SONICWALL®



EXECUTIVE BRIEF

You've Got Scam: Why Email is Your Primary Threat Vector

Most of today's devastating breaches still start with a single email.

Abstract

Phishing is not just about getting you to click a link to launch malware. More insidiously, it's about stealing power-user credentials. This allows criminals to gain access, send emails, make financial requests and spread malicious code everywhere that user's identity is authorized to go.

Email remains a primary threat vector. Organizations need to stay vigilant about protecting employees against advanced phishing and malware attacks starting as Business Email Compromise (BEC), email impersonation and fraud.

Introduction

People send nearly 320 billion emails a day. Email remains a primary way people share information – and threats. COVID-19 and work-from-home initiatives have contributed to email being the most extensive channel for all forms of phishing and ransomware attacks.

We've learned from past major data breaches that advanced attacks often involve multiple tactics, techniques and procedures to compromise the user. Typically, email is the starting point for social engineering attacks, such as BEC or credential phishing attacks.

For example, the 2020 Verizon Data Breach Report states that 22% of breaches involved social engineering, and 96% of those breaches came through email. In the same report, another 22% of breaches resulted from human failure where sensitive data is sent accidentally to the wrong recipient.

Another study by 451 Research found that while 87% of organizations have an email security product already deployed, 46% admit email still poses the most significant data risk. Also, 46% cited email as the biggest vulnerability, almost five times above their next-greatest concerns.

Microsoft and Google dominate the global cloud-based email market, as part of their broader office suite offerings. Worldwide market share of office suite technologies is split between Google and Microsoft. Globally, Gmail is the most popular email platform with over 1.8 billion users. As of year's end 2020, Microsoft Office 365 was used by over a million companies worldwide, with over 650,000 companies in the US alone using that suite.

Tempted by this massive pool of potential victims, criminals are constantly investing in new to scam users of these cloud-based email services. This makes cloud-based email one of the most desirable and lucrative attack vectors for opportunistic hackers.



The persistent effectiveness of phishing and email fraud

The crafting of phishing emails to look genuine sent from stolen or fake or stolen known identities can trick even the most trained and security-conscious users. Despite security education efforts, phishing attacks continue to be cited often as a weak link in security. Security leaders we've spoken with still see users clicking on targeted theme- and event-based phishing emails that have been personalized to mimic legitimate emails. Many are unable to discern legitimate emails from fake ones, recognize suspicious links or take cautionary actions such as authenticating the URL, sender's identity and company website.

What's more, propagation is simply human nature. Email and attachments between employees, partners, customers – not to mention family and friends - are prevalent in today's remote, collaborative workforce. We accept them because they are trusted identities, and because we need access to content and information to carry out our collective work.

Business Email Compromise

BEC tops the list for email impersonation and fraud. This type of attack typically involves using a compromised CEO or other executive-level email account. Scammers use the compromised account to send fraudulent financial requests, such as paying off a fake invoice or wiring money to close a phony business deal.

In most cases, social engineering or credential whaling attacks are behind the hijacking of higher-level executive accounts to carry out such attacks. The FBI's Internet Crime Complaint Center (IC3) reports that cybercrime in 2020 exceeded $4.1 billion, with BEC at $1.8 billion causing the most financial damage as a single threat vector.

It's too late once you realize that an executive's credentials have been compromised. It takes only one compromised account to create a viral reaction among user-to-user, device-to-device, and app-to-app that can be impossible to contain before damages occur.

Native cloud security is not enough

Email security developers have created ways to protect users from malicious links that bypass pre-delivery filters and reach the inbox, such as click-time protection, post-delivery retraction and web-browser filters. However, attackers are equally devoted to creating ways to reach the inbox.

A recent 2020 Microsoft ATP Report found that more than one in ten targeted phishing emails can reach the user's inbox. Each unique attack leverages various combinations of obfuscation methods explicitly designed to bypass Microsoft's Exchange Online Protection (EOP) and Advanced Threat Protection (ATP).

Some widespread email-born attacks bypass email security filters with a high degree of success. One example of these attacks is a low-volume, high-quality targeted phishing email that looks like it comes from Office 365 or Gmail. It renders well, personalizes, and is sent to a specific set of users rather than through a traditional high-volume campaign. These attacks are sophisticated in both their technique to reach the inbox and the user experience on the backend. Each link typically includes the user's email address so that the login page looks like the second page of the account challenge when you try to go to an admin page when you are logging in. It knows who you are and serves analytics on the backside.

The phishing innovation curve is now happening post-delivery. Meaning, instead of putting the malicious URL in the email, phishers link to a redirect server that acts as a gateway, sending queries from a security company to a benign site. In contrast, queries from the intended victims are directed to the phishing server.

Although Microsoft ATP applies four main policy engines for anti-phishing, spoof intelligence, Safe Links, and Safe Attachments, it is still a rule-based security technology. The security scan relies solely on static reputation-based filtering that hackers can reverse engineer until they find ways in which to bypass these filters. This weakness in the security layer puts enterprises in a state of constant risk, threatened by the likelihood of someone in their organization opening the wrong file, clicking a bad URL, or entering a password in the wrong place.

The visibility and access to the large population of cloud email users make them easy targets for every hacker. Never have they given so many user accounts and mailboxes with identical security. Hackers also leverage the fact that these cloud accounts are sources of authentication to other enterprise SaaS apps to spread malware or steal data. This is the real and present danger of the cloud security monoculture. What bypasses one bypasses all.

