FunkSec's FunkLocker: How AI Is Powering the Next Wave of Ransomware

Mauro Eldritch ⋮ ⋮ 10/1/2025

FunkSec's FunkLocker: How AI Is Powering the Next Wave of Ransomware

AI is part of our lives whether we like it or not. Even if you are not quite a fan, or not a user at all, you probably came across multiple AI-generated avatars, pictures, scenes, videos, articles and even malware.

All technological advancements are taken advantage of by society. They were discovered to be used, but some people just abuse them, and AI used for software development is not the exception.

This time we'll analyze FunkLocker, a ransomware strain by the FunkSec Ransomware group, whose creation was aided in an important part by artificial Intelligence.

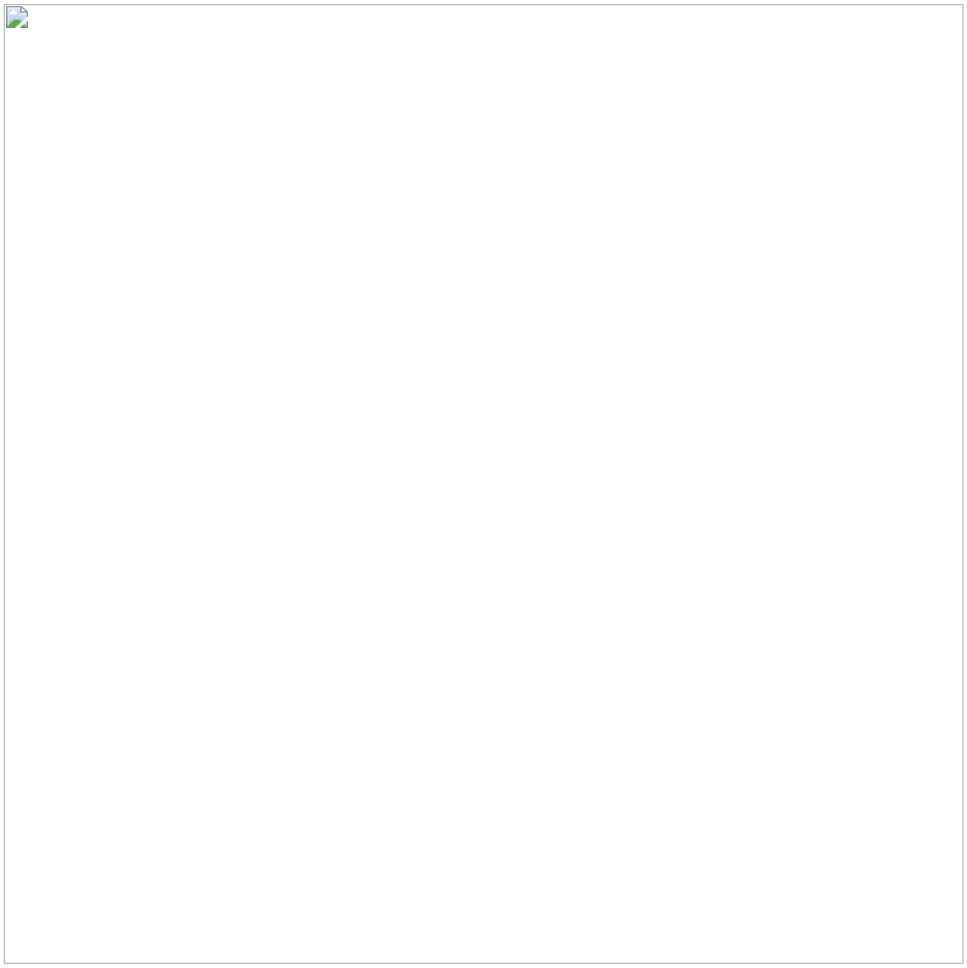
Key Takeaways

- **AI-assisted development:** FunkSec ransomware strains, including FunkLocker, show signs of "AI snippet" coding patterns (Ask AI → Paste snippet), making them easy to build but inconsistent in quality.
- **Multiple builds, mixed stability:** Some versions are barely functional, while others integrate advanced features such as anti-VM checks.
- **Aggressive disruption:** FunkLocker forcefully terminates processes and services using predefined lists, often causing unnecessary errors but still leading to full system disruption.
- **System tools abused:** Legitimate Windows utilities like taskkill.exe, sc.exe, net.exe, and PowerShell are heavily misused to stop apps, disable defenses, and prepare for encryption.
- **Local-only encryption:** Unlike many modern ransomware groups, FunkSec encrypts files locally without contacting a command-and-control server, using the .funksec extension.
- **Ransom note quirks:** Notes are dropped on the desktop, but system instability sometimes prevents victims from viewing them without a reboot.
- **Weak operational security:** Reused BTC wallets and locally derived or hardcoded keys suggest sloppy practices. This has allowed researchers (e.g., Avast Labs) to build a **public decryptor** for FunkSec victims.
- **Key MITRE ATT&CK techniques**: FunkLocker activity maps to techniques such as Masquerading (T1036.005), Service Stop (T1489), PowerShell execution (T1059.001), Network Share Discovery (T1135), and Inhibit System Recovery (T1490), among others.
- **Detection and Response**: SOCs can utilize ANY.RUN's Interactive Sandbox to safely detonate samples of FunkLocker, identify its malicious activities in seconds, and gather critical threat insights for fast mitigation of the attack.

Artificial Intelligence, Natural Evil

This is not the first time we see AI-aided malware, or even malware fully written by an AI. Just recently, another strain, PromptLocker, made it to the news, even though it was an educational non-malicious project. But FunkSec has been active for quite a while and even managed to publish many victims in their DLS.

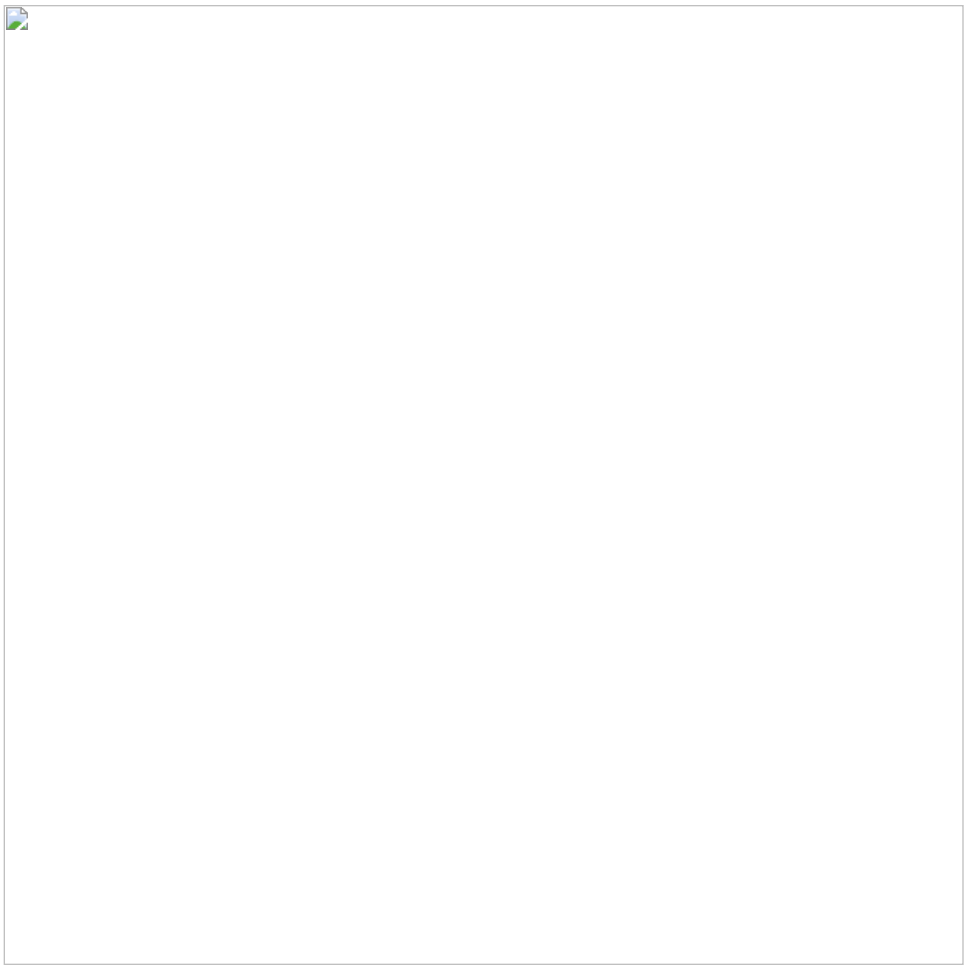
There are many samples, some more stable than others, and a few barely functional. Interestingly, the older builds (dating back to January of this year) included an anti-VM capability that detected virtualized environments with high accuracy before refusing to run.



