

2024: **A year of identity attacks**

Looking back on identity attacks in 2024 and what they tell us about how identity-based techniques and tools are evolving.

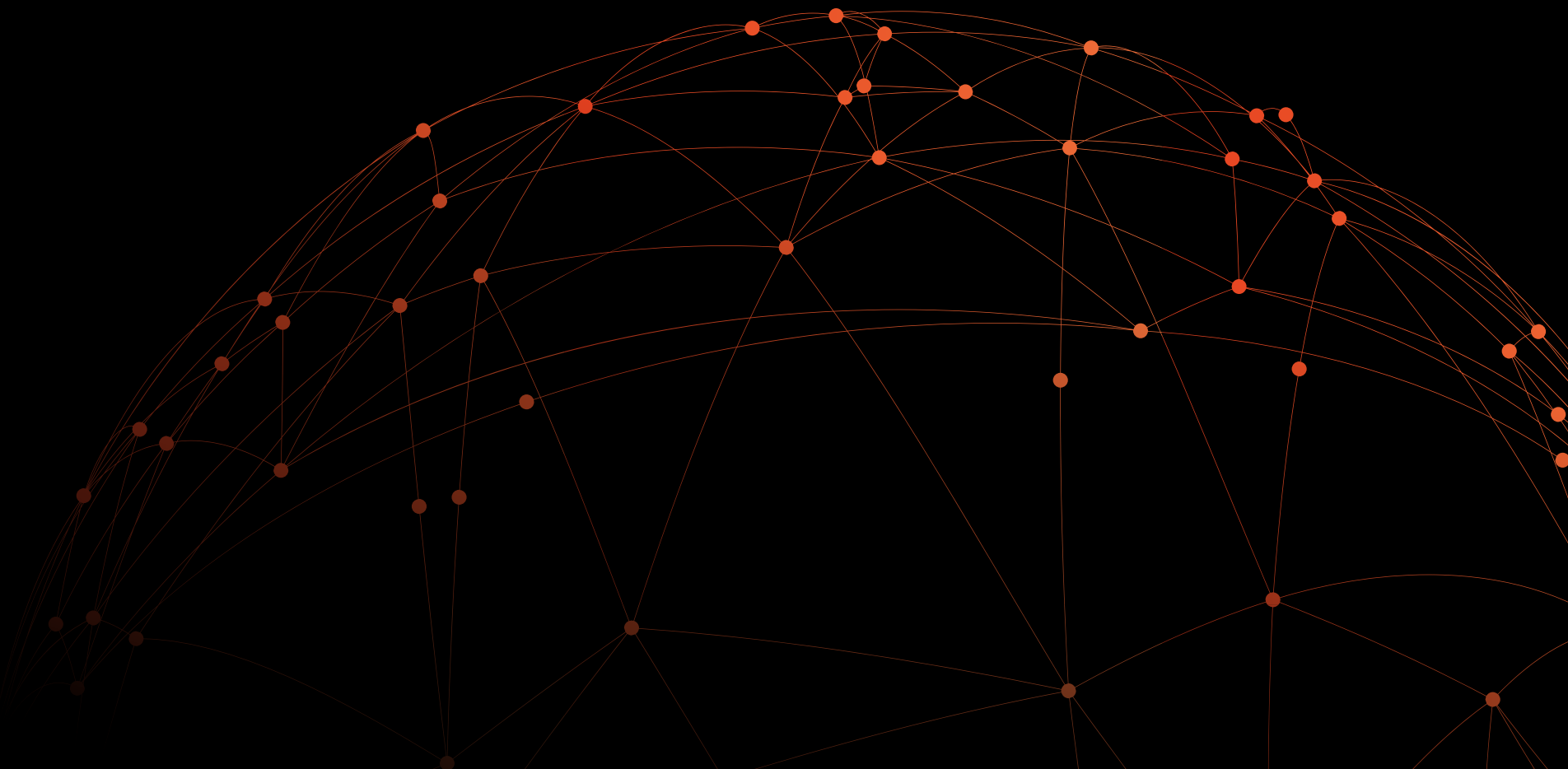
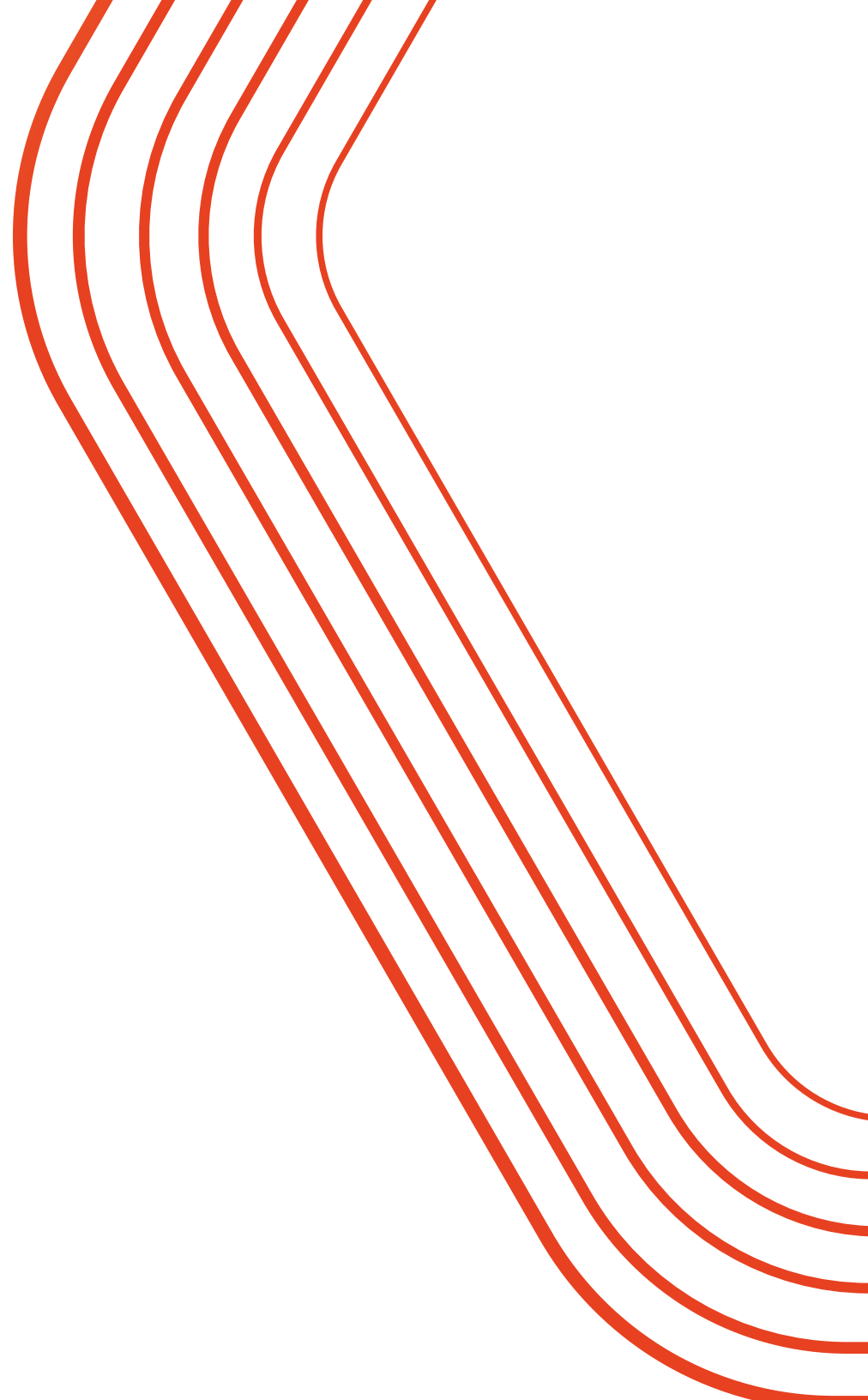


