DeerStealer Malware Campaign: Stealth, Persistence, and Rootkit-Like Capabilities

Published On : 2025-09-19

Executive Summary

At CYFIRMA, we are dedicated to providing current insights into prevalent threats and the strategies employed by malicious entities targeting both organizations and individuals. DeerStealer is a sophisticated malware designed to steal sensitive information from compromised systems. It is actively sold and supported through dark-web forums and Telegram channels. The malware uses deception and persistence mechanisms to evade detection, allowing it to run undisturbed for extended periods. DeerStealer targets a wide range of user and system data and communicates with remote servers to exfiltrate the harvested information. Its adaptive behavior and stealth features make it a significant threat in the current cybercrime landscape.

Introduction

This report provides a detailed analysis of the DeerStealer malware, examining its behavior, impact on infected systems, and the techniques it employs to evade detection. DeerStealer operates stealthily, often disguising itself as legitimate software to trick users into execution, and maintains persistence on compromised systems while collecting sensitive information for exfiltration to remote servers. The malware's design emphasizes adaptability, evasion, and long-term data theft, making it a persistent threat to both individuals and organizations. This analysis focuses on its infection process, persistence mechanisms, reconnaissance capabilities, and command-and-control infrastructure to support a deeper understanding of the threat and inform effective response strategies.

Key Findings

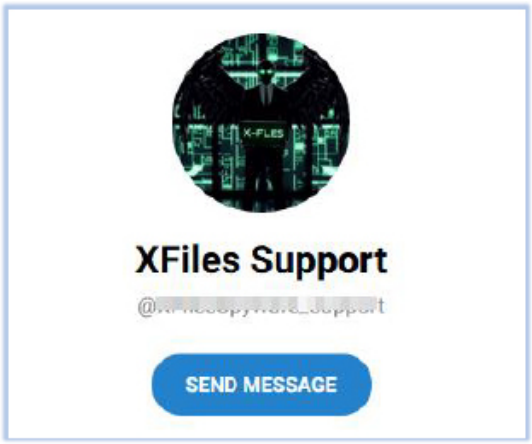
- DeerStealer is an information-stealing malware that targets a wide variety of data, including personal, sensitive information, and financial data.
- It employs signed executables and legitimate DLLs within the package to evade detection.
- It uses legitimate software as a decoy to deceive users and conceal malicious activity.
- Uses multi-stage execution, loads multiple payloads to perform persistence, data exfiltration, and core malicious functions.
- Establishes persistence through scheduled tasks to ensure automatic execution and survival across system reboots.
- Uses auto-elevated COM objects and rootkit-like techniques to execute and remain undetected.
- Maintains ongoing connections to C2 servers and can switch servers to evade detection.
- Sold and supported on dark-web forums and Telegram channels.

ETLM Attribution

This variant of DeerStealer is being distributed as the fake document reader update package. DeerStealer is an advanced piece of information-stealing malware, available for purchase through the dark web by the user @LuciferXfiles on hacking forums. While the creator refers to it as DeerStealer, the entire package—comprising the malware loader—is also sold under the name "XFiles Spyware."

Advertisement on the hacking forum

DeerStealer is also advertised, sold, and supported through various Telegram channels:



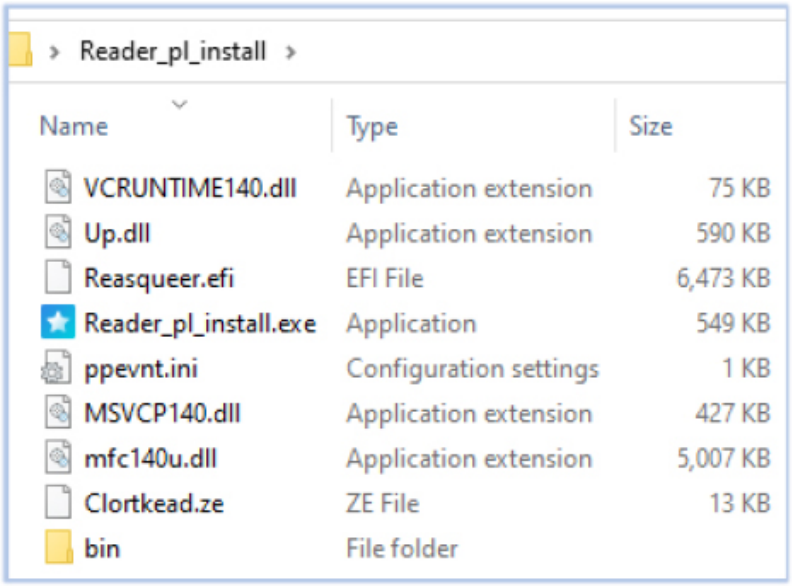
Threat Landscape:

DeerStealer malware operates within a dynamic threat landscape, constantly evolving to adapt to new detection methods and security measures. Its ability to hide in plain sight using deceptions such as masquerading as the legitimate software helps it avoid immediate detection. The use of data obfuscation and signed binaries, and its rootkit-like capabilities, makes it particularly difficult to track and neutralize. Its potential for switching between C2 servers remains a key feature of the malware's adaptive tactics. The malware can adapt its C2 infrastructure when needed to maintain persistence and evade detection. These characteristics make DeerStealer a highly resilient threat capable of sustained data exfiltration and command-and-control operations without triggering alarms.

