Unmasking Agent Tesla: A Deep Dive into a Multi-Stage Campaign | FortiGuard Labs

By Ariel Davidpur

Published: 2026-02-25 · Archived: 2026-04-05 12:56:05 UTC

Affected Platforms: Microsoft Windows
Impacted Users: Windows Users
Impact: Sensitive information stealing and keylogging
Severity Level: High

Background

Agent Tesla remains one of the most persistent threats in the cyber landscape today. It allows even low-skilled threat actors to harvest sensitive data through a highly sophisticated delivery pipeline. This research blog breaks down a recent multi-stage infection chain that utilizes a blend of phishing, obfuscated and encrypted scripts, and advanced in-memory execution and evasion techniques.

Infection Chain

Email > RAR attachment > JScript loader (.jse) > PowerShell (downloaded) > PowerShell (in-memory execution) > .NET loader (in-memory) > .NET Agent Tesla payload (in-memory)

Stage 1: The Initial Hook – A Classic Phishing Play

The campaign begins with a deceptive, business-themed phishing email.

- **The Lure:** Attackers use subject lines such as **"New purchase order PO0172"** to create a sense of urgency.

Stage 2: Script-Based Evasion and Encrypted Payloads

Once the victim executes the JSE file, it triggers a sequence of script-based evasion tactics.

- **The External Fetch:** The script contacts the file-hosting service catbox[.]moe to download a secondary, encrypted **PowerShell (.ps1) script**.

Stage 3: In-Memory Execution via Process Hollowing

Following the initial script-based evasion, the malware transitions into its most stealthy phase: **Process Hollowing**.

- **The Target Process:** The second-stage PowerShell script targets a legitimate system utility, specifically C:\Windows\Microsoft.NET\Framework\v4.0.30319\Aspnet_compiler.exe.
- **The Injection:** The script contains two Base64-encoded assemblies (identifiable by the MZ header). It launches the legitimate process in a suspended state, "hollows out" its memory, and replaces it with the malicious Agent Tesla code.
- **Stealthy Execution:** This allows the malware to run under the guise of a trusted Windows process, making it difficult for basic security tools to identify the malicious activity.

Stage 4: Anti-Analysis—The Final "Sanity Checks"

Once the malicious code is loaded into the hollowed process, it performs a series of defensive checks to ensure the environment is safe for data exfiltration.

- **Virtualization Probing:** The malware queries WMI to identify if the manufacturer is "VMware," "VirtualBox," or "Microsoft Corporation" (Hyper-V).
- **Evasion Trigger:** If these environment checks fail (indicating a researcher’s VM or a sandbox), the malware may cease operations to prevent further analysis of its C2 capabilities.

Stage 5: Data Theft and Exfiltration

Once firmly established, Agent Tesla begins its primary mission: harvesting sensitive data.

- **Credential Harvesting:** It systematically extracts browser cookies, including hostnames, expiry dates, and security flags.

Conclusion

Agent Tesla remains a cornerstone of the modern cyber-threat landscape, not because it is revolutionary, but because it is exceptionally adaptable. Operating under a "Malware-as-a-Service" model, it allows even low-skilled actors to deploy a highly sophisticated, multi-stage infection pipeline that rivals the complexity of advanced persistent threats.

As this analysis demonstrates, the true danger lies in its evasive delivery. From the initial obfuscated JSE loader to the reflective loading of .NET assemblies and process hollowing of legitimate Windows utilities, Agent Tesla is designed to stay invisible. Its extensive anti-analysis checks further ensure that it only reveals its true nature when it’s certain it isn't being watched.

Fortinet Protections

FortiMail detects and blocks phishing emails and strips malicious attachments (RAR/JSE). In addition, real-time anti-phishing protection provided by FortiSandbox, embedded across Fortinet’s FortiMail, web filtering, and antivirus solutions, enables advanced detection of both known and unknown phishing attempts. The FortiPhish phishing simulation service further supports user resilience by actively training and testing end users against real-

world phishing techniques, including impersonation, Business Email Compromise (BEC), and ransomware delivery.

FortiEDR detects and stops Process Hollowing and memory-based attacks in real-time, and FortiGate performs inline blocking of malicious downloads at the network edge.

The FortiGuard CDR (Content Disarm and Reconstruction) service, available on both FortiGate and FortiMail, can neutralize malicious content embedded in documents by removing active code while preserving document usability.

The FortiGuard IP Reputation and Anti-Botnet Security Service proactively blocks infrastructure associated with this campaign by correlating malicious IP intelligence collected from Fortinet's global sensor network, CERT collaborations, MITRE, trusted industry partners, and other intelligence sources.

Organizations seeking to strengthen foundational security awareness may also consider completing Fortinet Certified Fundamentals (FCF) training in Cybersecurity.

If you believe this or any other cybersecurity threat has impacted your organization, contact our Global FortiGuard Incident Response Team for assistance.

Indicators of Compromise (IOCs)

Indicator Type	Value
SHA256 Hashes	Cc2b26bbcbaa2d0593e15a45734fe3fd940451fc7290d49bc841c496b906a9c1 - PO0172.jse 83F9C6A3978D926F2C0155E22008C1BCE6510B321031598509A2937ADD2D5A54 - First encrypted PS1 30713C4BFC813848B3EC28EB227D2E439BE0E07C77237498553FD5DFA745F278 - stage 2 PS1 B133D75DE5010C3A5005606A8E682A08C413364A3921DFBDFBFDDE811A866E88 - Agent Tesla
Download URL	hxxps://files[.]catbox[.]moe/2x0j75[.]ps1
C2 Mail Server	mail[.]taikei-rmc-co[.]biz

TTPs:

Initial Access: Phishing: Spearphishing Attachment (T1566.001)

Execution: Command and Scripting Interpreter: PowerShell & JavaScript (T1059.001, T1059.007)

Defense Evasion: Process Injection: Process Hollowing & Reflective Code Loading (T1055.012, T1620)

Defense Evasion & Discovery: Virtualization/Sandbox Evasion: System Checks (T1497.001)

Credential Access: Steal Web Session Cookie & Credentials from Password Stores (T1539, T1555.003)

Collection: Data from Local System (T1005)

Exfiltration: Exfiltration Over Alternative Protocol: SMTP (T1048.003)