Table of contents

Introduction	2
Welcome to the identity era	4
Identity security's watershed moment: Snowflake	5
Identity is the new perimeter	6
Why attackers are focusing on vulnerable identities	7
How identities are exploited for account takeover	8
Why attack paths are changing with the shift to identity attacks	10
SaaS attacks aren't an add-on:	11
How attackers profit from identity attacks	12
2024 in review	13
Identity attacks by the numbers	13
Public identity breaches in 2024	14
Top 3 public identity related breaches in 2024	16
Threat actor case studies	17
APT29	18
Scattered Spider	20
ShinyHunters	22
How identity-based techniques evolved in 2024	24
Phishing 2.0	25
Infostealers 2.0	26
Credential stuffing 2.0	27
Session hijacking 2.0	28
Final thoughts	29



Introduction

Identity attacks where attackers look to take over accounts on internet-facing apps and services are by far the most common attack experienced by organizations today. But the events of 2024 show that they're now also the most impactful.

The major cyber security stories from 2024 have revolved around identity attacks, with identity-based campaigns from APT29 and Scattered Spider, infostealer campaigns and credential theft on an industrial scale, a booming underground marketplace for stolen data, and MFA-bypassing AitM and BitM phishing techniques becoming the new normal.

The standout story was the campaign against ~165 Snowflake customers, impacting hundreds of millions of end-customers and billed as one of the biggest breaches in history. Snowflake was a watershed moment for attackers and defenders that laid bare the threat posed by identity attacks and account takeover.

The rise in identity attacks is wrapped up in broader transformational change in IT and working practices, driven by the shift to remote working and the so-called SaaS revolution.

The result is that work now happens in employee browsers, across a vast ecosystem of internet-based apps and services. So, where identity was once governed and administered in your centralized identity store like Active Directory, it's now radically decentralized — with multiple identity providers, hundreds of apps, and thousands of identities per organization.

Naturally, this gives attackers a vast surface to target, where vulnerable identities are the lowest-hanging fruit. And to top it all off, the controls we've historically relied on to stop identity attacks are being routinely bypassed. When all an attacker needs to do is log into an internet-facing app and steal your data to be able to profit, they don't need to worry about bypassing your firewalls and EDR, for example.

There's no doubt that identity attacks are the #1 threat facing organizations today — but we're still only scratching the surface of what's possible in the world of interconnected SaaS and decentralized identity infrastructure.

It's vital that organizations arm themselves with the knowledge and understanding of how the threat has evolved — and re-evaluate their defenses accordingly.



Welcome to the identity era

Whenever there's a paradigm shift in cyber security, it's typically triggered by an event or series of events (usually a high-profile attack) that exposes the limitations of the status quo.

Identity is the new perimeter. But before we tell you why, let's first look at how we got here.

The dawn of modern network security: The SQL Slammer

The dawn of modern network security as we know it was spurred on by the infamous SQL Slammer worm in 2003, which infected ~75k servers worldwide, crippling retail POS systems and ATMs. This demonstrated the risk posed by universal attacks exploiting common vulnerabilities – a free-for-all rather than specific hosts or networks.

The response to the SQL Slammer, as well as the earlier CodeRed and Nimda worms, was to acknowledge the limitations of traditional network firewalls introduced in the late 1980s. These events moved the industry toward application-layer firewalls, deep packet inspection (beyond just IP addresses and ports), and intrusion prevention and detection systems,

as well as default-deny firewall policies. They also highlighted the need for routine patch management (the exploited vulnerability was 6-months old), prompting the Microsoft Trustworthy Computing initiative and the first ever Patch Tuesday.

This event ushered in an era where internet-exposed servers were the lowest hanging fruit for attackers to pick at – the first “perimeter” of modern computer networks — and building tall walls became the top objective for security departments.

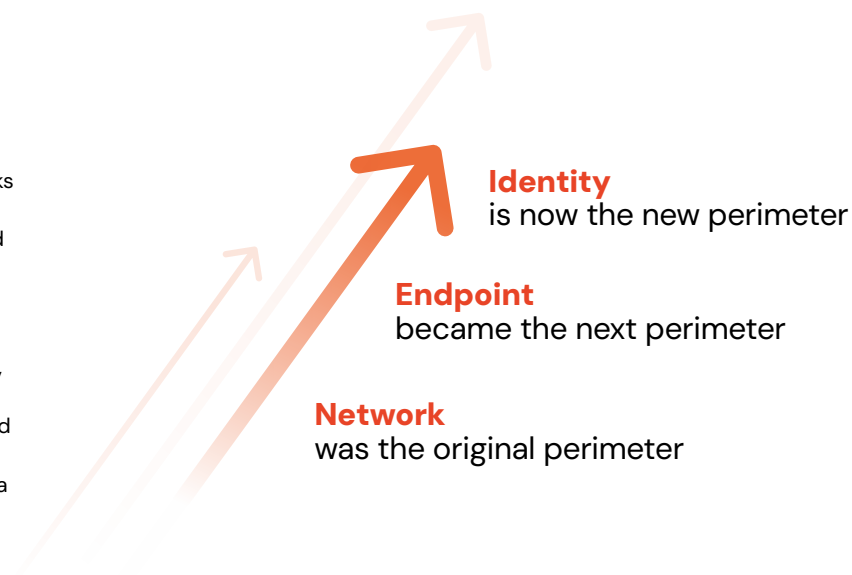
The shift to the endpoint: Operation Aurora

The next shift occurred in 2009 when Operation Aurora hit the headlines. This was a highly sophisticated series of attacks targeting U.S. technology and defense companies, attributed to state-sponsored hackers from China.

The attack, which exploited a zero-day vulnerability in Microsoft Internet Explorer, was one of the first widely publicized attacks where zero-day exploits were used in a targeted and sophisticated manner. The attacker deployed malware including a Remote Access Trojan, enabling them to

move laterally, escalate their privileges, and ultimately steal sensitive data from victims.

This attack highlighted the need for greater defense in depth as opposed to a model that was “crunchy on the outside, chewy in the middle” to be able to defend against unforeseeable zero-day exploits; equally, it exposed the limitations of the signature-based AV solutions that had failed to detect the custom malware used by the attacker. This inspired a new wave of specialist providers to come to market, and the EDR industry was born.



Identity security's watershed moment: Snowflake

The previous 18 months have seen a number of significant breaches propelled by identity attacks, with threat actors like Cozy Bear and Scattered Spider publicly leveraging identity attack techniques, and the Okta, Microsoft, MGM Resorts breaches getting plenty of news coverage.

But, it's the attacks on Snowflake customers in 2024 that will be remembered as the watershed moment for identity — touted by news outlets as “one of the biggest breaches ever”, impacting hundreds of millions of end-customers.

Between April and July this year, user accounts belonging to approximately 165 Snowflake

customers around the world were compromised using stolen credentials from infostealer infections dating back to 2020, enabling attackers to log into accounts without MFA (which was not turned on by default).

The attacker simply logged into the app, used a basic utility to gather information from accounts, and executed the same set of SQL commands across customer instances to exfiltrate data.

