

Security Community Service

Detektion von Code-Injection Angriffen

Datum: 06.06.2017

Klassifikation: TLP Grün

IOprotect GmbH Dürstelenstrasse 136 8335 Hittnau +41 (0)44 533 00 05 info@ioprotect.ch www.ioprotect.ch

### 1. Inhaltsverzeichnis

EIN	IFÜHRUNG	3
<u>1</u>	MONITORING USE CASE VIA GET-INJECTEDTHREAD	4
<u>2</u>	FALLBEISPIELE	5
2.1	WannaCry-Infektion	5
2.2	ReflectivePEInjection via PowerShell	8
2.3	PowerShell Empire	9
2.4	Metasploit Meterpreter	11
2.5	Ransomware mit Process Hollowing	12
<u>3</u>	BEMERKUNGEN	15

## Einführung

Indicator of Compromise (IOCs) sind derzeit in aller Munde. Mehr und mehr Firmen abonnieren IOC-Feeds, um mit der Menge an neu auftauchenden Malware-Samples Schritt halten und so infizierte Systeme rasch detektieren zu können. Aus Sicht von IOprotect haben IOCs durchaus ihren Wert, vor allem wenn es um Malware-Hunting im Unternehmen bei konkreten Fällen geht. Allerdings sind IOCs wenig nachhaltig. IOprotects bevorzugte Variante ist es vielmehr, den Modus Operandi der Angreifer zu verstehen und so nicht nach konkreter Malware zu suchen, sondern vielmehr deren auffälliges Verhalten zu detektieren. Das vorliegende Dokument soll genau ein solches Verhalten von Malware aufdecken: Code-Injection.

Im Dokument wird aufgezeigt, wie mit dieser Methode unterschiedlichste Formen von Angriffstools und Malware erkannt werden kann. Dies sind unter anderem folgende:

- PowerShell Empire
- Meterpreter via Migrate
- Process Hollowing
- WannaCry

# 1 Monitoring Use Case via Get-InjectedThread

Für die Umsetzung des Monitoring Use Cases wird ein PowerShell-Skript von Jared Atkinson (Get-InjectedThread.ps1) genutzt. Dieser Code stammt von der Präsentation "Taking Hunting to the Next Level: Hunting in Memory" gehalten von Jared Atkinson und Joe Desimone am SANS Threat Hunting Summit 2017. Der Quellcode ist unter folgendem Link zu finden: https://gist.github.com/jaredcatkinson/23905d34537ce4b5b1818c3e6405c1d2

Die Erklärung zum Skript<sup>1</sup>:



Abbildung 1: Erklärung zum PS-Skript

Mit dem Skript sollten damit klassische Code-Injection Techniken erkannt werden, auch wenn der Autor darauf hinweist, dass es keine Allheilmittel ist. Anhand von fünf Fallbeispielen wird die Effektivität des Monitoring Use Cases ermittelt:

- 1. WannaCry Ransomware
- 2. ReflectivePEInjection via PowerShell
- 3. PowerShell Empire
- 4. Metasploit Meterpreter
- 5. Ransomware mit EoP und Process Hollowing

4

<sup>&</sup>lt;sup>1</sup> https://www.youtube.com/watch?v=Hhpi3Sp4W4k

## 2 Fallbeispiele

### 2.1 WannaCry-Infektion

In diesem Fallbeispiel wurden zwei VMware-Systeme genutzt:

- Ein Zielsystem, auf welchem WannaCry ausgeführt wurde.
- Ein Logsystem, auf welchem das Skript Get-InjectedThread.ps1 via PS-Remoting und mit lokalen Administratorenrechten auf dem Zielsystem ausgeführt wurde. Die Ausführung erfolgte manuell und direkt mehrfach hintereinander.

Anbei sind zwei Printscreens des Setups aufgeführt:



Abbildung 2: Links das Zielsystem, rechts im Hintergrund das Logsystem



Abbildung 3: Das Logsystem ist im Vordergrund, mit dem auszuführenden PS-Remoting-Befehl

Unmittelbar nachdem die Malware auf dem Zielsystem lief, wurde der PS-Remoting-Befehle manuell und mehrfach hintereinander ausgeführt. Die Resultate sind automatisch in die Datei *out.txt* angefügt worden. Unten sind die Ergebnisse der ersten drei Läufe zu sehen:

ProcessName ProcessId Path KernelPath CommandLine PathMismatch ThreadId AllocatedMemoryProtection MemoryProtection MemoryType BasePriority IsUniqueThreadToken Integrity Privilege LogonId SecurityIdentifier UserName LogonSessionStartTime LogonType AuthenticationPackage BaseAddress Size Bytes PSComputerName RunspaceId	<pre>: tasksche.exe 2564 C:\ProgramData\dqhtorqn403\tasksche.exe C:\ProgramData\dqhtorqn403\tasksche.exe False 3360 PAGE_READWRITE PAGE_EXECUTE_READ MEM_COMMIT MEM_PRIVATE 8 False : : : : : : : : : : : : : : : : : : :</pre>
PupepacoId	• $9ch70c61-5fcd-4c0a-h7d7-168h21f88370$
kunspaceia	: 9CD/0001-51C0-4C0a-D/0/-108D211885/0
ProcessName	: tasksche.exe
ProcessId	: 2564
110000010	

© 2017, IOprotect GmbH, www.ioprotect.ch

Path KernelPath CommandLine PathMismatch ThreadId AllocatedMemoryProtection MemoryProtection MemoryState MemoryType BasePriority IsUniqueThreadToken Integrity Privilege	: ( : ( : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1 : 1	C:\ProgramData\dqhtorqn403\tasksche.exe C:\ProgramData\dqhtorqn403\tasksche.exe C:\ProgramData\dqhtorqn403\tasksche.exe False 2516 PAGE_READWRITE PAGE_EXECUTE_READ MEM_COMMIT MEM_PRIVATE 8 False
LogonId	:	
SecurityIdentifier	:	
UserName	:	
LogonSessionStartTime	:	
LogonType	:	
Recolddross	•	268453312
Size		12288
Bytes		{86, 139, 116, 36,}
PSComputerName	: :	172.16.57.200
RunspaceId	: !	9cb7ee61-5fcd-4c0a-b7d7-168b21f88370
ProcessName ProcessId Path KernelPath CommandLine	: f : 2 : (0 : (0 : (0	tasksche.exe 2564 C:\ProgramData\dqhtorqn403\tasksche.exe C:\ProgramData\dqhtorqn403\tasksche.exe C:\ProgramData\dqhtorqn403\tasksche.exe
PathMismatch	: 1	False
ThreadId	: 2	2176
AllocatedMemoryProtection	: 1	PAGE_READWRITE
MemoryProtection	: 1	PAGE_EXECUTE_READ
MemoryState	: 1	
MemoryType PacoPrioritu	: :	o PRIVATE
IsUniqueThreadToken	• •	v False
Integrity	•	
Privilege	:	
LogonId	:	
SecurityIdentifier	:	
UserName	: `	$\backslash$
LogonSessionStartTime	:	
LogonType	:	
AuthenticationPackage	:	
BaseAddress	: 2	268457776
Size	: 8	8192
Bytes	:	{83, 85, 86, 87}
PSComputerName	: :	172.16.57.200
RunspaceId	: !	9cb7ee61-5fcd-4c0a-b7d7-168b21f88370

Es wird immer derselbe Prozess angezeigt, aber die Aktionen von WannaCry oder zumindest einige davon sind via diesem Use Case detektierbar.

### 2.2 ReflectivePEInjection via PowerShell

Für das Fallbeispiel wird das Skript Invoke-ReflectivePEInjection.ps1<sup>2</sup> genommen. Dieses ermöglicht es einem Angreifer, eine ausführbare Datei in den PowerShell-Prozess zu laden. Das Skript wurde wie folgt ausgeführt:

```
$PEBytes = [IO.File]::ReadAllBytes('C:\Users\user\Desktop\mw.exe')
Invoke-ReflectivePEInjection -PEBytes $PEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -
ForceASLR
```

