Poweliks

CSC427 DMITRIY & JAMES

Defining Poweliks

“Poweliks is the name of a malicious program. This particular program is a Windows Trojan but what makes it noteworthy is that it does not rely on the presence of a Windows binary file (an executable file on disk) to maintain its infection of a computer.” - sophos.com

SANS Internet Storm Center

“POWELIKS hides its malicious code inside Windows Registry Key. Malware that does not exist in the file system are one of the reasons why memory forensics is important.” – isc.sans.edu

Presentation Outline

I. Background Info of Windows Environment

II. Architecture of Poweliks

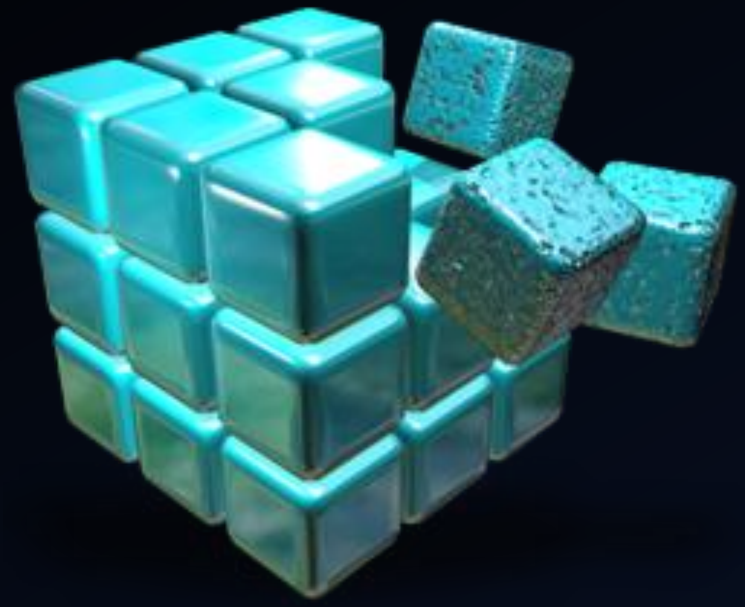
III. Demo

IV. Defense against Poweliks

V. Consequences of Poweliks

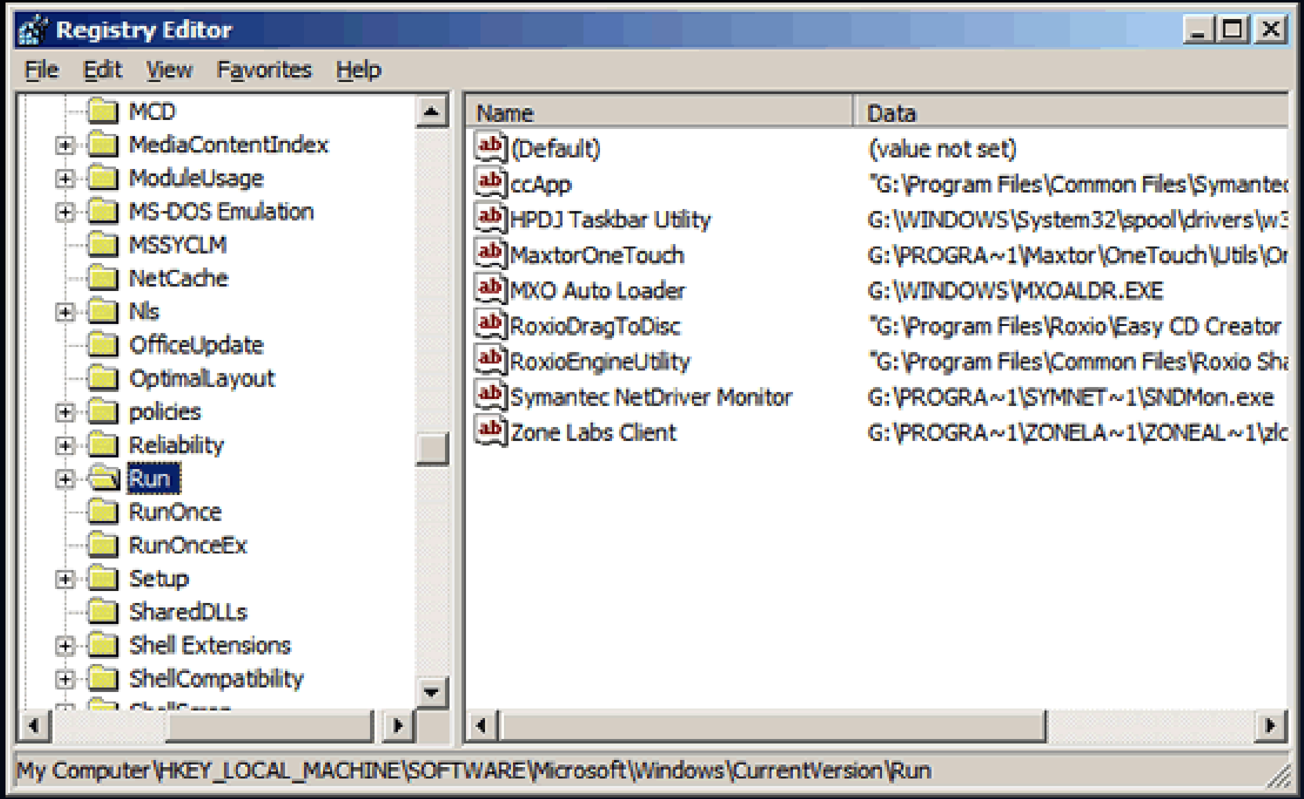
I. Background Information of Windows Environment

Windows Registry Introduction



“The registry is a database in Windows that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer.” - Microsoft

Registry Startup Programs



Name	Data
(Default)	(value not set)
ccApp	"G:\Program Files\Common Files\Symantec
HPDJ Taskbar Utility	G:\WINDOWS\System32\spool\drivers\w3
MaxtorOneTouch	G:\PROGRA~1\Maxtor\OneTouch\Utils\Or
MXO Auto Loader	G:\WINDOWS\MXOALDR.EXE
RoxioDragToDisc	"G:\Program Files\Roxio\Easy CD Creator
RoxioEngineUtility	"G:\Program Files\Common Files\Roxio Sha
Symantec NetDriver Monitor	G:\PROGRA~1\SYMNET~1\SNDMon.exe
Zone Labs Client	G:\PROGRA~1\ZONELA~1\ZONEAL~1\zlc

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The registry can be used to start programs.