Snowflake is just the tip of the iceberg. But it serves as a wake-up call for what's coming (or rather, what's already happening).



Identity is the new perimeter

In the wake of Snowflake, it's clear that identity is the new perimeter.

Identity attack is synonymous with account takeover, where the attacker hijacks an account connected to an application or service. Most commonly, identity techniques are used during the initial access phase of an attack.

The so-called SaaS revolution means that organizations are using hundreds of apps, with thousands of accounts as a result. Some are entirely SaaS-native, with no traditional network to speak of, but most have adopted a hybrid model with a mixture of on-premise, cloud, and SaaS services forming the backbone of business applications being used.

Not only this, they're no longer conveniently managed and administered from a central identity system like Active Directory (who'd have thought we'd miss it?).

Most organizations have looked to SSO and MFA as the key to tackling identity sprawl. Unfortunately, the reality is that:

- Requiring MFA when logging into an IdP account and requiring MFA at the application level are separate things — meaning SSO logins can have MFA enabled at the same time that local logins do not.
- Many apps lack the ability to enforce MFA by default, meaning that even if you are aware of an app and it's managed by the security team, there still might not be much you can do to track or improve user account security.
- SSO isn't always possible depending on your app and IdP combination. Not all apps support all SSO methods or provide integrations with every IdP.
- SSO doesn't prevent users from creating or using non-SSO logins alongside SSO (often this needs to be configured in-app, if it's possible at all).
- Because many apps are adopted organically by users, security teams aren't always aware of them to enroll them in SSO.
- When self-adopting an app, users often default to a username and password (and don't set MFA).



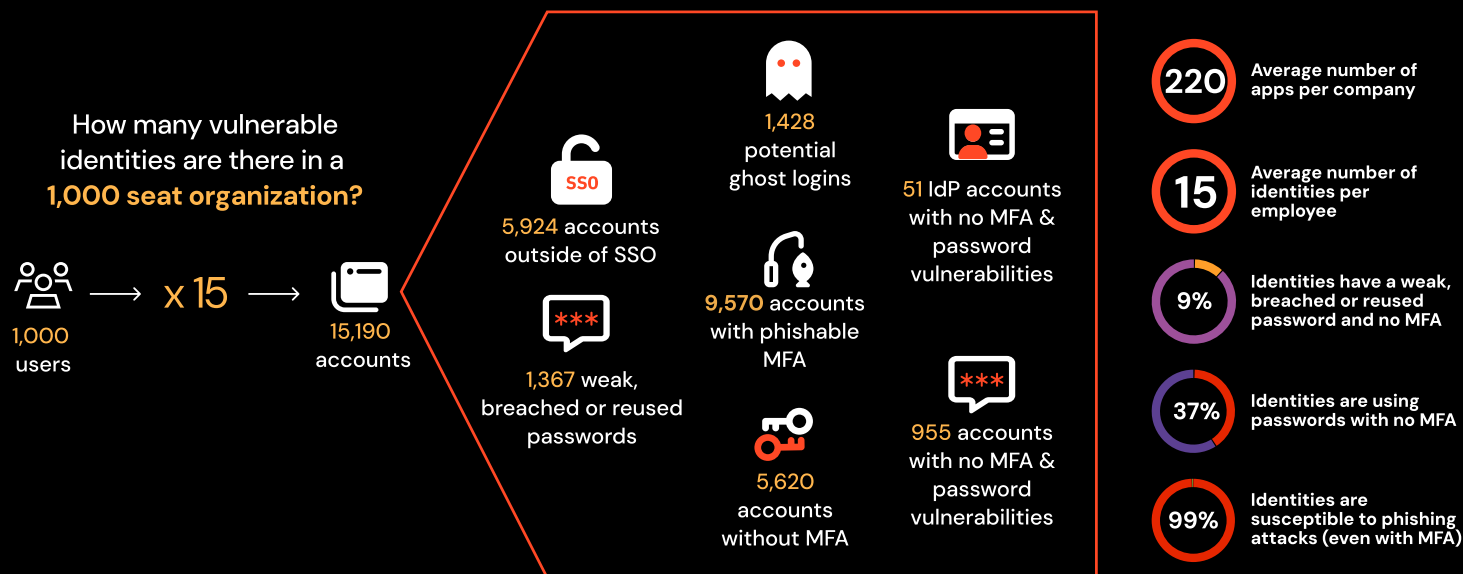
Why attackers are focusing on vulnerable identities

The scale of the challenge posed by managing identities in this modern context means that it's easy for identity misconfigurations and vulnerabilities to creep in. So identity vulnerabilities exist almost everywhere.

Some are certainly more likely to be exploited than others (e.g. an account with a reused password and no MFA is a higher risk than an account with MFA) but attackers have the means to take over most accounts using widely available tooling and know-how. A determined attacker can get into pretty

much any account, regardless of the configuration and most of the time account takeover can be achieved by using even the most basic techniques.

To bring this to life, let's look at an example identity attack surface for a 1,000 user organization using Push data.



How identities are exploited for account takeover

To be able to hijack an account, an attacker needs to possess one of two things:

- **Authentication material e.g. a username and password, with a login portal URL.**
- **Session material e.g. session cookies.**

Attackers mainly acquire these materials through credential phishing and infostealers, using stolen cookies and credentials to perform different account takeover techniques, albeit with the same goal: **Account takeover.**



Phishing

Attacker successfully phishes a victim to steal credentials & cookies, or deploy malware



Stolen credentials

Attacker steals auth material like usernames, passwords and phishable MFA factors



Infostealers

Victim downloads infostealer malware from the internet and their device is infected, resulting in saved passwords and sessions being stolen



