

A Peek Into Muddled Libra's Operational Playbook

 unit42.paloaltonetworks.com/muddled-libra-ops-playbook

Justin De Luna, Noah Rincon, Cuong Dinh

February 10, 2026

Executive Summary

During a September 2025 incident response investigation, Unit 42 discovered a rogue virtual machine (VM) which we believe with high confidence to be used by the cybercrime group Muddled Libra (aka Scattered Spider, UNC3944). The contents of this rogue VM and activity from the attack provide valuable insight into the operational playbook of this threat actor.

Muddled Libra created the VM after the group successfully gained unauthorized access to the target's VMware vSphere environment. Activities during the attack include:

- Performing reconnaissance
- Downloading tools
- Establishing persistence via a command and control (C2) channel
- Using stolen certificates
- Copying files from the rogue VM to the target's domain controller (DC)
- Interacting with the target's Snowflake infrastructure

Based on the characteristics of the attack, we assess with high confidence that Muddled Libra conducted it. This article provides a detailed analysis of our observations to shed further light on the threat actor's tactics, techniques and procedures (TTPs).

Palo Alto Networks are better protected from the threats discussed in this article through the following products and services:

- [Advanced WildFire](#)
- [Cortex Cloud](#)
- [Cortex XDR](#) and [XSIAM](#)

If you think you might have been compromised or have an urgent matter, contact the [Unit 42 Incident Response team](#).

Related Unit 42 Topics [Muddled Libra](#), [Cybercrime](#)

Who Is Muddled Libra?

As previously documented, threat actors affiliated with Muddled Libra use various [social engineering tactics](#) (e.g., smishing, vishing) to gain initial access to targeted organizations. Activities can include targeting call centers operated by potential victims, as well as those

outsourced to third-party firms. These third-party firms include business process outsourcing (BPOs) and managed service providers (MSPs). This expands the group’s range of potential targets.

Threat actors affiliated with Muddled Libra are highly proficient at exploiting human psychology by impersonating employees to attempt password and multi-factor authentication (MFA) resets. Figure 1 illustrates the composition of Muddled Libra in terms of their demographics, tradecraft, victim targeting and actions on objectives.

