F#RTINET. **OUTBREAK ALERTS**

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

released a detailed analysis blog on;

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.. Agent Tesla made its debut in 2014, and since then, numerous iterations of this malware have been released. This

Background

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

malware employs various tactics to avoid detection, rendering the process of analysis challenging. Agent Tesla is

CVE-2018-0802 vulnerability is exploited to download and execute the Agent Tesla file on the victim's device. 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

Vulnerabilities (CVE-2017-11882 and CVE-2018-0802) remains popular amongst threat actors, suggesting there

https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document

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+.

Fortinet customers remain protected from this campaign and other variants of Agent Tesla by FortiGuard's 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

Latest Developments

Announced

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity Reconnaissance Weaponization

FortiSASE

DB 91.06717

FortiMail

DB 91.06717

FortiCASB

DB 91.06717

FortiCWP

DB 91.06717

identify and protect themselves from phishing attacks and other best practices.

Delivery AV

PROTECT

Detects and blocks the new Agent Tesla malware

FortiGate

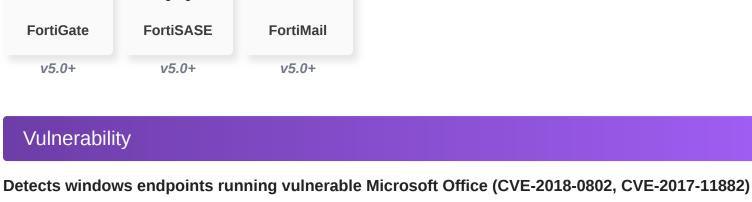
DB 91.06717

Anti-spam

FortiADC FortiProxy DB 91.06717 DB 91.06717

FortiClient

DB 91.06717



Detects and blocks the new Agent Tesla malware

FortiSandbox

DB 91.06717

Detects unwanted spam from reaching customers inbox

FortiWeb

DB 91.06717

Behavior Detection

FortiEDR

DB 91.06717

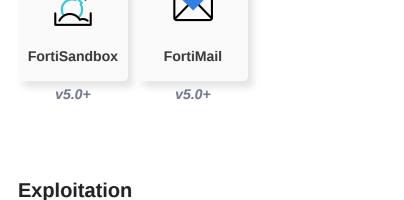
AV (Pre-filter)

FortiClient

v5.0+

FortiNDR

DB 91.06717



FortiSASE

DB 20.326

Detects unkown/new variants of Agent Tesla malware

Web & DNS Filter

FortiGate

DB 20.326

IPS

CVE-2017-11882)

Installation

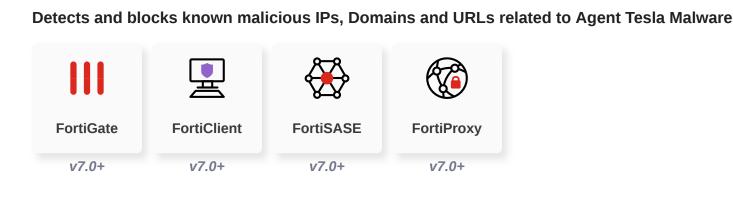
FortiADC

DB 20.326

FortiProxy

DB 20.326

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



Blocks connections channel with known C2 servers associated with Agent Tesla

FortiNDR

DB 20.326

DB 4.829+

Action

C2

Botnet C&C

FortiClient

DETECT

Outbreak Detection

FortiAnalyzer

DB 2.00019

FortiAnalyzer

v6.4+

FortiClient

DB 1.00013

FortiEDR

v5.0+

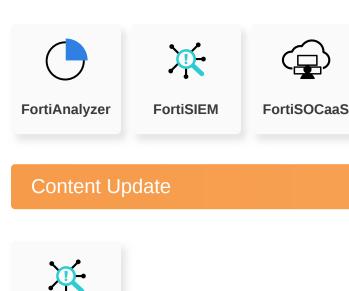
FortiSIEM

DB 319

IOC

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

Threat Hunting



FortiXDR

inciaent

Response

NOC/SOC Training

End-User Training

and other forms of cyberattacks.

cyberattacks.

NSE Training

Automated Response

RESPOND

Assisted Response Services

FortiRecon:

ACI

(and recovery from) security incidents:

Response

Readiness

Services that can automaticlly respond to this outbreak.

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for

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

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download

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

Develop containment techniques to mitigate impacts of security events:



IDENTIFY

Attack Surface Hardening

Security Rating

FortiClient

FortiRecon:

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

FortiEDR

Identify processes and assets that need protection:

Business Reputation Know attackers next move to protect against your business branding.

https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant

https://www.fortinet.com/blog/threat-research/fake-purchase-order-used-to-deliver-agent-tesla

https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document

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

Additional Resources

Learn more about FortiGuard Outbreak Alerts

F

Analysis of Agent Tesla (2018)

Analysis of Agent Tesla (2022)

Analysis of Agent Tesla (2023)