ActZero

THREAT INSIGHT

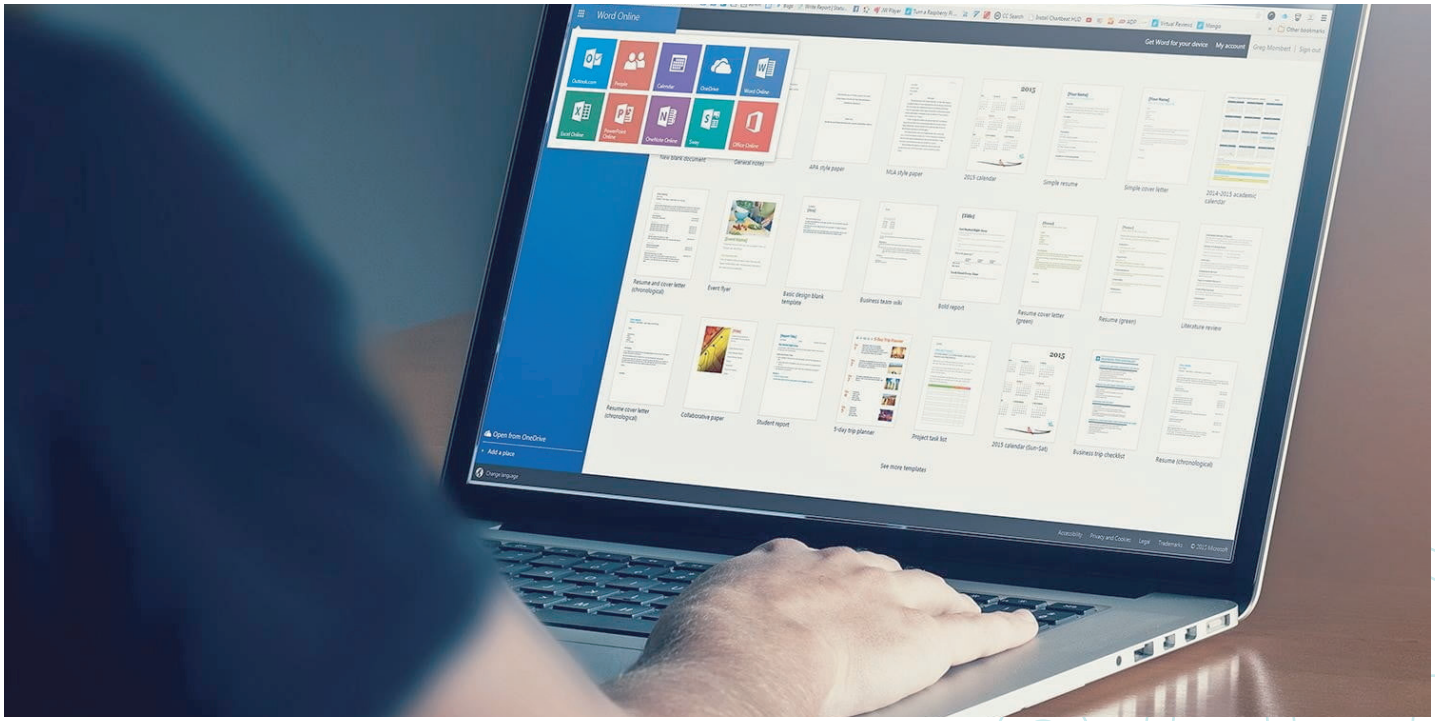
Office365 Account Takeover

What it is, and why detecting it early is crucial.

With the rapid adoption of cloud services like Microsoft's Office 365, and the distributed workforce, the risk of account takeover (ATO) fraud is increasing at alarming rates.

According to a recent Sift index, "ATO fraud attacks have especially spiked by almost 282% from the second quarter of 2019 until the second quarter of 2020". And we anticipate these numbers will continue to climb as more businesses move operations to the cloud.

Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials. Once initial access is gained, the damage chain can magnify quickly, with the threat actor using the compromised account to send messages to other employees inside the organization (or beyond) to inflict their damage. In fact, in ATO most cases have seen lateral movement across the network and supply chain almost immediately.



