Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Go-Based CrazyHunter Ransomware Strikes Taiwan

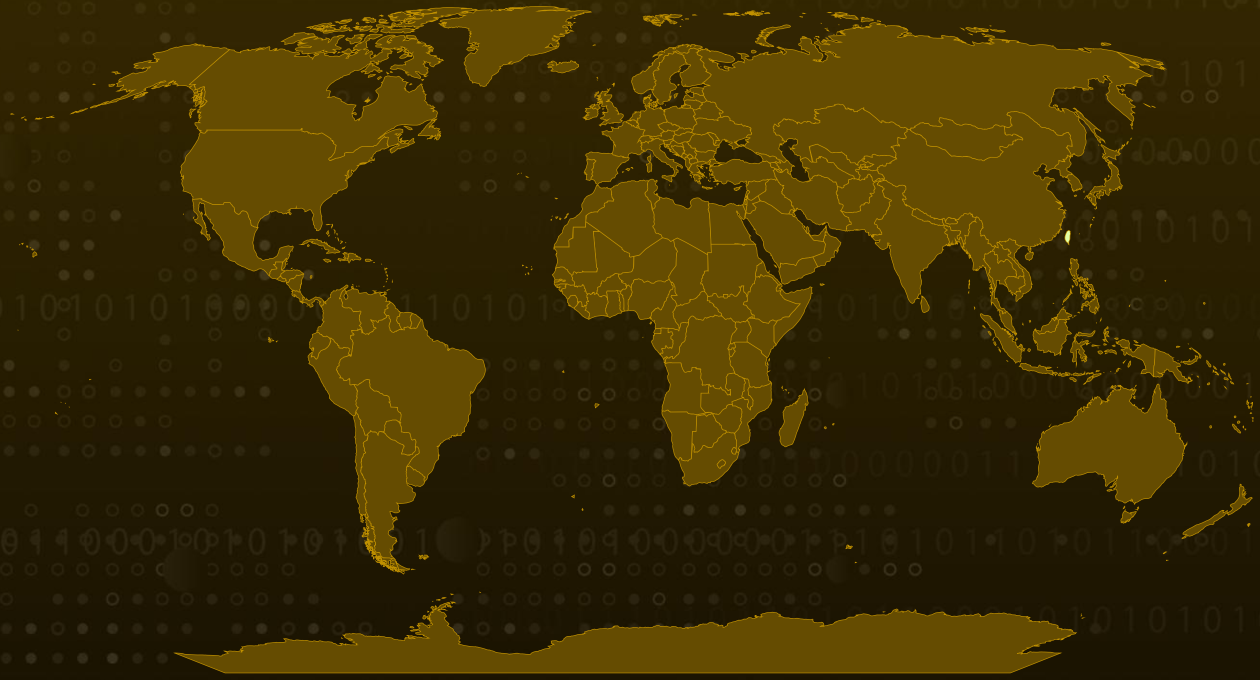
Date of Publication	Admiralty Code	TA Number
April 25, 2025	A1	TA2025128

Summary

Active Since: January 2025
Malware: CrazyHunter Ransomware
Ransom: $800,000 - $1,500,000
Targeted Country: Taiwan
Targeted Industries: Healthcare, Education, Manufacturing, Technology, Retail, Electronics

Attack: CrazyHunter, a new Go-based ransomware spotted in January 2025, is aggressively targeting Taiwan's critical sectors. Built on the open-source Prince encryptor and powered by 80% open-source tools. With a growing victim count and evolving methods, CrazyHunter poses a serious, adaptive threat to the region's operational security.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 In January 2025, a formidable new ransomware operation known as CrazyHunter emerged on the cyber threat landscape, swiftly establishing itself as a major adversary against Taiwanese organizations. From the outset, the group's campaigns have shown a clear focus to infiltrate and disrupt critical infrastructure sectors such as healthcare, education, and industrial manufacturing areas where operational downtime can have profound societal consequences.

#2 At its core, CrazyHunter is a Go-based ransomware strain, evolved from the open-source Prince encryptor family. Once deployed, it encrypts victims' files and leaves behind a ransom note titled "Decryption Instructions.txt", mimicking the formatting of earlier Prince ransomware attacks. However, what sets CrazyHunter apart is its highly adaptive and resourceful approach to operational tactics.

#3 One of the group's distinguishing characteristics is its extensive use of open-source tools, a strategic decision that lowers development costs while complicating attribution efforts. Approximately 80% of their toolkit comprises publicly available resources, carefully repurposed for malicious operations.

#4 Among these is ZammoCide, an open-source process termination utility, which the group has modified into an AV/EDR killer by exploiting a vulnerable driver to disable endpoint protection mechanisms. They leverage techniques such as Bring Your Own Vulnerable Driver (BYOVD) to bypass security controls, exploiting weaknesses in legitimate drivers to gain deeper system access.

#5 Additionally, tools like SharpGPOAbuse are employed for lateral movement within networks, while Donut is used to generate shellcode from PE files, facilitating payload delivery. The continuous evolution of CrazyHunter's tactics underscores a deliberate strategy to adapt and weaponize publicly accessible tools, enhancing their evasion techniques while maintaining operational agility.

Recommendations

System Hardening: Disable or remove legacy and unnecessary services and drivers to reduce the attack surface. Apply security baselines across servers and workstations to enforce best-practice configurations.

Network Segmentation and Zero Trust Principles: Segment networks by role and criticality, isolating domain controllers. Adopt Zero Trust Network Access (ZTNA) principles by verifying every connection and enforcing contextual security policies.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0009 Collection	TA0010 Exfiltration
TA0040 Impact	TA0042 Resource Development	T1059 Command and Scripting Interpreter	T1055 Process Injection

T1055.002 Portable Executable Injection	T1068 Exploitation for Privilege Escalation	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1078 Valid Accounts	T1211 Exploitation for Defense Evasion	T1036 Masquerading	T1027 Obfuscated Files or Information
T1087 Account Discovery	T1021 Remote Services	T1005 Data from Local System	T1071.001 Web Protocols
T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact	T1105 Ingress Tool Transfer	T1588 Obtain Capabilities
T1588.001 Malware			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	bb.execrazyhunter.sys, file.exe, go.exe, go2.exe, go3.exe, crazyhunter.exe, gpo.exe, ru.bat, zam64.sys
File Path	C:\Users\Public\Prince-Built.exe
URLs	hxxps[:]//t[.]me/Magic13377, hxxps[:]//t[.]me/CrazyHuntersTeam
TOR Address	7i6sfmfvmqfaabjksckwrttu3nsbopl3xev2vbxbkghsivs5lqp4yeqd[.]onion
Tox	E8481B6E149862EEEA79668EBBC50B96A6B6529C5DDD905491E2F838EF7D174FB73DB97F1FFD

TYPE	VALUE
Email	payment[.]attack-tw1337[@]proton[.]me
SHA1	0937377d1ef1d47a04f1e55d929fe79c313d7640, 1b826a12a630e777aa2c3036f1159db15f2bdd66, 15823b729ad7aad20192ebe3fc1c21ea985001d7, 318a601a5d758dd870c38b8c4792a2c3405e6c28, 79c3fd97d33e114f8681c565f983cd8b8f9d8d93, b6737248f7baed88177658598002df5433155450, bed4229e774f136e1898fad9d37bd96e9156369e, 9e126627dff082000a830b8e2e04206ced8663ff, 086262abb7e85c43ffb6c384966d130ca612169b, cd248648eafca6ef77c1b76237a6482f449f13be

Recent Breaches

https://analog.com.tw/
https://www.johnsonfitness.com/
https://www.asia.edu.tw/
http://huachengsz.com/

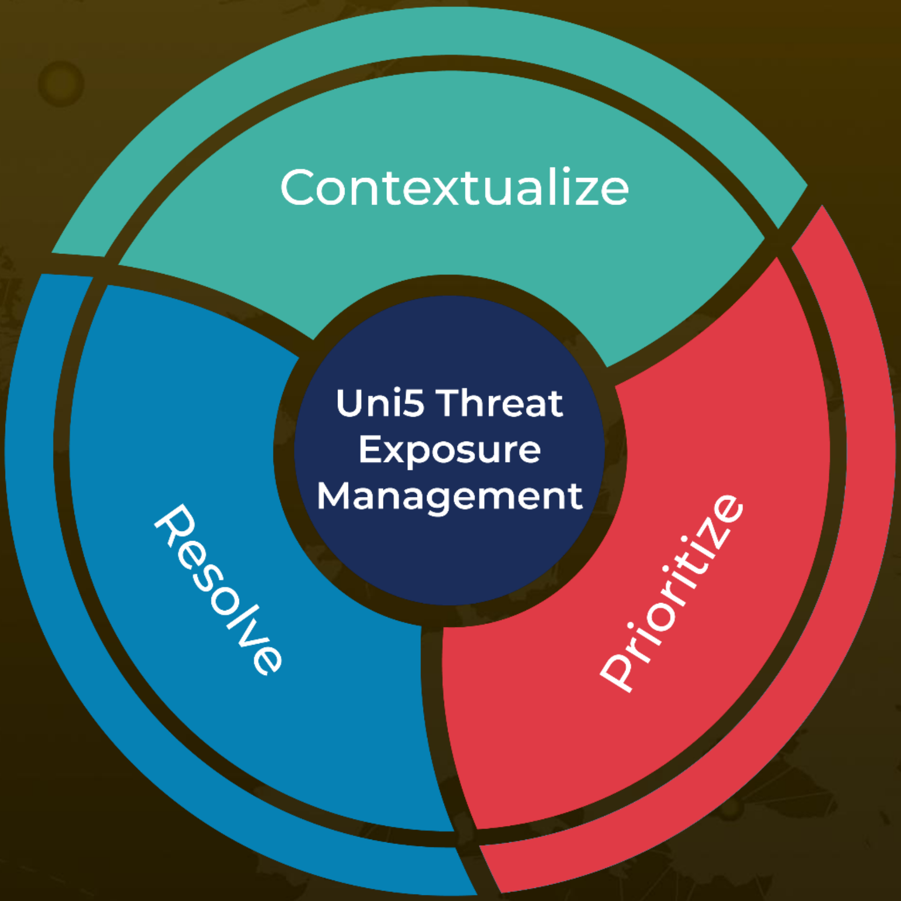
References

https://www.trendmicro.com/en_us/research/25/d/crazyhunter-campaign.html

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

April 25, 2025 • 6:30 AM

More at www.hivepro.com