



Agent Tesla Malware Attack

New Agent Tesla variant in the wild

<https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document>
 CVEs: CVE-2018-0802, CVE-2017-11882

FortiGuard Labs captured a phishing campaign that spreads a new Agent Tesla variant. This well-known malware family uses a .Net-based Remote Access Trojan (RAT) and data stealer to gain initial access by exploiting vulnerabilities Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802. The Agent Tesla core module can collect sensitive information from the victim's device that may include the saved credentials, keylogging information, and device screenshots..

Background
 Agent Tesla made its debut in 2014, and since then, numerous iterations of this malware have been released. This malware employs various tactics to avoid detection, rendering the process of analysis challenging. Agent Tesla is typically spread through phishing emails and has a range of capabilities, including keylogging, screen capture, form-grabbing, and the theft of credentials, among others. Additionally, it has the ability to gather credentials from various software programs, such as Google Chrome, Mozilla Firefox, and Microsoft Outlook, thereby significantly amplifying its potential for causing severe damage.

CVE-2017-11882 and CVE-2018-0802 are RCE (Remote Code Execution) vulnerabilities in Microsoft Office that can result in memory corruption inside the EQNEDT32.EXE process. In this particular case, CVE-2017-11882 and CVE-2018-0802 vulnerability is exploited to download and execute the Agent Tesla file on the victim's device.

Announced
 July, 2023: During late July this year, FortiGuard labs observed Agent Tesla's new variant being propagated and blocked automatically by Sandbox Behaviour engine. The telemetry shows a total of over 150 thousand blocked counts in July and August 2023.

September 05, 2023: FortiGuard Labs captured a phishing campaign that spreads a new Agent Tesla variant and released a detailed analysis blog on;
<https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document>

Vulnerabilities (CVE-2017-11882 and CVE-2018-0802) remains popular amongst threat actors, suggesting there are still unpatched devices in the wild, even after over five years. FortiGuard Labs observed and blocked over 3000+ attacks per day, at the IPS level and the number of observed vulnerable devices according to FortiGuard telemetry is around 1300+.

Latest Developments
 Fortinet customers remain protected from this campaign and other variants of Agent Tesla by FortiGuard's AntiSPAM, IPS, Web Filtering, AntiVirus services, and Behaviour Engine (AI/ML) services. As mentioned on the released Blog earlier, FortiGuard continue to recommend users and organizations to go through the NSE training: NSE 1 – Information Security Awareness, a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks and other best practices.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

AV

Detects and blocks the new Agent Tesla malware

 FortiGate DB 91.06717	 FortiWeb DB 91.06717	 FortiClient DB 91.06717	 FortiSASE DB 91.06717	 FortiMail DB 91.06717	 FortiCASB DB 91.06717	 FortiCWP DB 91.06717
 FortiADC DB 91.06717	 FortiProxy DB 91.06717					

Anti-spam

Detects unwanted spam from reaching customers inbox

 FortiGate v5.0+	 FortiSASE v5.0+	 FortiMail v5.0+
------------------------	------------------------	------------------------

Vulnerability

Detects windows endpoints running vulnerable Microsoft Office (CVE-2018-0802, CVE-2017-11882)

 FortiClient v5.0+

AV (Pre-filter)

Detects and blocks the new Agent Tesla malware

 FortiEDR DB 91.06717	 FortiSandbox DB 91.06717	 FortiNDR DB 91.06717
-----------------------------	---------------------------------	-----------------------------

Behavior Detection

Detects unknown/new variants of Agent Tesla malware

 FortiSandbox v5.0+	 FortiMail v5.0+
---------------------------	------------------------

Exploitation

IPS

Detects and blocks attack attempts to exploit a Code Execution vulnerability in Microsoft Office (CVE-2018-0802, CVE-2017-11882)

 FortiGate DB 20.326	 FortiSASE DB 20.326	 FortiNDR DB 20.326	 FortiADC DB 20.326	 FortiProxy DB 20.326
----------------------------	----------------------------	---------------------------	---------------------------	-----------------------------

Installation

Web & DNS Filter

Detects and blocks known malicious IPs, Domains and URLs related to Agent Tesla Malware

 FortiGate v7.0+	 FortiClient v7.0+	 FortiSASE v7.0+	 FortiProxy v7.0+
------------------------	--------------------------	------------------------	-------------------------

C2

Botnet C&C

Blocks connections channel with known C2 servers associated with Agent Tesla

 FortiClient DB 4.829+

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

 FortiClient DB 1.00013	 FortiAnalyzer DB 2.00019
-------------------------------	---------------------------------

Threat Hunting

 FortiEDR v5.0+	 FortiAnalyzer v6.4+
-----------------------	----------------------------

IOC

 FortiAnalyzer	 FortiSIEM	 FortiSOCaaS
-------------------	---------------	-----------------

Content Update

 FortiSIEM DB 319

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

 FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

 Incident Response	 FortiRecon: ACI
-----------------------	---------------------

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
------------------	------------------------

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

 Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

 Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

 FortiClient	 FortiEDR
-----------------	--------------

Business Reputation

Know attackers next move to protect against your business branding.

 FortiRecon: EASM

Additional Resources

- Analysis of Agent Tesla (2018) <https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant>
- Analysis of Agent Tesla (2022) <https://www.fortinet.com/blog/threat-research/fake-purchase-order-used-to-deliver-agent-tesla>
- Analysis of Agent Tesla (2023) <https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document>

Learn more about [FortiGuard Outbreak Alerts](#)