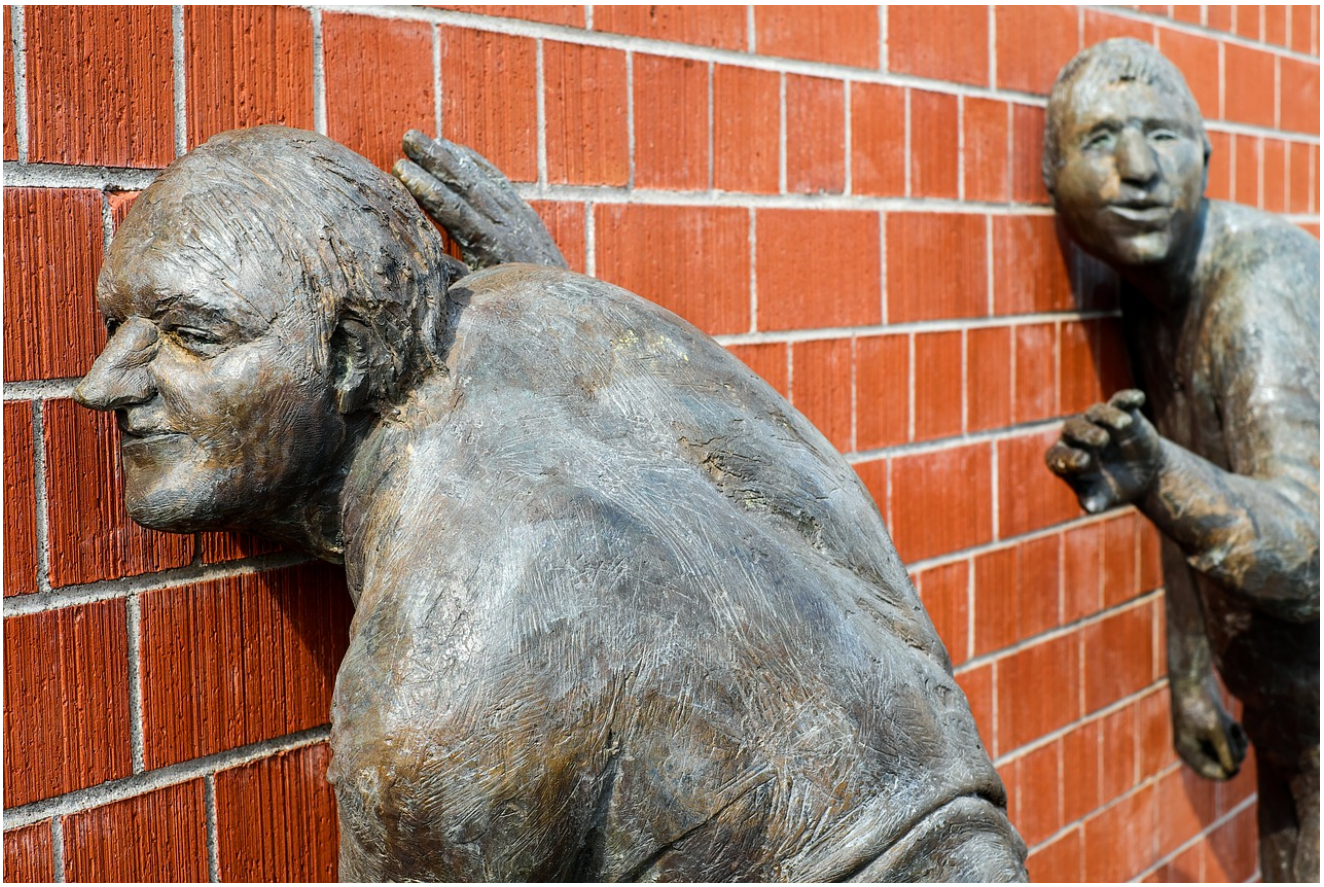
A deep dive down the Vermin RAThole

welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

July 17, 2018



ESET researchers have analyzed remote access tools cybercriminals have been using in an ongoing espionage campaign to systematically spy on Ukrainian government institutions and exfiltrate data from their systems

Kaspars Osis
17 Jul 2018 - 02:57PM

ESET researchers have analyzed remote access tools cybercriminals have been using in an ongoing espionage campaign to systematically spy on Ukrainian government institutions and exfiltrate data from their systems

In this blogpost, we will sum up the findings published in full in our white paper "Quasar, Sobaken and Vermin: A deeper look into an ongoing espionage campaign".

The attackers behind the campaign have been tracked by ESET since mid-2017; their activities were first publicly reported in January 2018. Our analysis shows that these cybercriminals continue to improve their campaigns by developing new versions of their espionage tools.

According to ESET's telemetry, the attacks have been targeted at Ukrainian government institutions, with a few hundred victims in different organizations. Attackers have been using stealthy remote access tools (RATs) to exfiltrate sensitive documents from the victims' computers.

We have detected three different strains of .NET malware in these campaigns: Quasar RAT, Sobaken RAT, and a custom-made RAT called Vermin. All three malware strains have been in active use against different targets at the same time, they share parts of their infrastructure and connect to the same C&C servers.

Quasar is an open-source RAT, which is freely available on GitHub. We were able to trace campaigns by these threat actors using Quasar RAT binaries back to October 2015.

Sobaken is a heavily modified version of the Quasar RAT. Some functionality was removed to make the executable smaller, and several anti-sandbox, and other evasion, tricks were added.

Vermin is a custom-made backdoor. It first appeared in mid-2016 and is still in use at the time of writing. Just like Quasar and Sobaken, it is written in .NET. To slow down analysis, the program code is protected using commercial .NET code protection system, .NET Reactor, or open-source protector ConfuserEx.

Vermin is a full-featured backdoor with several optional components. Its latest known version supports 24 commands, implemented in the main payload, and several additional commands implemented via optional components, including audio recording, keylogging and password stealing.

The analyzed campaigns have been based on basic social engineering, but also using several tricks to better lure the victims into downloading and executing the malware, served as email attachments. Among these tricks are using right-to-left override to obscure the attachments' real extension, email attachments disguised as RAR self-extracting archives, and a combination of a specially crafted Word document carrying a CVE-2017-0199 exploit.

All three malware strains are installed in the same way: a dropper drops a malicious payload file (Vermin, Quasar or Sobaken malware) into the %APPDATA% folder, into a subfolder named after a legitimate company (usually Adobe, Intel or Microsoft). Then, it creates a scheduled task that runs the payload every 10 minutes to ensure its persistence.

To make sure that the malware runs on targeted machines only and avoids automated analysis systems and sandboxes, the attackers have deployed several measures. The malware terminates if neither Russian or Ukrainian keyboard layouts are installed, and also if the target system's IP address is located outside these two countries, or is registered to one of several selected antimalware vendors or cloud providers. The malware also refuses to run on computers with usernames typical of automated malware analysis systems. To determine whether it is run in an automated analysis system, it tries to reach a randomly generated website name/URL and checks if the connection to the URL fails, as would be expected on a real system.

These attackers haven't received much public attention compared to others who target high-profile organizations in Ukraine. However, they have proved that with clever social engineering tricks, cyber-espionage attacks can succeed even without using sophisticated malware. This underscores the need for training staff in cybersecurity awareness, on top of having a quality security solution in place.

ESET detection names and other Indicators of Compromise for the mentioned campaigns can be found in the full white paper: Quasar, Sobaken and Vermin: A deeper look into an ongoing espionage campaign.

17 Jul 2018 - 02:57PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion