Threat Group Assessment: Muddled Libra (Updated)

unit42.paloaltonetworks.com/muddled-libra/

Kristopher Russo, Austin Dever, Amer Elsad September 15, 2023

By Kristopher Russo, Austin Dever and Amer Elsad

September 15, 2023 at 6:00 AM

Category: Threat Advisory/Analysis, Threat Briefs and Assessments

Tags: 0ktapus, Advanced URL Filtering, ALPHV, app-ID, BlackCat ransomware, Cortex XDR, Cortex XSIAM, Cortex XSOAR, DNS security, incident response, MITRE, Muddled Libra, next-generation firewall, Phishing, Scatter Swine, Scattered Spider, social engineering

This post is also available in: 日本語 (Japanese)

Executive Summary

At the intersection of devious social engineering and nimble technology adaptation stands Muddled Libra. With an intimate knowledge of enterprise information technology, this threat group presents a significant risk even to organizations with well-developed legacy cyber defenses.

Muddled Libra is a methodical adversary that poses a substantial threat to organizations in the software automation, BPO, telecommunications and technology industries.

Unit 42 researchers and responders have investigated more than half a dozen interrelated incidents from mid-2022 through early 2023, which we've attributed to the threat group Muddled Libra. This threat group favors targeting large outsourcing firms serving high-value cryptocurrency institutions and individuals. Thwarting Muddled Libra requires a combination of tight security controls, diligent security awareness training and vigilant monitoring.

Palo Alto Networks customers receive protection from the threats described in this blog through a modern security architecture built around Cortex XSIAM in concert with Cortex XDR. The Advanced URL Filtering and DNS Security Cloud-Delivered Security Services can help protect against command and control (C2) infrastructure, while App-ID can limit anonymization services allowed to connect to the network.

Update

As of Sept. 15, 2023, the Unit 42 team has been involved in several additional IR cases involving Muddled Libra. We've observed additional tradecraft used by these threat actors that warranted an update to our existing research.

Muddled Libra's tactics can be fluid, adapting quickly to a target environment. They continue to use social engineering as their primary modus operandi, targeting a company's IT help support desk. For example, in under a few minutes, these threat actors successfully changed an account password and later reset the victim's MFA to gain access to their networks.

One noticeable change of TTP is the heavy use of anonymizing proxy services. Attackers are using these proxy services to obscure their IP addresses and appear to be in a local geographic area.

In the cases we've recently been involved with, we observed Muddled Libra performing the following activities:

- Using NSOCKS and TrueSocks proxy services
- Creating email rules to forward emails from specific security vendors to the actors to monitor communications and those helping in the investigation
- Deploying a custom virtual machine into the environment
- Using an open-source rootkit, bedevil (bdvl) to target VMware vCenter servers
- Gaining administrative permissions

We also believe that members of Muddled Libra speak English as a first language, which provides them greater ability to conduct their social engineering attacks with other English speakers. The targets we've observed seem to be primarily in the U.S.

Since our recent research publication, Muddled Libra has been associated with the BlackCat (aka ALPHV) ransomware group and we believe they are an affiliate. BlackCat is considered one of the most active and persistent ransomware groups in the last 12 months. We have

seen at least 316 incidents posted on the BlackCat leak sites in the previous 12 months. BlackCat gives affiliates access to their kit, which includes the compiled ransomware binaries, support, negotiations and access to their leak site.

Related Unit 42 Topics	**Muddled Libra** (related to **Scattered Spider**, **Scatter Swine**), **0ktapus**

Threat Overview

The attack style defining Muddled Libra appeared on the cybersecurity radar in late 2022 with the release of the 0ktapus phishing kit, which offered a prebuilt hosting framework and bundled templates. With large numbers of realistic fake authentication portals and targeted smishing, attackers were able to quickly gather credentials and multifactor authentication MFA codes.

The speed and breadth of these attacks caught many defenders off guard. While smishing is not new, the 0ktapus framework commoditized the establishment of a normally complex infrastructure in a way that granted even low-skilled attackers a high success rate.

These features included prebuilt templates and a built-in C2 channel via Telegram, all for a cost of only a few hundred US dollars. This improvement in functionality led to cybercriminals launching a massive attack campaign targeting a wide range of organizations.

