



PHISHING WITH THE CLOUD

ONE MILLION WAYS ATTACKERS
BREACH OFFICE 365 EMAIL



EXECUTIVE SUMMARY

A decade ago in October 2010, Microsoft unveiled its cloud-based Office 365 platform. Touted then as one of the “moments in time when technology transforms the workplace,” Microsoft’s prediction has certainly come true. In Q3 2020, Microsoft reported **258 million paid Office 365** business seats; Gartner reports that **71 percent** of companies now use cloud or hybrid cloud email, primarily from Microsoft.

Yet, technology evolution doesn’t happen in isolation: cyber threat actors have also evolved with (and thrived because of) — the cloud.

This report examines the top threats missed by Office 365 and well-known secure email gateways (SEGs), based on an analysis of more than **1.5 billion messages** sent to 18 organizations across different industries. We found that in one six-month period (March to August 2020), Office 365 and well-known SEGs missed **nearly 1 million** — over **925,000** — **phishing emails**.

Additional findings included:

- In one example where a customer layered Office 365 with an SEG, **more than 300,000 malicious messages** were still missed;
- There was a **steady increase in targeted Business Email Compromise (BEC) attacks** — which would have amounted to several billion dollars in potential losses; and
- **Spoofed senders and newly registered domains (NRDs) accounted for 71.7 percent** of the missed email threats;
- The **summer months saw a sharp increase in phishing**, as attackers **took advantage of** coronavirus-related misinformation and remote workforce transitions.

Not only are threat actors exploiting Office 365 to launch new campaigns, but victims themselves are Office 365 users, complicating defense measures. A 2018 **report** from the U.S. Council of Economic Advisers pointed out cloud computing’s inherent vulnerabilities: there is *“a great degree of risk correlation between firms from cyber threats that otherwise would not exist if the firms’ data and services were located locally.”* Multi-tenant, cloud-first webmail plus cloud collaboration tools have also created economies of scale attractive to bad cyber actors hosting massive phishing campaigns.

Consider bad actors’ “nothing-is-sacred” approach to exploiting COVID-19. For example, our researchers have **observed** attackers launching Microsoft OneDrive-branded phishing campaigns under the guise of “sharing” CARES Act accounting information. Attackers have also **utilized Microsoft SharePoint and Microsoft Planner** to phish for user credentials, based on the premise of bonus pay for essential workers.

The good news is, despite the staggeringly large volume of phishing messages still getting through, Microsoft continues to improve Office 365’s native security defenses, including its Advanced Threat Protection (ATP). Additionally, more organizations are starting to invest in a layered approach to protecting cloud email, as noted in the latest Gartner Market Guide for Email Security (ID: G00722358).

However, because **96 percent of phishing attacks come through email**, the first step to closing any potential Office 365 security gaps is to understand all the different ways attackers breach Office 365 email.

Read on for more insights.



President & CEO, Area 1 Security

DISSECTING OFFICE 365'S TOP MISSED THREATS

When it comes to enterprise email and collaboration, Microsoft is a familiar name. With the increase of work-from-home employees in 2020, Microsoft's user base has continued to grow, especially for their Microsoft 365 (formerly named Office 365) product suite, which surpassed 258 million paid business seats in 2020.¹

The increase in users isn't just good for Microsoft's bottom line; cyber attackers are also benefiting. Office 365's growing user base means a larger attack surface area — and more targets. As one of the most popular enterprise collaboration tools, Office 365 offers plenty of possibilities for attackers to reach victims. Office 365's attack surface area ranges from external attacks originating outside the enterprise, to internal attacks within the organization, partner accounts, and through Microsoft's varied storage and collaboration tools.

When companies move their email infrastructure to the cloud, they have a certain expectation of security. When it comes to commodity security services, such as anti-spam and anti-virus, Microsoft's offerings are very effective and on par with some of the best anti-spam and anti-virus providers out there. **Yet advanced threats, such as Types 1-4 Business Email Compromise (BEC) attacks, continue to plague Office 365 email.**

With so many avenues for attack within the Microsoft environment, security vendors have built extensive defenses, such as Microsoft's own Advanced Threat Protection (ATP), in hopes of solving the problem. However, when it comes to advanced threats, these defenses fall short of the mark.

With a third of confirmed data breaches involving phishing and 96% of phishing attacks coming through email, missed phishing attacks are still a big problem.²

Over a recent six-month period, Area 1 Security analyzed over **1.5 billion email messages** from customers using Microsoft as their email provider. Some of these customers also had purpose-built secure email gateways (SEGs) deployed, like Proofpoint and Mimecast, to protect users from advanced threats. Despite these additional security measures, Area 1 Security discovered **more than 925,000 missed malicious messages and emails** that slipped through. In this report, we'll take a closer look at the top threats missed by Office 365 and legacy email security vendors.