Stolen cookies

Attacker steals session material e.g. session cookies



Valid accounts

Attacker logs into an account using a set of valid credentials



Session hijacking

Attacker imports stolen cookies into their browser to resume a valid session



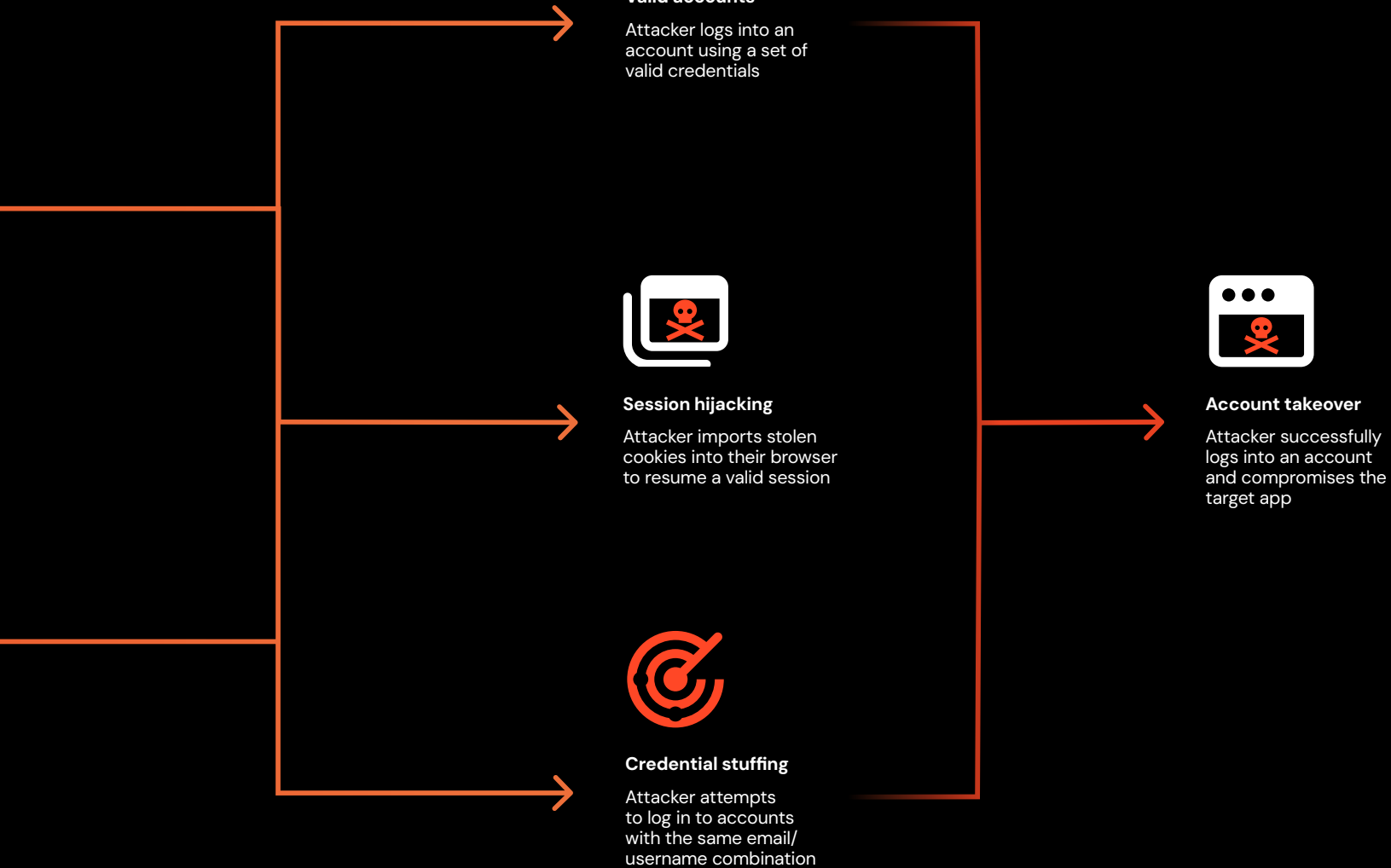
Credential stuffing

Attacker attempts to log in to accounts with the same email/username combination



Account takeover

Attacker successfully logs into an account and compromises the target app

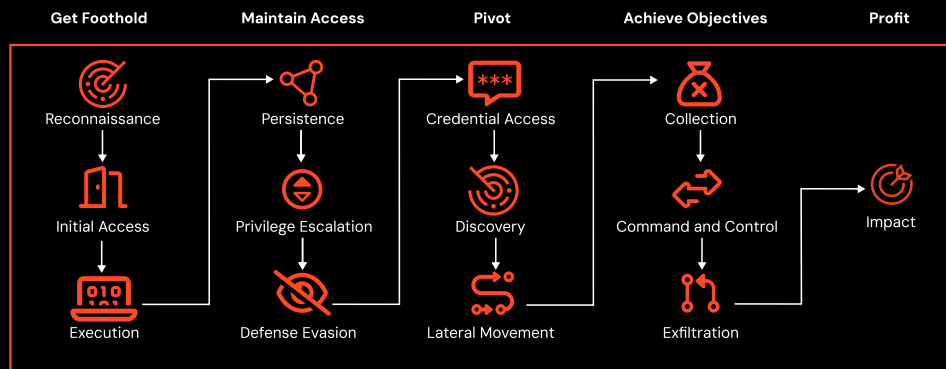


Why attack paths are changing with the shift to identity attacks

Because modern businesses effectively run on interconnected SaaS apps, attackers simply have to log into accounts on these apps to be able to exploit them.

So where the typical attack path once looked something like this:

Network compromise in traditional environment



It now looks more like this:

Account takeover on third-party web app



SaaS attacks aren't an add-on

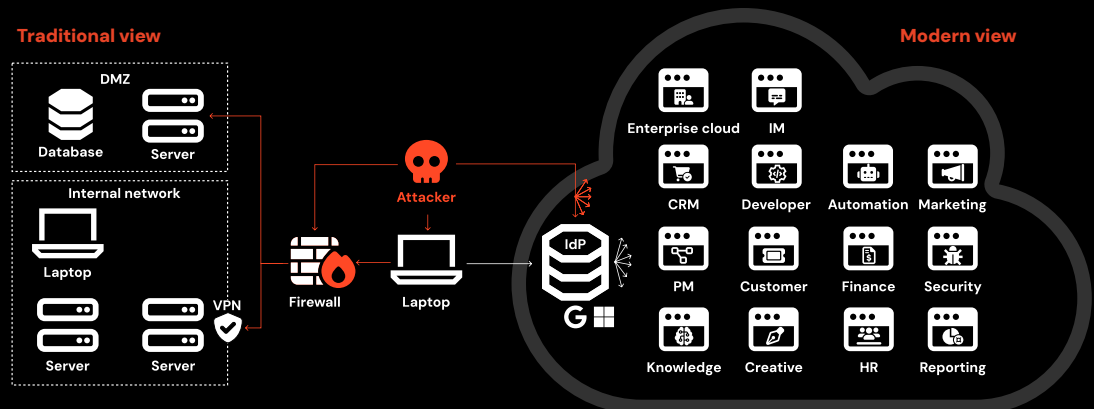
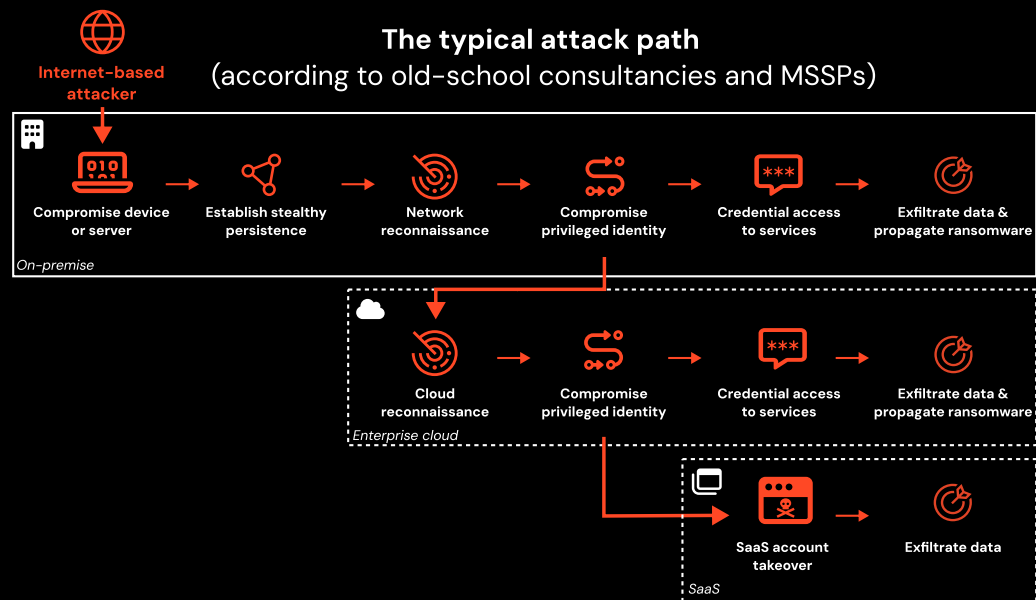
It's a common misconception that SaaS compromise typically comes after the traditional attack chain (a myth largely promoted by old-school consultancy providers, MSSPs, and managed SOC providers).

