Solution Brief

Office 365 Account Takeover— the New "Insider Threat"

Microsoft Office 365 has become so ubiquitous—with more than 100 million monthly active subscribers—that it's almost become part of our identities particularly inside the network with emails circulating internally. There's an inherent trust when we receive an email from a coworker using his or her correct address. We are nearly certain it is legitimate, but unfortunately, that's not always the case.

Cybercriminals have a long history of designing attacks to reach the largest number of eyeballs possible. From the early days of traditional spam, to search or trending topics on social platforms, criminals follow the users—and Office 365 has become a breeding ground for highly personalized, compelling attacks.

In this solution brief, we take a look at an increasingly popular threat—Office 365 account takeover—where attackers attempt to steal login credentials and ultimately gain access to launch attacks from within an organization. Here's what we've found.

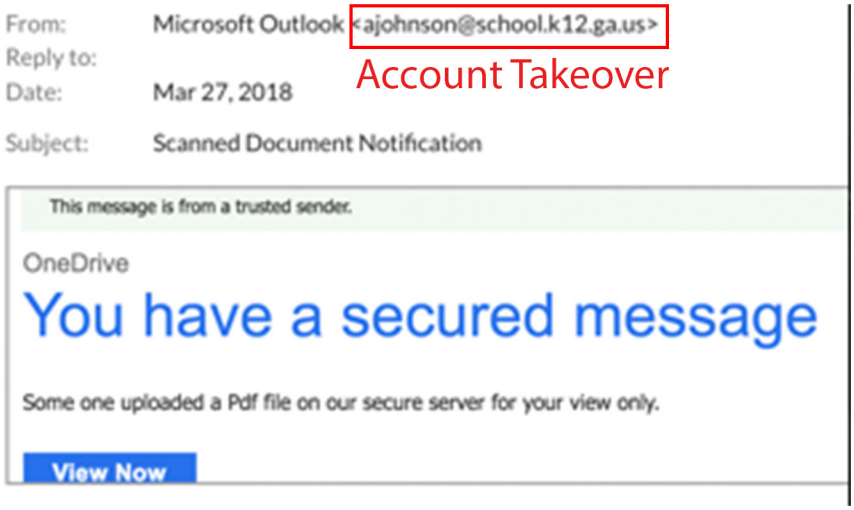
Highlighted Threat

Office 365 account takeover – attackers attempt to steal Office 365 user credentials in order to launch attacks from an internal account.

The Details

Many phishing attempts are easy for end users to sniff out because they contain bold requests, misspelled words, or questionable attachments that raise red flags. However, we are seeing an increase in the number of attacks that are much more difficult to spot due to the personalized nature in which they are carefully crafted and delivered; such is the case below.

If you take a look at the image of the email below, the message itself doesn't appear to be anything out of the ordinary. It appears to be coming from Microsoft to alert the user that they need to reactivate their Office 365 account.



There is one red flag, but nothing that is overly alarming:

- It mentions how the user's account "has been suspended" – which is not a typical action on Office 365 accounts.
- As is the case with any suspicious emails, the user should alert their IT department when a message like this is received.

But what happens if the user decides to follow the directions in this message?

This particular attack is designed to steal the user's Office 365 credentials and take over the account. The user clicks a link in the message that sends them to a well-crafted landing page where they are prompted to enter their credentials. Once they do that—game on. The attackers then will have login credentials and access to the account.

From this point, we've seen a few different scary scenarios.

A common scenario is that attackers setup forwarding rules on the account to observe the user's communications patterns, both with others inside and outside the organization. This knowledge can be used as leverage for future attacks such as ransomware or other advanced threats.

Another common scenario is where attackers use the compromised account to send messages to other employees inside the organization in an attempt to collect additional credentials or other sensitive information. This approach typically has more short-term success, as there's typically an immediate response or action required. The attacker wants the employee to click on a link that will take them to another site to collect credentials.

Office 365 is still a relatively new tool with a large and growing user base, and attackers are taking advantage of the accessibility.

Take Action

User Training and Awareness — Employees should be regularly trained and tested to increase their security awareness of various targeted attacks. Simulated attack training is by far the most effective form of training.

Multi-Factor Authentication — a form of multi-factor authentication is included with Office 365, but you can also purchase Azure multi-factor authentication that includes extended functionality.

Real-Time Spear Phishing and Cyber Fraud Defense — Barracuda Sentinel is a cloud service that utilizes AI to learn an organization's communications history and prevent future spear phishing attacks. It combines three powerful layers: an artificial intelligence engine that stops spear phishing attacks in real time and identifies the most high-risk individuals inside the company; domain fraud visibility using DMARC authentication to guard against domain spoofing and brand hijacking; and fraud simulation training for high-risk individuals.