CrazyHunter Campaign Targets Taiwanese Critical Sectors

By Maristel Policarpio, Sarah Pearl Camiling, Jacob Santos, Cj Arsley Mateo, Ieriz Nicolle Gonzalez (words)

Published: 2025-04-16 · Archived: 2026-04-05 23:50:21 UTC

Ransomware

This blog entry details research on emerging ransomware group CrazyHunter, which has launched a sophisticated campaign aimed at Taiwan's essential services.

By: Maristel Policarpio, Sarah Pearl Camiling, Jacob Santos, Cj Arsley Mateo, Ieriz Nicolle Gonzalez Apr 16, 2025 Read time: 8 min (2087 words)

Key takeaways

- CrazyHunter has established itself as a significant ransomware threat, specifically targeting Taiwanese organizations, predominantly in healthcare, education, and industrial sectors. Attacks on these critical sectors could disrupt the delivery of essential services.
- CrazyHunter employs sophisticated techniques, notably the Bring Your Own Vulnerable Driver (BYOVD) method, which allows them to circumvent security measures effectively.
- The group broadened its toolkit by integrating open-source tools from GitHub, such as the Prince Ransomware Builder and ZammoCide, to further enhance their operational capabilities.
- Approximately 80% of CrazyHunter's toolkit consists of open-source tool. It is important to monitor and secure these resources to prevent the adaptation for malicious use.
- Trend Vision One™ detects and blocks the malicious components used in the CrazyHunter campaign. Trend Vision One customers can also access hunting queries, threat insights, and intelligence reports to gain rich context on the latest CrazyHunter IoCs. For additional best practices, see security recommendations provided below.

CrazyHunter has quickly emerged as a serious ransomware threat. The group made their introduction in the past month with the opening of their data leak site where they posted ten victims – all located from Taiwan. We have followed some of their operations through internal monitoring since the start of January and have witnessed a clear pattern of specifically targeting organizations in Taiwan. The victims of the group consists mainly of hospitals and medical centers, educational institutions and universities, manufacturing companies, and industrial organizations, which reflects a targeted focus on organizations with valuable data and sensitive operations.

This report introduces the tactics, techniques, and procedures (TTPs) utilized by CrazyHunter. It highlights the use of Bring Your Own Vulnerable Driver (BYOVD) and open-source tools on the GitHub platform, like the Prince ransomware builder. Recent findings indicate CrazyHunter's toolset expansion, modification of the tools it initially used, and improved capability.

During hunting in our internal telemetry, we encountered malicious artifacts that contains the following interesting items: a hack tool taking advantage of Group Policy Object (GPO) policies, a vulnerable driver exploits in the form of a process killer, and a few executable files compiled with the Go programming language.

Key findings on CrazyHunter's campaigns

The addition of the Prince ransomware builder in their toolkit is especially concerning. This tool is readily accessible from GitHub and further lowers the barriers to entry for cybercriminals by providing a user-friendly means to create ransomware variants. Its BYOVD technique to evade security shows its advanced methods. Improvements on newly shared utilities from SharpGPOAbuse, better AV/EDR capabilities, and Go-compiled executables have made CrazyHunter's operations increasingly prevalent.

CrazyHunter's emergence presents a significant threat to critical sectors in Taiwan, particularly in sectors such as healthcare and education. Disruptions in these areas could affect the delivery of essential services.

During our investigation, we identified three main points of interest:

- Use of open-source software found on GitHub.
- An enhanced toolkit and tools for implementation.
- Attacks focusing mainly on Taiwan.

Our research discovered that the attackers strategically and deliberately targeted Taiwan, which indicates a campaign specifically against the region. They used open-source tools from GitHub and expanded their range of tools and methods to increase the sophistication of their operations.

The use of open-sourced tools from GitHub

Around 80% of CrazyHunter's toolset consists of open-source tools from GitHub. Our observations suggest that they modify these freely available source codes to fit their specific needs and significantly enhance their capabilities.

We've identified three open-sourced tools that came from GitHub, each serving a distinct purpose:

Defense Evasion

The group uses a tailored variant of an open-source process killer tool called **ZammoCideopen on a new tab** and adapts it to be an AV/EDR killer capable of terminating processes belonging to EDR products through a BYOVD approach taking advantage of the vulnerable driver *zam64.sys*.

Based on our internal telemetry, we observed that the group attempted to use modified versions of these tools in its attacks. We have numbered these versions according to their respective improvements and modifications. You may view the full details here.

Upon execution, it looks for the vulnerable Zemana Anti-Malware driver (zam64.sys) in the default path folder to exploit its ability to terminate high-privileged processes. It then creates and starts a service called "*ZammOcide*," which loads the driver and exposes a device object at \\.\ZemanaAntiMalware. A user-mode process communicates with the driver via IOCTL codes, triggering a kernel mode operation to forcefully terminate processes.

```
if ( (unsigned __int8)main_LoadDriver(
                        (int)"C:\\Users\\public\\zam64.sys",
                        25,
                        (int)"ZammOcide",
                        9,
                        os_Args,
                        qword_56BC08,
                        v2,
                        v3,
                        v4) )
{
  v18 = syscall_StringToUTF16Ptr((unsigned int)"\\\\.\\ZemanaAntiMalware", 21, v13, 9, v8, v14, v15, v16, v17, v25);
  golang_org_x_sys_windows_CreateFile(v18, -1073741824, 0, 0, 3, 128, 0, v19, v20, v25, v27, HIDWORD(v27));
  v34[0] = &RTYPE_string;
```

The program targets and terminates specific hardcoded process names, primarily associated with AV and EDR products, while also targeting processes from Microsoft Defender and Avira. While the disabler runs, it continuously terminates these processes, even if they respawn with different IDs.

Privilege Escalation / Lateral Movement

The team makes use of **SharpGPOAbuseopen on a new tab**, to exploit Group Policy Objects (GPO). Taking advantage of the edit rights the user possesses on a GPO, they are in a position to compromise the objects controlled through the GPO and therefore, deploy payloads and attain privilege escalation and lateral movements in the victim's network.

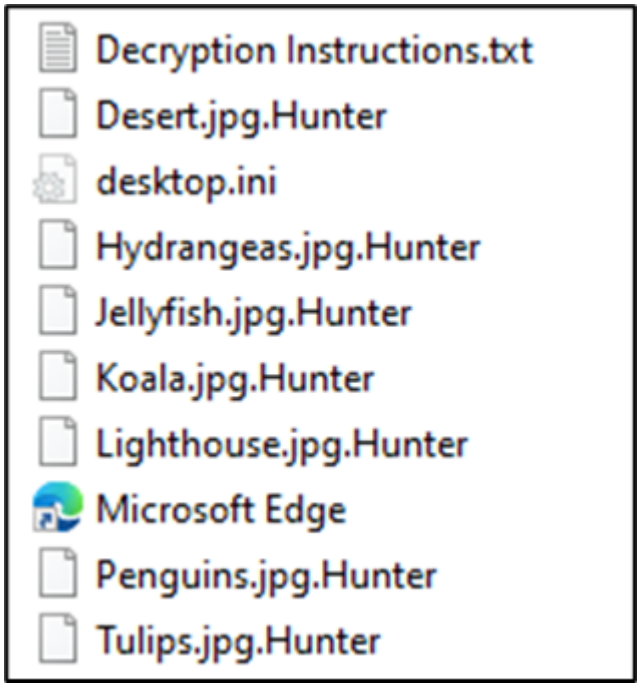
```
C:\Users\Win10x64\Desktop>gpo.exe

Usage:
        SharpGPOAbuse.exe <AttackType> <AttackOptions>

Attack Types:
--AddUserRights
        Add rights to a user account
--AddLocalAdmin
        Add a new local admin. This will replace any existing local admins!
--AddComputerScript
        Add a new computer startup script
--AddUserScript
        Add a new user startup script
--AddComputerTask
        Add a new computer immediate task
--AddUserTask
        Add a new user immediate task
```

Impact (Ransomware)

The attack is spearheaded by a variant of Prince ransomwareopen on a new tab, a Go-based bespoke ransomware. The ransomware uses ChaCha20 and ECIES encryption to encrypt the files securely, and the attackers have customized it the addition of the ".Hunter" extension to the encrypted files. The ransomware drops a ransom note named "Decryption Instructions.txt," modifies the victim's desktop wallpaper, and demands a ransom payment.



