Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

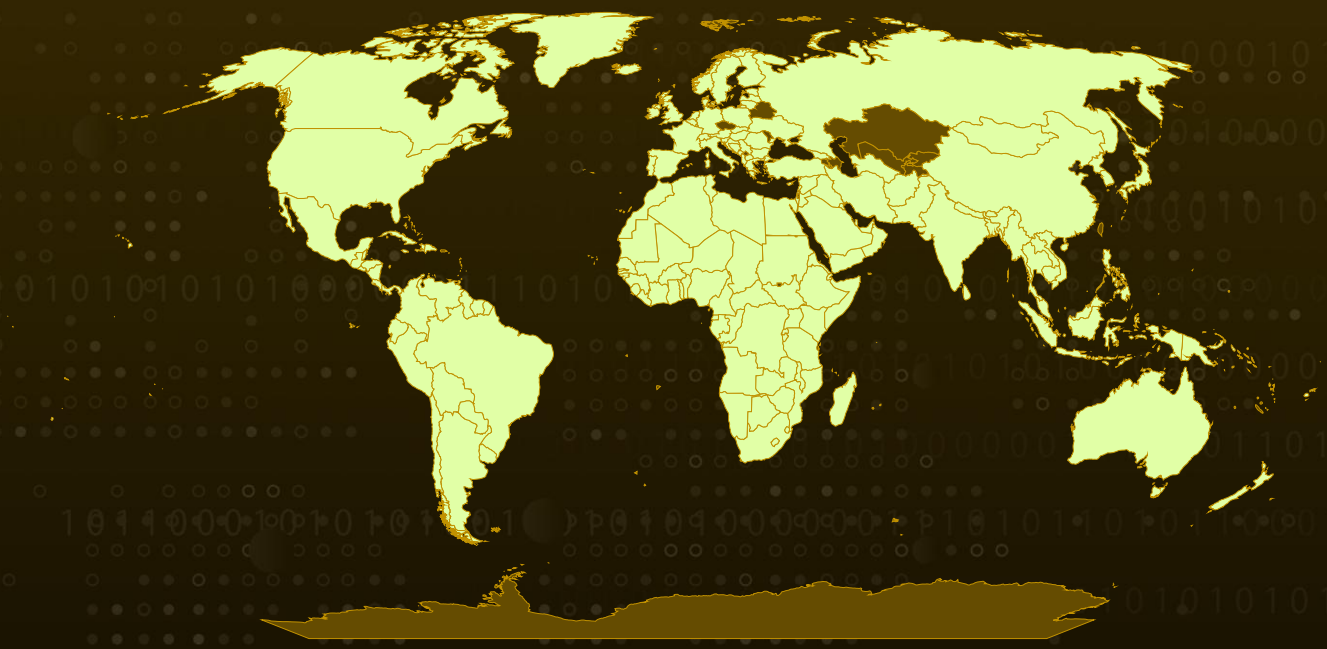
Katz Stealer: The Silent Thief Lurking in Trusted Apps

Date of Publication	Admiralty Code	TA Number
June 17, 2025	A1	TA2025190

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide (except CIS countries)
Affected Platform: Windows
Malware: Katz Stealer
Attack: Katz Stealer is a stealthy, malware-as-a-service threat that surfaced in 2025, designed to make credential theft easy and effective even for unskilled attackers. Delivered through phishing emails and fake software, it silently infiltrates systems, using clever tricks like hiding code in images, exploiting trusted tools like MSBuild and cmstp.exe, and hijacking apps like Discord to stay hidden and maintain access. Once active, it targets browsers to steal passwords, cookies, tokens, credit card details, and even crypto wallets decrypting sensitive data by mimicking legitimate browser behavior. Its reach spans email, VPNs, FTPs, gaming accounts, and over 150 crypto wallet extensions, all exfiltrated via encrypted channels to attacker-controlled servers.

Attack Regions



Attack Details

#1 Emerging in 2025, Katz Stealer has rapidly established itself as a formidable malware-as-a-service (MaaS) platform, offering a potent mix of credential theft, stealthy persistence, and system reconnaissance. Distributed via phishing campaigns and trojanized software downloads, it's built for stealth and efficiency. Katz Stealer can extract an alarming range of data from browser credentials and email logins to Discord tokens, VPN and Wi-Fi passwords, and even cryptocurrency wallets.

#2 Behind the scenes, Katz Stealer's infection chain is as intricate as it is evasive. The attack typically begins with a deceptive GZIP archive, delivered through phishing emails or distributed via cracked software websites. Inside lies an obfuscated JavaScript dropper that launches PowerShell commands via WScript.Shell, decoding and executing further payloads entirely in memory. The malware uses UAC bypasses, process hollowing via MSBuild, and scheduled tasks to ensure persistent access, all while avoiding disk writes that might trigger antivirus detection.