¹ <https://venturebeat.com/2020/07/22/microsoft-earnings-q4-2020/>

² <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

TOP MISSED THREATS IN OFFICE 365 EMAIL ENVIRONMENTS

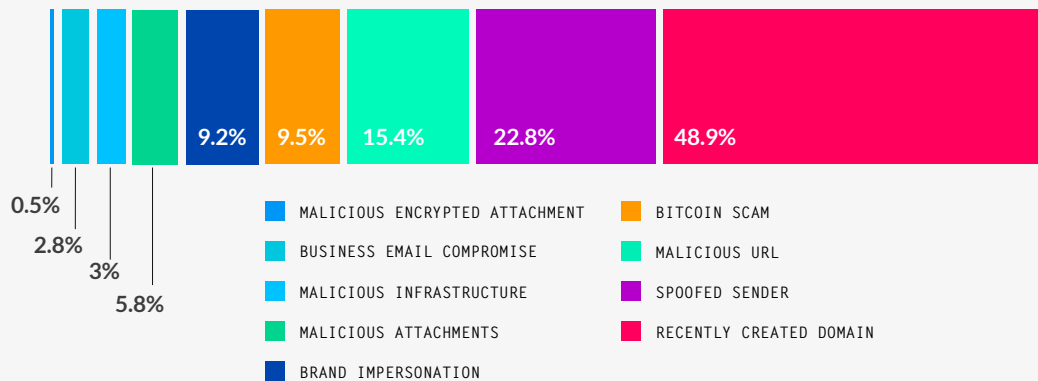


FIG. 1. BREAKDOWN OF TYPES OF MALICIOUS THREATS AND PHISH MISSED BY OFFICE 365 AND LEGACY EMAIL SECURITY VENDORS.

In our sample, the overall missed threat rate was “only” **0.06%**, but this still resulted in hundreds of thousands of missed threats that could have reached end user inboxes.³ Any one of these threats could also have been the source of a cyber breach resulting in financial repercussions, loss of intellectual property, and degradation of brand reputation.

NO VACATION FOR ATTACKERS

Despite the uncertainty and business disruptions in 2020 caused by the COVID-19 global pandemic, attackers did not seem to suffer a loss of productivity, as seen in the monthly missed threats breakdown in Fig. 2 below. **In fact, attackers took advantage of the pandemic to target companies as they transitioned to support a remote workforce.**

This instability has created a window of opportunity as workers try to figure out how to juggle remote work amongst various domestic challenges. This sudden change in work conditions have also dramatically

increased remote employees’ security risks due to a lack of enterprise security tools and reassigned security staff.

With working-from-home now the norm, Gartner has also named securing the remote workforce as 2020’s top security project.⁴ Remote work statistics support this; nearly half of global businesses have experienced a cybersecurity scare since moving to remote work.⁵ The FBI has also experienced a 4x increase in cybercrime reports since the onset of the pandemic.⁶

³ All missed threat data in this report was taken from production environments where Area 1 was inline in “blocking mode.”

All these threats were detected and stopped by Area 1.

