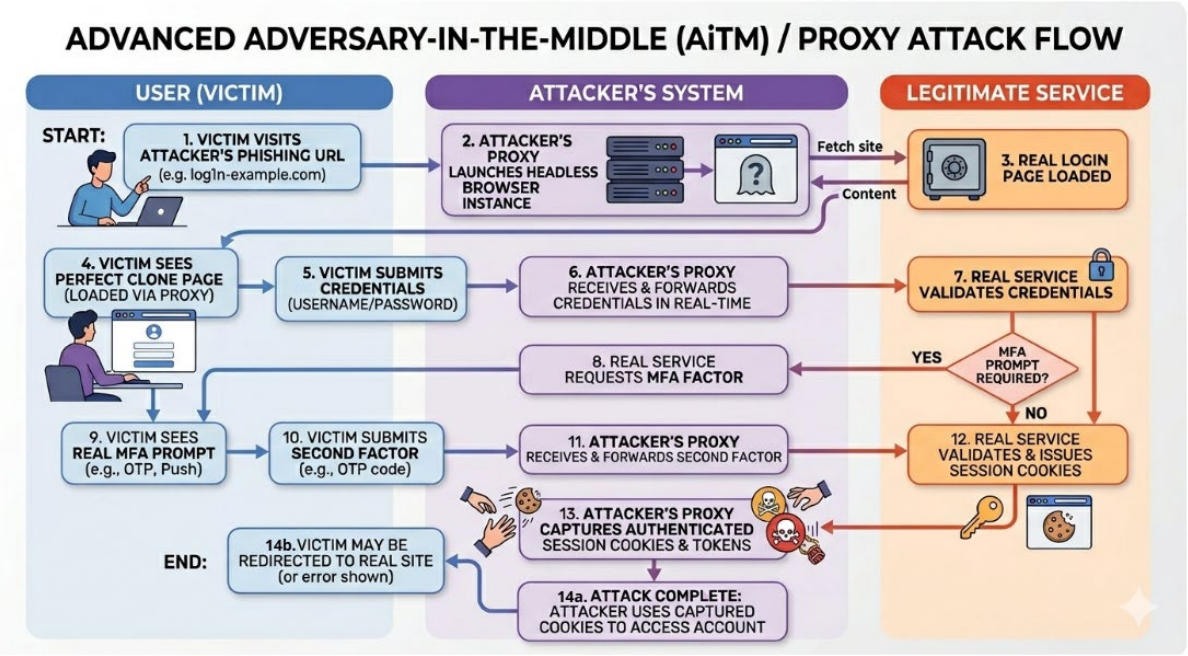
Tactic	Technique (ID)	Technique (Name)	Procedure / Description
Resource Development	T1583	Acquire Infrastructure	Operators use the platform which automates infrastructure provisioning like reverse proxies, TLS certificates, etc.
Initial Access	T1566.002	Phishing – Spear phishing Link	Campaigns are delivered via email containing embedded malicious links
	T1078	Valid Accounts	Attackers can gain access to legitimate accounts by capturing authenticated session tokens
Defence Evasion	T1027	Obfuscated Files or Information	The platform employs URL manipulation technique to evade detection
Credential Access	T1557	Adversary-in-the-middle	Starkiller acts as a reverse proxy between victim and legitimate service
	T1056.001	Keylogging	Starkiller records all keystrokes submitted during the authentication session

	T1056.003	Input Capture – Web Portal Capture	Victim enters credentials into a proxied legitimate login form
	T1539	Steal Web Session Cookie	After successful authentication, session cookies and tokens are intercepted and reused for account takeover
Collection	T1056	Input Capture	Platform captures user inputs beyond credentials, potentially including additional personal or organizational data

Core Capabilities

MFA Bypass Mechanism

One of the most significant capabilities of Starkiller is to bypass traditional multi-factor authentication (MFA) mechanisms through real-time adversary-in-the-middle proxy.



When attackers relay the entire authentication flow in real time, MFA protections can be effectively neutralized despite functioning exactly as designed.

Rest of the features are visible in the screenshot below -

Features of Starkiller
Source - Abnormal

Attack Flow of URL Masking

The URL masking feature easily helps an attacker to trick user to interact with a suspicious link that looks legit.

Phase 1 – Brand Impersonation

The operator selects a brand to impersonate (Microsoft, Google, Apple, Amazon, PayPal, Netflix, Facebook, etc.)

