MICROSOFT DEFENDER FOR OFFICE 365: IS IT GOOD ENOUGH?

A SPECIAL ANALYSIS

About This Report

This report shares an analysis of Microsoft 365 Email Security with its Defender Security product. To prepare this report, the Check Point Email Research Team (previously Avanan) analyzed three million real-world emails to evaluate the efficacy of Microsoft Defender for Microsoft 365.

In general, Microsoft 365 is a very secure service. That is a result of a massive and continuous investment from Microsoft. What this report does note is the challenge that Microsoft faces. As the default security for most organizations, many hackers design their attacks to bypass Microsoft's security. An excellent example of how hackers focus on Microsoft 365 comes in a series of blogs from Microsoft that details the attempts of a state-sponsored group to compromise their services.

This is most likely why we see a significant percentage of attacks bypassing Microsoft security. In this context, it's important to note that this does not mean that Microsoft's security has worsened. The hackers improved and learned more methods to obfuscate and bypass the default security.

For this reason, Check Point's security experts recommend that our customers add an extra layer of security on top of the default security provided by their cloud email service.

This report will offer data on Defender's effectiveness and explore how Defender fares in organizations of different sizes. We'll closely examine how the "Dumpster Diving" phenomenon still hurts organizations and show how Defender fares against various types of phishing. And finally, we'll summarize how these numbers affect your SOC and your business.

This report obviously could not analyze all Microsoft 365 customers. It is derived from analyzing customers using Microsoft Defender who also have Check Point's Email Security Solution. The results should be taken as a general guide to Microsoft's efficacy. We estimate that the data set is large enough to constitute a statistically representative sample of Microsoft 365 customers with some variance in the results for different organizations.

The Results

Check Point's research team found that **18.8% of phishing emails** bypassed Microsoft Exchange Online Protection (EOP) and Defender to make it to a user's inbox.

This is a **74% increase** compared to our previous report from February 2020, where we used a similar analysis method and found that only 10.8% of phishing emails were missed.

For the 2022 report, Check Point analyzed nearly 3,000,000 emails scanned by Microsoft Defender during one week. The four organizations in our sample ranged from 500 to 20,000 users, were from major industries, and were located in all parts of the United States.

We picked these organizations because they run both Microsoft Defender and Harmony Email and Collaboration Security (HEC). Because HEC runs inline behind Defender and connects via API, we can look at the following to help with classifications:

- Email headers added by Defender after files have been scanned but before they are released into quarantine, junk folders, or user inboxes
- Defender quarantine folder and event logs

We then analyzed the messages that Check Point's HEC classified as phishing, but EOP and Microsoft Defender did not. Without Check Point, these emails would have been delivered to the inbox. That number of emails classified as phishing by Check Point divided by the total email attacks gives us the percentage of missed phishing emails.

This increase may be due to a few factors. We conducted our previous analysis in February 2020, before COVID-19. At that time, we found that 10.8% of phishing emails bypassed Microsoft and made it into the inbox. Since then, the number of attacks has increased by almost 100%, focusing on sophisticated phishing campaigns that bypass built-in security.

Defender's Missed Phishing Rate is Higher in Larger Organizations

Our analysis found that when deployed in larger organizations, Microsoft Defender missed more phishing emails. The missed phishing rate for two large organizations in our research was 50-70%.

This is a change from our 2020 analysis. In 2020, we found no correlation between company size and missed phishing rate. We speculate that hackers are now focusing more of their efforts on more prominent organizations and, in particular, the advanced attacks that they don't want to 'waste' on targets less lucrative for them.

Remote work is another factor that may be at play. We conducted our 2020 analysis just before the COVID-19 pandemic. Now, many more employees are working from home, the volume of attacks has increased, and Business Email Compromise (BEC) and ransomware demands have become headline news worldwide.

For reasons we will discuss later in the report, the type of attacks used by bad actors is changing. Our analysis found that targeted financial attacks are specifically crafted to bypass Defender. Financial-based phishing attacks refer to many attack types, including fake invoice scams, fraudulent Bitcoin transfers, phony business proposals, fake wire transfer requests, and more. Defender misses 42% of these types of attacks. Financial attacks are more common against large organizations. The Verizon Data Breach Investigation Report confirms that financially motivated attacks are the most common attack vector.

The Dumpster Diving Problem

Another part of our analysis included emails Defender forwarded to a user's Junk Folder. In May 2020, Avanan coined the term Dumpster Diving. This refers to the practice where marketing emails, subscriptions, and targeted phishing attacks are commingled in the Junk folder, making them immediately accessible to the end-user. Many organizations send all Defender detections to the Junk folder. They deem this preferable to sending Defender detections to quarantine because it reduces the risk of blocking legitimate emails.