⁴ <https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/>

⁵ <https://www.helpnetsecurity.com/2020/06/17/work-from-home-security>

⁶ <https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/>

MALICIOUS VERDICTS BY MONTH

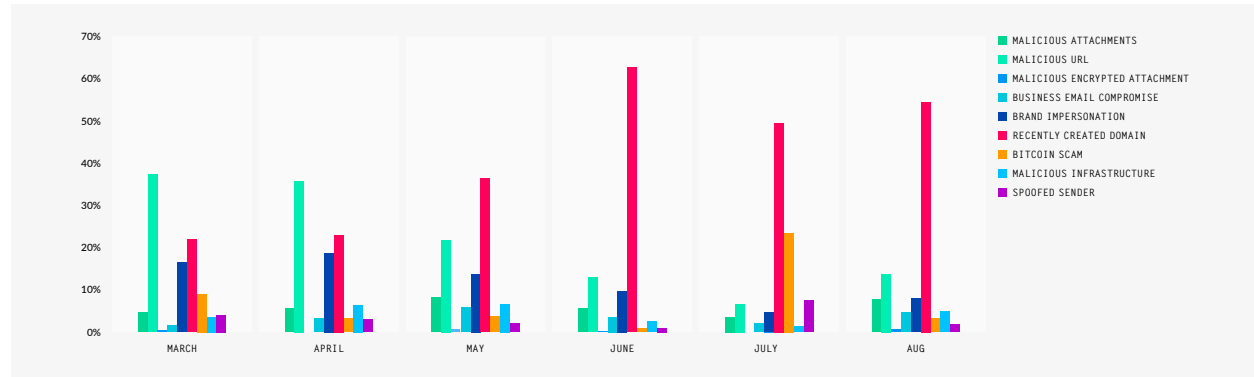


FIG. 2. THREAT TYPES IN OFFICE 365 EMAIL ENVIRONMENTS BY MONTHS IN 2020, AS A PERCENTAGE OF MISSED THREATS.

Our data also tells a parallel story of increasing threats. The large spike of recently created domains, Bitcoin scams, and spoofed emails in the summer 2020 months suggest attackers (like many required to shelter-in-place) also canceled their vacation and kept right on working. Other threat types remained fairly constant in the first few months and saw a substantial increase in August 2020.

THREAT SPOTLIGHT: BUSINESS EMAIL COMPROMISE (BEC)

One of the most dangerous and financially damaging types of phishing, Business Email Compromise, or BEC, relies on social engineering and exploitation of business processes instead of malware. According to the FBI, over 80% of organizations have suffered a BEC attack, with total loss comprising \$26 billion since 2016.⁷

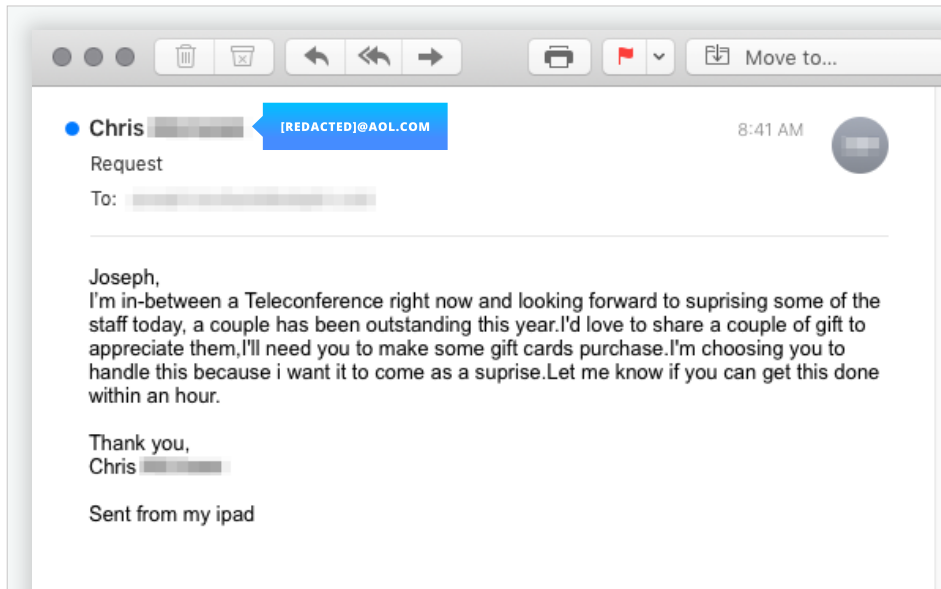
While BEC attacks have been around since the 2010s, they have become increasingly sophisticated, leveraging current events as lures. **Here's a quick breakdown of the different types of BECs and a deep-dive example of each type.** (A detailed explanation of each BEC type is also available in our [Guide to BEC](#) ebook.)

