Remote Access Trojan 'Agent Tesla' Targets Organizations with COVID-themed Phishing Attacks

Executive Summary

Agent Tesla is an established Remote Access Trojan (RAT) written in .Net. A successful deployment of Agent Tesla provides attackers with full computer or network access; it is capable of stealing credentials, sensitive information, keystrokes, screen and video activity, and form-grabbing. Researchers have identified a surge of campaigns using coronavirus-related content to deliver Agent Tesla malware using attachments titled 'COVID 19 NEW ORDER FACE MASKS.doc.rtf' or "COVID-19 Supplier Notice.zip." Agent Tesla campaigns exploit Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2017-8570. While Healthcare and Public Health (HPH) organizations are not uniquely vulnerable to RATs in general, or Agent Tesla specifically, this form of malware poses substantial risks to the HPH sector.

Report

RATs allow cybercriminals to exploit legitimate remote access functionality to gain control of victims' computers and networks. RATs are a popular form of malware and are commonly used in cyber-attacks. While some forms of malware are designed for a single type of attack, RATs are far more versatile. Because they provide the attackers with complete control over the victim's computer, there are far fewer limits on what an attacker can accomplish once the malware gains access.

Agent Tesla is an established RAT written in .Net. Because a successful deployment of Agent Tesla provides attackers with full computer or network access, it is capable of stealing credentials, sensitive information, keystrokes, screen and video activity, and form-grabbing. Form-grabbing allows malware to avoid HTTPS encryption by pulling information directly from a web form before it is passed via the Internet to a secure server. Pulling directly from the web form also allows attackers to intercept information inputted using a virtual keyboard, autofill, or copy and paste.


While this malware has been circulating since 2014, Agent Tesla saw a surge of popularity in 2018. Agent Tesla is also a highly-productized form of malware: the creators sell access via a surface website using a monthly-tiered subscription model. Although the malware's creators publicly disclaim that the software is only to be used to monitor the buyer's personal computer, both their website and their customer service platform contain numerous examples of support personnel providing instructions on how to best exploit vulnerabilities and avoid anti-virus software. Once a user subscribes, they gain access to a dashboard and, with a few clicks, can customize what information the malware targets and how the data is exfiltrated.

After security blog KrebsOnSecurity published an article discussing Agent Tesla in October 2018, the malware sellers updated their ecommerce site to again disclaim the use of Agent Tesla as malware, removed some functions of the malware, and announced the banning of some users. Despite this action, in April 2020, Check Point Security Technologies ranked Agent Tesla third on its list of top malware families and identified it as affecting up to three percent of organizations worldwide.

Recently, researchers have identified a surge of campaigns using coronavirus-related content to deliver Agent Tesla malware using attachments titled 'COVID 19 NEW ORDER FACE MASKS.doc.rtf' or "COVID-19 Supplier Notice.zip."

Recent Agent Tesla campaigns have exploited Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2017-8570. Attackers exploit the CVE-2017-11882 vulnerability by running an arbitrary code to deliver the Agent Tesla malware payload and take advantage of vulnerability CVE-2017-8570 to trigger the execution of scripts without user interaction. This vulnerability also downloads the .NET payload, exfiltrating sensitive data and logging victim's keystrokes. The image below (provided by security services provider Quick Heal Security Labs) shows the Agent Tesla attack chain.
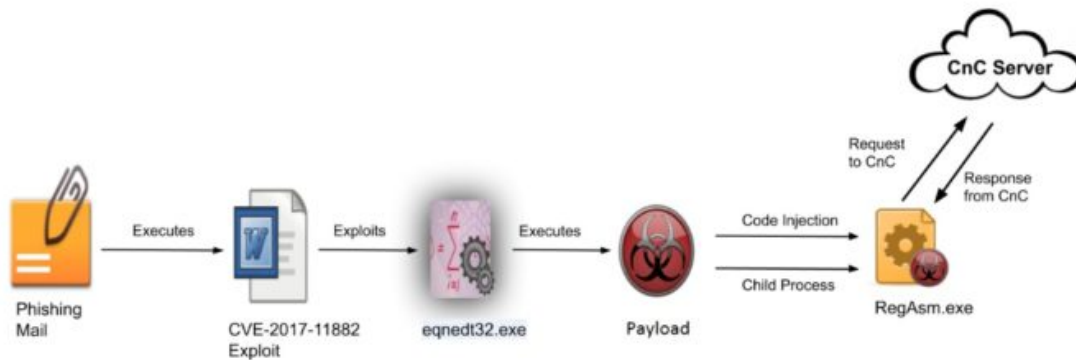
To patch CVE-2017-11882, Microsoft recommends users install security updates 4011604 for affected editions of Microsoft Office 2007, 4011618 for affected editions of Microsoft Office 2010, or updates 4011276 or 2553204. To patch CVE-2017-8570, Microsoft recommends users install the following security updates:

- 3213640 (Microsoft Office 2007 Service Pack 3)
- 3213624 (Microsoft Office 2010 Service Pack 2 (32-bit editions), Microsoft Office 2010 Service Pack 2 (64-bit editions))
- 3213555 (Microsoft Office 2013 RT Service Pack 1, Microsoft Office 2013 Service Pack 1 (32-bit editions), Microsoft Office 2013 Service Pack 1 (64-bit editions))
- 3213545 (Microsoft Office 2016 (32-bit edition), Microsoft Office 2016 (64-bit edition))

To reduce the likelihood that an organization is affected, employees and staff should be trained to recognize and avoid the phishing techniques likely to spread Agent Tesla. Implementing role-based access control can prevent the takeover of a single user's device from affecting larger, more sensitive systems, while regular, secure backups of sensitive data can reduce the impact of attacks that delete or change sensitive data. Organizations should also patch Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2017-8570.

References

Team, Labs. "Tales From the Field: The Surge of Agent Tesla," August 28, 2018.
    https://www.lastline.com/labsblog/surge-of-agent-tesla-threat-report/.

Cisomag. "Attackers Exploiting Flaws In MS Office To Distribute Agent Tesla Malware," May 1, 2020.
    https://www.cisomag.com/researchers-uncover-agent-tesla-malware-abusing-ms-office-
    vulnerabilities/.

Quick Heal Technologies Ltd. "Coronavirus-Themed Campaign Delivers Agent Tesla Malware," April 30,
    2020. https://blogs.quickheal.com/coronavirus-themed-campaign-delivers-agent-tesla-malware/.

"CVE-2017-11882 | Microsoft Office Memory Corruption Vulnerability," November 29, 2017.
    https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882.

"CVE-2017-8570 | Microsoft Office Remote Code Execution Vulnerability." portal.msrc.microsoft.com, July
    11, 2017. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570.

"Who Is Agent Tesla?,"
    https://krebsonsecurity.com/2018/10/who-is-agent-tesla/.

"April 2020's Most Wanted Malware: Agent Tesla Remote Access Trojan Spreading Widely In COVID-19
    Related Spam Campaigns," May 11, 2020. https://blog.checkpoint.com/2020/05/11/april-2020s-
    most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-
    campaigns/.