Muddled Libra Threat Assessment: Further-Reaching, Faster, More Impactful

Executive Summary

Unit 42 has tracked and responded to several waves of intrusion operations conducted by the cybercrime group we track as Muddled Libra (aka Scattered Spider, UNC3944) across different sectors in recent months. This article contains observations on Muddled Libra thus far in 2025 based on our incident response insights. We share defensive recommendations that we have seen organizations use successfully against the threat. We also include what's likely next for this prolific adversary.

Muddled Libra's recent activity follows a series of international law enforcement operations aimed at disrupting the threat group in mid-to-late 2024, including federal charges levied against five suspected members in November 2024. Since that time, Muddled Libra returned with enhanced capabilities, evolving its tradecraft to be further-reaching, faster and more impactful.

Palo Alto Networks customers are better protected from the threats described in this article 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.

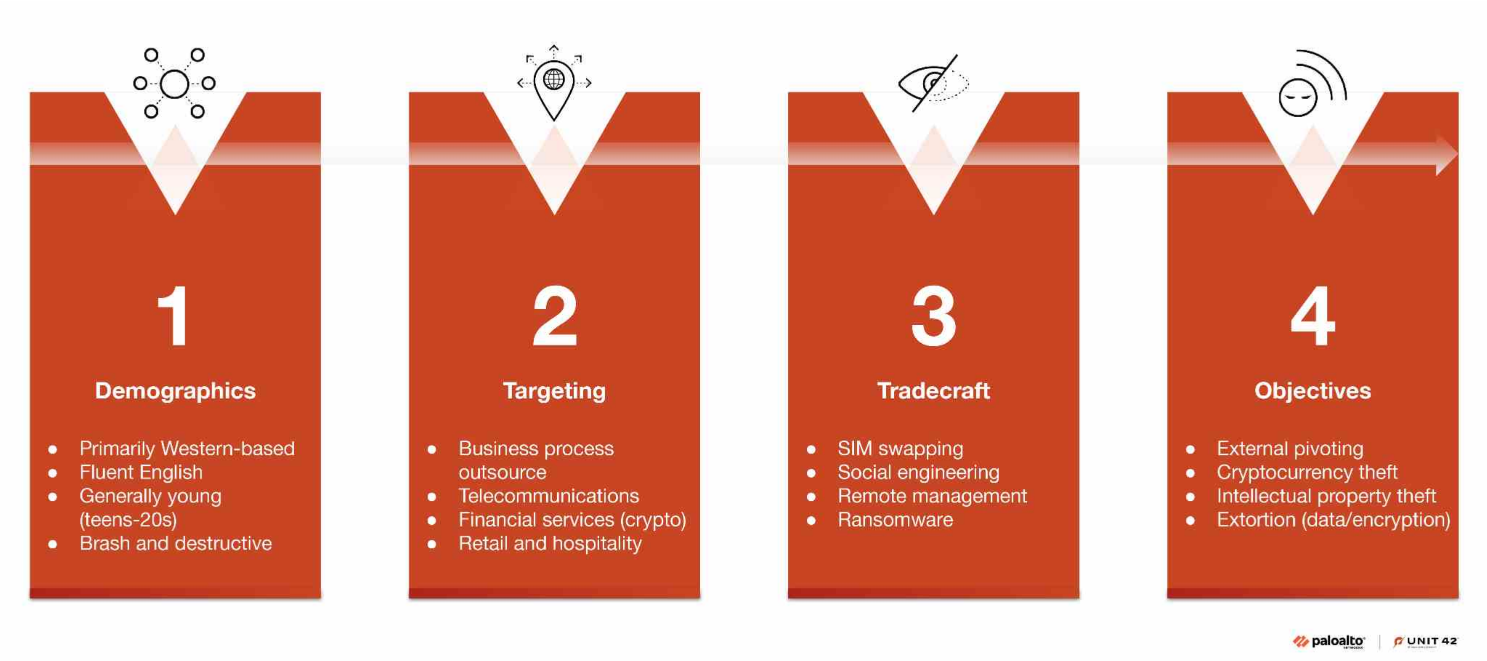
If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

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

Muddled Libra Threat Overview

As documented in prior Unit 42 publications on Muddled Libra, this group is highly adept at using various social engineering tactics (e.g., smishing, vishing) to gain initial access to targeted organizations. These activities can include targeting call centers operated by victims, as well as those outsourced to third-party firms (e.g., BPOs, MSPs), expanding the group's range of potential targets.

