

# Agent Tesla, Software S0331 | MITRE ATT&CK®

Archived: 2026-04-05 16:50:11 UTC

Enterprise [T1087 .001 Account Discovery: Local Account](#)

[Agent Tesla](#) can collect account information from the victim's machine.<sup>[4]</sup>

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[Agent Tesla](#) has used HTTP for C2 communications.<sup>[4][5]</sup>

[.003 Application Layer Protocol: Mail Protocols](#)

[Agent Tesla](#) has used SMTP for C2 communications.<sup>[6][5][2]</sup>

Enterprise [T1560 Archive Collected Data](#)

[Agent Tesla](#) can encrypt data with 3DES before sending it over to a C2 server.<sup>[7]</sup>

Enterprise [T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[Agent Tesla](#) can add itself to the Registry as a startup program to establish persistence.<sup>[1][8]</sup>

Enterprise [T1185 Browser Session Hijacking](#)

[Agent Tesla](#) has the ability to use form-grabbing to extract data from web data forms.<sup>[2]</sup>

Enterprise [T1115 Clipboard Data](#)

[Agent Tesla](#) can steal data from the victim's clipboard.<sup>[7][1][5][2]</sup>

Enterprise [T1555 Credentials from Password Stores](#)

[Agent Tesla](#) has the ability to steal credentials from FTP clients and wireless profiles.<sup>[3]</sup>

[.003 Credentials from Web Browsers](#)

[Agent Tesla](#) can gather credentials from a number of browsers.<sup>[2]</sup>

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Agent Tesla](#) has the ability to decrypt strings encrypted with the Rijndael symmetric encryption algorithm.<sup>[3]</sup>

Enterprise [T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol](#)

[Agent Tesla](#) has routines for exfiltration over SMTP, FTP, and HTTP.<sup>[7][2][8]</sup>

Enterprise [T1203 Exploitation for Client Execution](#)

[Agent Tesla](#) has exploited Office vulnerabilities such as CVE-2017-11882 and CVE-2017-8570 for execution during delivery.<sup>[8]</sup>

Enterprise [T1564 .001 Hide Artifacts: Hidden Files and Directories](#)

[Agent Tesla](#) has created hidden folders.<sup>[8]</sup>

[.003 Hide Artifacts: Hidden Window](#)

[Agent Tesla](#) has used `ProcessWindowStyle.Hidden` to hide windows.<sup>[3]</sup>

Enterprise [T1562 .001 Impair Defenses: Disable or Modify Tools](#)

[Agent Tesla](#) has the capability to kill any running analysis processes and AV software.<sup>[5]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[Agent Tesla](#) can download additional files for execution on the victim's machine.<sup>[7][4]</sup>

Enterprise [T1056 .001 Input Capture: Keylogging](#)

[Agent Tesla](#) can log keystrokes on the victim's machine.<sup>[7][4][5][2][8]</sup>

Enterprise [T1112 Modify Registry](#)

[Agent Tesla](#) can achieve persistence by modifying Registry key entries.<sup>[8]</sup>

Enterprise [T1027 Obfuscated Files or Information](#)

[Agent Tesla](#) has had its code obfuscated in an apparent attempt to make analysis difficult.<sup>[1]</sup> [Agent Tesla](#) has used the Rijndael symmetric encryption algorithm to encrypt strings.<sup>[3]</sup>

Enterprise [T1566 .001 Phishing: Spearphishing Attachment](#)

The primary delivered mechanism for [Agent Tesla](#) is through email phishing messages.<sup>[2]</sup>

Enterprise [T1057 Process Discovery](#)

[Agent Tesla](#) can list the current running processes on the system.<sup>[5]</sup>

Enterprise [T1055 Process Injection](#)

[Agent Tesla](#) can inject into known, vulnerable binaries on targeted hosts.<sup>[8]</sup>

[.012 Process Hollowing](#)

[Agent Tesla](#) has used process hollowing to create and manipulate processes through sections of unmapped memory by reallocating that space with its malicious code.<sup>[8]</sup>

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

[Agent Tesla](#) has achieved persistence via scheduled tasks.<sup>[8]</sup>

Enterprise [T1113 Screen Capture](#)

[Agent Tesla](#) can capture screenshots of the victim's desktop.<sup>[7][4][1][5][2]</sup>

Enterprise [T1218 .009 System Binary Proxy Execution: Regsvcs/Regasm](#)

[Agent Tesla](#) has dropped RegAsm.exe onto systems for performing malicious activity.<sup>[8]</sup>

Enterprise [T1082 System Information Discovery](#)

[Agent Tesla](#) can collect the system's computer name and also has the capability to collect information on the processor, memory, OS, and video card from the system.<sup>[1][5][3]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Agent Tesla](#) can collect the IP address of the victim machine and spawn instances of netsh.exe to enumerate wireless settings.<sup>[4][8]</sup>

[.002 Wi-Fi Discovery](#)

[Agent Tesla](#) can collect names and passwords of all Wi-Fi networks to which a device has previously connected.<sup>[3]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[Agent Tesla](#) can collect the username from the victim's machine.<sup>[4][1][3]</sup>

Enterprise [T1124 System Time Discovery](#)

[Agent Tesla](#) can collect the timestamp from the victim's machine.<sup>[4]</sup>

Enterprise [T1552 .001 Unsecured Credentials: Credentials In Files](#)

[Agent Tesla](#) has the ability to extract credentials from configuration or support files.<sup>[8]</sup>

[.002 Unsecured Credentials: Credentials in Registry](#)

[Agent Tesla](#) has the ability to extract credentials from the Registry.<sup>[8]</sup>

Enterprise [T1204 .002 User Execution: Malicious File](#)

[Agent Tesla](#) has been executed through malicious e-mail attachments <sup>[2]</sup>

Enterprise [T1125 Video Capture](#)

[Agent Tesla](#) can access the victim's webcam and record video. <sup>[4][7]</sup>

Enterprise [T1497 Virtualization/Sandbox Evasion](#)

[Agent Tesla](#) has the ability to perform anti-sandboxing and anti-virtualization checks. <sup>[3]</sup>

Enterprise [T1047 Windows Management Instrumentation](#)

[Agent Tesla](#) has used wmi queries to gather information from the system. <sup>[2]</sup>

---

Source: <https://attack.mitre.org/software/S0331>