A FunkSec strain refusing to run

That build was also characterized by its livid colours displayed in the terminal text while running. This one, found in late July, features a monochromatic style and is missing the anti-VM feature. While this could indicate it being an older build, the lack of a standardized versioning schema, like other groups such as LockBit, makes it hard to confirm.

Here is FunkSec's AI-assisted ransomware sample analyzed inside ANY.RUN's sandbox:



FunkLocker execution inside ANY.RUN's Interactive Sandbox

The sandbox exposes the threat in seconds, providing an actionable TTP and IOC report for fast, confident response and mitigation.

Detect threats faster with ANY.RUN's Interactive Sandbox
See full attack chain in seconds for immediate response

Get started with business email

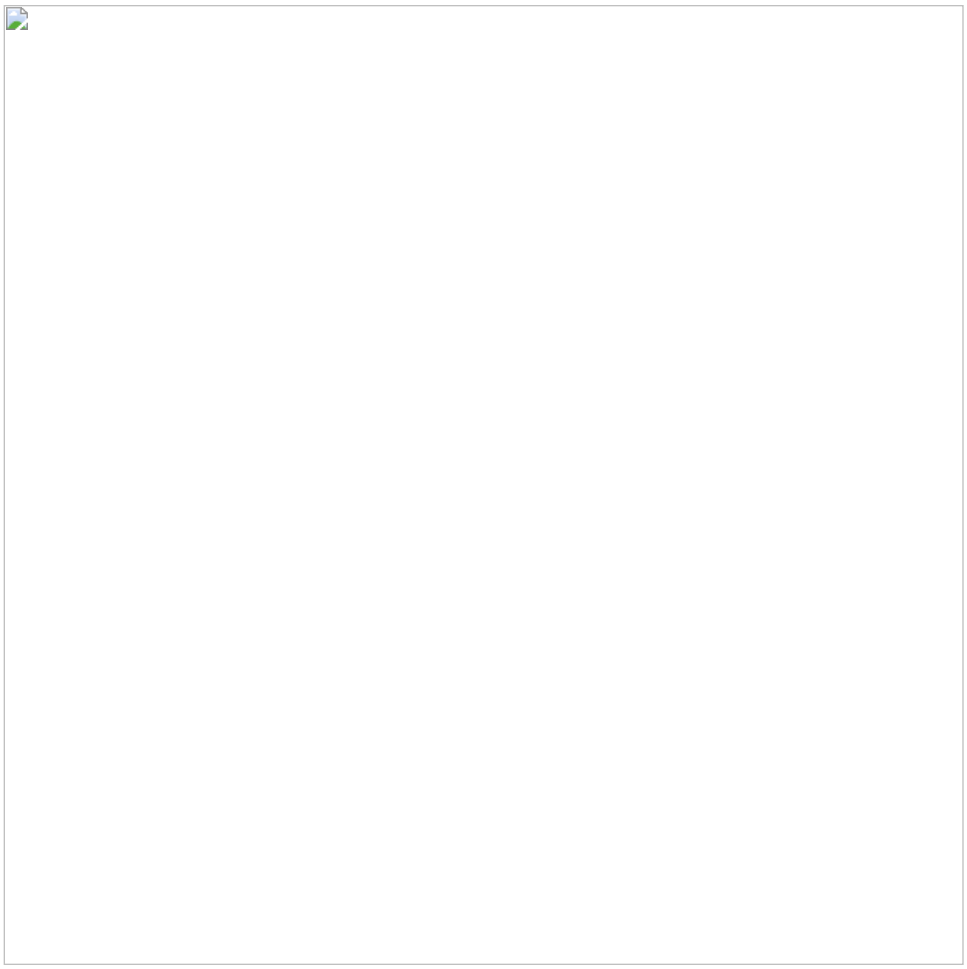
Victims and Target Regions

By early 2025, FunkSec had been linked to more than 120 compromized organizations worldwide, hitting targets in government institutions, the defense sector, tech companies, financial services, and higher education.

The group's first reported attacks surfaced in November 2024, and in December they launched a dedicated data leak site to publicize stolen information. Since then, the tally of known victims has continued to grow, with estimates ranging from 120 to 170, and some trackers recording as many as 172 cases. Notably, at least 30 of these incidents involved organizations in the United States, alongside confirmed cases in India, Spain, and Mongolia.

