SONICWALL®

EXECUTIVE BRIEF

Is Your 0365 and G-Suite Email Really Secure?

Why native cloud security is not enough

ABSTRACT

Cloud-based 0365 and G-Suite email communication is ubiquitous across today's organizations. Yet it is also a prime vector for cyberattacks that bypass native defense and Security Email Gateways (SEGs). This brief examines inherent security gaps, and requirements to truly secure cloud-based email against today's sophisticated attacks.

INTRODUCTION

According to a 451 Research study1, nearly 9 out of 10 organizations have an email security product already deployed. Yet almost half of surveyed respondents admit email still poses the greatest data threat. This is higher by a wide margin compared with other threats in the study. And nearly half cite email as their biggest vulnerability.

Cybercriminals that generate email-borne threats are quick to respond to mega-trends. The work-from-home movement and COVID-19 are just latest examples of what makes email traffic the ideal channel of attacks. Because email remains the primary way we communicate and share data for both professionally and personally, billions of people use email daily. However, most haven't been well-trained to discern legitimate emails from fake ones, recognize suspicious links or to take cautionary actions such as authenticating the URL or sender's company website.

Also, cybercriminals are so adept at crafting of phishing emails to look genuine today that even security-savvy users can be tricked. For example, phishing attacks emulating Coronavirus Aid, Relief, and Economic Security (CARES) Act email took advantage of anxious and confused victims during the COVID-19 pandemic.

With such a massive pool of fresh and unknowing victims, all sharing the same security monoculture, hackers have shifted and multiplied their attacks to cloud services like Office 365 and G Suite. There is no better target and bigger prize as their combined users increase double digits growth yearly. This no doubt continues to make cloud email and office suite applications the most desirable and lucrative attack vectors for all types of opportunistic hackers.

According to Verizon's 2019 Data Breach Investigations Report[2], 90% of attacks started with a phishingemail. Approximately 60% of the time, the compromised web application vector was the front-end to cloud-based email servers. Cloud-based email services create several security challenges:

- Native cloud security is not enough
- SEGs are not built for the cloud
- SEGs only secure inbound and outbound emails
- SEGs are limited to email
- SEGs broadcast themselves to hackers

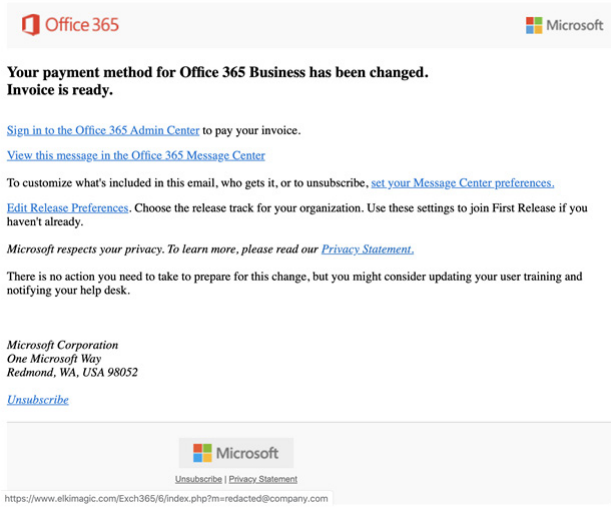
Native cloud security is not enough

A recent 2020 Microsoft ATP Report[3] found that, of over five hundred thousand messages analyzed, more than one in ten targeted phishing emails can reach the user's inbox.

Each unique attack leverages various obfuscation methods designed specifically to bypass Microsoft ATP. These proven techniques include multiple redirections, URL splits, HTML tag manipulation, polymorphic malware, and dynamic obfuscated scripts.

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 like traditional SEGs. 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 places enterprises in a state of constant risk, threatened by the likelihood of someone in their organization opens the wrong file, clicks on the wrong URL and/or enters the password in the wrong place.

Some attacks appear legitimately sent from Microsoft, as shown in Figure 1, below. They render very well, are professionally personalized, and sent to a specific set of users rather than the whole company.


Office 365

Microsoft

Your payment method for Office 365 Business has been changed.
Invoice is ready.

Sign in to the Office 365 Admin Center to pay your invoice.

View this message in the Office 365 Message Center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message Center preferences.

Edit Release Preferences. Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

Microsoft

Unsubscribe | Privacy Statement

https://www.elkimagic.com/Exch365/6/index.php?m=redacted@company.com

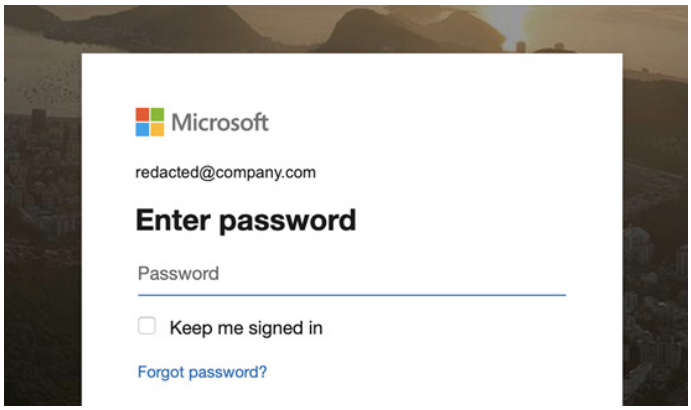


Figure 1

These attacks are sophisticated in both their technique to reach the inbox and the user experience on the back end. Each link included the user's email address so that the log-in page they land on looks like the second page of a Microsoft account challenge, which is exactly what happen when you try to go to an admin page when you are already logged in. The attack demonstrated that it already knows the victim's identity.