<pre>Windows PowerShell ISE (x86) File Edit View Debug Help File Edit</pre>		
File Edit View Debug Help Norke-ReflectivePEInjection.ps1 X EXAMPLE Load DemoEXE and run it locally. Forces ASLR on for the EXE. SPEBytes = [10.File]::ReadAllBytes('c:\users\user\Desktop\mw.exe') EXAMPLE RefectivePEInjection -PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -ForceASLR RefectivePI load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. SPEBytes = [10.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') Invoke-ReflectivePEInjection -PEBytes SPEBytes -ProcName lsass -ComputerName Target.Local NOTES PS C Content-Filter Test mit ausführbarem Programm. PS C: Content-Filter Test mit ausführbarem Programm. Content-Filter Test mit ausführbarem Programm. CitVindows\system32\cmd.exe CitVisers \user>tasklist i findstr mv.exe CitVisers \user Arg1 Arg3 Arg1 Arg2 Arg3 Arg1 Arg2 Arg3 Arg1 Arg2	Windows PowerShell ISE (x86)	
<pre>Invoke-ReflectivePEInjection.ps1 X Invoke-ReflectivePEInjection.ps1 X Invoke-ReflectivePEInjection.ps1 X Invoke-ReflectivePEInjection -PEBytes ASLR on for the EXE. SPEBytes = [10.File]::ReadAllBytes('c:\users\user\Desktop\mw.exe') Invoke-ReflectivePEInjection -PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -ForceASLR ReflectivePI load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. SPEBytes = [10.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') Invoke-ReflectivePEInjection -PEBytes SPEBytes -ProcName lsass -ComputerName Target.Local NOTES PS C 2013.IOprotect GmbH, www.ioprotect.ch Content-Filter Test mit ausführbarem Programm. PS CA Content-Filter Test mit ausführbarem Programm. Content-Filter Test mit ausführbarem Programm. Invoke-ReflectivePiceStasklist ! findstr mv.exe C:\Users\user&gt;tasklist ! findstr mv.exe C:\Users\user&gt;tasklist ! findstr powershell* provershell_ise exc 2588 Console 1 113.024 K E 113.024 K</pre>	File Edit View Debug Help	
Invoke-ReflectivePEInjection.ps1 X         9         .EXAMPLE         91         10.ad DemoEXE and run it locally. Forces ASLR on for the EXE.         35         36         37         38         39         10.ad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces ASLR on for the EXE.         39         11.cad DemoEXE and run it locally. Forces. and run it locally. Forces. and run it locally. The fore fore the fore the fore the fore the fore the fore the	1 🗠 🔒 🠇 🛍 🔉 🔍 🕫 🕨 🗈 🔳 😒 🖉	
<pre>ss .EXAMPLE load DemoEXE and run it locally. Forces ASLR on for the EXE. SPEBytes = [I0.File]::ReadAllBytes('c:\users\user\Desktop\mw.exe') Invoke-ReflectivePEInjection -PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -ForceASLR Refectively load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. SPEBytes = [I0.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') Invoke-ReflectivePEInjection -PEBytes SPEBytes -ProcName lsass -ComputerName Target.Local .NOTES P5 C 2013, IOprotect GmbH, www.ioprotect.ch PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 Content-Filter Test mit ausführbarem Programm. PS C:\ C CWindows\system32\cmd.exe C:\Users\user&gt;tasklist { findstr mw.exe C:\Users\user&gt;tasklist { findstr mu.exe C:\Users\user&gt;tasklist { findstr mu.exe C:\Users\user&gt;tasklist { findstr mu.exe C:\Users\user}tasklist { find</pre>	Invoke-ReflectivePEInjection.ps1 ×	۲
<pre>91 Load DemoEXE and run it locally. Forces ASLR on for the EXE. 92 SPEBytes = [I0.File]::ReadAllBytes('c:\users\user\Desktop\mw.exe') 1 Invoke-ReflectivePEInjection -PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -ForceASLR 95 .EXAMPLE 96 Refectively load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. 97 SPEBytes = [I0.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') 98 Invoke-ReflectivePEInjection -PEBytes SPEBytes -ProcName lsass -ComputerName Target.Local 100</pre>	89 .EXAMPLE	A
<pre>\$PEBytes = [I0.File]::ReadAllBytes('c:\users\user\Desktop\mw.exe') Invoke-ReflectivePEInjection -PEBytes \$PEBytes -ExeArgs "Arg1 Arg2 Arg3 Arg4" -ForceASLR .EXAMPLE  Refectively load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. \$PEBytes = [I0.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') Invoke-ReflectivePEInjection -PEBytes \$PEBytes -ProcName lsass -ComputerName Target.Local .NOTES  PS C Content-Filter Test mit ausführbarem Programm. PS C:\ Content-Filter Test mit ausführbarem Programm. C(Windows\system32\cmd.exe C:\Users\user&gt;tasklist : findstr mw.exe C:\Users\user&gt;tasklist : findstr mw.exe C:\Users\user&gt;tasklist : findstr mw.exe C:\Users\user&gt;tasklist : findstr mw.exe Divershell_ise.exe 2588 Console 1 113.624 K I I I 113.624 K I I I 113.624 K I I I I 113.624 K I I I I I I I I I I I I I I I I I I I</pre>	90 91 Load DemoEXE and run it locally. Forces ASLR on for	the EXE.
<pre>sign</pre>	92 <pre>\$PEBytes = [I0.File]::ReadAllBytes('c:\users\user\D</pre>	esktop\mw.exe')
<pre>stample stample s</pre>	93 Invoke-ReflectivePEInjection -PEBytes \$PEBytes -Exe	Args "Arg1 Arg2 Arg3 Arg4" -ForceASLR
<pre>96 97 Refectively load DemoDLL_RemoteProcess.dll in to the lsass process on a remote computer. 99 Jnvoke-ReflectivePEInjection -PEBytes \$PEBytes -ProcName lsass -ComputerName Target.Local 100 .NOTES P5 C © 2013, IOprotect GmbH, www.ioprotect.ch PEBytes \$PEBytes -ExeArgs "Arg1 Arg2 Arg3 P5 C C Content-Filter Test mit ausführbarem Programm. P5 C: Content-Filter Test mit ausführbarem Programm. P5 C: C C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr mw.exe 1 113,024 K 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>	95 .EXAMPLE	
<pre>97 Refectively load DemoDLL_RemoteProcess.dll in to the isass process on a remote computer. 98 SPEBytes = [I0.File]::ReadAllBytes('DemoDLL_RemoteProcess.dll') 99 Invoke-ReflectivePEInjection -PEBytes \$PEBytes -ProcName Isass -ComputerName Target.Local 100 .NOTES PS C © 2013, IOprotect GmbH, www.ioprotect.ch PEBytes \$PEBytes -ExeArgs "Arg1 Arg2 Arg3 Content-Filter Test mit ausführbarem Programm. PS C:\ Content-Filter Test mit ausführbarem Programm. PS C:\ OK C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K 1 113,024 K 1 113,024 K 1 113,024 K 1 113,024 K 1 1146 600 K</pre>	96	
<pre>99 Invoke-ReflectivePEInjection -PEBytes \$PEBytes -ProcName lsass -ComputerName Target.Local 100 101 .NOTES P5 C © 2013, IOprotect GmbH, www.ioprotect.ch PEBytes \$PEBytes -ExeArgs "Arg1 Arg2 Arg3 P5 C:\ Content-Filter Test mit ausführbarem Programm. P5 C:\ Content-Filter Test mit ausführbarem Programm. C:\Windows\system32\cmd.exe C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr powershell* powershell_ise.exe 2588 Console 1 113,624 K 1 1146 669 K </pre>	97 Refectively load DemoDLL_RemoteProcess.dll in to th 98 \$PEBytes = [IO.Fi]e]::ReadAllBytes('DemoDLL RemoteP	rocess.dll')
100       .NOTES         P5 C       © 2013, IOprotect GmbH, www.ioprotect.ch       PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3         Image: Content-Filter Test mit ausführbarem Programm.       PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3         P5 C:\//>        Content-Filter Test mit ausführbarem Programm.         P5 C:\///>        OK         Image: C:\Windows\system32\cmd.exe       Image: C:\// Image: C	99 Invoke-ReflectivePEInjection -PEBytes \$PEBytes -Pro	cName lsass -ComputerName Target.Local
PEBytes SPEBytes -ExeArgs "Arg1 Arg2 Arg3 PS C Content-Filter Test mit ausführbarem Programm. PS C:\ Content-Filter Test mit ausführbarem Programm. OK C:\Users\user>tasklist ! findstr mw.exe C:\Users\user>tasklist ! findstr mw.exe C:\Users\user>tasklist ! findstr mw.exe 1 113,624 K powershell_ise.exe 2588 Console 1 1146 660 K E	100 101 NOTES	
Prebytes spebytes -Exergs Argi Argi Argi Argi Argi Argi Argi Argi	DS C © 2012 IOnrotect GmbH years ionrotect ch	DEPutos (DEPutos Evoluses "Anol Anol Anol
Content-Filter Test mit ausführbarem Programm.		TEBYLES FEBYLES FERENIGS ANGLANGZ ANGS
Content-Filter Test mit ausführbarem Programm. Content-Filter Test mit ausführbarem Programm. OK OK C:\Windows\system32\cmd.exe C:\Users\user>tasklist ! findstr mw.exe C:\Users\user>tasklist ! findstr mw.exe C:\Users\user>tasklist ! findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K = 144,660 K		· · · · · · · · · · · · · · · · · · ·
PS C:\ OK OK C:\Windows\system32\cmd.exe C:\Users\user>tasklist   findstr mw.exe C:\Users\user>tasklist   findstr powershell* powershell_ise.exe 2588 Console 1 113,624 K = 1 113,624 K = 1 113,624 K = 1 113,624 K = 1 113,624 K = 1 113,624 K = 1 113,624 K = 	Content-Filter Test mit ausführbarem Programm.	
<pre>&gt; OK OK C:\Windows\system32\cmd.exe C:\Users\user&gt;tasklist ! findstr mw.exe C:\Users\user&gt;tasklist ! findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K powershell_ise.exe 1 144,600 K </pre>	PS C:\\	1
OK       C:\Windows\system32\cmd.exe       C:\Users\user>tasklist ! findstr mw.exe       C:\Users\user>tasklist ! findstr powershell*       powershell_ise.exe     2588 Console       1     113,024 K       powershell_ise.exe     144.600 K	>	
C:\Users\user>tasklist   findstr mw.exe C:\Users\user>tasklist   findstr mw.exe C:\Users\user>tasklist   findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K	ОК	
C:\Users\user>tasklist   findstr mw.exe C:\Users\user>tasklist   findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K rouweshell_ise.exe 9260 console 1 144,600 K	C:\Windows\system32\cmd.exe	
C:\Users\user>tasklist ¦ findstr mw.exe C:\Users\user>tasklist ¦ findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K powershell_ise.exe 2588 Console 1 144,600 K		
C:\Users\user>tasklist   findstr powershell* powershell_ise.exe 2588 Console 1 113,024 K powershell_ise.exe 9260 Console 1 144,600 K	C:\Users\user>tasklist ¦ findstr mw.exe	
powershell_ise_exe 2588 Console 1 113,024 K =	C:\Users\user>tasklist   findstr powershell*	
	powershell_ise.exe 2588 Console powershell_ise.exe 920 Console	1 113,024 K ≡ 1 144,600 K ≡

Abbildung 4: Die Datei mw.exe wird via Invoke-ReflectivePEInjection in den PowerShell-Prozess geladen

Ganz unten in der Abbildung ist zu sehen, dass kein Prozess mit dem Namen *mw.exe* existiert. Die PIDs der beiden laufenden PowerShell-Prozesse sind ebenfalls zu sehen.