Attackers from Muddled Libra have become experts at exploiting human psychology via impersonating employees to attempt password and multi-factor authentication (MFA) resets. Figure 1 below further illustrates the composition of Muddled Libra in terms of their demographics, tradecraft, victim targeting and actions on objectives.



1 Demographics

- Primarily Western-based
- Fluent English
- Generally young (teens-20s)
- Brash and destructive

2 Targeting

- Business process outsource
- Telecommunications
- Financial services (crypto)
- Retail and hospitality

3 Tradecraft

- SIM swapping
- Social engineering
- Remote management
- Ransomware

4 Objectives

- External pivoting
- Cryptocurrency theft
- Intellectual property theft
- Extortion (data/encryption)

Figure 1. Muddled Libra threat profile.

While their tradecraft has evolved over time, Muddled Libra continues to minimize the use of malware throughout the attack chain. Whenever possible, they prefer to use a victim’s own assets against them.

Victimology Timeline: Further-Reaching

In 2025, we have observed Muddled Libra intrusion activity in the government, retail, insurance and aviation sectors as shown below in Figure 2. This group has demonstrated a pattern of targeting multiple organizations within the same sector in a relatively short period of time. However, attackers do not strictly follow this pattern and have simultaneously targeted organizations operating in different sectors.

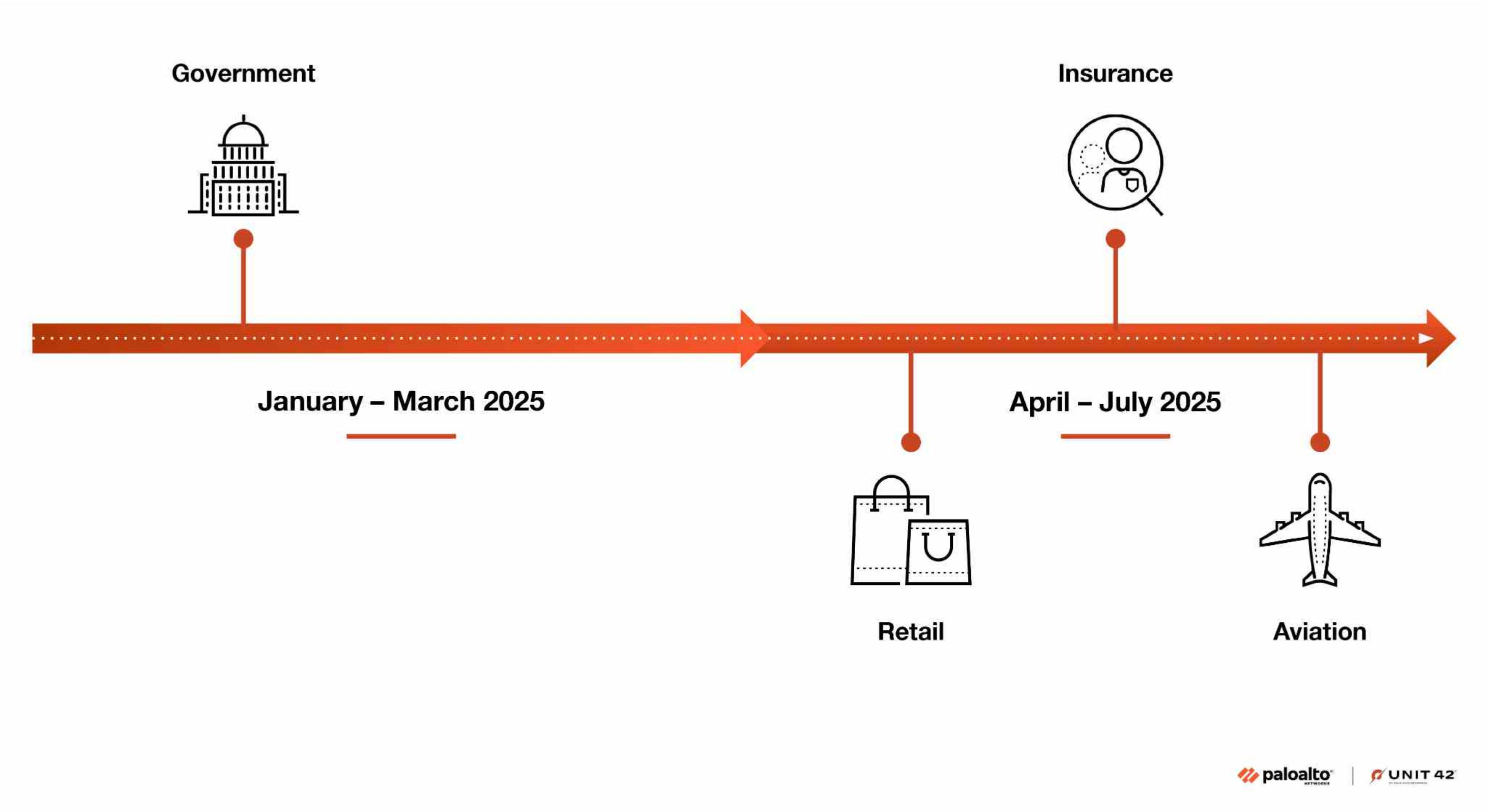


Figure 2. Timeline of Muddled Libra sector targeting in 2025.

Muddled Libra’s Game Plan: Faster

Thus far in 2025 cases, the shift away from smishing and phishing to more direct human interaction, as well as adoption of the ransomware-as-a-service (RaaS) playbook, have drastically shortened the time this actor is in an environment. The average time from initial access to containment was 1 day, 8 hours and 43 minutes.

Since at least April 2025, the group has partnered with the DragonForce RaaS program, operated by the group we track as Slippery Scorpius, to extort victims. In one case, we observed attackers exfiltrating over 100 GB of data during a two-day period, with encryption via DragonForce ransomware deployment.

Figure 3 below illustrates how the group was able to pivot from initial access via social engineering a helpdesk employee, to escalating privileges, to domain administrator rights in about 40 minutes, as previously noted in our 2025 Global Incident Response Report.

