Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

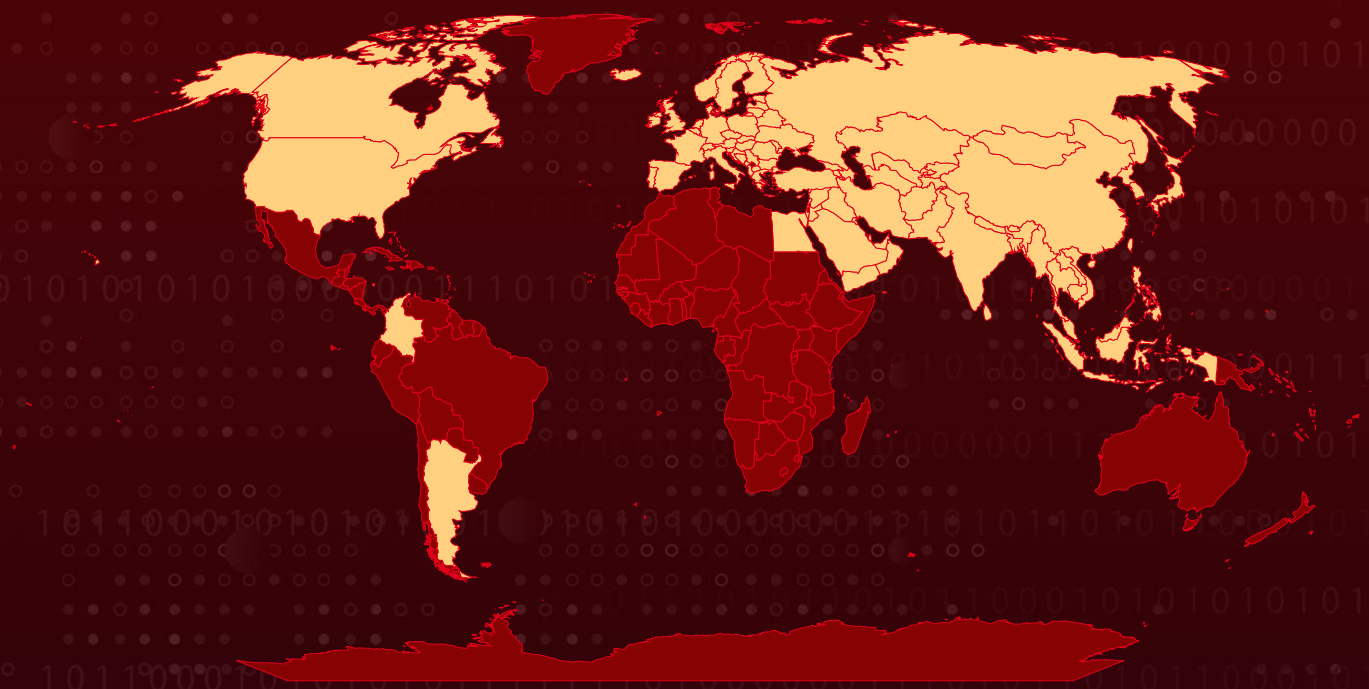
Crypto24 Ransomware Disrupts Businesses Using Custom EDR Bypass

Date of Publication	Admiralty Code	TA Number
August 20, 2025	A1	TA2025255

Summary

First Seen: September 2024
Malware: Crypto24 Ransomware
Affected Platform: Windows
Targeted Regions: Asia, Europe, Egypt, Canada, United States, Argentina, Colombia
Targeted Industries: Accounting Services, Aerospace, Agriculture, Banking, Business Services & Consulting, Defense, Education, Entertainment, Financial Services, Food Service, Gambling, Gaming, Healthcare, Human Resources, Insurance, IT, Legal, Logistics, Manufacturing, Pharmaceutical, Technology, Telecommunications, Transportation
Attack: Crypto24 ransomware, first detected in late 2024, has rapidly evolved into a global cyber threat, targeting critical industries across Asia, Europe, and the U.S. By combining legitimate IT tools with custom malware, the group carries out stealthy multi-stage attacks designed to evade defenses, maintain persistence, and deploy ransomware payloads. Its peak activity in mid-2025 marked a calculated surge, establishing Crypto24 as one of the most adaptive and disruptive ransomware operations.

