Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

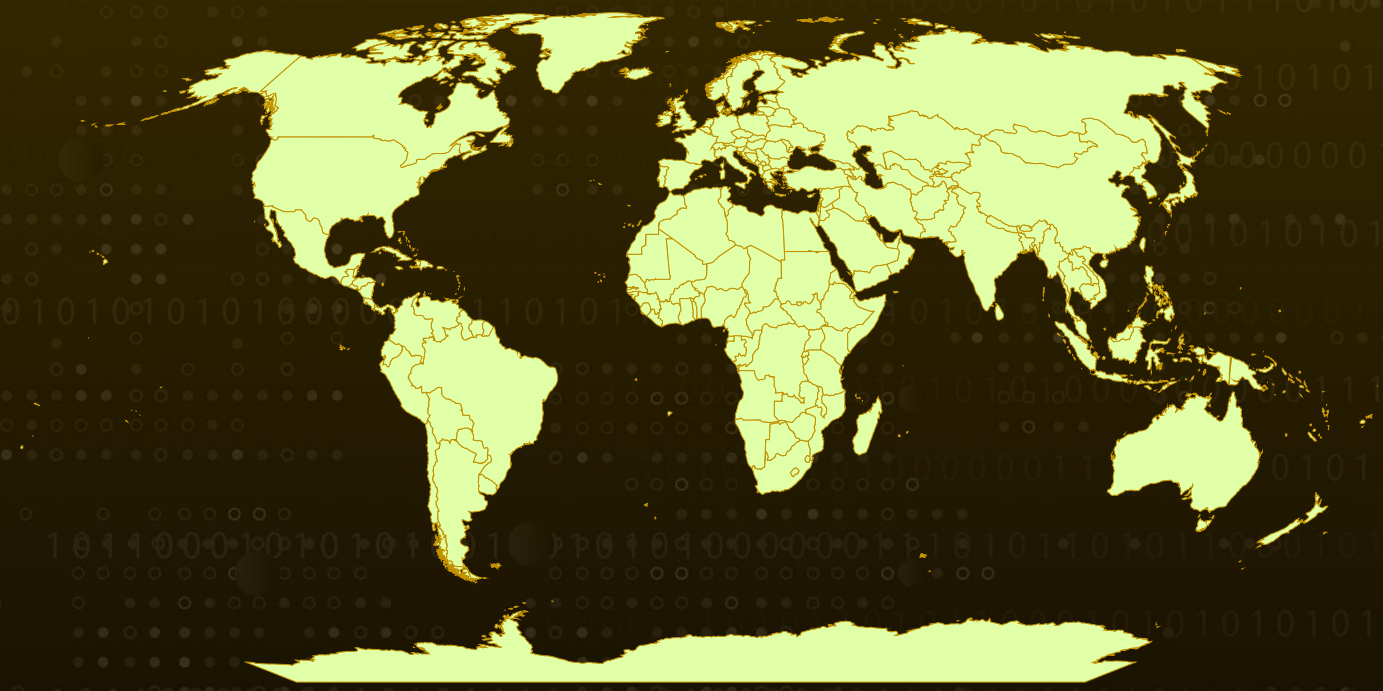
DarkCloud Uses Fileless Techniques Turning into a Nightmare for Windows

Date of Publication	Admiralty Code	TA Number
August 11, 2025	A1	TA2025246

Summary

Attack Commenced: April 2025
Malware: DarkCloud Stealer
Targeted Region: Worldwide
Affected Platform: Microsoft Windows
Affected Browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, Brave Browser
Attack: DarkCloud, a Windows-based information stealer first detected in 2022, resurfaced in 2025 with new delivery and obfuscation tactics, including ConfuserEx-protected files and a VB6 payload. Spread mainly via phishing emails with malicious RAR attachments, it uses JavaScript and PowerShell to deploy a fileless .NET DLL, gain persistence, and inject its payload into MSBuild.exe, stealing browser credentials and payment data for exfiltration via FTP or SMTP.

