USE CASE

Spearphishing for Microsoft Office 365 Credentials

WFH Places You at Risk of Account Takeover Attacks

In the past year, businesses around the world were forced to jump suddenly from in-person to remote workforces. As companies tried to keep their employees connected and productive, many turned to cloud services such as Microsoft Office 365 (O365).

Without the time to put proper security measures in place — or the funds to purchase more robust security packages — that rapid shift to cloud-based workforces put users at a dramatically higher risk of account takeover (ATO) attacks: Between Q2 2019 and Q2 2020, ATO attacks jumped by more than 280%.

How Do ATO Attacks Work?

ATO attacks begin when a malicious party obtains a user's account credentials, such as the login information for an Office 365 profile.

From there, the attacker can — and most often does — use that individual account as an access point to launch parallel or secondary attacks within your organization. Once attackers have privileged access, they can do anything from install ransomware to initiate wire fraud.

Phishing emails are one of the most frequently used points of entry for ATO attacks. For example, in a hypothetical scenario all too common in mid-sized businesses, a member of an engineering firm's marketing team — working from home — starts their computer on a Monday morning. They immediately see an urgent email requesting that they log in to the Microsoft Office 365 Portal to change their password before it expires.

Thinking the email is a legitimate request, the employee follows the provided prompts to the landing page and enters their credentials. In the URL, however, are instructions to forward the authorization token to another domain.

Once the employee enters their credentials, the attacker has access to their entire account.

How Do ATO Attacks Spread?

Once attackers have access to a single user's account, they may begin to launch a parallel attack immediately, or they may wait for months, using the compromised account to gather personal and corporate information.

In the scenario of the mid-sized engineering firm, for example, attackers could send out more phishing emails from the compromised marketing employee's account. These messages could take the same form as the original — misleading other employees with false messages that they need to update their passwords — or they could spread malicious files disguised as work materials to gain wider access in the company, spread malware, or install ransomware.

Even if they don't immediately install malware, attackers may lurk in the background, studying the organization and how its employees interact.

With that information and access to users' email accounts — which fall under the wider Office 365 umbrella — they can set specific inbox rules to filter certain messages into folders for easy access.

For example, if an executive or a member of the finance team emails an employee with a compromised account, those inbox rules could automatically move it into a folder where attackers can find it and steal important details from your company's most sensitive departments.

ATO attacks are particularly dangerous because malicious actors can carry out the entire process unnoticed by the user or anyone else in the company. The attack will only be flagged once they change an employee's password, multi-factor authentication settings, or recovery methods. At that point the damage is done, and your organization is compromised.

Your Normal Protections Aren't Enough

Your organization may have taken some steps to protect itself from other attacks, but firewalls, antivirus protection, and similar measures aren't enough to stop ATO threats.

None of these safeguards give you the visibility into the cloud traffic in and out of your organization to detect the attack. Once an attacker has access to even one user's account, they no longer need to rely on the phishing emails they used to start the attack — they can begin circulating compromised links or attachments from that internal, legitimate account. And they can continue doing so, unnoticed, until they achieve whatever goal they originally set out to accomplish, whether that's stealing financial information, installing ransomware, or otherwise.

Once an attacker gains access to one of your employee's accounts, there's no way to entirely avoid the fallout. The best, and only, option is to catch the threat as soon as possible to mitigate the damage.

To do that, you need something that monitors your cloud traffic and identifies the markers of an ATO attack the moment they appear.

As part of our Managed Detection Response (MDR) offerings, ActZero includes O365 ATO detection. Our automated system keeps tabs on the traffic coming and going from your organization, scanning continually for malicious IPs that attempt to log in to your O365 environment. If ActZero's system detects a threat, we immediately send you a notification, with the information you need to start responding and minimize the damage to your organization.

Using AI and machine learning, our team tracks threats in real time, giving ActZero customers the cloud visibility they need keep their workforces functioning remotely and securely, no matter where they are.

CONTACT US

ActZero

For more information on O365 ATO detection and other WFH considerations, check out our WFH Use Case. And, for more information on how ActZero's MDR services can help keep your business secure, request a demo now.

info@actzero.ai | 1 855 917 4981 | www.actzero.ai