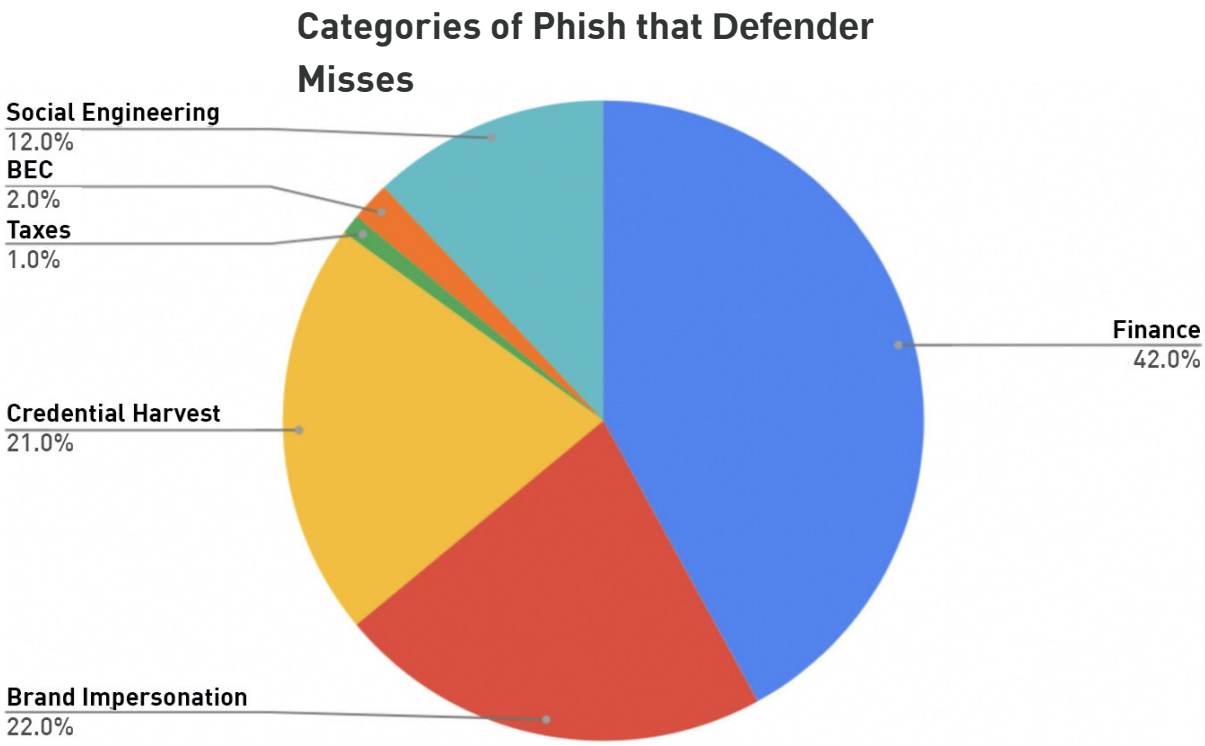
We found that, on average, Defender sends 7% of phishing messages to the Junk folder. End-users become accustomed to dumpster diving in the Junk folder for legitimate messages. Users may act on a phishing email by mistake with many emails to root through in the junk folder with no distinction between treasure and trash.

In some attacks, an additional email of high reputation points the recipient to the search their Junk folder for the message. We've seen the text in attacks such as: "Did you get my message? Please check your Junk folder. If you don't find it, let me know, and I'll resend it. The subject should be 'X.'" This attack serves two purposes. First, it sends the recipients Dumpster Diving through dangerous phishing emails. Second, when the email is found, the end-user tends to give it more validity as if the second email confirms the first is legitimate.

Forwarding phishing to the junk folder is very risky and one of the critical weaknesses in the Microsoft Defender and EOP.

Defender Versus Different Types of Threats

The following pie chart breaks down the attacks by categories:



As a quick overview, here are brief definitions of these types of phishing:

- **Finance, 42%:** This category refers to attacks having to make money, ranging from bitcoin scams to invoice fraud, fake wire transfers, and more
- **Brand impersonation, 22%:** This category refers to phishing emails that look like they are coming from a popular and legitimate brand