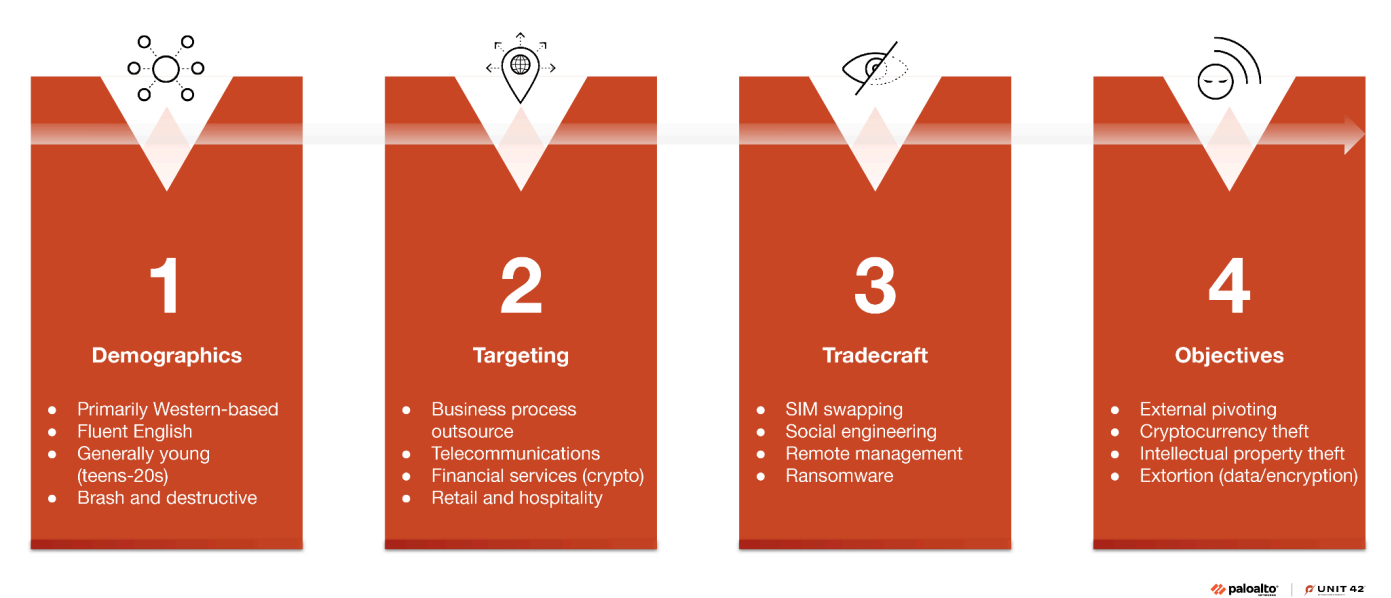


Figure 1. Muddled Libra threat profile.

While their tradecraft has evolved, threat actors affiliated with Muddled Libra continue to minimize their use of malware throughout the attack chain. Whenever possible, they prefer to use their targets' own assets against them.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product is flawed or malicious.

Background on the Attack Chain

We assisted a client with an incident response engagement in September 2025. Throughout our investigation, we identified and recovered a VM created and leveraged by the threat actor to conduct the early stages of its attack. Attackers were unable to delete this VM before their access was cut off. We often observe threat actors creating VMs within targeted environments to avoid detection from endpoint tools like endpoint detection and response (EDR) or extended detection and response (XDR).

By examining this VM, we discovered the tools the attackers leveraged and the basic troubleshooting they conducted during their unauthorized access. This provided insights into their operational methods.

Using forensic artifacts and logs, we uncovered a large amount of activity conducted from this VM, including lateral movement and tools used. Figure 2 further illustrates our observations during the investigation. Note that the analysis below is of a single system and does not cover the entire incident observed by Unit 42.

