Poweliks Update

Background

Poweliks is one of the most widespread pieces of malware infecting computers in recent months. It first appeared in early August, 2014 and has been spreading rapidly since October. This virus is very different from most in one important respect – it does not leave a malicious file on the infected computer. Instead, the malicious code is injected directly into the Registry by a Trojan dropper; once that injection is done, the dropper file is deleted.

As a result of this infection sequence, traditional anti-virus and anti-malware programs that scan the hard drive looking for infected files will not detect Poweliks. Unless a given scanning program knows exactly what to look for, it will erroneously pronounce a Poweliks-infected computer "clean."

Symptoms

It's easy to recognize the symptoms of a Poweliks infection:

- Multiple dllhost.exe processes are running
- CPU utilization is very high
- There is a large amount of network traffic
- Computer is running slowly as a result of these behaviors

More recent variants of Poweliks also disable the ability to download files, by using a "Custom" Security setting. It has also been reported that the infection creates a large number of files in the Temp folder and the Temporary Internet Files folder. This symptom has not been discussed or confirmed by any anti-virus vendors to my knowledge, but the logs I saw from one infected computer revealed almost 300,000 files in these folders – for a total size in excess of 9 GB.

Another case that was suspected to be a Poweliks infection turned out not to be. The tech who reported it saw multiple Conhost.exe processes running and suspected this might be a variant of the typical Poweliks infection. On further investigation, it appears that these processes were associated with Kaseya, which was a legitimate program running on that computer.

How it operates

(This description is based in part on the writeup of Poweliks by Adlice Software, creators of the RogueKiller program.)

The payload is stored in an encrypted Registry Value, and loaded at boot time by that subkey calling a rundll32.exe process on an encrypted Javascript payload. Once the payload is loaded in rundll32.exe, it tries to execute an embedded Powershell script in interactive mode (no UI). That Powershell script contains a base64-encoded payload (another one) which will be injected into a dllhost.exe process (the persistent item), which will be zombified and act as a Trojan downloader for other infections. The dllhost.exe injected thread is also responsible for protecting the Registry Value (persistence item) by recreating it when removed.

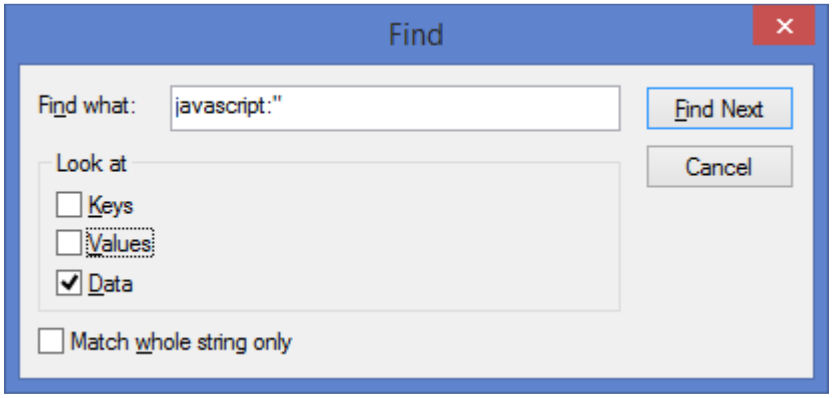
Where it is found

The payload of Poweliks has been found in two different areas of the Registry. In either case the Subkey name and the Value name are injected with unicode characters, so that the high-level API cannot read them and remove them. Said another way, that technique prevents the tech from being able to delete those entries in Regedit or most other Registry-editing tools.

The first generation of Poweliks infections appeared in the Run subkey under HKEY_CURRENT_USER. Later (and current) Poweliks samples have been found in HKEY_ CURRENT_USER \Software\classes\clsid\{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}\ LocalServer32 or HKEY_ CURRENT_USER \Software\classes\clsid\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\LocalServer32, but they actually could use any clsid subkey in the future. Note that most legitimate Clsid entries will be found under HKEY_LOCAL_MACHINE, not HKEY_CURRENT_USER. These legitimate subkeys will also be found at HKEY_CLASSES_ROOT\clsid\{...}.

Easy way to determine whether a computer is infected by Poweliks

Since the behavior of this infection has been consistent, regardless of the Registry subkey used or the exact payload, it is easy to detect its presence. In every case the first of two infected entries will begin with the value "rundll32.exe javascript:"". A simple Find in Regedit will reveal that instruction sequence if it is present. Here is all that needs to go into that Find command:



Be sure you are at the top of the Registry tree before you enter this Find command. If you reach the end of the Registry without finding that sequence, the computer is not infected by Poweliks.

How to remove a Poweliks infection

One problem with Poweliks removal is that the infected computer may be running so slowly that you could spend a lot of time waiting for each step to complete. There is one simple step you can take that will greatly reduce the CPU utilization of the Poweliks processes – disconnect the computer from the network (wired or wireless). Since much of the payload involves attempted communications with the Command and Control Server, breaking that connection will immediately produce a significant performance improvement.

