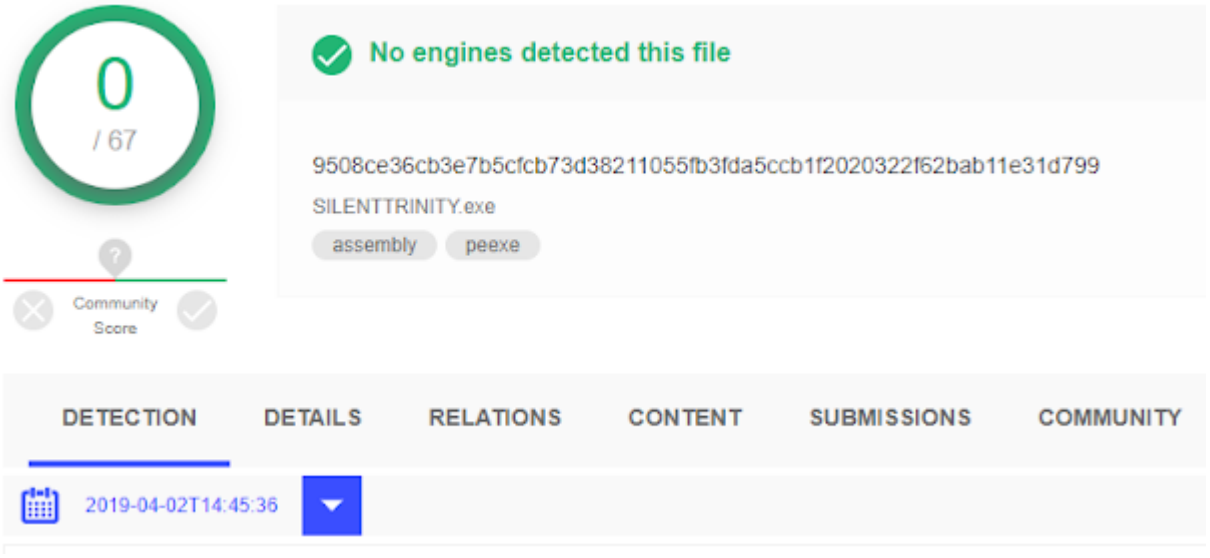
Croatia government agencies targeted with news SilentTrinity malware

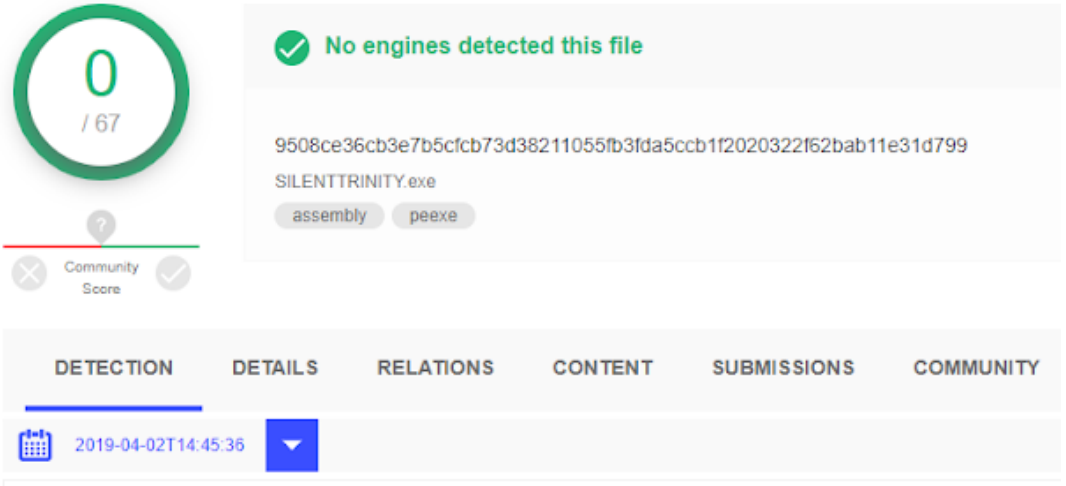
By Pierluigi Paganini

Published: 2019-07-07 · Archived: 2026-04-05 23:10:50 UTC



Croatia government agencies have been targeted by unknown hackers with a new piece of malware tracked as SilentTrinity.