The sheer number of targets being hit with this kit has created a fair amount of confusion in the research community about attributing these attacks. Previous reporting by Group-IB, CrowdStrike and Okta has documented and mapped many of these attacks to the following intrusion groups: 0ktapus, Scattered Spider and Scatter Swine. While these have been treated in the media as three names for one group, in actuality, it's likely multiple actors using a common toolkit. Muddled Libra is a subset of these actors.

During the Unit 42 incident response investigations, we identified several cases with overlapping trade craft. This indicated a subset of the previously mentioned groups focusing on a complex series of supply chain attacks, ultimately leading to high-value cryptocurrency targets.

Defining characteristics of Muddled Libra include the following:

- Using the 0ktapus phishing kit
- Long-term persistence
- Nondestructive presence
- Persistent targeting of the business process outsourcing (BPO) industry
- Data theft
- Use of compromised infrastructure in downstream attacks

Muddled Libra investigations demonstrate the use of an unusually large attack toolkit. Their arsenal ranges from hands-on social engineering and smishing attacks to proficiency with niche penetration testing and forensics tools, giving this threat group an edge over even a robust and modern cyber defense plan.

In the incidents the Unit 42 team has investigated, Muddled Libra has been methodical in pursuing their goals and highly flexible with their attack strategies. When an attack path is blocked, they have either rapidly pivoted to another vector or modified the environment to allow their favored path.

The Muddled Libra threat group has also repeatedly demonstrated a strong understanding of the modern incident response (IR) framework. This knowledge allows them to continue progressing toward their goals even as incident responders attempt to expel them from an environment. Once established, this threat group is difficult to eradicate.

Muddled Libra has shown a penchant for targeting a victim’s downstream customers using stolen data and, if allowed, they will return repeatedly to the well to refresh their stolen dataset. Using this stolen data, the threat actor has the ability to return to prior victims even after initial incident response. This demonstrates the attacker’s tenacity even after initially being discovered.

Furthermore, Muddled Libra has appeared to have clear goals for their breaches versus just capitalizing on opportunistic access. They've rapidly sought and stolen information on downstream client environments and then used it to pivot into those environments. They have demonstrated a strong understanding of their victims' high-value clients and what information would be most useful for follow-on attacks.

Attack Chain

While each incident is unique, Unit 42 researchers have identified enough commonalities in tactics, techniques and procedures (TTPs) to attribute multiple incidents to Muddled Libra. The attack chain is shown in Figure 1.