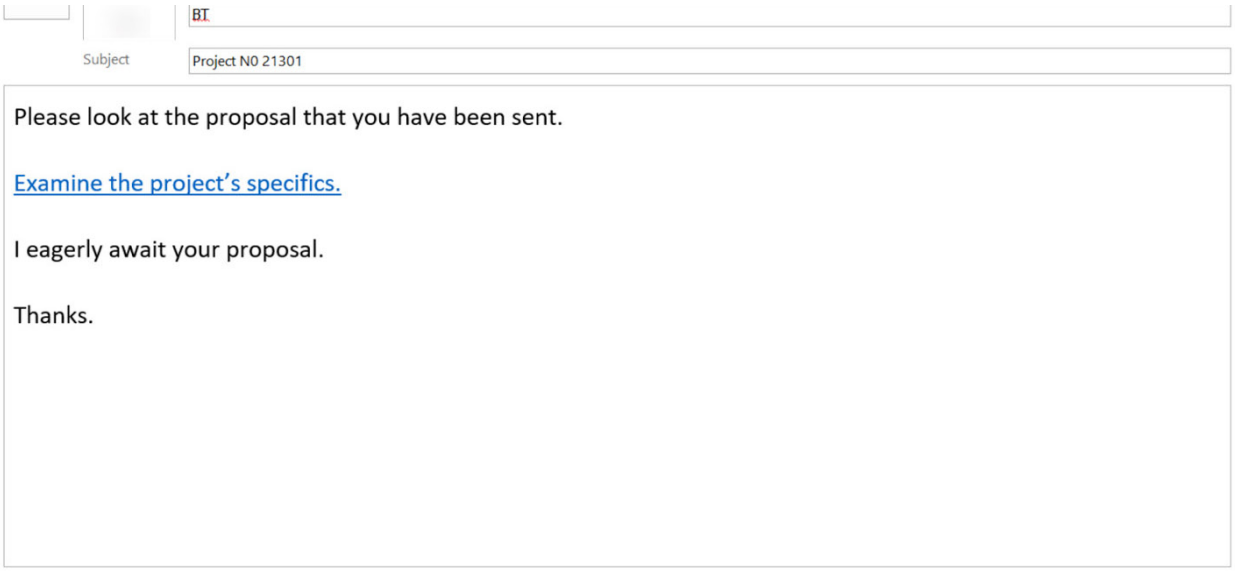
- **Credential harvest, 21%:** This is a broad category that refers to types of phishing emails with the overall goal of stealing usernames and passwords
- **Social engineering, 12%:** This is another broad category that refers to the idea of hackers tricking a user into doing something they don't want to do
- **Business Email Compromise, 2%:** Business Email Compromise (BEC) is a popular attack form that sees a hacker impersonating an executive, asking an underling for urgent action
- **Taxes, 1%:** This is a subset of phishing that takes advantage of tax fears to extract money

As discussed previously, targeted financial attacks are often successful against Defender. This broad category includes anything involving money – fake invoices, bitcoin transfers, etc. These scams tend to hit the enterprise space in larger quantities.

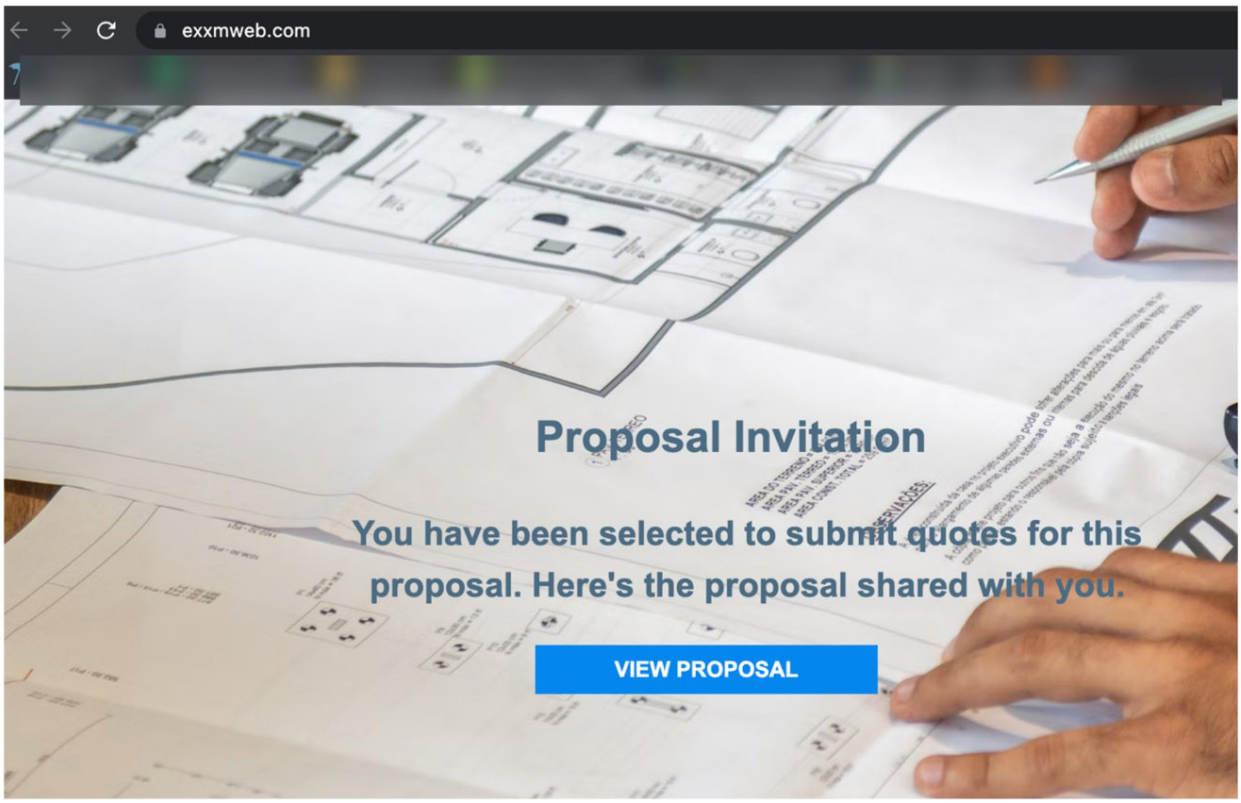
As discussed previously, targeted financial attacks are often successful against Defender. This broad category includes anything involving money – fake invoices, bitcoin transfers, etc. These scams tend to hit the enterprise space in larger quantities.