Execution and Process Disruption

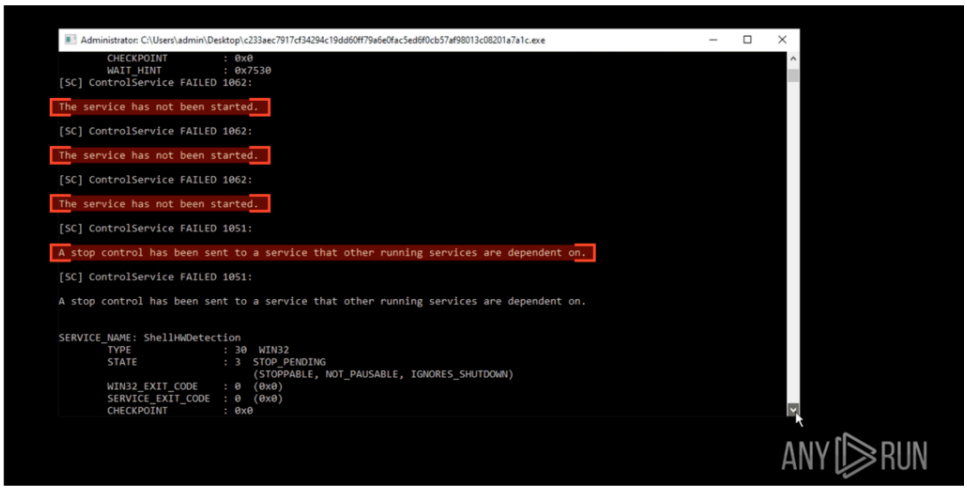
Immediately after execution, all our setup will go dark, and this is caused by the malware bashing its way through different processes in order to stop them. Why bashing? Because it doesn't take a fraction of a second to list the running applications and stop them in a strategic way; it just acts on a predefined list, causing multiple errors when trying to stop non-existing ones.



FunkLocker bashing through processes, bat in hand

It will also attempt to stop multiple services, again, matching them with a hardcoded predefined list, causing another set of errors. Some of these occur because the services are not running at all, and others because they simply can't be stopped due to dependencies from other services that rely on them to function.

This seems like the result of someone individually studying which services to stop and adding them to a list, without adding a layer of context on which ones depend on others or which ones could actually not be running (optional).