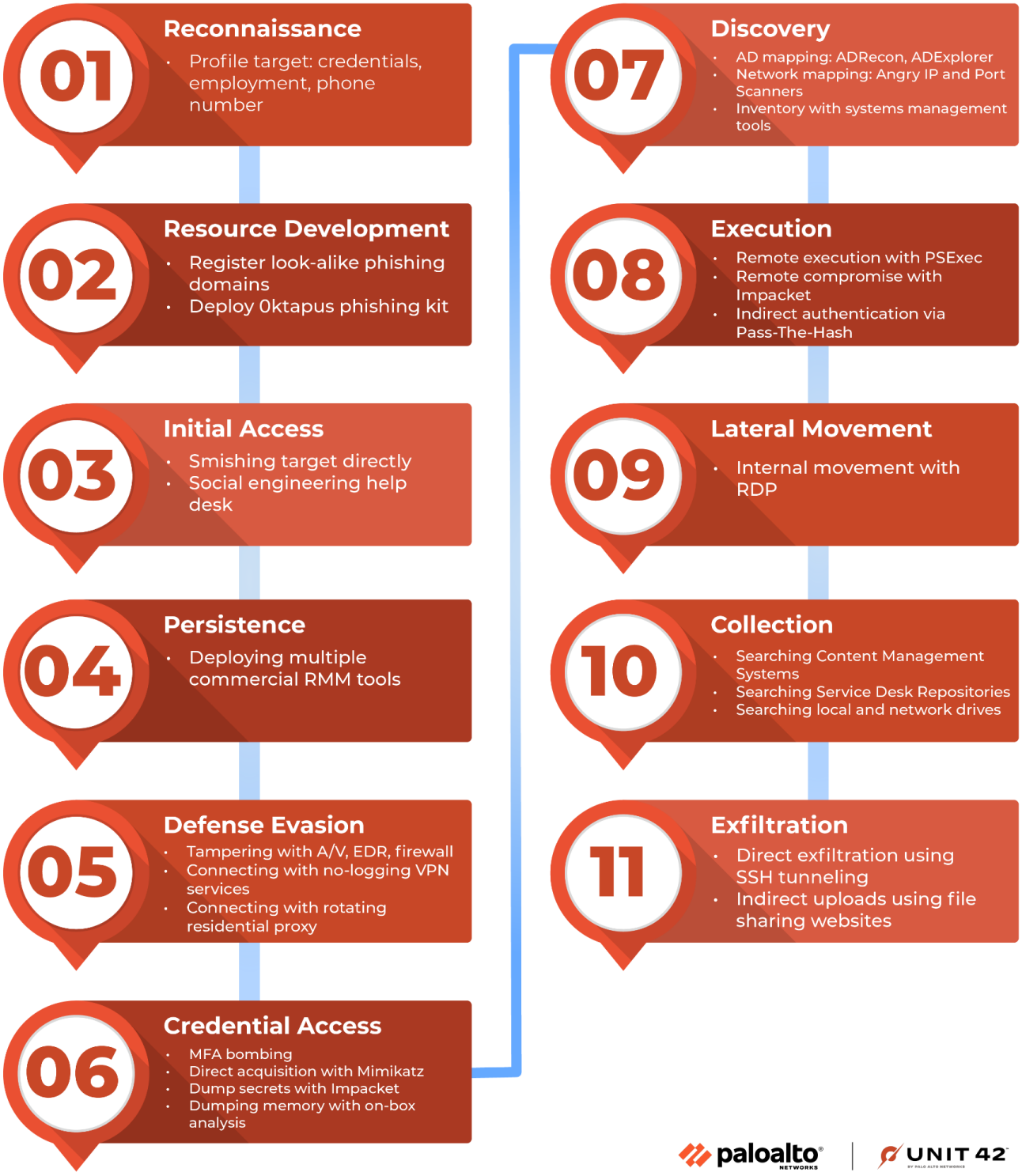

Figure 1. Muddled Libra attack chain.

We have mapped these to the MITRE ATT&CK framework, which is summarized below.

Reconnaissance

Muddled Libra has consistently demonstrated an intimate knowledge of targeted organizations, including employee lists, job roles and cellular phone numbers. In some instances, this data was likely obtained during earlier breaches against upstream targets.

Threat actors also frequently obtain information packs from illicit data brokers such as the now-defunct Genesis and Russian Markets. This data is typically harvested from infected devices, both corporate and personal, using malware such as RedLine stealer.

With the early advent of bring your own device (BYOD) policies, followed by the popularity of hybrid work solutions, corporate data and credentials are frequently used and cached on personal devices. Decentralizing the management and protection of IT assets creates a lucrative targeting opportunity for information-stealing malware.

Resource Development

Lookalike domains used in smishing attacks are a classic hallmark for Muddled Libra. This tactic is effective since mobile devices frequently truncate links in SMS messages.

Early clusters of attacks attributed to the 0ktapus campaign consistently used domains registered via Porkbun or Namecheap and hosted on Digital Ocean infrastructure. These domains tended to be short-lived, used only during the initial access phase, then quickly taken down.

In most investigations, Unit 42 noted the use of the 0ktapus phishing kit for harvesting credentials. Group-IB has well documented this versatile kit, which is widely available in the criminal underground. It requires little skill to stand up and configure, making it an ideal tool for highly targeted smishing attacks.

Initial Access

In all incidents where Unit 42 could determine an initial access vector, smishing and/or helpdesk social engineering was involved. In most incidents, the threat actor sent a lure message directly to the targeted employees' cellphones claiming they needed to update account information or reauthenticate to a corporate application. Messages contained a link to a spoofed corporate domain designed to emulate a familiar login page.

Persistence

Muddled Libra was particularly focused on maintaining access to targeted environments. While it is common for threat actors to use a free or demo version of a remote monitoring and management (RMM) tool during intrusions, Muddled Libra often installed half a dozen or more of these utilities. They did this to ensure that even if one were discovered, they would maintain a backdoor into the environment.

Using commercial RMM tools is particularly problematic as these tools are legitimate, business-critical applications that Muddled Libra is abusing. They could be present legitimately within the organization and defenders should weigh the risks of an outright block

versus carefully monitoring their use. Observed tools included Zoho Assist, AnyDesk, Splashtop, TeamViewer, ITarian, FleetDeck, ASG Remote Desktop, RustDesk and ManageEngine RMM.

None of these tools are inherently malicious and are frequently used in the day-to-day administration of many enterprise networks. Unit 42 recommends organizations block by signer any RMM tools that are not sanctioned for use within the enterprise.

