Windsor Day 3: Domain Keylogger

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

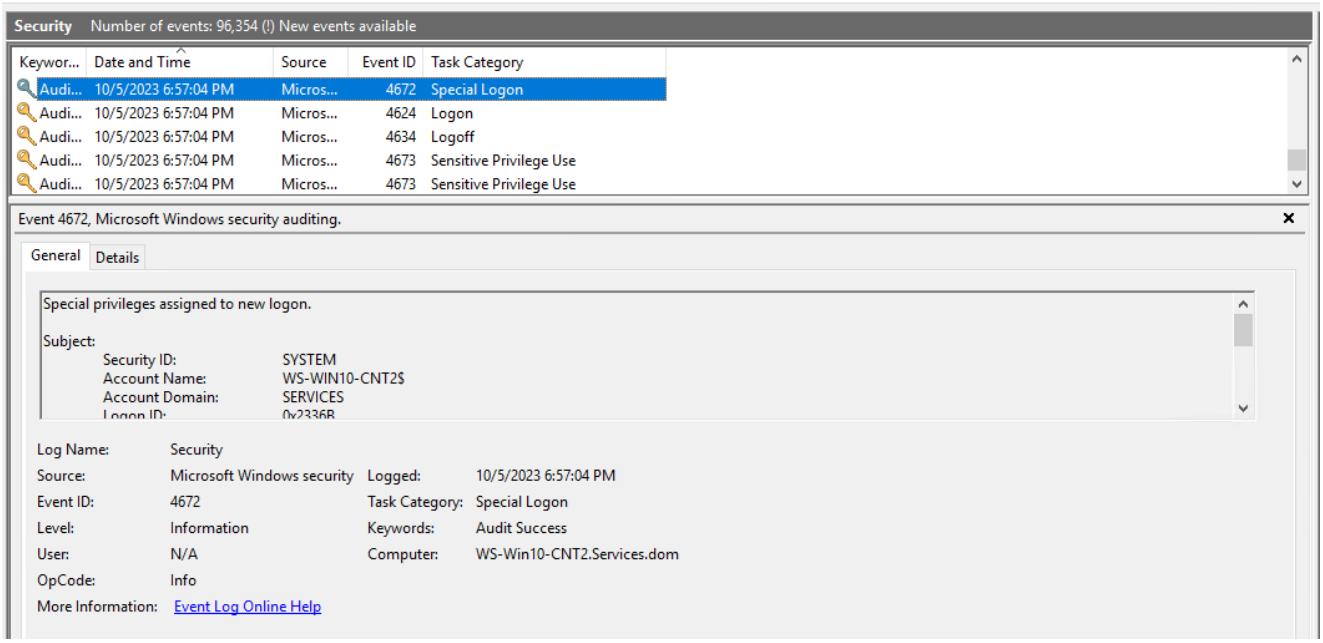
18:43 First packet from 213.0.0.86

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



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

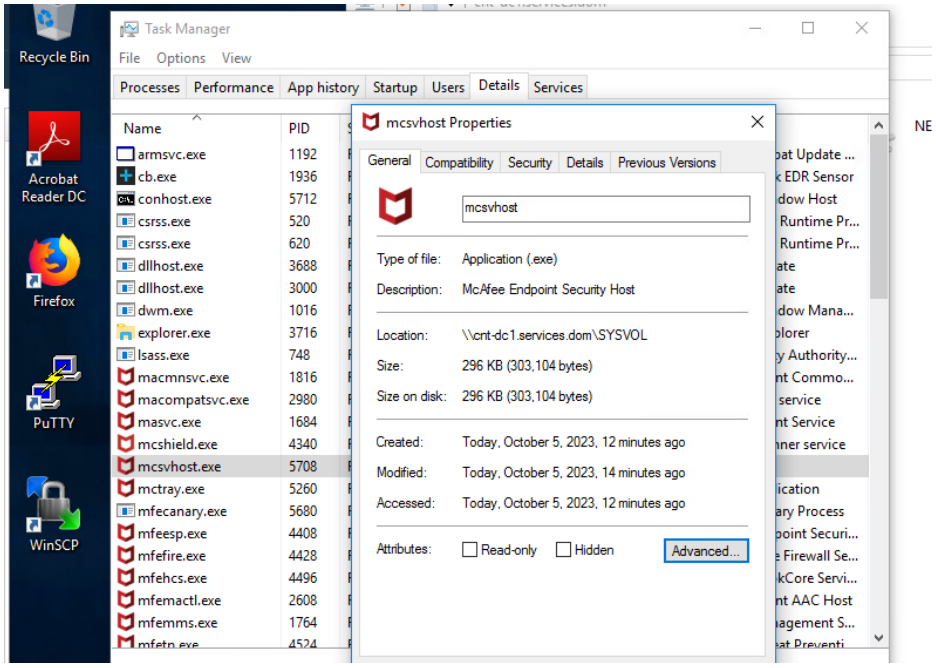
19:00 QRadar Offense Alert: Suspicious NET Traffic containing traffic end (Dest IP 213.0.0.86)