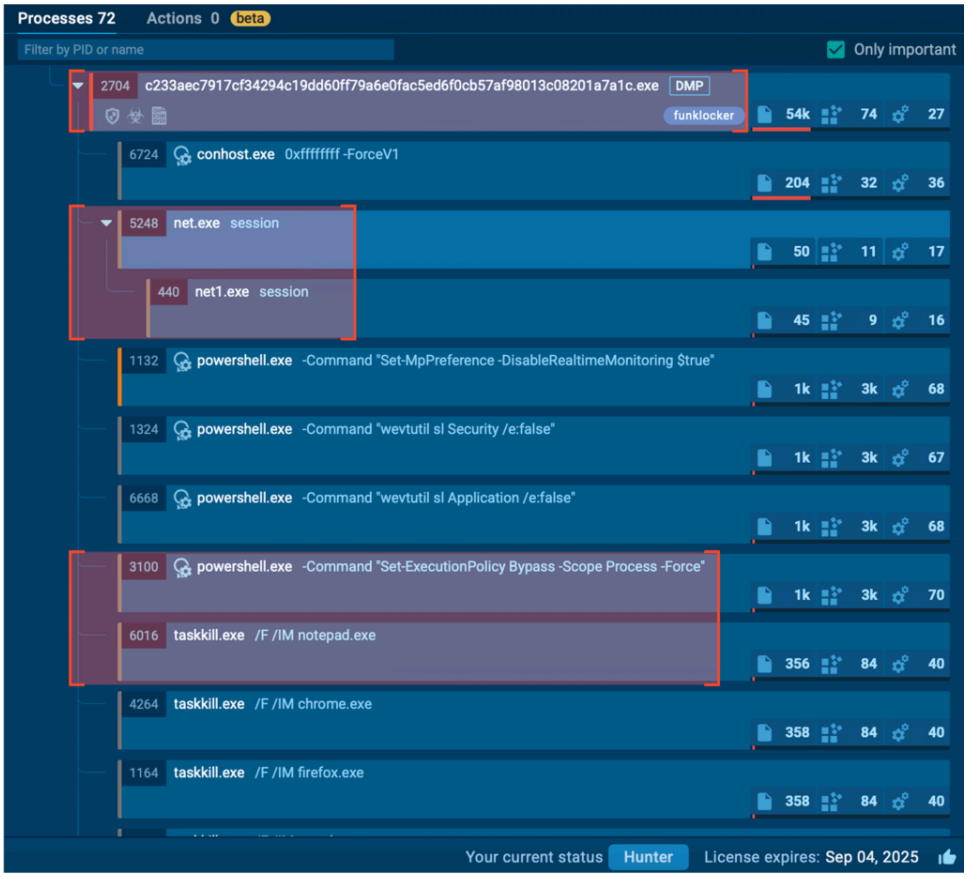


Applications being stopped forcefully

This doesn't stop the malware from continuing its raid, and eventually the file system is encrypted. The first and most obvious change is the extension of our files, which is now .funksec, but there's more than meets the eye.

Let's take a look at the process tree behind the sample. FunkLocker — aside from clubbing everything in its reach — is pretty "structured", where each of its steps is represented by a legit system tool being abused or a PowerShell

script executed procedurally, suggesting an “Ask AI → Get snippet → Paste snippet” development cycle.