Example Key Location:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

RUNDLL32

```
RUNDLL32.EXE <dllname>,<entrypoint> <optional arguments>
```

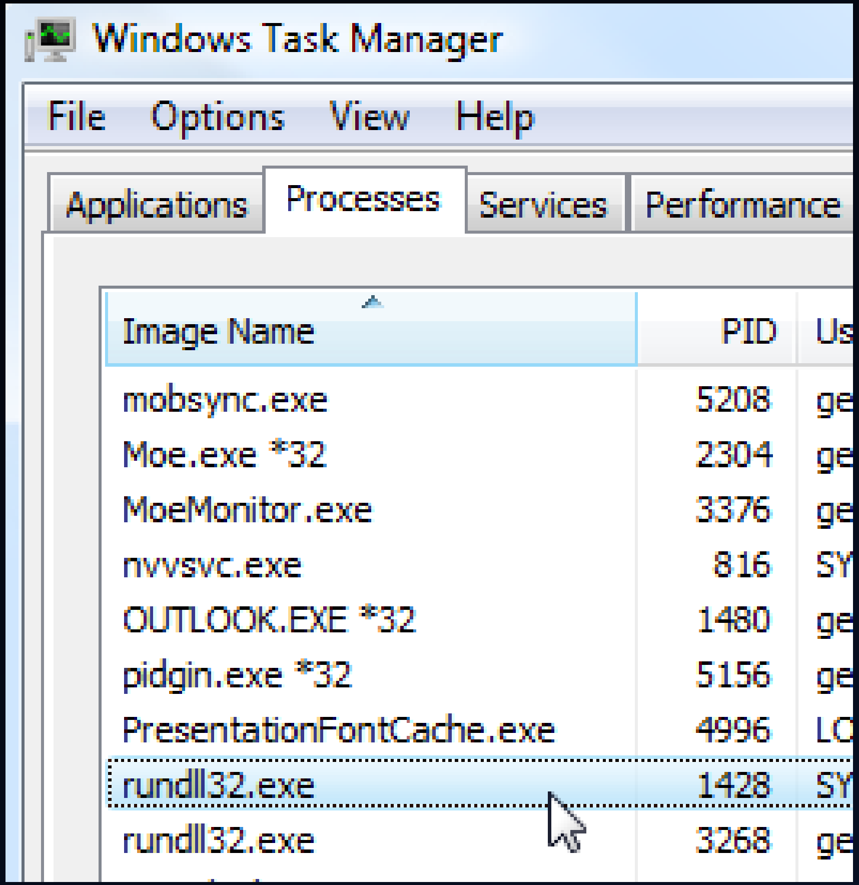


Image Name	PID	Us
mobsync.exe	5208	ge
Moe.exe *32	2304	ge
MoeMonitor.exe	3376	ge
nvvsvc.exe	816	SY
OUTLOOK.EXE *32	1480	ge
pidgin.exe *32	5156	ge
PresentationFontCache.exe	4996	LC
rundll32.exe	1428	SY
rundll32.exe	3268	ge

RUNDLL32.EXE is a program to execute a function from a DLL file

Scripting in Windows

- Batch Scripts
- JScript & VBScript
- PowerShell

II. Architecture of Poweliks

Exploiting Freedom of RUNDLL32

RUNDLL32 allows us to to run *ANY* DLL function!!!

Isn’t there an infamous browser notorious for security issues that conveniently ships with Windows?!

Command to execute javascript as IE:

```
RUNDLL32 javascript:"\..\mshtml,RunHTMLApplication ";alert("foo");
```

Running JS through RUNDLL32

Running javascript this way is much worse since it isn’t being run inside the context of a browser which has a security sandbox.

“Zone security is off, and cross-domain script access is allowed, we have read/write access to the files and system registry on the client machine.” – thisissecurity.net