 $<sup>^{2}\</sup> https://github.com/PowerShellMafia/PowerSploit/blob/master/CodeExecution/Invoke-ReflectivePEInjection.ps1$ 

Im zweiten PowerShell\_ISE.exe wird Get-InjectedThread.ps1 ausgeführt. Dabei zeigt sich folgendes Bild:



Abbildung 5: Das Skript Get-InjectedThread.ps1 identifiziert die Code-Injection in einem der beiden PowerShell\_ise.exe

Auch hier zeigt das Skript den richtigen Prozess an und detektiert somit diesen Angriff.

### 2.3 PowerShell Empire

In diesem Fallbeispiel wird PowerShell Empire<sup>3</sup> genutzt. Als erstes wird ein Agent auf dem Zielsystem ausgeführt, welcher eine Remote Verbindung zum Angreifer-System (Linux) aufbaut. Danach injiziert der Angreifer Code in den Isass.exe-Prozess und erhält dadurch einen zweiten Agenten.

<sup>&</sup>lt;sup>3</sup>https://www.powershellempire.com/

		ro	ot@Kali-Linux: /opt/Em	pire		(	•	6
File Edit View S	Search Terminal	Help						
cmd	2204 ×64	Wir	764bit\Admin 2.67 MB					
cmd msdtc	2216 x64 2228 x64	Wir NT TWO	764bit\user 2.86 MB AUTHORITY\NE 7.88 MB DRK SERVICE					
conhost SearchProtocolH ost	2352 x64 2392 x64	Wir NT	AUTHORITY\SY 7.85 MB					
PresentationFon	2552 x64	NT	AUTHORITY\LO 18.91 MB					
taskhost dwm explorer	2692 x64 2744 x64 2756 x64	Wir Wir Wir	1764bit\user 13.27 MB 1764bit\user 5.45 MB 1764bit\user 52.16 MB					
SearchFilterHos +	2824 x64	NT	AUTHORITY\SY 5.78 MB					
vmtoolsd powershell	2876 x64 2900 x64	Wir Wir Use	764bit\user 26.91 MB 764bit\Admin 60.52 MB					
SearchIndexer	3060 x64	NT STE	AUTHORITY\SY 18.62 MB					
(Empire: SCH3XXWZW22 (Empire: management, (Empire: management, Job started: Debug32 [+] Initial agent H)	CTDS2C) > psinjec (psinject) > exec (psinject) > 2 qv2uj (2LKUR4DGRNCNSL 1	t test 520 ute rom 172.16.57.2	200 now active					
(Empire: management/	<pre>/psinject) &gt; ager</pre>	its						
[*] Active agents:								
Name	Internal IP	Machine Name	Username	Process	Delay	Last Seen		
SCH3XXWZW2ZTDS2C HX2LKUR4DGRNCNSL	172.16.57.200 172.16.57.200	WIN764BIT WIN764BIT	*Win764bit\AdminUse *WORKGROUP\SYSTEM	rpowershell/2900 lsass/520	5/0.0 5/0.0	2017-05-19 2017-05-19	15:50:1 15:50:1	.8 9

Abbildung 6: Angreifer verfügt über zwei Agenten, wobei der zweite via lsass.exe ausgeführt wurde

Lässt man Get-InjectedThread.ps1 auf dem Zielsystem ausführen, zeigt sich folgendes Bild:

Applications -	Places 🔻	Terminal	-	Fri 15:52					
			roe	ot@Kali-Linux: /opt/E	mpire	Recycle Bin	procexo64	Get-Injecte	mw
File Edit	View S	earch Terminal	Help						
dwm		2744 x64	Win	764bit\user 5.45 MB	n		Eile Eile	ninistrator: Windows Edit View Debug	PowerShell ISE
SearchFilter	Hos	2756 X64 2824 X64	NT	AUTHORITY\SY 5.78 MB	ь		1 6		
vmtoolsd		2876 x64	Win	764bit\user 26.91 M	B	PowerSyringe	Until	Had1 pr1 Gat-Injac	rtadThread pr1 X
powershett		2900 X04	Use	AUTHORITY CV 10 C2 M	ь р		1	function Get-In	njectedThread
Searchindexe		3060 X64	STE	M	5		2	{	
(Empire: SCH (Empire: man (Empire: man	3XXWZW2Z agement/ agement/	TDS2C) > psinje psinject) > exe psinject) >	ct test 520 cute			WPCape	PS (	:\Windows\syste	em32> C:\Users\user\Desktop\Get-InjectedThread.ps1
[+] Initial a	agent HX	_qv2u] 2LKUR4DGRNCNSL	from 172.16.57.2	00 now active			Pro	essName	: lsass.exe
(Empire: mana	agement/	psinject) > age	nts				Pro	cessid	: 520 : C:\Windows\system32\lsass.exe
[*] Active a	gents:						Com	nandLine	: C:\Windows\System32\Isass.exe : C:\Windows\system32\lsass.exe
Name		Internal IP	Machine Name	Username	Process	Windows TShell	Path Three	Mismatch eadId catedMemoryProt	: False : 616 
SCH3XXWZW2	ZTDS2C	172.16.57.200	WIN764BIT WIN764BIT	*Win764bit\AdminUs *WORKGROUP\SYSTEM	erpowershel	ι,	Memo	oryProtection pryState	: PAGE_EXECUTE_READWRITE : MEM_COMMIT
(Empire: age	nts) > k	ill SCH3XXWZW2Z	rds2c				Memo Base	pryType Priority	: MEM_PRIVATE : 9
(Empire: age	nts) > [	!] Agent SCH3XX	vzwzziDS2C exiti				Inte	egrity	i Faise
(Empire: age	nts) > (	ıst					Logo	onId	
[*] Active a	gents:						User	Name	1
Name		Internal IP	Machine Name	Username	Process		Logo	onSessionStartTi onType	ime :
HX2LKUR4DG	RNCNSL	172.16.57.200	WIN764BIT	*WORKGROUP\SYSTEM	lsass/520		Auth	nenticationPacka Address	age : : 917504
(Empire: age	nts) >						Size	2	: 4096
							Inc. cz	Mindowel evetore	21×
							Comp	leted	
						1			

Abbildung 7: Der Isass.exe Prozess wird richtig identifiziert

Auch hier wird der entsprechende Prozess detektiert.

### 2.4 Metasploit Meterpreter

Meterpreter ist Teil des Metasploit Frameworks und ein sehr beliebtes Modul, um ein infiziertes Client-System via System unter Kontrolle des Angreifers fernzusteuern. Meterpreter ist ein Remote Administrations Tool und dient auch als Post Exploitation Framework. So lässt sich beispielsweise auch Mimikatz nachladen und via Meterpreter ausführen. Im Bild unten ist eine Meterpreter-Verbindung via Port 80 zu sehen. Der Angreifer kann damit Befehle mit den Rechten des eingeloggten Benutzers ausführen:

<pre>Imsf exploit(handler) &gt; run</pre>	
[*] Started HTTP reverse handler on http://	
[*] Starting the payload handler [*] http://9 80 handling request from 8; (UUID: hsxc	4yl5) Redirecting stageless cor
q1bWtu83wRcL_OphroH97cPmBNXTyaLWYCS0EepKsbF_R2ZgxrGv3BmSU1W8xTVGfiEw99Jkhic-       [*] http://9     80 handling request from     8; (UUID: hsxc	a8 with UA 'Mozilla/5.0 (Window 4yl5) Attaching orphaned/stagel
[*] Meterpreter session 3 opened ( 80 -> 80 -> 8:12362) a	t 2017-05-23 13:50:18 +0200
meterpreter > getuid	
Server username: Win764bit\AdminUser meterpreter >	

Abbildung 8: Angreifer erhält eine Remote Administrations Verbindung zu einem Windows-System via Meterpreter

meter	preter	> ps				
Proce	ss List					
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
216	504	TPAutoConnSvc.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\T
248	772	audiodg.exe	x64	0		
276	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
360	352	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
392	2228	powershell_ise.exe	x64	1	Win764bit\AdminUser	C:\Windows\system32\WindowsPowerShell\
400	352	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
412	392	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
468	392	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
504	400	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
512	400	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
520	400	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
576	624	WmiPrvSE.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe

In diesem Beispiel werden alle Prozesse auf dem Windows Client angezeigt sowie deren User:

Abbildung 9: Anzeigen aller laufenden Prozesse

Damit bestimmte Post Exploitation Module wie Mimikatz etc. ausgeführt werden können, muss der Angreifer zuerst in einen anderen Prozess migrieren, welcher SYSTEM Privilegien aufweist. Dazu benötigt er Administratorenrechte. Im Bild unten wurde in den Prozess 360 (csrss.exe) migriert und anschliessend Get-InjectedThread.ps1 mit Administratorenrechten ausgeführt.