A mysterious group of hackers carried out a series of cyber attacks against Croatian government agencies, infecting employees with a new piece of malware tracked as SilentTrinity. The SilentTrinity malware can take control over an infected computer, it allows attackers to execute arbitrary commands.



Between February and April, allegedly state-sponsored hackers have launched a spear-phishing campaign against government agencies.

The attack was discovered by researchers at Positive Technologies while hunting for new and cyber threats, the attackers used excel weaponized documents.

The phishing messages posed as delivery notifications from the Croatian postal or other retail services, they included a Microsoft Excel saved in the old .xls format and compiled the previous day.

The document included a malicious macro that borrows code from various projects hosted on StackOverflow.com, Dummies.com, Issuu.com, Rastamouse.me, or GitHub.com.

Once the victim has enabled the macro, the malicious code will download and execute the malware on the victim's machine. Experts observed attackers using the Empire backdoor and the SilentTrinity malware.

Searching online for SILENTTRINITY the experts found a reference in the PE file debugging information, the code comes for the IronPython project uploaded on GitHub in October 2018 by Marcello Salvati. The experts aimed at combining flexibility with the advantages of a well-known post-exploitation PowerShell framework by writing it in Python.

"we will describe the basic mechanism and a few highlights of the implementation." reads the analysis published by Positive Technologies.

"Here is what happens after the PE file is run (although the intermediate link does not necessarily have to be a PE file):

- *Contact is made with the C2 server to download a ZIP archive with necessary dependencies and main Python script.*
- *The archive contents are extracted, without being saved to disk.*
- *Dependencies are registered for properly handling Python scripts.*
- *The main Python script runs and waits for a task from the attacker.*
- *Each task is sent as a ready-to-run Python script.*
- *The task is run on the victim's system in a separate thread.*
- *The result is sent back to the C2 server."*

IronPython also supports the Boo language and allows to implement a fileless malware. The C2 traffic is encrypted with AES, the public key is generated using the Diffie–Hellman protocol, the network transport is implemented over HTTP(S) with proxy support.

The attack against Croatia was also spotted by experts at Information Systems Security Bureau (ZSIS) that issued two alerts about the attacks-

"The Office of Information Security (SIS) has, in its several jurisdictions, observed the most recent phishingcampaign most likely to be spread by electronic mail." reads one of the alerts.

"The page contains the content downloaded from the official Croatian web pages, and immediately after visiting the site, the user is offered the download of the ***notification_o_posiljki.xls*** *file.*

So far, two versions of the file are known.

- *The first version represents the SILENTTRINITY malware that runs in the computer's memory and communicates with the malicious server at* ***hxxps: //176.105.255.59: 8089*** *. The malicious program is retrieved via the SMB protocol.*
- *The second version represents the Powershell Empire malware that is downloaded from* ***hxxps: //posteitaliane.live/owa/mail/drafts.srf.***"

The Croatian Post has already taken steps to remove take down the malicious web sites and servers involved in the attacks.

The experts attempted to attribute the attacks to other malicious campaigns, the most important evidence collected they observed is that reuse of a C2 server involved in the attacks exploiting a WinRAR vulnerability to infect government targets in Ukraine.

Researchers at FireEye observed four hacking campaigns, including ones that delivered new pieces of malware. FireEye did not attribute the attack to specific APT, but the choice of targets and TTPs are aligned with Russian state-sponsored campaigns.

Further technical details, including IoCs are reported in the analysis shared by the experts.

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

Pierluigi Paganini

(SecurityAffairs – Croatia, SilentTrinity malware)

[adrotate banner="5″]

[adrotate banner="13″]

Source: https://securityaffairs.co/wordpress/88021/apt/croatia-government-silenttrinity-malware.html