FUNKSEC

THREAT REPORT

CERTMH_CTI_2025_24

2025

TABLE OF CONTENTS

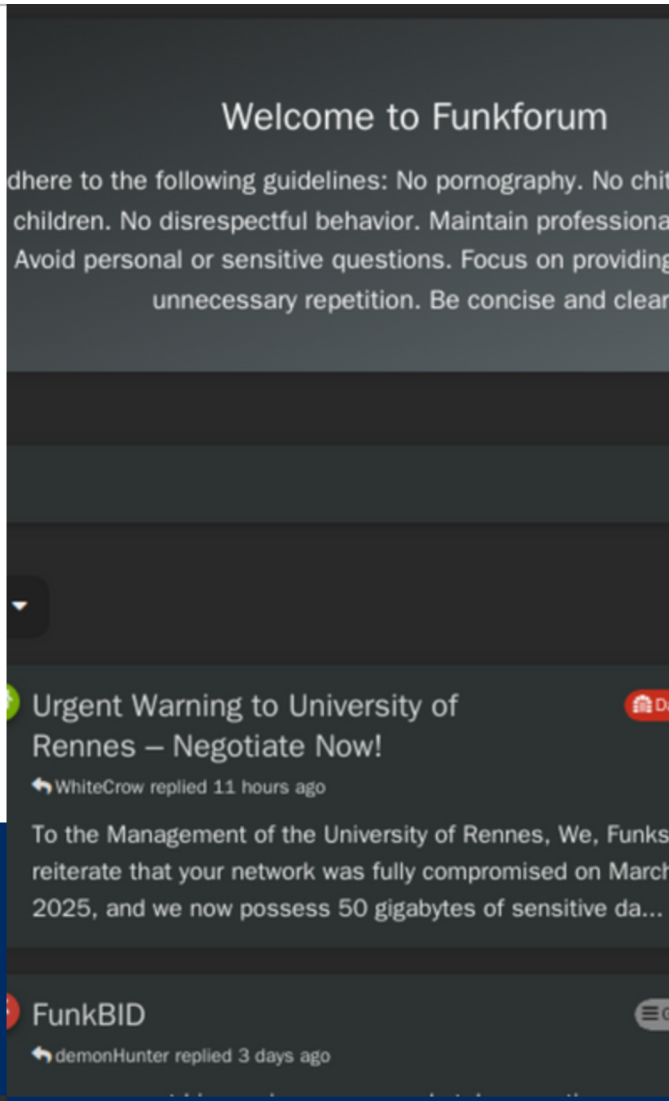
Introduction

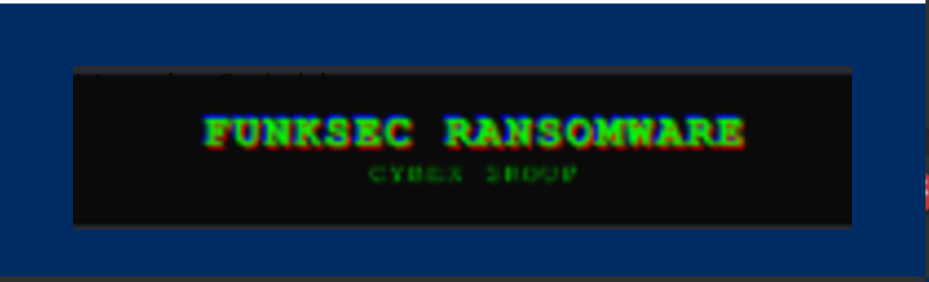
Funksec, a double extortion ransomware group, emerged in late 2024 and quickly gained notoriety by breaching databases and selling access to 15 government websites within just a month. Claiming to be entirely self-taught and operating without collaboration from other groups, Funksec is a four-member team driven primarily by financial motives.

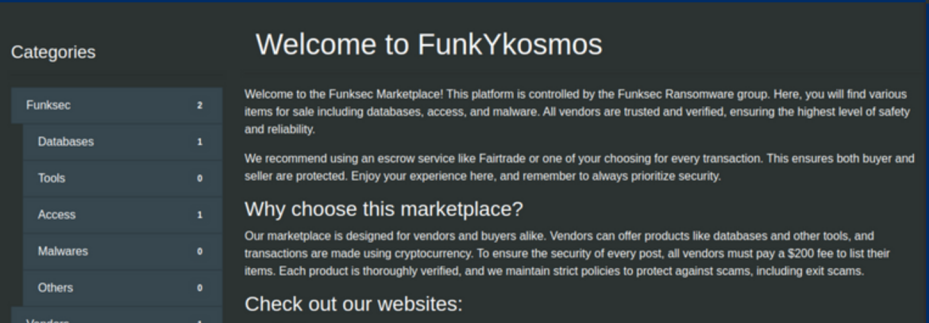
The group leverages AI for specific tasks, such as creating tools and phishing templates, though they emphasize that AI contributes to only about 20% of their operations. Notably, they have developed their own proprietary AI tool, WormGPT, a desktop application built entirely in-house.

To enhance their phishing campaigns, Funksec uses premium services like PhishingBox to create customized phishing templates, adding another layer of precision and sophistication to their methods.

After the interview, during some casual chit-chat, it came to light that the owner of Funksec was also behind an underground forum called DarkZone, which had been built in collaboration with GhostSec in the past.







Background

FunkSec is a new-age ransomware group that surfaced in late 2024, believed to have evolved from a hacktivist collective. Unlike traditional cybercriminal groups, FunkSec's operations are notable for being heavily AI-assisted—they use generative AI tools to help write and adapt malware, compensating for their limited in-house technical expertise.

Operating under a Ransomware-as-a-Service (RaaS) model, FunkSec quickly gained notoriety for volume-based attacks with modest ransom demands, typically around $10,000. This strategy aims for faster payouts and lower risk, helping them infect more victims without drawing excessive law enforcement scrutiny.

They've targeted a mix of government, education, and small to mid-sized enterprises, particularly in India, the U.S., and Israel. In early 2025, FunkSec publicly announced a collaboration with another group, FSociety, signaling ambitions to expand both reach and capability.

OBJECTIVES

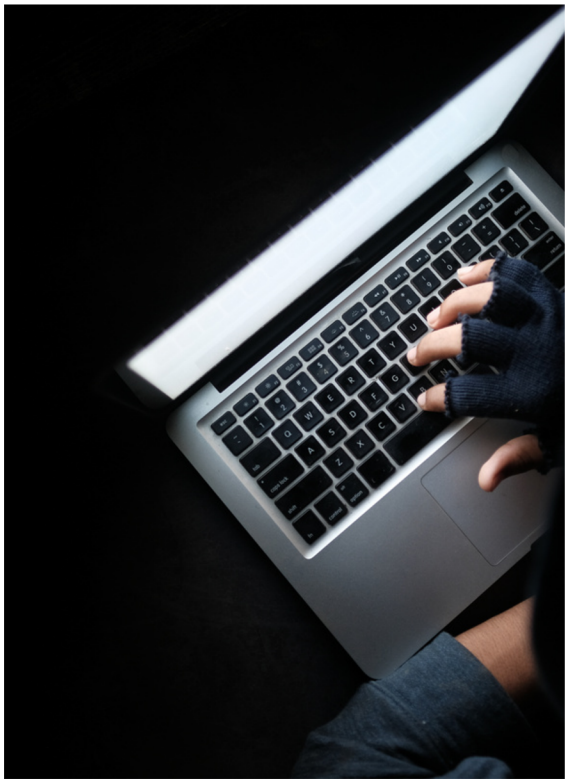
1. **Fast and Scalable Profit**
   - Focus on low ransom demands to encourage payment.
   - Target many victims simultaneously using automation.

2. **AI as a Force Multiplier**
   - Use generative AI to quickly build or modify ransomware.
   - Highlight AI's role in cybercrime, almost as a statement.

3. **Maintain Hacktivist Legacy**
   - Select targets with symbolic or political relevance.
   - Message-driven campaigns seen in earlier web defacements.

4. **Expand Underground Reputation**
   - Build credibility among cybercriminals through collabs and RaaS.
   - Create a "brand" that attracts affiliates and media attention.

MITRE ATT&CK TTPs



INITIAL ACCESS:

- **Phishing (T1566):** FunkSec often uses phishing emails containing malicious executables to trick users into launching the payload.

EXECUTION:

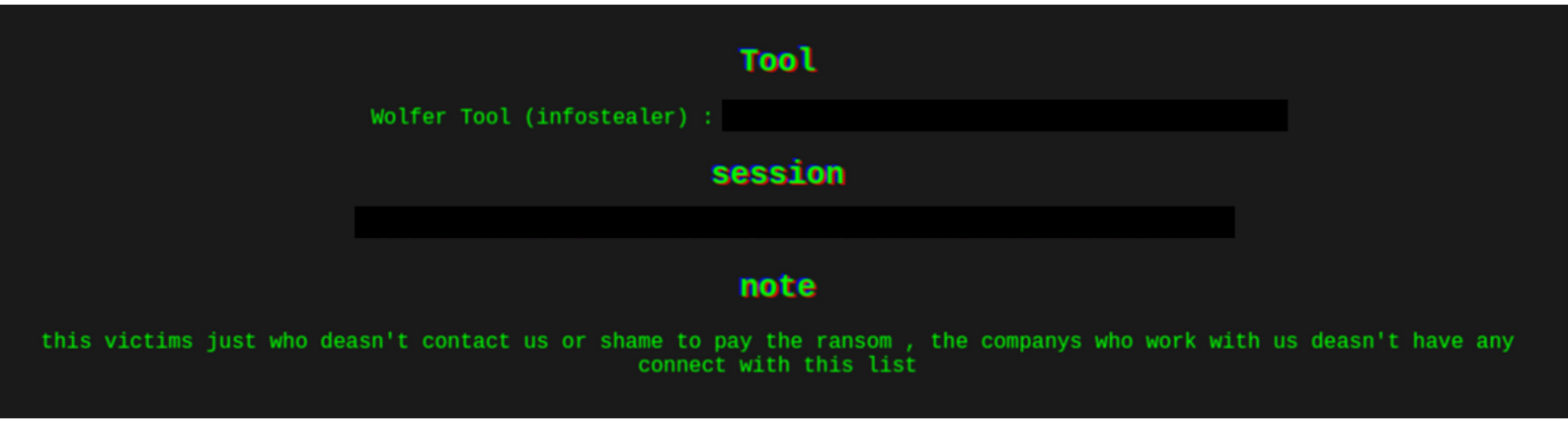
- **User Execution: Malicious File (T1204.002):** Victims manually execute disguised malicious files, often delivered through phishing emails.
- **Command and Scripting Interpreter: PowerShell (T1059.001):** PowerShell is used for executing commands and managing persistence.
- **Windows Command Shell (T1059.003):** cmd.exe is leveraged to run system information and discovery commands.

PERSISTENCE:

- **Boot or Logon Autostart Execution: Registry Run Keys (T1547.001):** FunkSec adds registry entries to ensure malware runs at system startup.
- **Scheduled Task/Job: Scheduled Task (T1053.005):** Creates scheduled tasks to maintain access after reboots.

DEFENSE EVASION:

- **Obfuscated Files or Information (T1027):** Uses obfuscated code to evade antivirus and endpoint detection tools.
- **Masquerading (T1036):** Renames malicious files to mimic legitimate software.



DISCOVERY:

- **System Information Discovery (T1082):** Gathers OS version, hostname, and other environment details using built-in commands like systeminfo.
- **Process Discovery (T1057):** Identifies running processes with tasklist or wmic for analysis and privilege escalation planning.
- **Security Software Discovery (T1518.001):** Scans for antivirus and endpoint protection software before proceeding.

CREDENTIAL ACCESS:

- **Credentials from Web Browsers (T1555.003):** Extracts stored passwords and session tokens from browsers like Chrome.
- **OS Credential Dumping (T1003):** Attempts to access password hashes using system utilities and tools.

COLLECTION:

- **Data from Local System (T1005):** Collects documents, browser data, Wi-Fi credentials, and screenshots from the victim's machine.

EXFILTRATION:

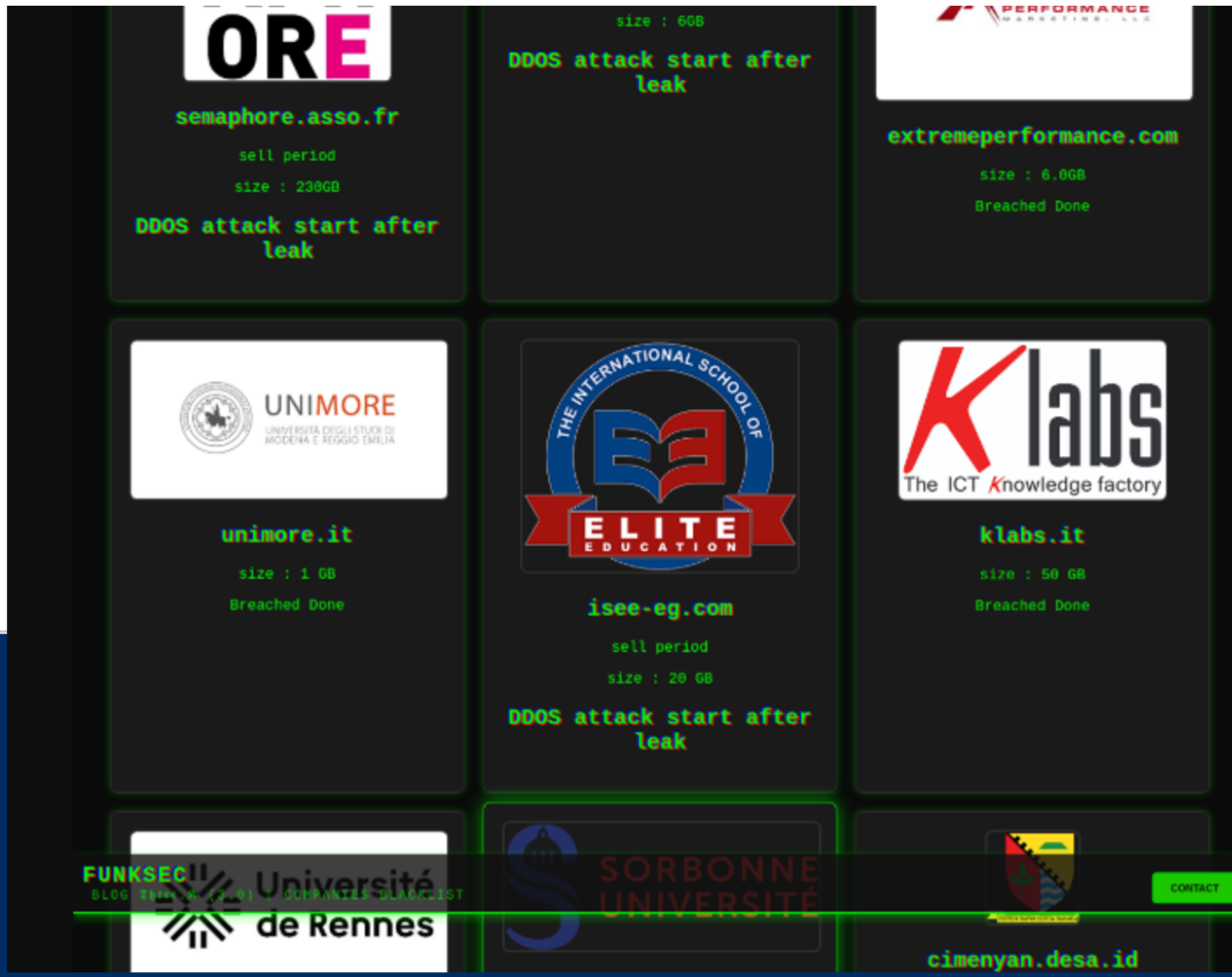
- **Exfiltration Over Web Service (T1567.002):** Stolen data is uploaded to services like gofile.io and the download link is sent via Telegram bots.
- **Automated Exfiltration (T1020):** Uses scripts to bundle and transmit stolen data automatically.