#### Abbildung 10: Migration in einen Prozess via Meterpreter; detektiert mit Get-InjectedThread.ps1

Der betroffene Prozess wird ebenfalls erkannt.

### 2.5 Ransomware mit Process Hollowing

Beim Process Hollowing startet die Malware einen legitimen Prozess, jedoch erst einmal im Suspended Mode. Beispiele für genutzte Prozesse sind explorer.exe oder lsass.exe. Bevor jedoch der erste Thread dieses Programms ausgeführt wird, ersetzt die Malware den ursprünglichen Code des legitimen Prozesses durch den Code der Malware selbst. Die Informationen im Process Environment Block (PEB) und den Dateiangaben zeigen jedoch auf die legitime Datei auf der Disk. Die groben Schritte des Angriffs sind wie folgt:

- 1. Start einer neuen Instanz von, z.B. explorer.exe, mit dem ersten Thread im Suspended Mode.
- 2. Die Datei Malware.exe öffnen und deren Inhalt in einen Buffer kopieren.
- 3. Speicherbereich des legitimen Prozesses freigeben. Die DLLs, die Heaps bleiben alloziert, File-Handles etc. offen.
- 4. Neues Speichersegment in explorer.exe allozieren. Dieser Bereich muss RWX Berechtigungen haben.
- 5. Kopieren des PE-Headers von malware.exe in den neu allozierten Speicherbereich in explorer.exe.
- 6. Kopieren jeder PE-Section des malware.exe-Prozesses in den explorer.exe-Prozess.
- 7. Startadresse des ersten Threads von explorer.exe an die AddressOfEntryPoint-Adresse des maliziösen Prozesses (malware.exe) setzen.
- 8. Thread aus dem Suspended Mode holen (Resume Thread).

Im Fallbeispiel wird folgende Datei verwendet:

	ustotal										
SHA256:	eb855e1f9ca899d48215975c86b65943c37d02c87c70515f31d75b589fee641d										
File name:	: sys.olk										
Detection ratio	Detection ratio: 51 / 62										
Analysis date:	Analysis date: 2017-04-05 13:00:14 UTC (1 month, 2 weeks ago)										
Analysis	, File detail 🚯 Additional information 🗩 Comments 😰 🤤 Votes 🔚 Behavioural information										
Antivirus	Result	Update									
Ad-Aware	Trojan.GenericKD.4422170	20170405									
AegisLab	Uds.Dangerousobject.Multilc	20170405									
AhnLab-V3	Trojan/Win32.Agent.C1780098	20170405									
ALYac	Trojan.GenericKD.4422170	20170405									
Arcabit	Trojan.Generic.D437A1A	20170405									
Avast	Win32:Malware-gen	20170405									

Abbildung 11: Ausgabe von VirusTotal zum Malware-Sample

© 2017, IOprotect GmbH, www.ioprotect.ch

Lässt man diese Datei auf einem nicht gepatchten Windows 7 System laufen, erscheint nach ein paar Sekunden ein explorer-exe-Prozess, welcher unter NT AUTHORITY\SYSTEM läuft. Diese Malware enthält damit auch einen Privilege Escalation Exploit, der im November 2016 gepatcht wurde.

an minogoritato		1,700 1	0,2071	400 NT //011010111 /0101EM	oyacom			
🖃 🔚 explorer.exe	0.07	29,676 K	48,556 K	2076 user-PC\user	Medium			
vm vmtoolsd.exe	0.12	11,824 K	18,604 K	2184 user-PC\user	Medium			
powershell_ise.exe	< 0.01	90,976 K	84,928 K	4024 user-PC\AdminUser	High			
css. cmd.exe		1,792 K	2,312 K	2020 user-PC\user	Medium			
💭 procexp.exe	1.26	10,232 K	20,164 K	1024 user-PC`\AdminUser	High			
explorer.exe	0.44	22,392 K	9,712	3804 NT AUTHORITY\SYSTEM	System			
			~					
						*		
< <u> </u>								
CPU Usage: 4.64% Commit Charge: 16.49% Processes: 55 Physical Usage: 35.21%								

Abbildung 12: Die Schadsoftware führt via Privilege Escalation Exploit eine neue Instanz von explorer.exe als SYSTEM aus

Lässt man wiederum Get-InjectedThread.ps1 mit erhöhten Rechten ausführen, wird der betroffene Prozess detektiert:

Authinistrator. Windows Powerone	Process Explorer - Sysinternals: www.sysinternals.com [user-PC\AdminUser]					
File Edit View Debug Help	File Options View Process Find Users Help					
1 🗀 🔒 🐇 🖻 🔈 🗐		× 4	•			
		Process	CPU	Private Bytes	Working Set	PID User Name
Untitled1.ps1 Get-InjectedThrea	o.psi A	svchost.exe		1,084 K	3,768 K	1904 NT AUTHORITY\LOCAL SERV
2276 Get-InjectedIhread		svchost.exe		1,268 K	4,292 K	1944 NT AUTHORITY\NETWORK S
22//		taskhost.exe	0.01	10,184 K	9,700 K	1860 user-PC\user
2279		SearchIndexer.exe	0.01	18,784 K	13,076 K	2412 NT AUTHORITY\SYSTEM
		SearchProtocolHost.e	< 0.01	2,108 K	6,208 K	2608 NT AUTHORITY\SYSTEM
PS C:\Windows\system32> C:	\Users\user\Desktop\Get-I	SearchFilterHost.exe		1,100 K	4,176 K	2900 NT AUTHORITY\SYSTEM
		(∑∋ msdtc.exe	0.01	2,512 K	6,504 K	2692 NT AUTHORITY\NETWORK S
Received Name		sppsvc.exe		2,292 K	7,848 K	2980 NT AUTHORITY\NETWORK S
ProcessName	. 2804	📇 msiexec.exe		6,284 K	11,984 K	3364 NT AUTHORITY\SYSTEM
Path	: C:\Windows\explorer exe	svchost.exe		1,120 K	4,000 K	3404 NT AUTHORITY\SYSTEM
KernelPath	: C:\Windows\explorer.exe	Presentation FontCache.e		14.056 K	11,752 K	2104 NT AUTHORITY\LOCAL SERV
CommandLine	: "C:\Windows\explorer.ex	EMET Service.exe		11,036 K	15,788 K	3312 NT AUTHORITY\SYSTEM
PathMismatch	: False	EMET_Agent.exe	0.03	27,744 K	44,496 K	3432 user-PC\user
ThreadId	: 3816	svchost.exe		48,440 K	54,224 K	808 NT AUTHORITY\SYSTEM
AllocatedMemoryProtection	: PAGE_EXECUTE_READWRITE	wmpnetwk.exe		8.312 K	21.052 K	3436 NT AUTHORITY\NETWORK S
MemoryProtection	: PAGE_EXECUTE_READWRITE	WmiAp Srv.exe	0.02	1,160 K	4,536 K	3976 NT AUTHORITY\SYSTEM
MemoryType	· MEM_COMMIT	TrustedInstaller.exe		2.388 K	7.004 K	2232 NT AUTHORITY\SYSTEM
BasePriority	: 8	dlhost.exe	0.01	2.904 K	8.620 K	2676 NT AUTHORITY\SYSTEM
IsUniqueThreadToken	: False	Isass.exe		2,848 K	7,920 K	508 NT AUTHORITY\SYSTEM
Integrity	:	sm.exe		1,220 K	3,104 K	516 NT AUTHORITY\SYSTEM
Privilege	:	E CSrss.exe	0.35	4,740 K	7,008 K	400 NT AUTHORITY\SYSTEM
LogonId	:	conhost.exe		916 K	4,996 K	872 user-PC\AdminUser
SecurityIdentifier		conhost.exe		948 K	5,056 K	1804 user-PC\user
LogonSessionStartTime	: `	🕼 winlogon.exe		1,664 K	5,272 K	436 NT AUTHORITY\SYSTEM
LogonType	-	E explorer.exe	0.08	29,608 K	48,544 K	2076 user-PC\user
AuthenticationPackage	:	vm vmtoolsd.exe	0.12	11.824 K	18.608 K	2184 user-PC\user
BaseAddress	: 5408512	powershell ise.exe	< 0.01	96,364 K	88,244 K	4024 user-PC\AdminUser
Size	: 704512	cmd.exe		1,792 K	2,312 K	2020 user-PC\user
Bytes	: {85, 139, 236, 106}	Drocexp.exe	2.11	10,228 K	20,420 K	1024 user-PC\AdminUser
		explorer.exe	< 0.01	22,408 K	9,728 K	3804 NT AUTHORITY\SYSTEM

#### Abbildung 13: Der betroffene Prozess wird durch den Monitoring Use Case detektiert

Interessante Beobachtung: Ein paar Monate später wurde dieselbe Malware wieder ausgeführt und anschliessend via Process Explorer und Virustotal-Anbindung untersucht. Jedoch wird mit diesem Vorgehen der maliziöse Prozess nicht erkannt.

