FunkSec – Alleged Top Ransomware Group Powered by AI

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

January 10, 2025

Key Points

- The FunkSec ransomware group emerged in late 2024 and published over 85 victims in December, surpassing every other ransomware group that month.
- FunkSec operators appear to use AI-assisted malware development which can enable even inexperienced actors to quickly produce and refine advanced tools.
- The group's activities straddle the line between hacktivism and cybercrime, complicating efforts to understand their true motivations.
- Many of the group's leaked datasets are recycled from previous hacktivism campaigns, raising doubts about the authenticity of their disclosures.
- Current methods of assessing ransomware group threats often rely on the actors' own claims, highlighting the need for more objective evaluation techniques.

Introduction

The FunkSec ransomware group first emerged publicly in late 2024, and rapidly gained prominence by publishing over 85 claimed victims—more than any other ransomware group in the month of December. Presenting itself as a new Ransomware-as-a-Service (RaaS) operation, FunkSec appears to have no known connections to previously identified ransomware gangs, and little information is currently available about its origins or operations.

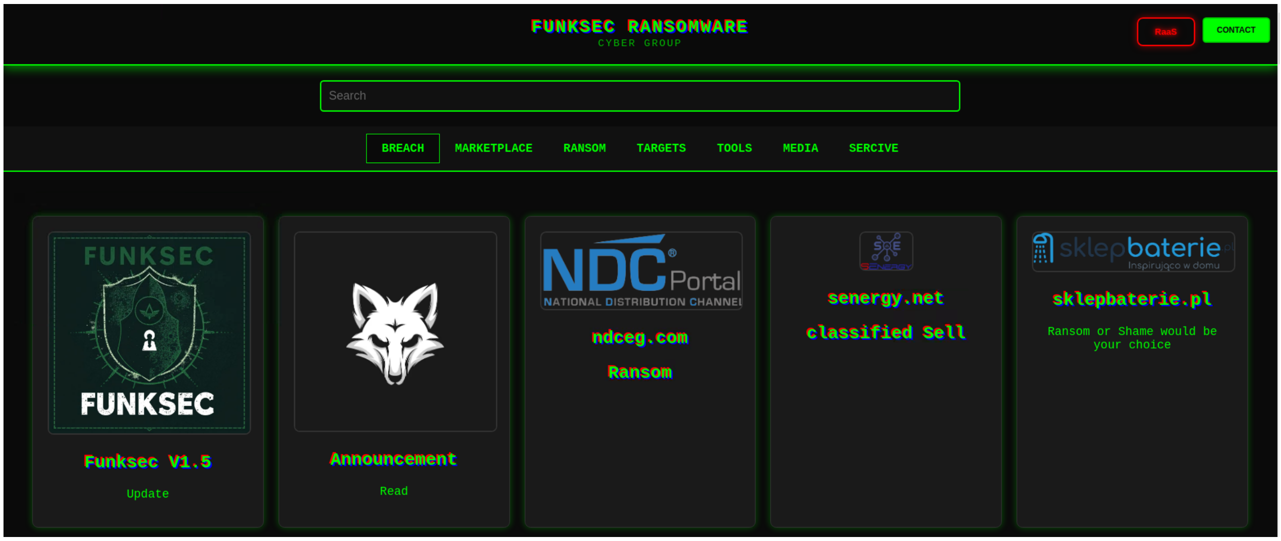
Our analysis of the group's activity indicates that the impressive numbers of published victims may mask a more modest reality both in terms of actual victims as well as the group's level of expertise. Most of FunkSec's core operations are likely conducted by inexperienced actors. In addition, it is difficult to verify the authenticity of the leaked information as the group's primary goal appears to be to gain visibility and recognition. Evidence suggests that in some instances, the leaked information was recycled from previous hacktivist-related leaks, raising questions about its authenticity.

In this report, we explore FunkSec's ties to hacktivist activity and provide an in-depth analysis of the group's public operations and tools, including a custom encryptor likely developed by a relatively inexperienced malware author based in Algeria. In a surprising discovery, our findings indicate that the development of the group's tools, including the encryptor, was likely AI-assisted, which may have contributed to their rapid iteration despite the author's apparent lack of technical expertise

This case highlights the increasingly blurred line between hacktivism and cybercrime, emphasizing the challenges in distinguishing one from the other. Whether such a distinction genuinely exists—or whether the operators are even aware of or concerned with defining it—remains uncertain. More importantly, It also calls into question the reliability of current methods for assessing the risk posed by ransomware groups, especially when those assessments rely on the public claims of the actors themselves.

Background – FunkSec Activity

FunkSec is an emerging ransomware group that launched its data leak site (DLS) in December 2024 to centralize their ransomware activities. The group uses double extortion tactics, combining data theft with encryption to pressure victims into paying ransoms. Their DLS features breach announcements, a custom-developed DDoS tool, and, more recently, a custom ransomware offered as a Ransomware-as-a-Service (RaaS).



Funksec V1.5
Update

Announcement
Read

ndceg.com
Ransom

senergy.net
classified Sell

sklepbaterie.pl
Ransom or Shame would be your choice

Figure 1 – FunkSec data leak site.

FunkSec gained public attention due to their aggressive tactics and the number of their targets, with more than 85 claimed victims in little over a month of activity. Notably, FunkSec demanded unusually low ransoms, sometimes as little as $10,000, and sell stolen data to third parties at reduced prices. The group's activities are widely discussed in cybercrime forums, further contributing to their growing notoriety.