BEC PHISHING EVOLUTION



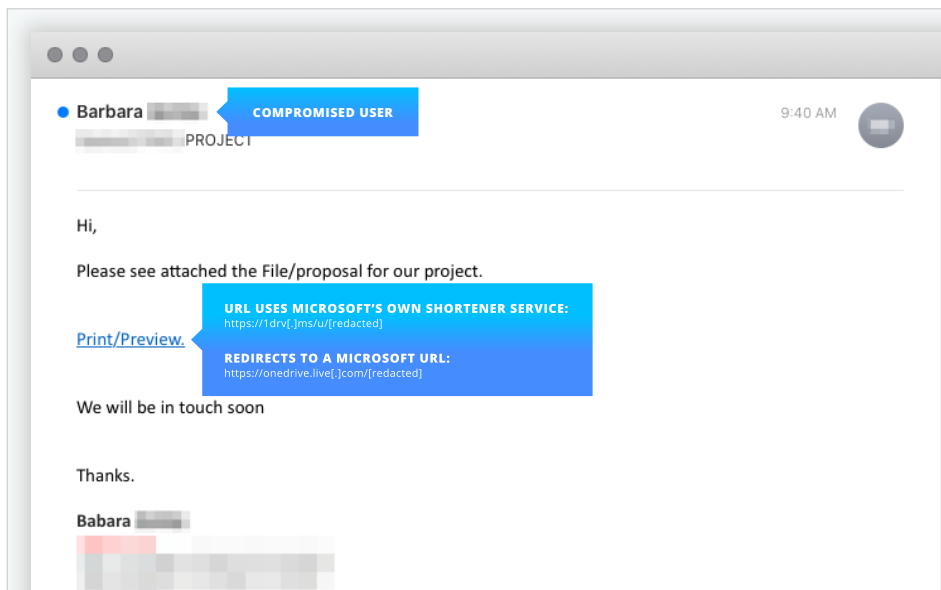
⁷ Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). "2019 Internet Crime Report," Feb. 11, 2020

BASIC TYPE 1 BEC: SPOOFED SENDER DOMAIN, CXO IMPERSONATION



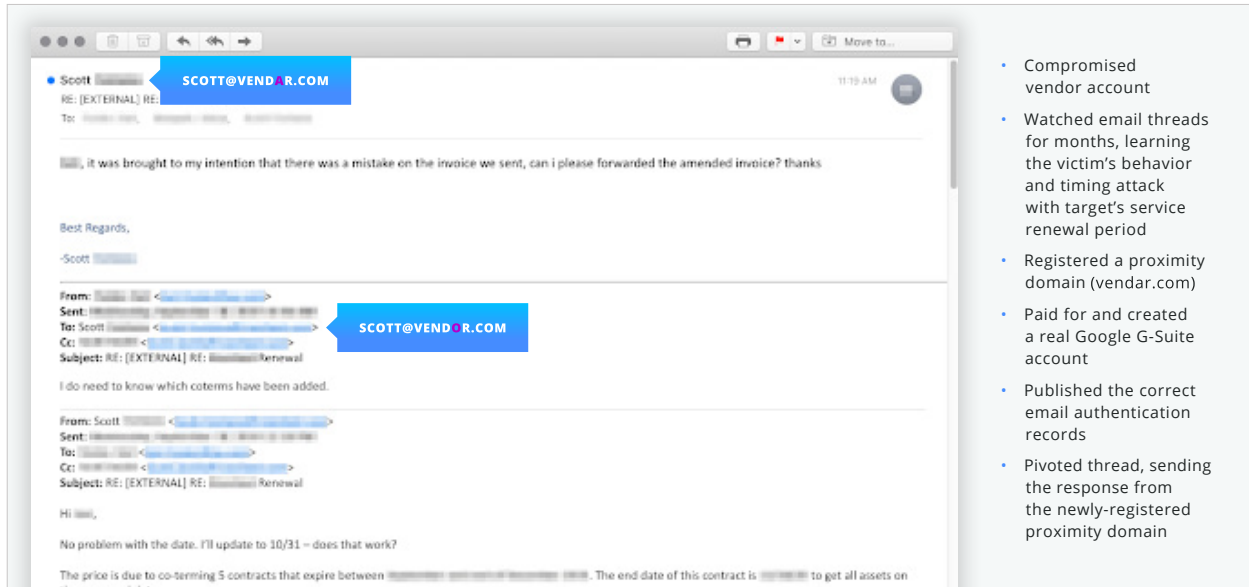
- Attacker uses a compromised AOL account
- Impersonates CXO
- Message passes email authentication (SPF, DKIM and DMARC)

ADVANCED TYPE 2 BEC: COMPROMISED EMPLOYEE



- Attacker uses a compromised employee's account to phish another colleague
- Uses a Microsoft URL shortener to mask link
- URL redirects to a credential harvester hosted on Microsoft OneDrive account
- Even users with security awareness training can be fooled by "legitimate" Microsoft Live link when hovering over URL

SOPHISTICATED TYPE 3 & 4 BEC: COMPROMISED BUSINESS PARTNER



- Compromised vendor account
- Watched email threads for months, learning the victim's behavior and timing attack with target's service renewal period
- Registered a proximity domain (vendar.com)
- Paid for and created a real Google G-Suite account
- Published the correct email authentication records
- Pivoted thread, sending the response from the newly-registered proximity domain

