Identity-based threats

Cisco Talos' findings reveal that threat actors heavily relied on identity-based attacks to power their operations in 2024, from initial access vectors to operational techniques further down the attack chain. We also explore how adversaries are targeting muti-factor authentication (MFA) weaknesses, which is a key way to compromise a user's identity. For further research and analysis, download Talos' full 2024 Year in Review report.

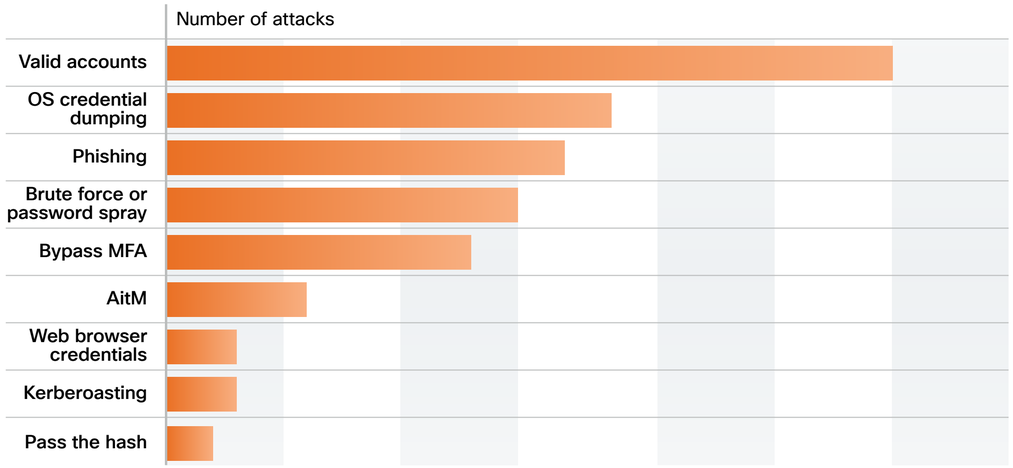
Identity attacks omnipresent throughout the attack chain

The most common tactic Talos Incident Response (IR) observed in engagements was the use of valid accounts — typically seen in the initial access phase — where adversaries obtained and abused credentials of existing accounts to carry out various phases of their operations. OS credential dumping and phishing round out the top three.

Identity in-the-wild: Compromising Active Directory

Attacks targeting Active Directory, a widely used Microsoft service for Windows, accounted for 44 percent of all identity-based attacks in Talos IR incidents. Active Directory holds critical user information like usernames, passwords, and access permissions, making it a gold mine of high-value data for attackers. Moreover, according to a recent U.S. government report, Active Directory is the most widely used authentication and authorization solution in enterprise IT networks globally.

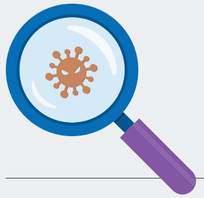
Types of identity attacks observed in Talos IR



Why are we seeing more identity-based attacks?

Growing attack surface

The use of web applications, cloud-based environments, BYOD policies, and SSO solutions have been on the rise in recent years, especially with the normalization of remote work. This, in turn, has increased the number of credential-enabled access points within a network that could be exploited by attackers.



Hard to detect

Many of these attacks leverage legitimate authentication processes, making them hard to detect at the network perimeter. Moreover, once an attacker gains access, malicious activity emanating from a valid user's compromised account is more likely to go unnoticed.

Easy to carry out

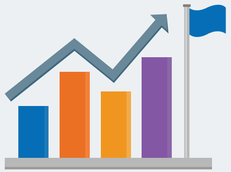
Attacks can easily obtain stolen credentials, often via the dark web and previous data breaches. Additionally, identity-based attacks largely rely on social engineering rather than technically sophisticated means.

Enables other operations

In addition to gaining initial access to a target device, threat actors can continue to use identity attacks throughout their operations to escalate privileges, move laterally, conduct internal social engineering attacks, and more.

Achieves significant access

Using relatively simple means, actors can beat identity-based security challenges and gain access to the Active Directory, where an entire organization's access and permissions are managed; cloud applications that power daily operations; or even IT networks and operational technology (OT) systems-crucial components of any organization's cybersecurity.



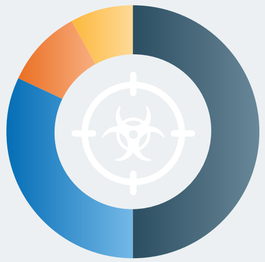
Case study: Active Directory attack

1. Extract local passwords and password hashes within AD database
2. Escalate to privileged admin accounts
3. Reset passwords; create new accounts to maintain persistence
4. Lateral movement to domain controllers and use of Mimikatz
5. Installation of backdoors and other software to maintain persistent access
6. Access backup systems
7. Result in pre-ransomware TTPs which could have eventually led to deployment of ransomware if not actioned swiftly

Identity attacks in 2024

We have seen a strong shift toward identity-based attacks in Talos IR incidents. In 2024, the most common technique used to gain initial access was valid accounts, making this the top access vector for the second consecutive year.

