Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

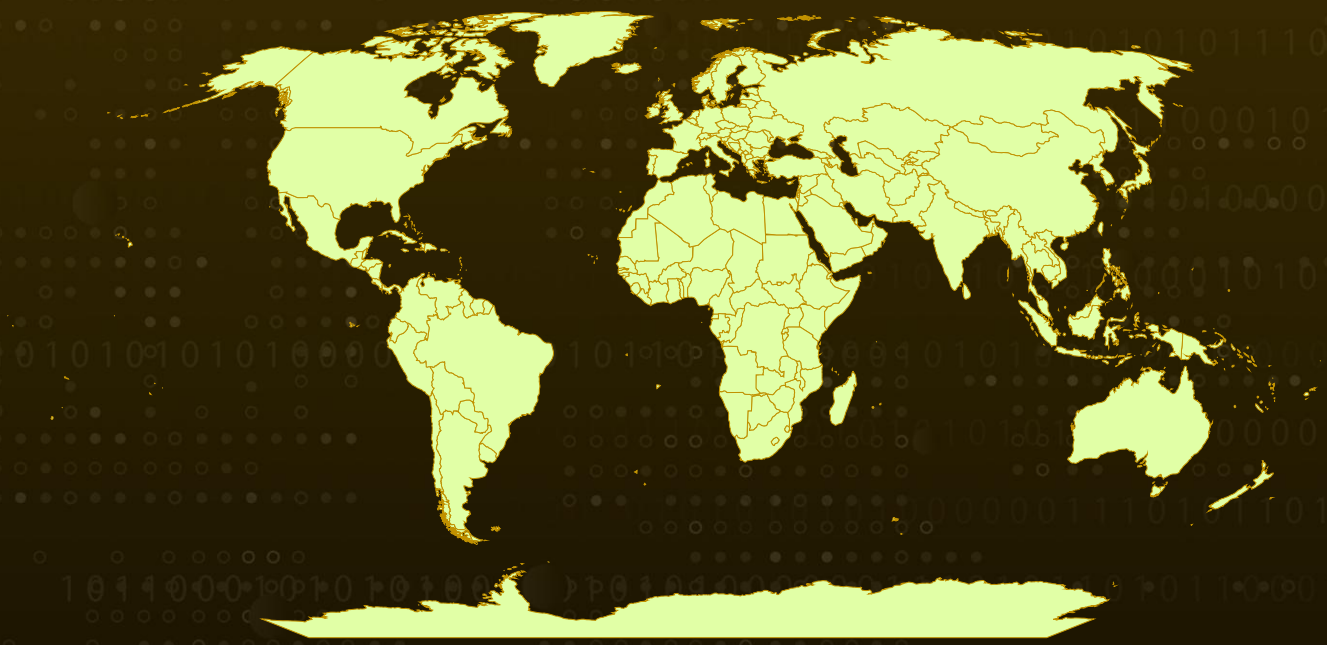
PupkinStealer: The Silent Thief Hiding in Plain Sight

Date of Publication	Admiralty Code	TA Number
May 13, 2025	A1	TA2025146

Summary

First Seen: April 2025
Malware: PupkinStealer
Affected Products: Chromium-based browsers
Affected Platform: Windows
Targeted Countries: Worldwide
Attack: PupkinStealer is a lightweight but dangerous malware that quietly steals browser passwords, Telegram and Discord session data, desktop files, and screenshots. Once executed, it zips up the stolen info and exfiltrates it via a Telegram bot, making it a stealthy threat aimed at quick data theft and account hijacking.

Attack Regions



Attack Details

#1 PupkinStealer, first discovered in April 2025, is written in C# using the .NET framework and is designed to quietly steal sensitive information from Windows computers. While not particularly complex, it is effective at what it does, stealing browser passwords, desktop files, data from messaging apps like Telegram and Discord, and even capturing screenshots of the victim's screen. Once the information is collected, it is compressed into a ZIP file and exfiltrated via a Telegram bot named botKanal.

#2 This malware is believed to be created by a developer who goes by the name Ardent. It's part of a growing trend of lightweight and customizable "info stealers" that are widely shared or sold in underground communities. These tools are attractive to low-skilled attackers because they're easy to use and don't require much technical know-how to deploy.

#3 Once PupkinStealer infects a system, it launches several tasks. One of its first actions is to steal saved passwords from popular browsers like Chrome, Edge, Opera, and Vivaldi. It decrypts these credentials using Windows' own built-in tools and stores the data in text files. It also searches the user's desktop for specific types of files, like documents or images and copies them into a folder for exfiltration.

#4 Another task involves stealing Telegram session data. This allows attackers to access the user's Telegram account without needing a password. If the Telegram process is running, the malware quietly shuts it down so it can copy session files without any issues. Similarly, it targets Discord by scanning for login tokens saved on the system. With these tokens, attackers can hijack Discord accounts and impersonate the victim.

#5 To gather even more information, PupkinStealer takes a screenshot of the user's desktop and saves it. After collecting everything, passwords, desktop files, Telegram sessions, Discord tokens, and the screenshot, it bundles it all into a compressed ZIP file. The ZIP also contains identifying details like the victim's username, IP address, and Windows Security Identifier (SID), helping the attacker track their victims. Finally, the malware sends this data to its operator through the Telegram Bot API.