SiteCloak is a good example of such a technique currently being used to bypass Microsoft 365 ATP Safe Links, also known as click-time protection. It takes phish obfuscation to the next level by using various tactics and techniques to hide the true intent of the target page, which is often a credential-harvesting page.

Victims of SiteCloak don't need to input their email addresses. They are taken directly to the password entry page, where the credential harvesting page uses the "Zero Font" technique to bypass Microsoft's email scanners. It places random characters of font size zero between characters on the page so Microsoft's natural-language filters would see the random text while human readers see what the attackers want them to see. In other words, Safe Links thinks it's a benign page while a realistic-looking credential harvesting page to the victim. Attackers enable the malicious content only after the email message has reached the inbox.

Conclusions

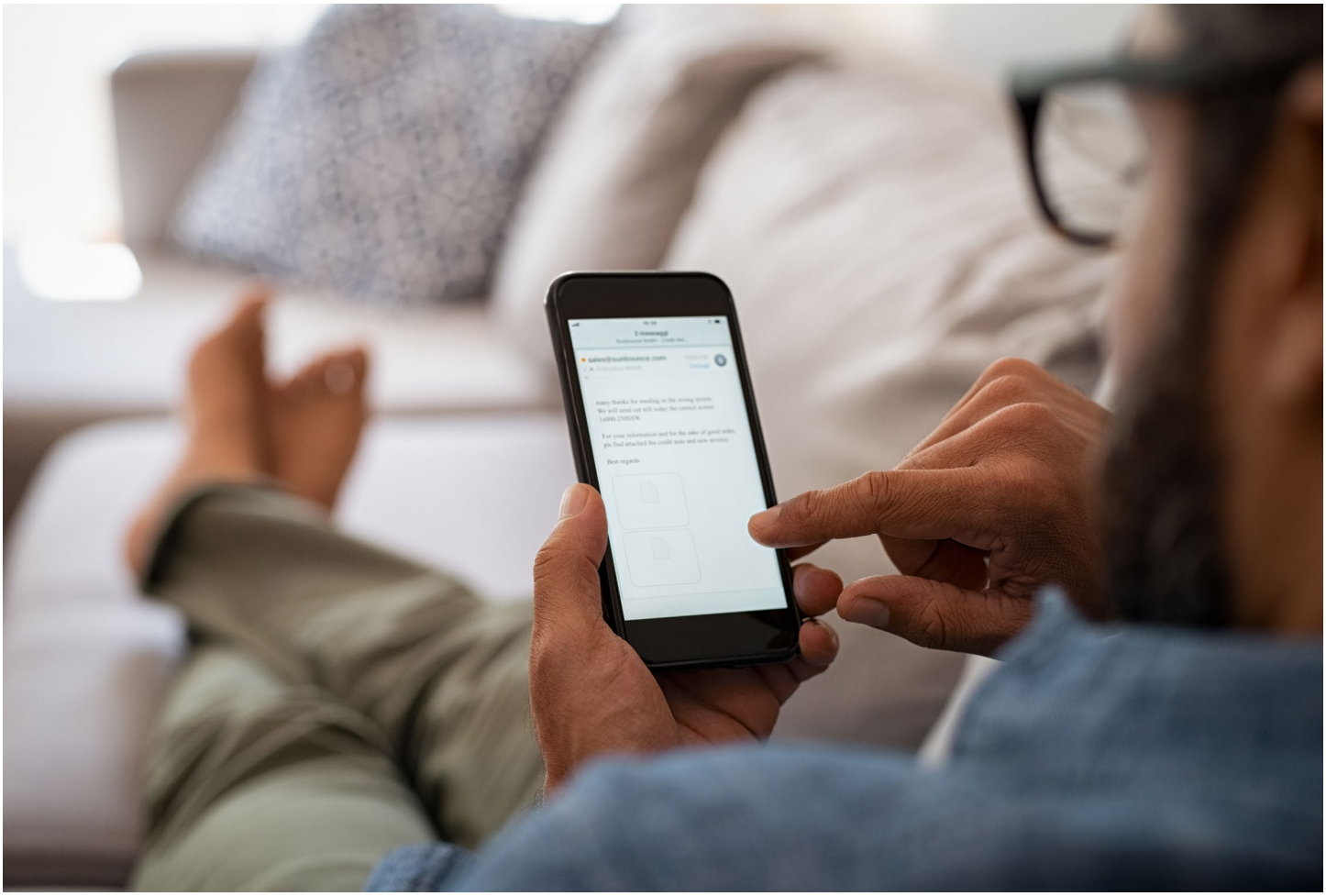
SiteCloak and other forms of email fraud exemplify that hackers can evade detection using well-researched and highly prepared personalized phishing attacks. These will not be the last that slips past cloud vendors' security filters. Businesses need additional levels of protection beyond what the built-in security of cloud office system provides.

SonicWall Email Security can be deployed as a robust virtual appliance, software application, hosted service or hardened physical appliance — ideal for organizations that need a dedicated on-premises solution. SonicWall's multi-layered solution provides comprehensive inbound and outbound protection. It defends against advanced email-borne threats such as ransomware, zero-day threats, spear phishing and business email compromise (BEC).

Learn more at www.sonicwall.com/email-security.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2021 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

ExecBrief-EmailThreatVector-US-COG-5264