Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

DeerStealer the $200 Doorway to Your Digital Secrets

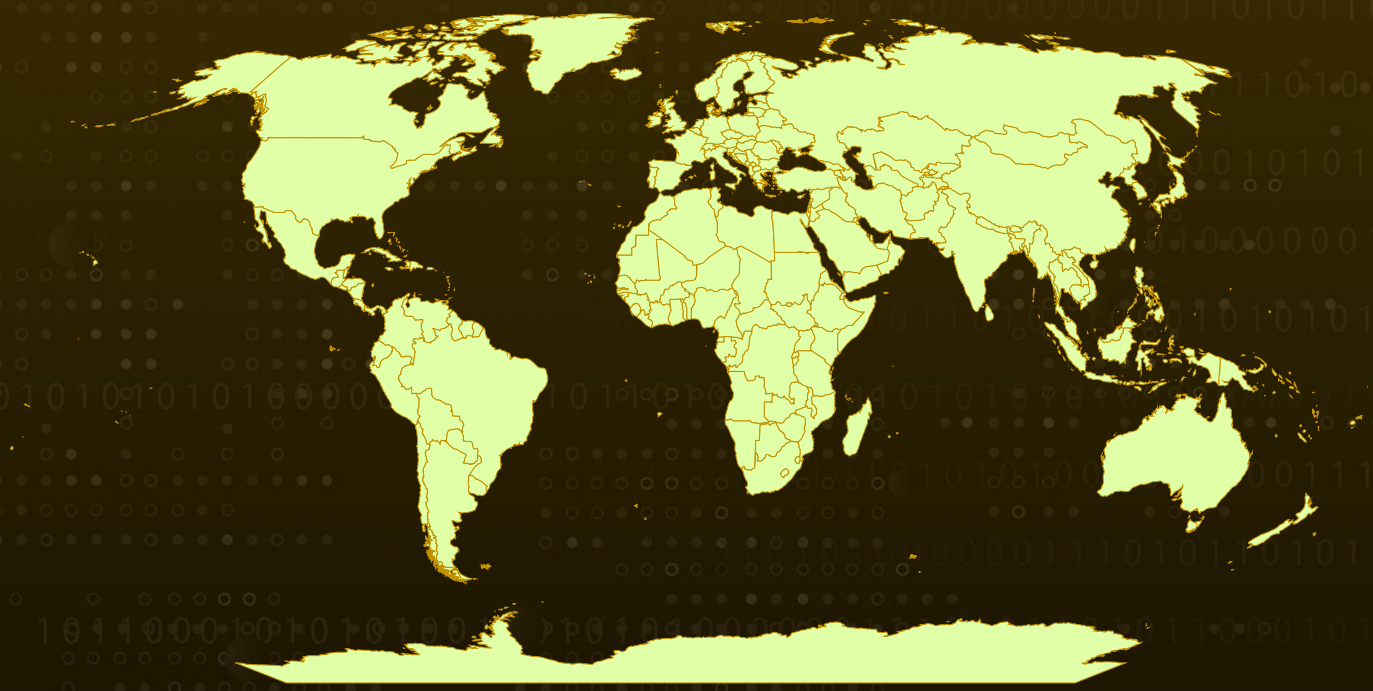
Date of Publication	Admiralty Code	TA Number
September 25, 2025	A1	TA2025295

Summary

Attack Commenced: May 2025
Malware: DeerStealer
DeerStealer Pricing Model: $200 - $3000
Targeted Regions: Worldwide

Attack: DeerStealer is a sophisticated information-stealing malware actively sold on dark-web forums and Telegram by the user LuciferXfiles. It disguises itself as legitimate software, such as fake document readers, to trick victims into execution while secretly harvesting passwords, financial data, cryptocurrency wallets, and browser information. With strong obfuscation and persistence techniques, DeerStealer poses a growing cybersecurity threat that continues to evolve across global attack campaigns.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 DeerStealer is malware designed to steal confidential information from compromised systems. It is actively marketed on dark-web forums by a user known as 'LuciferXfiles' and is also advertised through various Telegram channels. The malware is sold via a tiered subscription model, with pricing starting at $200 per month for the 'Premium' plan; $450 per month for 'Thief'; $1,500 per month for 'Thief+'; and $3,000 per month for the 'Professional' package.

#2 The creator markets the full package, which includes the malware loader, under the name 'XFiles Spyware.' DeerStealer operates covertly, often posing as legitimate software to trick users into executing it. Once active, it establishes persistence on compromised systems and exfiltrates sensitive information such as financial data, passwords, and cryptocurrency wallet details to remote servers.

#3 Its capabilities also extend to harvesting browser cookies, instant messaging content, and VPN information. In earlier campaigns, it was distributed as a fake Google Authenticator app, with the malicious binary hosted on GitHub. Developed in the Delphi programming language, recent variants are disguised as fake document reader updates.