#3 Once active, Katz Stealer embeds itself within trusted processes like MSBuild or Discord to maintain a low profile. It then connects to a C2 server, fetching additional modules for stealing sensitive data. These include .NET-based loaders and credential-harvesting DLLs that quietly run with system-level privileges. The malware uses stealthy tricks like geofencing, sandbox evasion, and delayed execution to avoid early detection, while its use of HTTPS and spoofed browser headers helps blend network traffic with legitimate activity.

#4 Katz Stealer is especially dangerous to web users and crypto holders. It targets Chromium-based browsers and Gecko-based ones, decrypting password stores and cookie files by mimicking the browsers' own decryption routines. The malware bypasses Chrome's Application-Bound Encryption (ABE) using native Windows APIs and pulls key credential files from Firefox profiles for offline decryption. It also goes after cryptocurrency wallets copying sensitive wallet files and seeds from apps like Exodus, Electrum, and Daedalus. Even browser extensions tied to crypto wallets aren't safe, with the malware scanning for over 150 targeted extension IDs.

#5 Perhaps most insidiously, Katz Stealer compromises the Discord desktop app for ongoing access. It injects backdoor code into Discord's startup script, which quietly connects to the attacker's server and executes remote commands all while letting Discord appear to function normally. The malware's control infrastructure is persistent and robust, relying on a continuous C2 channel to send stolen data, receive updates, and execute new payloads. Its C2 servers often use customized ports and fake browser headers, to evade detection. For attackers, the built-in dashboards provide searchable access to stolen data, making Katz not just a threat but a thriving data-harvesting service.

Recommendations

- **Be cautious:** Avoid downloading software or opening attachments from unknown sources especially cracked software or suspicious email links. These are often used as bait to spread malware like Katz Stealer.
- **Think before you paste or run code:** Never paste or run code from your clipboard or a random website unless you're 100% sure it's safe. Some malware tricks users into copying and executing harmful commands disguised as harmless steps.
- **Secure your web browsers and extensions:** Clear saved passwords from your browser and use a trusted password manager instead. Also, review your browser extensions remove anything you don't recognize or use, especially those related to crypto wallets.
- **Protect your cryptocurrency wallets:** Store crypto wallets in secure, offline locations when not in use. Avoid keeping wallet seed phrases or private keys unencrypted on your device they're prime targets for Katz Stealer.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1059.001 PowerShell	T1027 Obfuscated Files or Information

T1574 Hijack Execution Flow	**T1574.001** DLL	**T1547** Boot or Logon Autostart Execution	**T1095** Non-Application Layer Protocol
T1071 Application Layer Protocol	**T1102** Web Service	**T1176** Software Extensions	**T1176.001** Browser Extensions
T1140 Deobfuscate/Decode Files or Information	**T1055** Process Injection	**T1055.012** Process Hollowing	**T1555** Credentials from Password Stores
T1539 Steal Web Session Cookie	**T1115** Clipboard Data	**T1113** Screen Capture	**T1548** Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	**T1053** Scheduled Task/Job	**T1134** Access Token Manipulation	**T1497.001** System Checks
T1614 System Location Discovery	**T1082** System Information Discovery	**T1068** Exploitation for Privilege Escalation	**T1190** Exploit Public-Facing Application
T1074 Data Staged	**T1070** Indicator Removal	**T1041** Exfiltration Over C2 Channel	**T1106** Native API

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185[.]107[.]74[.]40, 31[.]177[.]109[.]39
Domain	twist2katz[.]com, pub-ce02802067934e0eb072f69bf6427bf6[.]r2[.]dev, katz-stealer[.]com, katzstealer[.]com
SHA256	22af84327cb8ecafa44b51e9499238ca2798cec38c2076b702c60c72505329cb, e4249cf9557799e8123e0b21b6a4be5ab8b67d56dc5bfad34a1d4e76f7fd2b19, fb2b9163e8edf104b603030cff2dc62fe23d8f158dd90ea483642fce2ceda027,