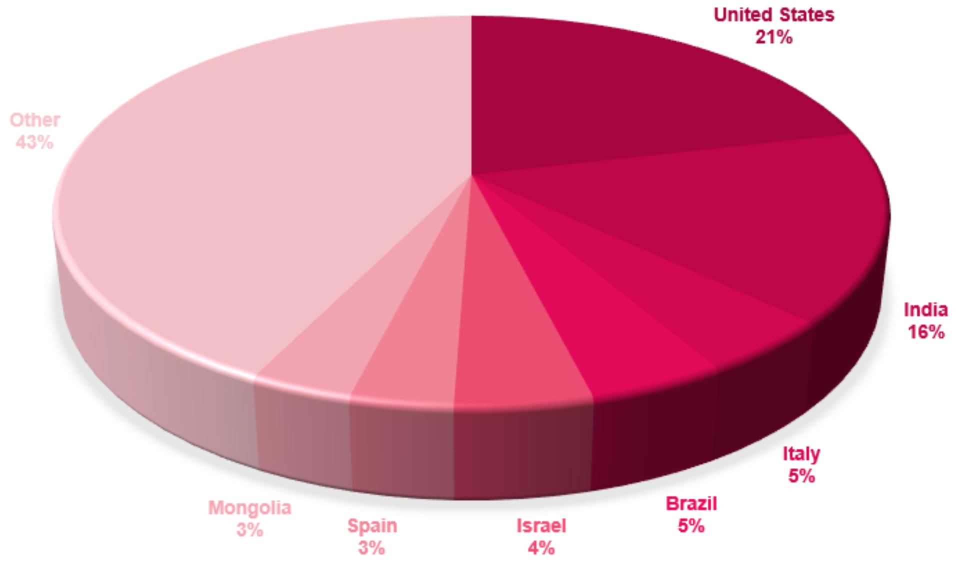


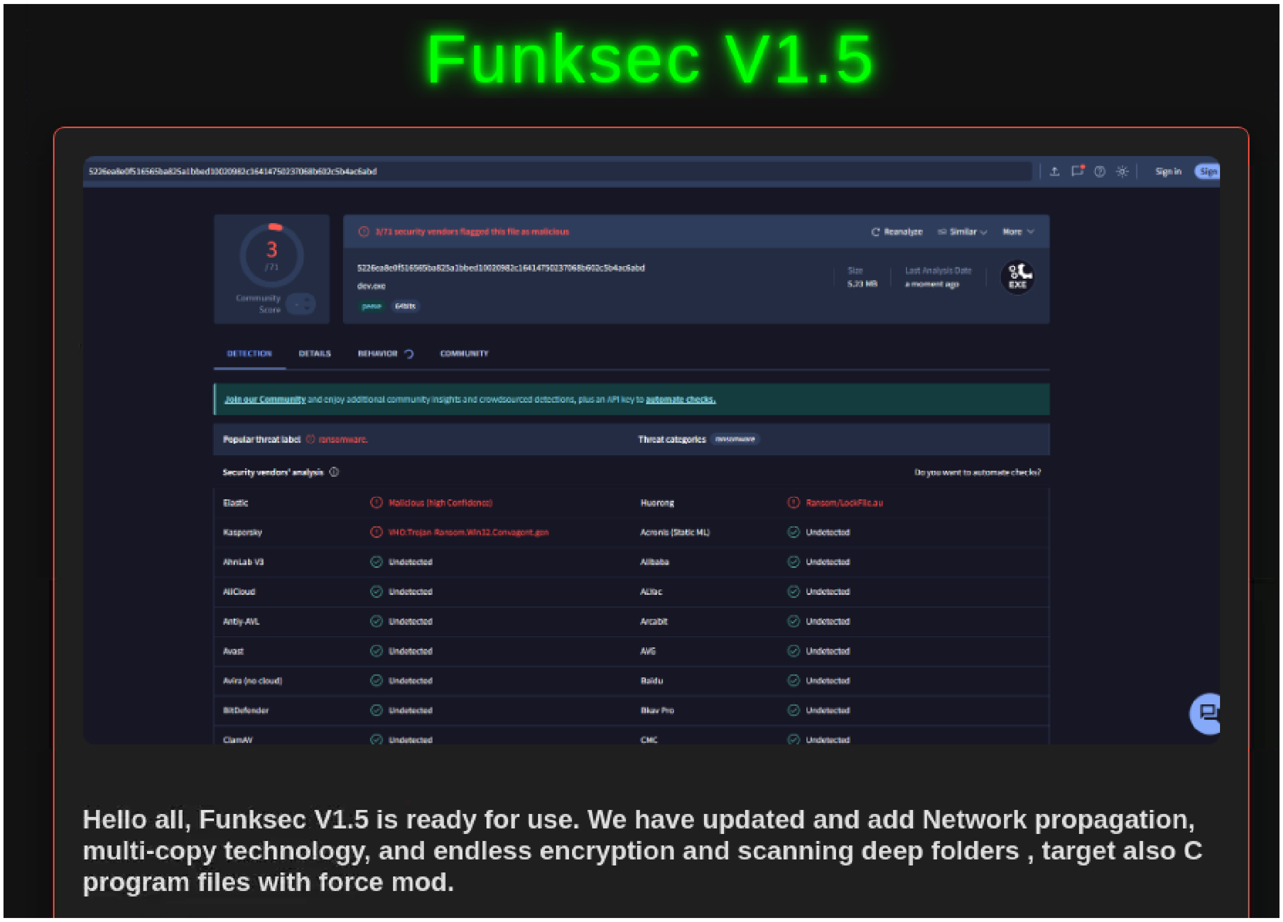
Figure 2 – Distribution of FunkSec claimed victims by country according to DLS.

Closer analysis of FunkSec's activities and DarkWeb discussions offers some tantalizing hints about the group, namely that their motivations seem to straddle the line between hacktivism and cybercrime. Interestingly, some members linked to FunkSec previously engaged in hacktivist activities, adding a complex layer to their operations and raising questions about their true objectives. This blend of tactics and backgrounds made FunkSec a particularly intriguing case for deeper investigation.

FunkSec Offerings

Ransomware

FunkSec operators recently began to offer their rapidly evolving custom ransomware. With each new version, many of them published only days apart, their website is updated to highlight the added features. In the announcement for the latest version V1.5, the operators boasted about its low detection rate, sharing a VirusTotal screenshot that showed it was detected by only three antivirus engines at the time of publication.



Funksec V1.5

5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd

3/71 security vendors flagged this file as malicious

5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd

dev.exe

Size 5.23 MB

Last Analysis Date a moment ago

Popular threat label ransomware.

Threat categories ransomware

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

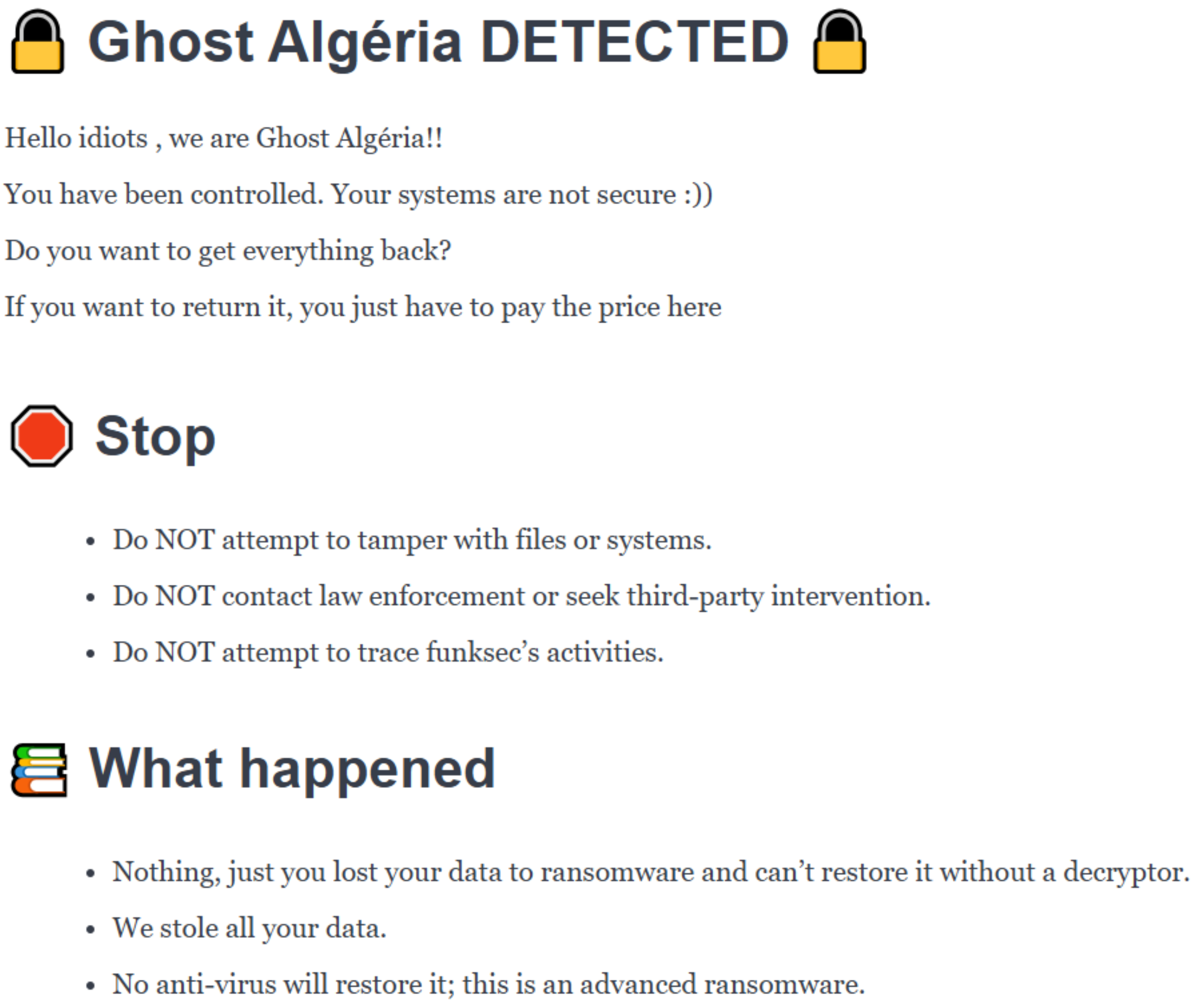
Elastic	Malicious (high Confidence)	Huorong	Ransom/LockFile.au
Kaspersky	VHO:Trojan-Ransom.Win32.Convagent.gen	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

Hello all, Funksec V1.5 is ready for use. We have updated and add Network propagation, multi-copy technology, and endless encryption and scanning deep folders , target also C program files with force mod.

Figure 3 – Funksec V1.5 publication announcement.

The file referenced in their publication(5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd), named dev.exe, was uploaded from an Algerian source, and truly was detected by only 3 engines at the time of upload. The ransomware is identified by using the extension ".funksec", written in Rust and compiled on the environment of C:\Users\Abdellah\. A full analysis of the malware is provided in the Technical Analysis section.

In our analysis of this ransomware, we uncovered all its versions which point to an ongoing development effort likely carried out by an inexperienced malware author. Notably, most of the versions were uploaded from Algeria, likely by the author himself. Analysis of those samples reveals two variants of the ransom notes. The first references FunkSec, and the second one references Ghost Algeria, another indication that the developer is from Algeria.



🔒 Ghost Algéria DETECTED 🔒

Hello idiots , we are Ghost Algéria!!

You have been controlled. Your systems are not secure :))

Do you want to get everything back?

If you want to return it, you just have to pay the price here

🛑 Stop

- Do NOT attempt to tamper with files or systems.
- Do NOT contact law enforcement or seek third-party intervention.
- Do NOT attempt to trace funksec's activities.

📚 What happened

- Nothing, just you lost your data to ransomware and can't restore it without a decryptor.
- We stole all your data.
- No anti-virus will restore it; this is an advanced ransomware.