MISSED BEC THREATS

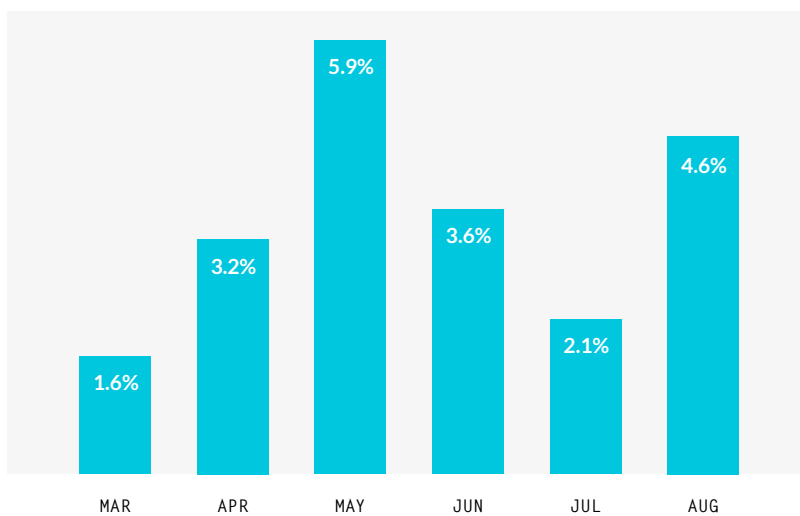


FIG. 3. MISSED BEC THREATS IN OFFICE 365 EMAIL ENVIRONMENTS OVER A SIX MONTH PERIOD IN 2020, AS A PERCENTAGE OF MISSED THREATS.

While the volume of BEC phishing was relatively low compared to other types of attacks, we did see a steady increase in their numbers over the six-month period considered in our data (Fig. 3).

Considering the average wire-transfer loss is \$80,000 per BEC attack, this would have amounted to several billion dollars in losses.⁸

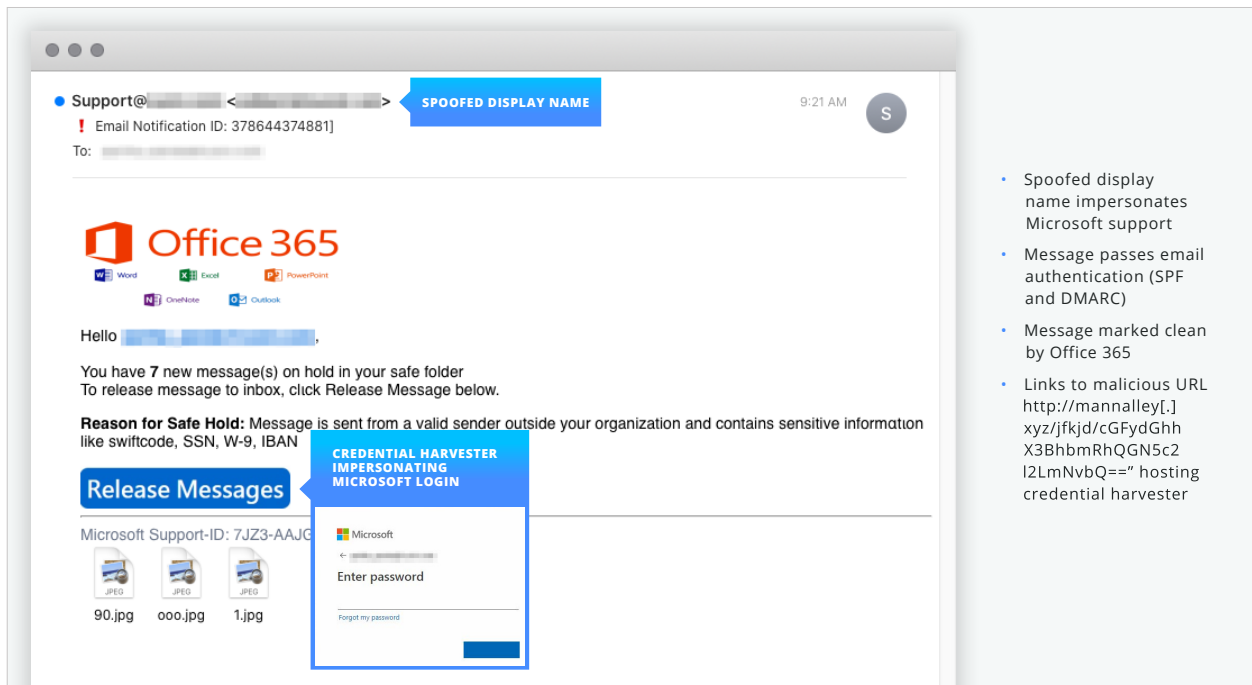
⁸ <https://threatpost.com/bec-wire-transfers-average-80k/158914/>

THREAT SPOTLIGHT: CREDENTIAL PHISHING

Credentials are the No. 1 type of data compromised in phishing attacks, leading to the parallel correlation that breaches involving actual malware have decreased by over 40%.⁹

Ironically, **attackers often use Microsoft's own tools and branding against them**, targeting Office 365 credentials and impersonating password reset notices from Microsoft or IT admins, as seen in the example attack intercepted by Area 1 below.