Attack Regions



Attack Details

#1 Crypto24 ransomware is a highly coordinated, multi-stage threat that leverages both legitimate administrative tools and custom-built malware to infiltrate networks, move laterally, and avoid detection. First identified in September 2024, Crypto24 remained relatively quiet until April 2025, when its activity began escalating.

#2 The group behind Crypto24 demonstrates careful planning and precision, often executing attacks during off-peak hours to minimize detection and maximize disruption. Their toolkit includes PSExec for lateral movement, AnyDesk for remote persistence, keyloggers for credential theft, multiple backdoors, and Google Drive for covert data exfiltration.

#3 Once inside a network, attackers establish persistence by enabling default Windows administrative accounts or creating new local users. They conduct reconnaissance using custom scripts to enumerate accounts, profile hardware, and analyze disk structures. Persistence is maintained through malicious Windows services and scheduled tasks, including WinMainSvc (a keylogger) and MSRuntime (a ransomware loader).

#4 To evade defenses, Crypto24 employs customized variants of RealBlindingEDR and abuses gpscript.exe to execute the legitimate Trend Vision One uninstaller. This tactic allows them to disable endpoint protections post-compromise with elevated privileges, an example of the “living off the land” approach where trusted tools are weaponized against organizations.

#5 Crypto24 activity surged in July 2025, marking its most aggressive campaign to date. Malaysia, the United States, and Italy were among the hardest-hit nations. In Malaysia, manufacturing, technology, and transportation were primary targets. U.S. organizations faced attacks on healthcare, education, and telecommunications, while Italy saw disruptions in aerospace, defense, and agriculture.

#6 This sustained offensive carried into August, demonstrating the group’s ability to strike multiple industries across regions simultaneously. The rise of Crypto24 underscores the evolving sophistication of ransomware operations. By blending into legitimate IT processes and exploiting trusted tools, threat actors are becoming increasingly difficult to detect and counter.

Recommendations

Strengthen Account and Access Controls: Regularly audit privileged accounts and restrict their creation and use. Disable unused or default administrative accounts. Implement multi-factor authentication (MFA) for all remote and high-privilege access.

Harden Remote Access and Network Configurations: Limit RDP and third-party remote tools (e.g., PsExec, AnyDesk) to authorized systems only. Routinely review and tighten firewall configurations to minimize exposure.

Enhance Monitoring and Detection: Detect and investigate unusual use of built-in Windows utilities and remote tools, which may indicate lateral movement. Regularly inspect scheduled tasks and service creations for unauthorized or suspicious activity. Monitor for unauthorized changes to system files and unusual outbound traffic, including data exfiltration attempts to cloud storage.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact

TA0011 Command and Control	**TA0010** Exfiltration	**T1133** External Remote Services	**T1059.003** Windows Command Shell
T1569.002 Service Execution	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1053** Scheduled Task/Job
T1136.001 Local Account	**T1078** Valid Accounts	**T1548.002** Bypass User Account Control	**T1053.005** Scheduled Task
T1562.001 Disable or Modify Tools	**T1562.004** Disable or Modify System Firewall	**T1056.001** Keylogging	**T1562** Impair Defenses
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1021** Remote Services	**T1087** Account Discovery
T1071 Application Layer Protocol	**T1548** Abuse Elevation Control Mechanism	**T1567.002** Exfiltration to Cloud Storage	**T1105** Ingress Tool Transfer
T1486 Data Encrypted for Impact	**T1071.001** Web Protocols	**T1574.001** DLL	**T1056** Input Capture
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4aaf5558277d742b180e3208e4340cc98dd0b94baf5c940c5ef0b0c2d9eea707, 10c3317566f52eaeb45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b, 0e36b1837e5a2cbd14fac2c3b709a5470b7b488bd15898d30840ec60448e83e0, 47ba2db66791b92e6b5a12f35717bbe6286777794b7964efb6a509e51a4e74f1,

