CyberTips

First Federal
MEMBER FDIC

Rise of Compromised Microsoft Office 365 Accounts

In this edition of Cyber Tips, we will be taking a look at the rise of **compromised Microsoft Office 365 accounts** over the past year.

Researchers from Barracuda Networks (one of the largest security service providers) have discovered that almost **30% of their monitored organizations** (approximately **4000** accounts) had their Office 365 accounts **compromised**.

34% of the nearly 4000 accounts had malicious **mailbox rules** to hide their activity.

By gaining access to these compromised accounts, the attackers were able to send **over 1.5 million** malicious spam emails to saved contacts.

How Are Attackers Gaining Access?

To successfully infiltrate Office 365 accounts, cybercriminals used a combination of **brand impersonation, social engineering, and phishing attacks** to convince potential victims into visiting previously set up landing pages in order to **harvest credentials**.

The bad actors also leveraged usernames and passwords acquired in **previous data breaches** as people most often use the same passwords for their different accounts.

Brute-force attacks were also observed by researchers. This

118 NE Third Street
PO Box 239
McMinnville, OR 97128

Phone: 503-472-6171
Fax: 503-435-0314
Email: communications@firstfedweb.com

We're Here

particular attack takes advantage of easy to guess information that may relate to personal information found online such as birthdays, maiden names, kid's names etc.

What's Next after a Takeover?

Cybercriminals rarely launch an attack after they have gained access to an account. The first step for an attacker is to **conduct reconnaissance** to maximize his or her chances of executing a successful attack.

Once the criminal has gained significant amounts of information about the compromised entity, they proceed to **target highly valued accounts**, with the focus on **internal** and **external executives** and **employees from finance departments**.

How Can We Stay Safe?

To **mitigate** the risk from an Office 365 hijack attack, Barracuda Networks recommends deploying technology that doesn't rely just on looking for malicious links and attachments. Instead, **machine learning applications that can analyze communication patterns** in order to spot anomalies that are possible indicators of an attack.

Multi-factor authentication, **two factor authentication**, and **two-step verification** is also advised so the attacker cannot leverage the account credentials.

Monitoring of mailboxes, **malicious rules**, and **continuous training** on phishing attacks has also been proven effective.