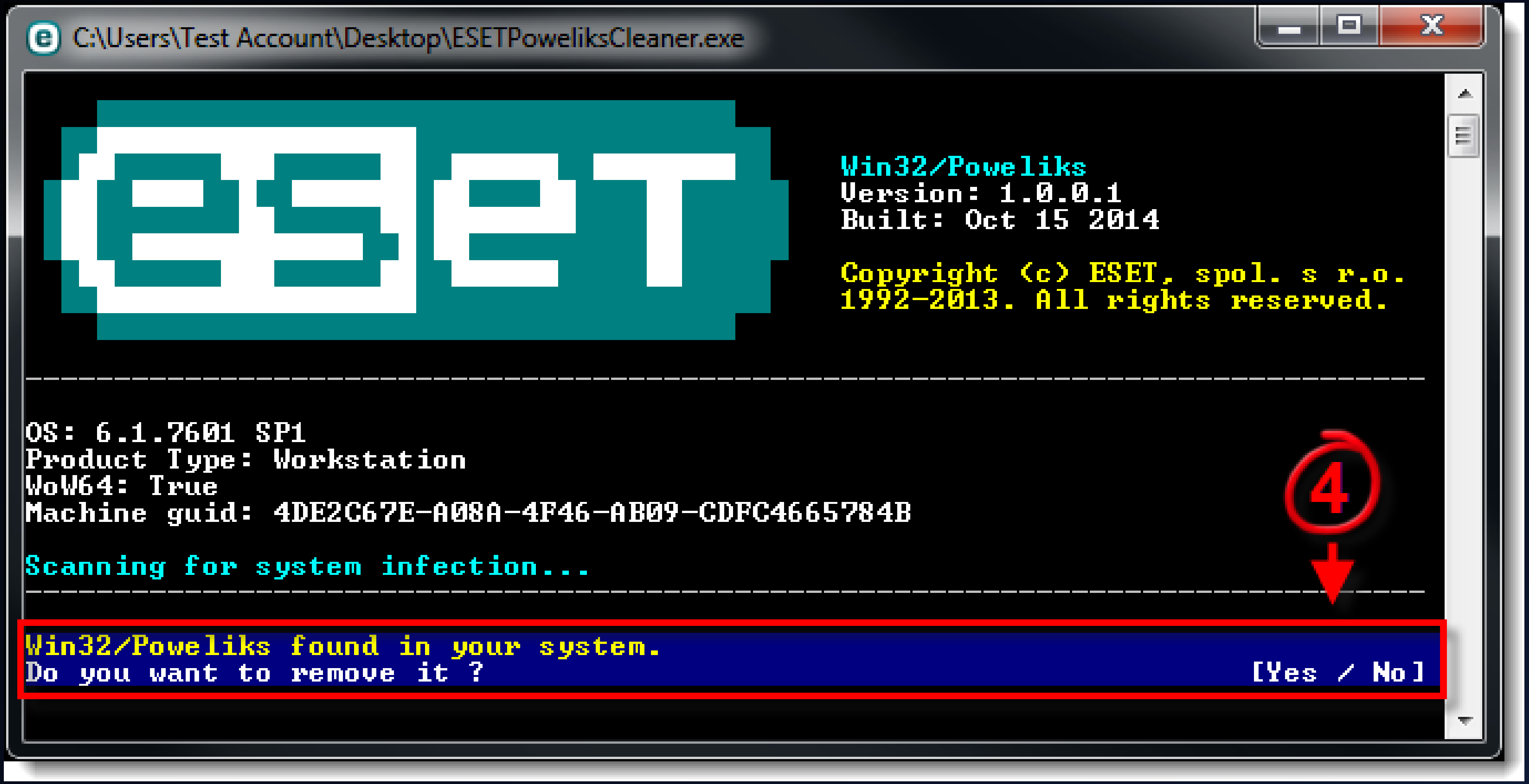
Poweliks at a High Level

- Selects a Registry Startup Program location
- Places an encoded RUNDLL32 command in this spot
- This RUNDLL32 command executes unprotected javascript in IE
- Unprotected javascript in IE can create ActiveXObjects
- ActiveXObjects can read & write to registry and to the file system
- DLLs can be encoded to live inside the registry in different keys

III. Demo

IV. Defense against Poweliks

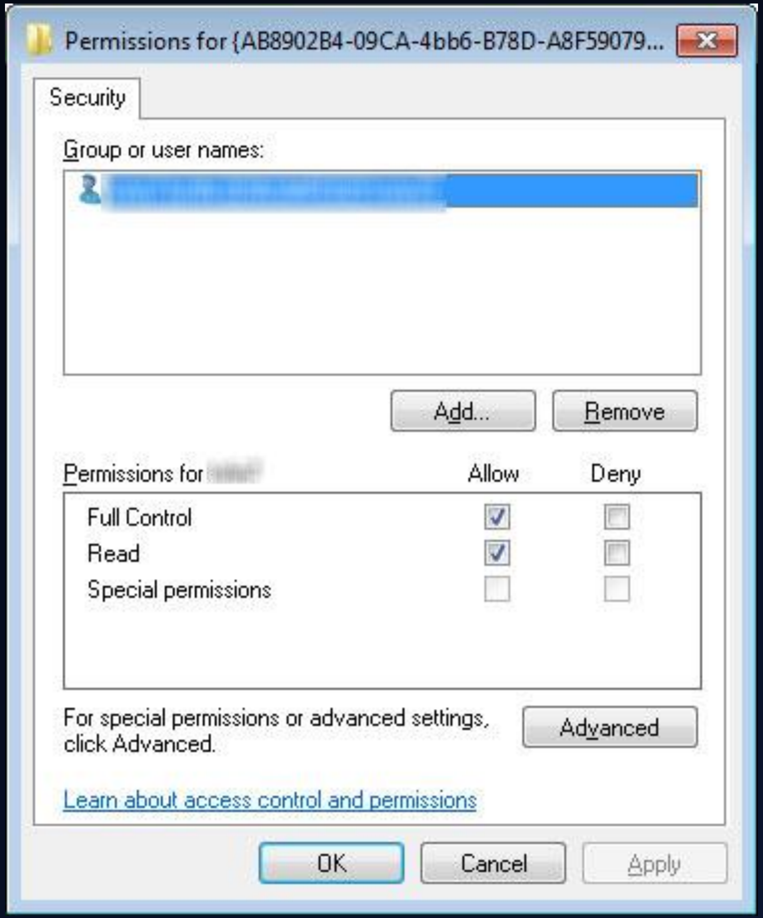
ESET Poweliks Remover



```
Win32/Poweliks
Version: 1.0.0.1
Built: Oct 15 2014

Copyright (c) ESET, spol. s r.o.
1992-2013. All rights reserved.

-------------------------------------------------------------------------------

OS: 6.1.7601 SP1
Product Type: Workstation
WoW64: True
Machine guid: 4DE2C67E-A08A-4F46-AB09-CDFC4665784B

Scanning for system infection...
-------------------------------------------------------------------------------

Win32/Poweliks found in your system.
Do you want to remove it ?                                              [Yes / No]
```

Registry Permissions

Poweliks malware can further hide itself by removing permissions for users.



Permissions for {AB8902B4-09CA-4bb6-B78D-A8F59079...

Group or user names:

[redacted]

Permissions for [redacted]

	Allow	Deny
Full Control	☑	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

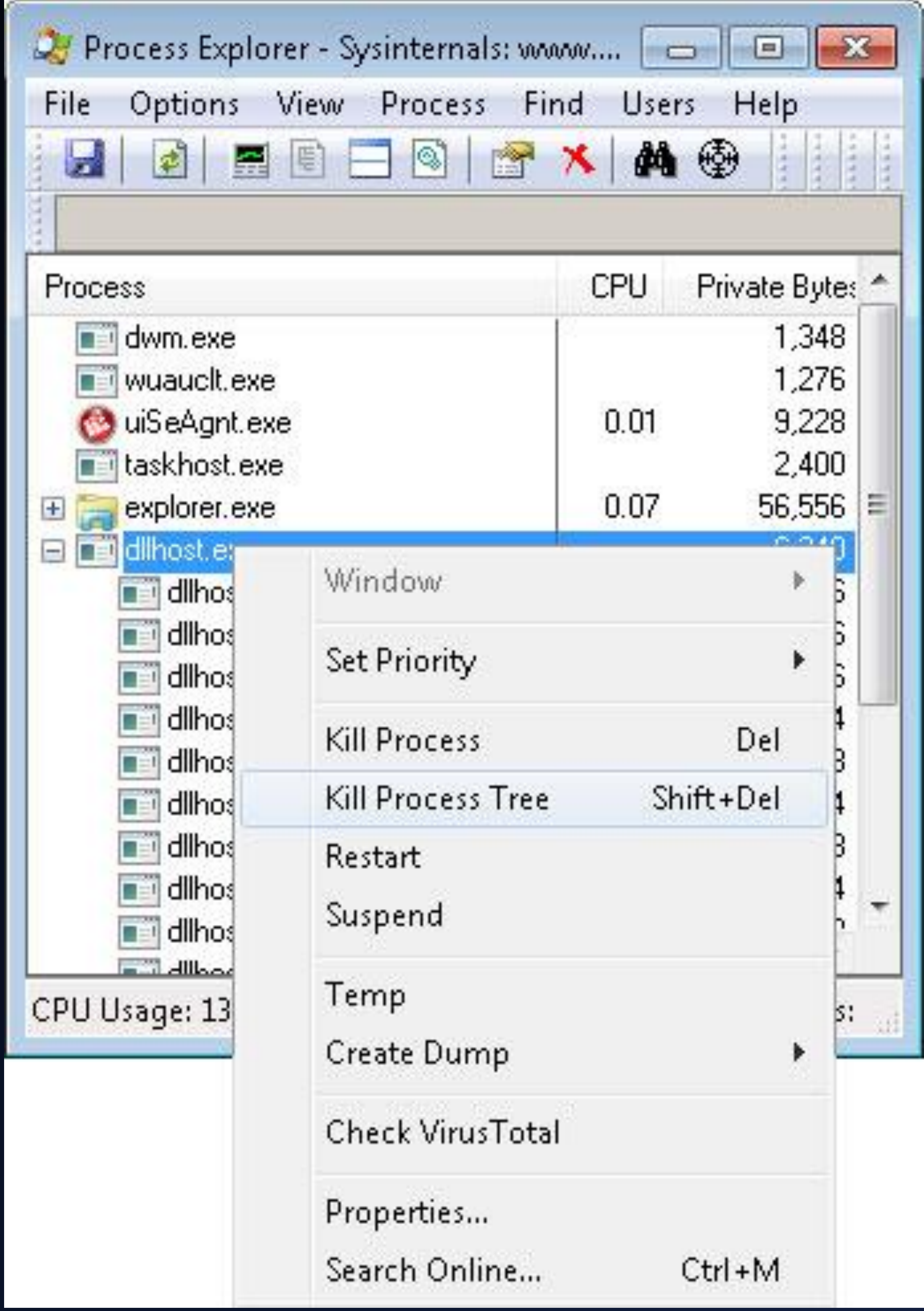
CLSID Registry Keys

"This CLSID is for Window's thumbnail cache, which Windows calls whenever a thumbnail for any file is needed – for images, audio, etc.

As such, when a CLSID is called, it will execute the registry entry to show the thumbnail of the file as well as the entry of POWELIKS in this key.