Analysis of DeerStealer

File Details	
File Name	Reader_pl_install.zip
File Size	15.34 MB
Signed	Not signed
MD5	4bb605fe8c29a3b05ef7268ec047da56
SHA-256	a03cec07324b0c3227e4f060b0fefc24d35482dfe690bc86df1a53211629837e
Latest Contents Modification	02-09-2025

The malware is delivered as a ZIP archive containing PE files and additional files of unknown types:

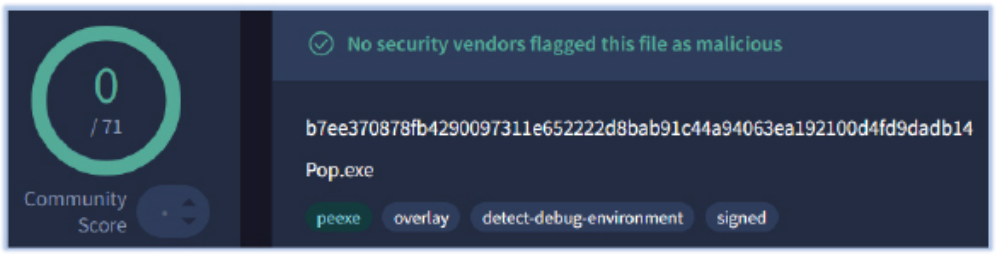


Content of zip archive

The primary payload, Reader_pl_install.exe, is a 32-bit GUI-based executable with the description “Pop-up notify” and the product name “AOMEI Partition Assistant.” It is signed with a valid digital certificate that appears to have been stolen from the issuing organization:

Information: Reader_pl_install.exe

As of the time of writing, this executable has no detections from security vendors:



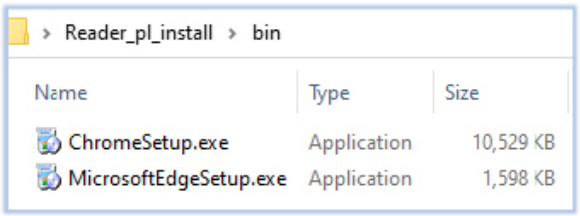
Another file, Up.dll, in the ZIP archive is signed with the same certificate as Reader_pl_install.exe, but its digital signature cannot be validated:

name	**AOMEI International Network Limited**
signature-info	The digital signature of the object did not verify.
issued-by	Sectigo Public Code Signing CA R36
signing-time	Sun Dec 29 19:30:43 2024
valid-from	Wed Nov 02 17:00:00 2022
valid-to	Sun Nov 02 16:59:59 2025
serial-number	00E04F3F5B78CA4D710F158ABFFE050F97

The use of the “Chinese (Simplified)” language in Reader_pl_install.exe and Up.dll is a potential indicator of Chinese origin:

dialog	.rsrc:0x00085700	168	F1DABC2066F4E552679AB6C821C9DD3...	chinese-simplified
bitmap	.rsrc:0x00085BC8	4130	BE10EA0874432E1BC82473DA1C2AE8A7...	chinese-simplified
dialog	.rsrc:0x000857A8	248	8CFD7A06BD1961BD09BDAD824223CED...	chinese-simplified
AFX_DIALOG_LAYOUT	.rsrc:0x00087C68	2	96A296D224F285C67BEE93C30F8A30915...	chinese-simplified
dialog	.rsrc:0x000858A0	344	F3BED09351AE10C8FA946E3D4F1BB5BD...	chinese-simplified
bitmap	.rsrc:0x00086BF0	436	6CC61A61E439A5DAFA0015657722687B...	chinese-simplified
bitmap	.rsrc:0x00086DA8	436	C2458C93C0D0DB7157C31CE3EFCACE0...	chinese-simplified
dialog	.rsrc:0x000859F8	460	9ED68E6C2ECFA4386303F96FDE5C52CB...	chinese-simplified
PNG	.rsrc:0x00086F60	1695	05DA8C810F18AF291DF1802224448FCD...	chinese-simplified
PNG	.rsrc:0x00087600	1359	F3EE8022AD23886849FE97118A3D48EF9...	chinese-simplified
PNG	.rsrc:0x00087B50	274	F78FA075F8C9D16021B63D4DED2B3BD2...	chinese-simplified
manifest	.rsrc:0x00087C70	381	4BB79DCEA0A901F7D9EAC5AA05728AE...	English-US