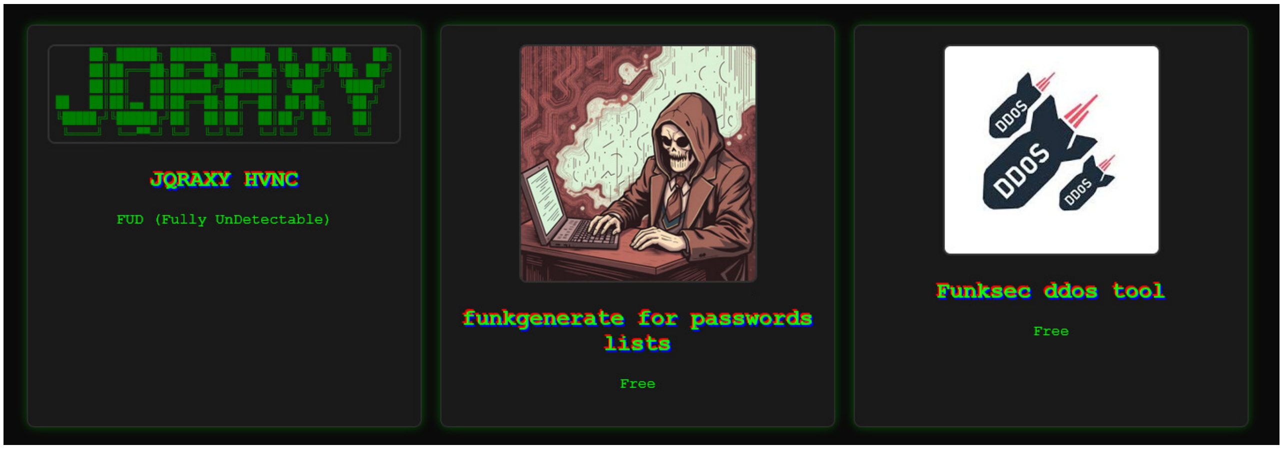
Figure 4 – Ransomware notes used by FunkLocker and Ghost Algeria.

Interestingly, the author also uploaded parts of the malware's source code, written in Rust. The source code file, named `*ransomware.rs*`, has parts of the functionality of the compiled binaries and was uploaded to VirusTotal on December 15 from an Algerian source. This prototype version of the ransomware is a simplified implementation and includes these functions:

- **Encrypt all files on the user's system** (in the `C:\` directory) using a combination of RSA and AES encryption. The original files are deleted after encryption, and encrypted versions with a new extension (`.funksec`) are created.
- **Create a ransom note** (`readme.me`) informing the user that their files have been encrypted and providing instructions for paying a ransom to obtain a decryption key.
- **Modify the system environment** (e.g., changing the desktop background to black).
- Check for **administrative/root privileges** before executing.

Other free tools

In addition to the ransomware, the FunkSec group offers additional tools, most of them commonly associated with hacktivist activity.



JQRAXY HVNC

FUD (Fully UnDetectable)

funkgenerate for passwords lists

Free

Funksec ddos tool

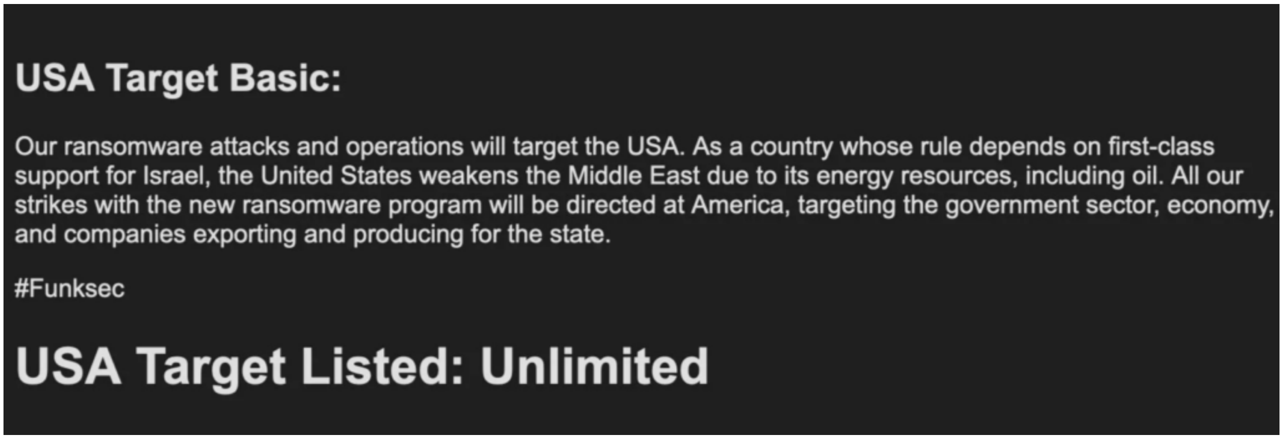
Free

Figure 5 – Additional offerings by FunkSec.

- FDDOS, a Python “Scorpion DDoS Tool”, is a network stress-testing tool designed to perform Distributed Denial-of-Service (DDoS) attacks using either HTTP or UDP flood methods.
- JQRAXY_HVNC an HVNC Server and client C++ program is designed for remote desktop management, automation, and data interaction.
- funkgenerate is a smart password generation and scraping tool designed to scrape emails and potential passwords from given URLs and generate new password suggestions.

Associated Threat Actors

In late 2024, FunkSec emerged without warning and quickly dominated ransomware victim feeds and monitors, seemingly under the guise of hacktivism. By targeting India and the U.S., and aligning with the “Free Palestine” movement, the group leveraged multiple personas and aliases to craft its image and gain visibility.



USA Target Basic:

Our ransomware attacks and operations will target the USA. As a country whose rule depends on first-class support for Israel, the United States weakens the Middle East due to its energy resources, including oil. All our strikes with the new ransomware program will be directed at America, targeting the government sector, economy, and companies exporting and producing for the state.

#Funksec

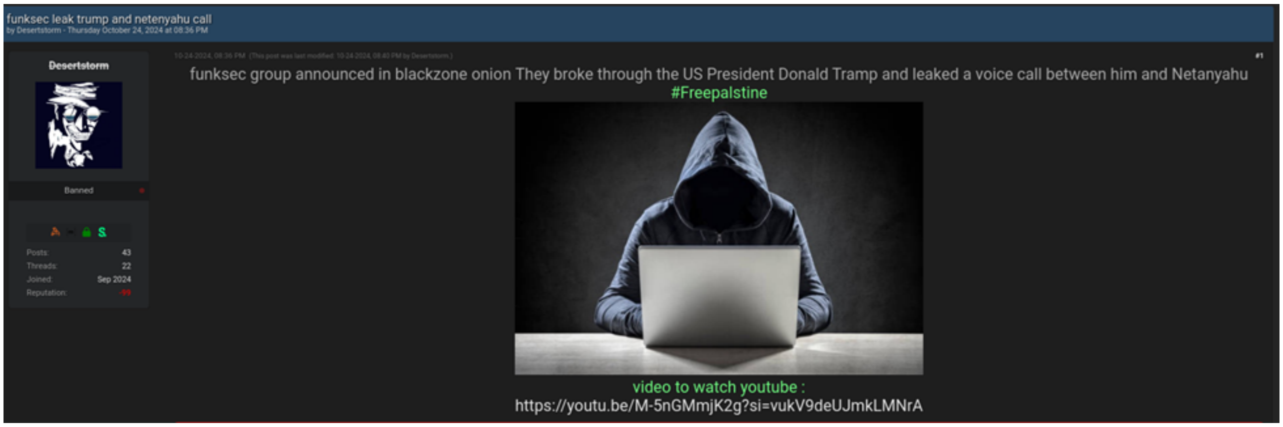
USA Target Listed: Unlimited

Figure 6 – FunkSec claims about US targets.

Scorpion

Scorpion is the most prominent member of FunkSec and is associated with major portions of the group public profiles. This actor uses multiple aliases, most prominently **DesertStorm**.

The actor first surfaced on the Breached Forum, introducing the FunkSec name through a YouTube video posted via the channel “Scorpion” (@scorpioncybersec) in October 2024. The video alleged that FunkSec leaked a call between then-U.S. presidential candidate Donald Trump and Israeli Prime Minister Benjamin Netanyahu. However, the recording was clearly AI-generated.



funksec leak trump and netenyahu call
by Desertstorm - Thursday October 24, 2024 at 08:36 PM

Desertstorm

Banned

Posts: 43
Threads: 22
Joined: Sep 2024
Reputation: -99

10-24-2024, 08:36 PM (This post was last modified: 10-24-2024, 08:40 PM by Desertstorm.)

