AgentTesla Information-Stealing Malware Delivered in Cyber-Attacks on Ukrainian Government Entities

WRITTEN BY
Veronika Telychko

July 20, 2022 · 4 min read

Due to the global cyber war fueled by Russia's full-scale invasion of Ukraine, the attacks in the cyber domain against Ukrainian government entities are continuously on the rise. A week after the phishing campaign by the UAC-0056 group delivering Cobalt Strike Beacon, another cyber-attack targeting Ukrainian officials using information-stealing malware comes on the scene.

On July 20, 2022, CERT-UA issued an alert warning cyber defenders of an ongoing cyber-attack against Ukrainian government entities abusing the war-related topic and spreading a notorious RAT dubbed AgentTesla (also spelled as Agent Tesla). The infection chain is triggered by a malicious file that contains a lure thumbnail related to the Operational Command South (OC South). As a result of the malicious operation, the compromised computers can be infected by the AgentTesla malware.

What Is AgentTesla Spyware: Analysis of the Latest Cyber-Attack on Ukraine

Throughout the ongoing cyber war against Ukraine, adversaries have already applied information-stealing malware strains, like in the malicious campaign of April 2022 distributing IcedID Trojan. That cyber-attack was attributed to the adversary activity of the UAC-0041

hacking collective, which was also linked to the delivery of AgentTesla spyware Trojan in earlier malicious operations against Ukraine.

According to the CERT-UA investigation, the latest cyber-attack targeting Ukrainian government institutions also involves the delivery of AgentTesla samples. This infamous RAT emerged in the cyber threat arena in 2014, and since then, it has continuously evolved to use various advanced techniques to evade detection. AgentTesla is commonly delivered via the phishing attack vector and is capable of stealing credentials from web browsers and multiple software programs like Microsoft Outlook.

In the most recent adversary campaign, the AgentTesla infostealer has been delivered via a PPT file activating a malicious macro that further infects the targeted system. The PPT file contains a lure JPEG thumbnail related to the topic of the Russia-Ukraine war, which provides a reference to the OC South, a formation of the Ukrainian Ground Forces in the southern part of Ukraine. Once opened and enabling a macro, the latter creates and launches both a shortcut LNK file and an executable one. The EXE file is a NET-based program, which applies the ConfuserEx obfuscation tool, downloads a JPEG file, decodes and decompresses the data, and further ends up executing the AgentTesla infostealer on the compromised system.

Detect Malicious Activity Covered by the CERT-UA#4987 Alert

To help organizations protect against AgentTesla spyware Trojan distributed in the most recent cyber-attack on Ukrainian state bodies, SOC Prime's Detection as Code platform offers a batch of dedicated Sigma rules that can be automatically converted to multiple SIEM, EDR, and XDR formats. For streamlined content search, all Sigma rules are tagged as *CERT-UA#4987* based on the corresponding CERT-UA alert. To gain access to this detection stack, please make sure to sign up or log into SOC Prime's platform and then follow the link below:

Sigma rules to detect the malicious activity covered by the CERT-UA#4987 alert

To timely identify the AgentTesla malware samples in the organization's environment, access the entire list of detection algorithms by clicking the **Detect & Hunt** button. Also, cybersecurity professionals can browse SOC Prime to explore the latest threat context linked to the AgentTesla malware, including MITRE ATT&CK® and CTI references along with a list of dedicated Sigma rules. Click the **Explore Threat Context** button to instantly drill down to the comprehensive threat-related information.

DETECT & HUNT | EXPLORE THREAT CONTEXT

MITRE ATT&CK® Context

To dive into into the context of the latest cyber-attack against Ukraine covered by the CERT-UA#4987 alert, all dedicated Sigma rules are aligned with the MITRE ATT&CK framework addressing the corresponding tactics and techniques:

Tactics	Techniques	Sigma Rule
Initial Access	Phishing (T1566)	MSOffice Drops Files to Suspicious Location (via file_event)

Defense Evasion	Signed Binary Proxy Execution (T1218)	Execute Payload with Spoofed Extension (via cmdline)
		LOLBAS rundll32 (via cmdline)

Was this article helpful?

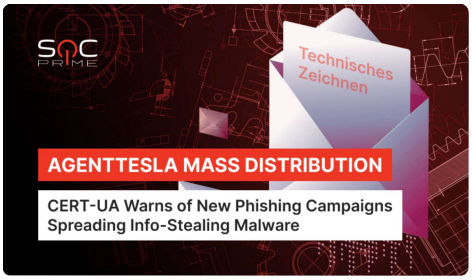
Like and share it with your peers.

0

Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

JOIN FOR FREE BOOK A MEETING

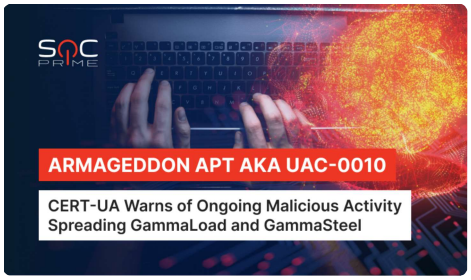
Related Posts



Blog, Latest Threats — 4 min read

AgentTesla Spyware Massively Distributed in Phishing...

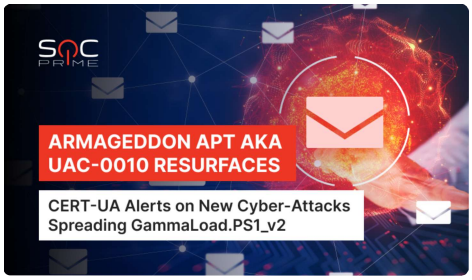
Veronika Telychko



Blog, Latest Threats — 4 min read

Armageddon APT aka UAC-0010 Uses GammaLoad and...

Veronika Telychko



Blog, Latest Threats — 4 min read

Armageddon Threat Actors aka UAC-0010 Spread...

Veronika Telychko