#4 DeerStealer often masquerades as software like Adobe Acrobat Reader, enabling it to blend in and evade detection. It is typically delivered in ZIP archives containing executable (PE) files and supporting payloads. The malware uses data obfuscation, signed binaries, and rootkit-like techniques, making it difficult to detect and remove.

#5 Its ability to switch between command-and-control (C2) servers further strengthens its persistence and adaptability. To maintain access, DeerStealer creates scheduled tasks that ensure automatic execution after system reboots. In May 2025, threat actors attempted multiple DeerStealer deployments, often delivered as the final payload through **HijackLoader**. These attack chains commonly leveraged the ClickFix access method, redirecting victims to phishing pages that instructed them to execute malicious commands in the Windows Run Prompt.

Recommendations

Implement Advanced Endpoint Protection: Deploy next-generation antivirus and endpoint detection solutions capable of detecting obfuscated binaries, rootkit-like behaviors, and malicious PE files to prevent malware execution.

Protect Sensitive Data and Credentials: Implement multi-factor authentication, secure password storage, and regular audits of financial, VPN, and crypto wallet credentials to reduce the impact if DeerStealer gains access.

Implement Network Segmentation and Zero Trust Architecture: Segment networks to limit ransomware spread across interconnected systems. Apply zero trust principles, verify identity and device posture before granting access, regardless of location. Use micro-segmentation tools to define fine-grained access rules.

Regularly Review and Harden File System Permissions: Audit permissions for sensitive directories and ensure that only essential processes and users have write access. Disable file sharing where not required and use access control lists (ACLs) to limit exposure.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1566 Phishing	T1189 Drive-by Compromise	T1204 User Execution
T1059 Command and Scripting Interpreter	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1036 Masquerading

T1622 Debugger Evasion	**T1027** Obfuscated Files or Information	**T1014** Rootkit	**T1027.013** Encrypted/Encoded File
T1497 Virtualization/Sandbox Evasion	**T1082** System Information Discovery	**T1087** Account Discovery	**T1087.001** Local Account
T1217 Browser Bookmark Discovery	**T1673** Virtual Machine Discovery	**T1574.001** DLL	**T1041** Exfiltration Over C2 Channel
T1001 Data Obfuscation	**T1056** Input Capture	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a03cec07324b0c3227e4f060b0fefc24d35482dfe690bc86df1a53211629837e, b7ee370878fb4290097311e652222d8bab91c44a94063ea192100d4fd9dadb14, 49ad6431fb67c29e1a2745092232898c491652ddf7115e0332382b42466d0734, ce62130f0392b40ab047392b47d523f66a55260c9fc2ec3d3727fab13fc87933, d4b3a879fb6907c39a3b843ec5272a005e8fec25d8012c4a9fe9d0ada9f71d1f, e189e7fe9cd6d63ecece8b8e8fafb773003db6009fb0c45dc2b21e77167938ba, 0feaaabe6d0a2e29b636cf1f5f9d1b3f727518507ffc93fc881d64feefa2ab81, 623ff1e6662986ab36336919fde5c48805b4a87b97af6f9abe09732e9ac45b8f, 1432faeddfe57877873e8608ace13739ca66e8ce12b3453531e7eec4753df21d, 6f1bfbb8ba6d4eb4e7ce3ff16f1b8e95d601a5eccdd0d743141ac7c3841b11f3,

TYPE	VALUE
SHA256	263484f65c76fd3be147ad124a1feaa5240a1d0ce1695855f08f6c6968d1a30d, 5ec174af8a18a5516b8a6e11d8a27481d70df14d1edb67c48b5458ff44df9146, 24475ae7781189075f64a2de1a7d1fd69b341b7adee67f0bd2286cfbf1f0b7f9, eb17f8296482b0c096a2249844a62988b6abdd8ffe8cbbe3398f422968d46875, e34d753f2b992cf74c1b9db61bad4d6c6089ab8ef9fb942c865290b2dd64b4ad, 9163f9237ad869a74715f9b126f7c577bd1f12afb8eae37ba07c11f00a39fa3e, 4640d425d8d43a95e903d759183993a87bafcb9816850efe57ccfca4ace889ec, 569ac32f692253b8ab7f411fec83f31ed1f7be40ac5c4027f41a58073fef8d7d, 5e2839553458547a92fff7348862063b30510e805a550e02d94a89bd8fd0768d, 66282239297c60bad7eeae274e8a2916ce95afeb932d3be64bb615ea2be1e07a, a6f6175998e96fcecad5f9b3746db5ced144ae97c017ad98b2caa9d0be8a3cb5, b116c1e0f92dca485565d5f7f3b572d7f01724062320597733b9dbf6dd84dee1, b5ab21ddb7cb5bfbedee68296a3d98f687e9acd8ebcc4539f7fd234197de2227, cb08d8a7bca589704d20b421768ad01f7c38be0c3ea11b4b77777e6d0b5e5956, d9db8cdef549e4ad0e33754d589a4c299e7082c3a0b5efdee1a0218a0a1bf1ee, E24c311a64f57fd16ffc98f339d5d537c16851dc54d7bb3db8778c26ccb5f2d1
Domains	telluricaphelion[.]com, loadinnnhr[.]today, nacreousoculus[.]pro, upcdnnodes[.]cfd, sciecdn[.]cfd, cloused-flow[.]site, debianlist[.]cfd, soft-metal-software[.]cfd, quitarlosi[.]cfd, cdnnode-01[.]cfd, sonorous-horizon-cfd[.]cfd, servicesmesh[.]pro, ncloud-servers[.]shop, brokpolok[.]shop,