If downloads have been blocked, you can restore that functionality by going into Internet Options | Security tab | Custom level... | Downloads (Enable) or by changing the Security level for this zone back to Medium-high.

In the time since Poweliks first appeared, many articles and blog posts have been written, procedures documented, and tools produced by various software vendors to help in the removal process. The quality and effectiveness of these different methods ranges from poor to very good, and some vendors have updated their tools and procedures as they have learned more about how Poweliks operates and how it protects itself.

Based on feedback I have received from quite a few graduates of my Virus Remediation Training program, as well as my own hands-on work on several Poweliks-infected computers, these are the best solutions I have found to date:

1. ESET offers a free Poweliks removal tool, at http://www.eset.com/int/download/utilities/detail/family/252/. Everyone I have talked with who has used this tool reports that it successfully removed the infection, with minimal effort.

2. MalwareBytes reports that the latest version of their MalwareBytes Anti-Rootkit program detects and removes Poweliks infections. Note that this is NOT the standard MalwareBytes Anti-Malware that we have all been using for long time; that program, good as it is, does not deal effectively with Poweliks. Also note that MBAR is still in Beta testing, as it has been for a long time. I normally do not recommend use of any programs in Beta, but I make a significant exception in this case. You can download it here: http://downloads.malwarebytes.org/file/mbar. Here is a link to a discussion on Poweliks removal in a MalwareBytes forum: https://forums.malwarebytes.org/index.php?/topic/160693-removal-instructions-for-poweliks/.

   Feedback from my alumni who have used this program on Poweliks infections does not reflect 100% success, but it's possible some of them may not have followed the instructions carefully, or they may have tried the program before the Poweliks removal code was included in it.

3. The first solution I distributed involved use of RogueKiller, from Adlice Software. That procedure was effective, if a bit involved. RogueKiller has since updated their program to automatically terminate the dllhost.exe processes, so it is no longer necessary to perform that step manually if you want to stick with RogueKiller for removal. Their article (updated 11/21/14), and the link to download the program, are here: http://www.adlice.com/poweliks-removal-with-roguekiller/.

4. By all accounts I've heard, the Farbar Recovery Scan Tool is effective in finding and removing Poweliks infections. It is also the most confusing to use (for me, at least!), thus its placement at #4 on this list. You may download it from Bleeping Computer here: http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/.

These solutions are listed in the order of my preference, based on reported results, ease of use, and least time required. Any of them should work to find and remove these infections, so it comes down to a matter of personal preference.

Additional resources

Most of the major anti-virus and anti-malware vendors have information about Poweliks on their web sites, although some of it is pretty dated (and thus inaccurate) by now. Here are some of those details, if you want to do further research on your own. These vendors are listed in alphabetical order, with no preference expressed or intended on my part.

- BitDefender – A search for Poweliks on their web site produces no hits. A second-hand conversation with one of their techs confirms that they are aware of Poweliks, but my phone calls and e-mails requesting further information have not been answered.

- Emsisoft – I received a detailed response to my questions from a Malware Analyst at Emsisoft, which was greatly appreciated. Emsisoft has historically been one of the first vendors to detect and effectively deal with emerging malware threats. With regard to Poweliks, the response indicated that "Emsisoft's behavior blocker detects code injection and can block installation of the malware." On the other hand, the analyst follows up by saying, "While Emsisoft products successfully detect Poweliks during installation, at this moment removal after a scan is not yet guaranteed. We are currently working on a safe and reliable way to incorporate this into our engine (rather than adding a solution that might put the system at risk)." I appreciate their candor in this regard, and this response reinforces my high regard for Emsisoft.

- ESET – In addition to their removal tool mentioned above, they have confirmed to me that their normal anti-virus program protects against Poweliks infections.

- Kaspersky – A search for Poweliks on their web site produces no hits. A second-hand conversation with one of their techs confirms that they are aware of Poweliks, but my phone calls and e-mails requesting further information have not been answered.

- Sophos – One of the first vendors to document Poweliks and its behavior. Their article is here: http://www.sophos.com/en-us/support/knowledgebase/121370.aspx, although it has not been updated since September 29. In my own experience of trying their procedure on two infected computers, I was not successful on either. It's possible that I did not give their scanner enough time to complete, and their procedure made no mention of the need to terminate the running dllhost.exe processes.

- Symantec – They offer a manual removal procedure for Poweliks, and a removal tool, which you can find here: http://www.symantec.com/security_response/writeup.jsp?docid=2014-080408-5614-99&tabid=3. While one of my alumni reported successful removal by following the manual procedure, it seems unnecessarily complex and time-consuming to me. If the removal tool works, that is probably a better and faster solution.

Conclusion

Poweliks has presented an unusual challenge in several respects, especially when it was first introduced and the concept of "file-less" malware was unknown. As it has become more widespread, some vendors have developed more effective responses to it. I will continue to keep you updated as we learn more about this infection.