Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

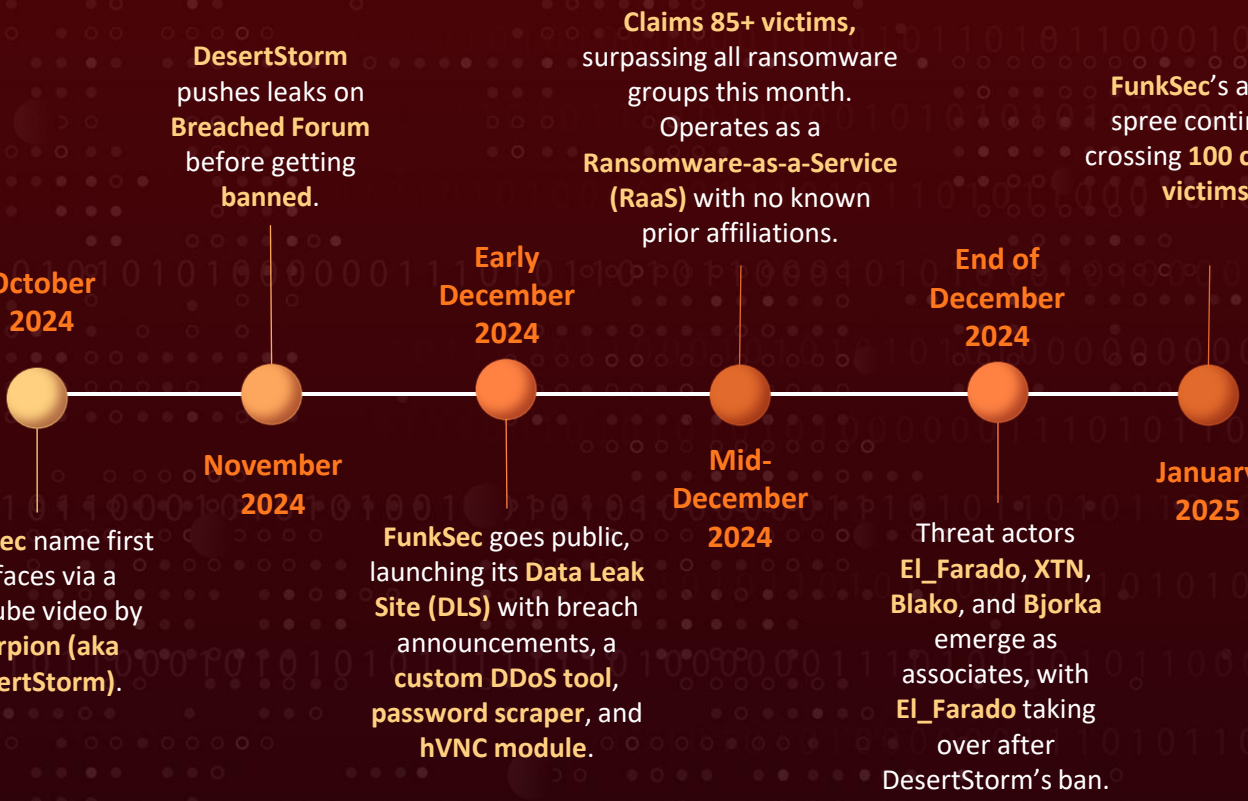
Fast-Tracking FunkSec Ransomware with the Twist of AI-Driven Havoc

Date of Publication	Admiralty Code	TA Number
January 31, 2025	A1	TA2025026

Summary

Active Since: December 2024
Malware: FunkSec Ransomware
Targeted Industries: Government, Defense, Manufacturing, Technology, Business Services, Media, Fashion, Education, Automotive, Professional Services, Environmental Services, Retail, Electronics, Information Technology, Hospitality, Energy, Financial Services, Transportation, Charitable Organizations, Agriculture
Targeted Countries: United States, India, Italy, Brazil, Israel, Spain, Mongolia, South Africa, Uganda, United Kingdom, Nigeria, Algeria, Bangladesh, Paraguay, Pakistan, United Arab Emirates, Greece, Mexico, Germany, Jordan, South Korea, Myanmar, Egypt, Colombia, Russia, Morocco, Canada, Poland, Tunisia, France, Thailand, Peru, Qatar
Attack: FunkSec made a splash in late 2024, quickly becoming one of the most active ransomware groups. With AI-driven tools and a mix of cybercrime and hacktivism, they've claimed dozens of victims in a matter of weeks. Operating under the radar, FunkSec's ransomware evolves fast, demanding low ransoms and leaving security teams scrambling. Who's behind it? A mix of shady figures, but one thing's clear FunkSec is a force to watch in the growing world of AI-powered cyber threats.