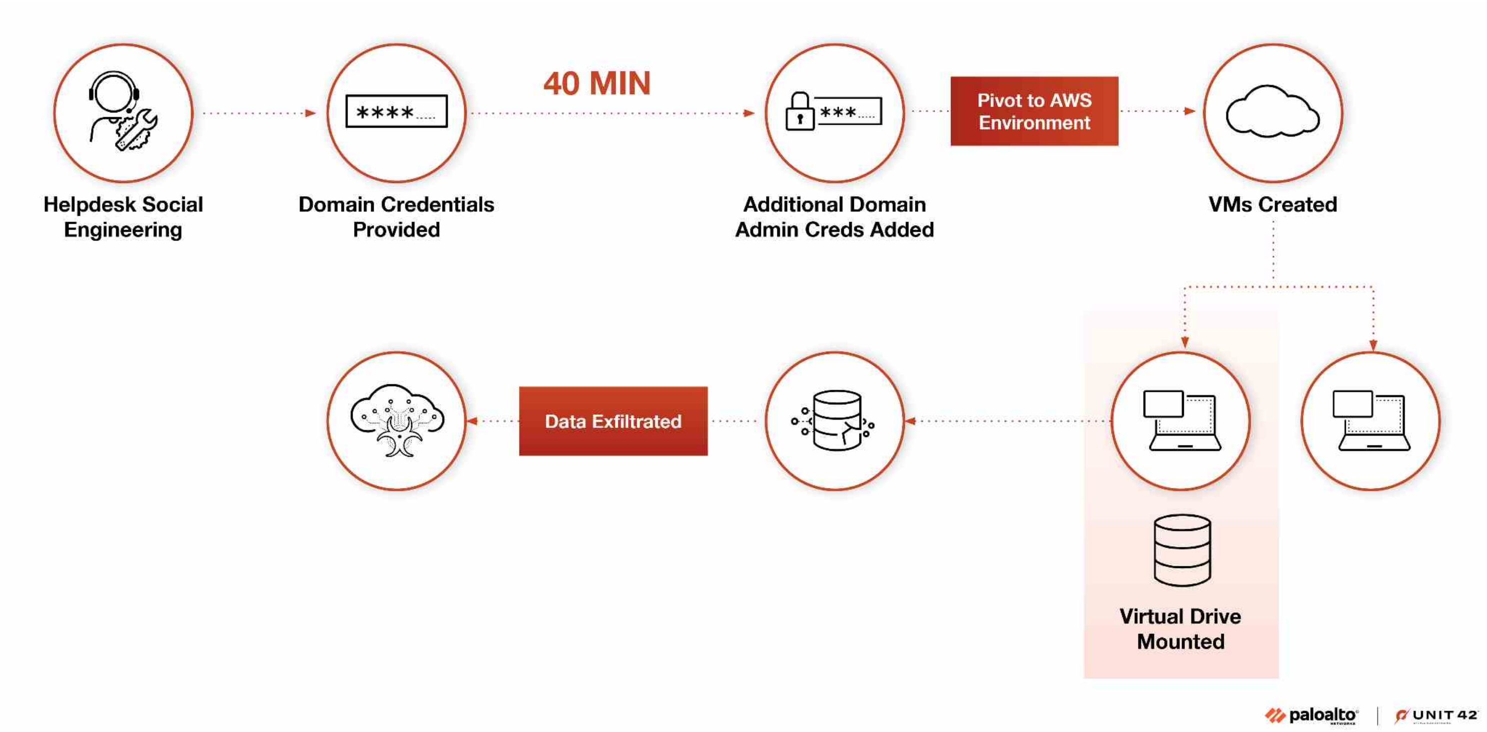
