Endpoint Protection

symantec.com/connect/blogs/kovter-malware-learns-poweliks-persistent-fileless-registry-update

Sep 24, 2015 08:55 AM

A L Johnson

Poweliks made headlines in 2014 as the first persistent, fileless, registry-based malware. This technique had not been seen before Poweliks (Trojan.Poweliks) arrived, but it was only a matter of time until other malware authors adopted it. A variant of Kovter (Trojan.Kotver), first seen in May 2015, looks to be one of the first to incorporate techniques from Poweliks in order to evade detection and remain persistent on the compromised computer.

When the new Kovter variant compromises a computer, the Trojan has the ability to reside only in the registry and not maintain a presence on disk. It accomplishes this by using registry tricks in an attempt to evade detection. The threat is also memory resident and uses the registry as a persistence mechanism to ensure it is loaded into memory when the infected computer starts up.

The Kovter malware family has been around since at least 2013 and has evolved over time. The threat rose to prominence in 2013 and 2014 thanks to its association with traditional ransomware (Trojan.Ransomlock.AK) which locks a victim's computer screen and displays a message demanding a fine for illegal activity. However, Kovter itself is known to perform click-fraud activities.

A fileless threat

Similar to Poweliks, Kovter (version 2.0.3 onwards) has memory-resident, fileless capabilities and uses several techniques to persist in the registry. During initial infection, Kovter checks to see if PowerShell is already installed on the compromised computer. If PowerShell is not found on the computer and internet access is available, then the Trojan downloads a version of the framework. If no internet access is available at the time of infection, then Kovter reverts to being a more traditional file-based malware.

In a fileless infection, Kovter adds a value to one or more of the registry run keys to execute JavaScript using the legitimate MSHTA program.

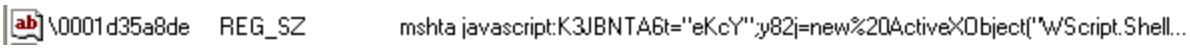

Figure 1. Registry run key value used to execute the malicious JavaScript

Once executed, this JavaScript runs another layer of JavaScript from a different Kovter registry entry. This second JavaScript decodes and executes a malicious Kovter PowerShell script stored within the same JavaScript.

Figure 2. Kovter registry entry containing second JavaScript

The PowerShell script then executes shellcode that decrypts and loads the main Kovter module into memory from a registry entry as seen in figure 2. After a fileless infection, Kovter then deletes the initial file infector from disk. A similar technique was implemented by Poweliks.

Protecting the registry entry

Similar to Poweliks, Kovter attempts to protect its registry entries by using a value name that starts with a null or 0 byte character followed by a string of hexadecimal characters (such as "\x007a865e5da" where "\x00" is the null character). The null character makes it difficult to view the run key values using tools such as Regedit, as they expect registry values to use printable characters.

