KOVTER: An Evolving Malware Gone Fileless

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless

by John Sanchez (Trend Micro Threat Researcher)

While a large number of malware come and go, rarely seen after their initial campaigns, some have remained strong through the years. A common feature of the most persistent malware is their ability to evolve: their initial infection methods, behaviors and payloads rarely stay unchanged.

KOVTER (detected by Trend Micro as KOVTER family) is one example of a constantly evolving malware. Initially starting out as a police ransomware, it eventually evolved into a much more effective and evasive fileless malware. Here is a closer look at KOVTER, as well as tips on how organizations can lessen its impact in case of infection.

[Read more: How are fileless threats abusing PowerShell?]

How has KOVTER evolved over the years?

The malware known as KOVTER has gone through various changes during its lifespan.

The earliest reports of the malware pegged it as a police ransomware, where it remained in a target system waiting for the right opportunity—usually when the user downloaded illegal files. Once triggered, it notifies the user of illegal activity along with a “fine”, which equates to its ransom demand. However, this early version was not too effective, as it required the correct set of conditions and could easily be detected and removed.

The second, and perhaps most visible variant of KOVTER was that of a click fraud malware. This variant used code injection to infect its target, after which it stole information that it then sent to its Command & Control (C&C) servers.

In 2015, KOVTER evolved again into a fileless malware, which it did via the installation of autorun registry entries. It evolved further in 2016, adding file components and registry entries that made use of a shell spawning technique to read the malicious registry entry.

How does the current KOVTER variant work?

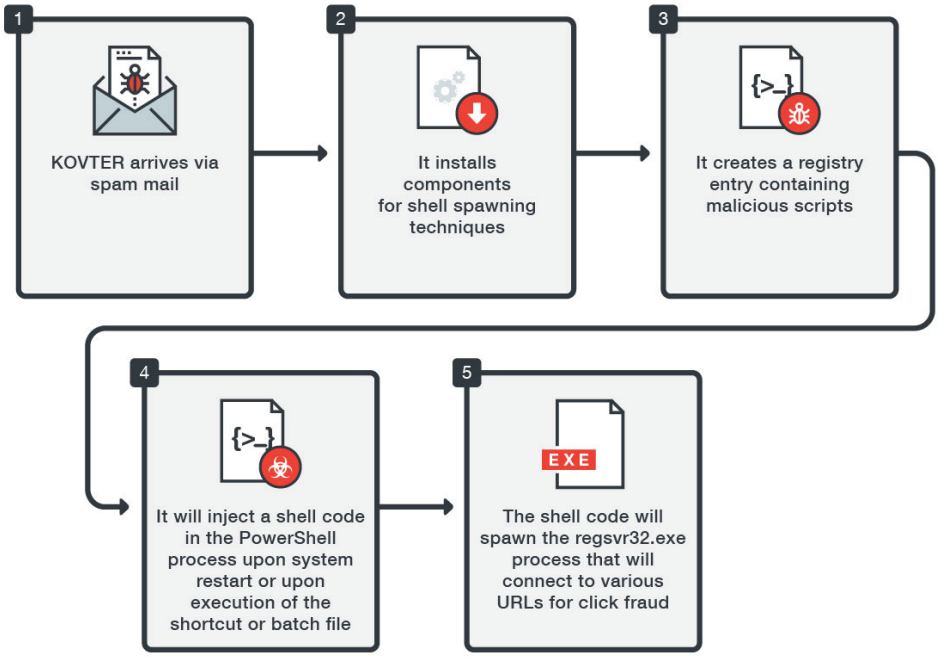

Figure 1: KOVTER infection flow

One of the most common infection methods for KOVTER is via attachments coming from macro-based malicious spam. Once the malicious attachment—usually compromised Microsoft Office files—are clicked, the malware installs a shortcut file, batch file, and a random file with a random file extension in a randomly named folder usually located in %Application Data% or %AppDataLocal%. Registry entries based on the random file extension are also installed in Classes Root to direct the execution of the random file into reading a registry entry. These components are used to perform the malware's shell-spawning technique.

For the next part, the registry entry for the random file is created, containing malicious scripts that perform KOVTER's processes. This means that the moment the infected machine restarts or either the shortcut or batch files are triggered, the malicious script in the registry entry is loaded into memory. The malicious script contains a shell code that the malware injects into the PowerShell process. The shell code will then decrypt a registry entry located in the same registry key. This registry entry is a binary file that is injected into a spawned process (usually regsvr32.exe). The spawned regsvr32.exe would then try to connect various URLs as a part of its click fraud activity.

Upon installation of all these file components and registry entries, the malware spawns a watchdog process that continuously monitors the existence of these components.

How can organizations mitigate the impact of KOVTER?

Given its almost fileless technique, KOVTER has become much more difficult to detect and mitigate. However, there are some things organizations can do to mitigate the malware's impact. Here are some examples of effective mitigation techniques:

Due to its arrival via spam mail, the organization should look into implementing policies that protect against email threats.This includes setting up anti-spam filters that can block malicious emails before they can even reach the endpoint user.

One of the simplest and most effective ways to stop fileless malware is to apply security updates as soon as they are available. Organizations should ensure that their systems have the latest updates to prevent being infected by fileless malware—especially those that exploit vulnerabilities.

PowerShell is frequently abused by fileless malware, thus organizations should take necessary precautions to secure this component. This includes implementing steps on properly utilizing PowerShell in operational or cloud environments. Organizations can also list triggers for detection, which can be based on commands known to be used by malicious PowerShell scripts. Threat actors, for instance, often use the "^" symbol to obfuscate their command prompt parameters when invoking PowerShell. Organizations can also consider disabling PowerShell itself if necessary.

While fileless malware is more difficult to detect, organizations should still put in the effort to monitor and secure all their endpoints. Using firewalls and solutions that can monitor inbound and outbound network traffic can go a long way towards preventing fileless malware from infecting an organization.

Finally, organizations should implement multilayered security solutions such as Trend Micro™ Deep Discovery™, which provides detection, in-depth analysis, and proactive response to today's stealthy malware and targeted attacks in real-time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle. In addition, Trend Micro™ Deep Security™ and Vulnerability Protection provide virtual patching that protects endpoints from threats that abuses vulnerabilities. OfficeScan's Vulnerability Protection shield endpoints from identified and unknown vulnerability exploits even before patches are deployed.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Malware