Attack Campaigns

FunkSec has conducted multiple low-sophistication, high-volume ransomware attacks since late 2024, primarily targeting government, education, and healthcare sectors in countries like India, the U.S., and Israel. Their campaigns typically begin with phishing emails delivering AI-generated malware, such as the Wolfer infostealer.

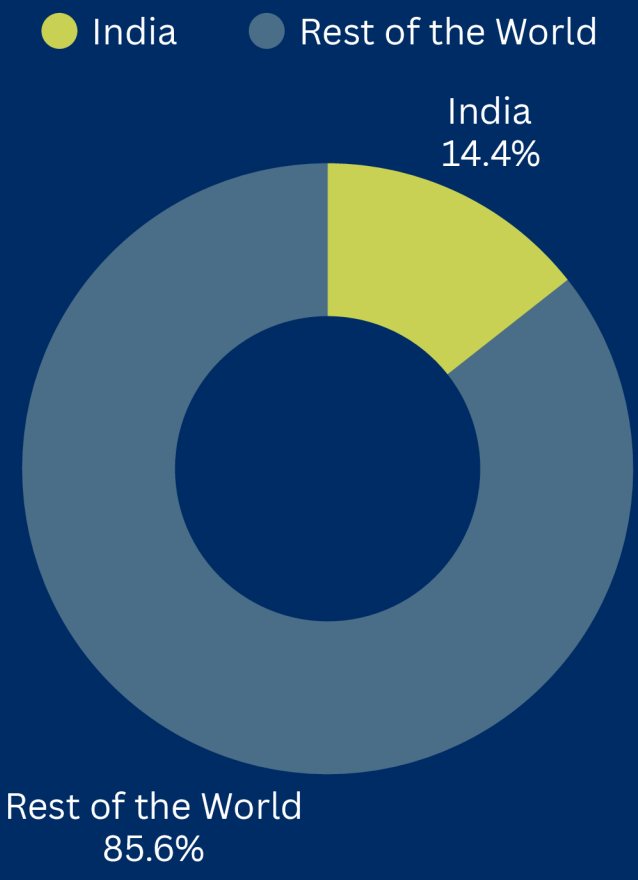
They focus on quick data exfiltration, followed by double extortion tactics—threatening to leak stolen data if ransoms aren't paid. Most attacks demand modest ransoms (~$10K) and rely heavily on public file-sharing services and Telegram bots for exfiltration and communication.

A notable campaign in early 2025 involved collaboration with FSociety, signaling their expansion efforts and growing ambitions within the ransomware ecosystem.



Targeting Preferences

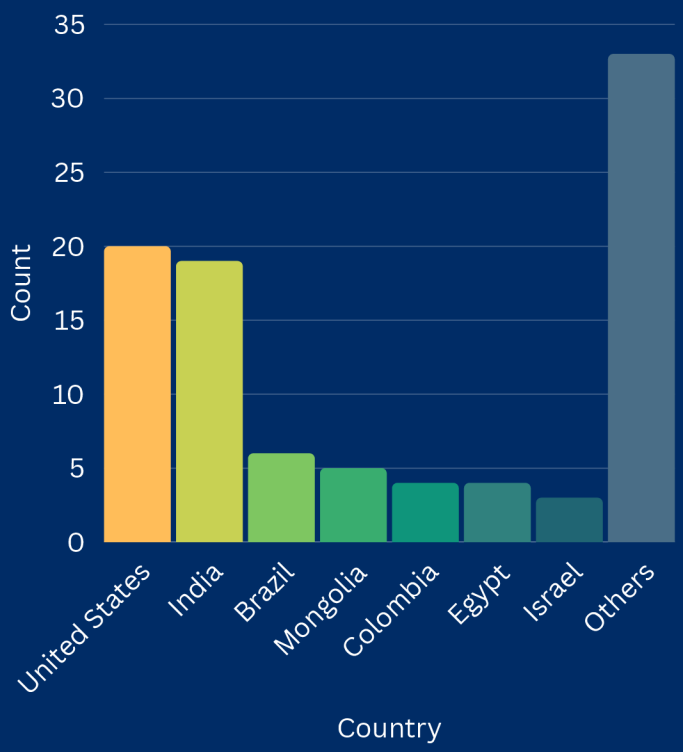
According to their Data Leak Site (DLS), FunkSec has been responsible for targeting organizations across various industries and geographic regions. Their attacks, as documented, provide insight into their operational focus and victim preference



FunkSec primarily targets small to mid-sized organizations with weaker cybersecurity defenses. Their main focus is on government agencies, educational institutions, and healthcare providers—especially in India, the U.S., and Israel. They prefer sectors with sensitive data and limited IT resources, making them more likely to pay modest ransoms quickly. FunkSec also occasionally selects targets based on political or symbolic value, reflecting its hacktivist roots.

Country Wise Targeting

Global Reach, Local Impact:
FunkSec's operations have affected victims across 47 countries, reflecting a truly global threat landscape. The United States (20 victims) and India (19 victims) are the top targets, followed by Brazil, Mongolia, and several countries in South America, Africa, and Asia. Their diverse targeting shows a blend of opportunism and strategic intent, particularly against nations with developing cybersecurity infrastructure.



