27 January 2026

TLP: WHITE

INTEL471

EMERGING THREATS

CrazyHunter Ransomware Group

The CrazyHunter ransomware variant emerged as a highly disruptive ransomware threat observed throughout 2025, with campaigns heavily targeting organizations in Taiwan, and a notable focus on critical sectors such as healthcare. Researchers observed CrazyHunter being deployed in real-world incidents where operational impact was immediate, including a case study involving a hospital environment where compromise resulted in widespread disruption and system encryption. The threat group demonstrates a clear evolution from opportunistic execution into a repeatable and stealth-driven intrusion operation, combining ransomware deployment with defense evasion techniques that significantly increase the likelihood of success. It is worthy to note that reporting attributes CrazyHunter to a Prince ransomware fork, which indicates the actors are leveraging an existing ransomware codebase while operationalizing it into a distinct campaign structure tailored for real-world enterprise attacks.

THREAT SUMMARY

The CrazyHunter ransomware variant emerged as a highly disruptive ransomware threat observed throughout 2025, with campaigns heavily targeting organizations in Taiwan, and a notable focus on critical sectors such as healthcare. Researchers observed CrazyHunter being deployed in real-world incidents where operational impact was immediate, including a case study involving a hospital environment where compromise resulted in widespread disruption and system encryption. The threat group demonstrates a clear evolution from opportunistic execution into a repeatable and stealth-driven intrusion operation, combining ransomware deployment with defense evasion techniques that significantly increase the likelihood of success. It is worthy to note that reporting attributes CrazyHunter to a Prince ransomware fork, which indicates the actors are leveraging an existing ransomware codebase while operationalizing it into a distinct campaign structure tailored for real-world enterprise attacks.

Over the past several months, CrazyHunter's operational behavior has shown signs of increased maturity, specifically through the consistent use of stealth tactics and security tooling suppression prior to encryption. Instead of immediately encrypting systems upon access, the actors have been observed preparing environments by escalating privileges and weakening endpoint protections, allowing them to execute ransomware in a way that maximizes business interruption. This is especially damaging for healthcare and other high-availability sectors, where downtime can directly impact patient care, logistics, and critical services. Given CrazyHunter's ability to combine stealth intrusion activity with ransomware execution at scale, it is important to assess, understand, and prepare for this threat as it continues evolving and expanding across additional organizations and regions.

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

SYNOPSIS

In observed CrazyHunter intrusions, the ransomware deployment sequence is structured around stealth, privilege enablement, and reducing resistance from security controls before the encryption phase begins. Researchers describe CrazyHunter as being linked to a Prince ransomware fork, which aligns with its ransomware behavior and execution pattern, while also highlighting that the operators demonstrate deliberate tradecraft instead of pure commodity execution. A particularly important detail that sets CrazyHunter apart is the use of BYOVD techniques, where the attackers leverage a legitimate but vulnerable driver to gain elevated control over the system and interfere with endpoint defenses. In reporting tied to CrazyHunter, the driver zam64.sys, associated with Zemana AntiMalware, is identified as being abused in order to disable or degrade protective tooling and increase the success rate of ransomware execution across enterprise endpoints.

Once defensive posture is weakened, CrazyHunter can proceed with encryption at scale, impacting a large number of systems in a short time window and creating immediate operational disruption. The documented hospital case study supports a pattern of preparation followed by high-impact execution, where attackers prioritize broad system reach and ransomware detonation that cripples availability and business continuity. This approach allows CrazyHunter operators to compromise victim systems more effectively, evade detection long enough to stage execution, and encrypt endpoints in environments that require uptime. Given the ability to disable defenses through driver abuse and then deploy encryption broadly, CrazyHunter represents a serious operational threat, especially to healthcare networks and critical infrastructure sectors that may not be able to tolerate extended downtime or system-wide disruption.

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

CRAZYHUNTER RANSOMWARE HUNT COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('e7602d04-10c8-4ef4-90c7-ac3b639e2bc2'),touched:!t)

RELATED HUNT PACKAGES

Timeout Delayed Execution

https://hunter.cyborgsecurity.io/research/hunt-package/350e41b2-b2b7-410b-85cc-74a3536a5950

Potential Use of Findstr or Find with Tasklist

https://hunter.cyborgsecurity.io/research/hunt-package/ee9bb6c4-378e-498e-ad04-fe469da49046

SharpGPOAbuse Tool Utilization

https://hunter.cyborgsecurity.io/research/hunt-package/2a76099b-8991-44c2-b3fc-82b367bad3ca

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

MITRE CONTEXT

- MITRE Tactic Names:
  - Persistence
  - Defense Evasion
  - Privilege Escalation
  - Discovery
- MITRE Technique Names:
  - Group Policy Modification
  - Time Based Evasion
  - Account Manipulation
  - Security Software Discovery
- MITRE Technique IDs:
  - T1484.001
  - T1497.003
  - T1098
  - T1518.001

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

REFERENCES

1. https://www.trellix.com/blogs/research/the-ghost-in-the-machine-crazyhunters-stealth-tactics/
2. https://www.trendmicro.com/en_us/research/25/d/crazyhunter-campaign.html
3. https://teamt5.org/en/posts/the-case-study-hospital-crazyhunter-ransomware-attack/
4. https://socradar.io/blog/dark-web-profile-crazyhunter-ransomware/

Copyright © 2026 Intel 471, Inc. All Rights Reserved.