TYPE	VALUE
Domains	d-nodes[.]shop, uplink-mirrors[.]shop, gg2024[.]info, authentificator-gogle[.]com, authetificator-gogle[.]com, authentificcatorgoolgle[.]com, authenticattor-googl[.]com, paradiso4[.]fun, authenticcator-descktop[.]com, updater-pro[.]com, gg2024[.]com, authentificator-googl[.]com, authenficatorgoogle[.]com, bflow-musico[.]fun, authentificatorgogle[.]com, authentificatorgoogle[.]com, chromstore-authentificator[.]com, authentifficatorgogle[.]com, authenticator-googl[.]com
File Path	C:\Users\[user-name]\AppData\Roaming\DebugdebugIRG_debug\ZZDCDNTCCJTZXIUKRCZH, C:\Users\[user-name]\AppData\Roaming\Outspan, C:\ProgramData\DebugdebugIRG_debug, C:\Users\[user-name]\AppData\Roaming\ValidArchive4, C:\Users\[user-name]\AppData\Roaming\DebugdebugIRG_debug
Filename	Reader_pl_install.zip
IPv4	104[.]21[.]112[.]1, 103[.]246[.]144[.]118, 172[.]67[.]195[.]171

References

https://www.cyfirma.com/research/deerstealer-malware-campaign-stealth-persistence-and-rootkit-like-capabilities/

https://www.esentire.com/blog/dont-get-caught-in-the-headlights-deerstealer-analysis

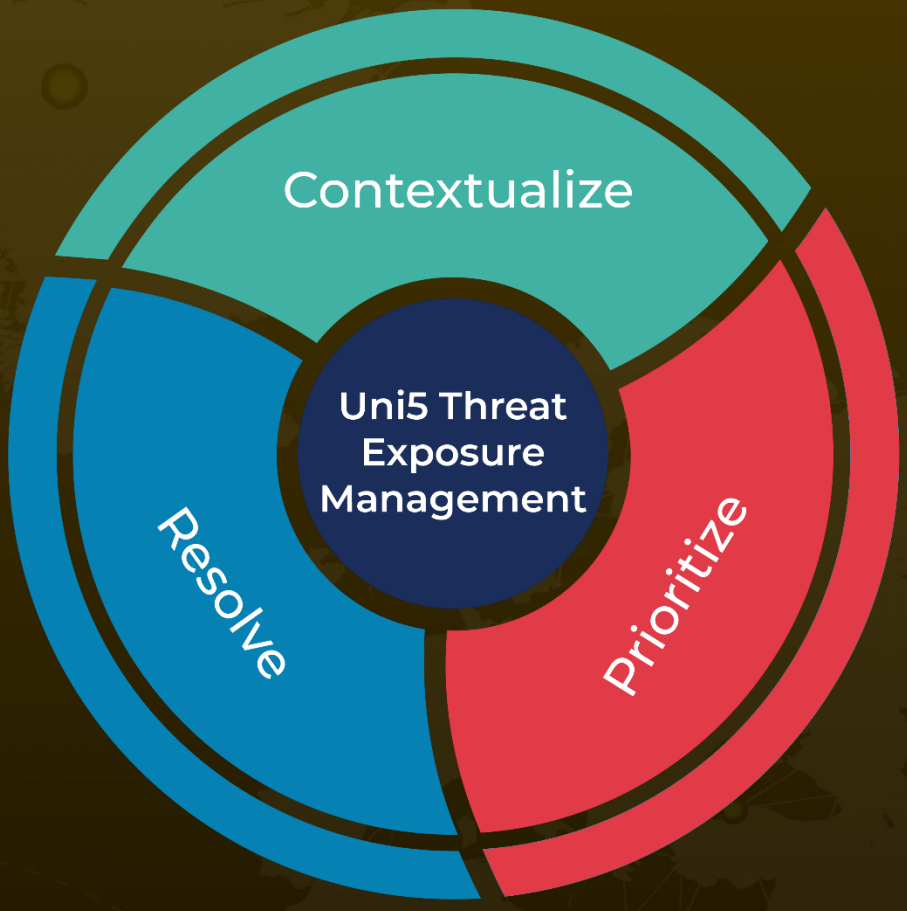
https://any.run/cybersecurity-blog/deerstealer-campaign-analysis/

https://hivepro.com/threat-advisory/hijackloader-a-deceptive-modular-malware-loader/

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

September 25, 2025 • 6:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com