FunkLocker’s process tree shown in ANY.RUN’s Interactive Sandbox

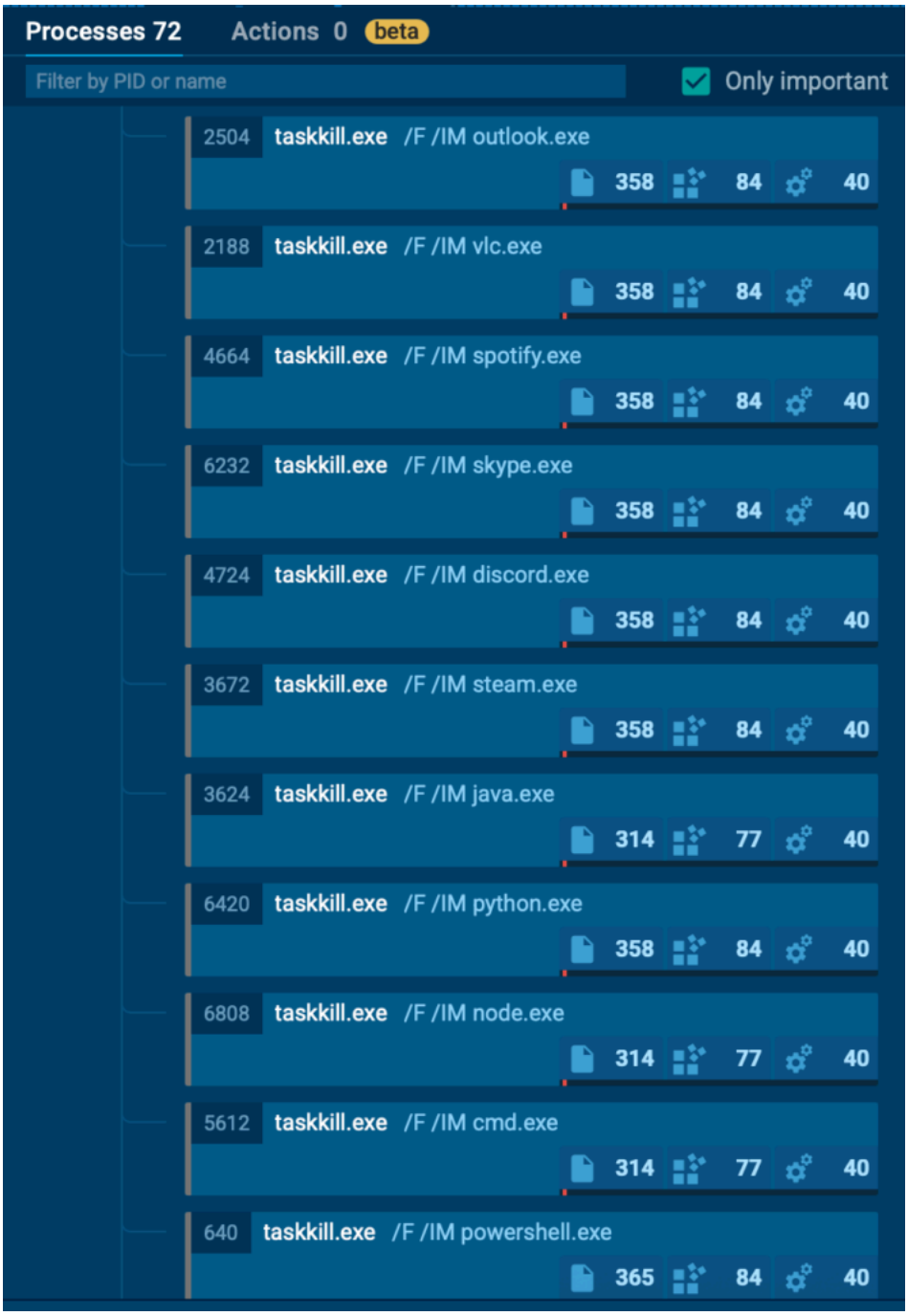
PowerShell and System Abuse

The PowerShell routine is based on four commands:

- The first one stops Windows Defender via DisableRealtimeMonitoring.
- The second one relies on wevtutil to deactivate Security Events logging.
- The third one uses wevtutil again to deactivate Application Events logging.
- The fourth and final one sets the Execution Policy to Bypass, allowing unrestricted PowerShell execution during that session.

Abused tools include net.exe and its compatibility-mode counterpart net1.exe, used to check if there are any network sessions established.

taskkill.exe is used naturally to stop applications or tasks — in this case used to forcefully stop browsers like Chrome, Firefox, and Edge, daily-use apps like Notepad, Skype, Spotify, programming environments like Java, Python, and Node, and even Steam, among a long list of other apps.

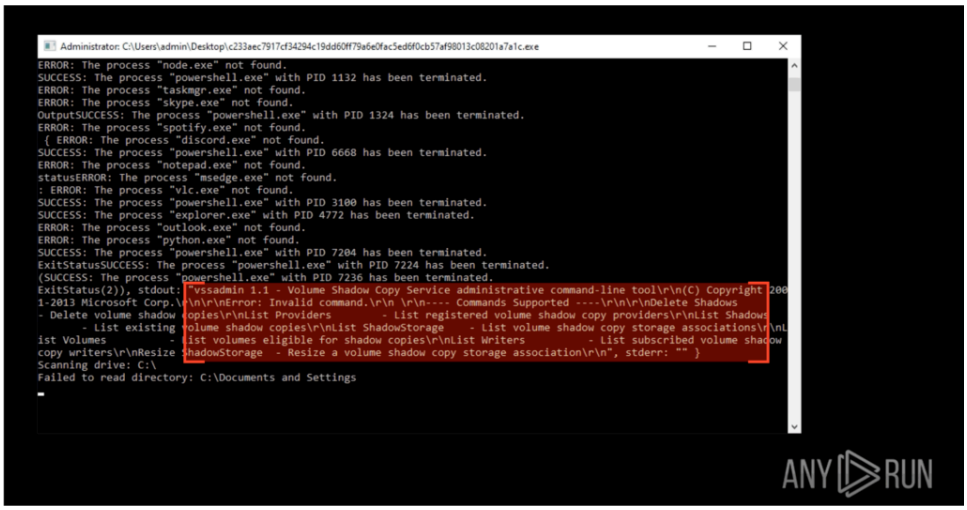


Arbitrary list of apps to be stopped

sc.exe, which is Windows Service Control, is used as a tool (or club) to stop services like Windows Defender & Firewall, SMB (Shared Folders), the Event Log, the Shell Experience Host (which is why our screen turns black), and other absolutely not-necessary services like Bluetooth or Audio.

Encryption and Ransom Note

After that, Shadow Volume Copies are taken care of, deleted, by abusing the Volume Shadow Service Administrator (vssadmin) to wipe them silently. This prevents the victim from locally restoring the system to a previous state, effectively removing any chance of rollback using Windows' built-in recovery mechanisms.