CREDENTIAL PHISHING ATTACK



The screenshot shows an email interface with a spoofed sender 'Support@...' and a 'SPOOFED DISPLAY NAME' callout. The email body features the Office 365 logo and a message about 7 new messages on hold. A 'Release Messages' button is present. Below it, a 'Microsoft Support-ID: 7JZ3-AAJG' link is shown. A callout box points to a link labeled 'CREDENTIAL HARVESTER IMPERSONATING MICROSOFT LOGIN' which leads to a password entry page.

- Spoofed display name impersonates Microsoft support
- Message passes email authentication (SPF and DMARC)
- Message marked clean by Office 365
- Links to malicious URL `http://mannalley[.]xyz/jfkjd/cGFydGhhX3BhbmRhQGN5c2l2LmNvbQ==` hosting credential harvester

⁹ <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

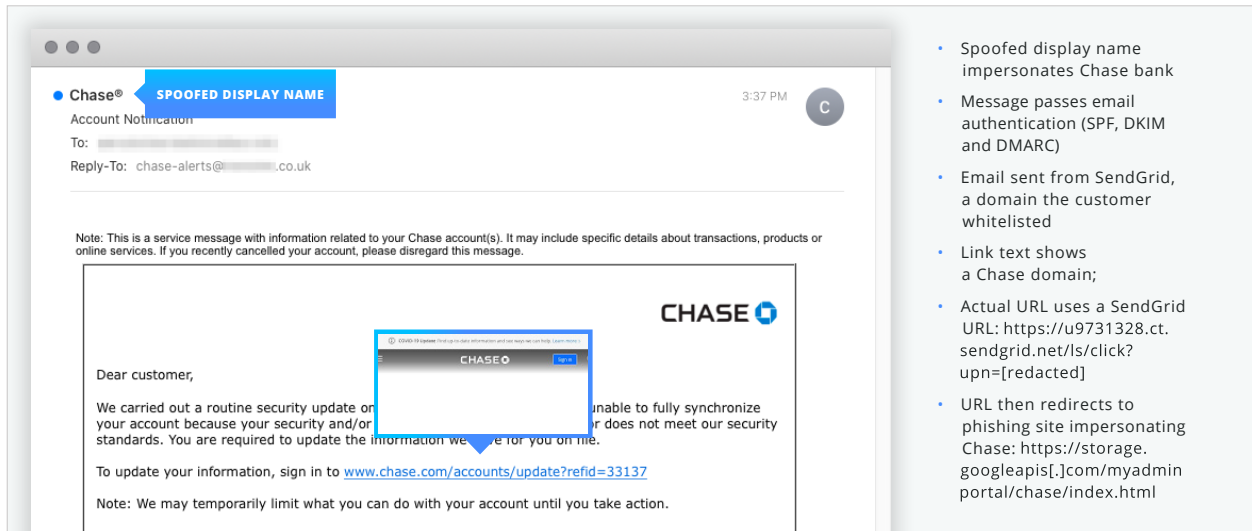
THREAT SPOTLIGHT: BRAND IMPERSONATION

Brand impersonation is a tactic used by attackers to make malicious emails and websites appear legitimate by stealing branding elements like names, logos and site designs. Attackers often go to great lengths to trick users, hiring web designers to recreate malicious sites

that look almost exactly like the legitimate sites they're impersonating.

Here's an example breakdown of a brand impersonation phish that bypassed Office 365, as well as passed SPF, DKIM and DMARC:

BRAND IMPERSONATION PHISH



The screenshot shows an email interface with a spoofed sender name 'Chase®' and a 'SPOOFED DISPLAY NAME' label. The email content includes a note about a security update and a link to a phishing site. The right-hand list details the following:

- Spoofed display name impersonates Chase bank
- Message passes email authentication (SPF, DKIM and DMARC)
- Email sent from SendGrid, a domain the customer whitelisted
- Link text shows a Chase domain;
- Actual URL uses a SendGrid URL: `https://u9731328.ct.sendgrid.net/ls/click?upn=[redacted]`
- URL then redirects to phishing site impersonating Chase: `https://storage.googleapis[.]com/myadminportal/chase/index.html`

MISSED BRAND IMPERSONATION THREATS

In our data, we saw a steady increase in brand impersonation phishing within our six month window (Fig. 4).