Current Search Parameters:

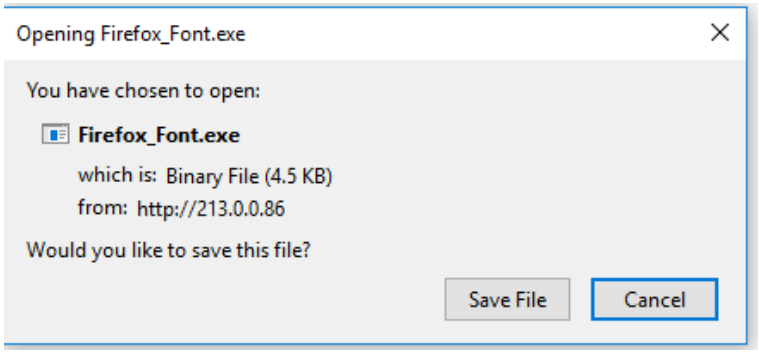
Exclude Hidden Offenses . (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description
	41	Suspicious Net Traffic containing Traffic End

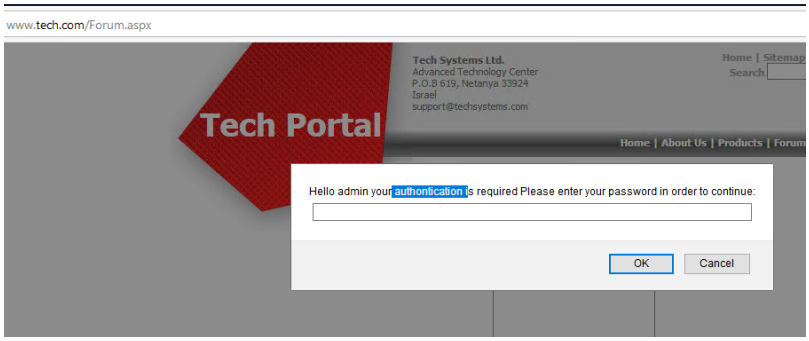
19:00 Mcsvhost accessed/modified on Windows 10-CNT2 (\\cnt-dc1.services.dom\SYSVOL)



??? Binary file uploaded from 213.0.0.86



Hello admin your “authontication” required

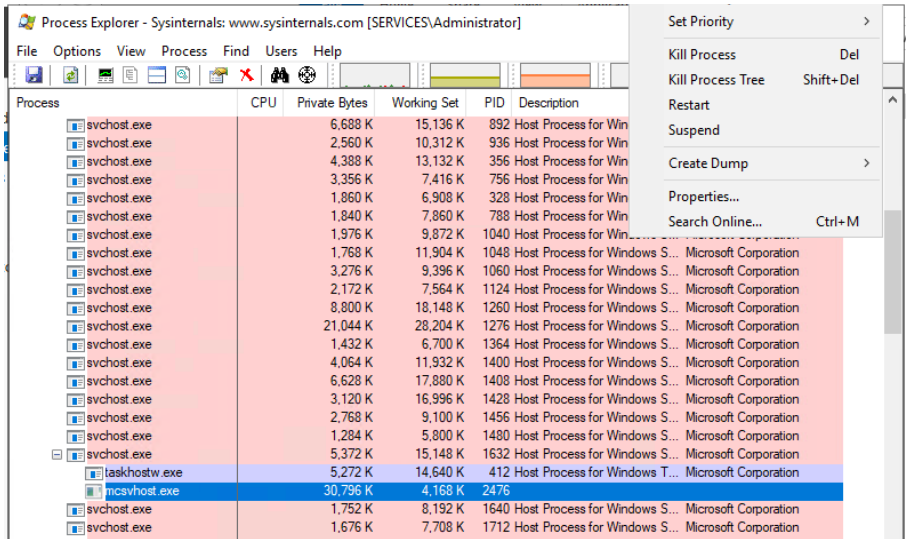


20:15 QRadar Offense Alert: 192.168.200.1 Suspicious Probes 502 Events.