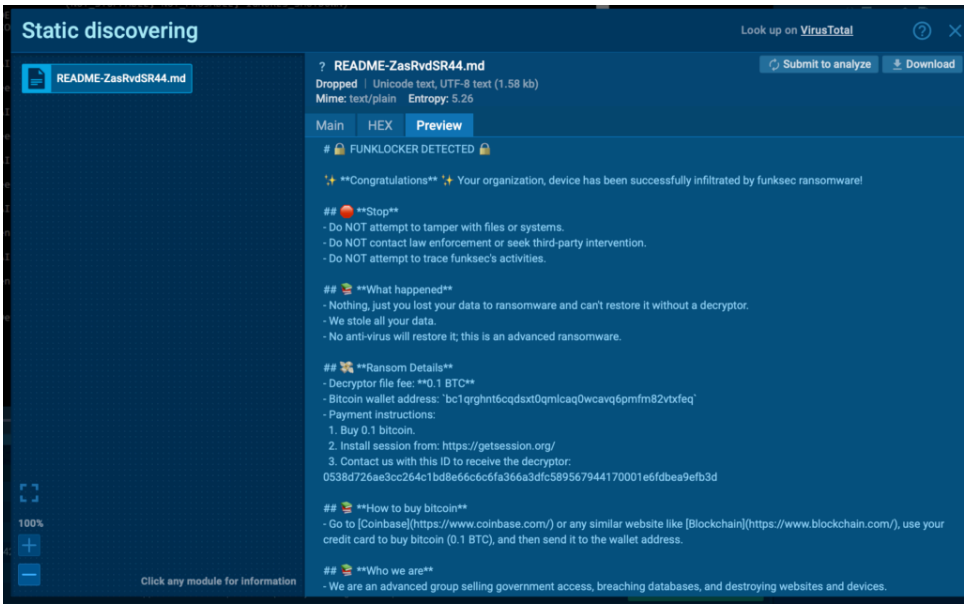
The ransomware deletes Shadow Volume Copies

Now for the encryption part — FunkLocker didn't attempt to contact a remote server at any time, as all the encryption process occurred locally. We've seen similar behavior in a previous article when we analyzed Mamona Ransomware.

While this may seem like it could make the malware easier to hide and harder to track — due to the lack of network infrastructure in the short term — it is beneficial in the long run, and you'll soon see why.

The ransom note is dropped right on the desktop but, with the unnecessary killing of the Shell Experience Host service, we're left with few chances but to reboot our server to view it (if it ever boots again after its intense contusions session).

Luckily, ANY.RUN's Interactive Sandbox has a reliable system which allows us to capture any created, deleted or modified file directly from its GUI. So, let's take a look.



A ransom note captured by ANY.RUN filesystem hook

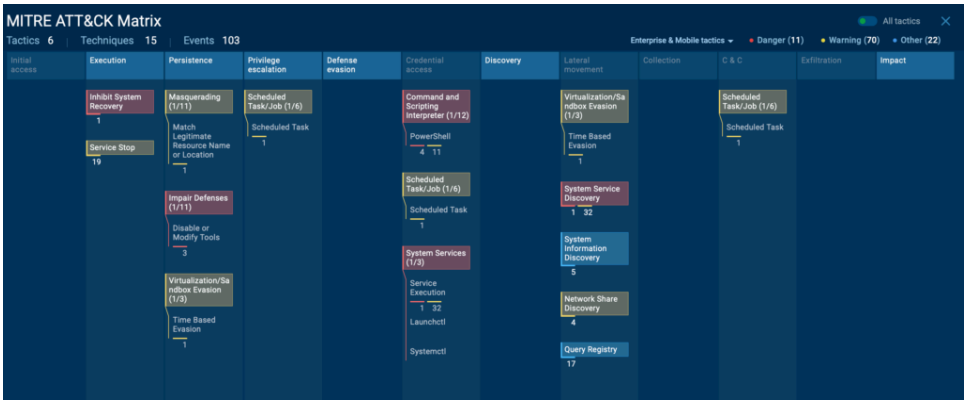
From here we can notice a BTC address which, after a quick inspection, shows that it has transacted just a few times for around $3,000 USD, suggesting once again that this wallet is shared across different victims or is a default one.

Using this instead of receiving a unique wallet, summed up with the technical aspects we saw before. And the chances of encryption keys being either derived locally or hardcoded, highlights the "homemade AI-assisted" fashion of this strain.

This is where things get shinier for victims, because deriving keys locally (or having them hardcoded) greatly improves the chances of a decryptor being made. And this is exactly what happened: Avast Labs was able to create a decryptor for FunkSec, which will give some hope to affected organisations.

After sharing the bad news (ransomware) and the good news (decryptors), it's time to move on to the ATT&CK Matrix, which ANY.RUN does automatically for us.