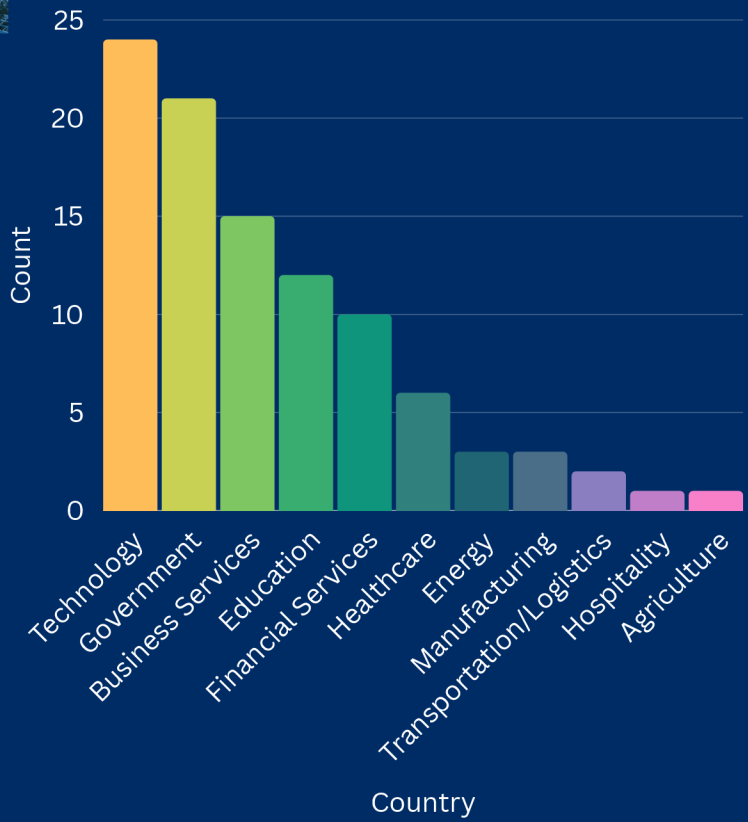
India Among Most Targeted by FunkSec

INSIGHTS:

- U.S. (20 attacks) – Most targeted, likely due to data value and digital dependency.
- India (19 attacks) – Significant focus, especially on government and public infrastructure.
- Brazil, Colombia, and Egypt (3–6 each) – Emerging hotbeds of ransomware targeting in Latin America and MENA.
- 33 countries with single-victim incidents show FunkSec's wide attack surface and automated campaign approach.

Industry Wise Targeting

FunkSec's operations have impacted multiple critical sectors, including technology, government, business services, education, and finance. In India, the group has increasingly targeted government agencies, educational institutions, and IT firms, indicating a focus on sectors that are vital to national infrastructure and digital operations.



Top Sectors Targeted by FunkSec

INSIGHTS:

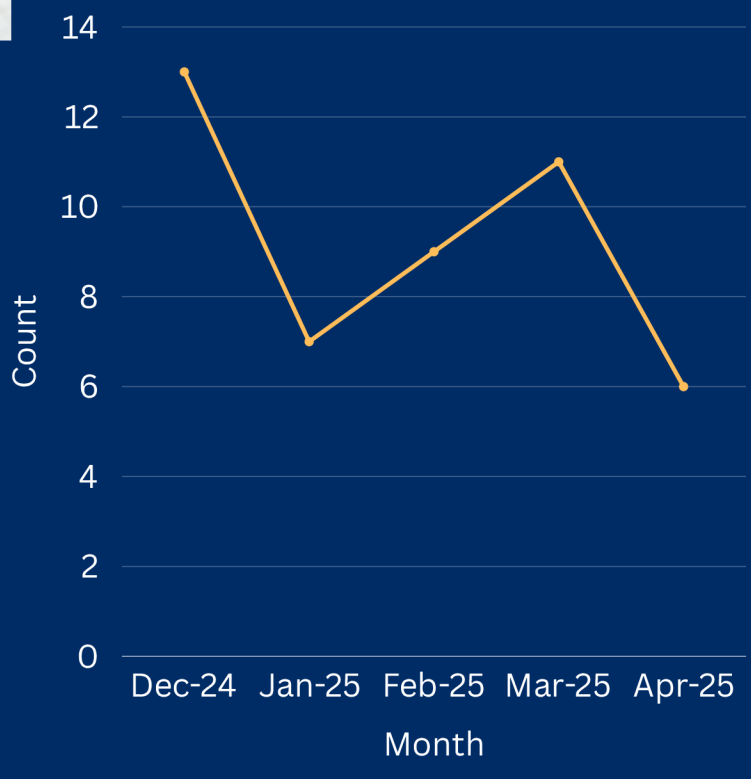
- Technology (24 attacks) is the top targeted sector, likely due to its high data value and ransomware profitability.
- Government (21 attacks) reflects an intent to disrupt essential public services, a key concern for India's growing digital governance model.
- Education & Finance (12 and 10 attacks) point to exploitation of sectors handling sensitive citizen data with often weaker security practices.
- India's inclusion across all top-targeted sectors indicates its growing prominence in both global cybercrime maps and regional threat landscapes.

Monthly Targeting

FunkSec's operations have shown a consistent presence in India over recent months. The group has targeted various sectors, with a noticeable concentration in the early months of 2025. This trend underscores the group's sustained interest in exploiting vulnerabilities within India's critical infrastructure and services.