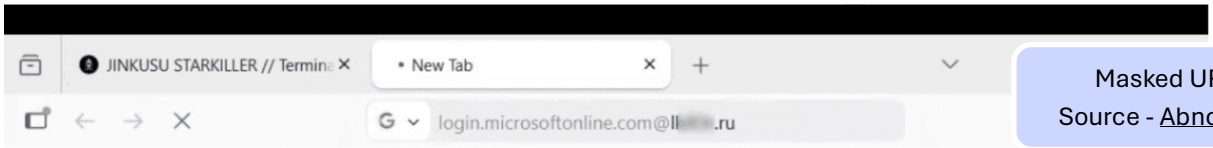
Phase 2 – Deceptive URL Generation

Once brand is selected, it generates a deceptive phishing URL designed to visually resemble the legitimate domain. The URL can be customized with words like

- login
- verify
- security
- account
- signin
- auth
- myaccount

Phase 3 – Obfuscation and Delivery Enhancement

It integrates URL shorteners such as TinyURL (is,gd, v,gd) and uses classic @ symbol URL trick. Everything before "@" is treated as user information and displayed prominently while actual domain is after "@." Due to Starkillers's point-and-click interface, even novice cybercriminals do not need URL parsing.



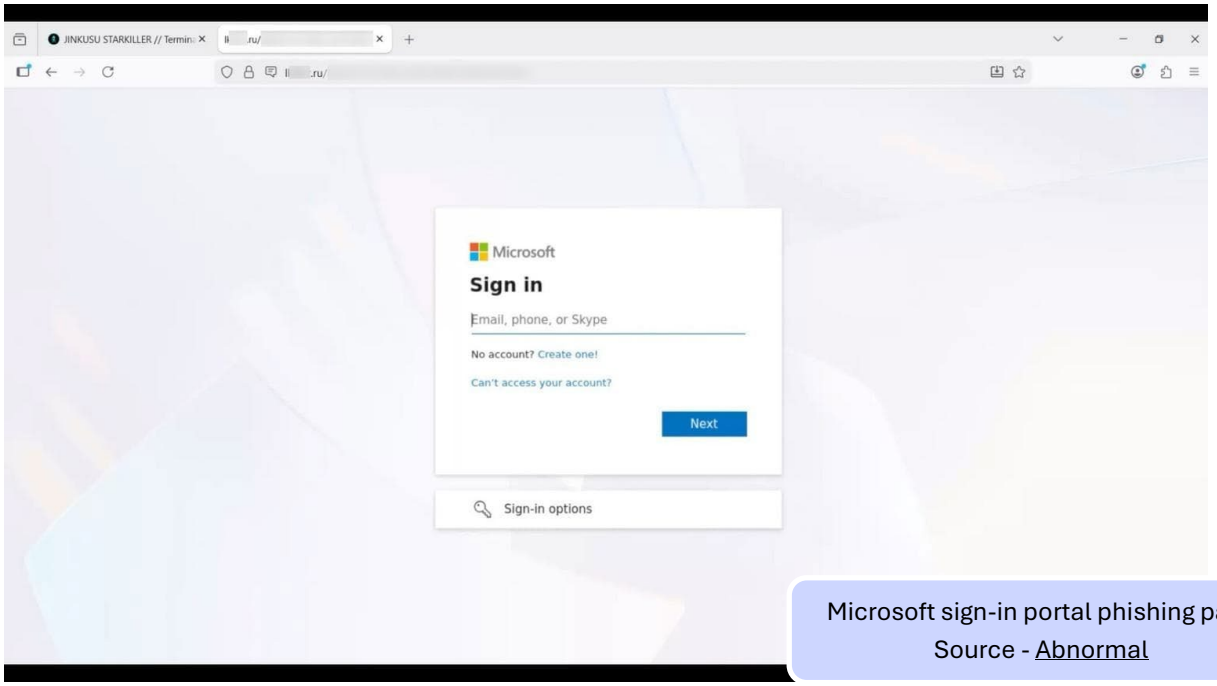
Masked URL
Source - Abnormal

Phase 4 – Victim Interaction

When recipient clicks the phishing link:

- The attacker's server loads the legitimate website in headless browser (e.g., a Microsoft login page)
- Server acts as a reverse proxy
- Legitimate HTML, CSS, and JS are forwarded to victim's browser.

From victim's perspective, the login page appears authentic, the only anomaly is URL which has already been masked and obfuscated.



Microsoft sign-in portal phishing page
Source - Abnormal

Phase 5 – Credential & Session Interception

When victims interact with the login page and enter the credentials, all the traffic passes through attacker-controlled infrastructure and keystrokes, the cookies and tokens also get logged.

Phase 6 – Live Session Monitoring

From the control panel, the attacker can watch the session in real time including their:

- Location
- Device type
- IP Address
- Session status (active or not)

Attackers can inject additional prompts to gather more information or terminate the session entirely.

Email: The primary delivery channel

Starkiller, unlike traditional adversary-in-the-middle frameworks that require manual configuration of:

- Reverse proxy rules
- TLS certificates
- Hosting environments
- Domain routing

The platform can easily deploy phishing pages and can monitor with a single control panel reducing complexity to launch campaigns easily.