#6 PupkinStealer might seem simple on the surface, but it poses a serious threat. Its quiet behavior, combined with the ability to steal valuable personal data, makes it effective and dangerous. To protect against such threats, users should be careful when downloading unknown files or clicking suspicious links.

Recommendations

Strengthen Email Security: To strengthen email security, use advanced filtering to block spear-phishing, sandbox attachments for safe analysis, and enable DMARC, DKIM, and SPF to prevent spoofed emails. These measures help protect against malicious threats.

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.

Protect Your Devices with Security Software and Updates: Make sure you're using a trusted antivirus or endpoint protection tool, and keep it updated. These tools help catch threats like PupkinStealer before they can do harm. Also, don't ignore software updates. Keeping your operating system, web browsers, and everyday apps up to date ensures known security holes are patched, making it much harder for attackers to get in.

Tighten App Permissions and Secure Messaging Accounts: Review what access your apps really need, especially lesser-used or third-party ones. Limiting their access to your files and network helps reduce the chances of malware slipping through. Also, protect your Telegram and Discord accounts by enabling two-factor authentication (2FA), keeping an eye out for unusual login activity, and never reusing the same password across different services.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	T1059 Command and Scripting Interpreter
T1204 User Execution	T1204.002 Malicious File	T1027 Obfuscated Files or Information	T1027.015 Compression
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers

T1528 Steal Application Access Token	**T1082** System Information Discovery	**T1005** Data from Local System	**T1113** Screen Capture
T1074 Data Staged	**T1074.001** Local Data Staging	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage	**T1560** Archive Collected Data		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	fc99a7ef8d7a2028ce73bf42d3a95bce
SHA256	9309003c245f94ba4ee52098dadbaa0d0a4d83b423d76c1bfc082a1c29e0b95f
URL	hxxps[:]//api[.]telegram[.]org/bot[BotToken]/sendDocument?chat_id=7613862165&caption
File Path	%APPDATA%\Temp\[Username]\Grabbers\Browser\passwords.txt, %APPDATA%\Temp\[Username]\Grabbers\TelegramSession*, %APPDATA%\Temp\[Username]\Grabbers\Discord\Tokens.txt, %APPDATA%\Temp\[Username]\Grabbers\Screenshot\Screen.jpg, %APPDATA%\Temp\[Username]\DesktopFiles*, %APPDATA%\Temp\[Username]\[Username]@ardent.zip

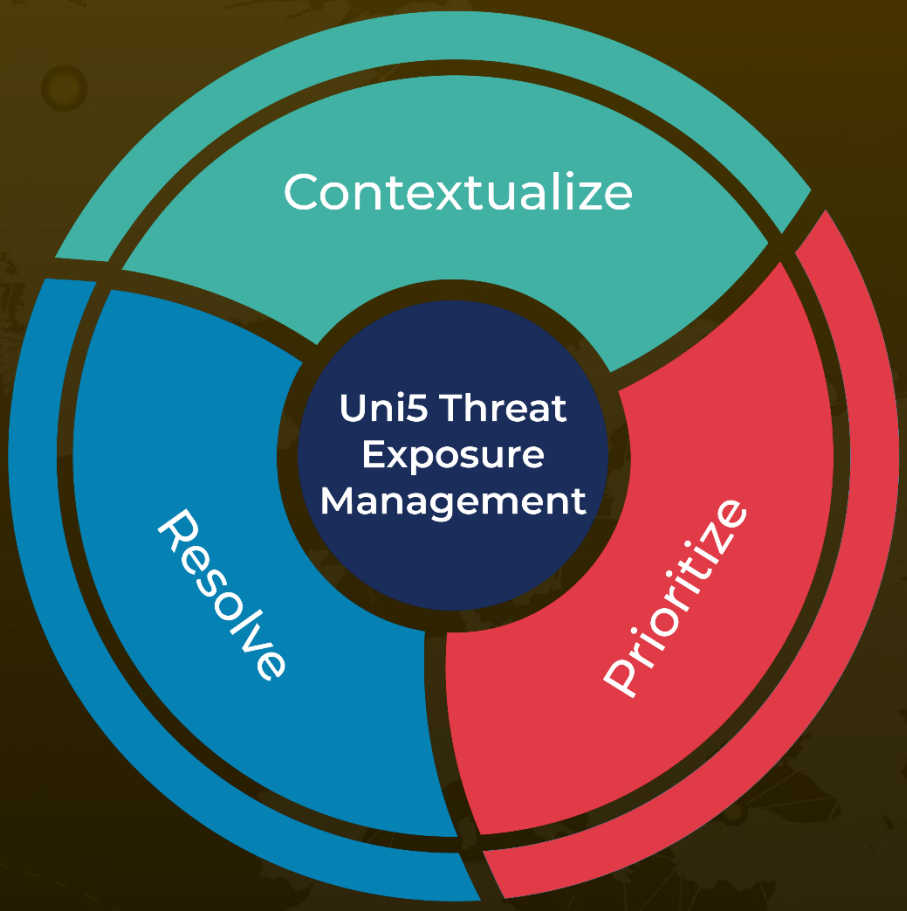
References

https://www.cyfirma.com/research/pupkinstealer-a-net-based-info-stealer/

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

May 13, 2025 • 4:50 AM

More at www.hivepro.com