There's no need for an attacker looking to take over a SaaS account to target the conventional network first — and many organizations today simply no longer have one.

This isn't to say that there aren't examples of SaaS compromises involving lateral movement from SaaS to SaaS or SaaS to cloud (we created a whole attack matrix demonstrating the art of the possible here). Equally, there are examples of very short and direct account takeover in enterprise cloud environments leading to ransomware deployment.

But statistically, the average SaaS attack path involves little to no lateral movement, privilege escalation, and defense evasion, particularly when compared to a conventional network or hybrid attack.

These attacks are so successful because they bypass many of the existing security tools and frameworks that we've come to rely on — like EDR, firewalls, IDS, etc. — because they don't touch the environments that they protect. And without the luxury of defense in depth, the controls that are still in play are having their limitations exposed.




How attackers profit from identity attacks









Most cyber attacks that businesses encounter can be boiled down to one of three financially motivated end-goals:

- **Fraud** — Social engineering a victim to unknowingly perform a malicious action on the attacker's behalf. There are many overlaps here with business email compromise (BEC) — except business email isn't the only possible context.
- **Data theft** — Stealing data to extort a ransom payment, blackmail end-customers, and/or sell the data via underground criminal marketplaces.
- **Ransomware** — All the elements of data theft but also involving forced encryption of services and devices.

Most account takeover attacks result in data theft opportunities, since ransomware deployment would involve additional lateral movement to conventional network resources (on-premise or cloud-hosted). And as many organizations today are SaaS-native, this isn't always worthwhile (or even possible).

Of course, it depends on the app in question, but most business apps contain sensitive data that can be monetized — either directly in-app, or via an OAuth integration with another app or service.



Critical	 Identity provider Compromise any/all connected apps
	 Developer Steal sensitive customer & product data, compromise connected services and infrastructure
	 Enterprise cloud Steal data, pivot to connected apps, systems & devices
	 Business email / instant messenger Steal sensitive data, social engineer users and customers
High	 CRM Steal sensitive customer and commercial data
	 Automation Steal sensitive data from connected apps, backdoor systems and apps
Medium	 Customer support Steal sensitive customer or commercial data, social engineer customers
	 Finance Issue fraudulent payments, submit fraudulent invoices, steal payment information, steal customer information

Top app types by ATO risk

2024

in review

Identity attacks by the numbers

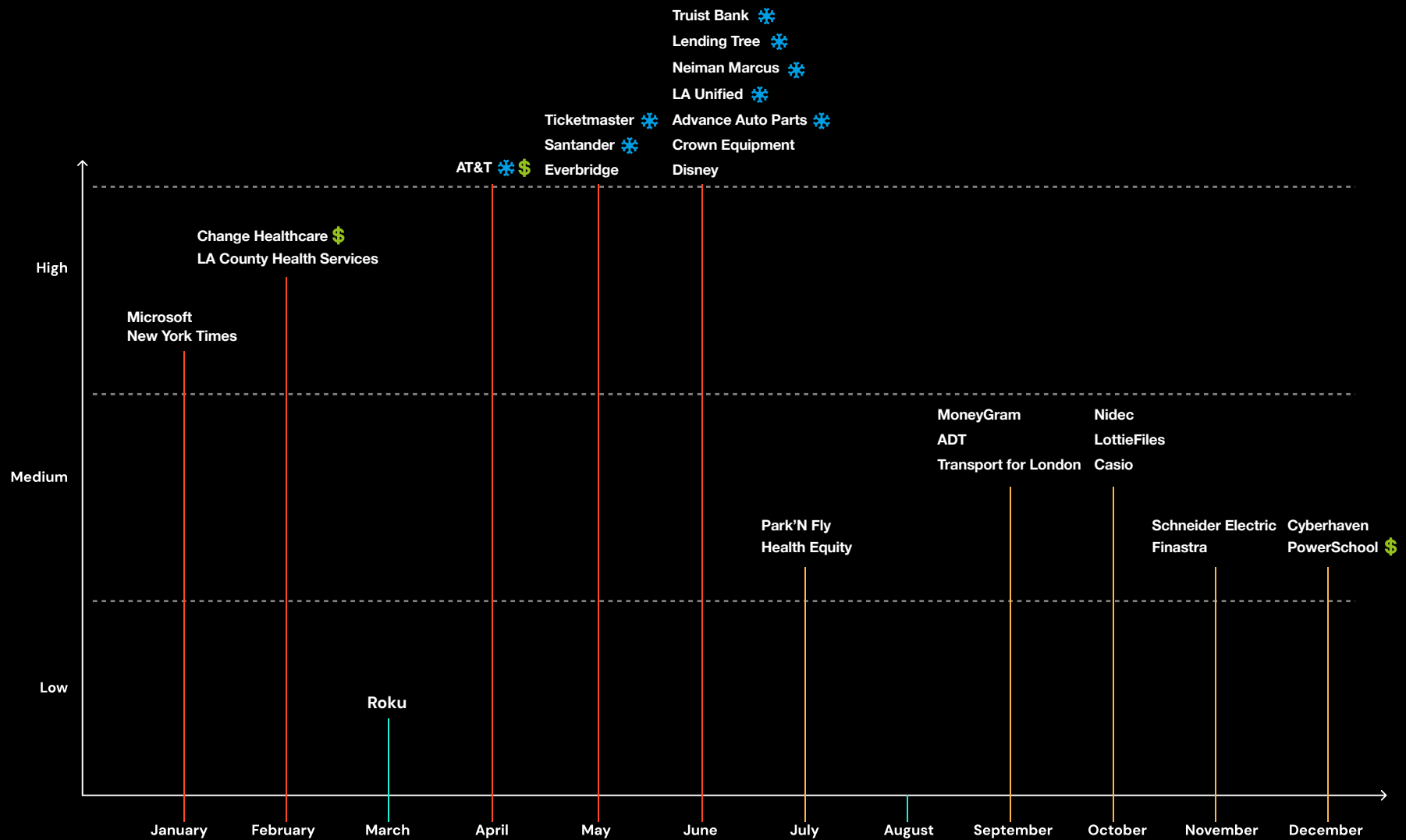
We've curated some of the most impactful identity-related stats from reports issued in 2024.

- There are **600 million** identity attacks per day (Microsoft).
- **79% of web application compromises** were the result of breached credentials (Verizon).
- **75% of attacks in 2023 were malware-free** and "cloud conscious" attacks increased by 110% (CrowdStrike).
- **Infostealer activity increased by 266% in 2023**, while the number of attacks featuring valid credentials saw a 71% increase year-over-year (IBM).
- **One million new infostealer logs** are distributed every month (Flare).
- **Nearly half of the malware detected last year** targeted victims' data specifically, and the majority of that malware was classified as infostealers (Sophos).
- **39,000 session token attacks** are detected per day and AitM attacks increased 146% in 2023 (Microsoft).
- Attacks on session cookies happen **at the same rough order of magnitude** as password-based attacks (Google).

Public identity breaches in 2024

In 2024, we experienced a notable spike in news relating to data breaches where identity attacks played a significant role — usually as the method of initial access to company systems (either in the form of third-party SaaS or managed servers/devices/appliances).

Given that publicly reported breaches are the very tip of the iceberg, and rarely provide any real information about the attack (it's hard to argue that an attacker logging in with stolen credentials is evidence of a 'sophisticated' attack, after all), this is a trend we should take note of.