Defense Evasion

Demonstrating proficiency with various security controls, Muddled Libra evaded common defenses.

Their actions included the following:

- Disabling antivirus and host-based firewalls
- Attempting to delete firewall profiles
- Creating defender exclusions
- Deactivating or uninstalling EDR and other monitoring products

Attackers also re-enabled and used existing Active Directory accounts to avoid triggering common security information and event management (SIEM) monitoring rules. They were also observed operating within endpoint detection and response (EDR) administrative consoles to clear alerts.

Muddled Libra was careful with operational security, consistently using commercial virtual private network (VPN) services to obscure their geographic location and attempt to blend in with legitimate traffic. The Mullvad VPN was preferred in most incidents Unit 42 researchers investigated, but multiple other vendors were also observed, such as ExpressVPN, NordVPN, Ultrasurf, Easy VPN and ZenMate.

Unit 42 researchers also observed the usage of rotating residential proxy services as well. As reported by Brian Krebs in 2021, residential proxy services typically hide their code inside of browser extensions, allowing operators to lease out residential connections for legitimate and malicious use alike.

Credential Access

Once the credentials to be used for initial access were captured, the attacker took one of two paths. In one case they continued with the authentication process from a machine they controlled and requested a multi-factor authentication (MFA) code immediately. In the other case, they later generated an endless string of MFA prompts until the user accepted one out of fatigue or frustration (aka MFA bombing).

In cases where MFA bombing was unsuccessful, the threat actor contacted the organization's help desk claiming to be the victim. They would then state that their phone was inoperable or misplaced, and would request to enroll a new, attacker-controlled MFA authentication device.

Muddled Libra's social engineering success is notable. Across many of our cases, the group demonstrated an unusually high degree of comfort engaging both the help desk and other employees over the phone, convincing them to engage in unsafe actions.

After establishing a foothold, Muddled Libra moved quickly to elevate access. Standard credential-stealing tools employed in this phase included Mimikatz, ProcDump, DCSync, Raccoon Stealer and LAPSToolkit. When the group was unable to quickly locate elevated credentials, they turned to Impacket, MIT Kerberos Ticket Manager and NTLM Encoder/Decoder.

In some incidents, Muddled Libra took the unusual step of employing specialized tools to directly search memory contents for credentials using MAGNET RAM Capture and Volatility. As these are legitimate forensics tools that Muddled Libra is abusing, defenders should carefully consider the downsides to blocking them, including the possibility of security team activity generating false positive alerts.

This raises an important point for defenders. Even though user accounts might be protected through privileged access management, endpoints often have elevated credentials cached for system management or to run services. Care should be taken to ensure that privileged credentials only have the permissions necessary to perform their intended functions and that they are closely monitored for deviations from normal behavior.

Discovery

Muddled Libra's discovery methods were consistent from case to case. In our investigations, the group used well-known, legitimate penetration testing tools to map the environment and identify targets of interest. Their toolkit included SharpHound, ADRecon, AD Explorer, Angry IP Scanner, Angry Port Scanner and CIMplant.

Muddled Libra also proved proficient with commercial systems administration tools such as ManageEngine, LANDESK and PDQ Inventory for discovery and automation. VMware PowerCLI and RVTools were also used in virtual environments.

Defenders should be vigilant in identifying unsanctioned network scanning and unusual rapid access to multiple systems or access that crosses logical business segments.

Execution

Across our investigations, Muddled Libra appeared primarily interested in data and credential theft, and we infrequently saw remote execution. When needed, the group accomplished execution with Sysinternals PsExec or Impacket. Captured credentials or authentication hashes were used for privilege elevation.

Lateral Movement

For lateral movement, Muddled Libra preferred to use remote desktop protocol (RDP) from compromised beachhead boxes. This approach helped to minimize discoverable external network artifacts in logs that could alert defenders and help investigators with attribution.

Collection

Muddled Libra appeared familiar with typical enterprise data management. They successfully located sensitive data on the victim's machines in a wide range of common data repositories, both structured and unstructured, including the following:

- Confluence
- Git
- Elastic
- Microsoft Office 365 suite (e.g., SharePoint, Outlook)
- Internal messaging platforms

They also located data in the victim's environment from common service desk applications like Zendesk and Jira. Mined data included credentials for further compromise and they directly targeted sensitive and confidential information.

