Hackers steal WiFi passwords using upgraded Agent Tesla malware

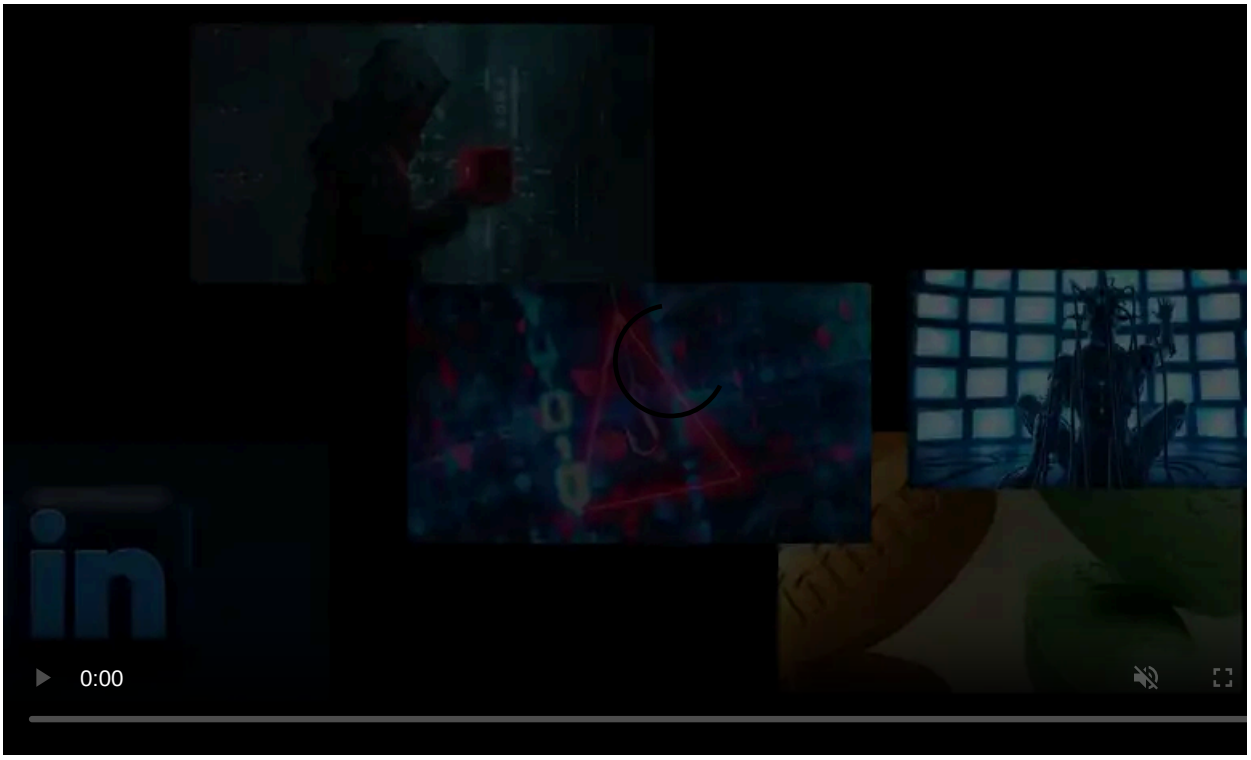
By Sergiu Gatlan

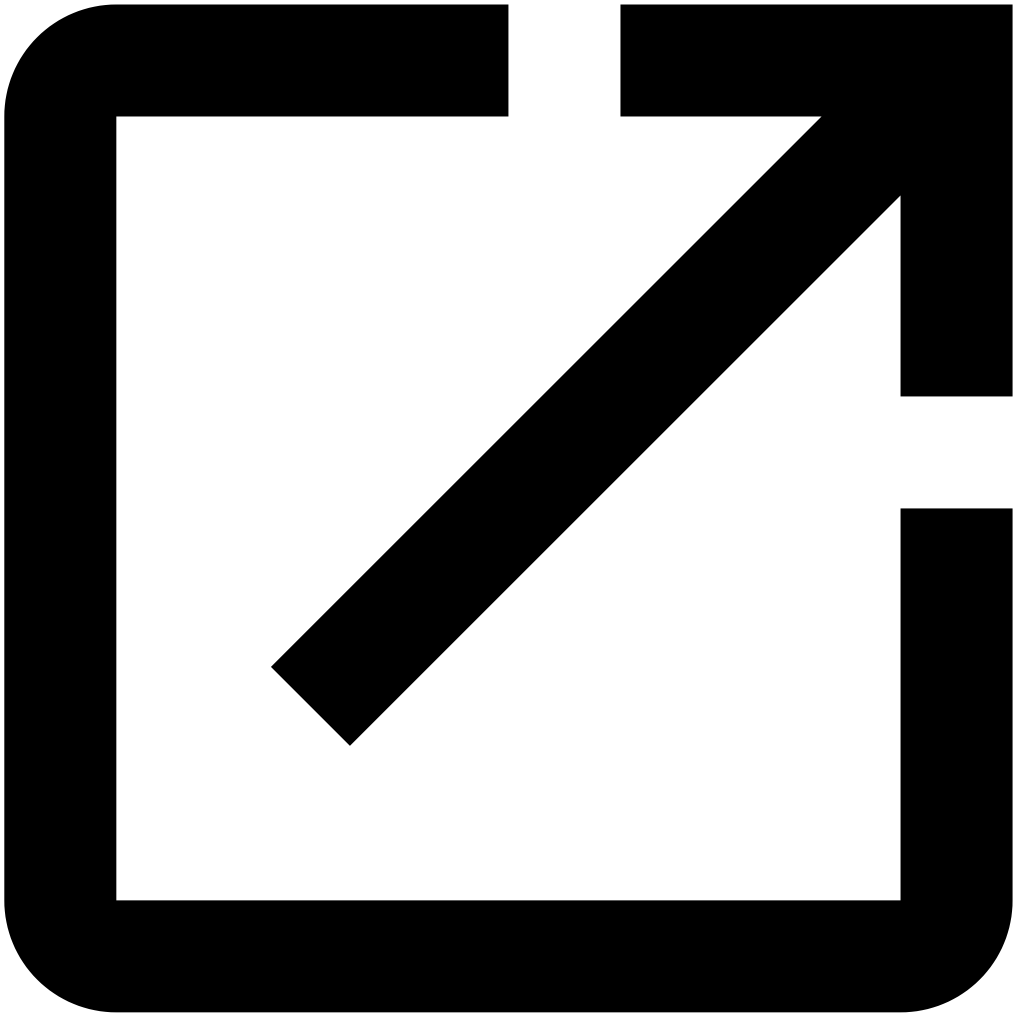
Published: 2020-04-16 · Archived: 2026-04-05 15:47:59 UTC

Some new variants of the Agent Tesla info-stealer malware now come with a dedicated module for stealing WiFi passwords from infected devices, credentials that might be used in future attacks to spread to and compromise other systems on the same wireless network.

The new samples are heavily obfuscated and are designed by the malware's author to collect wireless profile credentials from compromised computers by issuing a *netsh* command with a *wlan show profile* argument for listing all available WiFi profiles.