Attack Regions



Attack Details

#1 DarkCloud is a stealthy, Windows-based information-stealing malware first identified in 2022. It is designed to harvest sensitive data, including stored login credentials, financial information, and contact details. In April 2025, notable changes were observed in DarkCloud's distribution methods and obfuscation techniques.

#2 These updates introduced an additional infection chain, incorporating obfuscation through ConfuserEx, an open-source protector for .NET applications, and delivering a final payload developed in Microsoft Visual Basic 6 (VB6). Files processed with ConfuserEx typically contain identifiable watermarks.

#3 By early July 2025, a new DarkCloud variant emerged, spread through phishing emails containing malicious RAR archives. When opened in WinRAR, the archive reveals a standalone JavaScript file. Once executed, this script decodes and runs PowerShell commands, which in turn load an encrypted, fileless .NET DLL disguised as a legitimate Task Scheduler module.

#4 The DLL establishes persistence, retrieves and decrypts a remote payload, and leverages process hollowing to inject the final DarkCloud VB6-based payload into MSBuild.exe. This payload extracts saved credentials and payment data from popular web browsers. Exfiltration of the stolen information is conducted via both FTP and SMTP protocols, ensuring data reaches the attacker's infrastructure.

Recommendations

Enhance Email Security: Deploy advanced filtering and sandboxing to detect phishing, especially emails with attachments. Keep detection rules updated to reflect emerging threats.

Adopt Zero Trust Security Models: Apply a Zero Trust approach to user access and network segmentation, ensuring that even if credentials are compromised, lateral movement is limited. Use multifactor authentication and restrict access to sensitive design, IP, and financial systems.

Harden Browser Security: Limit the storage of credentials and payment details in browsers. Encourage use of secure password managers instead of browser-based storage.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1204** User Execution
T1566 Phishing	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript	**T1059.001** PowerShell
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1055** Process Injection	**T1055.012** Process Hollowing
T1071 Application Layer Protocol	**T1574.001** DLL	**T1071.002** File Transfer Protocols	**T1071.003** Mail Protocols
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1119** Automated Collection	**T1048** Exfiltration Over Alternative Protocol
T1114 Email Collection	**T1027.011** Fileless Storage	**T1566.001** Spearphishing Attachment	**T1112** Modify Registry
T1543 Create or Modify System Process	**T1212** Exploitation for Credential Access	**T1217** Browser Information Discovery	**T1083** File and Directory Discovery
T1057 Process Discovery	**T1082** System Information Discovery	**T1497** Virtualization/Sandbox Evasion	**T1140** Deobfuscate/Decode Files or Information
T1053 Scheduled Task/Job			

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	Quote #S_260627.RAR, Quote #S_260627.js, WScript.exe, ThunderBirdContacts.txt, 163MailContacts.txt, EMClient10Contacts.txt, OutlookContacts.txt
File Path	C:\Users\Public\Downloads\edriophthalma.js
URL	hxxp[:]//paste[.]ee/d/0WhDakVP/0, hxxps[:]//archive[.]org/download/universe-1733359315202-8750/universe-1733359315202-8750[.]jpg, hxxp[:]//176[.]65[.]142[.]190, hxxps[:]//api[.]telegram[.]org/bot7684022823[:]AAFw0jHSu-b4qs6N7yC88nUOR8ovPrCdIrs/sendMessage?chat_id=6542615755
SHA256	381aa445e173341f39e464e4f79b89c9ed058631bcbbb2792d9ecbdf9ffe027d, 82ba4340be2e07bb74347ade0b7b43f12cf8503a8fa535f154d2e228efbef69c, bd8c0b0503741c17d75ce560a10eeeaa0cdd21dff323d9f1644c62b7b8eb43d9, 9588c9a754574246d179c9fb05fea9dc5762c855a3a2a4823b402217f82a71c1, 6b8a4c3d4a4a0a3aea50037744c5fec26a38d3fb6a596d006457f1c51bbc75c7, F6d9198bd707c49454b83687af926ccb8d13c7e43514f59eac1507467e8fb140, 72d3de12a0aa8ce87a64a70807f0769c332816f27dcf8286b91e6819e2197aa8, fa598e761201582d41a73d174eb5edad10f709238d99e0bf698da1601c71d1ca, 2bd43f839d5f77f22f619395461c1eeaee9234009b475231212b88bd510d00b7, 24552408d849799b2cac983d499b1f32c88c10f88319339d0eec00fb01bb19b4, ce3a3e46ca65d779d687c7e58fb4a2eb784e5b1b4cebe33dbb2bf37cccb6f194

References

https://www.fortinet.com/blog/threat-research/unveiling-a-new-variant-of-the-darkcloud-campaign

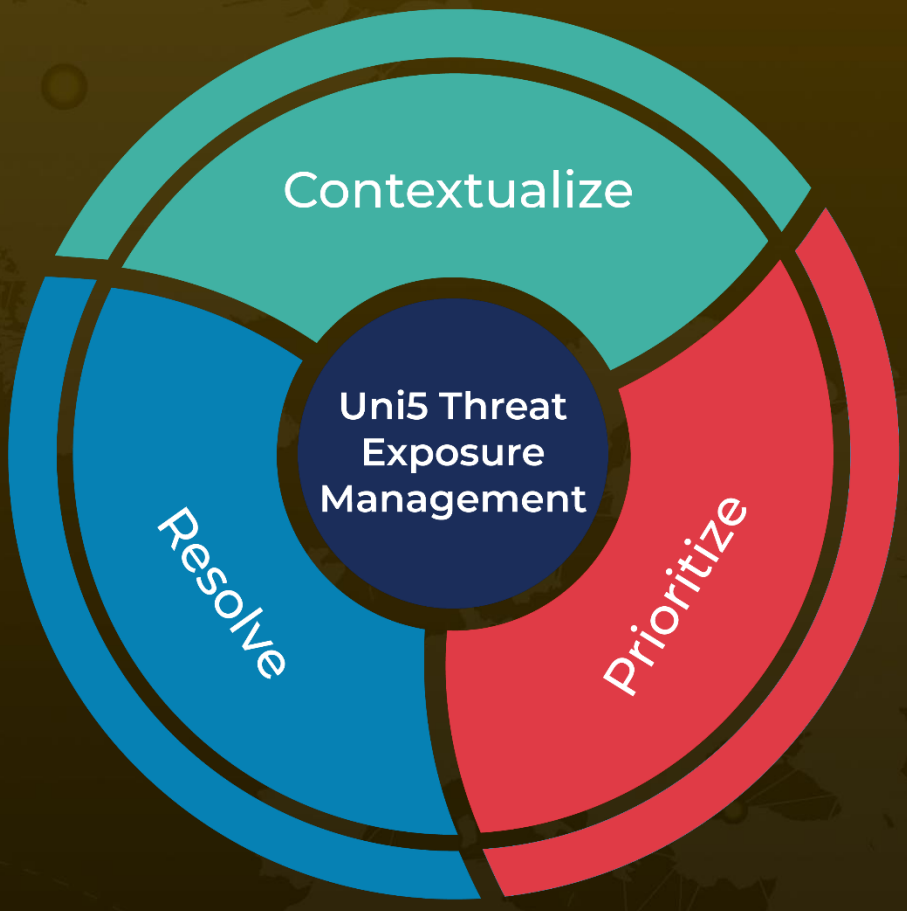
https://unit42.paloaltonetworks.com/new-darkcloud-stealer-infection-chain/

https://hivepro.com/threat-advisory/darkcloud-stealer-a-multi-stage-malware-that-pilfers-sensitive-data/

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 11, 2025 • 6:30 AM

More at www.hivepro.com