Adversaries' goals in identity attacks



- **50%** Ransomware and pre-ransomware
- **32%** Credential theft for monetization
- **10%** Data theft for future operations
- **8%** Financial fraud

60%

More than half of Talos IR cases had an identity attack component in 2024.

44%

Nearly half of all identity attacks targeted the Active Directory. Another 20% targeted cloud applications.

We frequently observe accounts (i.e., user, admin, and service) with excessive or incorrect privileges, accounts with weak or default passwords, flat network architectures, and missing or misconfigured MFA. Our recommendations for mitigating Active Directory compromises are in line with CISA's strategies to mitigate the 17 most common techniques used by adversaries and malicious actors to compromise Active Directory.

Attacks against MFA

Threat actors capitalize on a variety of MFA weaknesses

Multi-factor authentication (MFA) weakness was the leading security weakness in Talos IR data in 2024, illustrating that it is an enduring trend year over year. Lack of MFA enrollment made up a quarter of the MFA issues observed; however, we saw a variety of other ways in which organizations insufficiently deployed MFA this year, enabling threat actors to gain access to key resources and establish persistence in targeted networks.

MFA attackers go straight for IAM applications

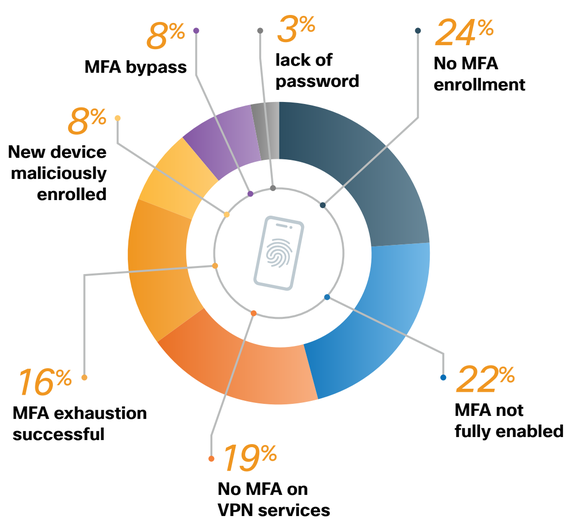
Based on Cisco Duo data, the identity and access management (IAM) applications were most frequently targeted in MFA attacks, accounting for nearly a quarter of related incidents.

High volume, easily preventable spray attacks are most common

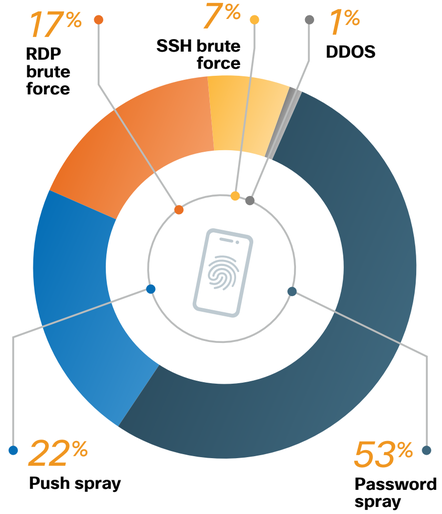
Attackers are probing for organizations lacking or incorrectly configuring MFA. Password spray attacks were the most frequent type of threat Talos IR observed against MFA-protected applications. However, MFA is highly effective at mitigating brute force and password spray attacks due to the additional authentication measure that is required, which often results in lower success rates for these types of campaigns.

Push spray was the second most common attack type. This technique, also known as MFA "bombing" or "fatigue," goes beyond the simple password guessing approach represented by spray attacks.

Observed MFA weaknesses in Talos IR cases



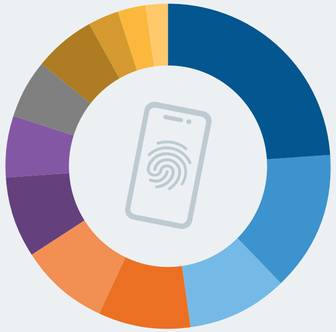
Types of MFA attacks



Though MFA is proven to provide strong security, some organizations may choose not to employ it, given the cost and complexity of knowing which systems and resources to defend with it.

Types of applications targeted in MFA attacks

- **24%** Identity and access management (IAM)
- **14%** Network security
- **10%** Authentication and networking
- **9%** Remote access
- **9%** Application delivery and security
- **8%** Software development kit (SDK)
- **6%** Authentication protocol
- **6%** Authentication and network access control (NAC)
- **6%** Cloud security and authentication
- **3%** Operating system
- **3%** API communication protocol
- **2%** Email and collaboration



MFA in-the-wild: Phishing and device compromise lead to major breach at large university

The following case study is an example of how we see these trends play out in everyday scenarios. In this Talos IR incident, a large university (more than 100,000 users) was the victim of both phishing and device compromise.

Victim: Large university

(100,000+ users)