

HiveForce Labs

# THREAT ADVISORY

 **ATTACK REPORT**

## **FunkLocker: Emerging AI-Assisted Ransomware**

Date of Publication

October 3, 2025

Admiralty Code

A1

TA Number

TA2025304

# Summary

**First Seen:** December 2024

**Targeted Countries:** United States, India, Spain, Mongolia, Italy, Brazil, Israel

**Malware:** FunkLocker Ransomware

**Affected Platform:** Windows

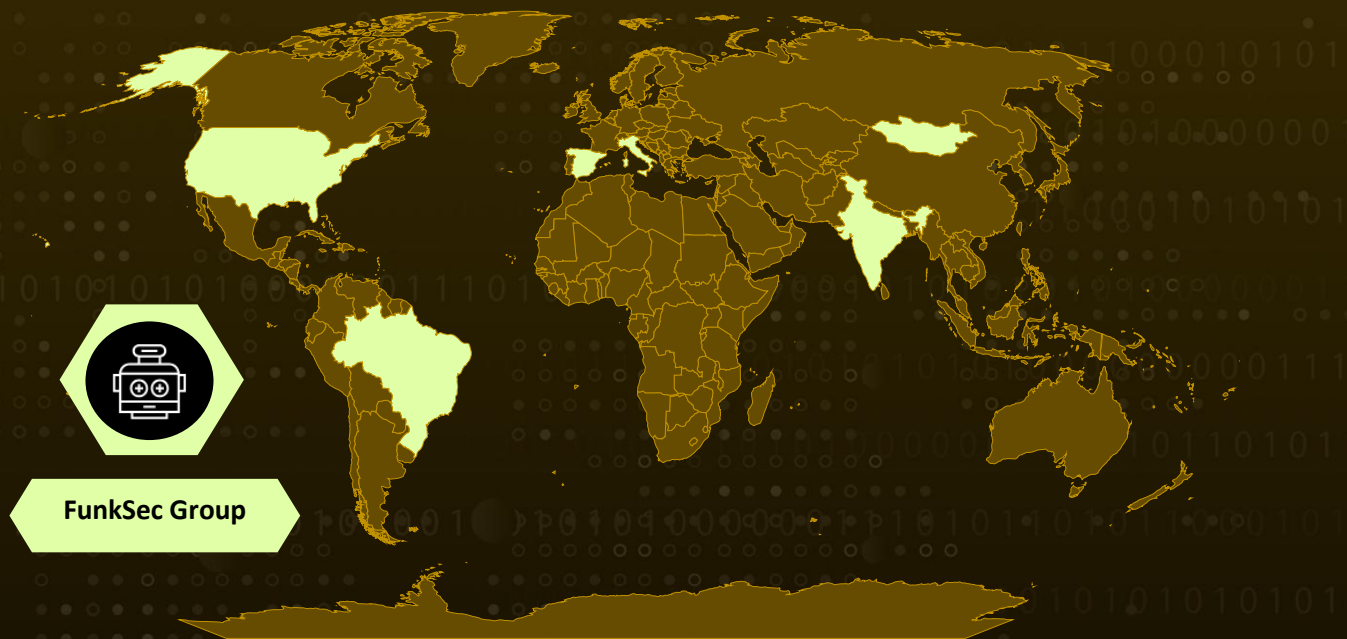
**Targeted Industries:** Government, Defense, Finance, Higher Education

**Threat Actor:** FunkSec Group

**Attack:** FunkLocker is an AI-assisted ransomware strain developed by the FunkSec group, which operates under a ransomware-as-a-service model. The group blends cybercrime and hacktivism, targeting a wide range of public and private sector organizations worldwide. Ransom demands are relatively low typically around 0.1 Bitcoin, encouraging faster payments and increasing the number of victims. The ransomware encrypts files locally using a combination of RSA-2048 and AES-256 encryption, appending the .funksec extension to affected files.



## Attack Regions



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

# Attack Details

## #1

FunkLocker is a recently identified ransomware strain developed by a group known as [FunkSec](#). Unlike many ransomware campaigns that rely on external servers or sophisticated communication channels, FunkLocker operates locally on the infected system. Once deployed, it takes aggressive steps to disrupt a computer by stopping critical processes, disabling security tools, and preventing system recovery. This is achieved by misusing built-in Windows utilities such as taskkill.exe, sc.exe, and PowerShell, which makes its actions blend into normal system operations at first glance.

## #2

After disabling defenses, FunkLocker proceeds to encrypt the victim's files. Encrypted files are marked with the .funksec extension, rendering them inaccessible until a ransom is paid. The malware does not attempt to establish communication with a command-and-control server, which is unusual compared to other modern ransomware families. While this design limits its ability to spread dynamically or receive instructions, it also reduces opportunities for defenders to detect its presence early through network monitoring.


## #3


FunkLocker appears to be partially generated with the assistance of artificial intelligence. This allows its creators to rapidly develop and modify new versions of the malware. However, this approach has also introduced errors and inconsistencies into the code, such as hardcoded encryption keys and the reuse of the same cryptocurrency wallets across multiple attacks. These flaws have made it possible for researchers to develop free decryption tools, reducing the effectiveness of FunkLocker in some cases.


## #4


Despite its shortcomings, FunkLocker has already had a significant impact. Over 120 organizations worldwide have been targeted, with a particular focus on government agencies, defense contractors, financial institutions, and universities. Victims have been reported in countries including the United States, India, Spain, and Mongolia. The broad range of targets highlights the opportunistic nature of the campaign, as the attackers seek to maximize disruption and ransom payouts. Its emergence underscores the growing trend of AI-assisted cybercrime and the challenges defenders face in anticipating and responding to these threats.