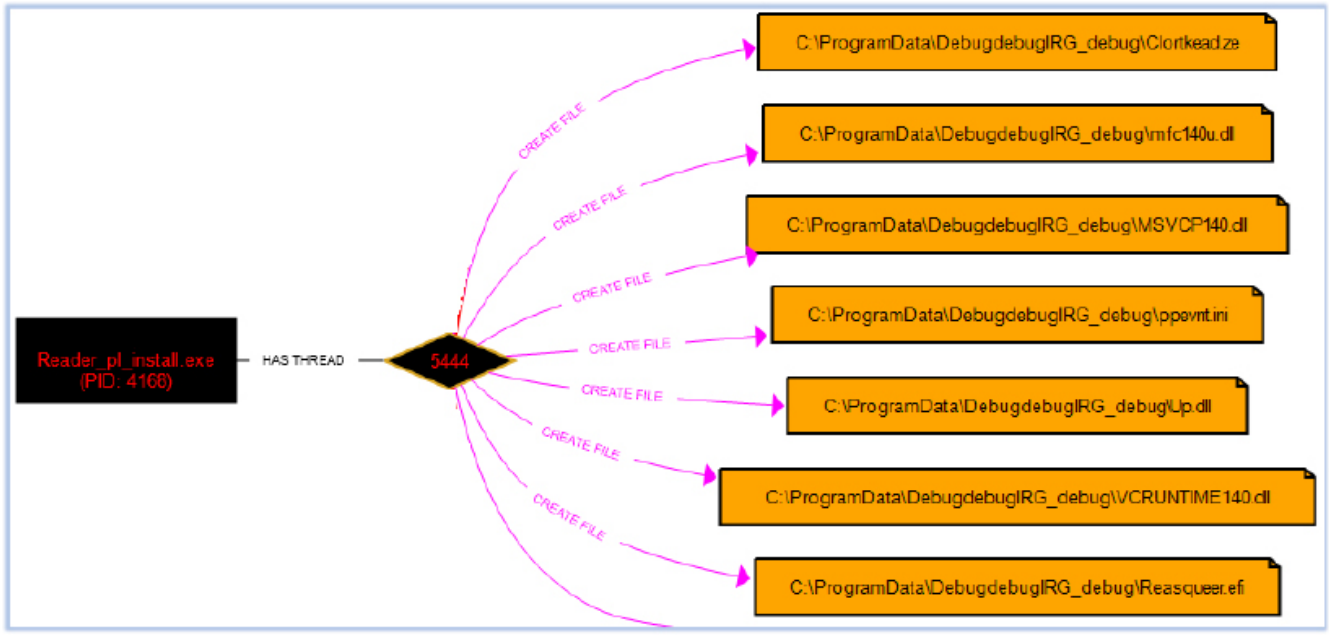
Other files in the ZIP archive, such as VCRUNTIME140.dll, MSVCP140.dll, and mfc140u.dll, are legitimate DLLs distributed by Microsoft. The files Reasqueer.efi and Clortkead.ze contain obfuscated content, while the bin folder contains a browser installation setup that is not inherently malicious.



Behavioral & Code Analysis

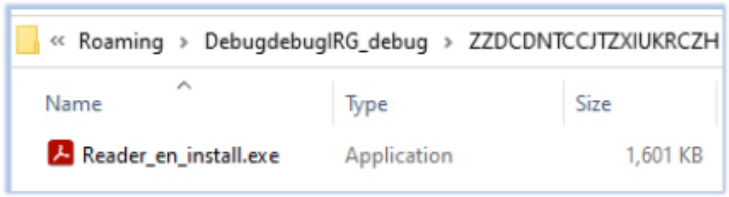
Stage 1:

When executed, Reader_pl_install.exe loads all the required DLLs, including those present in the ZIP archive. It then creates the directory C:\ProgramData\DebugdebugIRG_debug\ and copies files from the current working directory into this newly created folder.



File operations: Reader_pl_install.exe

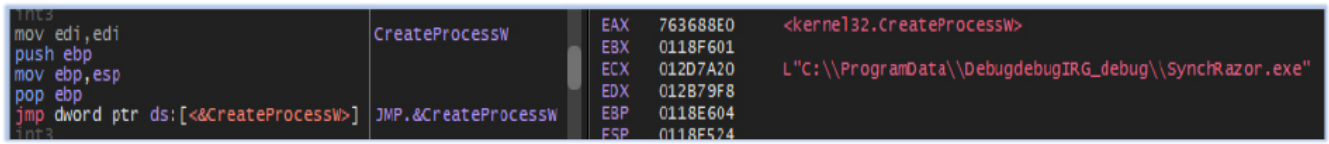
It also creates the directory C:\Users\AP\AppData\Roaming\DebugdebugIRG_debug\ and drops Reader_en_install.exe into the ZZDCDNTCCJTZXIUKRCZH folder within it. Reader_en_install.exe is the legitimate Adobe Acrobat Reader installer, a non-malicious executable signed with a valid Adobe certificate. It is used as a deception during a later stage of execution.



It also drops XPFix.exe in the DebugdebugIRG_debug directory. This is another executable signed with a valid digital signature:

Information: XPFix.exe

Reader_pl_install.exe also attempted to locate and execute a non-existent executable named SynchRazor.exe, but this attempt ultimately failed:

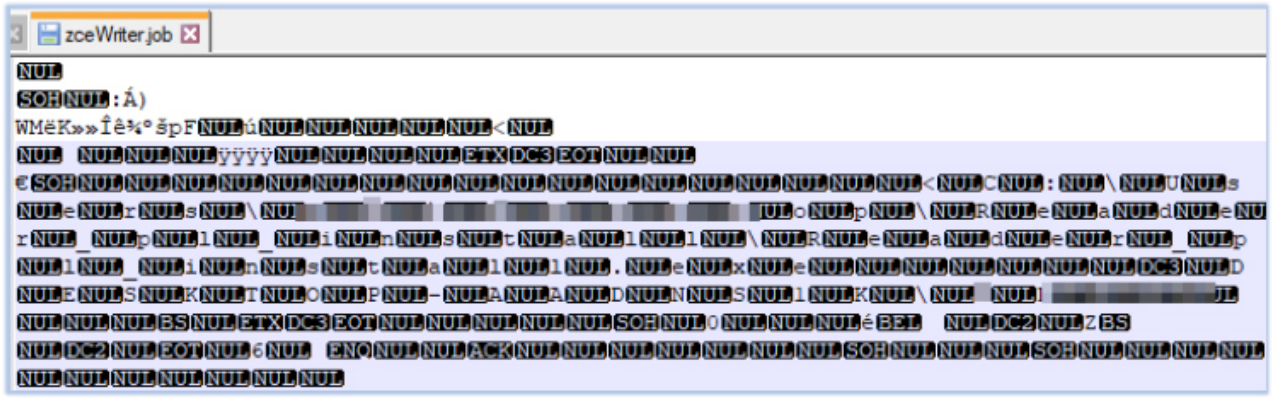


Execution attempt: non-existent executable

This instance of Reader_pl_install.exe terminates itself immediately after initiating the next stage.