#1

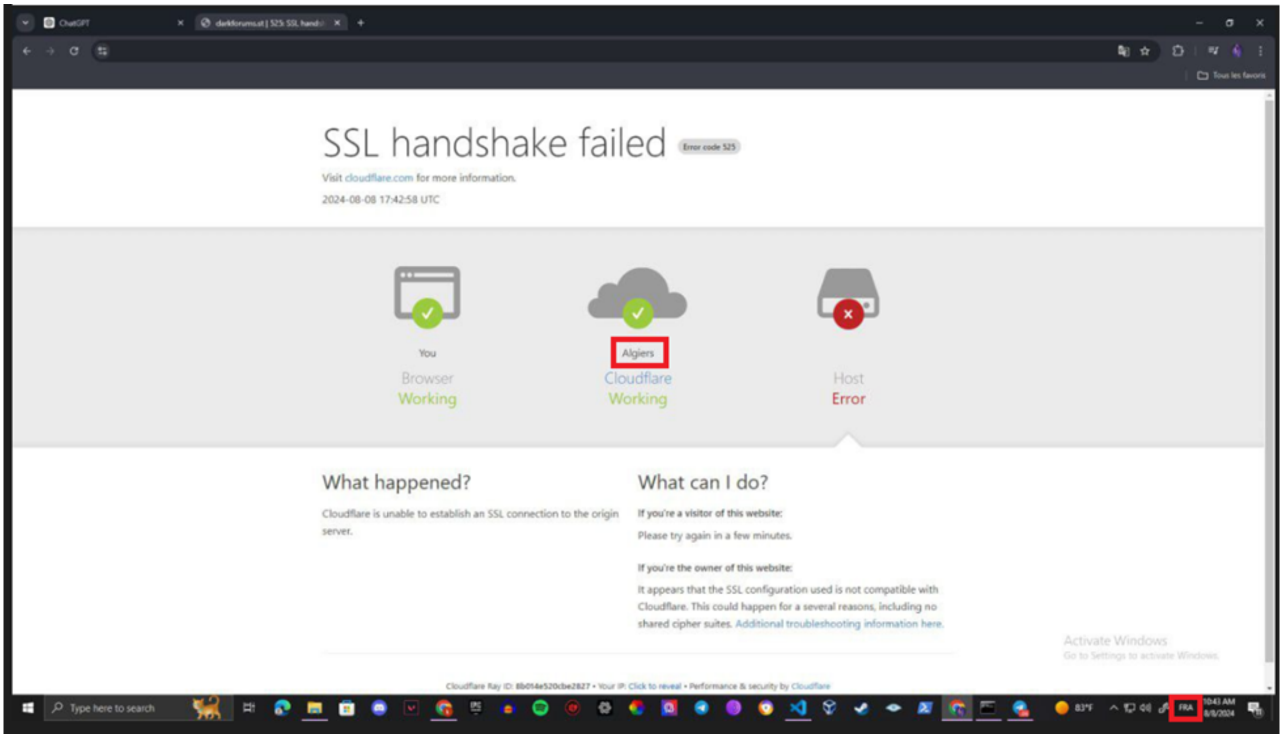
funksec group announced in blackzone onion They broke through the US President Donald Tramp and leaked a voice call between him and Netanyahu
#Freepalstine

video to watch youtube :
https://youtu.be/M-5nGMmjK2g?si=vukV9deUJmkLMNrA

Figure 7 – Announcement of the allegedly leaked call between Donald Trump and Benjamin Netanyahu.

DesertStorm’s YouTube profile listed their location as Russia, though the video’s shared URL suggested it was uploaded from Brazil. DesertStorm continued posting leaks on Breached Forum—most unverified or not credited to FunkSec—until the account was banned in November 2024.

In one of DesertStorm’s posts, they inadvertently shared compromising screenshots that revealed their location to be Algeria, with French-language keyboard settings. A suspected associate, **XTN**, publicly alerted DesertStorm to this operational security (OpSec) lapse, but DesertStorm did not remove the compromising information.



SSL handshake failed Error code 525

Visit cloudflare.com for more information.

2024-08-08 17:42:58 UTC

You
Browser
Working

Algiers
Cloudflare
Working

Host
Error

What happened?

Cloudflare is unable to establish an SSL connection to the origin server.

What can I do?

If you're a visitor of this website:

Please try again in a few minutes.

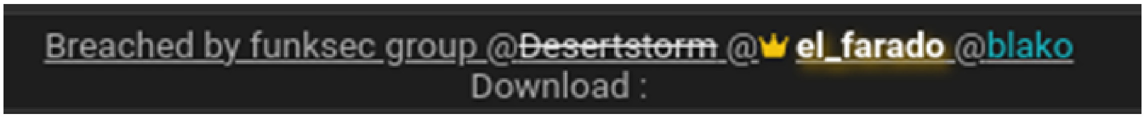
If you're the owner of this website:

It appears that the SSL configuration used is not compatible with Cloudflare. This could happen for a several reasons, including no shared cipher suites. Additional troubleshooting information here.

Cloudflare Ray ID: 8b014e520cbe2827 • Your IP: Click to reveal • Performance & security by Cloudflare

Figure 8 – Screenshot tying DesertStorm to Algeria.

Before DesertStorm’s ban, the actor began tagging two other users, **El_Farado** and **Blako**, in forum posts related to FunkSec leaks and activities. While Blako remained inactive on the forums, El Farado gradually assumed a prominent role, promoting FunkSec on forums, sharing leaks, and adding the group’s .onion site to their signature.



Breached by funksec group @~~Desertstorm~~ @👑 el_farado @blako
Download :

Figure 9 -Connection between DesertStorm and El_farado

The actor is also linked to a Keybase account under the name "Scorpionlord," where they are listed as the admin of FunkSec. This account is tied to the FunkSec shame site and DesertStorm's user on Breached Forum. Scorpionlord is also the username on two other cybercrime forums where the FunkSec's website was promoted (these users were since removed).

Notably, El Farado's Keybase profile was registered on the same day as Scorpionlord's, suggesting a coordinated effort. A third Keybase profile, **Blako**, was registered only a few days later, further supporting the idea that these personas were all closely linked.

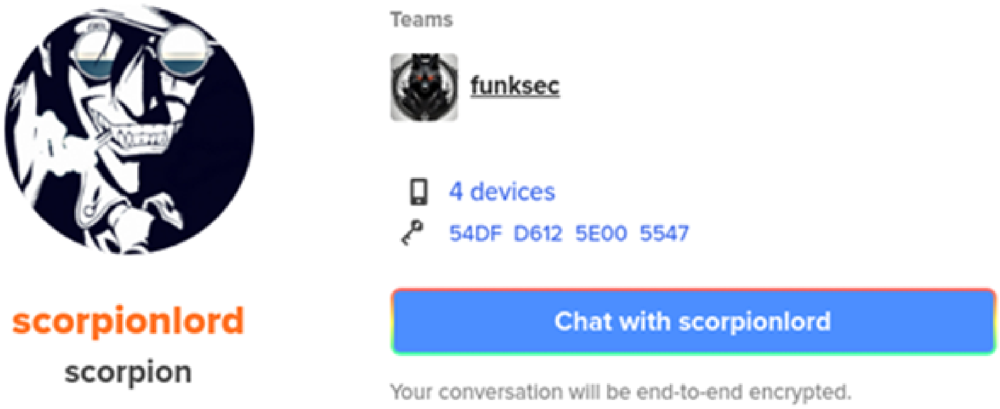


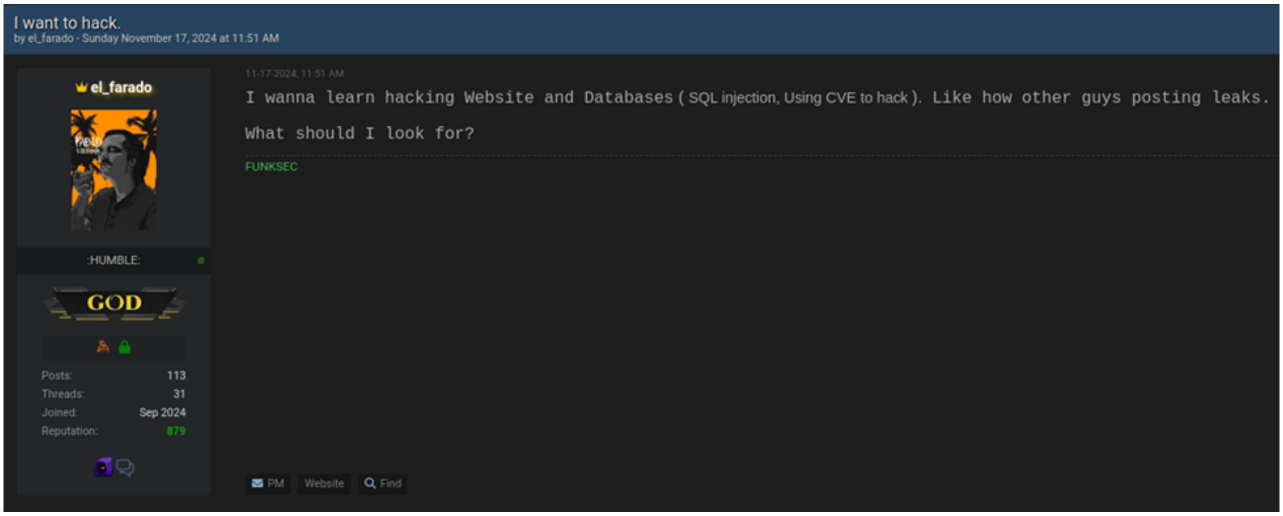
Figure 10 – Scorpion Keybase profile.

