Title: Group Triage Challenge 3

Group/Name: Marty Schneider

Indicators and Technical Details

Include all relevant technical details and indicators regarding your investigation that pertains to your analysis, findings, and summary statements.

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
	C:\Windows\explorer.EXE		Unusual process running with weird path and odd spelling. Had network data despite explorer typically not having any network activity. PID 4836 and Parent PID 4860
	NetworkDLL.dll	TG1055.001	Dynamic-link library injection
	3.223.192.12		IP that the process was making TCP connection to

Executive Summary

An unusual process was found making outbound connections to an amazon EC2 instance. This process was potentially exfiltrating sensitive data to be used or sold. It is not persistent and can be neutralized by rebooting and removing the malicious DLL.

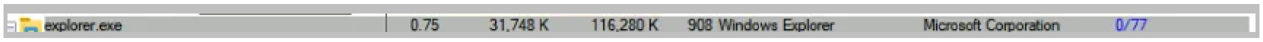
Technical Summary

An unusual process was found masking itself as the Windows explorer. It was found due to its odd path and spelling: C:\Windows\explorer.EXE with PID 4836 and Parent PID 4860. Upon further inspection it was found to be creating outbound TCP connections to an external amazon EC2 instance at 3.223.192.12:8080. It was able to achieve this by using DLL injection with NetworkDLL.dll Mitre tactic T1055.001.

Findings and Analysis

What is the name of the suspect process repeatedly establishing outbound TCP connections?

explorer.exe



```
explorer.exe    0.75    31,748 K    116,280 K    908 Windows Explorer    Microsoft Corporation    0/77
```

What is the remote IP Address that the process connects to?

3.223.192.12:8080

What remote port is that process connecting to?

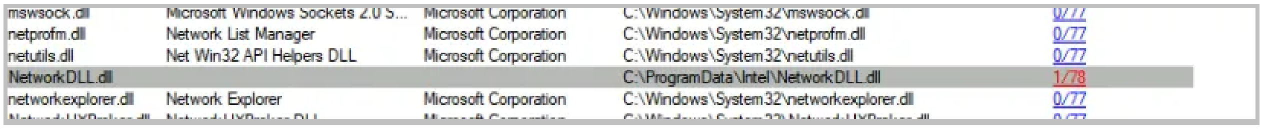
8080

What is the primary significance of this network activity?

Originating process does not normally have network activity

What is the name of the suspicious DLL loaded into the process?

networkDLL.dll



mswsock.dll	Microsoft Windows Sockets 2.0 S...	Microsoft Corporation	C:\Windows\System32\mswsock.dll	0/77
netprofm.dll	Network List Manager	Microsoft Corporation	C:\Windows\System32\netprofm.dll	0/77
netutils.dll	Net Win32 API Helpers DLL	Microsoft Corporation	C:\Windows\System32\netutils.dll	0/77
NetworkDLL.dll			C:\ProgramData\Intel\NetworkDLL.dll	1/78
networkexplorer.dll	Network Explorer	Microsoft Corporation	C:\Windows\System32\networkexplorer.dll	0/77

What correlates this DLL to the originally discovered network activity?

It was a loaded module of the original suspect process, it was recently modified and had references to HTTP in the strings.

What is the SHA-256 has of the DLL?

71755a9f83c290f20ab3e1be93ba4534515acccde9ebd7f112fb12be9cee7432

What attack technique is this an example of?

DLL injection

What form of persistence did this malware establish?

None

What is the most direct way to remove this malware?

Reboot and delete the malicious file.

Remediation and Recommendations

In order to remediate, it is recommended to reboot the target machine and delete the malicious DLL.