The email below shows an example of a financial scam missed by Defender. If a user clicks the purported business proposal link, it takes them to a fake Microsoft 365 portal.

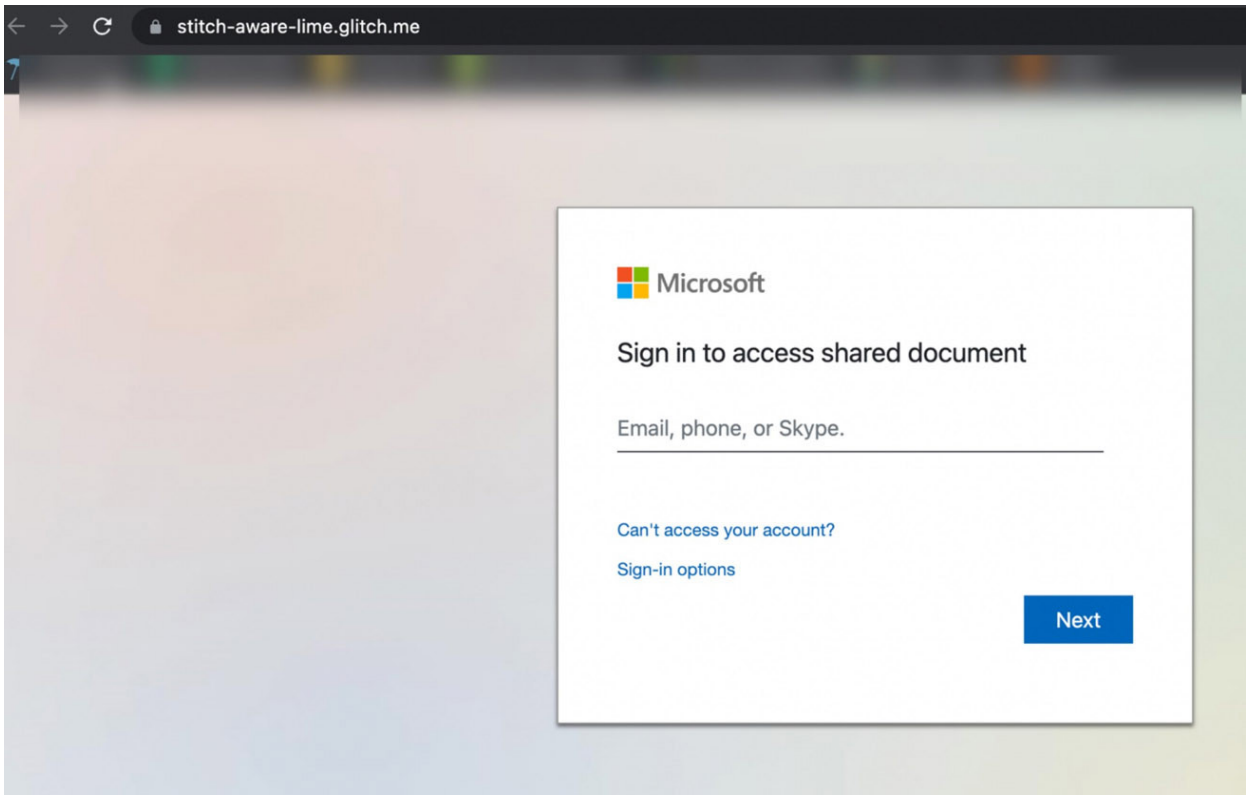
There are a few 'tells' in the email. In the body, notice how a zero is used in place of the letter 'o' in the subject.



After clicking, users are directed to these pages. Pay attention to the strange URL and the off-center text.