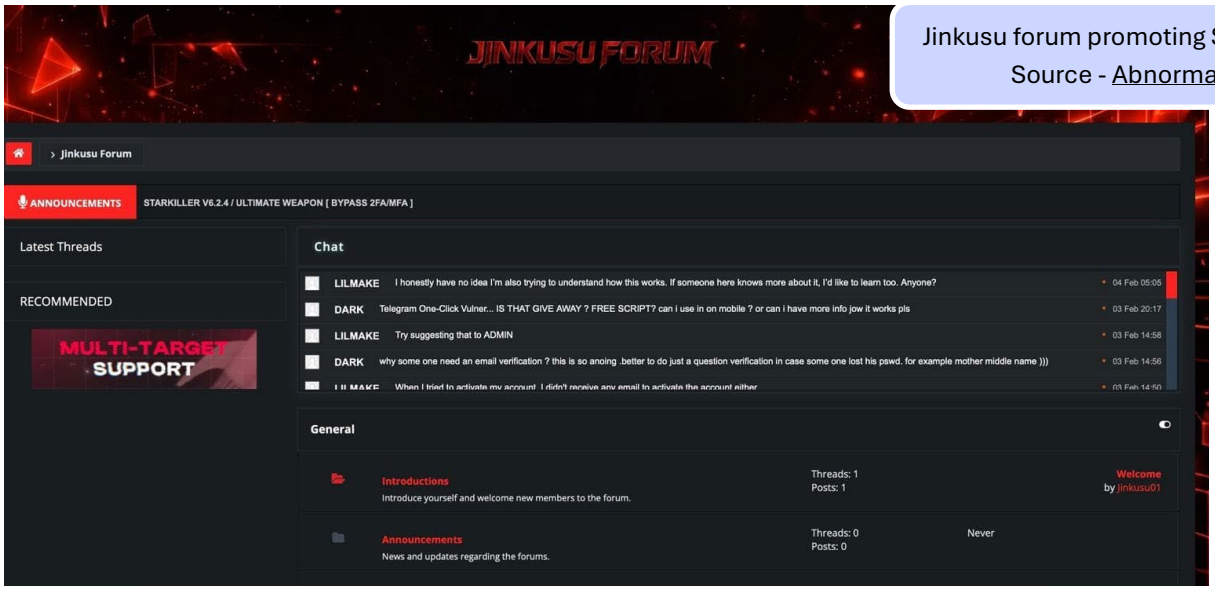
It is well-positioned for use in business-focused phishing campaigns as it can impersonate many enterprise platforms such as Microsoft, Google, Apple, Amazon, PayPal, and other major providers.

When recipient clicks on embedded links, the framework loads legitimate login page in real time due to which victim sees authentic HTML, CSS and JavaScript. This removes the visual inconsistency that can expose a phishing page. It also has an email harvesting feature which extracts contact information and email address from compromised sessions.

Due to this, threat actors can compromise a user using a phishing email harvested from the session. They can create a list of new targets from previous compromised accounts and expand their campaign.

Forum

As mentioned earlier, it is sold by Jinkusu which maintains a community forum where cybercriminals can discuss techniques, request features and troubleshoot deployments. The operators receive dedicated support, monthly framework updates, and documentation through Telegram. It protects its operators by using one-time password and multi-factor authentication.



Jinkusu forum promoting Starkiller
Source - Abnormal

How to prevent such attacks?

As we know that Starkiller uses a live proxy to show the actual website rather than displaying a static clone of website. It provides an easy way of using URL masking, MFA

bypass, session hijacking, etc. to novice cybercriminals. Starkiller dynamically create phishing pages for every session, traditional approaches like static page analysis, domain blocklisting, etc. are inadequate.

We should start behavioural analysis such as unusual login behaviours, session token reuse from unexpected locations, and identity-aware analysis that can identify a compromised session even when the phishing page appears flawless, must be the focus of detection. Also, we should examine the behavioural context of each email rather than solely relying on the content of links to stop these types of attacks.

Threat Intelligence Sharing Initiative

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

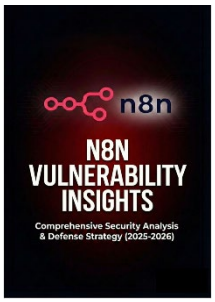
These reports cover focused topics including:

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

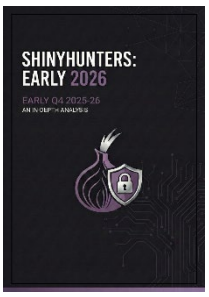
We invite you to join the DSCI LinkedIn group and stay updated with research-driven intelligence reports shared by the team.

Darkweb Report: Evolution of LockBit

APT41 Threat Group Report

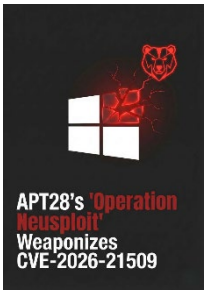


n8n Vulnerability Insights



SHINYHUNTERS: Early 2026

VoidLink Malware Framework



APT28's 'Operation Neusploit'

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