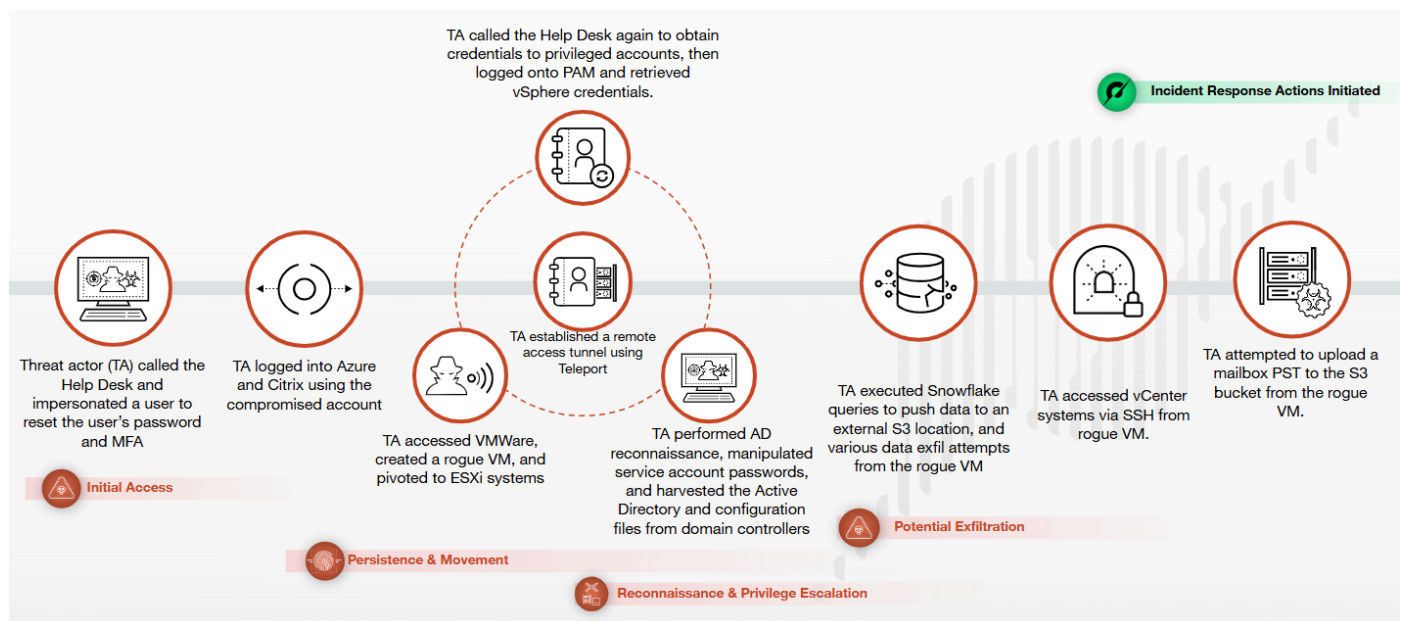


Figure 2. High-level chain of events in the attack investigated by Unit 42.

A Peek Into Muddled Libra Tactics

Approximately two hours after gaining initial access to the target's environment, we observed the attackers accessing the target's vSphere portal and creating a new VM named "New Virtual Machine." The attackers then leveraged this VM for the early stages of the incident as a beachhead host using the local Administrator account.

Shortly after logging into the newly created VM, attackers downloaded stolen certificates from the targeted environment. They leveraged these certificates to forge tickets throughout their attack chain.

Within three minutes, attackers established additional persistence in the target's environment using an SSH tunnel through the [Chisel](#) tool. This tool was contained in a ZIP archive named `goon.zip` that was hosted on an AWS S3 bucket under the attackers' control.

Nearly one minute after they downloaded the ZIP archive containing Chisel, we observed malicious network connections to an attacker-controlled IP address over TCP port 443 (HTTPS). We observed this connection for a total of 15 hours. Figures 3-5 illustrate these observations.

```
[ZoneTransfer]
ZoneId=3
HostUrl=https[REDACTED]prd1.s3.us-east-2.amazonaws.com/goon.zip
```

Figure 3. URL hosting archive containing the Chisel tool.

[REDACTED]	.\Users\Administrator\Downloads	goon.zip
	.\Users\Administrator\Downloads	goon.zip:Zone.Identifier

Figure 4. The downloaded tool, goon.zip.

[REDACTED]	.\Users\Administrator\Desktop	chisel.exe
	.\Users\Administrator\Desktop	chisel.exe:Zone.Identifier

Figure 5. The SSH tunneling tool, chisel.exe, extracted from goon.zip.

A minute later, we observed them logging in interactively with a new local user account named gooner.

Approximately 15 minutes after creating the VM, the attackers began using vSphere to power down two of the target's virtualized DCs. They then mounted the virtual machine disks (VMDKs) of the powered-down DCs. This allowed them to copy the NTDS.dit and SYSTEM registry hive files from these two DCs and place them on the desktop of the Administrator account on their newly created VM.

Approximately two minutes later, they wrote two files, result and result.kerb, to the local Administrator account's desktop. We retrieved these files and determined that these were decrypted versions of the target's NTDS.dit Active Directory database, which contained hashes of all users. Figures 6 and 7 illustrate these observations.

```

mks - MKS PowerOff
svga - SVGA thread is exiting
mks - MKS thread is exiting
vmx -
vmx - scsi0:1: numIOs = 0 numMergedIOs = 0 numSplitIOs = 0 ( 0.0%)
vmx - Closing disk 'scsi0:1'
vmx - DISKLIB-CBT : Shutting down change tracking for untracked fid 2103136621.
vmx - DISKLIB-CBT : Successfully disconnected CBT node.
vmx - DISKLIB-VMFS : "/vmfs/volumes/6092022e-df7c5457-bb07-0025b52a00ff/[REDACTED]DC01/"
vmx -
vmx - scsi0:0: numIOs = 0 numMergedIOs = 0 numSplitIOs = 0 ( 0.0%)
vmx - Closing disk 'scsi0:0'
vmx - DISKLIB-CBT : Shutting down change tracking for untracked fid 1835618653.
vmx - DISKLIB-CBT : Successfully disconnected CBT node.
vmx - DISKLIB-VMFS : "/vmfs/volumes/6092022e-df7c5457-bb07-0025b52a00ff/[REDACTED]DC01/"

```

Figure 6. VMware logs of the shutdown activities of the DC.