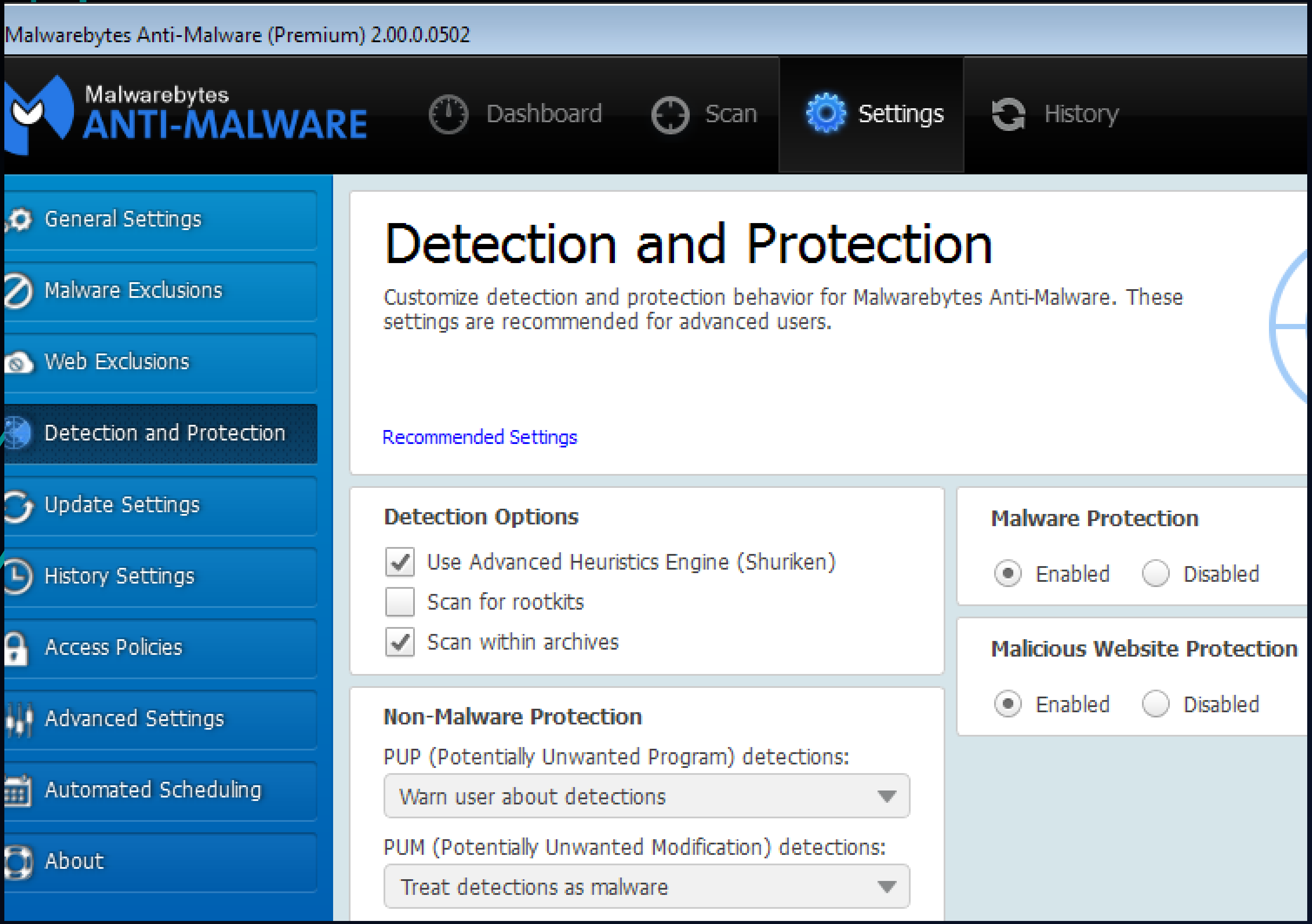
POWELIKS uses dllhost.exe and also dllhst3g.exe to load itself on the system. Each dllhost.exe indicates a running POWELIKS."

- trendmicro.com



Process	CPU	Private Bytes
dwm.exe		1,348
wuauclt.exe		1,276
uiSeAgnt.exe	0.01	9,228
taskhost.exe		2,400
explorer.exe	0.07	56,556
dllhost.e		
dllhos		
dllhos		
dllhos		
dllhos		
dllhos		
dllhos		
dllhos		
dllhos		
dllhos		

Malwarebytes



Malwarebytes Anti-Malware (Premium) 2.00.0.0502

Detection and Protection

Customize detection and protection behavior for Malwarebytes Anti-Malware. These settings are recommended for advanced users.

Detection Options

☑ Use Advanced Heuristics Engine (Shuriken)
☐ Scan for rootkits
☑ Scan within archives