Unit 42 researchers also observed the use of the open-source data mining tool Snaffler and native tools to search registries, local drives, and network shares for keywords like *password*, and securestring. Compromised data was then staged and archived for exfiltration using WinRAR or PeaZip.

Defenders should regularly perform keyword searches in their own environments to identify improperly stored data and credentials as part of a broader data management and classification strategy.

Exfiltration

In several cases, Muddled Libra attempted to establish reverse proxy shells or secure shell (SSH) tunnels for command and control or exfiltration. Muddled Libra also used common file transfer sites such as put[.]io, transfer[.]sh, wasabi[.]com or gofile[.]io to both exfiltrate data and pull down attack tools. We also observed the use of Cyberduck as a file transfer agent.

Impact

Impact directly observed by Unit 42 was some combination of the theft of sensitive data and/or Muddled Libra leveraging trusted organizational infrastructure for follow-on attacks on downstream customers.

Conclusion and Mitigations

Muddled Libra is a methodical adversary that poses a substantial threat to organizations in the software automation, BPO, telecommunications and technology industries. They are proficient in a range of security disciplines, able to thrive in relatively secure environments and execute rapidly to complete devastating attack chains.

Muddled Libra doesn't bring anything new to the table except for the uncanny knack of stringing together weaknesses to disastrous effect. Defenders must combine cutting-edge technology and comprehensive security hygiene, as well as diligent monitoring of external threats and internal events. The high-stakes risk of loss of internal and customer data is a strong incentive to modernize information security programs.

In addition to the mitigation recommendations included in the Attack Chain subsections above, we recommend organizations:

- Implement MFA and single sign-on (SSO) wherever possible – preferably Fast Identity Online (FIDO). In the cases we investigated, Muddled Libra was most successful when they convinced employees to help them bypass MFA. When they were unable to do so, they appeared to move onto other targets.
- Defenders should also consider how best to implement security alerting and account lockout on repeated MFA failures.
- Implement comprehensive user awareness training. Muddled Libra is heavily focused on social engineering both help desk and other employees via phone and SMS. Employee training on identifying suspicious non-email based outreach is critical.
- In case of a breach, assume this threat actor knows the modern IR playbook. Consider setting up out-of-band response mechanisms.
- Ensure credential hygiene is up to date. Only grant access when and for as long as necessary.
- Monitoring and managing access to critical defenses and controls is critical to defending against skilled attackers. Rights should be restricted to only what is necessary for each job function. Identity threat detection and response (ITDR) tools such as Cortex XDR and Cortex XSIAM should be used to monitor for abnormal behavior.
- Defenders should limit anonymization services allowed to connect to the network, ideally at the firewall by App-ID.

To defend against the threats described in this blog, Palo Alto Networks further recommends organizations employ the following capabilities:

- Network security: delivered through a Next-Generation Firewall (NGFW) configured with machine learning enabled, and best-in-class, cloud-delivered security services. This includes, for example, threat prevention, URL filtering, DNS security and a malware prevention engine capable of identifying and blocking malicious samples and infrastructure.
- Endpoint security: delivered through an XDR solution that can identify malicious code through the use of advanced machine learning and behavioral analytics. This solution should be configured to act on and block threats in real time as they are identified.
- Security automation: delivered through an XSOAR or XSIAM solution capable of providing SOC analysts with a comprehensive understanding of the threat derived by stitching together data obtained from endpoints, network, cloud and identity systems.

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: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Indicators of Compromise

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, 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.

IPs observed during this activity

- 104.247.82[.]11
- 105.101.56[.]49
- 105.158.12[.]236
- 134.209.48[.]68
- 137.220.61[.]53
- 138.68.27[.]0
- 146.190.44[.]66
- 149.28.125[.]96
- 157.245.4[.]113
- 159.223.208[.]47
- 159.223.238[.]0
- 162.19.135[.]215
- 164.92.234[.]104
- 165.22.201[.]77

- 167.99.221[.]10
- 172.96.11[.]245
- 185.56.80[.]28
- 188.166.92[.]55
- 193.149.129[.]177
- 207.148.0[.]54
- 213.226.123[.]104
- 35.175.153[.]217
- 45.156.85[.]140
- 45.32.221[.]250
- 64.227.30[.]114
- 79.137.196[.]160
- 92.99.114[.]231

Additional Resources

Updated September 15, 2023, at 4:40 p.m. PT to add new TTPs observed from IR cases.