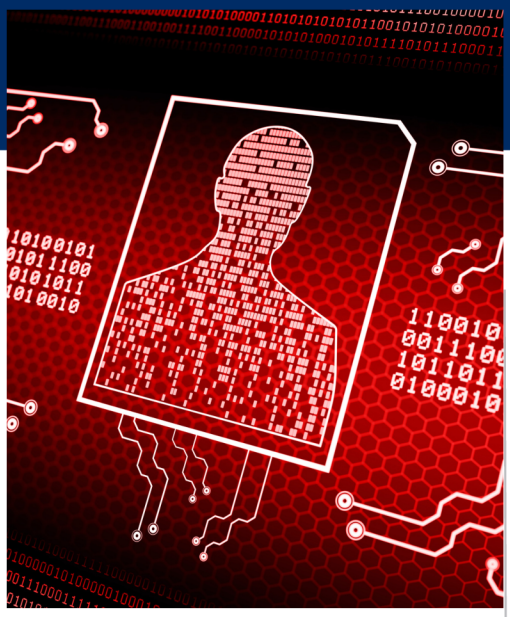
INSIGHTS:

- December 2024 witnessed a spike in attacks, indicating a possible testing phase or initial infiltration attempts.
- January to March 2025 saw steady activity, suggesting established footholds and continued exploitation.
- April 2025 shows a slight decline, which may reflect shifts in tactics or increased defensive measures by Indian organizations.



FunkSec Monthly Attack Trends

Attribution & Analysis



THREAT ACTORS

Type	Actor
Individual	Blako
Individual	El_Farado
Individual	Sentap
Individual	Scorpion (aka DesertStorm)
Individual	XTN
Individual	Bjorka

Key Threat Actors Behind FunkSec

1. Scorpion (aka DesertStorm)

- **Role:** Founder and primary promoter of FunkSec.
- **Background:** First introduced FunkSec in October 2024 via Breached Forum and a YouTube video. Initially claimed to be based in Russia, but evidence suggests a location in Algeria. Known for using AI-generated content to boost the group's profile.

2. El_Farado

- **Role:** Prominent promoter and spokesperson for FunkSec post-DesertStorm's ban.
- **Background:** Actively shared leaks and promoted FunkSec's activities on forums. Registered a Keybase profile simultaneously with Scorpionlord, indicating close collaboration.

3. XTN

Role: Associated with FunkSec's "data-sorting" services.

Background: Linked to FunkSec through forum interactions and shared signatures. Publicly cautioned DesertStorm about operational security lapses.

4. Blako

Role: Alleged associate of FunkSec.

Background: Tagged in posts by DesertStorm alongside El_Farado. Limited public activity, but Keybase registration aligns with other core members, suggesting involvement.

5. Bjorka

Role: Indonesian hacktivist with a murky connection to FunkSec.

Background: Known for previous hacktivist activities. Some FunkSec-related leaks have been attributed to Bjorka on DarkForums, though direct collaboration remains unconfirmed.

EXTORTION TYPES

Attack Victim Employees	Attack Victim Employees Families	Blackmail
Data Auctions	Direct Extortion	DoS
Double Extortion	Extortion Advertisements	Free Data Leaks
Victim Re-Attack		

COMMUNICATION

Medium	Identifier
miniapps.ai	[AI Chatbot] https[:]//miniapps[.]ai/funksec
	https[:]//miniapps[.]ai/u/yservos
Session Messenger	0538d726ae3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9efb3d
Twitter | X	https[:]//x[.]com/FunksecCM
BTC	bc1qrghnt6cqdsxt0qmlcaq0wcavq6pmfm82vtxfeq
Chat servers	http[:]//funk45xqgrkrtej4743evcgv65oi3w4shwvjx3cvrdtqwul7gzkxuxqd[.]onion/
Dark Web URL	http[:]//7ixfdvqb4eaju5lzj4gg76kwlrxg4ugqpuog5oqkkmgfyn33h527oyyd[.]onion/

News & Recent Developments

08th Dec 2024 – FunkSec attack on National Center for Financial Education

FunkSec ransomware group claimed responsibility for an attack on the National Centre for Financial Education (NCFE) in India. This incident was publicly disclosed on December 8, 2024, when FunkSec listed NCFE on their dark web leak site. The breach was identified by cybersecurity monitoring teams, highlighting the group's expanding focus on educational and financial institutions in India.

Key Details of the NCFE Breach

Domain: ncfe.org.in

Date Listed on Leak Site: December 8, 2024

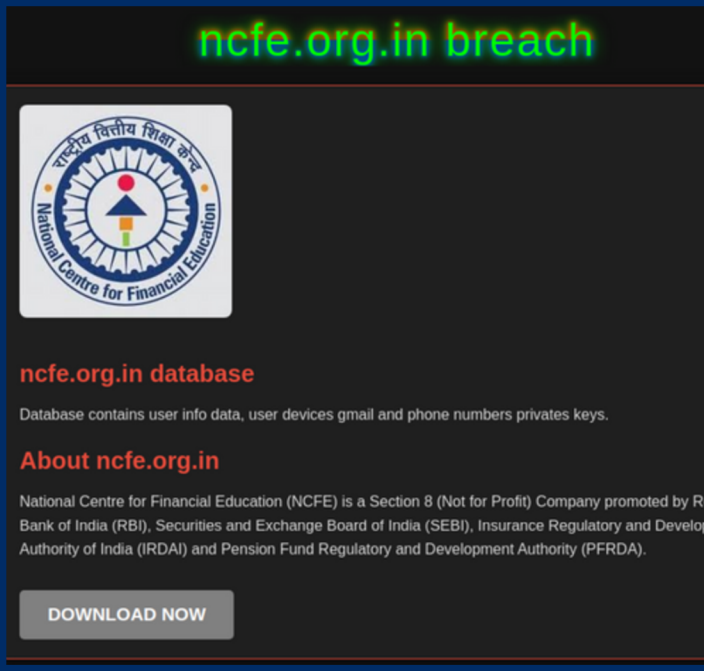
Sector Targeted: Financial education and awareness