El_farado

El Farado emerged as a key figure in FunkSec's operations after DesertStorm's ban from Breached Forum in November 2024. El Farado took on the task of promoting FunkSec, ensuring its visibility on the forum and sharing alleged leaks.

Key connections to FunkSec include:

- **Tagged by DesertStorm:** DesertStorm's posts frequently tagged El Farado, linking them directly to FunkSec.
- **Keybase Profile Registration:** El Farado's Keybase account was registered on the same day as Scorpionlord's, implying a strong connection between the two personas.
- **Promotional Activity:** El Farado actively promoted FunkSec's .onion site on Breached Forum and shared leaks (often unreliable or recycled).
- **Rookie Behavior:** El Farado occasionally posted threads asking basic hacking questions like "What do hackers do with leaked data?" This behavior suggests inexperience, corroborating some Scorpion's admission of the group's lack of technical know-how.


I want to hack.
by el_farado - Sunday November 17, 2024 at 11:51 AM

el_farado

:HUMBLE:

GOD

Posts: 113
Threads: 31
Joined: Sep 2024
Reputation: 879

11-17-2024, 11:51 AM

I wanna learn hacking Website and Databases (SQL injection, Using CVE to hack). Like how other guys posting leaks.

What should I look for?

FUNKSEC

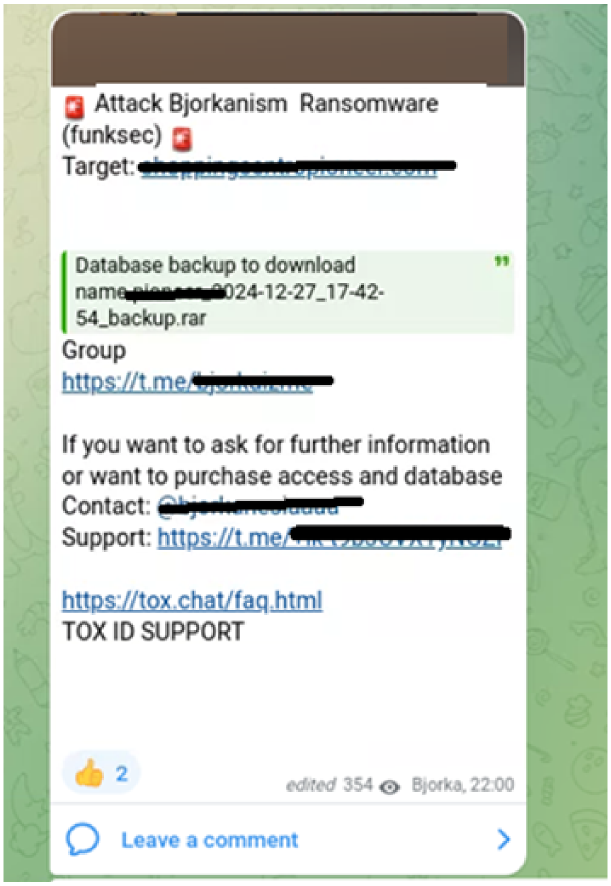
Figure 11 – el_farado asking for hacking assistance.

XTN

XTN is associated with FunkSec's "data sorting" service advertised on their website, while this service's purpose is not fully clear. Their Keybase account, "xtnn," connects to their Breached Forum profile, where they describe their location as "El Farado's room" and reference El Farado in their signature. XTN further solidified their link to FunkSec by publicly warning DesertStorm about their OpSec lapse.

Bjorka

Bjorka, a known Indonesian hacktivist, has a murkier connection to FunkSec. While leaks attributed to FunkSec were reposted by a user named Bjorka on DarkForums, no direct collaboration was verified. Additionally, a Telegram channel named "Bjorkanism" claimed credit for some FunkSec operations, referring to them as "Bjorkanism Ransomware (FunkSec)." These claims are not supported by Bjorka's official platforms, suggesting attempts at impersonating Bjorka or at most, a loose affiliation.



Attack Bjorkanism Ransomware (funksec)
Target: [redacted]

> Database backup to download
> name[redacted]024-12-27_17-42-54_backup.rar

Group
https://t.me/[redacted]

If you want to ask for further information or want to purchase access and database
Contact: [redacted]
Support: https://t.me/[redacted]

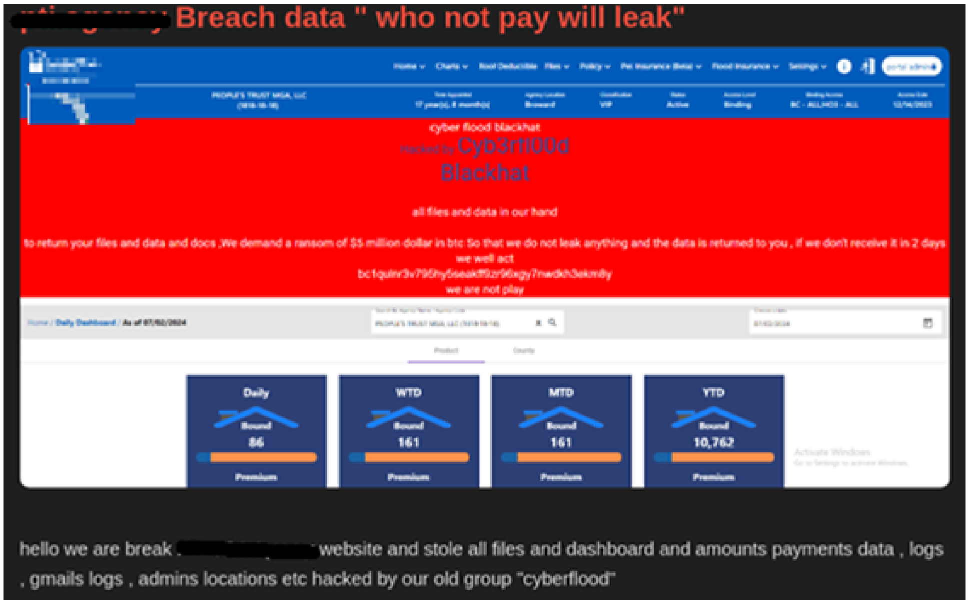
https://tox.chat/faq.html
TOX ID SUPPORT

Figure 12 – Bjorkanism referenced as FunkSec ransomware.

Related Hacktivist Groups

FunkSec attempted to associate itself with several defunct hacktivist groups:

- **Ghost Algéria:** Referenced in a ransomware note nearly identical to FunkSec's.
- **Cyb3r Fl00d:** A defacement screenshot from this group was included in FunkSec-related activity, with FunkSec claiming Cyb3r Fl00d was their "old group."



[redacted] Breach data " who not pay will leak"

cyber flood blackhat
Hacked by Cyb3rfl00d
Blackhat

all files and data in our hand

to return your files and data and docs ,We demand a ransom of $5 million dollar in btc So that we do not leak anything and the data is returned to you , if we don't receive it in 2 days we well act
bc1qulnr3v795hy5seakff9zr96xgy7nwdkh3ekm8y
we are not play

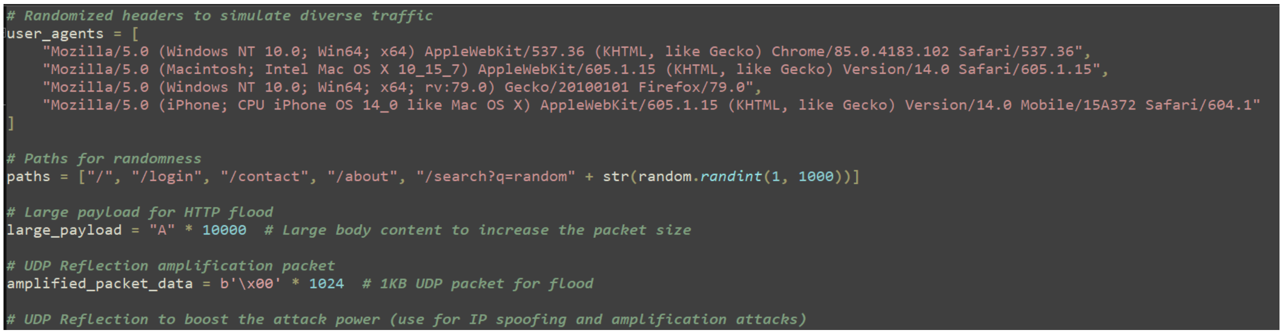
hello we are break [redacted] website and stole all files and dashboard and amounts payments data , logs , gmails logs , admins locations etc hacked by our old group "cyberflood"

Figure 13 -Affiliation between FunkSec and Cyb3r Fl00d

These associations likely represent attempts to boost FunkSec's credibility by aligning with well-known names rather than direct membership or collaboration.