TYPE	VALUE
SHA256	d2294aa892494220bd08e6cbbd16e3b744d03074a56dd897adc3614111cdc53d, 3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac, 686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac, 24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73
SHA1	c4da41d0f40152c405ba399a9879d92b05ac1f61, ba4685594714e3ffde4f52a82cc07c6f94324215, a60c6a07d3ba6c2d9bf68def208566533398fe8f, dd389b5f3bb7e946cc272bf01d412d661635f10b, 9a9f52554c1a9938725b7dabd0f27002b0f8e874, e573f4c395b55664e5e49f401ce0bbf49ea6a540, 71a528241603b93ad7165da3219e934b00043dd6, 74bc31f649a73821a98bef6e868533b6214f22a4, b23d0939b17b654f2218268a896928e884a28e60, 093902737a7850c6c715c153cd13e34c86d60992, 5d1f44a2b992b42253750ecaed908c61014b735a, 8057d42ddb591dbc1a92e4dd23f931ab6892bcac, eeafb2d4f6ed93ab417f190abdd9d3480e1b7b21, 3922461290fa663ee2853b2b5855afab0d39d799
Email	crypto24support[@]pm[.]me, noreply[@]crypto24lab[.]com
TOR Address	j5o5y2feotmhvr7cbcp2j2ewayv5mn5zenl3joqwx67gtfchhezjznad[.]onion

Recent Breaches

https://palmgold-mgmt.com/
https://cms.law/en/int/
https://www.karndean.com/
https://www.sunnydayssunshinecenter.com/
https://www.soubeiranchobet.com.ar/
https://transcore.com/
https://larimart.it/
https://www.warisantc.com/
https://www.tanchonggroup.com/
https://www.terracellars.es/
https://www.tanchong.com/en/index.aspx
https://www.arianadx.com/

https://www.sagence-ai.com/
https://www.ourforte.com/
https://www.tientuan.com.vn/
https://choice.de/
http://www.elaser.com.tw/
https://mkklaw.net/
https://www.taxplann.ca/
https://iris.com.co/
https://www.technoforte.co.in/
https://www.modulusgroup.eu/en/
https://www.ibsns.com/

References

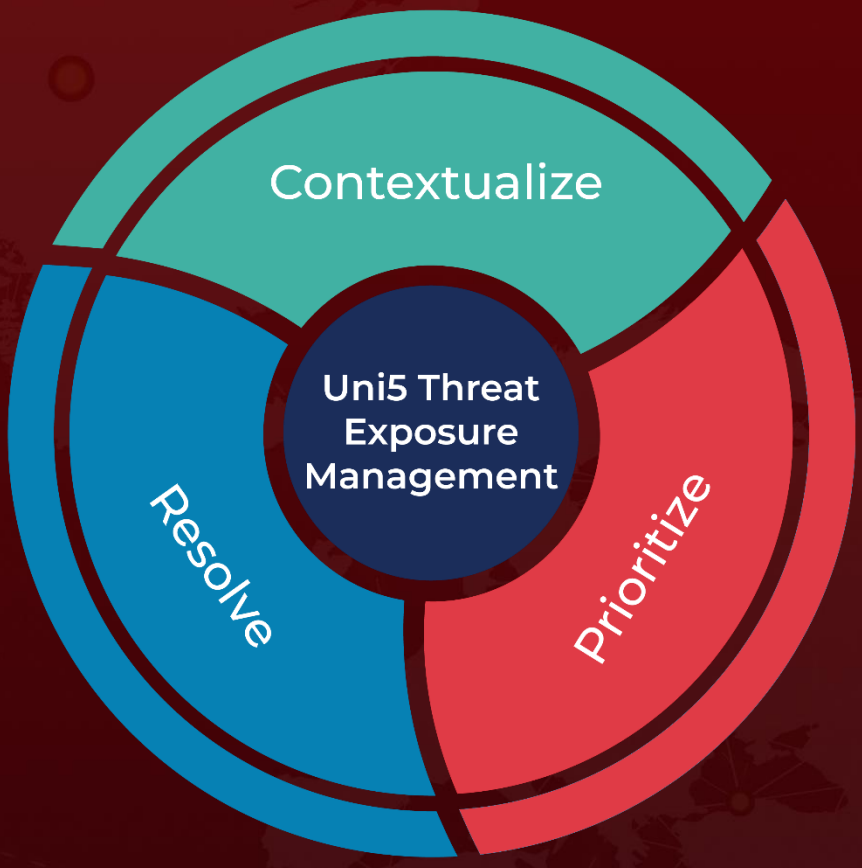
https://www.trendmicro.com/en_nl/research/25/h/crypto24-ransomware-stealth-attacks.html

https://www.sangfor.com/blog/cybersecurity/vietnam-cmc-group-ransomware-attack-anatomy-asian-cyber-shock

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

August 20, 2025 • 7:00 AM

More at www.hivepro.com