How do Account Takeovers occur?

Threat actors can have many tools at their disposal when it comes to mining for credentials. Not surprisingly, many of these are aimed squarely at the unsuspecting (and often overly trusting) end users. Each presents a slightly different approach to gaining access, but their common goal is the same - steal a user's credentials or account, to exfiltrate data or cause disruption.

Phishing Scams: Phishing attempts often appear as a pop-up or an email indicating that account credentials are 'suspended', need to be 'verified' or 'reset'. Unsuspecting users follow the prompts, ending on a well-crafted landing page where they are prompted to enter credentials. Attackers then have the login credentials and access to the account, immediately setting up forwarding rules on the account to surmise the user's communications patterns (internal and external to the organization). This knowledge can be used as leverage for future attacks such as ransomware or other advanced threats.

Additionally, Attackers can use the compromised account to send messages to other employees inside the organization in an attempt to collect additional credentials. These often come in the form of a PDF attachment whereby either a colleague (really the attacker) can forward a PDF document to review with casual instructions informing that the document can be accessed by entering a work email and password, or, a Vendor (the attacker) sends an invoice that requires the recipient to log on to a "web portal" to view the (fake) invoice.

Password-based Attacks

- **Credential Stuffing:** One of the simplest forms of attacks is to, by brute force, use common passwords and credentials compromised by attackers in public breaches to attack organizations and hope for a hit. Considering that as many as "65% of people reuse the same password for multiple or all accounts", according to a 2019 security survey conducted by Google, attackers have been pretty successful.
- **Password Brute Forcing:** Attackers may also try to gain access to accounts and credentials by brute forcing their way into a network, submitting many passwords or passphrases on the odd chance that they get one correct. These attacks generally have a low yield, but due to the low level of password 'intelligence' required, they are a quick go-to for attackers.
- **Password spraying:** Attackers may also try password spraying which uses a relatively small number of passwords one at a time across all known accounts sequentially. The advantage of password spray is that it can avoid account lockout.

OAuth Consent Phishing: Sometimes known as 'App Attacks', OAuth attacks occur when threat actors leverage an Office 365 app created using information stolen from a legitimate organization. The attacker sends an email, text or other communication purporting to be from Microsoft asking users to complete an action.

After the user signs into their O365 account, they're redirected to the official O365 consent process that prompts them to grant permissions to the actor's application. If the user grants the app the access it requested, attackers take full control of the victim's account - email, OneDrive, contact lists, and any other data or assets tied to the account. And because access is granted through the malicious app, a password reset would be ineffective. The only way to deny the attacker access to the account would be to delete the app.

All of the above could lead to big disruptions to both the user and the business. So what can be done to prevent it, or at least mitigate the potential damage.

Speed of Detection is key

The problem with account takeover fraud is that by the time you detect it, it's often too late. Reducing the opportunity, or at least the time to detection is critical. So what can be done to thwart the attack, or limit the damage if a takeover occurs?

- Enforce MFA, Passwords and Privileged Access: Microsoft noted in a March 2020 presentation that "99.9% of compromised accounts did not use multi-factor authentication", and that 'only 11% of enterprises used MFA at all'. Always set up O365 with multi-factor authentication. Disable legacy authentications where ever possible. Yes, some legacy applications don't support modern authentication, however, MFA can be used to block legacy applications that may be targeted for ATO campaigns. Also, consider going passwordless, or, at minimum, require strict policies preventing password re-use. And, ensure privileged access management where possible.
- Invest in Security Awareness Training: Keeping your employees up-to-date with knowledge of the latest threat risks, and their role in adhering to proper security policy and procedures.
- Account Takeover Detection: The final wall of defense, if you will, is being able to detect if an attacker has gained access to an account, or attempting to do so. You need to be able to do so very quickly, and with good accuracy so that you're not managing a huge volume of false positives. This won't be a feat easily accomplished on your own. You'll ideally want a vendor that automates the threat hunt process as much as possible on your behalf.

With ActZero's O365 ATO detection capabilities, when we suspect an ATO, we'll automatically send you an email with guidance on how to mitigate the account takeover.
Learn more about how ActZero can protect your business against account takeovers by contacting us now.