.\Users\Administrator\Desktop	ntds.dit
.\Users\Administrator\Desktop	SYSTEM
.\Users\Administrator\Desktop	result
.\Users\Administrator\Desktop	result.kerb

Figure 7. List of files discovered for credential dump, NTML hash and Kerberos hash.

At nearly 30 minutes of access to this newly created VM, the attackers began executing the Active Directory enumeration tool [ADRecon](#). We observed and retrieved dozens of files associated with ADRecon, including a PowerShell script and output files.

These files contained information such as:

- Domain details
- Forest
- Trusts
- Sites
- Subnets
- Schema
- Password policy
- DCs
- Service Principal Names (SPNs)
- Users
- Group Policy Objects (GPOs)

The output of the ADRecon tool would then be placed in a ZIP archive named <VICTIM ORGANIZATION>.zip (where <victim organization> represents the name of the victim, redacted for this report). We also observed the attackers downloading the tool ADExplorer64.exe directly from the Microsoft SysInternals domain. Figure 8 illustrates these observations.

.\\Users\\Administrator\\Desktop\\ADRecon-Report-		CSV-Files
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Domain.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Forest.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Trusts.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Sites.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Subnets.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	SchemaHistory.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	DefaultPasswordPolicy.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	DomainControllers.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Users.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	UserSPNs.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Groups.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	GroupChanges.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	GroupMembers.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	OUs.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	GPOs.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	gPLinks.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Printers.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	Computers.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	ComputerSPNs.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	LAPS.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	AboutADRecon.csv
.\\Users\\Administrator\\Desktop\\ADRecon-Report-	CSV-Files	<Redacted>.zip

ZIP archive named after
victim organization

Figure 8. List of ADRecon output files discovered during our investigation.

Within the ADRecon output, the threat actors only opened the CSV file ComputerSPNs.csv. This file contained all available service principal names (SPNs) associated with hosts in the environment. Attackers gather this information to help identify critical services running that they are interested in targeting. These critical services include:

- Veeam
- Terminal services
- Hyper-V
- MSSQL
- Exchange
- Other similar systems as shown in Figure 9

- LimeWire
- upload[.]jee
- uploadnow[.]io
- filetransfer[.]io
- filebin[.]io
- Dropbox

Figures 11-13 illustrate these observations.

https://app.snowflake.com/us-east-1/marketing/#/data/databases/		Table
https://app.snowflake.com/us-east-1/marketing/#/data/databases/		Table
https://app.snowflake.com/us-east-1/marketing/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/search?query=transaction&corpus=tableView		Search
https://app.snowflake.com/enterprise/#/search?query=cvv&corpus=tableView		Search
https://app.snowflake.com/enterprise/#/search?query=card&corpus=tableView		Search
https://app.snowflake.com/enterprise/#/search?query=card_number&corpus=tableView		Search
https://app.snowflake.com/enterprise/#/search?query=ip%20address&corpus=tableView		Search
https://app.snowflake.com/enterprise/#/search?query=ip%20address&corpus=all		Search
https://app.snowflake.com/enterprise/#/search?query=ip&corpus=all		Search
https://app.snowflake.com/enterprise/#/search?query=ip%20address&corpus=all		Search
https://app.snowflake.com/enterprise/#/search		Search
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/query		Snowflake
https://app.snowflake.com/enterprise/#/query		Snowflake
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/query		Snowflake
https://app.snowflake.com/enterprise/#/query		Snowflake
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Table
https://app.snowflake.com/enterprise/#/data/databases/		Database Explorer
https://app.snowflake.com/enterprise/#/data/databases/		Database Explorer
https://app.snowflake.com/enterprise/#/data/databases/		Database Explorer
https://app.snowflake.com/enterprise/#/data/databases/		Database Explorer
https://app.snowflake.com/enterprise/#/data/databases/		Database Explorer
https://www.bing.com/search?q=app.snowflake.com&cvid=		app.snowflake.com - Search

Figure 11. List of Snowflake web browsing activities documented from our investigation.

upload files no registration - Search
upload files no registration - Search
upload files no registration - Search
upload files no registration - Search
upload files no registration - Search
upload files - Search
upload files - Search

Figure 12. Web searches for cloud storage services discovered during our investigation.

https://filebin.net/	Access Blocked
https://uploadnow.io/en/upload	Access Blocked
http://www.upload.ee/	Access Blocked
https://www.upload.ee/	Access Blocked
https://limewire.com/	Access Blocked
https://we.tl/	Access Blocked

Figure 13. Web browsing activities to cloud storage services discovered during our investigation.