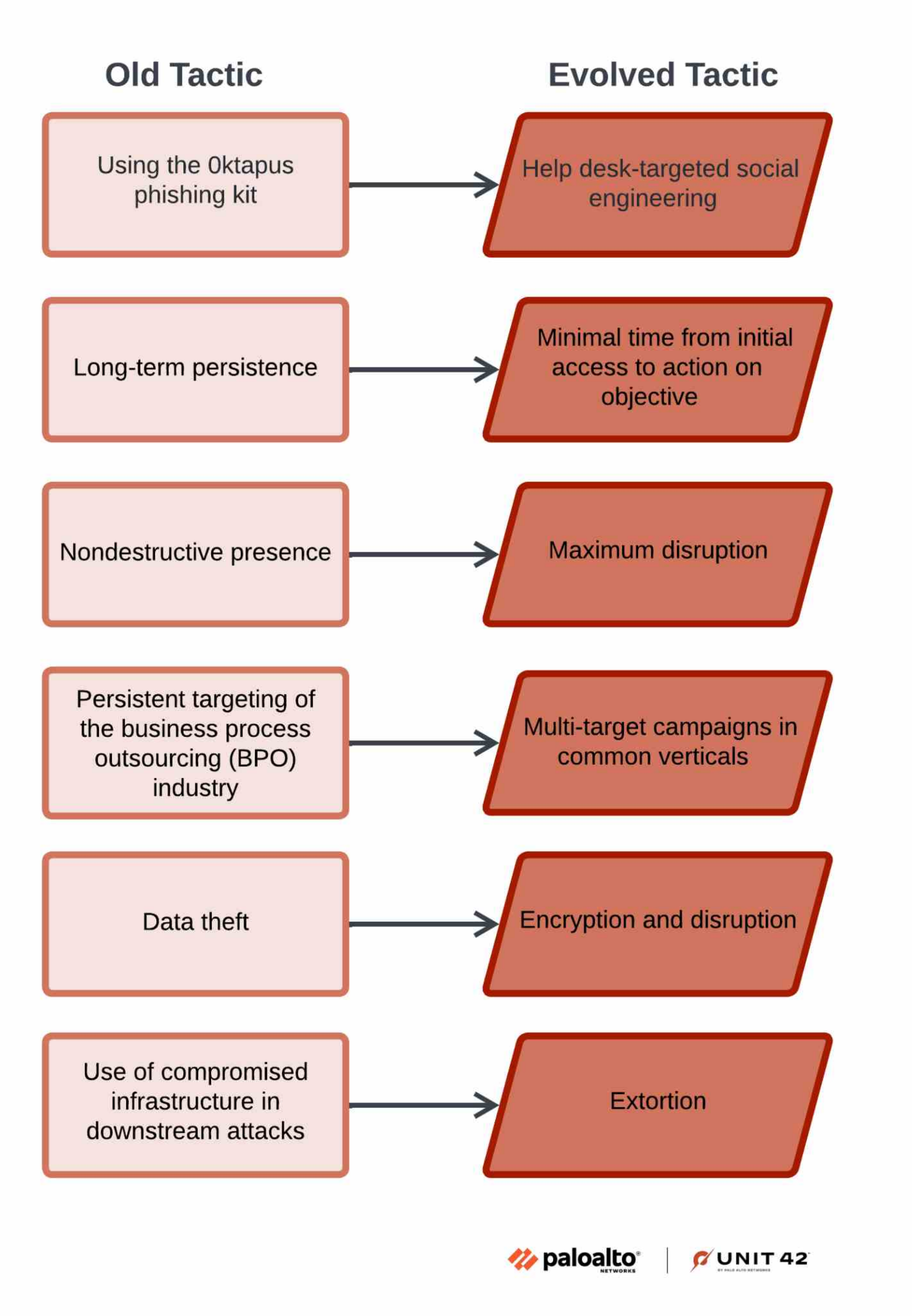