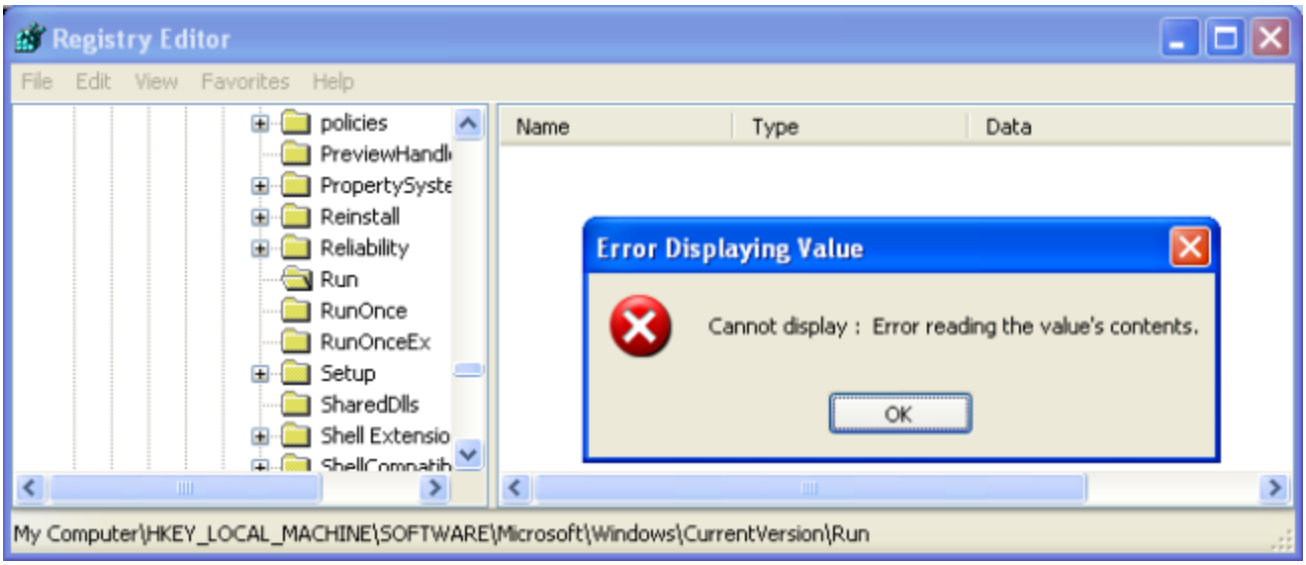

Figure 3. Regedit error when opening Kovter's run key

Distribution

Similar to other common threat actors, the attackers behind Kovter have opted for an affiliate business model to push their threat onto victims' computers. This has led to the Trojan's distribution method changing overtime. Lately, these methods have included malvertisment campaigns targeting adult content websites and news sites. The following exploit kits have reportedly been used to spread the Kovter malware through these attacks:

- Fiesta
- Angler
- Nuclear
- Neutrino
- Sweet Orange

More recently, Kovter has been one of many threats included in a spam campaign's malicious file attachments. These attachments arrive in various forms, such as .zip files containing malicious JavaScript or .scr files. If the files are executed, then they download Kovter and other malware onto the spam recipient's computer.

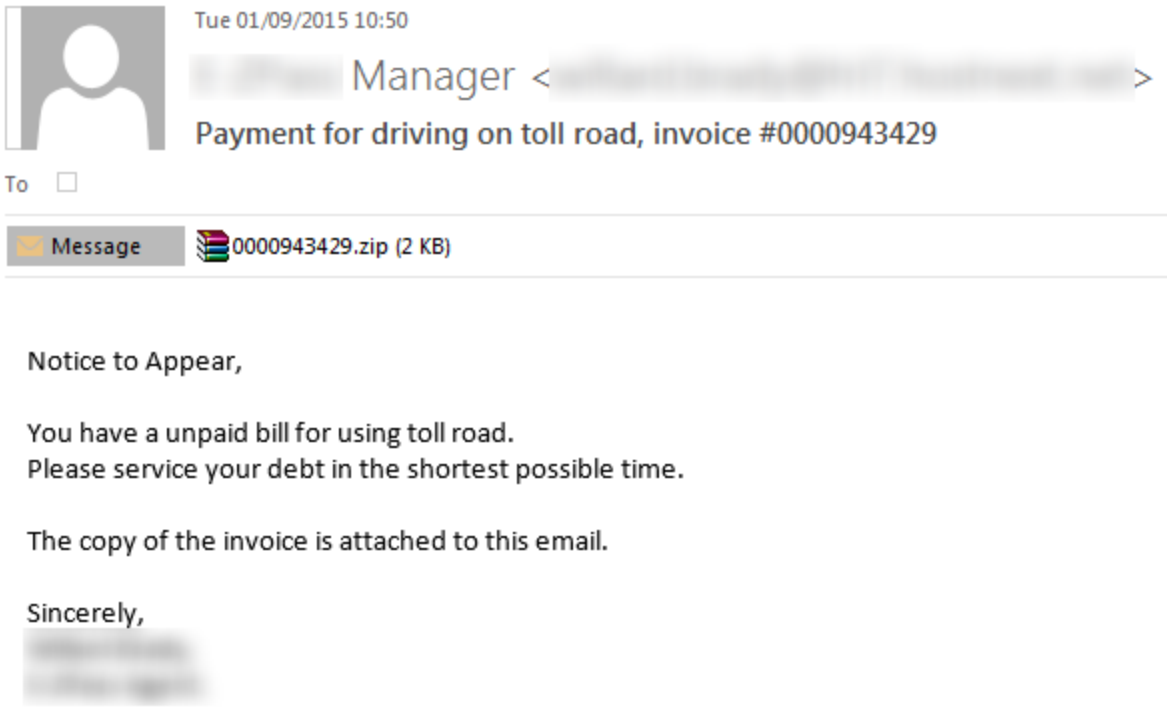

Figure 4. Example of malicious spam emails spreading Kovter

Prevalence

While there are no indications to suggest that Kovter is targeting specific regions, Symantec's telemetry clearly shows that the US is the most affected region. Other impacted areas include the UK, Canada, Germany, Australia, and Japan.

