Threat of the Month: Office 365 Phishing

Phishing and cloud email

As the popularity of cloud-based email has grown, attackers have crafted phishing campaigns to mimic popular cloud services, such as Office 365. They start out by building phishing sites meant to look like the Office 365 login page. Next, they send phishing emails to users, hoping to trick them into visiting the site and entering their user names and passwords. The attackers gather up the stolen credentials from the phishing site so that they can use them in further attacks

What can happen if an account is phished?

further malicious activities. This is especially concerning because, since they're logging into legitimate accounts, these attacks are now coming from within your organization. Attackers can spread malware, spam, and phishing internally. They can carry out tailored attacks such as spear phishing or Business Email Compromise. They can even target your partners and customers. Attacks are not isolated to sending further malicious emails either. Having access to a company's email system, there are a number of other reconnaissance-based attacks that they can perform. They can pull down global company email address lists. They can scan the compromised account for other credentials, as well as personal or company information. These types of activities can easily go unnoticed simply due to their passive nature–the attacker is quietly gathering information, as opposed to aggressively attacking systems and users.

The move to the cloud

There are a lot of advantages to hosting company email in the cloud. First and foremost, it takes a lot of headaches out of the administration of email services. It also simplifies the user experience, giving users the option to go to a single login point, enter their company credentials, and log right into their corporate email account from anywhere they choose.

Factor in the reduction in costs that cloud hosted email can bring, and it sounds like the ideal solution.

Further reading

https://blogs.cisco.com/security/office-365-phishing

https://www.us-cert.gov/ncas/analysisreports/AR19-133A

How common are these attacks?

Over the last few quarters there has been a measurable increase in the number of phishing emails that impersonate Microsoft. In fact, between January and March, more than 50 percent of phishing attempts that impersonate well-known brands masqueraded as emails from Microsoft.

What about security in cloud offerings?

To its credit, Microsoft has included several security features in Office 365. However, in terms of phishing attacks, the malicious actors are carrying out their attacks outside of Microsoft's network. This means that unfortunately the security features in Office 365 cannot prevent them.

How does Cisco protect you?

Cisco Email Security	Leading, advanced protections against phishing, spam, malware, and other threats
Cisco Umbrella	Can be used to identify and block domains involved in phishing attacks.
Duo Trusted Access	Multi-factor authentication can prevent malicious actors accessing compromised accounts.
Cisco Threat Response	Used to integrate threat responses across multiple products, including email security, to visualize, validate, and stop threats faster.

06/19