The lists below detail the extensions and directories whitelisted by the ransomware. These whitelisted items are excluded from encryption, allowing critical system functions and specific applications to continue running. This strategy helps evade detection and facilitates the ransomware's objectives.

List of whitelisted extension:

- .bat
- .com
- .dll
- .exe
- .inf
- .ini
- .lnk
- .msi
- .ps1
- .reg
- .scr
- .sys
- .vbs

List of whitelisted directories:

- .dotnet
- .gradle
- .nuget
- .vscode
- \\system volume information
- appdata
- boot
- efi
- intel

- microsoft
- msys64
- perflogs
- program files
- program files (x86)
- programdata
- public
- public
- system volume information
- system32
- windows

An expanded toolset and methods of execution

The attackers have not only relied on open-source tools but have also broadened their toolset and methods of execution. This indicates a strategic effort to enhance the complexity and effectiveness of their operations, ensuring the success of their attacks

Execution

The group utilizes a batch script to execute multiple binaries, ultimately leading to the deployment of the ransomware payload.

```
@echo off
start C:\Users\Public\go2.exe
timeout /t 10 /nobreak > nul
start C:\Users\Public\go.exe
timeout /t 10 /nobreak > nul
start C:\Users\Public\go3.exe

tasklist /FI "IMAGENAME eq go.exe" 2>NUL | find /I "go.exe" > NUL
if %errorlevel% equ 0 (
    echo go.exe is running.
) else (
    start C:\Users\Public\av-1m.exe
)

timeout /t 10 /nobreak > nul

start C:\Users\Public\bb.exe -f C:\Users\Public\crazyhunter.sys
timeout /t 60 /nobreak > nul

tasklist /FI "IMAGENAME eq bb.exe" 2>NUL | find /I "bb.exe" > NUL
if %errorlevel% equ 0 (
    echo bb.exe is running.
) else (
    start C:\Users\Public\crazyhunter.exe
)
```

The script initiates a sequence to deploy ransomware while avoiding detection:

1. Initial Execution:

- Run *go2.exe* and *go.exe* to exploit *zam64.sys* for disabling processes.
- Launch *go3.exe* for ransomware deployment.

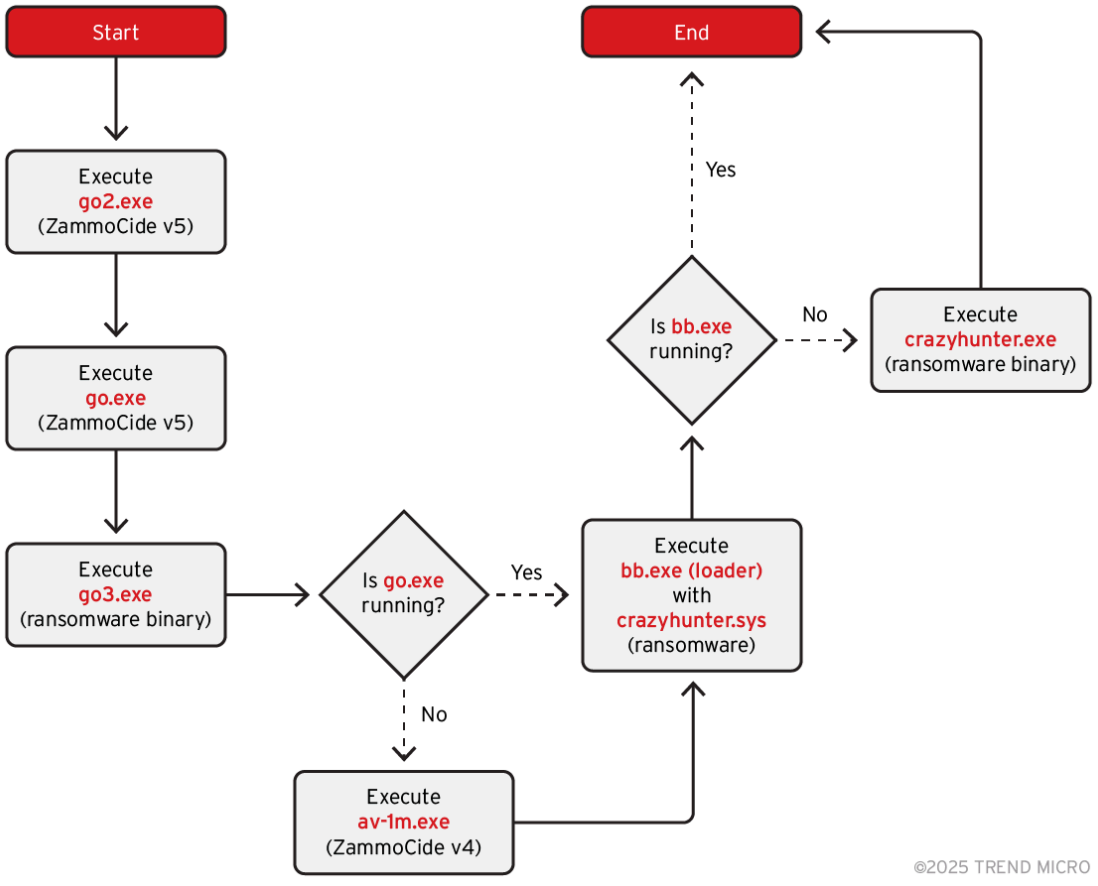
2. Ensuring Anti-AV Measures:

