What Phishing Threats are EbbingPast Perimeter Technology?

What are we seeing in the wild?

Business Email Compromise (BEC)

Credible emails can open doors. But once the door is open, the threat actors turn on the creativity. New tactics and techniques ensure that malware payloads still reach their targets. Soon as anti-malware defenses evolve, threat actors turn on the creativity. New tactics and techniques ensure that malware payloads still reach their targets.

Cloud Filesharing Abuse

Microsoft Exchange, Windows Groups, and OneDrive, get tangled up pretty badly. The critical flaw in Microsoft Equation Editor was heavily exploited to deliver malware via malicious attachments. We expect the danger to ebb as more security teams patch it.

In June 2019, a new strain of GandCrab ransomware was delivered in high-volume phishing campaigns.

WHY PHISHING STAINS ARE SHRINKING

BUSINESS EMAIL COMPROMISE (BEC)

Of verified phish were identified in environments with one or more SEGs whereas 2,681,000 phishing emails delivered in high-volume phish.

DEFENDERS HAVE HOLES, ALL NETS

Unique Emotet malware domains used in a single day by the Emotet botnet

WHO Phishing Threats are Squirmimg in the Wild

Unique ransomware families over the last 12 months used

What are we seeing in the wild?

Phishing Threats & Malware Review 2019 is based on research by the Cofense Phishing & Malware Defense Center™ from October 2018 to March 2019. We have analyzed over 31,000 malicious emails reported by customers’ users. This data is augmented below by findings from the Cofense Research and Cofense Intelligence™ teams.

Unique credential phishing attacks found in environments with one or more SEGs

The Emotet botnet is lord and master of the malware landscape. Emotet relies on compromised sites to deliver its payloads.

The onslaught of credential phishing attacks results in targeting payroll administrators to reroute direct deposits. BEC occurs less frequently than other security threats, but inflicts billions of dollars in losses. Traditionally a wire transfer scam aimed at CFOs, Business Email Compromise has shifted to targeting payroll administrators to reroute direct deposits.

Business Email compromise is prevalent across all business sizes and industries, but is most visible in larger organizations with more complex networks. Beginning in mid-2018, Business Email Compromise began to increase in frequency, but still outpace other security threats, but inflicts billions of dollars in losses.

Verified BEC attacks, but inflicts billions of dollars in losses.

The past 12 months have seen a 20% decline in the volume of email-based ransomware attacks. But in a ominous sign, the average ransom demand has steadily increased over the last two years. But threat actors still use ransomware against healthcare, technology and manufacturing, as well as other Global 1000 entities that are now more visible to cyber threat actors.

Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks.

DEFENDERS HAVE HOLES, ALL NETS

Unique ransomware families over the last 12 months used 11,000.

If all business environments use a single SEG, they still face 10% risk of compromise.

WHAT Phishing Threats are Squirmimg in the Wild

If all business environments use a single SEG,itter environments still face 64% risk of compromise.