Non-Malware Protection

PUP (Potentially Unwanted Program) detections: Warn user about detections

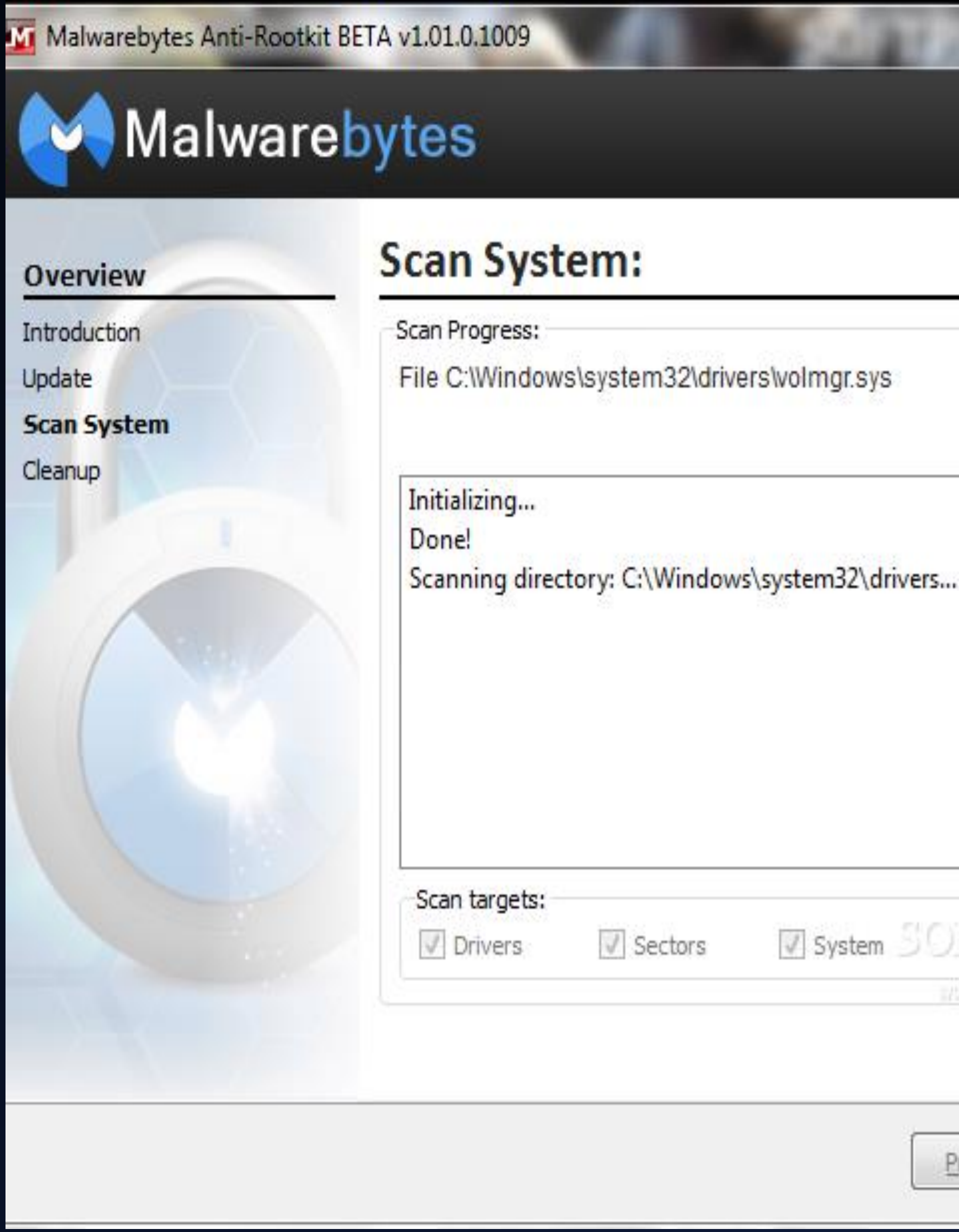
PUM (Potentially Unwanted Modification) detections: Treat detections as malware

Malware Protection

● Enabled ○ Disabled

Malicious Website Protection

● Enabled ○ Disabled



Malwarebytes Anti-Rootkit BETA v1.01.0.1009

Scan System:

Scan Progress:

File C:\Windows\system32\drivers\volmgr.sys

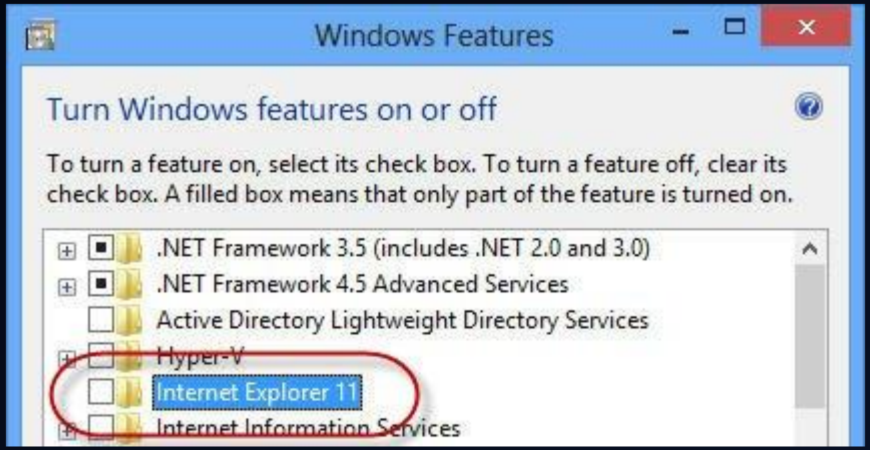
```
Initializing...
Done!
Scanning directory: C:\Windows\system32\drivers...
```

Scan targets:

☑ Drivers ☑ Sectors ☑ System

Managing Internet Explorer

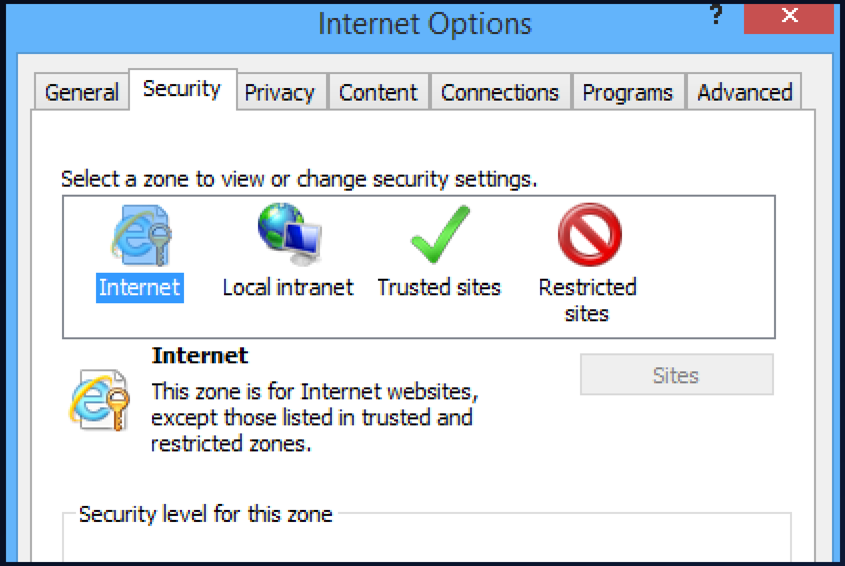
“Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system will receive technical supports and security updates. Internet Explorer 11 is the last version of Internet Explorer, and will continue to receive security updates, compatibility fixes, and technical support on Windows 7, Windows 8.1, and Windows 10.” - Microsoft



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Hyper-V
- □ Internet Explorer 11
- □ Internet Information Services



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Installing a More Secure Browser

An alternative browser like Chrome should be used.