Figure 3. Speed of Muddled Libra intrusion from initial access to domain admin.

Evolution of Muddled Libra: More Impactful

Figure 4 illustrates changes we have observed in Muddled Libra's tradecraft that help make the group more impactful.



Old Tactic	Evolved Tactic
Using the 0ktapus phishing kit	Help desk-targeted social engineering
Long-term persistence	Minimal time from initial access to action on objective
Nondestructive presence	Maximum disruption
Persistent targeting of the business process outsourcing (BPO) industry	Multi-target campaigns in common verticals
Data theft	Encryption and disruption
Use of compromised infrastructure in downstream attacks	Extortion

Figure 4. Muddled Libra tradecraft evolution.

Some of our notable observations are detailed in the sections below.

Initial access

(T1566.004)

Shift to voice-based phishing (aka vishing) as a primary social engineering technique to manipulate IT help desk personnel into resetting credentials and MFA for staff that attackers are attempting to impersonate; over 70% of the numbers used by this group in 2025 leveraged Google Voice as a Voice Over Internet Protocol (VoIP) service.

As an example, Muddled Libra typically calls into an organization’s help desk pretending to be a user that has lost access to their MFA device. By preying on help desk associates' natural tendency to want to be helpful, the threat actors manipulate them into bypassing organizational authentication controls and resetting both an end user’s credentials and MFA method. Another example involves calling a victim directly while claiming to be from the organization’s help desk. In this case, the threat actors manipulate the victim into launching or downloading remote management software and then proceed with the attack from the victim’s desktop.

Persistence and Lateral Movement

Using various remote monitoring and management (RMM) tools that enable re-entry if the threat actors are discovered. Frequent targeting of existing systems management tools and even endpoint detection and response (EDR) platforms, in addition to hypervisors and cloud management tools.

Credential Access

(T1003.003, T1555.005)

Dumping credentials from password vaults including NTDS.dit to achieve full enterprise password stores and Active Directory compromise, respectively.

Collection

(T1114.002, T1213.002)

Accessing victim Microsoft 365 and SharePoint instances as a means of conducting internal reconnaissance.

Exfiltration

(T1567.002)

Transferring stolen data to cloud storage services, including in some cases being sent directly from victims’ environments.

A Tale of Two Victims: Conditional Access Policies

Organizations using Microsoft Entra ID for cloud-based identity and access management (IAM) can significantly disrupt Muddled Libra intrusions by properly implementing Conditional Access Policies (CAPs).