AI-Assisted capabilities

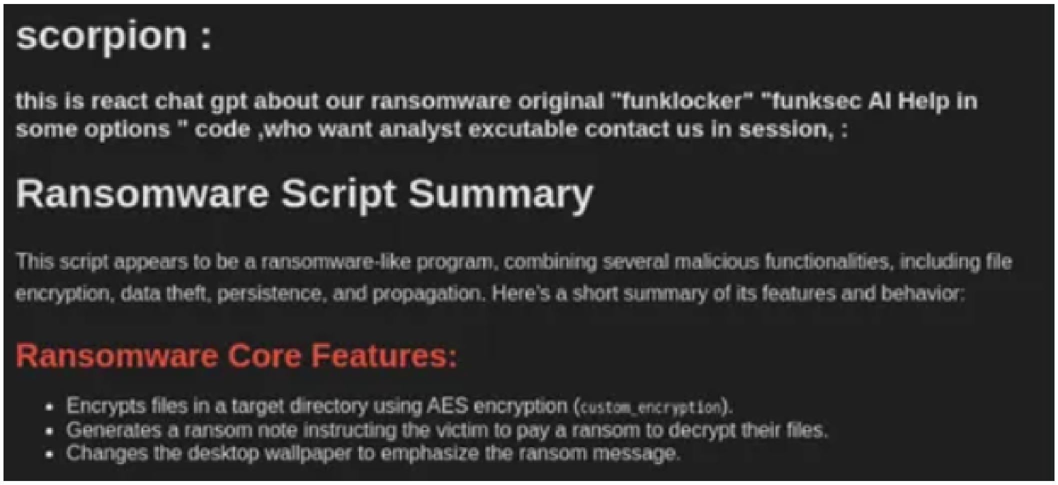
The individuals behind FunkSec appear to have extensively leveraged AI to enhance their capabilities, as evidenced by their publications and tools. Their public script offerings include extensive code comments with perfect English (as opposed to very basic English in other mediums), likely generated by an LLM agent. Similar patterns are visible in the Rust source code linked to the group's ransomware, suggesting it may have been developed with AI assistance.



```
# Randomized headers to simulate diverse traffic
user_agents = [
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0",
    "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15A372 Safari/604.1"
]

# Paths for randomness
paths = ["/", "/login", "/contact", "/about", "/search?q=random" + str(random.randint(1, 1000))]

# Large payload for HTTP flood
large_payload = "A" * 10000  # Large body content to increase the packet size

# UDP Reflection amplification packet
amplified_packet_data = b'\x00' * 1024  # 1KB UDP packet for flood

# UDP Reflection to boost the attack power (use for IP spoofing and amplification attacks)
```

Figure 14 – Detailed comments in Scorpion DDoS script.

In some of their published messages, the group specifically linked the development of their ransomware to AI-assisted agents, likely providing it with the source code for the ransomware and simply shared the output on their site.



scorpion :

this is react chat gpt about our ransomware original "funklocker" "funksec AI Help in some options " code ,who want analyst excutable contact us in session, :

Ransomware Script Summary

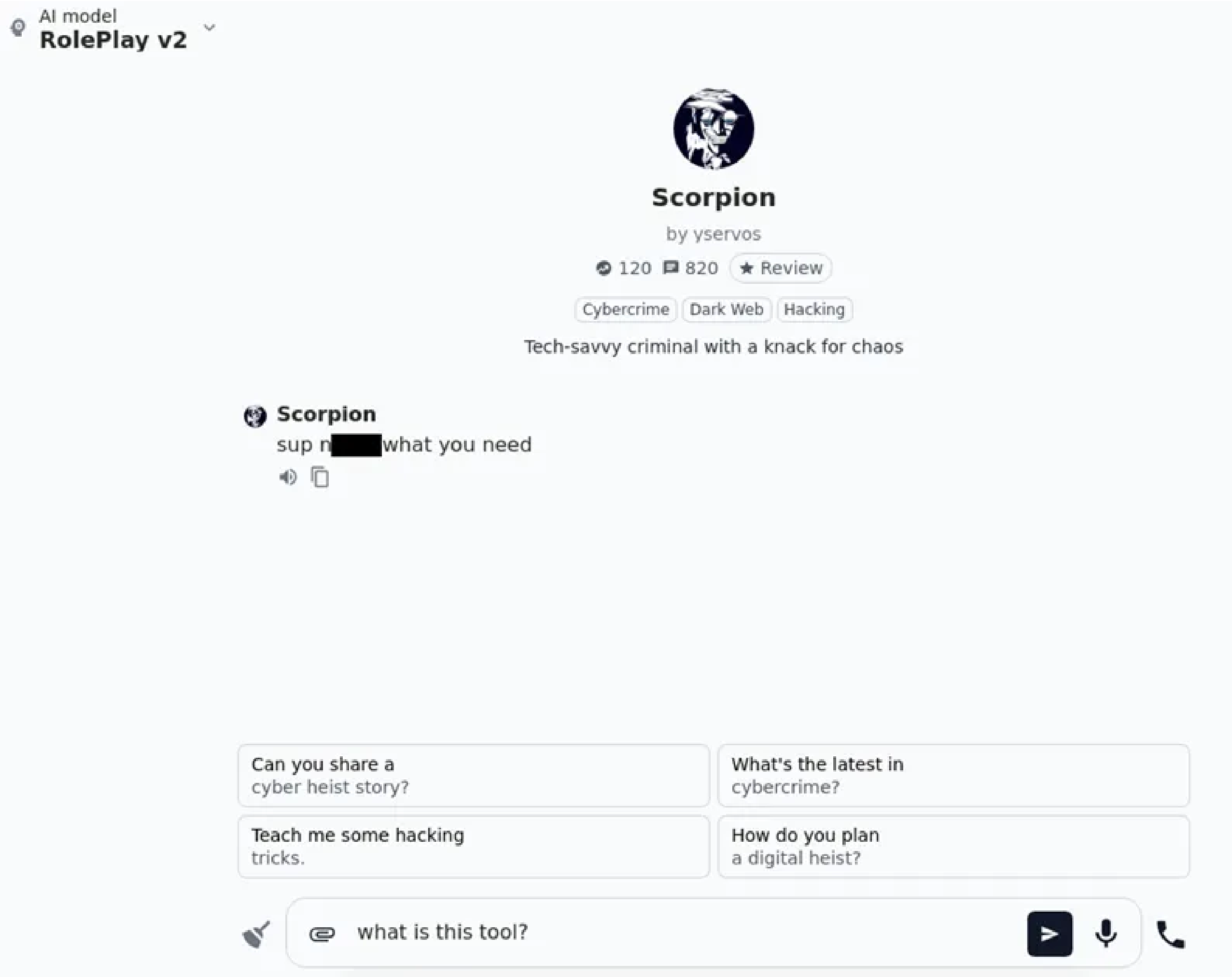
This script appears to be a ransomware-like program, combining several malicious functionalities, including file encryption, data theft, persistence, and propagation. Here's a short summary of its features and behavior:

Ransomware Core Features:

- Encrypts files in a target directory using AES encryption (custom_encryption).
- Generates a ransom note instructing the victim to pay a ransom to decrypt their files.
- Changes the desktop wallpaper to emphasize the ransom message.

Figure 15 – FunkSec claims of AI interpretation of their Ransomware code.

The use of such tools aligns closely with the group's public claims, as they also released an AI chatbot based on Miniapps to support their operations. Miniapps is a platform that facilitates the creation and use of AI applications and chatbots, often without the restrictions found in more popular systems like ChatGPT. The bot developed by FunkSec is specifically designed to support malicious activities.



AI model
RolePlay v2

Scorpion

by yservos

120 820 ★ Review

Cybercrime | Dark Web | Hacking

Tech-savvy criminal with a knack for chaos

Scorpion
sup [redacted] what you need

Can you share a cyber heist story?

What's the latest in cybercrime?

Teach me some hacking tricks.

How do you plan a digital heist?