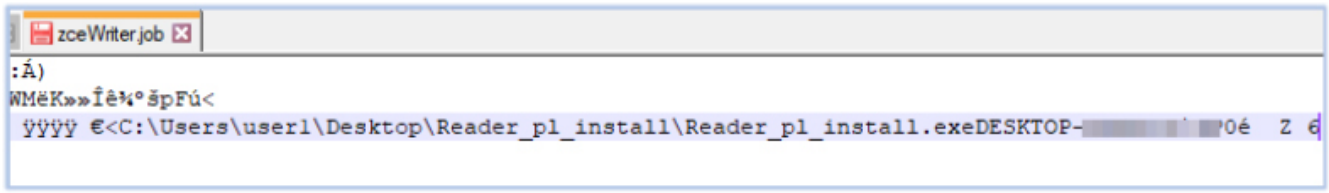
Stage 2: Deception

If Reader_pl_install.exe is executed without administrative privileges, it launches XPFix.exe. XPFix.exe reads the temporary file created at an earlier stage, then creates and writes to the zceWriter.job file in the C:\Windows\Tasks\ directory. The content of the zceWriter.job file is obfuscated:



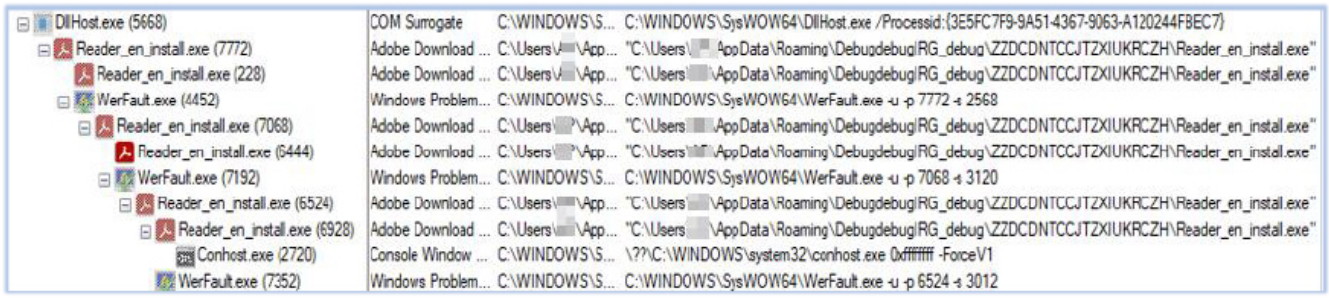
Obfuscated content: zceWriter.job

Files placed in this directory are often used to schedule tasks that run silently. Deobfuscation reveals that the process creates a scheduled task:



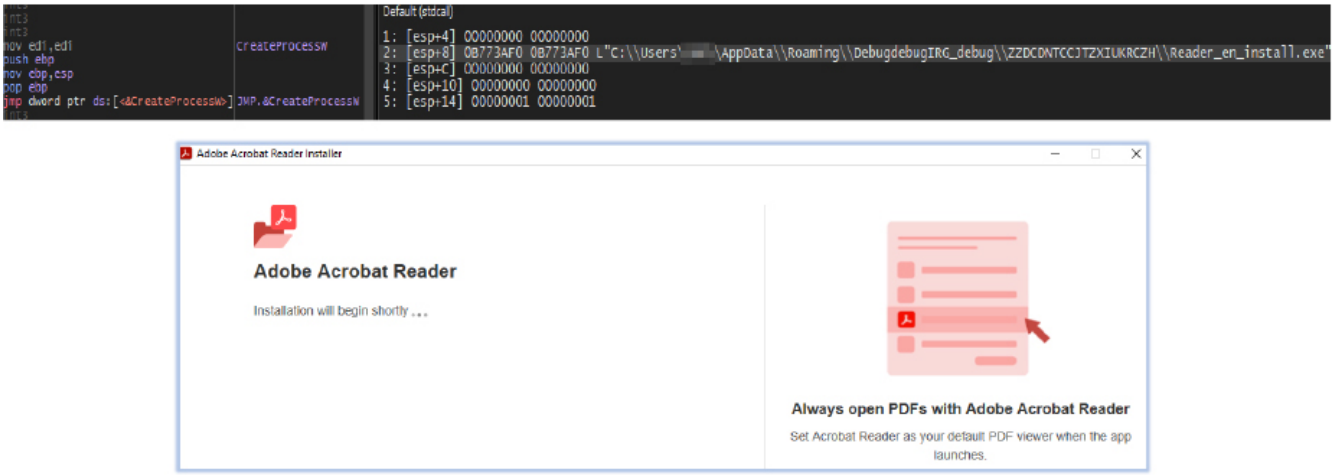
Deobfuscated content: zceWriter.job

Next, the malware leveraged a trusted, auto-elevated COM object (ICMLuaUtil) via DllHost.exe to execute Reader_en_install.exe without triggering a User Account Control (UAC) prompt. This is a known UAC bypass technique that abuses COM object elevation.