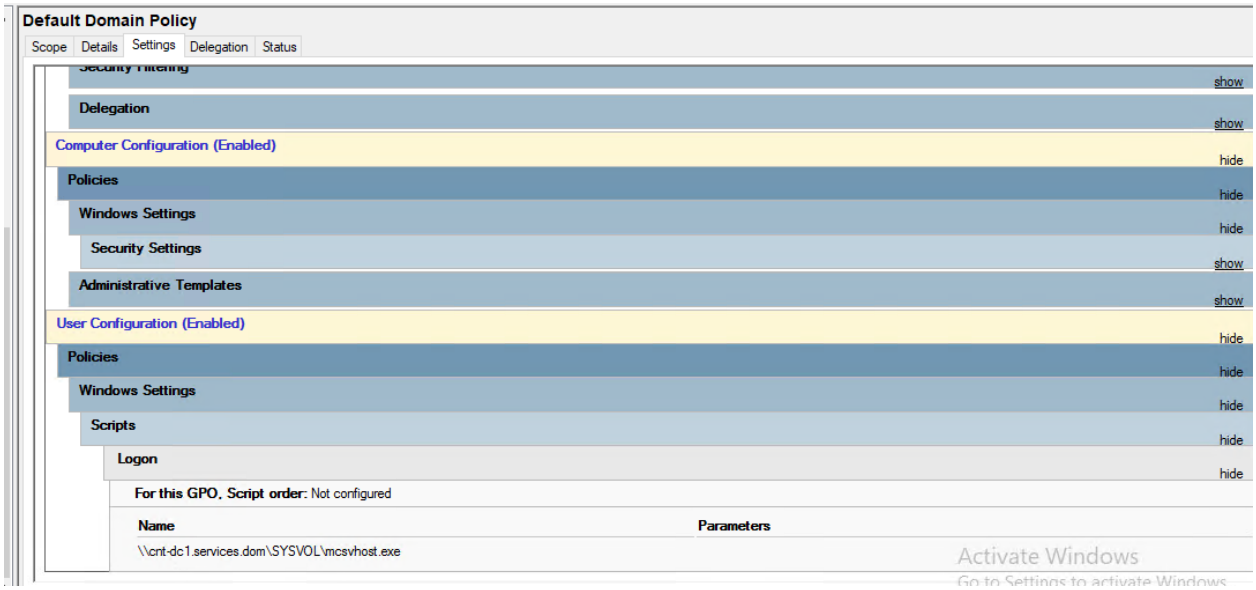
Offense 43

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

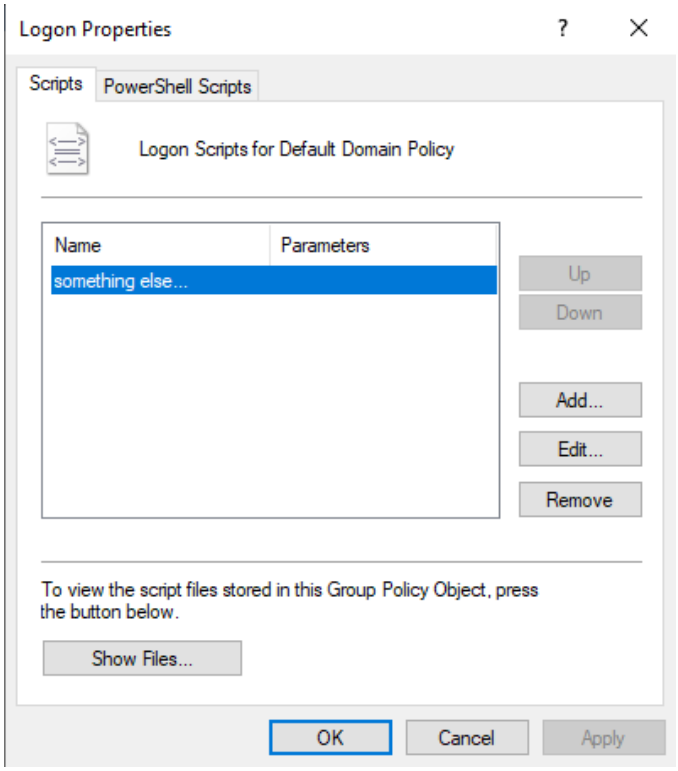
Unsigned mcsvhost.exe file running



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



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