ALL NETS HAVE HOLES

90% **OF VERIFIED PHISHING EMAILS WERE FOUND IN ENVIRONMENTS USING SECURE EMAIL GATEWAYS (SEGS)**

This key finding[1] in the Cofense™ Phishing Threat & Malware Review 2019 is based on research by the Cofense Phishing Defense Center™. From October 2018 to March 2019, our team verified over 31,000 malicious emails reported by customers' users. This data is augmented below by findings from the Cofense Research and Cofense Intelligence™ teams.

WHAT PHISHING THREATS ARE SQUIRMING PAST PERIMETER TECHNOLOGY?

CREDENTIAL PHISH

The onslaught of credential phishing shows no signs of letting up. Threat actors are seeking network credentials, the keys to the enterprise kingdom.

nearly 75%
Of verified phish were credential phish

91.2%
Of credential phishing attacks were found in environments with one or more SEGs

almost 300,000
Distinct credential phishing URL's have been identified in the wild since Q1 2018
Source: Cofense Research

MALWARE DELIVERY

The game of Whack-A-Mole continues. As soon as anti-malware defenses evolve, threat actors turn on the creativity. New tactics and techniques ensure that malware payloads still reach their targets.

over 4,800
Verified phishing emails that delivered malware

89.6%
Of phishing attacks delivering malware were found in environments with one or more SEGs

BUSINESS EMAIL COMPROMISE (BEC)

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

2,681
Verified BEC attacks

$26B
In global business losses due to BEC attacks
Source: FBI, Sept 2019

88.1%
Of BEC attacks were found in environments with one or more SEGs

CLOUD FILESHARING ABUSE

Two Microsoft services, Sharepoint and OneDrive, got roughed up pretty badly. We analyzed over 9,000 phish that abused cloud filesharing services and found:

55%
Of payloads were hosted on Sharepoint

21%
Of payloads were hosted on OneDrive

WHAT ARE WE SEEING IN THE WILD?

EMOTET

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

678,000
Unique Emotet malware infections through April 2019
Source: Cofense Research

over 500
Unique domains used on a single day by the Emotet botnet
Source: Cofense Research

CVE-2017-11882

A geezer as vulnerabilities go (it dates back to 2000), this 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.

45%
Of all malicious attachments over the last 12 months exploited CVE-2017-11882

22%
Of all malicious attachments over the last 12 months used malicious macros

RANSOMWARE

And finally, a ray of hope. Ransomware has steadily declined over the last two years. But threat actors still use ransomware against select high-profile targets.

Fewer Than 10
Unique ransomware families delivered in high-volume phishing campaigns
Source: Cofense Intelligence

64%
Of these total campaigns delivered GandCrab ransomware. It's the king crab in a smaller sea.

GET THE FULL STORY— DOWNLOAD THE REPORT

Download your copy of our Phishing Threats & Malware Review 2019.

[1] Identified SEG providers included Barracuda, BitDefender, Cisco Ironport, CloudMark, Cyren, Fortinet, Kaspersky, Microsoft Exchange Online Protection, Microsoft Advanced Threat Protection, Mimecast, Proofpoint, Symantec Email Security, and Trend Micro.