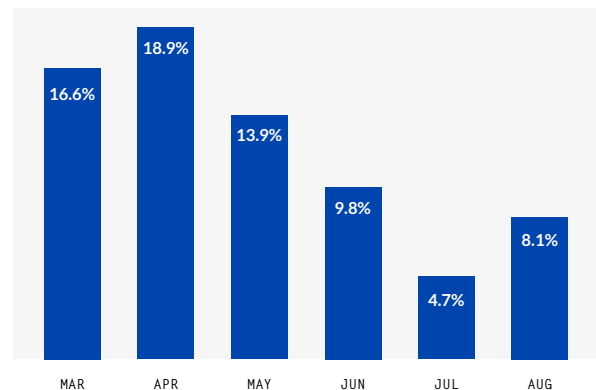


FIG. 4. MISSED BRAND IMPERSONATION PHISHING IN OFFICE 365 EMAIL ENVIRONMENTS OVER A SIX-MONTH PERIOD IN 2020, AS A PERCENTAGE OF MISSED THREATS.

! COVID-19 PHISHING: GLOBAL PANDEMIC LEADS TO A PHISHING OUTBREAK

Threat actors are nothing if not opportunistic, picking up the latest trending topics to use as lures. In the case of COVID-19, threat actors capitalized on the panic surrounding the global pandemic, resulting in a spike in coronavirus-themed phishing.

Shortly after the World Health Organization declared COVID-19 a pandemic on March 13, 2020, Area 1's [security researchers](#) detected over 88,000 [corona-virus-related phish](#) within a single day.

COVID-19 PHISHING DETECTIONS

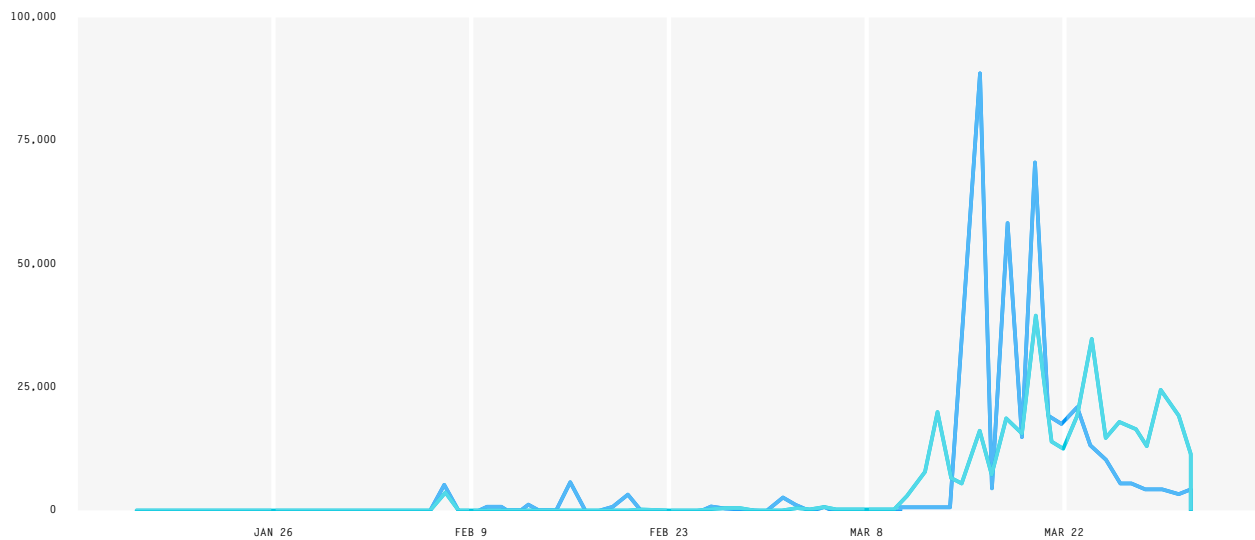


FIG. 5. COVID-19-RELATED PHISHING DETECTIONS MADE BY AREA 1 SHORTLY AFTER PANDEMIC DECLARATION.



Watch our threat research team's on-demand COVID-19 webinar to see a detailed breakdown of coronavirus-related phishing attacks from spring 2020.