© 2017, IOprotect GmbH, www.ioprotect.ch

File       Options       View       Process       Find       U.U. Users       Help         Process       CPU       Provate Byte       Visionig Ser       PID       Like View       Cetter       Visionig Ser       PiD       Like View       Cetter       Cetter       Pidendia       Cetter	🍣 Process Explore	er - Sysinternals: w	ww.sysinterna	ls.com [Win764	4bit\AdminUse	r]				a x
Image       CPU       Process       CPU       Provide Stee       Plot Leer Name       Image       Integrity       Vus Total       Verified Styrer       Automation         Process       CPU       Provide Stee       0.44       0.2       0.4       0.5       0.4<	File Options Vi	ew Process Fi	nd DLL Us	ers Help						
Norma         Description         Company Name         Path         VestRes         Outside         VestRes         Outside         VestRes         VestRes         Outside         VestRes		n 🥅 🏘 🛃	🗙 👪 🚳	1						
Name         0.44         0 K         0/k         0/k </td <td>Process</td> <td></td> <td>CPU</td> <td>Private Bytes</td> <td>Working Set</td> <td>PID User Name</td> <td>Image Integrity</td> <td>VirusTot</td> <td>al Verified Signer</td> <td>*</td>	Process		CPU	Private Bytes	Working Set	PID User Name	Image Integrity	VirusTot	al Verified Signer	*
■ mase ace         372 kl         1.036 kl         276 ht TAUTHORITY-SYSTEM         64-bt System         0_{0.11}         (Verfied) Monosch           ■ minist ace         1.220 kl         4.076 kl         300 ht TAUTHORITY-SYSTEM         64-bt System         0_{0.51}         (Verfied) Monosch           ■ minist ace         0.02         3.668 kl         100 ht TAUTHORITY-SYSTEM         64-bt System         0_{0.51}         (Verfied) Monosch           ■ minist ace         0.01         2.212 kl         3.664 kl         420 kl         X2 ht TAUTHORITY-SYSTEM         64-bt System         0_{0.51}         (Verfied) Monosch           ■ control exe         0.01         2.212 kl         3.664 kl         420 kl XL TAUTHORITY-SYSTEM         64-bt System         0_{0.52}         (Verfied) Monosch           ■ control exe         0.41         7.866 kl         2.000 kl XL TAUTHORITY-SYSTEM         64-bt System         0_{0.52}         (Verfied) Monosch           ■ windoprice exe         0.05         31.376 kl XL 2200 kl XL TAUTHORITY-SYSTEM         64-bt Medum         0_{0.51}         (Verfied) Monosch           ■ windoprice exe         0.14         10.864 kl S200 kl TAUTHORITY-SYSTEM         64-bt Medum         0_{0.51}         (Verfied) Monosch           ■ windoprice exe         0.05         31.376 kl S2652 kl 2000 kl TAUT	Interrupts		0.44	0 K	0 K	n/a	64-bit			
Image: Source         1.220 K         4.076 K         350 NT AUTHORITY-SYSTEM         64-bit System         0_011         (Verfied) Microsoft           Image: Sources ave         0.12 X         4.065 K         4.006 K         4.065 K         4.065 K         4.076 K         4.0	smss.exe			372 K	1,036 K	276 NT AUTHORITY\SYSTEM	64-bit System	0/61	(Verified) Microsoft	
■         ■         1.320 K         4.086 K         4.00 NT AUTHORITY's YSTEM         64-bit System         0./£1         (Verfied) Morosoft           ■         ■         ■         ■         ■         ■         ■         ●	CSISS.exe			1,820 K	4,076 K	360 NT AUTHORITY\SYSTEM	64-bit System	0/61	(Verified) Microsoft	
Bit envices exe         0.61         (Verfied) Microsoft           Bit envices exe         0.02         3.688 K         4.824 K         4.82	🖃 🔳 wininit.exe			1,320 K	4,068 K	400 NT AUTHORITY\SYSTEM	64-bit System	0/61	(Verified) Microsoft	
Line Researce         0.02         3.665 K         10.268 K         448 HT AUTHORITY SYSTEM         64bb System         0.61         Verified Microsoft           Image: Control exe         0.14         7.958 K         9.12 K         412 NT AUTHORITY SYSTEM         64bb System         0.61         (Verified) Microsoft           Image: Control exe         0.14         7.958 K         9.12 K         412 NT AUTHORITY SYSTEM         64bb System         0.051         (Verified) Microsoft           Image: Control exe         0.05         3.1376 K         52.052 K         200 Win764hr Luser         64bb Modum         0.051         (Verified) Microsoft           Image: Control exe         0.05         3.1376 K         52.652 K         200 Win764hr Luser         64bb Modum         0.251         (Verified) Microsoft           Image: Control exe         0.05         3.1376 K         22.02 K         123 Win764hr Luser         64bb Modum         0.251         (Verified) Microsoft           Image: Control exe         0.14         10.884 K         2.320 K         304 Win764hr Luser         64bb Modum         0.252         (Verified) Microsoft           Image: Control exe         0.14         10.884 K         2.320 K         123 Win764br Luser         32bb System         0.252         (Verified) Microsoft <td>+ services.ex</td> <td>e</td> <td></td> <td>4,824 K</td> <td>8,024 K</td> <td>476 NT AUTHORITY\SYSTEM</td> <td>64-bit System</td> <td>0/61</td> <td>(Verified) Microsoft</td> <td></td>	+ services.ex	e		4,824 K	8,024 K	476 NT AUTHORITY\SYSTEM	64-bit System	0/61	(Verified) Microsoft	
Immune         0.01         2.212 K         3.364 K         492 KT AUTHORITYSYSTEM         64-bb System         0./28         (Verfied) Microsoft           Immonia         0.14         7,958 K         9,132 K         412 KT AUTHORITYSYSTEM         64-bb System         0.51         (Verfied) Microsoft           Immonia         0.14         7,958 K         9,132 K         62,450 K         900 W7/644 user         64-bb System         0.51         (Verfied) Microsoft           Immonia         0.14         7,958 K         2,200 K         200 W7/644 user         64-bb System         0.51         (Verfied) Microsoft           Immonia         0.25         7,736 K         17,456 K         2120 W7/644 user         64-bb Medum         0.52         (Verfied) Microsoft           Immonia         0.25         7,736 K         17,456 K         2120 W7/644 user         64-bb Medum         0.51         (Verfied) Microsoft           Immonia         0.14         10.364 K         23.207 K         124 W7/644 user         64-bb Medum         0.51         (Verfied) Microsoft           Immonia         0.14         10.364 K         23.207 K         128 W7/644 user         32.20 K         With With Verfiel User         32.20 K           Immonia         0.14         10.75	sass.exe		0.02	3,668 K	10,268 K	484 NT AUTHORITY\SYSTEM	64-bit System	<u>0/61</u>	(Verified) Microsoft	
Image: Series exe control exe contr	sm.exe		0.01	2,212 K	3,964 K	492 NT AUTHORITY\SYSTEM	64-bit System	0/58	(Verified) Microsoft	
Security State         964 K         2.900 K         820 Win764bruser         64-bit Medum         0/51         (Verfied) Microsoft                windogon.exe         0.05         31,976 K         52,622 K         200 Win764bruser         64-bit Medum         0/51         (Verfied) Microsoft                windogon.exe         0.25         7,736 K         17,456 K         2120 Win764bruser         64-bit Medum         0/51         (Verfied) Microsoft                windogon.exe         0.14         10,864 K         22,300 K         128 Win764bruser         64-bit Medum         0/51         (Verfied) Microsoft                windogon.exe         0.14         10,864 K         22,300 K         128 Win764bruser         64-bit Medum         0/51         (Verfied) Microsoft                windogon.exe         0.14         10,864 K         22,300 K         228 Win764bruser         64-bit Medum         0/52         (Verfied) Microsoft                windogon.exe         0.14         10,864 K         22,300 K         228 Win764bruser         64-bit Medum         0/52         (Verfied) Microsoft                windogon.exe         0.14         10,864 K         22,300 K         228 Win764bruser         62-bit Medum         0/52         (Verfied) Microsoft	- CSrss.exe		0.14	7,968 K	9,132 K	412 NT AUTHORITY\SYSTEM	64-bit System	0/61	(Verified) Microsoft	
2.400 K       6.436 K       504 NT AUTHORITY/SYSTEM       64-bit Medum       0.25       (Verified) Microsoft       □         □       exclorer exe       0.25       7.736 K       17.456 K       2120 Win 76-bit user       64-bit Medum       0.51       (Verified) Microsoft       □         □       exclorer exe       0.25       7.736 K       17.456 K       2120 Win 76-bit user       64-bit Medum       0.51       (Verified) Microsoft       □         □       exclorer exe       0.14       10.86 K       25.320 K       128 Win 76-bit user       64-bit Medum       0.51       (Verified) Microsoft       □       0.14       10.86 K       25.320 Kit 128 Win 76-bit user       64-bit Medum       0.52       (Verified) Microsoft       □       0.14       10.86 K       25.320 Kit 128 Win 76-bit user       32-bit Low       0.52       (Verified) Microsoft       □       0.16 Hitting       0.16 Hitting<	conhost.ex	e		964 K	2,900 K	920 Win764bit\user	64-bit Medium	0/61	(Verified) Microsoft	-