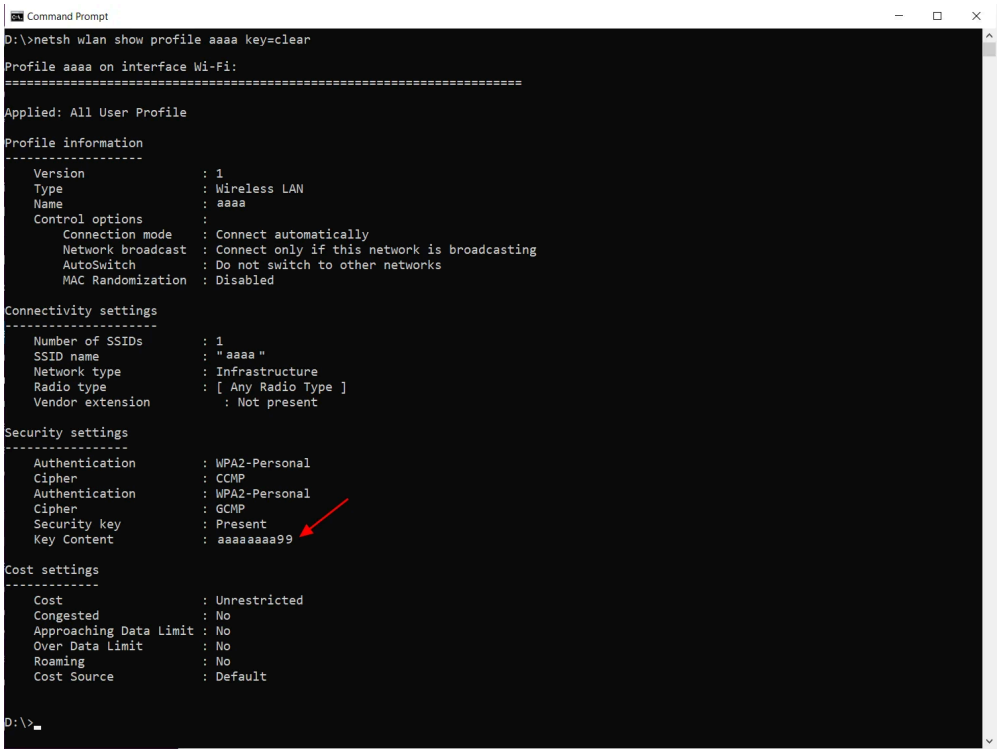
To get the WiFi passwords from the discovered SSIDs (the Wi-Fi networks names), the Agent Tesla info-stealer issues a new *netsh* command adding the SSID and a *key=clear* argument to show and extract the password in plain text for each profile as Malwarebytes' Threat Intelligence team found.


0:00



"In addition to wifi profiles, the executable collects extensive information about the system including FTP clients, browsers, file downloaders, machine info (username, computer name, OS name, CPU architecture, RAM) and adds them into a list," Malwarebytes' report says.

"We believe this may be used as a mechanism to spread [..] or perhaps to set the stage for future attacks."



WiFi password shown in plain text

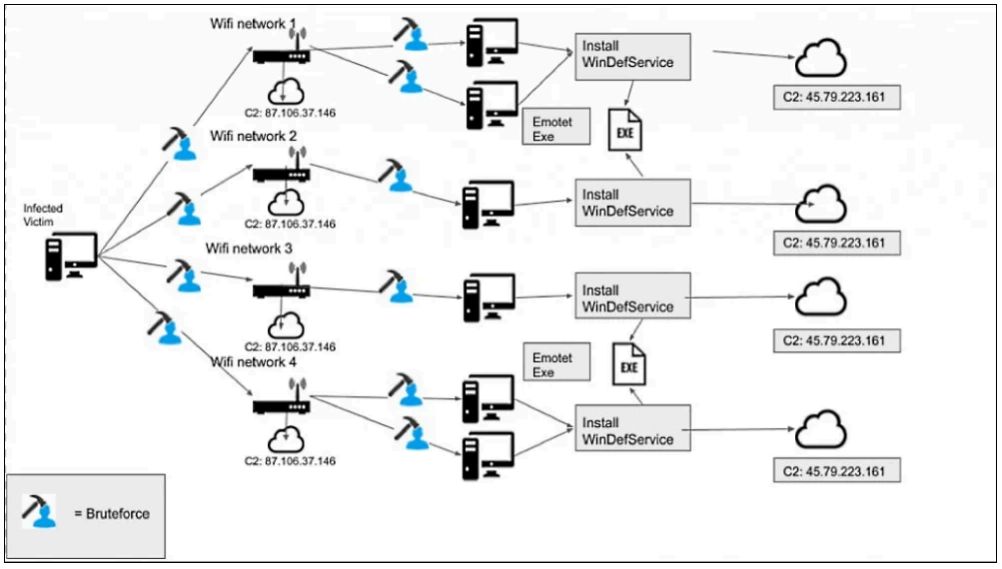
Emotet also got upgraded with a WiFi module

Agent Tesla is not the only malware that has recently been updated with WiFi capabilities. An Emotet Trojan sample spotted earlier this year also got upgraded with a standalone WiFi spreader tool allowing it to infect new victims connected to nearby insecure wireless networks.