PLENTY OF PHISH

Why so much phish? The short answer, from an economic standpoint, is because it's become a cheaper tactic.

Widespread adoption of cloud-based services and free webmail have tipped the economies of scale in favor of the attackers. It is far easier and cheaper to use an established, reputable provider to host malicious content than to compromise systems. Cloud email providers like Office 365 and Gmail allow organizations to host their email domains for a nominal cost, making these options a financially attractive way for attackers to defeat email authentication protocols.

In fact, solely relying on email authentication results, like SPF, DKIM, and DMARC, can create a false sense of security and even lend legitimacy to phishing emails.

Email authentication has also turned out to be an error-prone technology to implement, with companies often confusing the inbound and outbound uses cases of email authentication.

Attackers have found ways to easily defeat email authentication by using webmail, exploiting the difficulty in deploying it correctly and inconsistencies with its enforcement. At the end of the day, **email authentication simply fails to stop phish.**

Additionally, evasive techniques such as using images instead of text in email, hosting malware on newly-created domains without reputation, and nesting malicious URLs mean that plenty of phishing messages continue to slip through legacy email security vendors.

SECURE EMAIL GATEWAYS AREN'T ENOUGH

As previously mentioned, some deployments in our analysis employed a SEG in addition to Office 365's native defenses. These deployments didn't fare much better in terms of catching phish, **missing more than 300,000 malicious messages** within a single customer environment in some cases (Fig. 6).

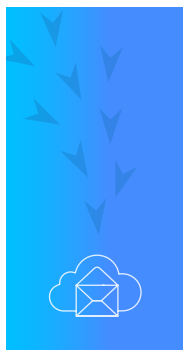


FIG. 6. MISSED DETECTIONS BY VENDOR ON SAMPLE DATA COLLECTED OVER A SIX MONTHS PERIOD.

These SEGs were deployed as the MX record, providing a first line of defense against phishing emails before "clean" messages are delivered into Office 365, where Office 365 gets the opportunity to apply its own detection technologies. In other words, the missed phish that were identified in these heavily fortified email environments were missed by both the SEG and Office 365.

HOW TO PROTECT YOUR OFFICE 365 EMAIL ENVIRONMENT

It's clear from these findings that attackers are constantly looking for new ways to circumvent Office 365's native defenses. Additionally, even if email authentication (DMARC, SPF, DKIM) is properly configured and enabled, phishing messages can still get through. SEGs are also falling short when it comes to stopping advanced phishing and targeted attacks.



Gartner's 2020 Market Guide for Email Security (ID G00722358), states that "Gartner clients report dissatisfaction with natively available capabilities [of G Suite and Office 365] and are, therefore, choosing to supplement with third-party products, as discussed in the Representative Vendors section."

The guide goes on to note that "there are also a number of solutions now positioned as an alternative to an SEG. These integrated email security solutions (IESSs) provide many of the capabilities in an SEG such as advanced malware protection, sandbox analysis and URL analysis, intercepting malicious emails before they reach a user's inbox. When used in combination with the native capabilities provided by Google and Microsoft, these can be a viable alternative to gateway protection."

ADVANCED DETECTION TECHNOLOGIES FOR PROTECTING CLOUD EMAIL ENVIRONMENTS

At Area 1 Security (a Representative Vendor for Integrated Email Security Solutions in Gartner's 2020 Market Guide for Email Security), our preemptive technology employs proprietary ActiveSensors™ that crawl the web at massive scale to reveal emergent campaign infrastructure and aggregate attack data. Our Small Pattern Analytics Engine, SPARSE™, also identifies phishing attack infrastructure, patterns of attack formation and threats within datasets generated by the ActiveSensors network.

Effectively defending against cloud email threats also requires:

- **Comprehensive email security techniques:** These should include AI and Machine Learning (ML) models, computer vision, Natural Language Understanding (NLU) and intent analysis, among other advances.
- **Creating an automated social/partner graph for your organization:** Identify your partner organizations and perform universal message classification to understand

the natural interactions the organization has with the rest of the world.

- **Combining preemptive threat data, message sentiment analysis and conversational context analysis:** This provides a high level of accuracy into the malicious detections, especially in cases where a partner has been compromised and becomes the source of targeted phishing attacks.

Finally, as threat actor patterns evolve, it's important to ensure that your phishing detection models are continually enhanced, to proactively identify and stop phishing attacks *before* they launch.

To learn more about Area 1 Security's preemptive capabilities and how to protect your Office 365 environment from advanced phishing attacks, watch our "Office 365, Compromised" on-demand webinar, or request a complimentary Phishing Risk Assessment.