Identity-related breaches by customer impact

Top 3 public identity-related breaches in 2024

#3 – Microsoft

The threat group known as APT29, associated with the Russian SVR intelligence service, utilized password spray attacks that successfully compromised a non-production tenant account that did not have multi-factor authentication (MFA) enabled. They then leveraged this account to compromise a 'test' OAuth application that had elevated access to the Microsoft corporate environment. This was then used to access the email accounts of Microsoft employees.

The attacks then continued throughout the year using information stolen from Microsoft mailboxes, with password spraying attacks increasing tenfold since the initial attack, resulting in the further compromise of source code repositories.

Microsoft has shared limited information about the breach, but despite this it caused a significant stir. We can expect the number of email accounts compromised to be significant, given that it was later suggested that at least 100 external organizations had been contacted by Microsoft regarding their communications being breached (we only know this because 100-ish organizations reported the email as spam). The list of companies impacted included both public and private sector organizations, from major enterprises to government agencies in the US and other countries.

#2 – Change Healthcare

In February, attackers stole 6TB of data from UnitedHealth subsidiary Change Healthcare as part of a severe ransomware attack that caused massive disruption to the US healthcare industry. This impacted a wide range of critical services used by healthcare providers across the U.S., including payment processing, prescription writing, and insurance claims, and caused financial damages estimated at \$872 million. The attack impacted the personal medical data of over 100M customers.

The attacker used stolen credentials to breach the company's Citrix remote access service, which did not have multi-factor authentication enabled, as the initial breach vector for the attack.

Following the attack, the organization's IT team replaced thousands of laptops, rotated credentials, and completely rebuilt Change Healthcare's data center network and core services.

The UnitedHealth Group admitted to paying a ransom demand to receive a decryptor and for the threat actors to delete the stolen data. The ransom payment was allegedly \$22 million, according to the BlackCat ransomware affiliate who conducted the attack.


#1 – Snowflake

165 organizations around the world were targeted using stolen credentials gathered from infostealer infections dating back to 2020.

The impacted accounts lacked MFA, meaning successful authentication only required a valid username and password. As the Snowflake credentials found in infostealer malware credential dumps had not been rotated or updated, they remained valid and could be used to authenticate to user accounts on Snowflake tenants belonging to various customers. It has been touted by some news outlets as 'one of the biggest breaches ever'.

In total, nine public victims were named following the breach, collectively impacting hundreds of millions of their respective customers. Data was put up for sale on criminal forums for fees ranging from \$150k to \$2m per organization, while AT&T was also confirmed as paying an undisclosed ransom fee.





Threat actor case studies

Let's take a closer look at the tactics, techniques and procedures (TTPs) used by some of the more prolific threat actors from 2024 known for identity-related attacks.

APT29

Aliases: The Dukes, Cozy Bear, Midnight Blizzard

Public victims: Microsoft, Hewlett-Packard Enterprises, TeamViewer, various government agencies & departments

Public campaigns: SolarWinds (~50 public victims)

APT29 is a cyber espionage group and part of the Russian Foreign Intelligence Service (SVR).

Previously known for now-infamous campaigns such as the supply-chain attacks on SolarWinds customers in 2020, APT29 demonstrated a flexible approach to the TTPs used, but demonstrated a conscious adoption of identity-based techniques in 2024 in order to target cloud-based services and infrastructure.

In January 2024, APT29 executed a cleverly executed password-guessing attack against Microsoft to compromise test cloud identities that were also lacking MFA. Attackers then leveraged this access to compromise OAuth applications that allowed lateral movement to Microsoft's corporate environment.

APT29 was able to authenticate to Microsoft Exchange Online and target Microsoft corporate email accounts, stealing sensitive data. Since the initial attack there has been evidence of continued targeting, with password spraying attacks reportedly increasing tenfold, likely informed by stolen information.

"To access the majority of the victims' cloud hosted network, actors must first successfully authenticate to the cloud provider. Denying initial access to the cloud environment can prohibit SVR from successfully compromising their target. In contrast, in an on-premise system, more of the network is typically exposed to threat actors."

- UK National Cyber Security Centre (NCSC)

The following identity-based TTPs have been commonly observed over the last 12 months:

Credential stuffing: Using brute forcing and password spraying to access service accounts used to run and manage applications and services, and dormant accounts belonging to inactive users that have not been deleted.

Session hijacking via stolen tokens: Authenticating with system-issued access tokens to access their victims' accounts without needing a password.

MFA bypass: Bypassing MFA using MFA fatigue attacks in which the actors repeatedly push MFA requests to a victim's device until the victim accepts the notification.

Residential proxies: Using residential proxy networks to hide the true source of the traffic and evade less prescriptive access control policies.

Malicious OAuth integrations: Granting and abusing existing access to OAuth applications with high permissions to elevate privileges in a compromised application or environment after an initial account takeover.



Scattered Spider

Aliases: Oktapus, Octo Tempest

Public victims: MoneyGram, Transport for London, Caesars, MGM resorts, Clorox, DoorDash, Twilio, Reddit, Coinbase, MailChimp, Okta, HubSpot, Cloudflare, Activision

Public campaigns: OktaPus

Scattered Spider is a native English-speaking cybercriminal group that gained notoriety in 2023 and 2024 with a string of high-profile attacks, becoming known for social engineering attacks involving SIM swapping and helpdesk scams.

The attacks perpetrated by the group involved a combination of ransomware deployment via compromised enterprise cloud environments, data exfiltration, and extortion.

Members of Scattered Spider were arrested in 2024 including an alleged ringleader, where Bitcoins worth \$27m were discovered from the proceeds of extortion.

"Octo Tempest leverages tradecraft that many organizations don't have in their typical threat models, such as SMS phishing, SIM swapping, and advanced social engineering techniques".

– Microsoft

The following identity-based TTPs have been commonly observed over the last 12 months:

Social engineering: Targeting technical administrators, such as support and help desk personnel, who have permissions that could enable the threat actor to gain initial access to accounts through performing password and MFA resets.

Credential theft: Purchasing stolen credentials and/or session tokens on criminal marketplaces for credential stuffing or to be used in conjunction with social engineering attacks.

MFA bypass: Using adversary in the middle (AitM) phishing toolkits to acquire MFA factors and/or authenticated sessions and using SIM swapping or call forwarding to complete MFA checks.

Credential harvesting: Automated data gathering across data repositories and storage containers for additional credentials to perform lateral movement within and across cloud environments.



ShinyHunters

Aliases: UNC5537

Public victims: Ticketmaster, Santander, Neiman Marcus, Los Angeles Unified, Pure Storage, Advance Auto Parts, Truist Bank, Lending Tree, AT&T

Public campaigns: Snowflake

ShinyHunters is the alleged threat group behind the infamous attacks on ~165 Snowflake customers in 2024, which resulted in hundreds of millions of breached customer records and other sensitive data breaches. The defining feature of the Snowflake campaign was the use of stolen credentials that were available online — either publicly or through commercial feeds.

Recent arrests of two alleged members indicate that the hackers and their co-conspirators extorted at least three victims for at least 36 Bitcoins, or \$2.5 million at transaction time, as well as any profits from the resale of stolen data on criminal forums.

“According to Mandiant and Snowflake’s analysis, at least 79.7% of the accounts leveraged by the threat actor in this campaign had prior credential exposure. The earliest infostealer infection date observed associated with a credential leveraged by the threat actor dated back to November 2020. In total, Mandiant identified hundreds of customer Snowflake credentials exposed via infostealers since 2020.”