Figure 2, below, examines the same sample attack campaign across multiple organizations during the testing period. In almost every case, whether an organization saw 5 or 50, most of the malicious emails bypassed EOP and ATP. In two cases show with the blue bar, EOP was able to eventually block the attack, but only after missing over 30 instances of the attack.

The widespread adoption of Office 365 and G-Suite makes it an easy target for every hacker. Never have so many mailboxes had identical security. Hackers also leverage the fact that these cloud accounts are sources of authentication to other enterprise SaaS apps. This is the danger of cloud security monoculture. What bypasses one, bypasses all.

Hackers have consistently demonstrated their ingenuity to evade detection using targeted phishing attacks, and escape cloud vendors' security filters. Organizations clearly need additional levels of protection beyond that of Microsoft ATP and other SEGs.

SEGs are not built for the cloud

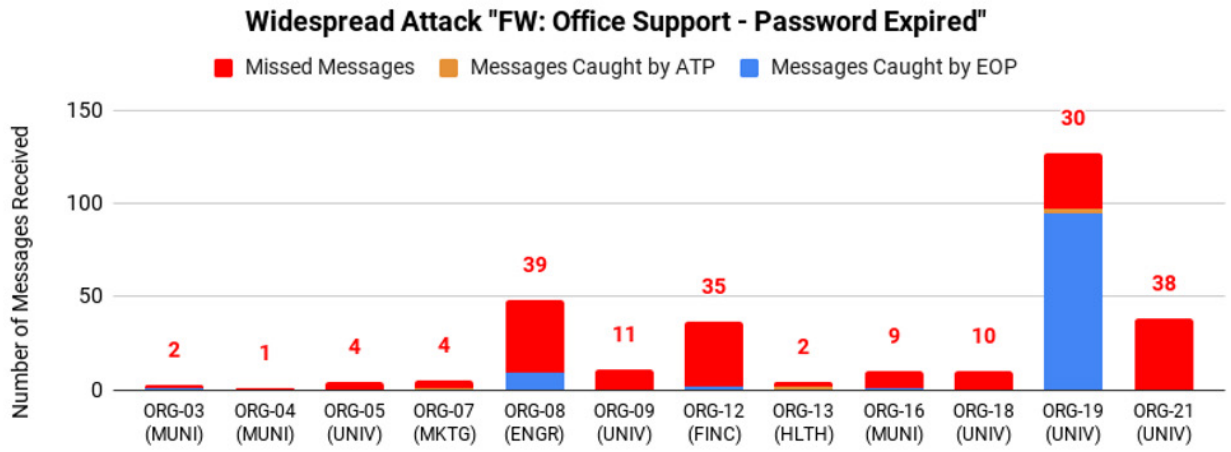
SEGs were originally designed around a hardened perimeter to secure on-prem email environments. As email moves to the cloud via services like Office 365 Email and Gmail, SEGs retooled and adapted to this new environment. However, the approach suffers many shortcomings due to their non-native design.

The greatest SEG deficiency is the impediment to existing security. Their required changes to MX records impairs or completely erases embedded filters. This means that instead of augmenting security scans, they completely replace the default, and in turn deactivate valuable defenses from those inherent layers. Moreover, because these solutions are deployed at the perimeter, they have limited visibility. They are typically blind to internal threats such as compromised accounts and employee-to-employee messages.

SEGs only secure inbound and outbound emails

Since SEGs connect to the mail flow outside of the email provider's cloud, internal emails are not scanned for threats.

SONICWALL



In a cloud environment, account compromise is much more common because of credential access. Internal emails can be just as threat borne as inbound and outbound emails.

Some email gateways use journaling rules to scan internal emails. However, this method only scans emails post-delivery, and does not prevent the email from making it to the inbox. This does not adequately protect users from malicious internal emails, since the email is clickable by the recipient in the time between the delivery and the scan.

SEGs are limited to email

In a cloud environment, email is not the only attack vector. File sharing, messaging applications, and other SaaS-based applications are all interconnected, providing additional channels for threats to reach users within an organization. The inbox-level protection that SEGs provide simply does not suffice in this interconnected landscape. Unless the customer purchases add-on security modules, SEGs do not have visibility to these connected applications. As a result, they cannot identify threats in that part of the environment.

SEGs broadcast themselves to hackers

In order to reroute email through a SEG, an organization must change their MX records to that of the gateway. This is public information through sites like MXToolbox, which enables hackers to design targeted attacks tailored to bypass the scan of a specific SEG.

Conclusion

Email-borne cyberattacks are on the rise and more sophisticated than ever. A layered approach is vital to closing security gaps. SonicWall Cloud App Security (CAS) delivers full-suite protection for cloud email and SaaS applications. It catches email-borne and zero-day attacks that Microsoft and SEG solutions miss via a multi-layered inline threat prevention system that easily deploys within minutes via API. CAS stops Business Email Compromise, targeted phishing, malware, zero-days, account takeover and insider threats across your enterprise.

Learn more. *Visit www.sonicwall.com/cas.*

[1]451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects, Q1 2019

[2]https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[3]https://track.eng.sonicwall.com/browse/WWW2-3226

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

SolutionBrief-CASforOffice365-COG-3021