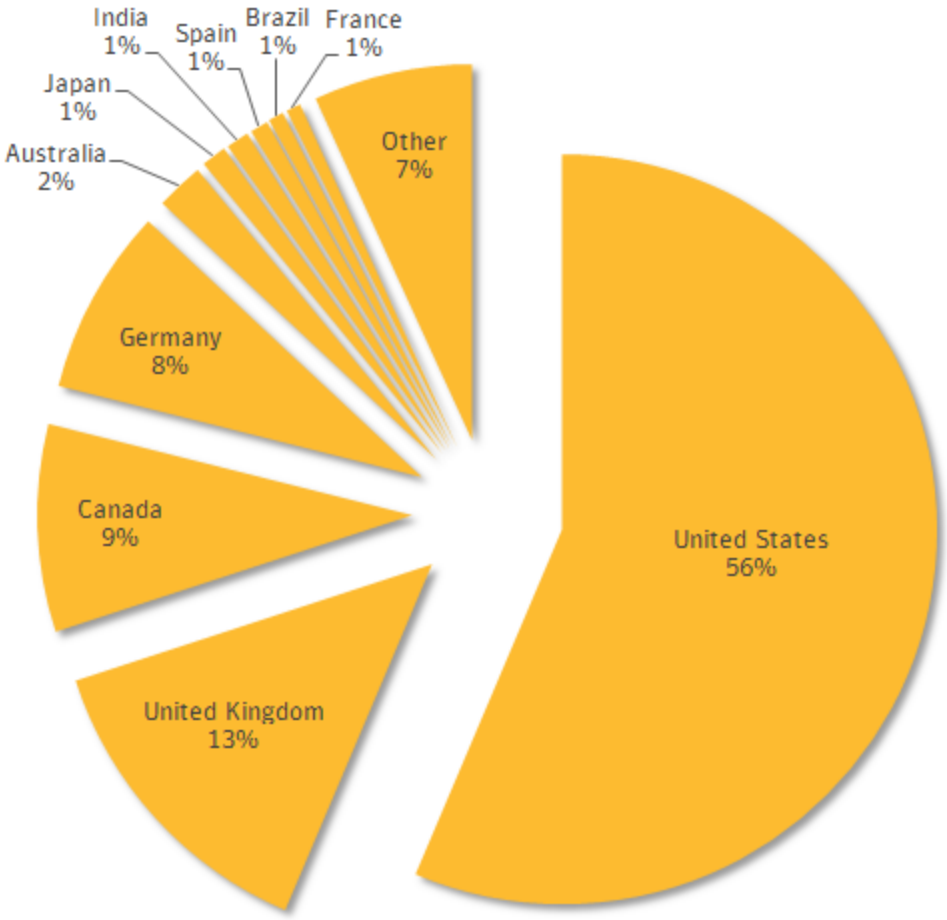

Figure 5. Top 10 regions reporting Kovter detections

Conclusion

It was inevitable that other malware authors would implement the techniques used by Poweliks. With these updates, Kovter's association with ransomware no longer aligned with its stealthy, persistent nature. This has led Kovter to continue its click-fraud activities, allowing the attackers to take advantage of Trojan's stealth capabilities and potential longevity of infection. However, if the malware authors feel that this business model is not profitable enough, then they are still in a position to hold infected computers to ransom.

The Kovter malware family has continually evolved since it was first discovered and shows no signs of leaving the threat landscape anytime soon.

Removal tool

If you believe you have been affected by Kovter or if an intrusion protection signature related to the threat has triggered on your computer, then you should run the following removal tool:

Trojan.Kotver Removal Tool

Symantec and Norton products detect Kovter samples through the following detections:

Antivirus detections

Heuristic detections

Reputation detections

Intrusion protection signatures

Symantec and Norton customers that use the Symantec.Cloud service are also protected from the spam messages which distribute this malware.