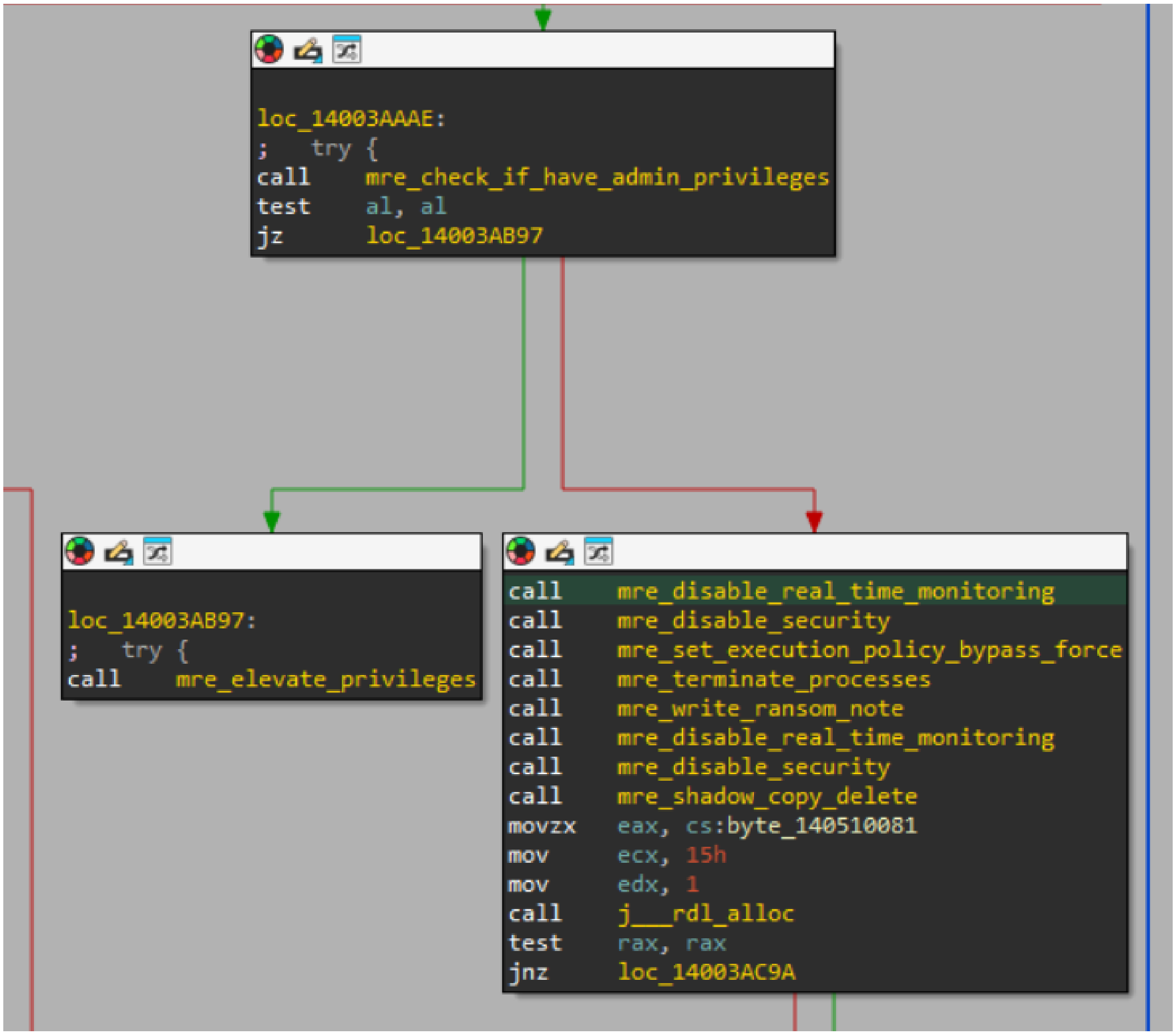
what is this tool?

Figure 16 – Scorpion miniapps chat.

Technical Analysis

To better understand the malware, we examined one of the circulated samples. This is a stripped Rust binary, which makes it challenging to effectively reverse engineer. In particular, it is subject to aggressive in-lining of library code (see our previous publication, Inside Akira Ransomware's Rust Experiment for a clear demonstration of how this works, and how this complicates reverse engineering tasks), and contains many trait implementations that a disassembler may not recognize out of the box, many of which are wrappers for e.g. `WriteFileEx` or `CryptGenRandom`. However, a careful analysis reveals some interesting details.

Overall, we were mainly struck by the amount of redundancy in the binary. Control flow seems to repeat itself and call functions again and again from various execution paths; in a typical ransomware, these would only be called once. For example, in this sequence of operations:



```
loc_14003AAAE:
;   try {
call    mre_check_if_have_admin_privileges
test    al, al
jz      loc_14003AB97
```

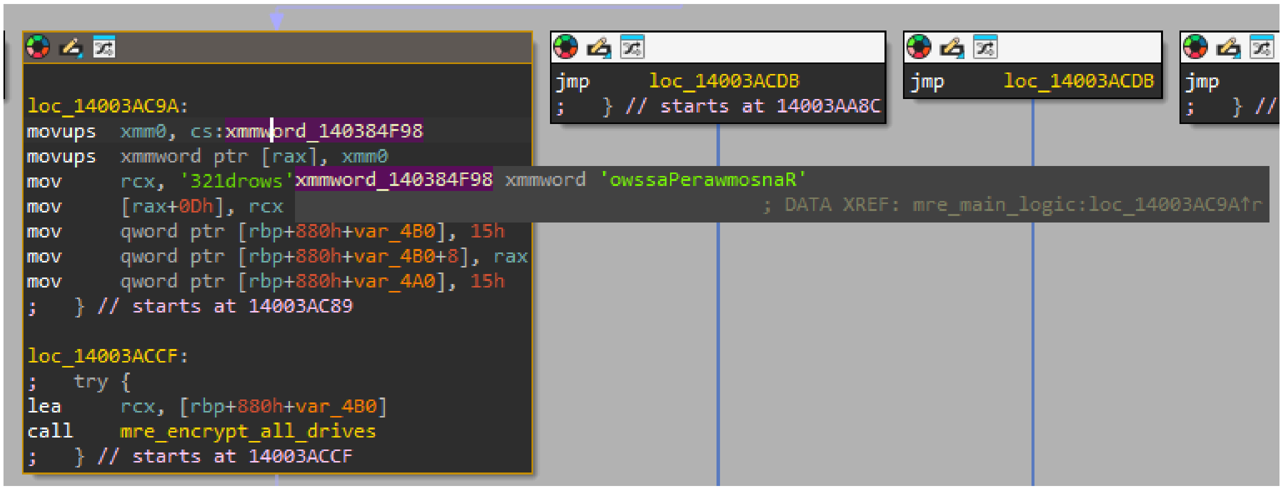
```
loc_14003AB97:
;   try {
call    mre_elevate_privileges
```

```
call    mre_disable_real_time_monitoring
call    mre_disable_security
call    mre_set_execution_policy_bypass_force
call    mre_terminate_processes
call    mre_write_ransom_note
call    mre_disable_real_time_monitoring
call    mre_disable_security
call    mre_shadow_copy_delete
movzx   eax, cs:byte_140510081
mov     ecx, 15h
mov     edx, 1
call    j___rdl_alloc
test    rax, rax
jnz     loc_14003AC9A
```

Figure 17 – Functions called multiple times in the FunkSec Ransomware.

Across the entire binary many of these functions are called twice, or even three or four times; the 'disable security' routine, seen above, is called twice in the same basic block. The below recursive function, which iterates into all subdirectories of a given directory and encrypts the targeted files in it, is called a total of *five* times across the binary.

Some of the repetition is due to duplicated code that invokes the 'encrypt all directories' logic with different hardcoded constants each time, such as this invocation that uses the constant `RansomwarePassword123`:



```
loc_14003AC9A:
movups  xmm0, cs:xmmword_140384F98
movups  xmmword ptr [rax], xmm0
mov     rcx, '321drows'
mov     [rax+0Dh], rcx
mov     qword ptr [rbp+880h+var_4B0], 15h
mov     qword ptr [rbp+880h+var_4B0+8], rax
mov     qword ptr [rbp+880h+var_4A0], 15h
;   } // starts at 14003AC89

loc_14003ACCF:
;   try {
lea     rcx, [rbp+880h+var_4B0]
call    mre_encrypt_all_drives
;   } // starts at 14003ACCF
```

```
xmmword_140384F98 xmmword 'owssaPerawmosnaR'
                  ; DATA XREF: mre_main_logic:loc_14003AC9A↑r
```

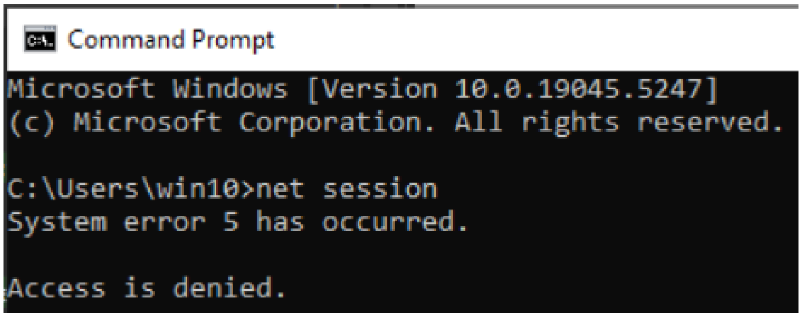
```
jmp     loc_14003ACDB
;   } // starts at 14003AA8C
```

```
jmp     loc_14003ACDB
```

```
jmp
;   } //
```

Figure 18 – RansomwarePassword123 constant in the code.