This standalone spreader version was used by the Emotet gang for at least two years without any notable changes researchers at Binary Defense who discovered the newly upgraded Emotet samples told BleepingComputer.

Emotet's developers later upgraded the spreader to a fully-fledged Wi-Fi worm module and started using it in the wild according to a researcher who observed evidence of the Emotet Wi-Fi spreader being used to spread throughout one of his client's networks.

With their new focus on this WiFi spreader module, the Emotet gang is on a straight path to developing a highly capable and very dangerous Wi-Fi worm module that will show up more and more often while actively used in the wild.



Emotet's Wi-Fi spreader in action (*Binary Defense*)

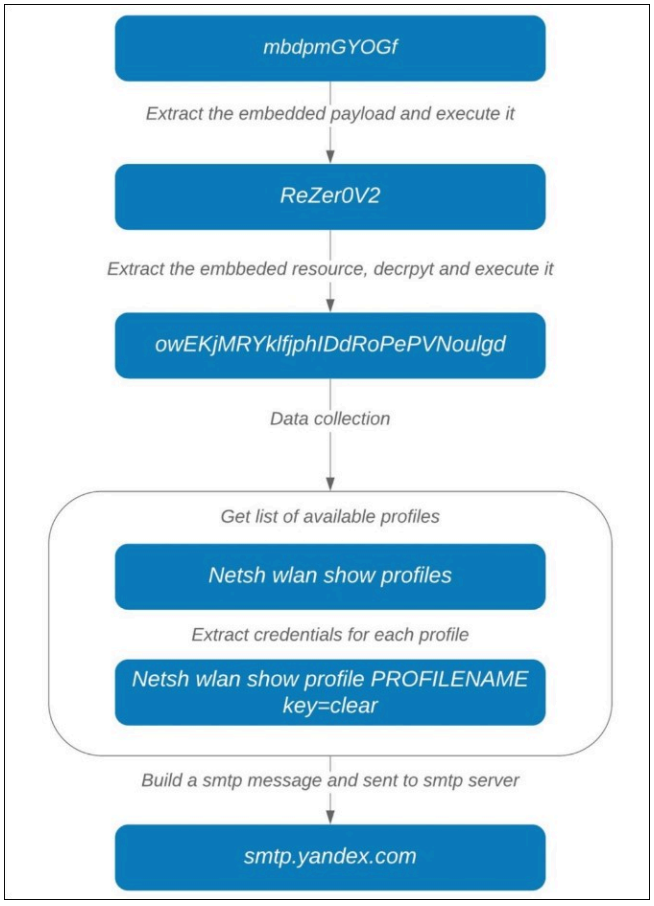
Malware with keylogging and RAT features

Agent Tesla is a commercially available .Net-based info-stealing program with keylogging and remote access Trojan (RAT) capabilities active since at least 2014.

"During the months of March and April 2020, it was actively distributed through spam campaigns in different formats such as ZIP, CAB, MSI, IMG files, or Office documents," Malwarebytes says.

It is currently highly popular among business email compromise (BEC) scammers who use it for recording keystrokes and taking screenshots of infected machines.

The info-stealer can also be used for collecting system information, for stealing clipboard contents data from the clipboard, and for killing running analysis processed and antivirus solutions.



Agent Tesla stealing WiFi passwords (*Malwarebytes*)

To avoid getting infected with a malicious Agent Tesla payload, you have to be very cautious when opening suspicious emails or when visiting hyperlinks received via email, as well as avoid downloading email attachments received from unknown senders.

Agent Tesla ranked second in a 'Top 10 most prevalent threats' ranking published by interactive malware analysis platform Any.Run in December 2019, with 10,324 sample uploads submitted for analysis throughout last year.

Source: https://www.bleepingcomputer.com/news/security/hackers-steal-wifi-passwords-using-upgraded-agent-tesla-malware/