Exclusive: Researchers dumped Gigabytes of data from Agent Tesla C2Cs

By Pierluigi Paganini

Published: 2021-10-06 · Archived: 2026-04-05 16:46:46 UTC

Resecurity researchers dumped Gigabytes of data from Agent Tesla C2Cs, one of the most well-known cyberespionage tools suffers a data leakage.

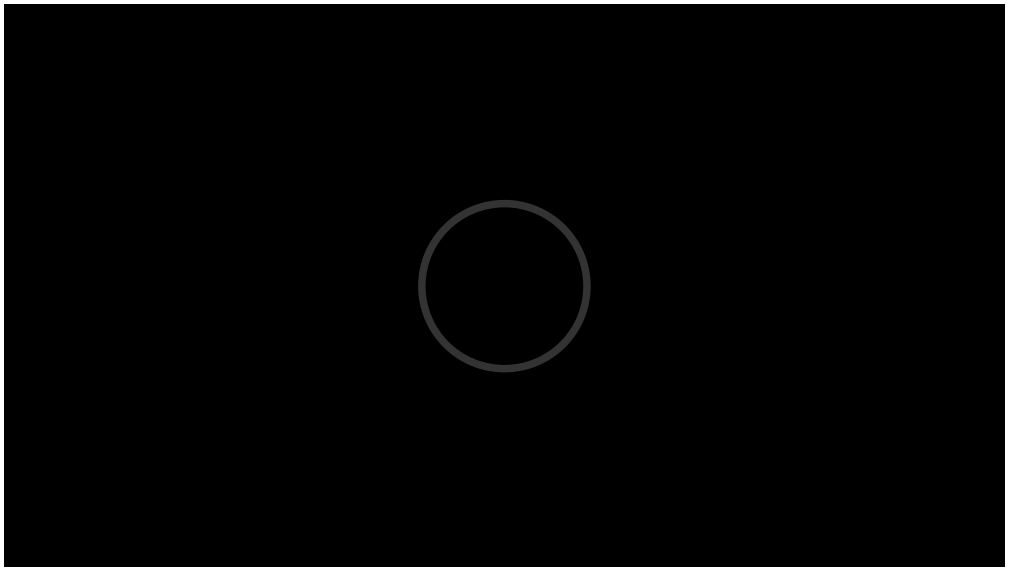
Agent Tesla, first discovered in late 2014, is an extremely popular “malware-as-a-service” Remote Access Trojan (RAT) tool used by threat actors to steal information such as credentials, keystrokes, clipboard data and other information from its operators’ targets.
Both cybercriminal groups and actors involved in espionage operations use this RAT due to Agent Tesla’s stability, flexibility and functionality that allows for the collection of sensitive data and exfiltration from the victim.

Los Angeles-based Resecurity, Inc. and its cyber threat intelligence and R&D unit, HUNTER, drained the Agent Tesla Command & Control Servers (C2) and extracted over 950GB of logs containing compromised Internet users credentials, files and other sensitive information stolen by malicious code. The data extraction was made possible through a collaboration with Resecurity, law enforcement and several ISPs in the European Union, Middle East and North America.

The collected information allowed for the recovery of knowledge about the victims and the timeline of the campaigns conducted by actors leveraging Agent Tesla.
The distribution of victims per geographical area included: USA, Canada, Italy, Germany, Spain, Mexico, Colombia, Chile, Brazil, Singapore, South Korea, Malaysia, Taiwan, Japan, Egypt, United Arab Emirates (UAE), Kuwait, Kingdom of Saudi Arabia (KSA) and other countries in the Gulf region.

The majority of intercepted credentials by Agent Tesla related to financial services, online-retailers, e-government systems and personal and business e-mail accounts.

Researchers found active instances of Agent Tesla and developed a mechanism to enumerate the affected clients and extract compromised data. To share knowledge and encourage information security researchers to combat malicious code, Resecurity's HUNTER unit has prepared an educational video demonstrating the .NET reverse engineering and deobfuscation techniques used for the Agent Tesla analysis.



"Successful tracking of Agent Tesla activity allowed for the recovery of critical insights about the victims affected by it globally and the probable threat actors targeting them. In some cases, we saw obvious patterns of cybercriminals. However, we also saw other actors closely affiliated with particular foreign states leveraging this cyberespionage tool due to its availability in underground hacking communities," said Ahmed Elmalky, an Offensive Cyber Security Researcher at Resecurity, Inc.

According to multiple independent cybersecurity researchers and companies involved in Agent Tesla tracking, this RAT remains a consistent threat for the Microsoft Windows environment and is primarily delivered via e-mail as a malicious attachment.

In the recent update, Agent Tesla is targeting Microsoft's anti-malware software interface (ASMI) in order to avoid detection, alongside using sophisticated evasion mechanisms to transfer stolen data.

Last year, Agent Tesla was spotted in highly targeted campaigns against the oil and gas industry. In one of these campaigns, the actors were impersonating a well-known Egyptian engineering contractor involved in onshore and offshore projects (Enppi – Engineering for Petroleum and Process Industries) to target the energy industry in Malaysia, the United States, Iran, South Africa, Oman and Turkey.

The second campaign, impersonating the shipment company, used legitimate information about a chemical/oil tanker, to make the email believable when targeting victims from the Philippines.

About the author: Resecurity's cyber threat intelligence and R&D unit

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner="9″]	[adrotate banner="12″]

Pierluigi Paganini

(SecurityAffairs – hacking, malware)

[adrotate banner="5″]

[adrotate banner="13″]

Source: https://securityaffairs.co/wordpress/123039/malware/agent-tesla-c2c-dumped.html