Attack Timeline



Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 FunkSec burst onto the ransomware scene in late 2024, quickly becoming the most active group by December, with over 85 claimed victims in a matter of weeks. What sets FunkSec apart isn't just the speed of its operations but its heavy reliance on AI-assisted malware development. This approach lowers the technical barrier, allowing even inexperienced actors to generate and iterate ransomware rapidly.

#2 While FunkSec presents itself as a politically motivated hacktivist group, much of its leaked data appears to be recycled from older breaches, casting doubt on its credibility. The group's tactics blend hacktivism with cybercrime, making its true motives difficult to pin down. Its Data Leak Site (DLS) serves as a hub for extortion, featuring breach announcements, a Python-based DDoS tool, and its custom ransomware, now offered as Ransomware-as-a-Service (RaaS).

#3 FunkSec's ransomware, written in Rust, employs RSA and AES encryption, appends a ".funksec" extension to encrypted files, and aggressively disables security features. The group demands surprisingly low ransoms sometimes as little as $10,000 and resells stolen data at discounted rates on cybercrime forums.

#4 FunkSec claims to target India and the U.S., aligning itself with the "Free Palestine" movement while also attempting to associate with defunct hacktivist groups like Ghost Algeria and Cyb3r Fl00d. Several key figures are linked to FunkSec, though their exact roles vary.

#5 Scorpion (aka DesertStorm), likely based in Algeria, was one of the group's main promoters on cybercrime forums before being banned. El_Farado stepped in to handle publicity, despite displaying limited technical expertise.

#6 XTN is believed to be involved in an ambiguous "data-sorting" service, while Blako has been mentioned alongside El_Farado in group-related discussions. Meanwhile, the alias Bjorka, tied to Indonesian hacktivism, has surfaced in connection with FunkSec leaks on DarkForums potentially indicating collaboration or an impersonation attempt.

#7 AI plays a central role in FunkSec's operations, from malware development to automation. FunkSec has even experimented with AI-powered chatbots to assist in cybercrime activities. FunkSec claims to have breached a Dubai Civil Defense sub-portal, but the leaked data appears outdated, indicating it may have come from an inactive or abandoned system rather than a live target.

#8 FunkSec's rapid evolution highlights a growing trend: AI is making sophisticated cyber threats more accessible to lower-skilled actors. As AI-generated malware continues to advance, traditional detection methods will struggle to keep up. Their focus on low ransom demands and high-volume attacks indicates a strategy aimed at maximizing visibility rather than solely financial gain.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Implement Strong Endpoint Security: FunkSec uses advanced techniques such as remote desktop control tools (hVNC) and a DDoS tool in addition to ransomware. Organizations should deploy strong endpoint detection and response (EDR) tools that can prevent lateral movement, system manipulation, and remote access by ransomware actors

AI-Based Cyber Defense Strategies: Since FunkSec allegedly utilizes AI for malware development, defenders must counter AI with AI. Deploying behavioral AI-driven endpoint protection and anomaly-based detection can help identify irregular patterns indicative of AI-generated malware before execution.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1057** Process Discovery	**T1071** Application Layer Protocol
T1587 Develop Capabilities	**T1587.001** Malware	**T1486** Data Encrypted for Impact	**T1498** Network Denial of Service
T1543 Create or Modify System Process	**T1055** Process Injection	**T1070** Indicator Removal	**T1070.004** File Deletion
T1213 Data from Information Repositories	**T1083** File and Directory Discovery	**T1041** Exfiltration Over C2 Channel	**T1059** Command and Scripting Interpreter
T1140 Deobfuscate/Decode Files or Information	**T1560** Archive Collected Data	**T1588.007** Artificial Intelligence	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966, 7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603
TOR Address	7ixfdvqb4eaju5lzj4gg76kwlrxg4ugqpuog5oqkkmgfyn33h527oyyd[.]onion, pke2vht5jdeninupk7i2thcfvxegsue6oraswpka35breuj7xxz2erid[.]onion, ykqjcrptcai76ru5u7jhvspkeizfsvpgovton4jmreawj4zdwe4qnlid[.]onion, funkxxkovrk7ctnggbjnthdajav4ggex53k6m2x3esjwlxrkb3qiztid[.]onion, funknqn44slwmgwgnewne6bintbooauwkaupik4yrlgtycew3ergraid[.]onion