Powershell Script:

```
(new-object
System.Net.WebClient).DownloadFile('http://dl.google.com/chrome/install/375.
126/chrome_installer.exe', 'c:/temp/chrome.exe');. c:/temp/chrome.exe
/silent /install;rm c:/temp -rec
```

V. Consequences of Poweliks

POP QUIZ

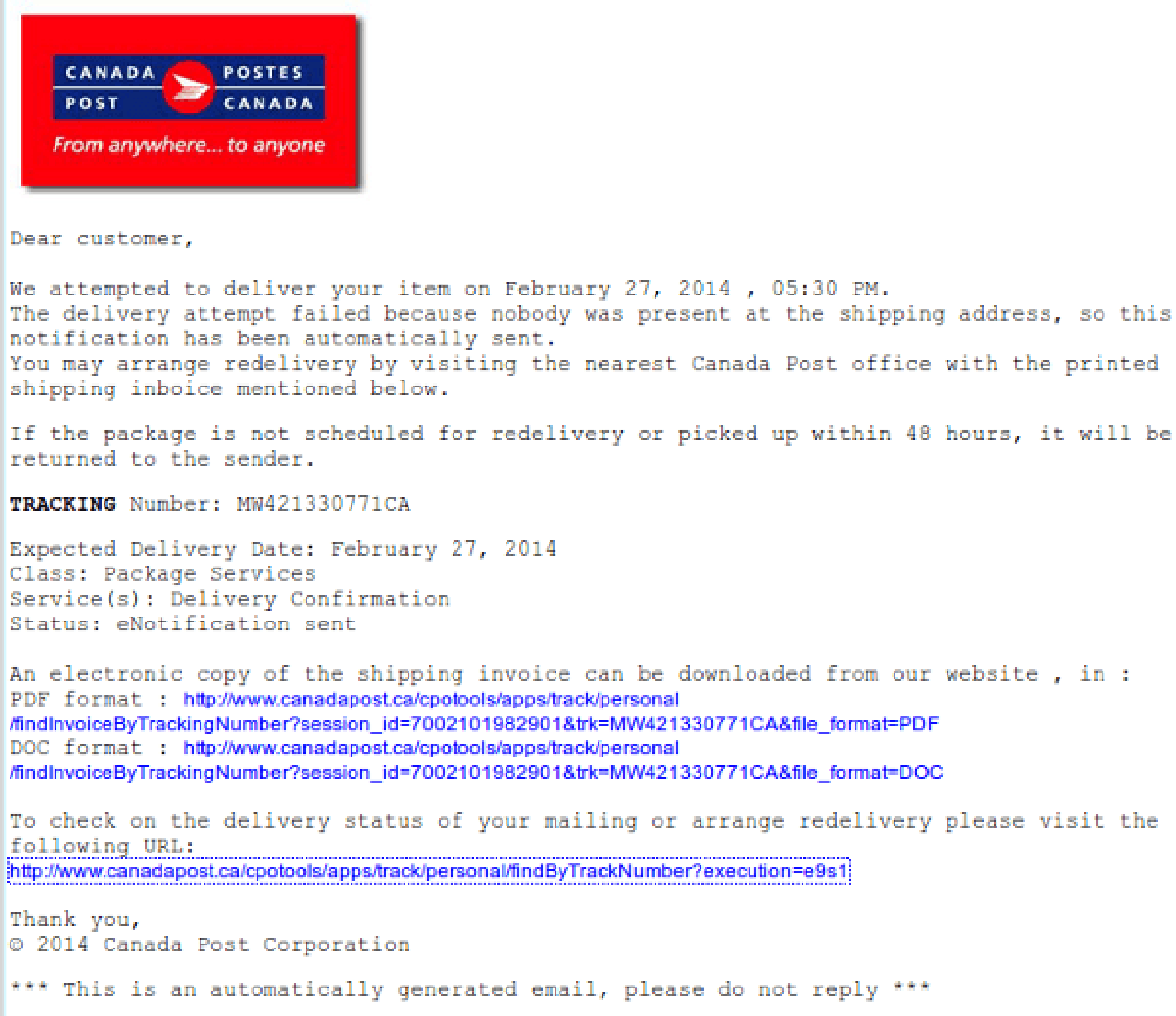
For Poweliks, what are possible infection vectors?

a) USB drive with an elusive “install.exe”

b) An email containing an attachment

c) Viewing a web address with IE

d) MS Word Document



Dear customer,

We attempted to deliver your item on February 27, 2014 , 05:30 PM.
The delivery attempt failed because nobody was present at the shipping address, so this notification has been automatically sent.
You may arrange redelivery by visiting the nearest Canada Post office with the printed shipping inboice mentioned below.

If the package is not scheduled for redelivery or picked up within 48 hours, it will be returned to the sender.