TYPE	VALUE
SHA256	0df13fd42fb4a4374981474ea87895a3830eddcc7f3bd494e76acd604c4004f7, 4f12c5dca2099492d0c0cd22edef841cbe8360af9be2d8e9b57c2f83d401c1a7, 6dc8e99da68b703e86fa90a8794add87614f254f804a8d5d65927e0676107a9d, e73f6e1f6c28469e14a88a633aef1bc502d2dbb1d4d2dfcaaef7409b8ce6dc99, 2798bf4fd8e2bc591f656fa107bd871451574d543882ddec3020417964d2faa9, e345d793477abbecc2c455c8c76a925c0dfe99ec4c65b7c353e8a8c8b14da2b6, 15953e0191edaa246045dda0d7489b3832f27fdc3fcc5027f26b89692aefd6e1, c601721933d11254ae329b05882337db1069f81e4d04cd4550c4b4b4fe35f9cd, fdc86a5b3d7df37a72c3272836f743747c47bfbc538f05af9ecf78547fa2e789, 25b1ec4d62c67bd51b43de181e0f7d1bda389345b8c290e35f93ccb444a2cf7a, 964ec70fc2fdf23f928f78c8af63ce50aff058b05787e43c034e04ea6cbe30ef, d92bb6e47cb0a0bdbb51403528ccfe643a9329476af53b5a729f04a4d2139647, b249814a74dff9316dc29b670e1d8ed80eb941b507e206ca0dfdc4ff033b1c1f, 925e6375deaa38d978e00a73f9353a9d0df81f023ab85cf9a1dc046e403830a8, 96ada593d54949707437fa39628960b1c5d142a5b1cb371339acc8f86dbc7678, b912f06cf65233b9767953ccf4e60a1a7c262ae54506b311c65f411db6f70128, 2852770f459c0c6a0ecfc450b29201bd348a55fb3a7a5ecdcc9986127fdb786b, 5dd629b610aee4ed7777e81fc5135d20f59e43b5d9cc55cdad291fcf4b9d20eb
File Names	\AppData\Local\Temp\katz_ontop.dll, \AppData\Local\Temp\received_dll.dll, \AppData\Roaming\decrypted_chrome_key.txt, \AppData\Roaming\decrypted_brave_key.txt, \AppData\Roaming\decrypted_edge_key.txt

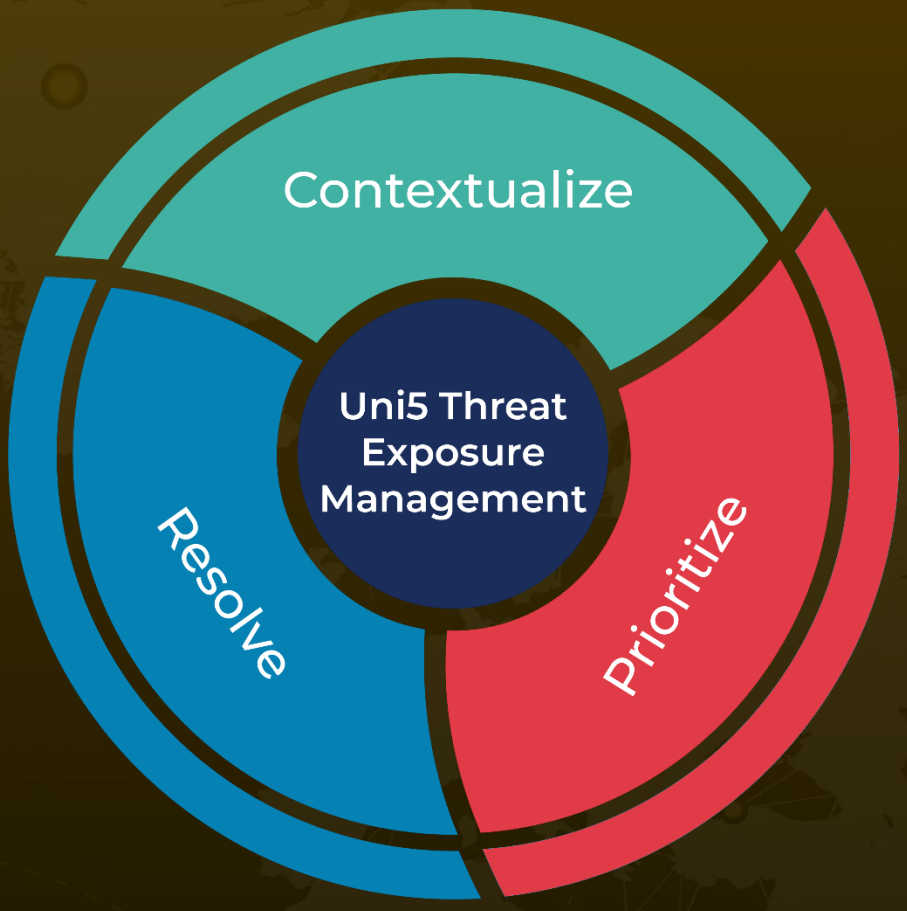
References

https://www.nextron-systems.com/2025/05/23/katz-stealer-threat-analysis/

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

June 17, 2025 • 5:50 AM

More at www.hivepro.com