Shortly after interacting with the data, the attackers began lateral movement using multiple then-compromised accounts with their SSH tunnel, RDP and PsExec. They downloaded the PsExec tool directly from the Microsoft SysInternals domain.

Approximately four hours after the creation of their VM, the attackers began looking for additional sensitive data. At that time, we observed them having compromised a handful of accounts, one of which they used to access the mailboxes of other accounts to download a Personal Storage Table (PST) file. However, based on Bing search history, they had difficulty accessing the mailbox via Office.

The attackers then searched the web for “office[.]com old setup download” and “is there a place to download an older version of Outlook?” Attackers also reviewed various Reddit posts related to this query. Shortly after, they downloaded and ran OfficeSetup.exe from Microsoft.

They then began troubleshooting items such as “Outlook slow downloading emails” and performed several internet speed checks using the site fast[.]com. Figures 14-17 illustrate these observations.

https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	login	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Sign in to your account
https://login.microsoftonline.com	saml2?SAMLRequest=	Working...
https://login.microsoftonline.com	saml2?SAMLRequest=	Working...
https://login.microsoftonline.com	saml2?SAMLRequest=	Working...
https://login.microsoftonline.com	saml2?SAMLRequest=	Working...
https://login.microsoftonline.com	saml2?SAMLRequest=	Working...
https://login.microsoftonline.com/kmsi		Working...

Figure 14. Online Outlook login activities discovered during our investigation.

https://support.microsoft.com/en-gb/office/install-or-reinstall-classic-outlook-on-a-windows-pc-5c94902b-31a5-4274-abb0-b07f4661edf5	Install or reinstall classic Outlook on a Windows PC - Microsoft Support
https://support.microsoft.com/en-gb/office/you-can-t-open-classic-outlook-on-a-new-windows-pc-5c94902b-31a5-4274-abb0-b07f4661edf5	Install or reinstall classic Outlook on a Windows PC - Microsoft Support
https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016	Microsoft Office 2016 - Microsoft Lifecycle Microsoft Learn
https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016	Microsoft Office 2016 - Microsoft Lifecycle Microsoft Learn

Figure 15. Web searches for Outlook agents discovered during our investigation.

is there a place to download an older version of outlook? : r/Outlook
r=2&hsh=4&fclid=233b7d1d-e12d-6b53-1758-6b7be09d6ada&psq=office.com+old+setup+download+reddit&u=a1aHR0cHM6
office.com old setup download reddit - Search
is there a place to download an older version of outlook? : r/Outlook
r=2&hsh=4&fclid=233b7d1d-e12d-6b53-1758-6b7be09d6ada&psq=office.com+old+setup+download+reddit&u=a1aHR0cHM6
office.com old setup download reddit - Search
Why is it so hard to find the installation file for Office 2016? : r/microsoft
2&hsh=4&fclid=233b7d1d-e12d-6b53-1758-6b7be09d6ada&psq=office.com+old+setup+download+reddit&u=a1aHR0cHM6Ly!
office.com old setup download reddit - Search
office.com old setup download reddit - Search

Figure 16. Web searches for older Outlook versions discovered during our investigation.

speedtest - Search
outlook slow downloading emails - Search
outlook slow downloading emails - Search

Figure 17. Web searches to troubleshoot slow email download issues and perform a speed test.

In addition to troubleshooting their download speeds, attackers used Bing to identify the location of the Outlook ODT file. Figure 18 illustrates this observation.

Figure 18. Web search for the Outlook ODT file location discovered during our investigation.