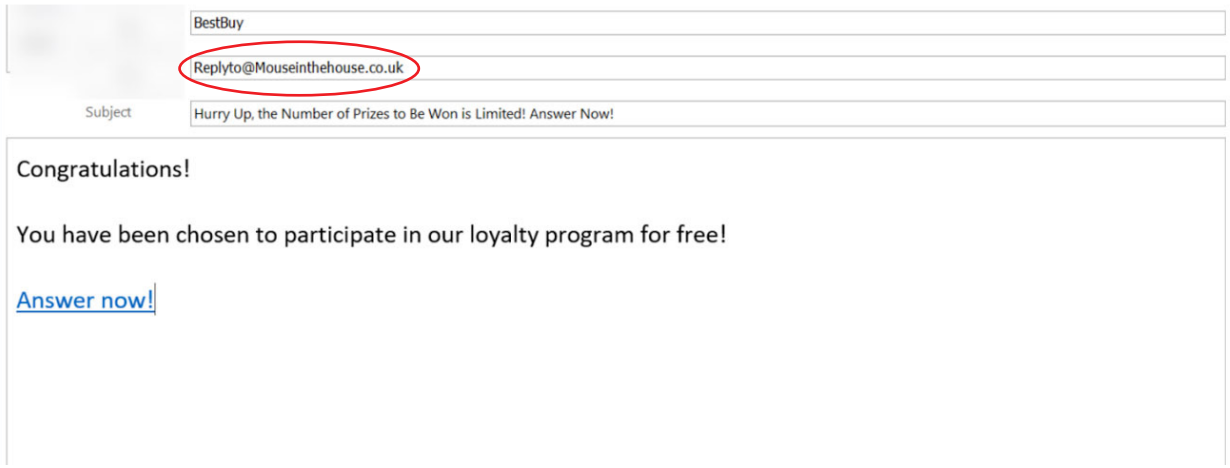


After clicking "View Proposal," the user is taken to this spoof of a Microsoft login page. Notice the random URL.



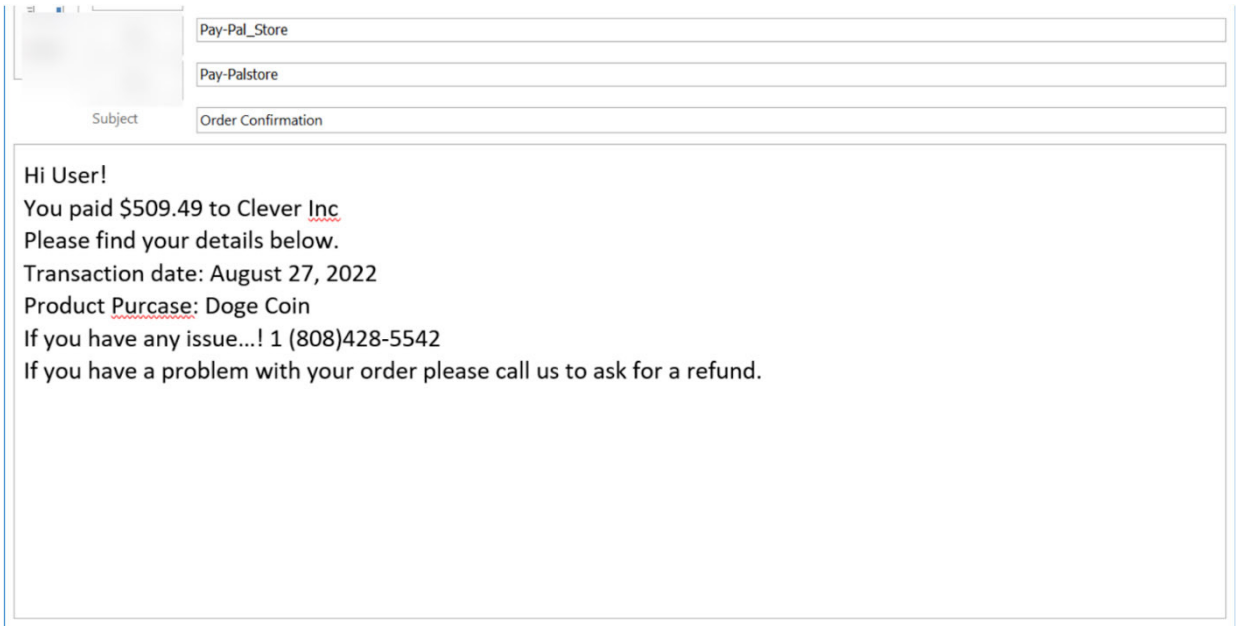
Brand impersonation is another method hackers choose to bypass Defender. These emails claim to come from a well-known brand but are a hacker trying to get information.

In the attack shown below, hackers spoof Best Buy. However, the reply-to address offers some clues as to its legitimacy.



Finally, credential harvesting attacks saw success against Defender. The idea is to steal something from the end user. These attacks range from attempts to harvest Microsoft 365 login credentials to something more sophisticated, like the attack seen below.

In this attack, the end-user sees an email from what appears to be PayPal. It shows a purchase of $509.49. At the bottom, it encourages recipients to call a phone number if they do not recognize the transaction. When they reach the number, it gets routed to a 'support rep' who asks for banking information.