As part of Muddled Libra threat activity, we’ve seen a significant difference in organizations’ ability to slow down attackers post-intrusion and enable more effective containment actions when CAPs are in place, limiting overall impact. In scenarios where victims had not implemented CAPs or they were configured improperly, Muddled Libra could accelerate its operational tempo to deploy ransomware (most recently DragonForce) to extort payment.

Some specific examples of CAPs that were successful in slowing down Muddled Libra include:

- A CAP that prevents unmanaged devices from accessing sensitive resources
- A CAP that enforces employees being on-premises to set up MFA
- A CAP that blocks authenticators based on geographic locations (e.g., countries)
- A CAP that requires MFA to access virtual desktop infrastructure (VDI) and/or virtual private networks (VPN)

Looking Ahead

Based on recent and historical observations of Muddled Libra, we assess with high confidence that this group will continue to play to its strengths in terms of social engineering activities. The group will also continue misusing overly permissive identities within targeted organizations to accomplish its mission objectives.

Additionally, the group is likely to persist in its cloud-first mindset. This means that its prior success in exploiting access within cloud platforms will embolden this trend going forward, especially because many organizations lack proper visibility and necessary controls to monitor and protect these environments.

Furthermore, given Muddled Libra's success in partnering with various RaaS programs, it is unlikely to deviate from this path. These RaaS programs include:

- Akira (Howling Scorpius)
- ALPHV (Ambitious Scorpius)
- DragonForce (Slippery Scorpius)
- Play (Fiddling Scorpius)
- Qilin (Spikey Scorpius)
- RansomHub (Spoiled Scorpius)

Members of this group will likely continue to extort victims and monetize their intrusion operations, as it provides a streamlined process to conduct and profit from such attacks.

Finally, we expect that public and private sector information-sharing concerning Muddled Libra will continue to provide organizations with early indications of intrusion activity. This will help disrupt the group's operations. International law enforcement operations, such as the recent arrests of four individuals connected to the cyberattacks against three UK-based retailers, will hopefully act as a form of deterrence. It should also remind similar cybercrime syndicates that there are consequences for their actions. At its core, cybersecurity is a team sport and we must work collectively to gain a proactive operational advantage against this ever-evolving adversary.

Recommendations

We have a list of prevention, detection and containment measures that organizations should strongly consider implementing to address the evolving threat presented by Muddled Libra. Figure 5 below provides a macro view of these recommendations, with more descriptive measures listed thereafter.

