

Attack Vectors at a Glance

Executive Insights from the Unit 42 Incident Response Report

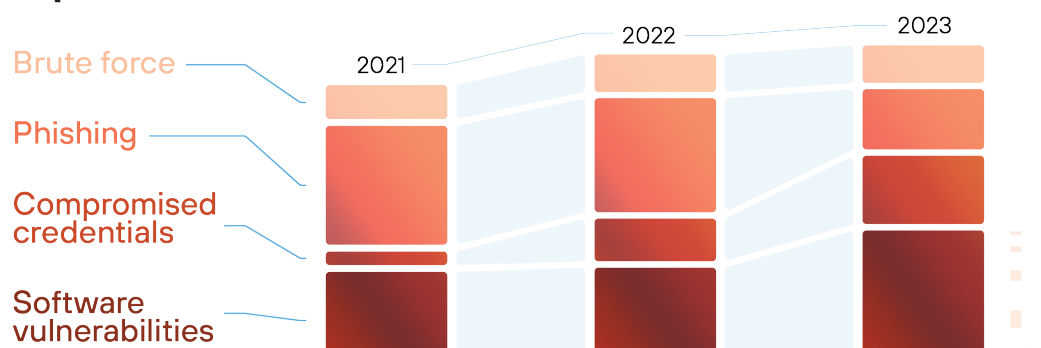
An attack vector is the method an attacker uses to get access to a target environment. The [2024 Incident Response Report](#) details the most exploited attack vectors of the past year. It also spotlights the cybercriminal group known as *Muddled Libra* and analyzes its most successful attack patterns to determine how the most sophisticated attackers may attempt to breach your defenses.

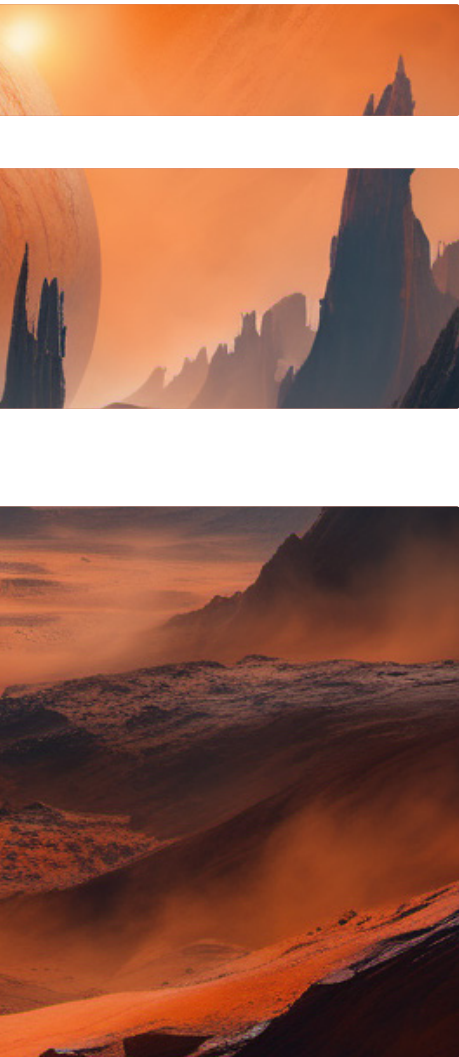
Threat Actors Vs. Attack Vectors

When hardening defenses against cyberattacks, it's important to understand the interplay between the who and the how. While you need to identify the most likely threats to your organization, you also need to identify how threat actors exploit common attack vectors.

Preventing and responding to attacks requires *threat-informed defenses*. By examining threat actors and their behaviors, we're able to identify the most common attack vectors and recommend strategies for securing them. Here's what our experts have seen in this year's Incident Response Report.

Top 4 initial attack vectors



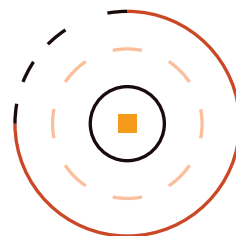


Trending Attack Vectors

Cybercriminals will seek the path of least resistance when infiltrating your organization. While software vulnerabilities continue to provide attackers with alluring entry points, it's important to remember that sophisticated attacks often involve the exploitation of multiple attack vectors.

1. Software Vulnerabilities

In most of the cases we examined, cybercriminals exploited internet-facing applications to gain an initial foothold.



Software vulnerabilities have always been a weak spot for organizations for a few reasons:

- Software vulnerabilities often aren't discovered until they're already being exploited.
- Vendors may not release security updates for software quickly enough.
- Engineers have to test patches in a virtual environment to minimize impact to production, which takes time.

Organized groups like [Muddled Libra](#) have their own research and development teams. They uncover software vulnerabilities and build automated tools for discovering potential targets. Now that they've infused AI into their operations, they find software bugs, locate vulnerable targets, and exploit them on a much greater scale.

Our Recommendation:

Proactive discovery and analysis of your assets – especially those exposed to the internet – is the first step. A tool like [Cortex Xpanse](#) can help you proactively find and fix exposures on your internet-connected assets before attackers can exploit them.

You'll also want to incorporate threat intelligence into your security operations. Your team can subscribe to various threat intel feeds to stay up to date on the latest vulnerability disclosures.

As always, routine testing and implementing patches as quickly as possible will reduce the likelihood that your software will provide an open door for attackers.

2. Stolen Credentials

Think of your cyber environment as a maze of locked doors. Your employees have the keys to unlock these doors. However, the burden of keeping up with those keys and who has them compounds as your company grows.