Additionally, we observed Microsoft Defender, presumably installed on the VM by default, taking action on multiple malicious files on this VM. This included ADRecon, Chisel and GoSecretsDump. Figure 19 lists these detections.

file:_C:\Users\Administrator\Desktop\gosecretsdump_win_v0.3.1.exe	Malware name: HackTool:Win64/SecretDump.Aldha	Description: Tool (High)
file:_C:\Users\Administrator\Desktop\ADRecon.ps1	Malware name: HackTool:PowerShell/ADRecon!pz	Description: Tool (High)
file:_C:\Users\Administrator\Desktop\chisel.exe; process:_pid:5840,Process...	Malware name: Trojan:Win32/Wingo!MTB	Description: Trojan (Severe)

Figure 19. Microsoft Defender detections on tools discovered during our investigation.

After some time, the attackers then began attempting to exfiltrate the Outlook PST file. They first searched for the [S3 Browser](#) tool. Once they downloaded the tool from the S3 Browser website, attackers then attempted to exfiltrate the PST file by uploading it to their S3 bucket. Figures 20 and 21 illustrate these observations.

17:42:26.1922476	.\Users\Administrator\Downloads	s3browser-12-6-1.exe
17:42:26.1922476	.\Users\Administrator\Downloads	s3browser-12-6-1.exe:SmartScreen

Figure 20. Downloaded S3 browser executable discovered during our investigation.

[I]	[REDACTED]	0:59:50]	Uploading (1 of 7) C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 113
[W]	[REDACTED]	10:59:50]	System.IO.IOException: The process cannot access the file because another process has locked a portion of the file.
			at System.IO._Error.WinOSError(Int32 errorCode, String maybeFullPath)
			at System.IO.FileStream.ReadCore(Byte[] buffer, Int32 offset, Int32 count)
			at System.IO.FileStream.Read(Byte[] array, Int32 offset, Int32 count)
			at rl.c(Stream fps, Stream fpt, Boolean fpu)
			at rs.Do()
			at ru.Do()
			at yf.c(xz gko) TaskID: 113
[I]	[REDACTED]	0:59:51]	Task stopped (maximum number of retry attempts reached) TaskID: 113
[W]	[REDACTED]	10:59:51]	Task failed (System.IO.IOException: The process cannot access the file because another process has locked a portion of the file.
			) TaskID: 113
[I]	[REDACTED]	0:59:51]	Collecting files from [REDACTED]prd1/ (page 1) TaskID: 130
[I]	[REDACTED]	0:59:51]	Successfully collected files from [REDACTED]prd1/ TaskID: 130
[I]	[REDACTED]	0:59:52]	Total objects: 2 (1 files and 1 folders) 3.56 MB (3 735 501 bytes)
[I]	[REDACTED]	1:01:36]	Successfully uploaded part 7 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 119
[I]	[REDACTED]	1:02:17]	Successfully uploaded part 5 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 117
[I]	[REDACTED]	1:02:19]	Successfully uploaded part 3 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 115
[I]	[REDACTED]	1:02:20]	Successfully uploaded part 6 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 118
[I]	[REDACTED]	1:02:22]	Successfully uploaded part 4 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 116
[I]	[REDACTED]	1:02:22]	Successfully uploaded part 2 of 7 C:\Users\Administrator\Documents\Outlook Files\backup.pst to [REDACTED]prd1/backup.pst TaskID: 114

Figure 21. S3 Browser logs of PST file upload.

After approximately 15 hours of access to their VM, attackers began browsing various VMware ESXi hosts. They continued to pivot through the network, leveraging access to multiple compromised accounts before their access was terminated by the targeted organization’s security team. Figure 22 illustrates this observation.

https://		/ui/#/login	Login - VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/login	Login - VMware ESXi
https://		/	- VMware ESXi
https://		/ui/	- VMware ESXi
https://		/ui	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/host	- VMware ESXi
https://		/ui/#/login	- VMware ESXi
https://		/	- VMware ESXi
https://		/ui/	- VMware ESXi
https://		/ui	- VMware ESXi

Figure 22. Browsing activities to the target's VMware ESXi hosts discovered during our investigation.