Attack Method: Double extortion ransomware

Data Leaked: Approximately 50 GB

Data Compromised: Internal documents, backend screenshots, user records

Impact Noted: Risk to financial literacy initiatives and public trust



16th Dec 2024 – FunkSec attack on Indian Aerospace and Engineering

FunkSec ransomware group claimed responsibility for an attack on Indian Aerospace and Engineering, a prominent aviation training institute in Mumbai. The breach was publicly disclosed on December 16, 2024, when FunkSec listed the institution on their dark web leak site. This incident underscores the group's expanding focus on educational institutions within critical infrastructure sectors in India.

Key Details of the Indian Aerospace & Engineering Breach

Domain:
indianaerospaceandengineering.com

Date Listed on Leak Site: December 16, 2024

Sector Targeted: Aviation education and training

Attack Method: Double extortion ransomware

Data Compromised: Internal documents, backend system screenshots, user records

Data Leaked: Approximately 300 MB

Impact Noted: Potential disruption to aviation training programs and compromise of sensitive regulatory compliance documents

13th Jan 2025 – FunkSec attack on State Child Protection Society

FunkSec ransomware group claimed responsibility for an attack on the State Child Protection Society (SCPS) of Madhya Pradesh, India. The breach was publicly disclosed in mid-January 2025, when FunkSec listed SCPS on their dark web leak site. This incident underscores the group's expanding focus on governmental organizations involved in child welfare and protection in India.

Key Details of the SCPS Breach

Domain: scps.mp.gov.in

Date Listed on Leak Site: January 14, 2025

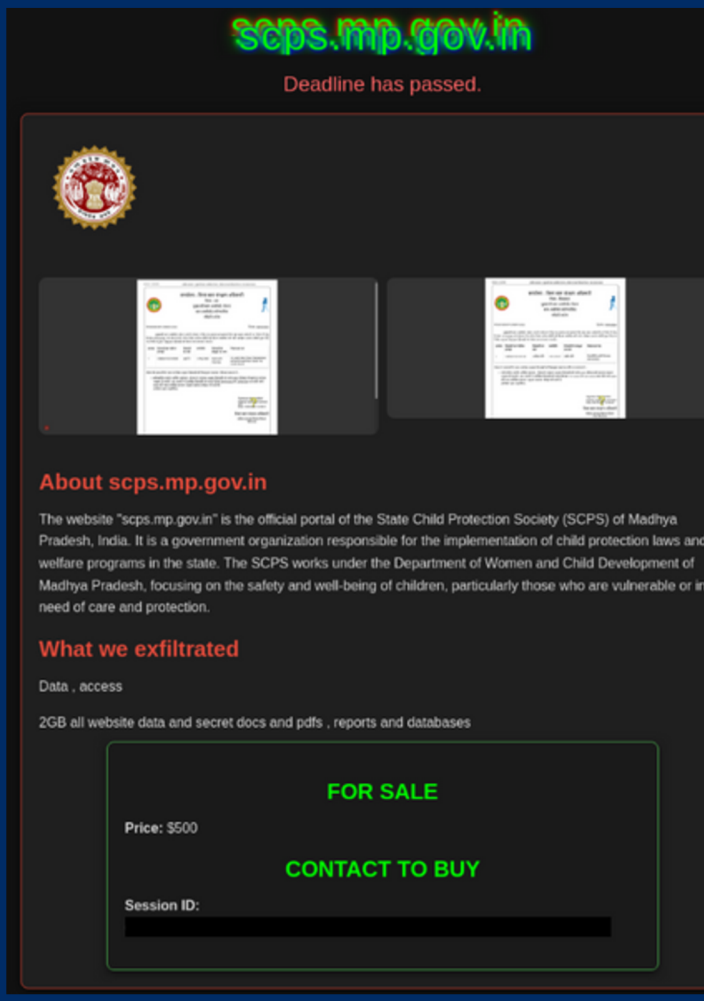
Sector Targeted: Child welfare and protection

Attack Method: Double extortion ransomware

Data Compromised: Internal documents, backend system screenshots, user records

Data Leaked: Approximately 2 GB

Impact Noted: Potential exposure of sensitive child welfare information and disruption to child protection services



26th Jan 2025 – FunkSec attack on Government of Punjab

FunkSec ransomware group claimed responsibility for an attack on the Government of Punjab, India. The breach was publicly disclosed on January 26, 2025, when FunkSec listed the government domain on their dark web leak site. This incident underscores the group's expanding focus on governmental organizations within India.

Key Details of the Punjab Government Breach

Domain: punjab.gov.in

Date Listed on Leak Site: January 23, 2025

Sector Targeted: State government administration

Attack Method: Double extortion ransomware

Data Compromised: Internal documents, backend system screenshots, user records

Data Leaked: Approximately 2.5 GB
Impact Noted: Potential exposure of sensitive governmental information and disruption to public services

28th Feb 2025 – FunkSec attack on StayzApp

FunkSec ransomware group claimed responsibility for an attack on StayzApp, a travel and accommodation booking platform based in India. The breach was publicly disclosed on February 28, 2025, when FunkSec listed StayzApp on their dark web leak site. This incident underscores the group's expanding focus on technology-driven service providers in India's travel and hospitality sector.