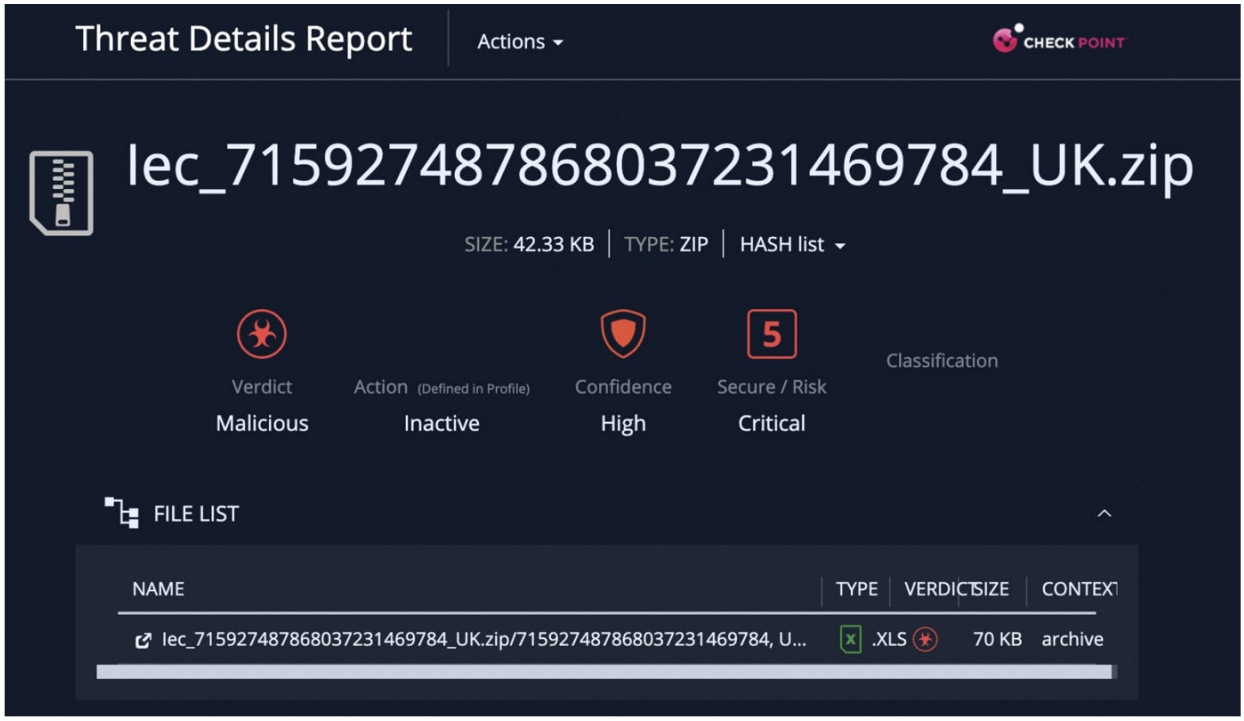


Malicious Files

Malware propagating through files remains a significant attack vector. These are often considered separately from phishing, but too often, phishing techniques lead to malicious content and vice-versa. The goal is to infect the endpoint for remote control or ransomware.

For example, Microsoft Defender missed the real-world email below and delivered it to an end-user's inbox. It describes a business proposal. While this email doesn't look like a traditional phishing attack, the file attached to the document is a macro-infested Excel document.

Check Point Research's analysis of the infected file shows it's malicious and a critical security risk.



The Impact on the Security Operations Center

Combating the rise in missed phishing attacks falls on the SOC team. To evaluate the impact on the SOC, we compared our customers in HEC's prevent mode, which actively blocks malicious emails, with two customers using HEC's Monitor Only mode. In Monitor Only, SOC staff will be alerted to issues, but the problems will need to be assessed and responded to manually. Check Point found that manually managing email problems takes up to 23% of the staff's total time. That work involves remediating email threats, responding to end-user requests, and more. In some environments, that number is even higher.

Another method we used to evaluate the load on the SOC team was to look at the time spent by SOC staff before and after deploying Check Point's email security. In one large company, before deploying Check Point, in an average week, there were 910 reported phishing emails. The IT team could not catch up; they could only remediate an average of 59 per week (or less than 7% of total reports). This organization estimated they would need 16 full-time employees to deal with the user-reported phishing problem. When moving to full HEC's prevent mode, this number was reduced to two user-reported phishing emails per week. We analyzed another organization prior to deploying Check Point and found that they spend 879 hours or 36 full days annually researching phishing reports. A third organization spent 2,500 hours a year reviewing suspicious email reports from end-user. That's the equivalent of 104 days.

That time drain leads to other priorities being overlooked and massive burnout among the IT and engineering staff. With users reporting both actual and imagined phishing emails, the SOC spends far too much time sifting through the smoke, unable to locate the fire.