– Mandiant

The following identity-based TTPs have been commonly observed over the last 12 months:

Stolen credentials: The attacker harvested credentials already available online, collecting all available credentials belonging to Snowflake accounts to be used in a mass credential stuffing campaign.

Targeting unmanaged devices: Many of the infostealer infections were traced back to unmanaged devices (many belonging to contractors or business process outsourcing (BPO) firms, which often lack endpoint security controls such as EDR.

Exfiltration via in-app functionality: The attacker executed similar SQL commands across all customer instances to stage and exfiltrate data to the attacker’s C2 servers.

Session hijacking via stolen tokens: Authenticating with system-issued access tokens to access their victims’ accounts without needing a password.



How identity-based techniques evolved in 2024

As attackers double down on identity-based techniques, well-known TTPs are taking on new and improved forms that make them more difficult than ever to detect and prevent.

Phishing 2.0

AitM & BitM

MFA-bypassing phishing kits are now the standard choice for attackers.

Adversary-in-the-Middle (AitM) and Browser-in-the-Middle (BitM) kits have become the new normal, with Phishing-as-a-Service (PhaaS) platforms like Tycoon and NakedPages sending hundreds of millions of phishing messages each month. Attackers are also making use of commercial tools like Evilginx, which while nominally a tool for offensive security researchers, has been detected by Push in the wild being used against customers.

Since the victim is prompted to complete the MFA request as part of the attack, most forms of MFA (with the exception of domain-bound passwordless methods like passkeys or biometrics) can be phished in this way.

Because the victim is accessing the legitimate site, these techniques have an increased sense of authenticity and makes the compromise less obvious. For example, if accessing their webmail, the user will see all their real emails; if accessing their cloud file store then all their real files will be present — all reducing the likelihood of detection.

To make matters worse, attackers are also implementing various obfuscations to get around the other anti-phishing controls that organizations typically rely on, such as secure web gateway (SWG) controls, email/webpage scanning solutions, and TI-driven blocklists.

Attackers are using obfuscation techniques like:

- Hacking legit sites or using Cloudflare Workers to get a reputable domain
- Serving different URLs on a rotation, and continually refreshing the pool of URLs
- Randomizing the HTML title for the web page
- Using one-time phishing links that only work the first time they are accessed
- Requiring JavaScript execution to load malicious elements
- Loading malicious elements only when certain parameters are met

This makes it highly unlikely that an attack will be intercepted before the victim is successfully phished.



Infostealers 2.0

Infostealers have to take a lot of the credit for the rise in identity attacks using stolen credentials that we've seen in the last year.

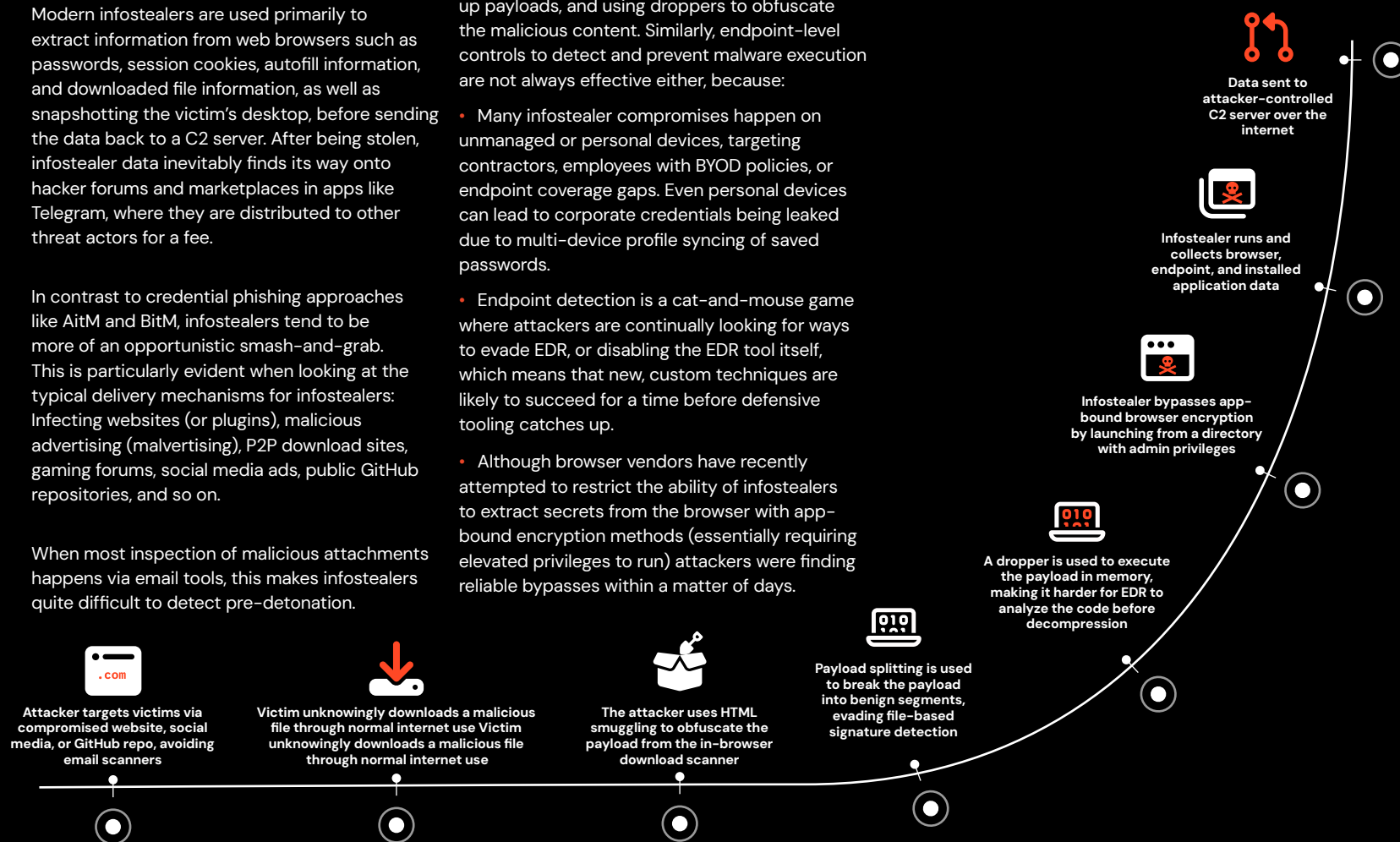
Modern infostealers are used primarily to extract information from web browsers such as passwords, session cookies, autofill information, and downloaded file information, as well as snapshotting the victim's desktop, before sending the data back to a C2 server. After being stolen, infostealer data inevitably finds its way onto hacker forums and marketplaces in apps like Telegram, where they are distributed to other threat actors for a fee.

In contrast to credential phishing approaches like AitM and BitM, infostealers tend to be more of an opportunistic smash-and-grab. This is particularly evident when looking at the typical delivery mechanisms for infostealers: Infecting websites (or plugins), malicious advertising (malvertising), P2P download sites, gaming forums, social media ads, public GitHub repositories, and so on.

When most inspection of malicious attachments happens via email tools, this makes infostealers quite difficult to detect pre-detonation.