Process tree: Reader_en_install.exe

If Reader_pl_install.exe is executed with administrative privileges, it directly launches Reader_en_install.exe:

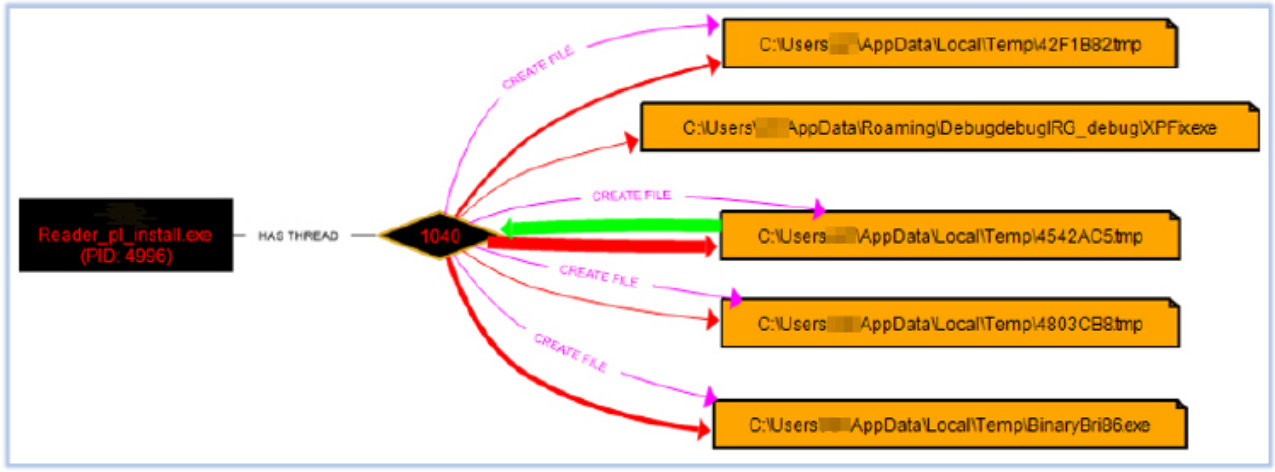


Execution: Reader_en_install.exe

This creates an effective deception, using the legitimate Adobe Acrobat Reader downloader to mask the malware's primary malicious activity.

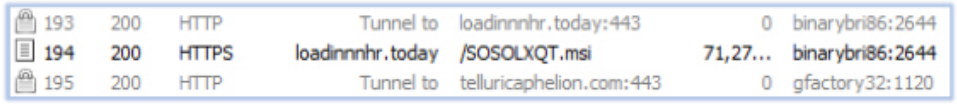
Stage 3:

In the next stage, another instance of Reader_pl_install.exe is executed via the scheduled task. It drops an additional executable, BinaryBri86.exe, into the Temp directory:

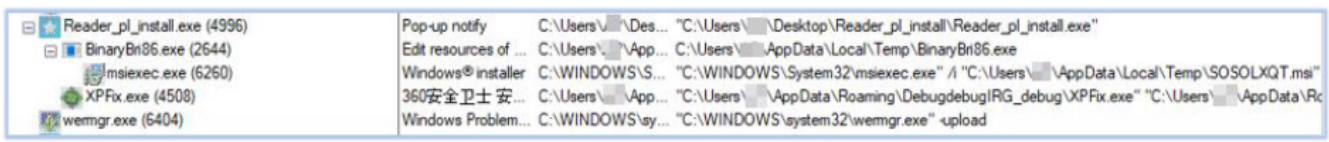


File operations: Reader_pl_install.exe (2nd instance)

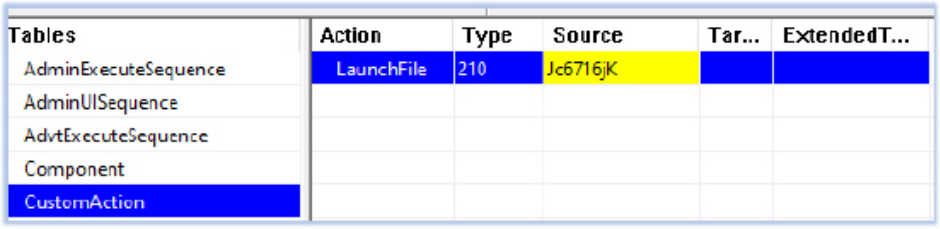
BinaryBri86.exe downloads SOSOLXQT.msi package from loadinnnhr[.]today:



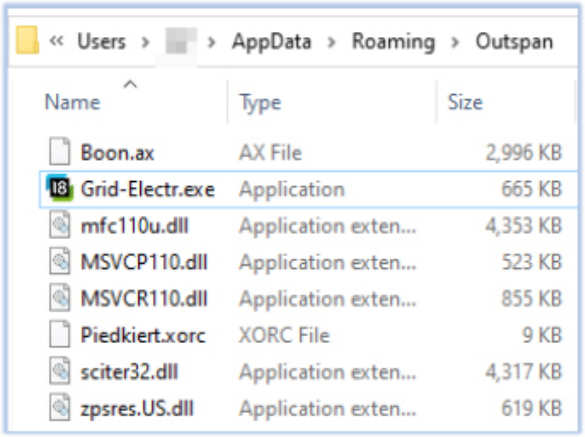
The SOSOLXQT.msi package is then executed using misexec.exe as a child process of BinaryBri86.exe:



msiexec.exe triggers its custom action, which copies and executes Jc6716jK from the Outspan folder as Grid-Electr.exe under C:\Users\user\AppData\Roaming. The SOSOLXQT.msi module is responsible for the core malicious activity of the DeerStealer:

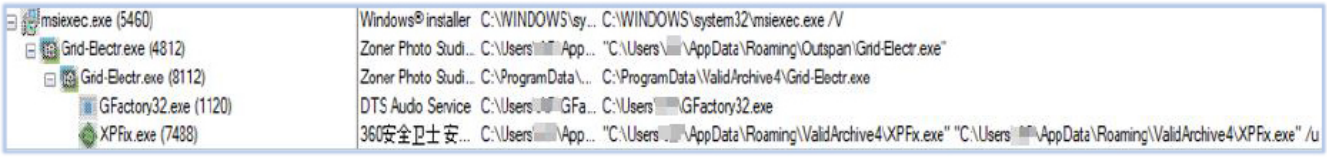


Custom action: SOSOLXQT.msi



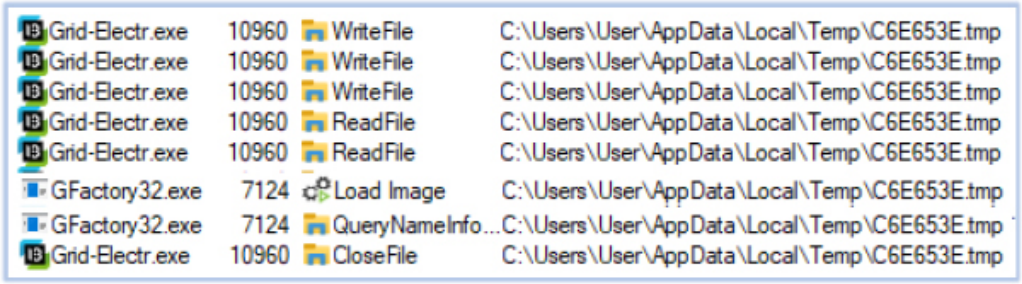
File copied from SOSOLXQT.msi

Grid-Electr.exe copies itself to the C:\ProgramData\ValidArchive4\ directory. Upon further execution, it drops and runs C:\Users\AP\GFactory32.exe:



Process tree: Grid-Electr.exe

GFactory32.exe is an inherently non-malicious executable, a signed file used by Acer Inc. (DTS Audio Service). It loads the C6E653E.tmp file into its process memory from C:\Users\user\AppData\Local\Temp, which was dropped by Grid-Electr.exe. This file enables information and data-stealing capabilities.:



C6E653E.tmp (a randomly generated name that varies with each execution) is hidden by the user-level process and cannot be accessed using standard user-mode tools or methods. This behavior indicates rootkit-like capabilities of

the malware, suggesting that the malware can operate stealthily at a low system level, evading detection and maintaining persistence while performing malicious activities.

GFactory32.exe performs data and information theft on the compromised system. Its targets include, but are not limited to, system information, installed software, user-sensitive data, cryptocurrency wallets, connected devices, web browser data, media players, Office applications, OneDrive, FTP clients, VPN clients, remote access tools, chat applications, and email applications:

GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Armory
GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\Coinomi\Coinomi\wallets
GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\Coinomi\Coinomi\db
GFactory32.exe	ReadFile	C:\$Directory
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Exodus\exodus.wallet
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Guarda\Local Storage\leveldb
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Ever-Surf\Local Storage\leveldb
GFactory32.exe	CreateFile	C:\Users\User\Documents\Monero\wallets
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Electrum
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\atomic\Local Storage\leveldb

Data harvesting: Cryptocurrency wallets

GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\Google\Chrome\User Data
GFactory32.exe	QueryDirectory	C:\Users\User\AppData\Local\Google\Chrome\User Data
GFactory32.exe	QueryDirectory	C:\Users\User\AppData\Local\Google\Chrome\User Data
GFactory32.exe	CloseFile	C:\Users\User\AppData\Local\Google\Chrome\User Data

Data harvesting: Web browser

GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\FileZilla\filezilla.xml
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\FileZilla\sitemanager.xml
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\FileZilla\recentservers.xml
GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\ProtonVPN
GFactory32.exe	CreateFile	C:\Program Files\OpenVPN\config
GFactory32.exe	CreateFile	C:\Program Files\OpenVPN\config-auto
GFactory32.exe	CreateFile	C:\Users\User\OpenVPN\config

Data harvesting: FTP and VPN client

GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\RealVNC
GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\RealVNC
GFactory32.exe	CreateFile	C:\Users\User\AppData\Local\RealVNC\vncviewer.d\passwords.json
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\RealVNC
GFactory32.exe	CreateFile	C:\Program Files\UltraVNC\ultravnc.ini
GFactory32.exe	CreateFile	C:\Program Files\uvnc bvba\UltraVNC\ultravnc.ini
GFactory32.exe	CreateFile	C:\Program Files (x86)\UltraVNC\ultravnc.ini
GFactory32.exe	CreateFile	C:\Program Files (x86)\uvnc bvba\UltraVNC\ultravnc.ini
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\UltraVNC

Data harvesting: remote access tools

GFactory32.exe	7124	CreateFile	C:\Users\User\AppData\Roaming\AnyDesk
GFactory32.exe	7124	CreateFile	C:\Users\User\AppData\Local\Microsoft\Outlook

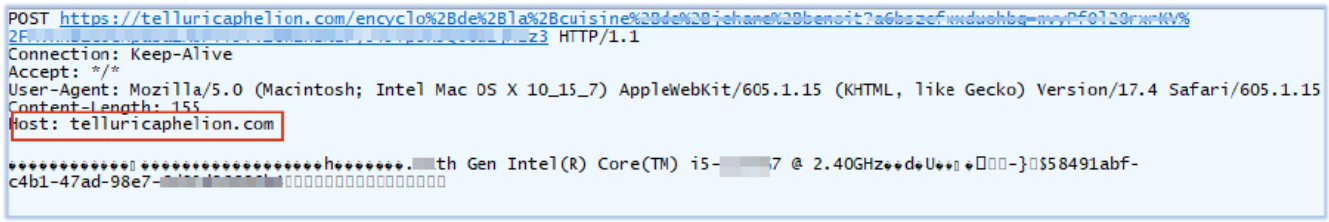
Data harvesting: remote access tools, email application

GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\discordcanary\Local State
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\discordptb\Local Storage\leveldb
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\discordptb\Local State
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\discorddevelopment\Local Storage\leveldb
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\discorddevelopment\Local State
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Telegram Desktop\tdata
GFactory32.exe	CreateFile	C:\Users\User\AppData\Roaming\Telegram Desktop\tdata

Data harvesting: Chat/Messaging applications

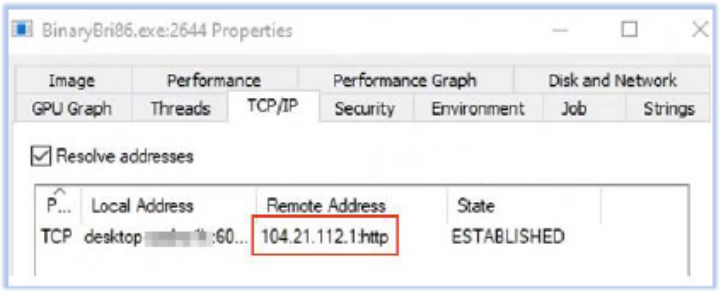
C2 communication:

The harvested data is subsequently exfiltrated to the C2 server at telluricaphelion[.]com.



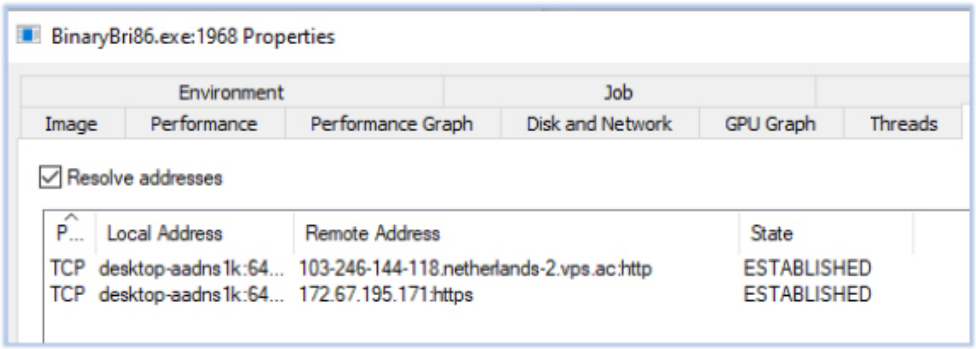
Data Exfiltration

BinaryBri86.exe maintains an open connection with the C2 server, indicating ongoing command-and-control communication, which may be used to receive instructions:



C2 connection

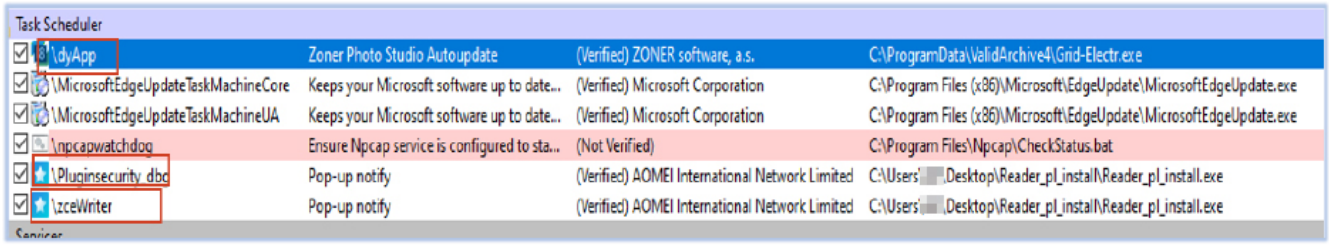
During our analysis, we also observed a change in the C2 server, suggesting possible server migration or an attempt to evade detection:



Change in C2 connection

Persistence:

DeerStealer establishes persistence by creating multiple scheduled task entries, ensuring it runs automatically and survives system reboots:



Created a scheduled task

DeerStealer Capabilities

Analyzing DeerStealer malware offers important insights into its operational features. Based on the findings, the following points summarize the key features of this malware:

- Information theft: Steals system info, credentials, cryptocurrency wallets, browser and app data, media, Office files, OneDrive, FTP/VPN clients, chat, and email data.
- Signed binaries: Use signed executables and legitimate DLLs to evade detection
- Deception: Masquerades as legitimate software like the Adobe Acrobat Reader installer.
- Multi-stage execution: Runs multiple payloads (XPFix.exe, BinaryBri86.exe, SOSOLXQT.msi) for persistence and data theft.
- Persistence: Creates scheduled tasks to survive reboots.
- Privilege escalation: Uses auto-elevated COM objects to bypass UAC.
- Rootkit-like behavior: Hides files like C6E653E.tmp from user-mode tools.
- Data obfuscation: Uses obfuscated files and content to conceal malicious activity and evade detection.
- Adaptive C2: Communicates with C2 servers and can switch servers to evade detection.
- Data exfiltration: Sends stolen data to remote servers stealthily.
- Distribution: Delivered via ZIP archives; sold and supported on dark-web forums and Telegram channels.

Conclusion

DeerStealer is a sophisticated, multi-stage information-stealing malware that employs deception, persistence mechanisms, signed binaries, and rootkit-like capabilities to evade detection and maintain stealth on compromised systems. Its adaptive design, including the ability to switch C2 servers and use obfuscated files, allows it to exfiltrate sensitive information effectively while remaining hidden from user-mode tools and security software. The malware's broad targeting of personal, financial, and system data, combined with its use of legitimate-looking decoys and multi-stage execution, makes it a persistent and potent threat to both individual users and organizations.