What Defender Does Well

In addition to the sections outlined below, we've observed that Defender does an excellent job with malware – Check Point has found that, with unknown malware, Microsoft catches 90%. Further, Microsoft Defender includes URL rewriting, a key feature to prevent time-of-click attacks. In our analysis, we've observed that in the environments sampled; Defender limited the amount of phishing in these categories:

DMARC Spoofing

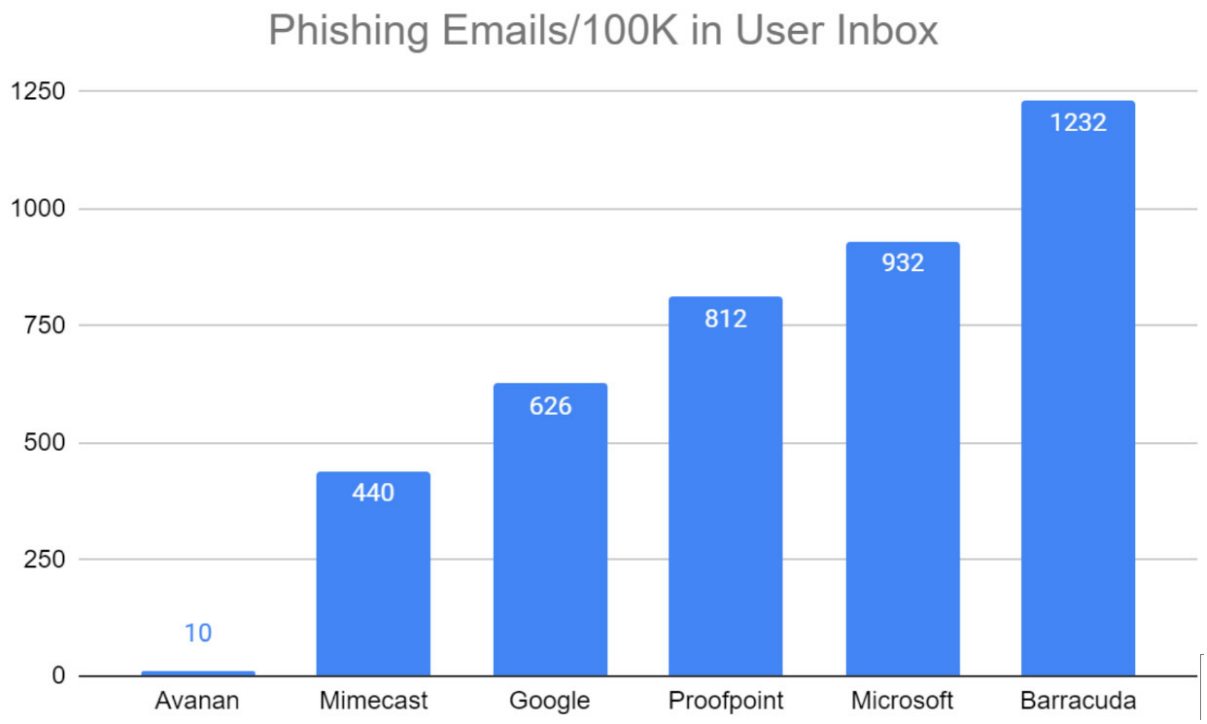
DMARC, or Domain-based Message Authentication, Reporting & Conformance, is an email standard used to authenticate an email. It's a way for operators to identify legitimate emails. The idea is to prevent hackers from spoofing an organization. However, in our analysis, we found that in 2.5% of cases, when Defender finds a case of a spoofed email and DMARC failed, it still sends it to the Junk Folder.

Business Email Compromise

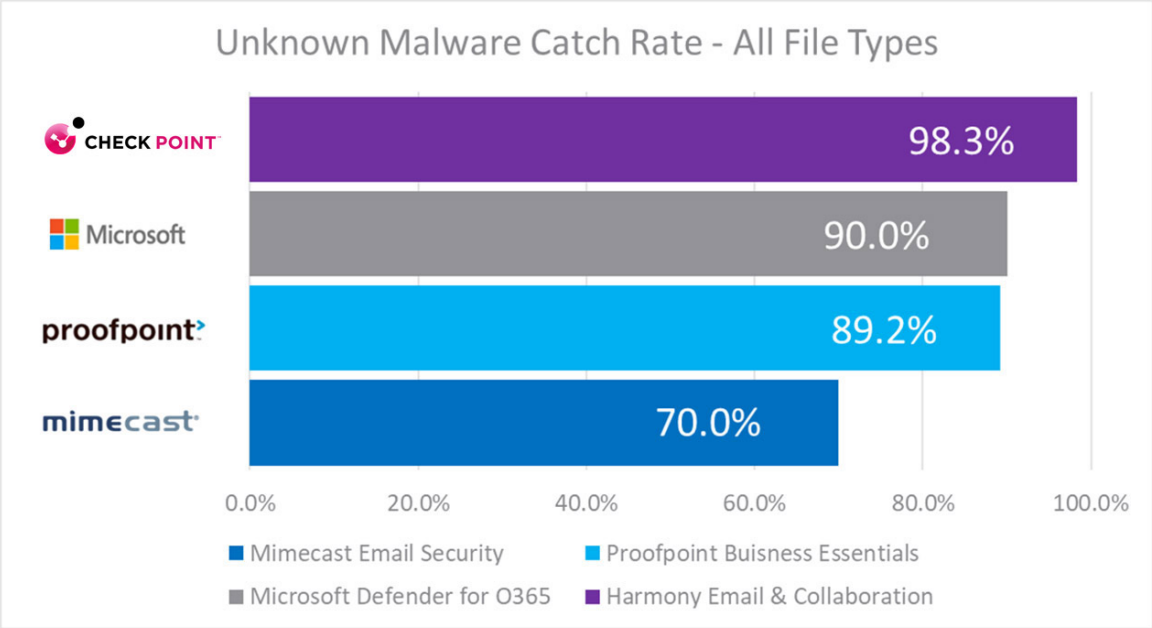
Business Email Compromise (BEC) is one of the fastest growing and most successful attack vectors. Though simple, it works because it uses social engineering and doesn't include any malware or malicious links. The idea is to spoof an executive asking an underling for an urgent favor. This can be the purchase of gift cards or other financial transactions. Since 2016, BEC-related losses have totaled over $43 billion.In our analysis, Microsoft did an excellent job limiting these attacks from reaching the inbox, allowing just 2.0% to pass.