Aside from the duplicated functionality, the main execution flow of the malware first calls the operations sequence seen earlier ("disable security", and so on) and then transfers execution to an 'encrypt all drives' function. The operations sequence begins by checking whether it has elevated privileges (by trying to execute `net session`). If not, the binary attempts to relaunch itself with elevated privileges, using the method described here (`start-process -wait -Verb runas -filepath '%~nx0' -ArgumentList '<arguments>'`).



```
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\win10>net session
System error 5 has occurred.

Access is denied.
```

Figure 19 – Sample output of `net session` without elevated privileges.

Once it has elevated privileges, the malware executes the following commands:

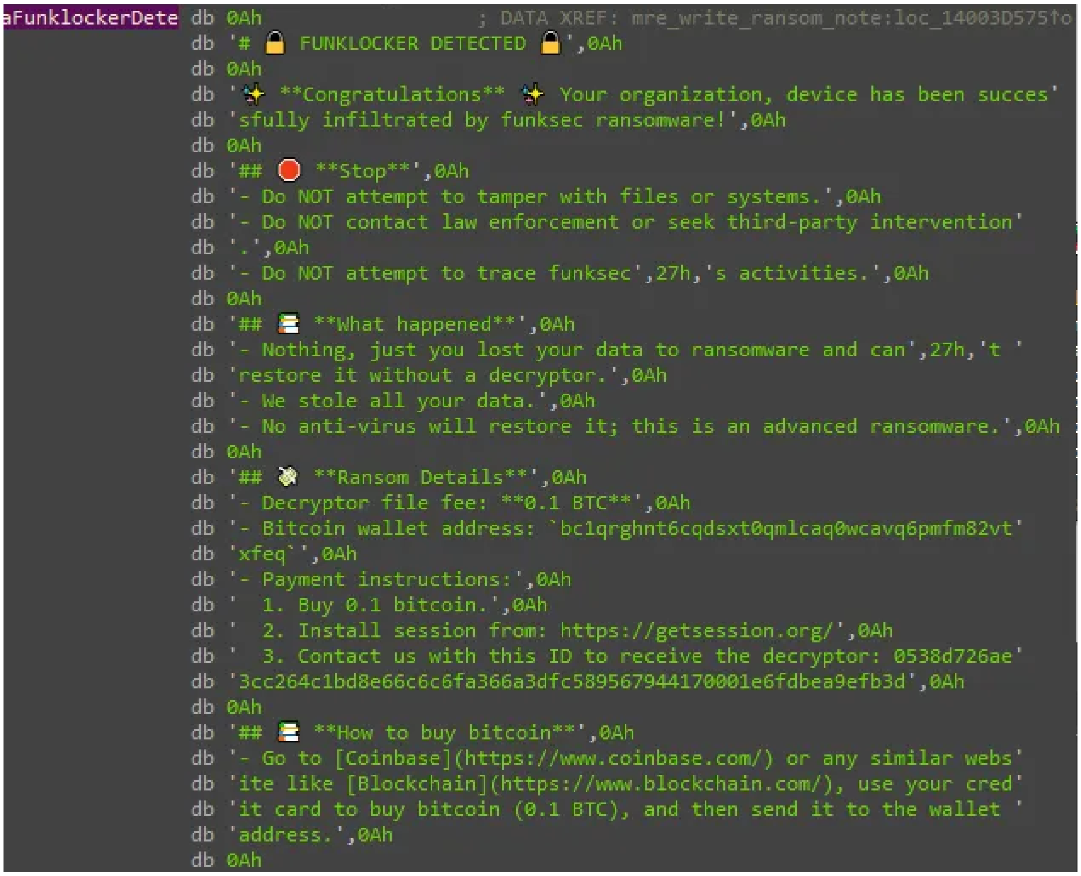
Command	**Functionality**
`Set-MpPreference -DisableRealtimeMonitoring $true`	Disable Windows Defender real-time protection.
`wevtutil sl Security /e:false`	Disable Security event logging.
`wevtutil sl Application /e:false`	Disable Application event logging.
`Set-ExecutionPolicy Bypass -Scope Process -Force`	Disable restrictions placed by the Powershell execution policy.
`vssadmin delete shadows /all /quiet`	predictably, delete shadow copy backups.

The `terminate_processes` function contains a hardcoded list of processes and services to terminate:

chrome.exe	firefox.exe	msedge.exe	explorer.exe	outlook.exe	vlc.exe
spotify.exe	skype.exe	discord.exe	steam.exe	java.exe	python.exe
node.exe	cmd.exe	powershell.exe	taskmgr.exe	wmplayer.exe	tscon.exe
notepad.exe	spooler	bits	dnsclient	lanmanworkstation	winmgmt
netsh	iphlpsvc	wuauserv	RemoteAccess	ShellHWDetection	SCardSvr
TrkWks	wscsvc	CryptSvc	msiserver	MpsSvc	defragsvc
upnphost	WindowsUpdate	srservice	wsmprovhost	AppIDSvc	AudioEndpointBuilder
Schedule	eventlog	PlugPlay	Netman	bthserv	ShellExperienceHost
SMB	WinDefend				

Next, the malware moves on to iterating over each letter drive, recursing through its subdirectories and encrypting each file with one of the targeted extensions. For file encryption, the symmetric encryption used is the chacha20 implementation available in the orion.rs crate. Ephemeral keys are generated using a thin wrapper for `CryptGenRandom` (and the descriptively-named `SystemFunction036`). The newly created filename, with the hardcoded `.funksec` extension, is created using a call to Rust's `format!` macro.

The malware then writes to disk the (rather emoji-fied) ransom note.



```
aFunklockerDete db 0Ah                     ; DATA XREF: mre_write_ransom_note:loc_14003D575↑o
                db '# 🔒 FUNKLOCKER DETECTED 🔒',0Ah
                db 0Ah
                db '✨ **Congratulations** ✨ Your organization, device has been succes'
                db 'sfully infiltrated by funksec ransomware!',0Ah
                db 0Ah
                db '## 🛑 **Stop**',0Ah
                db '- Do NOT attempt to tamper with files or systems.',0Ah
                db '- Do NOT contact law enforcement or seek third-party intervention'
                db '.',0Ah
                db '- Do NOT attempt to trace funksec',27h,'s activities.',0Ah
                db 0Ah
                db '## 📚 **What happened**',0Ah
                db '- Nothing, just you lost your data to ransomware and can',27h,'t '
                db 'restore it without a decryptor.',0Ah
                db '- We stole all your data.',0Ah
                db '- No anti-virus will restore it; this is an advanced ransomware.',0Ah
                db 0Ah
                db '## 💰 **Ransom Details**',0Ah
                db '- Decryptor file fee: **0.1 BTC**',0Ah
                db '- Bitcoin wallet address: `bc1qrghnt6cqdsxt0qmlcaq0wcavq6pmfm82vt'
                db 'xfeq`',0Ah
                db '- Payment instructions:',0Ah
                db '  1. Buy 0.1 bitcoin.',0Ah
                db '  2. Install session from: https://getsession.org/',0Ah
                db '  3. Contact us with this ID to receive the decryptor: 0538d726ae'
                db '3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9efb3d',0Ah
                db 0Ah
                db '## 📚 **How to buy bitcoin**',0Ah
                db '- Go to [Coinbase](https://www.coinbase.com/) or any similar webs'
                db 'ite like [Blockchain](https://www.blockchain.com/), use your cred'
                db 'it card to buy bitcoin (0.1 BTC), and then send it to the wallet '
                db 'address.',0Ah
                db 0Ah
```

Figure 20 – FunkSec ransomware note.

Summary

This report provides an in-depth analysis of FunkSec, a ransomware group with apparent hacktivist tendencies. The custom encryptor, developed by an inexperienced Algerian author, features AI-assisted elements which enables rapid development and improvement. FunkSec's data leaks often recycle information from previous hacktivist campaigns, casting doubt on the authenticity of their claims. Despite these limitations, their Tor-based operations and low ransom demands have drawn widespread attention in cybercrime forums.

FunkSec's operations highlight the role of AI in malware development, the overlap between hacktivism and cybercrime, and the challenges in verifying leaked data. It also raises questions about how we assess the threat posed by ransomware groups, as we often rely on the groups' own claims. These findings reflect a changing threat landscape, where even low-skill actors can make use of accessible tools to cast a very large shadow.

Harmony Endpoint provides comprehensive endpoint protection at the highest security level, crucial to avoid security breaches and data compromise and protects against this threat.

IOCs:

```
c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd
dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac
b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd
e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22
20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d
dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603
```

GO UP
BACK TO ALL POSTS