Key Details of the StayzApp Breach

Domain: stayzapp.in

Date Listed on Leak Site: February 28, 2025

Sector Targeted: Travel and hospitality technology

Attack Method: Double extortion ransomware

Data Compromised: Internal documents, backend system screenshots, user records

Data Leaked: Approximately 1.2 GB

Impact Noted: Potential exposure of customer booking information and disruption to service operations

Mitigation Strategies

To protect your organization from FunkSec and similar ransomware threats, it's essential to implement a multi-layered defence strategy:

1. Frequent Data Backups: Ensure all critical data is backed up regularly and stored securely, either offline or in isolated cloud storage, to minimize the impact of a ransomware attack.

2. Advanced Endpoint Security: Deploy next-gen endpoint security solutions that include behavioral analysis, anti-ransomware protection, and real-time threat detection to identify and block ransomware before it can execute.

3. Patch Management: Regularly update operating systems, software, and security systems to close vulnerabilities that ransomware could exploit.

4. Block PowerShell Script Execution: Disable or restrict the execution of PowerShell scripts via Group Policy (Turn on Script Execution set to Disabled) or using AppLocker/WDAC to prevent script-based payloads from executing during ransomware deployment.

5. Network Segmentation: Segment your network to limit lateral movement within your environment, preventing ransomware from spreading across all systems in the event of an infection.

11. Multi Factor Authentication (MFA): Enforce MFA for accessing sensitive systems to reduce the likelihood of unauthorized access or credential theft.

12. Monitoring Lateral Movement: Babuk has used tools like PSExec, RDP, and SMB for internal propagation. Network monitoring helps detect this movement early.

13. Macro Blocking: While not Babuk's primary vector, weaponized documents have been part of their phishing toolkit. Blocking macros disrupts initial access.

Combining these strategies, organizations can strengthen their defenses and minimize the risk of falling victim to FunkSec and similar ransomware threats.

6. Apply the Principle of Least Privilege: Restrict user access to only essential files and systems to prevent attackers from escalating privileges or encrypting critical data.

7. Monitor and Detect Suspicious Activity: Implement intrusion detection systems (IDS) and continuously monitor network traffic for unusual behavior, which may indicate ransomware infiltration.

8. RDP Hardening/Disabling: Initial access for Babuk has been gained via brute-force attacks on exposed RDP. Disabling or restricting RDP blocks a primary entry point.

9. Controlled Folder Access: Babuk encrypts files on servers and critical endpoints. Controlled Folder Access prevents unauthorized encryption attempts by ransomware binaries.

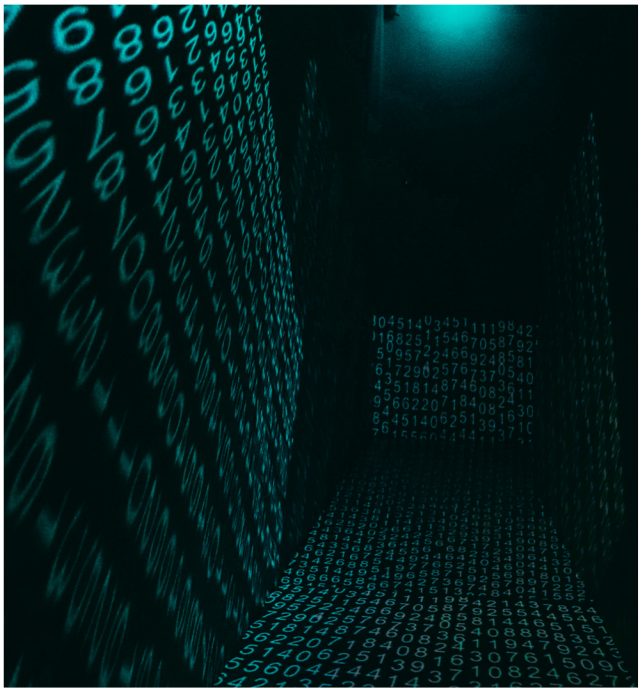
10. App Whitelisting WDAC or AppLocker: Babuk uses custom executables and scripts that can be blocked if not whitelisted. This strategy directly prevents execution of unknown payloads.

Conclusion

FunkSec's recent surge in ransomware activity, particularly against Indian institutions, reveals a calculated shift toward sectors where disruption can cause maximum chaos—education, government, finance, and public services. Their pattern of double extortion, wide sectoral reach, and increasing data leak volumes reflect a maturing threat actor with both capability and intent.

As India advances digitally, the stakes for protecting sensitive data and critical infrastructure grow exponentially. Proactive threat intelligence, stronger cyber hygiene, and swift response mechanisms are essential to staying ahead of groups like FunkSec.

The message is clear: In today's cyber battlefield, no sector is too small, and no data is too obscure to be targeted.



REFERENCES

Watchguard

- https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/funksec

SOCRadar

- https://socradar.io/dark-web-profile-funksec/

Check Point

- https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/funksec-ransomware-ai-powered-group/

Ransomware Live

- https://www.ransomware.live/group/funksec

State of New Jersey

- https://www.cyber.nj.gov/Home/Components/News/News/1574/214

Ransomlook

- https://www.ransomlook.io/group/funksec