MITRE ATT&CK Techniques



ANY.RUN's Interactive Sandbox maps TTPs to the MITRE ATT&CK matrix

FunkLocker does a lot of things which could be pinned down individually and used as "footprints" to understand how it works:

Technique ID	Technique name	Observed behaviour / notes
T1036.005	Masquerading: Match Legitimate Resource Name or Location	The malware creates files with names similar to legitimate system files and drops them directly in the system drive root.
T1569.002	Service Execution: Service Commands	Launches sc.exe to manage Windows services (e.g., stopping them as part of its disruption routine).
T1007	System Service Discovery	Uses sc.exe to query or discover system services before acting on them.
T1489	Impact: Service Stop	Executes taskkill.exe to forcefully terminate: - Office apps - Running processes - Web browsers like Chrome, Firefox, Edge
T1059.001	Command and Scripting Interpreter: PowerShell	Runs multiple PowerShell commands to: - Disable Windows Defender real-time protection - Change the execution policy to Bypass (allowing unrestricted script execution)
T1135	Discovery: Network Share Discovery	Uses net.exe to display or manage information about current active sessions.
T1490	Impact: Inhibit System Recovery	Deletes Volume Shadow Copies using vssadmin delete shadows /all /quiet to prevent recovery via system restore points.
T1562.001	Defense Evasion: Disable or Modify Tools	Modifies Windows Defender configuration to weaken or disable protection mechanisms.

How Security Teams Should Respond

FunkSec shows how AI is changing the pace and style of ransomware development. For security leaders, the lesson is less about one strain and more about the trend it represents. A few priorities stand out:

- **Prioritize behavioral detection:** Static indicators aren't enough when code can be generated and tweaked with AI. Monitoring behaviors, especially misuse of system tools, becomes essential.
- **Invest in rapid visibility:** The longer it takes to understand what's happening inside an endpoint, the higher the cost of downtime. Tools that reveal the full execution chain within minutes are critical.
- **Test your recovery:** With shadow copies removed, recovery depends on isolated backups and practiced response playbooks. Tabletop exercises should assume ransomware disables standard rollback options.
- **Close the skill gap:** AI makes it easier for criminals to write malware, but defenders can also lean on AI-driven or interactive platforms to augment analysts and shorten investigation times.

The takeaway: FunkSec isn't just about today's attacks. It's a signal that the future of ransomware will be **faster, messier, and more frequent,** and security leaders should prepare their defenses accordingly.

About ANY.RUN

Over 500,000 cybersecurity professionals and 15,000+ companies in finance, manufacturing, healthcare, and other sectors rely on ANY.RUN to streamline malware investigations worldwide.

Speed up triage and response by detonating suspicious files in ANY.RUN's Interactive Sandbox, observing malicious behavior in real time, and gathering insights for faster, more confident security decisions. Paired with Threat Intelligence Lookup and Threat Intelligence Feeds, it provides actionable data on cyberattacks to improve detection and deepen your understanding of evolving threats.

Explore more ANY.RUN's capabilities during 14-day trial→

Further Reading and IOCs

ANY RUN's sandbox session

FunkLocker Decrypted: https://www.gendigital.com/blog/insights/research/funksec-ai

SHA256: c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c

FileName: C:\Users\admin\Desktop\README-ZasRvdSR44.md

SHA256: e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033

Mauro Eldritch

+ posts

Mauro Eldritch is an Argentinian-Uruguayan hacker, founder of BCA LTD and DC5411 (Argentina / Uruguay). He has spoken at various events, including DEF CON (12 times). He is passionate about Threat Intelligence and Biohacking. He currently leads Bitso's Quetzal Team, the first in Latin America dedicated to Web3 Threat Research.

Follow Mauro on:
X
LinkedIn
GitHub

ANYRUN cybersecurity malware analysis malware behavior

Mauro Eldritch

Mauro Eldritch is an Argentinian-Uruguayan hacker, founder of BCA LTD and DC5411 (Argentina / Uruguay). He has spoken at various events, including DEF CON (12 times). He is passionate about Threat Intelligence and Biohacking. He currently leads Bitso's Quetzal Team, the first in Latin America dedicated to Web3 Threat Research.

Follow Mauro on:
X
LinkedIn
GitHub
View all posts Twitter

What do you think about this post?

1 answers

- Awful
- Average
- Great

No votes so far! Be the first to rate this post.

Cancel reply

Verification expired. Check the checkbox again.

0 comments