Recent Breaches

https://www.builders.co.za/
https://qed.co.ug/
https://treehotel.co.uk/
https://achieverssciencejournal.org/ajosrojs/index.php/ajosr/index
https://www.foxblossom.com/
https://technotouch.co/
https://navy.mil.bd/

https://gsw.co.in/
https://www.traditiondata.com/
https://ndc.energy.mn/
https://www.kurosu.com.py/
https://barilga.gov.mn/
https://ribernuez.com/
https://genrepurchase.bankatm.in/
https://senergy.net/
https://www.mindev.gov.gr/
https://www.linxe.com/
https://ndceg.com/odeysysportal/login/loginForm
http://www.funkforum.net/
https://equitiesfirst.com/hk/
https://www.citybankplc.com/home
https://carc.gov.jo/
https://iptime.com/iptime/
https://ayswrewards.com/
https://bluai.ai/
http://kuzstu-nf.ru/
https://www.wissenhive.com/
https://seocommarrakech.com/
https://abd.ong/
https://scps.mp.gov.in/
https://www.sklepbaterie.pl/
https://www.dcd.gov.ae/portal/en/

References

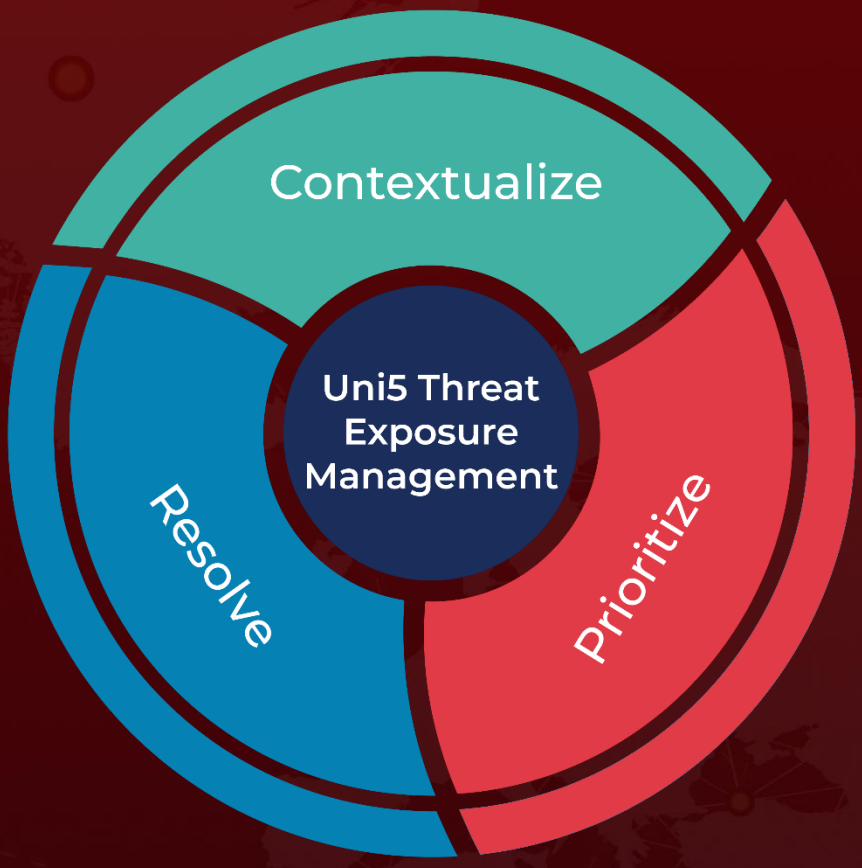
https://research.checkpoint.com/2025/funksec-alleged-top-ransomware-group-powered-by-ai/

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 31, 2025 . 5:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com