# Recommendations

- 

**Preventive Security Measures:** Implementing strong preventive controls is essential to stop FunkLocker before it can execute. Application whitelisting should be used to block unapproved software and scripts, particularly those exploited by the ransomware, such as PowerShell, taskkill.exe, and sc.exe. Ensuring endpoints are fully patched and protected with advanced security solutions reduces the risk of successful infiltration. Limiting administrative privileges further prevents ransomware from stopping services or accessing critical files.
- 

**Network Segmentation and Access Controls:** Limit ransomware lateral movement by segmenting networks and enforcing least privilege policies for administrative access.
- 

**Implement Strong Access Controls:** Enforce the principle of least privilege for users and services. Limit administrative rights and restrict access to sensitive data to only necessary personnel. This reduces the potential for ransomware to spread laterally across networks.
- 

**Conduct Regular Data Backups and Test Restoration:** Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an FunkLocker ransomware attack, up-to-date backups enable recovery without paying the ransom.

## Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0007</u> Discovery
<u>TA0005</u> Defense Evasion	<u>TA0040</u> Impact	<u>TA0042</u> Resource Development	<u>T1588</u> Obtain Capabilities
<u>T1036.005</u> Match Legitimate Name or Location	<u>T1036</u> Masquerading	<u>T1569</u> System Services	<u>T1569.002</u> Service Execution

<b><u>T1007</u></b> System Service Discovery	<b><u>T1489</u></b> Service Stop	<b><u>T1059.001</u></b> PowerShell	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1135</u></b> Network Share Discovery	<b><u>T1490</u></b> Inhibit System Recovery	<b><u>T1562.001</u></b> Disable or Modify Tools	<b><u>T1562</u></b> Impair Defenses
<b><u>T1587</u></b> Develop Capabilities	<b><u>T1587.001</u></b> Malware	<b><u>T1486</u></b> Data Encrypted for Impact	<b><u>T1498</u></b> Network Denial of Service
<b><u>T1588.007</u></b> Artificial Intelligence			

## ✂ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033
<b>Filepath</b>	C:\Users\admin\Desktop\README-ZasRvdSR44.md

## ✂ Recent Breaches

<https://semaphore.asso.fr>  
<https://sanirent.com.mx>  
<https://unimore.it>  
<https://extremepformance.com>  
<https://isee-eg.com>  
<https://the-lastcompany.com>  
<https://klabs.it>  
<https://univ-rennes.fr>  
<https://sorbonne-universite.fr>  
<https://cimenyan.desa.id>

## References

<https://any.run/cybersecurity-blog/funklocker-malware-analysis/>

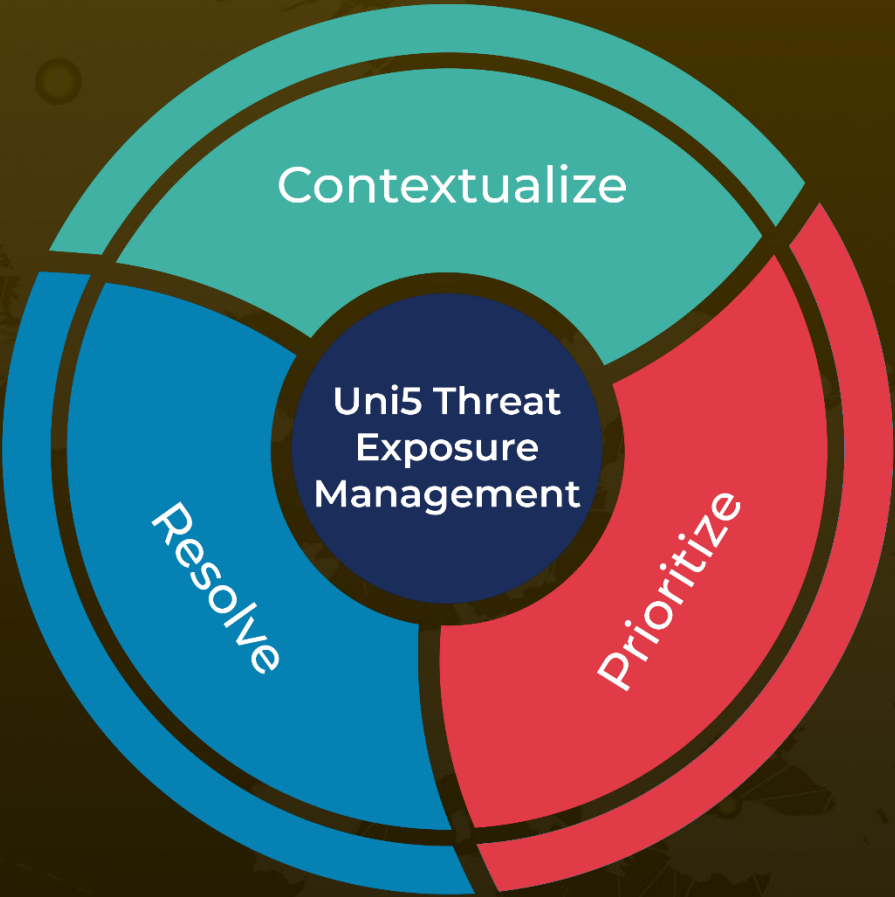
<https://www.sentinelone.com/anthology/funklocker/>

<https://hivepro.com/threat-advisory/fast-tracking-funksec-ransomware-with-the-twist-of-ai-driven-havoc/>

# 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

October 3, 2025 • 10:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)