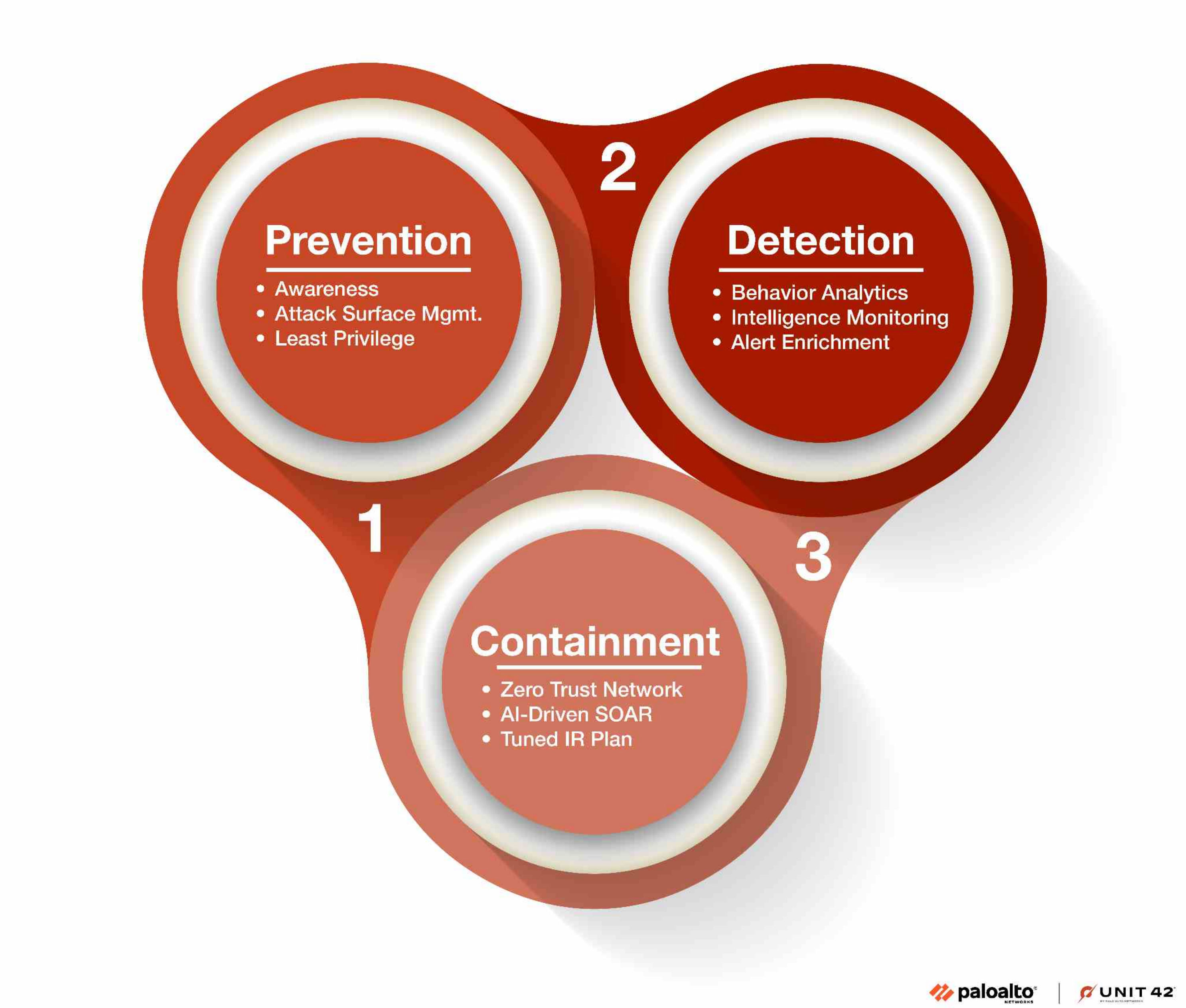


Figure 5. Effective controls to defend against Muddled Libra.

Prevention:

- Provide tailored, intelligence-driven user awareness training, especially for IT support desk personnel to be able to identify potential social engineering (vishing) attempts
- Implement rigorous procedures for resetting account credentials and MFA, including some form of verification such as video identification or supervisor validation
- Implement MFA (non-SMS) and conditional access policies, especially on any remote access portals
- Strictly enforce the principle of least privilege
- Block network traffic by App-ID to file-sharing sites and those providing access to unapproved RMM tools

Detection:

- Identify changes to enterprise IAM infrastructure, such as newly enrolled and connected devices
- Develop robust logging and monitoring capabilities in cloud environments
- Develop logging of and be able to identify suspicious call center activities

Containment:

- Segment and restrict access to virtual resources, including VMs, ESXi hosts and vCenter servers
- Implement out-of-band communication channels in case an adversary is able to compromise traditional mediums (e.g., Slack, Teams)
- Implement a comprehensive incident response plan and strongly consider having an active retainer in place for third-party incident response support

Conclusion

The new era of Muddled Libra has arrived, and activity from this group continues to proliferate.

Palo Alto Networks customers are better protected from the threats described in this article 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.

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: 00080005045107`

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.

Additional References

- Threat Briefing: A Deep Dive Into Muddled Libra - Unit 42, Palo Alto Networks
- Threat Group Assessment: Muddled Libra - Unit 42, Palo Alto Networks
- 2025 Global Incident Response Report - Unit 42, Palo Alto Networks
- Muddled Libra Discussion With Unit 42 Senior Consultant Stephanie Regan – Threat Vector Podcast, Unit 42 on CyberWire Daily
- Exposing Muddled Libra's Meticulous Tactics With Unit 42 Senior Researcher Kristopher Russo – Threat Vector Podcast, Unit 42 on CyberWire Daily
- Muddled Libra's Evolution to the Cloud – Unit 42, Palo Alto Networks