And even when malicious downloads are intercepted and analyzed, attackers are getting increasingly creative to evade these controls, using techniques like HTML smuggling, splitting up payloads, and using droppers to obfuscate the malicious content. Similarly, endpoint-level controls to detect and prevent malware execution are not always effective either, because:

- Many infostealer compromises happen on unmanaged or personal devices, targeting contractors, employees with BYOD policies, or endpoint coverage gaps. Even personal devices can lead to corporate credentials being leaked due to multi-device profile syncing of saved passwords.
- Endpoint detection is a cat-and-mouse game where attackers are continually looking for ways to evade EDR, or disabling the EDR tool itself, which means that new, custom techniques are likely to succeed for a time before defensive tooling catches up.
- Although browser vendors have recently attempted to restrict the ability of infostealers to extract secrets from the browser with app-bound encryption methods (essentially requiring elevated privileges to run) attackers were finding reliable bypasses within a matter of days.



Credential Stuffing 20

Despite the rise in SSO use and MFA adoption, accounts continue to be hacked as a result of weak, reused, and/or previously breached credentials. Infostealers are the main source of compromised credentials, along with Phishing-as-a-Service platforms.

The sheer number of apps and accounts connected to an organization and its users means that the likelihood and impact of stolen credentials is significantly heightened. If a user is reusing passwords across multiple apps (and we find that 1 in 5 users are) then there's a bigger chance that they're using the same password multiple times.

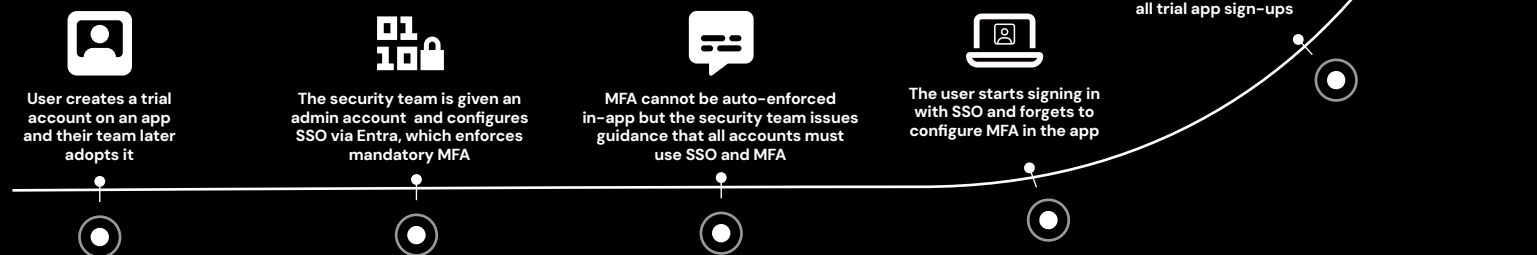
This means if the password is breached for one app, an attacker may be able to use the same set of credentials to access several apps. Given the fact that 2 in 5 accounts lack MFA (increasing to 4 in 5 where a password is the only registered login method), there's a strong possibility that attackers will be able to log in with a single-factor breached password. And because organizations are now using so many different apps (more than 200 on average), there are thousands of accounts for attackers to choose from.

But because of the sheer amount of compromised credential data available online, there's a huge amount of noise for security teams to deal with. We found that fewer than 1% of the credentials found in compromised credential feeds were valid — in other words, 99.5% of the findings were false positives.

This makes finding and rotating compromised credentials across thousands of accounts per organization a bit like looking for a needle in a haystack.

Credential stuffing is also enabled by ghost logins: where a local password is set alongside SSO. Often, MFA is only configured at the IdP level, meaning local credentials are not protected with a second factor — effectively giving attackers an easy backdoor to the app.

Ghost logins are easily introduced through the process of normal app adoption, but organizations often lack the visibility and in-app controls to be able to tackle them at scale.



20

Session hijacking

When we think of the classic example of session hijacking, we think of old-school Man-in-the-Middle attacks that involved snooping on unsecured local network traffic to capture credentials or, more commonly, financial details like credit card data. Or, by conducting client-side attacks compromising a webpage, running malicious JavaScript and using cross-site scripting to steal the victim's session ID.

Session hijacking looks quite different these days. No longer network-based, modern session hijacking is an identity-based attack performed over the public internet targeting cloud-based apps and services.

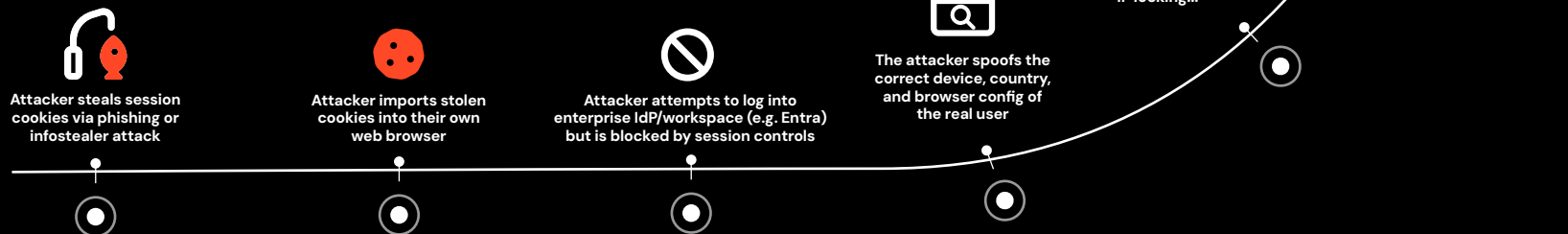
Unlike legacy session hijacking, which often fails when faced with basic controls like encrypted traffic, VPNs, or MFA, modern session hijacking is much more reliable in bypassing standard defensive controls.

Session hijacking involves an attacker using stolen cookies extracted from the victim's browser (either via an infostealer compromise or a browser-based exploit such as a malicious extension).

Typically, defenders are reliant on limited session cookie lifetimes and access control policies to combat these attacks. However:

- It's not unusual for cookies to have a lifetime of a month or more (sometimes indefinitely), meaning that attackers have plenty of time to use them before they expire.
- Unless strictly locked to a specific office IP range, access control policies can usually be fooled by mimicking the victim's browser and device setup, and using a VPN to bypass geo-restrictions.
- Most SaaS apps don't have strict access control policies available — this control is usually limited to enterprise platforms like O365.

This means that even if you have a locked down IdP solution and are using SSO to access downstream apps, attackers can still hijack downstream SaaS accounts using stolen cookies.



Final thoughts

Account takeover via identity attacks is now the go-to approach for threat actors.

- The threat of identity attacks is significantly increased by the SaaS-ification of business IT due to the increased identity attack surface.
- Identity attacks are routinely evading many established controls, including MFA, SSO, SWG, EDR, and so on, leaving organizations unknowingly exposed.
- Many accounts are highly vulnerable to even basic attacks, while even more robust configurations can be bypassed using widely accessible tooling and techniques.
- Attackers can compromise many organizations by targeting the various company tenants of a single SaaS app, often following repeatable steps post-account takeover.
- Once an account is compromised, attack paths can be very short, resulting in quicker time-to-value for the attacker.

It may have been a landmark year for identity attacks, but we're still only scratching the surface of what's possible in the new world of decentralized, SaaS-centric IT. **There's no doubt that we should expect the threat of identity attacks to grow further in 2025.**

This means that it's essential that organizations re-evaluate and strengthen their defenses against identity attacks.

If you'd like to stay up to date with our latest threat research and content, you can find our blog and sign up for future updates [here](#).

And if you'd like to learn more about how Push's browser-based ITDR platform stops identity attacks, sign up for a demo below:

[Book a demo now](#)