Attackers like Muddled Libra aren't going to pick your locks when they can steal keys from your employees instead. In the past year, they've successfully employed several tactics:

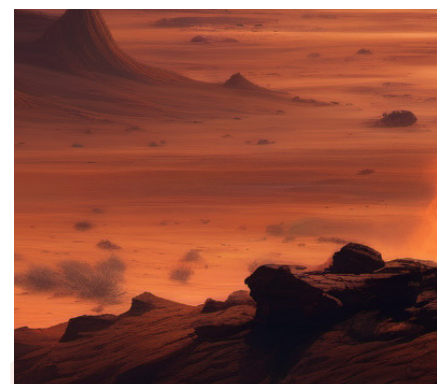
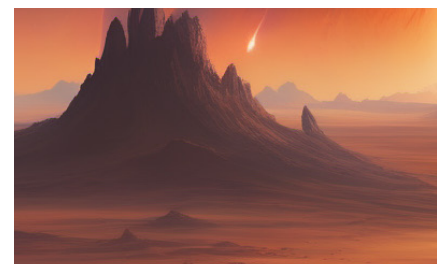
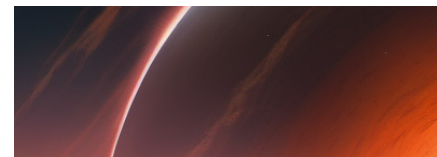
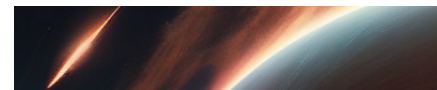
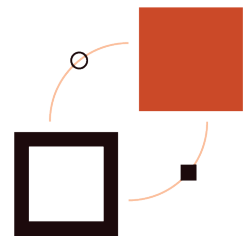
- Social engineering on help-desk employees to gain the credentials of specific users.
- Stealing credentials from individuals and purchasing compromised ones.
- Using malware to steal credentials saved in applications.
- Buying previously stolen credentials from access brokers.

Our Recommendation:

Most importantly, you must implement technologies that can account for human error. Even the best employees have bad days, and your technology should support them when their senses fail. Monitor the traffic on your network for uncommon behavior. Look for [detection and response tools](#) that can answer questions about who, what, when and where attacker activity might be. They should identify anomalous behavior, and consider augmenting them with security [operations tools that integrate and automate](#) your SOC processes.

You should also train your team to detect and respond to social engineering attempts. Unlike many hacker groups, we believe members of Muddled Libra speak English natively. This allows them to more believably pass as a member of your staff in a phishing attempt. Your employees should know what an attempted attack looks like, how to react, and who to contact if they think they've fallen victim.

Multifactor authentication (MFA) can reduce the risk of stolen credentials, but MFA solutions can also be compromised, too. Train your users not to approve MFA requests they didn't solicit and to report lost or stolen devices.

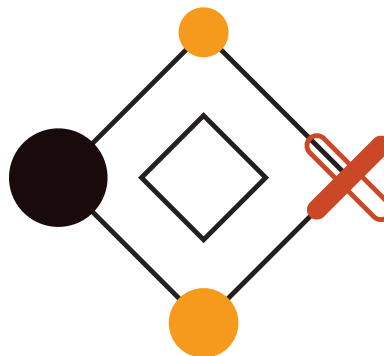


3. Third Parties and Misconfigurations

Third-party vulnerabilities and misconfigurations both stem from a lack of visibility. Muddled Libra and other groups exploit these vectors to gain easy access and move laterally. In contrast to the locked-door analogy, these are doors left ajar.

Third-party vendors often pose a threat because their partner organizations grant them too much trust and access. Defending your organization is hard enough, but incorporating third-party vendors multiplies your attack surface.

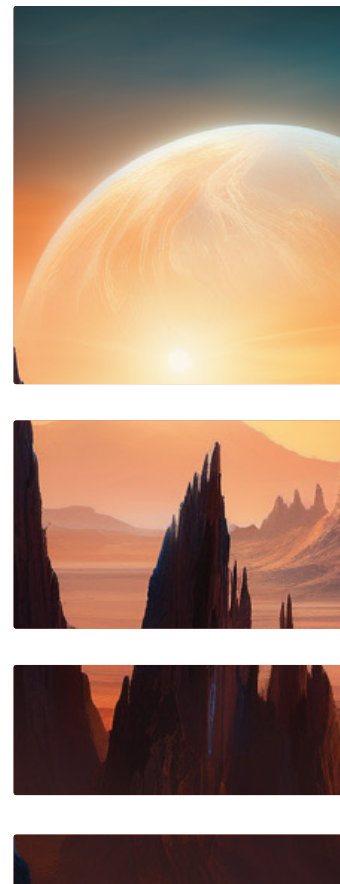
Misconfigurations occur when tools and devices are deployed without documented standards and procedures. They present even greater risk without ongoing monitoring and maintenance to ensure they remain secure. They then become invisible holes in your defenses for attackers to pivot through.



Our Recommendation:

Adopt a [Zero Trust](#) network access framework to mitigate the risk of anyone or anything accessing your organizational resources. Zero Trust isn't a tool. It's a philosophy and a full ecosystem of controls that implement best-practice security across your entire organization.

You should also regularly scan and analyze your organization for misconfigurations that might lead to compromise. While policies should dictate who can add what to the network and how it should be configured, you need technology-based methods to enforce them.



The Bigger Picture

Attack vectors are just one consideration when securing your organization. In many cases, the how can be derived from the who – who you are, how large your organization is, what industry you're in, and who your most likely threat actors are.

We study groups like Muddled Libra and their methodologies so we can better inform you about their activities. The tactics used by well-resourced threat groups represent the attacks that future commodity cybercriminal groups will leverage against people on an automated basis.

Our best advice: don't go at it alone. Security teams should never rely solely on their own security assessments. Talk to Unit 42 and find [a trusted security partner](#) who can identify opportunities for improvement and help you fix them.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>

All other marks mentioned herein may be trademarks of their respective companies.