Image: Second reference       0.05       31.976 K       52.652 K       2004 Win 756bt User       64-bit Medum       0.611       (Verified) Microsoft         Image: Second Se	winlogon.exe			2,400 K	6,496 K	504 NT AUTHORITY\SYSTEM	64-bit System	0/59	(Verified) Microsoft	=
Image         0.25         7.78 k         17.46 k         2120 Wn764b1 vser         64 bt Meduum         0.752         Verfield / Mircred /	= axplorer.exe		0.05	31,976 K	52,652 K	2004 Win764bit\user	64-bit Medium	0/61	(Verified) Microsoft	
Procesp64.exe       2.11       20.18 K       32.920 K       3044 Win764bit/\admin.lber       64-bit High       0.759       (Verified) Microsoft                imagione exe imagione exe	vm vmtoolsd.ex	xe	0.25	7,736 K	17,456 K	2120 Win764bit\user	64-bit Medium	0/57	(Verified) VMware	
<ul> <li></li></ul>	procexp64.	exe	2.11	20,184 K	32,920 K	3044 Win 764bit \Admin User	64-bit High	0/59	(Verified) Microsoft	
Bigsplore.exe         19,972 K         29,072 K         2832 Win764bit user         32-bit Low         0/62         (Verfied) Microsoft           Windows         23,748 K         11,756 K         2088 NT AUTHORITY/SYSTEM         32-bit System         0/60         (Verfied) Microsoft         v           Name         Description         Company Name         Path         Verfied Signer         *           Amme         Description         Company Name         Path         0/25         (Verfied) Microsoft         *           Amme         Description         Company Name         Path         Verfied Signer         *           dirpcsvc6 dil         DHCPV Glent         Microsoft Coporation         C:Windows/SysWOW64/secur32.dll         0/22         (Verfied) Microsoft         #           colarla         Netrosoft Coporation         C:Windows/SysWOW64/secur32.dll         0/22         (Verfied) Microsoft         #           colarla         Netrosoft Coporation         C:Windows/SysWOW64/secur32.dll         0/22         (Verfied) Microsoft         #           colarla         Nicrosoft Coporation         C:Windows/SysWOW64/secur32.dll         0/22         (Verfied) Microsoft         #           colarla         Microsoft GDI+         Microsoft Coporation         C:Windows/SysWOW64/se	iexplore.exe	в	0.14	10,864 K	26,320 K	128 Win 764bit \user	64-bit Medium	0/61	(Verified) Microsoft	
Register exe         23.748 K         11.756 K         2088 NT AUTHORITY/SYSTEM         32/bit         System         0/60         (Verified) Microsoft           Name         Description         Company Name         Path         Vina Total         Verified Signer         ////////////////////////////////////		.exe		19.972 K	29.072 K	2832 Win764bit\user	32-bit Low	0/62	(Verified) Microsoft	
Name         Description         Company Name         Path         Visua Total         Verified Signer           Mame         Security Support Provider Interface         Microsoft Corporation         C:Windows/SysWOW64\secur32.dll         0.226         (Verified) Microsoftdll         #           Inagai dll         Nicrosoft Desktop Window Manag         Microsoft Corporation         C:Windows/SysWOW64\dwmapi.dll         0.227         (Verified) Microsoftdll)         #           Inagai dll         Nicrosoft Desktop Window Manag         Microsoft Corporation         C:Windows/SysWOW64\dwmapi.dll         0.227         (Verified) Microsoftdll)         # <td>explorer exe</td> <td></td> <td></td> <td>23.748 K</td> <td>11,756 K</td> <td>2088 NT AUTHORITY\SYSTEM</td> <td>32-bit System</td> <td>0/60</td> <td>(Verified) Microsoft</td> <td></td>	explorer exe			23.748 K	11,756 K	2088 NT AUTHORITY\SYSTEM	32-bit System	0/60	(Verified) Microsoft	
Name         Description         Company Name         Path         Vinus Total         Verified Signer           Name         Description         Company Name         Path         Vinus Total         Verified Signer         A           secur32.dll         Security Support Provider Interface         Microsoft Corporation         C:\Windows\SysWOW64\secur32.dll         0/22         (Verified) Microsof         E           dhopcsvc6.dll         DHCPv6 Client         Microsoft Corporation         C:\Windows\SysWOW64\dwmapi.dll         0/22         (Verified) Microsof         E           Iocale nls         Microsoft Desktop Window Mang         Microsoft Corporation         C:\Windows\SysWOW64\dwmapi.dll         0/22         (Verified) Microsof         E           SotDefault nls         0/266         (Verified) Microsof         C:\Windows\SysWOW64\dwmapi.dll         0/227         (Verified) Microsof           SotDefault nls         0/256         (Verified) Microsoft         C:\Windows\SysWOW64\secur32.dll         0/259         (Verified) Microsof           GdiPlus.dll         Microsoft GDI+         Microsoft Corporation         C:\Windows\SysWOW64\secur32.dll         0/259         (Verified) Microsof           sepicit.dll         Security Support Provider Interface         Microsoft Corporation         C:\Windows\SysWOW64\secur32.dll         <									(	_
Name         Description         Company Name         Path         Virus Total         Verified Signer         A           secur32.dll         Security Support Provider Interface         Microsoft Corporation         C:\Windows\SysWOW64\secur32.dll         0/22         (Verified) Microsoft         et/diamatrix         <										*
secur32.dll         Securty Support Provider Interface         Microsoft Corporation         C:\Windows\SysWOW64\secur32.dll         Q.22         (Verified) Microsof           dhopcsvc6.dll         DHCPv6 Client         Microsoft Corporation         C:\Windows\SysWOW64\dmap; dll         Q.227         (Verified) Microsof           nlaapi.dll         Microsoft Desktop Window Mang         Microsoft Corporation         C:\Windows\SysWOW64\dmap; dll         Q.227         (Verified) Microsof           locale nls         Microsoft Corporation         C:\Windows\SysWOW64\dmap; dll         Q.227         (Verified) Microsof           SotDefault nls         C:\Windows\SysWOW64\dmap; dll         Q.227         (Verified) Microsof           ceale nls         C:\Windows\SysWOW64\dmap; dll         Q.255         (Verified) Microsof           SotDefault nls         C:\Windows\SysWOW64\verified; Microsoft.         C:\Windows\SysWOW64\verified; Microsoft           GdiPlus.dll         Microsoft Corporation         C:\Windows\SysWOW64\verified; Microsoft         Q/58         (Verified) Microsof           seciol.dll         Host for SCM:SDDL/LSA Lookup         Microsoft Corporation         C:\Windows\SysWOW64\verified; Microsof         Q/59         (Verified) Microsof           sepicil.dll         Intersoft for poration         C:\Windows\SysWOW64\verified; Microsof         Q/59	Name	Description		Company N	lame	Path		VirusTotal	Verified Signer	A
dhcpcsyc5.dll       DHCPv6 Glient       Microsoft Corporation       C:Windows/SysWOW64/shcpcsyc5.dll       Q/27       (Verfied) Microsoft         dwmapi.dll       Microsoft Desktop Window Manag       Microsoft Corporation       C:Windows/SysWOW64/shcpcsyc.6.dll       Q/27       (Verfied) Microsoft         locale n/s       Microsoft Desktop Window Manag       Microsoft Corporation       C:Windows/SysWOW64/shcmapi.dll       Q/27       (Verfied) Microsoft         locale n/s       SottDefault n/s       Q/56       (Verfied) Microsoft       C:Windows/SysWOW64/shcmapi.dll       Q/27       (Verfied) Microsoft         explorer.exe.mui       Windows Explorer       Microsoft Corporation       C:Windows/SysWOW64/sec-US/sexplorer.exe.mui       Q/58       (Verfied) Microsoft         gdi/bus.dll       Microsoft Corporation       C:Windows/SysWOW64/sec-US/sexplorer.exe.mui       Q/59       (Verfied) Microsoft         explorer.exe.mui       Windows Explorer       Microsoft Corporation       C:Windows/SysWOW64/sec-US/sexplorer.exe.mui       Q/59       (Verfied) Microsoft         sechost.dll       Host for SCM/SDDL/LSA Lookup       Microsoft Corporation       C:Windows/SysWOW64/sechost.dll       Q/59       (Verfied) Microsoft         sepidel_mui       Winsock2 Helper DLL (TL/IPv6)       Microsoft Corporation       C:Windows/SysWOW64/sechost.dll       Q/59	secur32.dll	Security Support P	rovider Interface	e Microsoft Co	rporation	C:\Windows\SysWOW64\secur32.	dli	0/26	(Verified) Microsof	
dwmapi.dl         Microsoft Desktop Window Mang         Microsoft Corporation         C:Windows/SysWOW64/uhmapi.dl         Q/27         (Verfied) Microsof           nlaapi.dl         Network Location Awareness 2         Microsoft Corporation         C:Windows/SysWOW64/uhmapi.dl         Q/27         (Verfied) Microsof           SortDefault nis         0/256         (Verfied) Microsof         Q/257         (Verfied) Microsof           SortDefault nis         0/256         (Verfied) Microsof         Q/257         (Verfied) Microsof           SortDefault nis         0/257         (Verfied) Microsof         Q/258         (Verfied) Microsof           SortDefault nis         0/258         (Verfied) Microsof	dhcpcsvc6.dll	DHCPv6 Client		Microsoft Co	rporation	C:\Windows\SysWOW64\dhcpcsv	c6.dll	<u>0/27</u>	(Verified) Microsof	E