As threats like DeerStealer continue to evolve, it is essential for organizations to implement robust cybersecurity measures and proactive defense strategies to mitigate associated risks. Users should exercise caution when opening files from untrusted sources or clicking on unfamiliar links, particularly those promoting suspicious software or content. Implementing strong cybersecurity practices—such as using reputable antivirus solutions, regularly updating all software, and staying alert to social engineering tactics—can greatly enhance protection against sophisticated malware. Additionally, educating users about potential threats and fostering a security-conscious culture within organizations are critical steps in reducing the risk posed by DeerStealer malware and similar threats.

Indicators Of Compromise

S/N	Indicators	Type	Context
1	a03cec07324b0c3227e4f060b0fefc24d35482dfe690bc86df1a53211629837e	File	Reader_pl_install
2	b7ee370878fb4290097311e652222d8bab91c44a94063ea192100d4fd9dadb14	File	Reader_pl_install
3	49ad6431fb67c29e1a2745092232898c491652ddf7115e0332382b42466d0734	File	Up.dll
4	ce62130f0392b40ab047392b47d523f66a55260c9fc2ec3d3727fab13fc87933	File	Reasqueer.efi
5	d4b3a879fb6907c39a3b843ec5272a005e8fec25d8012c4a9fe9d0ada9f71d1f	File	Clortkead.ze
6	e189e7fe9cd6d63ecece8b8e8fafb773003db6009fb0c45dc2b21e77167938ba	File	BinaryBri86.exe
7	0feaaabe6d0a2e29b636cf1f5f9d1b3f727518507ffc93fc881d64feefa2ab81	File	SOSOLXQT.msi
8	623ff1e6662986ab36336919fde5c48805b4a87b97af6f9abe09732e9ac45b8f	File	Boon.ax
9	1432faeddfe57877873e8608ace13739ca66e8ce12b3453531e7eec4753df21d	File	Grid-Electr.exe
10	6f1bfbb8ba6d4eb4e7ce3ff16f1b8e95d601a5eccdd0d743141ac7c3841b11f3	File	Piedkiert.xorc
11	263484f65c76fd3be147ad124a1feaa5240a1d0ce1695855f08f6c6968d1a30d	File	sciter32.dll
12	5ec174af8a18a5516b8a6e11d8a27481d70df14d1edb67c48b5458ff44df9146	File	XPFix.exe
13	telluricaphelion[.]com	Domain	C2
14	loadinnnhr[.]today	Domain	C2
15	nacreousoculus[.]pro	Domain	C2
16	104.21.112[.]1	IP	C2
17	103.246.144[.]118	IP	C2
18	172.67.195[.]171	IP	C2
19	Task Name: \zceWriter	Scheduled Task	Persistence mechanism
20	Task Name: \dyApp	Scheduled Task	Persistence mechanism
21	Task Name: \Pluginsecurity_dbg	Scheduled Task	Persistence mechanism
22	C:\Users\[user-name]\AppData\Roaming\DebugdebugIRG_debug\ZZDCDNTCCJTZXIUKRCZH	Directory	Malware binary presence
23	C:\Users\[user-name]\AppData\Roaming\Outspan	Directory	Malicious binary presence
24	C:\ProgramData\DebugdebugIRG_debug	Directory	Malicious binary presence
25	C:\Users\[user-name]\AppData\Roaming\ValidArchive4	Directory	Malicious binary presence
26	C:\Users\[user-name]\AppData\Roaming\DebugdebugIRG_debug	Directory	Malicious binary presence

MITRE ATT&CK Tactics and Techniques

No.	Tactic	Technique
1	Initial Access (TA0001)	T1566: Phishing T1189: Drive-by Compromise
2	Execution (TA0002)	T1204: User Execution T1059: Command and Scripting Interpreter
3	Persistence (TA0003)	T1053.005: Scheduled Task
4	Defense Evasion (TA0005)	T1036: Masquerading T1622: Debugger Evasion

		T1070.004: Signed Binary Proxy Execution T1027: Obfuscated Files or Information T1014: Rootkit T1027.013: Encrypted/Encoded File T1497: Virtualization/Sandbox Evasion
5	Discovery (TA0007)	T1082: System Information Discovery T1087.001: Local Account T1217: Browser Information Discovery T1673: Virtual Machine Discovery
6	Collection (TA0009)	T1005: Data from Local System T1056: Input Capture
7	Exfiltration (TA0010)	T1041: Exfiltration Over C2 Channel
8	Command and Control (TA0011)	T1001: Data Obfuscation
9	Privilege Escalation (TA0004)	T1548.002: Bypass User Account Control

Recommendations

- Implement threat intelligence to proactively counter the threats associated with DeerStealer malware.
- To protect the endpoints, use robust endpoint security solutions for real-time monitoring and threat detection, such as an Antimalware security suite and a host-based intrusion prevention system.
- Continuous monitoring of the network activity with NIDS/NIPS and using the web application firewall to filter/block the suspicious activity provides comprehensive protection from compromise due to encrypted payloads.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with DeerStealer malware command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Employ application whitelisting to allow only approved applications to run on endpoints, preventing the execution of unauthorized or malicious executables.
- Conducting vulnerability assessment and penetration testing on the environment periodically helps in hardening the security by finding the security loopholes, followed by the remediation process.
- Use of security benchmarks to create baseline security procedures and organizational security policies is also recommended.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.
- Security awareness and training programs help to protect from security incidents, such as social engineering attacks. Organizations should remain vigilant and continuously adapt their defenses to mitigate the evolving threats posed by DeerStealer malware.
- Update security patches, which can reduce the risk of potential compromise.

Back to Listing