Conclusion

Intrusion operations Muddled Libra conducts have affected the business operations of many organizations across the globe. This is not because they use advanced malware or novel exploits, but because they exploit the weakest link: humans.

While focusing on identity compromise and social engineering, this threat actor leverages legitimate tools and existing infrastructure to blend in. They operate quietly and maintain persistence.

This incident offers a rare window into an operational playbook used by Muddled Libra, revealing how a single rogue VM can serve as a powerful foothold for lateral movement and data theft. The threat actor's methods underscore the importance of:

- Strengthening identity security
- Enforcing strict access controls
- Continuously monitoring for anomalous use of administrative tools and cloud environments

Organizations should adopt a defense-in-depth strategy centered on:

- Protecting identity
- Maintaining least-privileged access
- Detecting living-off-the-land behaviors

While Muddled Libra's tactics may appear simple, their effectiveness reminds us that cybersecurity resilience begins not with complexity, but with vigilance, visibility and disciplined access management.

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

The [Advanced WildFire](#) machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.

[Cortex Cloud](#) customers can better protect their cloud infrastructure from the topics discussed within this article through the proper placement of Cortex Cloud [XDR endpoint agent](#) and [serverless agents](#) within their cloud environment. Designed to protect a cloud's posture and runtime operations against these threats, Cortex Cloud helps detect and prevent the malicious operations or configuration alterations or exploitations discussed within this article.

[Cortex XDR](#) and [XSIAM](#) help to prevent the threats described in this blog, by employing the [Malware Prevention Engine](#). This approach combines several layers of protection, including [WildFire](#), Behavioral Threat Protection and the Local Analysis module, designed to prevent both known and unknown malware from causing harm to endpoints.

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107
- South Korea: +82.080.467.8774

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

Indicators of Compromise

Host Based

Important note: The following files are not malicious, but they are indicators because they were used during the attack.

SHA256 hash:

- 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
- Filename: psexec.exe
- File description: Sysinternals PsExec — remote execution / lateral movement tool (observed downloaded from Sysinternals).

SHA256 hash:

- 996e68f2fe1c8bb091f34e9bf39fd34d95c3e21508def1f54098a1874bfb825e
- Filename: chisel.exe
- File description: Chisel — SSH/HTTPS tunneling tool (persistence via SSH tunnel observed).

SHA256 hash:

- 6784e652f304bf8e43b42c29ad8dd146dd384fa9536b9c6640dfbc370c3e78de
- Filename: s3browser-12-6-1.exe
- File description: S3 Browser client — used to upload files to S3 (used for exfiltration attempts).

SHA256 hash:

- e451287843b3927c6046eaabd3e22b929bc1f445eec23a73b1398b115d02e4fb
- Filename: ADEplorer64.exe
- File description: ADEplorer (Sysinternals) — Active Directory data browsing tool.

SHA256 hash:

- 088f2aced9ed60c2ce853b065f57691403459e1e0d167891d6849e1b58228173
- Filename: goon.zip
- File description: Archive containing attacker tools (observed in S3 bucket).

SHA256 hash:

- 6e2c39d0c00a6a8eef33f9670f941a88c957d3c1e9496392beedc98af14269a2
- Filename: OfficeSetup.exe
- File description: Microsoft Office installer/setup executable (observed use by the attackers while attempting to access mailboxes/PSTs).

Network Based

IP Address or Domain	Description
----------------------	-------------

162.125.3[.]18	Associated with Dropbox — destination IP address observed in firewall logs from the attackers' VM
104.16.100[.]29	Associated with Dropbox — destination IP address observed in firewall logs from the attackers' VM
upload[.]je	Online cloud storage
uploadnow[.]io	Online cloud storage
limewire[.]com	Online cloud storage
we[.]tl	Online cloud storage
s3browser[.]com	S3 browser, used for exfiltration
sean-referrals-commissions-electricity.trycloudflare[.]com	Online cloud storage
fast[.]com	Used by attackers to check the internet speed
filetransfer[.]io	Online cloud storage
filebin[.]io	Online cloud storage

Additional Resources

[Muddled Libra Threat Assessment: Further-Reaching, Faster, More Impactful](#) – Unit 42, Palo Alto Networks