Protect your Microsoft 365 accounts from pervasive attacks.

Barracuda researchers have revealed a startling rise in account takeover, one of the fastest growing email security threats. A recent analysis of account-takeover attacks targeted at Barracuda customers found that 20 percent of organizations had their Microsoft 365 accounts compromised by hackers in March 2022. Our research of almost 12,000 compromised Microsoft 365 accounts showed that they were used to send over 3 million malicious messages and spam.

Hackers executed the account-takeover attacks using a variety of methods. In some cases, hackers leveraged usernames and passwords acquired in previous data breaches. Because people often use the same password for different accounts, hackers were able to reuse stolen credentials and gain access to additional accounts. Hackers also use stolen passwords for personal emails and use access to that account to try to get access to business email. Brute-force attacks are also used in account takeover attacks because many people use very simple passwords are that easy to guess, and they don't change them often enough. Attacks also come via web and business applications, including SMS.

With more than half of all global businesses already using Microsoft 365, and adoption continuing to grow quickly, hackers are turning increasingly to account takeover because it gives them a gateway into your network and data.

Here's a closer look at account takeover and solutions to help detect and block attacks.

Highlighted Threat

Account Takeover

Cybercriminals use brand impersonation, social engineering, and phishing to steal login credentials and access Microsoft 365 accounts. Once the account is compromised, hackers moniter and track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled, so they can launch successful attacks, including harvesting additional login credentials for other accounts.

The Details

Microsoft 365 account-takeover attacks begin with infiltration. Microsoft is the world's most impersonated brand used in 57% of phishing attacks. Cybercriminals rely on social-engineering tactics to try to trick email recipients into visiting a phishing website and disclosing their login credentials.

Once the account has been compromised, hackers rarely launch an attack right away. Instead, they moniter email and track activity in the company, to maximize the chances of executing a successful attack. As part of their reconnaissance, scammers often set up mailbox rules to hide or delete any emails they send from the compromised account. In the March 2022 analysis performed by Barracuda researchers, hackers set up malicious rules to hide their activity in 36 percent of the nearly 12,000 compromised accounts.

After the reconnaissance has been performed, cybercriminals use the harvested credentials to target other high-value accounts, especially executives and finance department employees, to try to harvest their credentials through spear phishing and brand impersonation. For example, scammers use email to impersonate a trusted entity, such as a well-known company or a commonly-used business application. Typically, attackers try to get recipients to give up account credentials or click on malicious links. Attackers often use domain-spoofing techniques or lookalike domains to make their impersonation attempts convincing.

Hackers also use compromised accounts to monetize attacks by stealing personal, financial, and confidential data and using it to commit identity theft, fraud, and other crimes. Compromised accounts are also used to launch external attacks targeting partners and customers. With conversation hijacking, hackers insert themselves into important conversations or threads, such as during a wire transfer or other financial transaction.

Protecting Your Business

Take advantage of artificial intelligence

Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against spear-phishing attacks, including business email compromise and brand impersonation. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachment. Using machine learning to analyze normal communication patterns within your organization allows the solution to spot anomalies that may indicate an attack.

Deploy account-takeover protection

Some of the most devastating and successful spear-phishing attacks originate from compromised accounts, so be sure scammers aren't using your organization as a base camp to launch these attacks. Deploy technology that uses artificial intelligence to recognize when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

Use multifactor authentication

Multi-factor authentication, also called MFA, two-factor authentication, and two-step verification, provides an additional layer of security above and beyond username and password, such as an authentication code, thumb print, or retinal scan.

Monitor inbox rules and suspicious logins

Use technology to identify suspicious activity, including logins from unusual locations and IP addresses, a potential sign of a compromised account. Be sure to also monitor email accounts for malicious inbox rules, as they are often used as part of account takeover. Criminals log into the account, create forwarding rules and hide or delete any email they send from the account, to try to hide their tracks.

Train staffers to recognize and report attacks

Educate users about spear-phishing attacks by making it part of security-awareness training. Ensure staffers can recognize these attacks understand their fraudulent nature, and know how to report them. Use phishing simulation for emails, voicemail, and SMS to train users to identify cyberattacks, test the effectiveness of your training, and evaluate the users most vulnerable to attacks. Help employees avoid making costly mistakes by creating guidelines that put procedures in place to confirm requests that come in by email, including making wire transfers and buying gift cards.

Your journey, secured.