TRACKING Number: MW421330771CA

Expected Delivery Date: February 27, 2014
Class: Package Services
Service(s): Delivery Confirmation
Status: eNotification sent

An electronic copy of the shipping invoice can be downloaded from our website , in :
PDF format : http://www.canadapost.ca/cpotools/apps/track/personal/findInvoiceByTrackingNumber?session_id=7002101982901&trk=MW421330771CA&file_format=PDF
DOC format : http://www.canadapost.ca/cpotools/apps/track/personal/findInvoiceByTrackingNumber?session_id=7002101982901&trk=MW421330771CA&file_format=DOC

To check on the delivery status of your mailing or arrange redelivery please visit the following URL:
http://www.canadapost.ca/cpotools/apps/track/personal/findByTrackNumber?execution=e9s1

Thank you,
© 2014 Canada Post Corporation

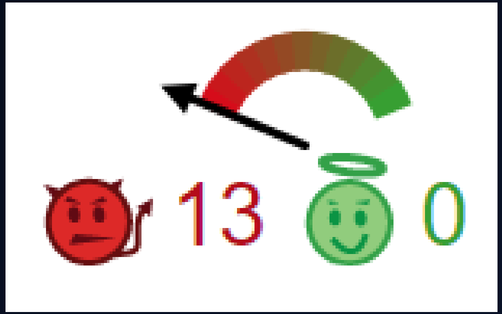
*** This is an automatically generated email, please do not reply ***

Shocking Phishing Emails

Mostly legitimate looking except for the subtle spelling mistake

Contained an “innocent looking” Word Document download which contained malware according to scans by VirusTotal

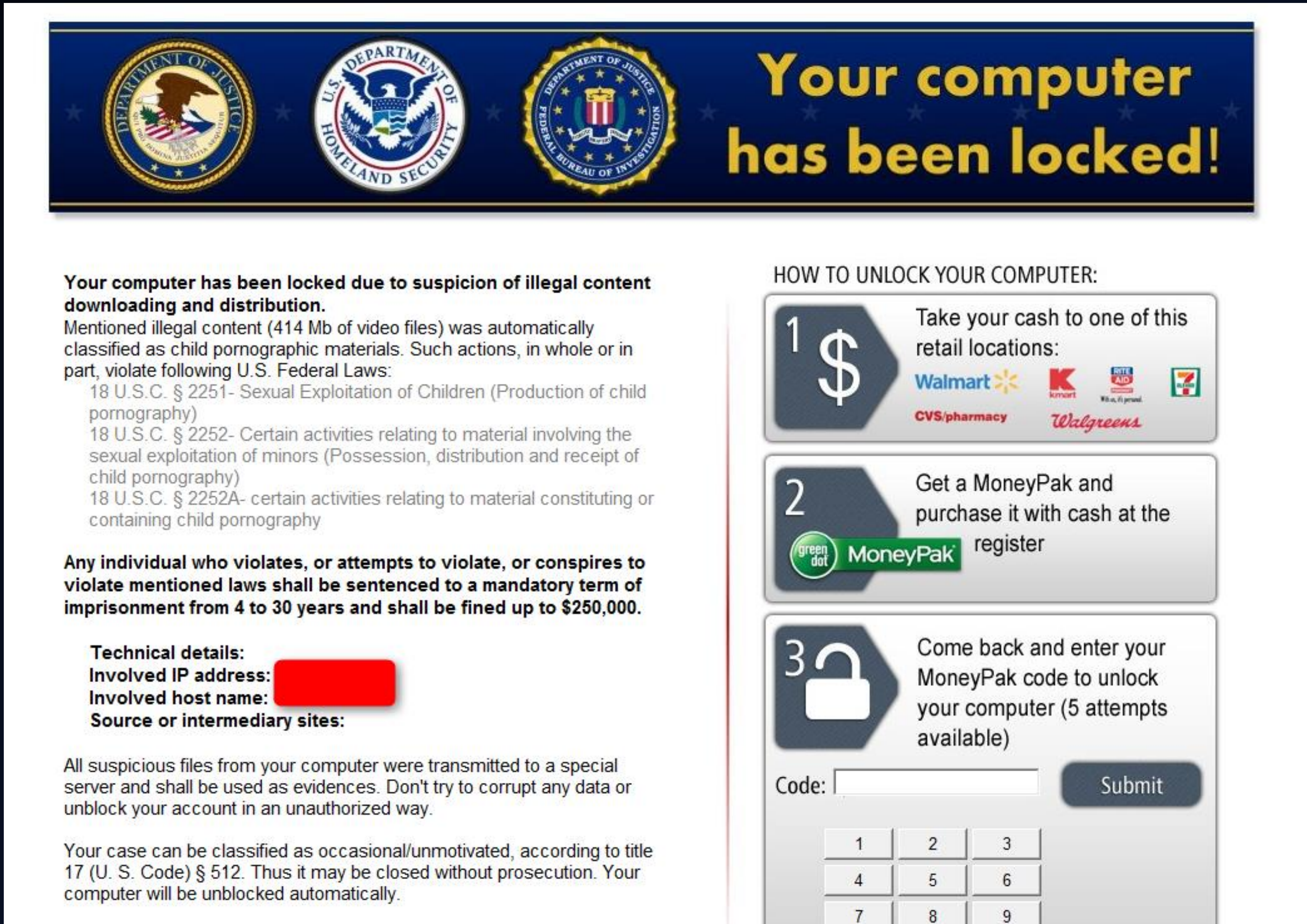
Detection Ratio : 37/54 (~68.5%)



Malware Evolution

Upgrades to existing malware:

- Kovter
- Phasebot
- Angler Exploit Kit



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code: Submit

References & Further Reading

Windows Environment

http://windows.microsoft.com/en-ca/windows-vista/what-is-the-registry
https://support.microsoft.com/en-us/kb/164787
https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977(v=vs.85).aspx

Poweliks

https://www.sophos.com/en-us/support/knowledgebase/121370.aspx
https://isc.sans.edu/forums/diary/Fileless+Malware/19619/
http://thisissecurity.net/2014/08/20/poweliks-command-line-confusion/
http://blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild/
https://www.linkedin.com/pulse/survey-file-less-malware-approach-using-javascript-ruwan-geeganage