- If *go.exe* is not running, execute *av-1m.exe* (similar functionality to *go2.exe* and *go.exe*, but compiled in C++).

3. Final Ransomware Deployment:

- To evade detection, use *bb.exe* to load and execute *crazyhunter.sys* for ransomware deployment.
- If *crazyhunter.sys* execution fails, launch the compiled EXE version of the ransomware for final deployment.

These redundant measures ensure that ransomware deployment remains effective even if primary methods fail. Figure 6 illustrates the flowchart of the ransomware deployment process to visualize these events.



Persistence / Exfiltration

Another Go-based program named "file.exe" is also used. It serves as a monitoring tool for changes in Web-related files and a file server for potential exfiltration. Its main function provides two primary operating modes:

1. **Monitor Mode** - Periodically scans files with specific extensions
2. **File Server Mode** - Runs a web server on a configurable port

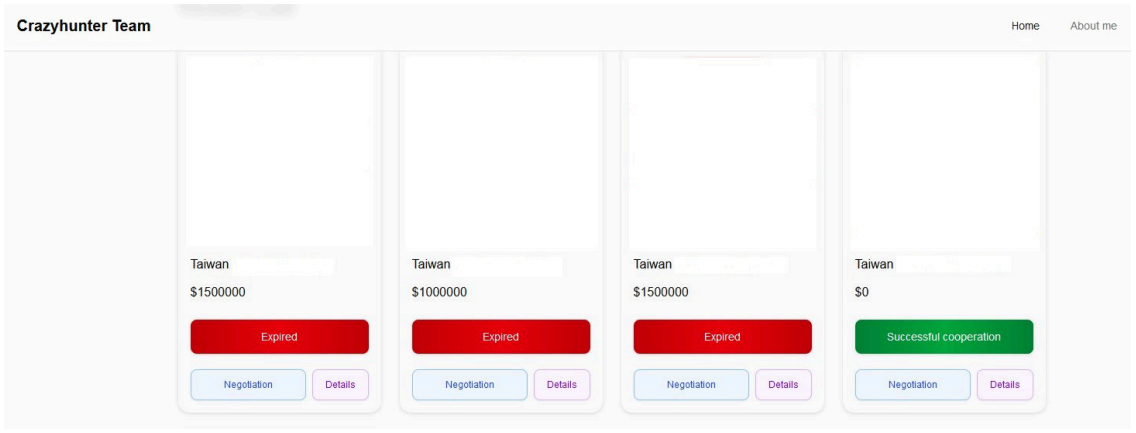
This file accepts several command-line flags:

Flag	Type	Default	Description
-white	bool	FALSE	Toggle between whitelist (true) and blacklist (false) mode
-e	string	".asp"	File extensions to monitor (.asp, .php, .jsp)
-d	string	Current path	Directory path to monitor or serve
-func	string	""	Function mode: "monitor" or "fileserver"
-port	int	9999	Port number for file server mode
-f	string	"1.asp"	Files to exclude from monitoring
=-t	int	1000	Time interval in seconds (1000=1S)

Table 1: Command-Line parameters of file.exe with its description

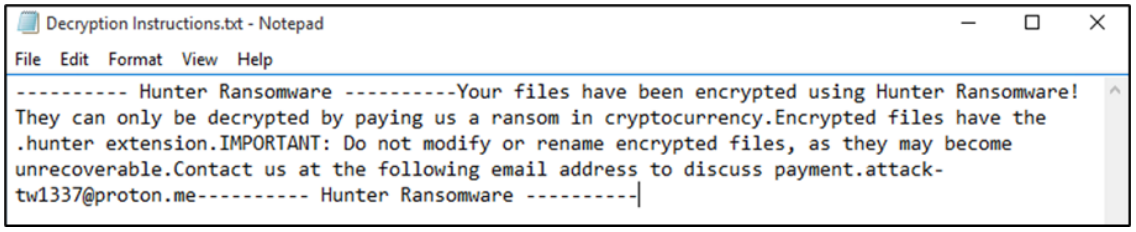
Attacks focusing mainly on Taiwan

The geographical focus of these attacks has been predominantly on Taiwan, indicating a targeted campaign against this specific region. Based on their leak site, the ten victims identified are from Taiwan. Our internal data also reveals that this group exclusively targets small and medium-sized businesses within Taiwan.



We also observed that the customized group contact email, ***payment[.]attack-tw1337@proton[.]me***, prominently displayed on the ransom note, contains the "***tw***" designation. This suggests that the ransomware group specifically

targets Taiwanese entities.



The strategic use of open-source tools from GitHub significantly enhanced the group's capabilities for defense evasion, lateral movement, and impactful operations. By expanding their toolset and methods of execution, attackers have demonstrated an evolution in their strategies along with their persistence. Their deliberate and focused campaign stresses the growing threat they pose. This highlights the pressing need for strong cybersecurity measures to counteract the advanced techniques used by ransomware groups.

Security recommendations

Ransomware is a growing threat, and enterprises must adopt a proactive approach to safeguard their operations. Here are general best practices, including specific guidelines to protect against threats leveraging Bring Your Own Vulnerable Driver (BYOVD) techniques and open-source tools from platforms like GitHub:

- Ensure users only have access to the data and systems essential for their roles.
- Require MFA for all user accounts, particularly for administrative access.
- Ensure that all operating systems, applications, and drivers are regularly updated and patched to eliminate known vulnerabilities.
- Perform daily backups of critical data and systems to an isolated environment that ransomware cannot reach.
- Periodically audit user permissions and revoke those that are no longer needed.
- Utilize endpoint protection software that specifically guards against BYOVD techniques by monitoring and blocking unauthorized driver installations.
- Regularly conduct training sessions to help employees recognize phishing attempts, suspicious links, and other common attack vectors.
- Maintain an inventory of all device drivers in use and regularly review them for any unauthorized installations or modifications.
- Regularly review the list of installed drivers and disable any that are not in use to minimize potential attacks.
- Ensure that only approved versions of drivers are allowed and that they are kept up-to-date.

Proactive security with Trend Vision One™

Trend Vision Oneone-platform™ is the only AI-powered enterprise cybersecurity platform that centralizes 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 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 can

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]

- *Critical Threat: CrazyHunter Ransomware Leverages BYOVD Against Taiwan's Vital Services*

Trend Vision One Threat Insights App

- **Emerging Threats:** Critical Threat: CrazyHunter Ransomware Leverages BYOVD Against Taiwan's Vital Services

Hunting Queries

Trend Vision One Search App

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.

BYOVD Attack Using Zemana Anti-Malware (ZAM64) – Registry Modification Detected

eventSubId: 402 AND objectRegistryKeyHandle: ZammOcide AND objectRegistryData: zam64.sys

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabledproducts.

Indicators of Compromise (IoC)

The indicators of compromise for this entry can be found here.

Tags