nlaapi.dll       Network Location Awareness 2       Microsoft Corporation       C:Windows/Sy9WOW64vhaapi.dll       Q/22       (Verfied) Microsof         SortDefault.nls       Q/25       (Verfied) Microsof       Q/25       (Verfied) Microsof         SortDefault.nls       Q/25       (Verfied) Microsof       Q/25       (Verfied) Microsof         Gid/Rus.dll       Microsoft GDI+       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexplorer.xxe.mui       Q/55       (Verfied) Microsof         Gid/Rus.dll       Microsoft GDI+       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexplorer.xxe.mui       Q/59       (Verfied) Microsof         sepicit.dll       Sectost.dll       Host for SCM/SDD/L/SA Lookup       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexploret.Adll       Q/59       (Verfied) Microsof         sepicit.dll       Interset for SCM/SDD/L/SA Lookup       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexploret.adll       Q/59       (Verfied) Microsof         wininet.dll       Interset for SCM/SDD/L/SA Lookup       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexplorej.adll       Q/59       (Verfied) Microsof         winipet_dll       Interset for SCM/SDD/L/SA Lookup       Microsoft Corporation       C:Windows/Sy9WOW64Ven-US/sexplorej.adll       Q/59       (Verfied) Microsof	dwmapi.dll	Microsoft Desktop	Window Manag	g Microsoft Co	rporation	C:\Windows\SysWOW64\dwmapi.dll		<u>0/27</u>	(Verified) Microsof	
locate n/s       C:Windows/System32/locate n/s       0/55       (Verfied) Microsof         sortDefault n/s       C:Windows/System32/locate n/s       0/52       (Verfied) Microsof         explorer.exe.mui       Windows Explorer       Microsoft Corporation       C:Windows/SysWOW64/ven-US/explorer.exe.mui       0/53       (Verfied) Microsof         Gdi/Bus.dll       Microsoft Corporation       C:Windows/SysWOW64/ven-US/explorer.exe.mui       0/59       (Verfied) Microsof         sechost.dll       Host for SCM/SDDL/LSA Lookup       Microsoft Corporation       C:Windows/SysWOW64/ven-US/explorer.exe.mui       0/59       (Verfied) Microsof         sechost.dll       Host for SCM/SDDL/LSA Lookup       Microsoft Corporation       C:Windows/SysWOW64/ven-US/explorer.exe.mui       0/59       (Verfied) Microsof         wininet.dll       Intersect Corporation       C:Windows/SysWOW64/ven-US/exploref.all       0/59       (Verfied) Microsof         wininet.dll       Intersect Corporation       C:Windows/SysWOW64/ven-US/winhet.dll       0/59       (Verfied) Microsof         wininet.dll       Intersect Corporation       C:Windows/SysWOW64/ven-US/winhet.dll       0/59       (Verfied) Microsof         winiped.dll.mui       Winsock2 Helper DLL (TL/IPv6)       Microsoft Corporation       C:Windows/SysWOW64/ven-US/winhet.dll       0/59       (Verfied) Microsof	nlaapi.dl	Network Location	Awareness 2	Microsoft Co	rporation	C:\Windows\SysWOW64\nlaapi.dll		<u>0/27</u>	(Verified) Microsof	
SortDetaut.nls       C::Windows:\SysWOW64\verturn.sty/swOW64\verturn.sty/sy/WW64\verturn.sty/sy/WW64\verturn.sty/sy/WW64\verturn	locale.nls					C:\Windows\System32\locale.nls		0/56	(Verified) Microsof	
explorer         Microsoft Corporation         C: Windows SysWOW64 Ven-US Vexplorer exet mul         U258         (Vertiled) Microsoft           gdrllbs.dll         Microsoft Corporation         C: Windows SysWOW64 Ven-US Vexplorer exet mul         U258         (Vertiled) Microsoft           ipcrt4.dll         Remote Procedure Call Runtime         Microsoft Corporation         C: Windows SysWOW64 Ven-L5 Vexplorer exet mul         U259         (Vertiled) Microsoft           sechost.dll         Host for SCM/SDDL/LSA Lookup         Microsoft Corporation         C: Windows SysWOW64 Ven-L4 dll         U259         (Vertiled) Microsoft           sepicit.dll         Security Support Provider Interface         Microsoft Corporation         C: Windows SysWOW64 Ven-L5 Vexplorer Exet mul         U259         (Vertiled) Microsoft           winipet.dll         Intermet Extensions for Win32         Microsoft Corporation         C: Windows SysWOW64 Ven-US wishlp6.dll.mul         U259         (Vertiled) Microsoft           wishlp6.dll.mul         Winsock2 Helper DLL (TL/IPV6)         Microsoft Corporation         C: Windows SysWOW64 Ven-US wishlp6.dll.mul         U259         (Vertiled) Microsoft           vishlp6.dll.mul         Winsock2 Helper DLL (TL/IPV6)         Microsoft Corporation         C: Windows SysWOW64 Ven-US wishlp6.dll.mul         U259         (Vertiled) Microsoft           vishlp6.dll         Corporation	SortDefault.nls					C:\Windows\Globalization\Sorting\	ortDefault.nls	0/57	(Verified) Microsof	
Gali Husia         Microsoft GDI+         Microsoft Coporation         C:/Windows/sysWOW64/var.V4.dll         U/232         (Verified) Microsoft           port4.dll         Remote Procedure Call Runtime         Microsoft Coporation         C:/Windows/SysWOW64/var.V4.dll         0/559         (Verified) Microsoft           sechat.dll         Host for SCM/SDDL/LSA Lookup         Microsoft Coporation         C:/Windows/SysWOW64/var.V4.dll         0/559         (Verified) Microsoft           spici.dll         Interset Extensions for Win32         Microsoft Coporation         C:/Windows/SysWOW64/var.V5/SWOW64/var.V5/S9         (Verified) Microsoft           wininet.dll         Interset Extensions for Win32         Microsoft Coporation         C:/Windows/SysWOW64/var.V5/SWOW64/var.V5/S9         (Verified) Microsoft           wininet.dll         Interset Extensions for Win32         Microsoft Coporation         C:/Windows/SysWOW64/var.V5/SWoM64/var.V5/S9         (Verified) Microsoft           winipet.dll.mui         Winsock2 Helper DLL (TL/IPv6)         Microsoft Coporation         C:/Windows/SysWOW64/var.V5/SWoM64/var.V5/S9         (Verified) Microsoft           griggrigzizi         Configuration Manager DLL         Microsoft Coporation         C:/Windows/SysWOW64/var.V5/SWOW64/var.V5/S9         (Verified) Microsoft           dipcpscvc.dll         DHCP Client Service         Microsoft Coporation         C:/Windows/SysWOW64/var.	explorer.exe.mui	Windows Explorer		Microsoft Co	rporation	C:\Windows\SysWOW64\en-US\es	kplorer.exe.mui	0/58	(Verified) Microsof	
mpcrt-all         Hemote Procedure Call Function         C:/Vindows/SysWOW64 vpcrt-all         Upsg         (Verfied) Microsof           sepchot.all         Host for SCM/SDDL/LSA Lookup.         Microsoft Corporation         C:/Windows/SysWOW64 vpcrt-all         0/59         (Verfied) Microsof           sspicil.dll         Security Support Provider Interface         Microsoft Corporation         C:/Windows/SysWOW64 vpcrt-all         0/59         (Verfied) Microsof           wininet.dll         Intermet Extensions for Win32         Microsoft Corporation         C:/Windows/SysWOW64 vpcrt/Swship6 all.mui         0/59         (Verfied) Microsof           wship6.dll.mui         Winsock2 Helper DLL (TL/IPv6)         Microsoft Corporation         C:/Windows/SysWOW64 vpcrt/Swship6 all.mui         0/59         (Verfied) Microsof           vship6.dll.mui         Winsock2 Helper DLL (TL/IPv6)         Microsoft Corporation         C:/Windows/SysWOW64 vpcrt/Swship6 all.mui         0/59         (Verfied) Microsof           vship6.gll.mui         Winsock2 Helper DLL (TL/IPv6)         Microsoft Corporation         C:/Windows/SysWOW64 vert/Sisship6 all.mui         0/59         (Verfied) Microsof           vship6.gll.mui         DHCP Clent Service         Microsoft Corporation         C:/Windows/SysWOW64 vert/Sisship6 all.mui         0/60         (Verfied) Microsof           vsplorer.xw         Windows Spslover         <	GdiPlus.dll	Microsoft GDI+	C. I. D	Microsoft Co	inporation	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b		0/59	(Ventied) Microsof	
secrost.dli hds for SUM SDD LSA Lookup Microsoft Corporation C: Windows SysWOW44 secrost.dli 0/59 (Verfied) Microsoft spicit.dli Security Support Provider Interface wininet.dli Internet Extensions for Win32 Microsoft Corporation C: Windows SysWOW44 secrost.dli 0/59 (Verfied) Microsoft wishtcpi.all.mui Winsock2 Helper DL (TL/IPv6) Microsoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft wishtcpi.all.mui Winsock2 Helper DL (TL/IPv6) Microsoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft ofgrgr32.dli Configuration Manager DLL Microsoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft dircosoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft ofgrgr32.dli Configuration Manager DLL Microsoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft dircosoft Corporation C: Windows SysWOW44 ver-US wishtcpi.all.mui 0/59 (Verfied) Microsoft dircosoft Corporation C: Windows SysWOW44 vertual 0/60 (Verfied) Microsoft explorer zwe Windows Explorer Microsoft Corporation C: Windows SysWOW44 vertual 0/60 (Verfied) Microsoft ietutil.dll Run time utility for Internet Explorer Microsoft Corporation C: Windows SysWOW44 vertual.dll 0/60 (Verfied) Microsoft pik.dll Language Pack Microsoft Corporation C: Windows SysWOW44 virm32.dli 0/60 (Verfied) Microsoft phk.dll Language Pack Processes: 47 Physical Usage: 48.48%	rpcrt4.dll	Hemote Procedure	e Call Runtime	Microsoft Co	rporation	C:\Windows\SysWOW64\rpcrt4.dll		0/59	(Ventied) Microsof	
sapidlai       Security Support Provider Interfactor       Microsoft Corporation       C:/Windows/SysWOW64 sepidlai       0/252       (Verified) Microsoft         winipet.dll       Interfactor       Microsoft Corporation       C:/Windows/SysWOW64/ven-US/wishtpb.dll.mui       0/253       (Verified) Microsoft         winipet.dll       Winsock2 Helper DLL (TL/IPv6)       Microsoft Corporation       C:/Windows/SysWOW64/ven-US/wishtpb.dll.mui       0/253       (Verified) Microsoft         gragr32.dll       Configuration Manager DLL       Microsoft Corporation       C:/Windows/SysWOW64/ven-US/wishtpb.dll.mui       0/259       (Verified) Microsoft         dhcpcsvc.dll       DHCP Client Service       Microsoft Corporation       C:/Windows/SysWOW64/ven/US/wishtcpip.dll.mui       0/260       (Verified) Microsoft         explorer.exe       Windows Explorer       Microsoft Corporation       C:/Windows/SysWOW64/ven/US/wishtcpip.dll.mui       0/260       (Verified) Microsoft         explorer.exe       Windows Explorer       Microsoft Corporation       C:/Windows/SysWOW64/ven/Us/wishtpip.dll.mui       0/260       (Verified) Microsoft         imm32.dll       Nutri-User Windows MM32.API Cli       Microsoft Corporation       C:/Windows/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us/SysWOW64/ven/Us	secnost.dll	Flost for SCIM/SDL	JL/LSA LOOKUP	Microsoft Co	rporation	C:\Windows\SysWOW64\sechost.dll		0/55	(verned) Microsof	
wining       interface Data statistical winits 2         winitschild       Winitschild <td>sspicit.dll</td> <td>letomot Extension</td> <td>for Win22</td> <td>e Microsoft Co</td> <td>rporation</td> <td>C:\Windows\SysWOW64\sspici.dll</td> <td></td> <td>0/59</td> <td>(ventied) Microsof</td> <td></td>	sspicit.dll	letomot Extension	for Win22	e Microsoft Co	rporation	C:\Windows\SysWOW64\sspici.dll		0/59	(ventied) Microsof	
Winlock2 Helper DL (TL/TV/9)       Microsoft Corporation       C:Windows/SysWOW64/er/DS/winlop/all/uli       0/252       (Verified) Microsoft.         cfgmg/32.dll       Configuration Manager DLL       Microsoft Corporation       C:Windows/SysWOW64/er/DS/winlop/all/uli       0/250       (Verified) Microsoft.         dhopcsvc.dll       DHCP Client Service       Microsoft Corporation       C:Windows/SysWOW64/er/Dgrgr32.dll       0/60       (Verified) Microsoft.         explorer.see       Windows Explorer       Microsoft Corporation       C:Windows/SysWOW64/er/Dgrgr32.dll       0/60       (Verified) Microsoft.         explorer.see       Windows Explorer       Microsoft Corporation       C:Windows/SysWOW64/er/Dgrer.exe       0/60       (Verified) Microsoft         iertuiti.dll       Run time utility for Internet Explorer       Microsoft Corporation       C:Windows/SysWOW64/winm32.dll       0/60       (Verified) Microsoft         jbk.dll       Language Pack       Microsoft Corporation       C:Windows/SysWOW64/winm32.dll       0/60       (Verified) Microsoft         jbk.dll       Language Pack       Microsoft Corporation       C:Windows/SysWOW64/winm32.dll       0/60       (Verified) Microsoft         QPU Sage: 4.64%       Corporation       C:Windows/SysWOW64/winm32.dll       0/60       (Verified) Microsoft       v	wininet.dli internet Extensions for Win32 Winsock 2 Helper DLL (TL /IPv6)		Microsoft Co	moration	C:\Windows\SysWOW64\wininet.dll		0/59	(Verified) Microsof		
Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           dirpgr32.dl         Configuration Manager DLL         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           dirpcrsvc.dl         DHCP Client Service         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           explorer.exe         Windows Explorer         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           iertuil.dl         Run time utility for Internet Explorer         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           imm32.dll         Multi-User Windows IMM32 API Cli         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           jpk.dll         Language Pack         Microsoft Corporation         C:/Windows/SysWOW64/sigms22.dl         Ø/60         (Verified) Microsoft           CPU Usage: 4.64%         Corporation         C:/Windows/SysWOW64/sigms23.dl         Ø/60         (Verified) Microsoft         v	wship6.dil.mui Winsock2 Helper DLL (TL/IPv6) wshtopin dll mui Winsock2 Helper DLL (TL/IPv4)		Microsoft Co	moration	C:\Windows\SysWOW64\en-US\w	shipo.air.mai ehtopin dli mui	0/59	(Verified) Microsof		
Barborne         DHCP Client Service         Microsoft Corporation         C:Windows/SysWOW64/bjcsvc.dll         D/260         (Verified) Microsoft           explorer.exe         Windows Explorer         Microsoft Corporation         C:Windows/SysWOW64/vertuil.dll         D/60         (Verified) Microsoft           entruit.ldll         Run time utility for Internet Explorer         Microsoft Corporation         C:Windows/SysWOW64/vertuil.dll         D/60         (Verified) Microsoft           imm32.dll         Mutti-User Windows IMM32 API Cli         Microsoft Corporation         C:Windows/SysWOW64/vertuil.dll         D/60         (Verified) Microsoft           jbr.dll         Language Pack         Microsoft Corporation         C:Windows/SysWOW64/vertuil.dll         D/60         (Verified) Microsoft           CPU Usage: 4.64%         Commit Charge: 17.68%         Processes: 47         Physical Usage: 48.48%         E	cfomor32 dl Configuration Manager DLL		Microsoft Co	moration	C:\Windows\SysWOW64\cfamar32	) dll	0/60	(Verified) Microsof		
explorer.exe Windows Explorer Microsoft Corporation C:\Windows\SysWOW64\explorer.exe 02.60 (Verified) Microsoft iertuil.dll Run time utility for Internet Explorer Microsoft Corporation C:\Windows\SysWOW64\extual.dll 02.60 (Verified) Microsoft jmm32.dll Mutti-User Windows IMM32 API Cli Microsoft Corporation C:\Windows\SysWOW64\extual.dll 02.60 (Verified) Microsoft pix.dll Language Pack Microsoft Corporation C:\Windows\SysWOW64\extual.dll 02.60 (Verified) Microsoft CPU Usage: 4.64% Commit Charge: 17.68% Processes: 47 Physical Usage: 48.48%	dhoposvo dli DHCP Client Service		Microsoft Co	rporation	C:\Windows\SvsWOW64\dhcncsv	c.dl	0/60	(Verified) Microsof		
Interval         Run time utility for Internet Explorer         Microsoft Corporation         C:\Windows\SysWOW64\sertutil.dll         0/60         (Verified) Microsoft           imm32.dll         Multi-User Windows IMM32 API Cli         Microsoft Corporation         C:\Windows\SysWOW64\sertutil.dll         0/60         (Verified) Microsoft           lpk.dll         Language Pack         Microsoft Corporation         C:\Windows\SysWOW64\pik.dll         0/60         (Verified) Microsoft           CPU Usage: 4.64%         Cormit Charge: 17.68%         Processes: 47         Physical Usage: 48.48%         C	explorer exe Windows Explorer		Microsoft Co	rooration	C:\Windows\SvsWOW64\explorer	exe	0/60	(Verified) Microsof		
imm32.dll Multi-User Windows IMM32 API Cli Microsoft Corporation C:\Windows\SysWOW64\imm32.dll <u>0/60</u> (Verified) Microsoft [pk.dll Language Pack Microsoft Corporation C:\Windows\SysWOW64\lpk.dll <u>0/60</u> (Verified) Microsof ▼ CPU Usage: 4.64% Commit Charge: 17.68% Processes: 47 Physical Usage: 48.48%	iertutil.dll	Run time utility for	Internet Explore	r Microsoft Co	poration	C:\Windows\SysWOW64\iertutil.dll		0/60	(Verified) Microsof	
Ipk.dll         Language Pack         Microsoft Corporation         C:\Windows\SysWOW64\lpk.dll         0/60         (Verified) Microsoft         ▼           CPU Usage: 4.64%         Commit Charge: 17.68%         Processes: 47         Physical Usage: 48.48%         Verified)	imm32.dll	Multi-User Window	s IMM32 API C	li Microsoft Co	poration	C:\Windows\SysWOW64\imm32.dll		0/60	(Verified) Microsof	
CPU Usage: 4.64% Commit Charge: 17.68% Processes: 47 Physical Usage: 48.48%	lpk.dll	Language Pack		Microsoft Co	poration	C:\Windows\SysWOW64\lpk.dll		0/60	(Verified) Microsof	-
	CPU Usage: 4.64%	Commit Charg	e: 17.68% Pro	ocesses: 47 Ph	iysical Usage: 4	8.48%				

Abbildung 14: Virustotal erkennt den bösartigen Code nicht

## 3 Bemerkungen

Eine mögliche Einbettung dieses Monitoring Use Cases in das interne Log-Monitoring Framework kann z.B. mittels eines Scheduled Tasks und der Überwachung des entsprechenden Logfile Directories erfolgen. Zu klären ist, ob installierte Third-Party Applikationen (z.B. AV) ebenfalls diese Technik nutzen und entsprechend in eine Whiteliste aufzunehmen sind.