Defender vs. Secure Email Gateways

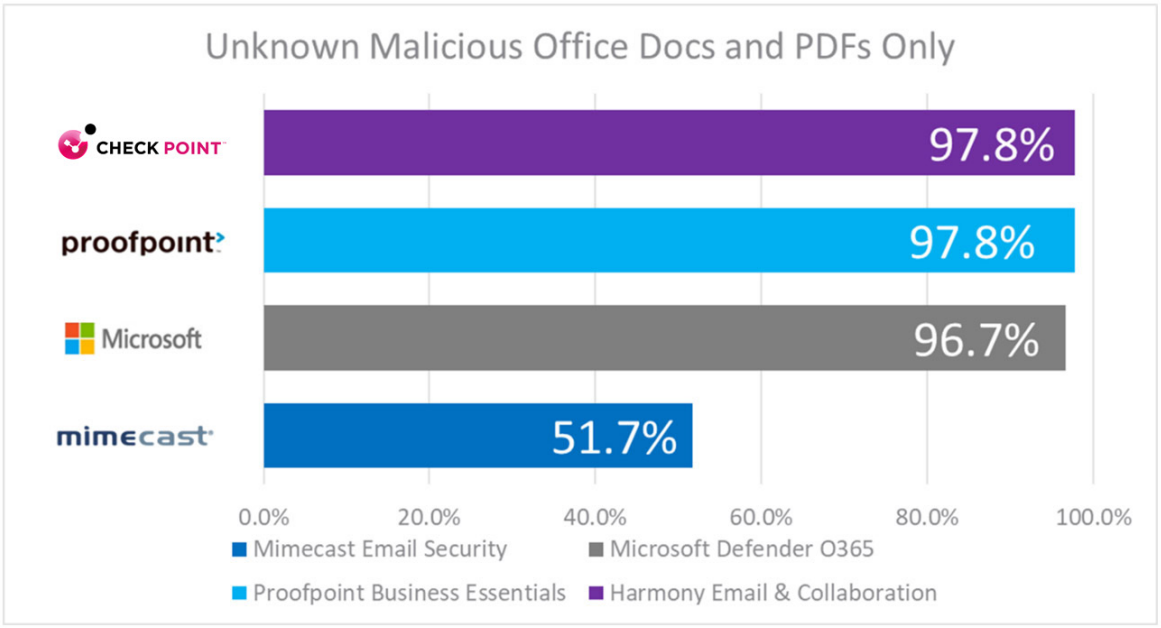
In one study analyzing 300 million emails, we found that Microsoft is in the middle of the pack compared to other Secure Email Gateways. Per every 100,000 emails, Microsoft's catch rate of phishing emails is better than some Secure Email Gateways and worse than others.



Where Microsoft does shine, as mentioned above, is malware. After analyzing 360 samples of both known and unknown malicious PDF, DOC, XLS, and other executable files, we were able to determine the catch rate for all malicious file types:



To break this down further, Microsoft's efficacy is even higher for just unknown malicious Office Docs and PDFs.



When considering email security options, it's essential to consider the entirety of a solution's offering.

Conclusion

Microsoft 365 is the most used and targeted email service worldwide. After thoroughly analyzing nearly three million emails, the Check Point's Research team found that Microsoft Defender misses 18.8% of phishing emails. This represents a 74% increase in missed attacks compared to the previous report from February 2020. This is not necessarily a decline in Microsoft's effectiveness, but rather an increase in hacker sophistication and specifically an increase in targeted attacks designed specifically to bypass Microsoft Defender. Hackers, in other words, have stepped up their game faster than Defender can respond.

Our security experts recommend a "defense-in-depth" strategy for all security, including email. Layering an additional level of protection on top of the default, whether Microsoft or Google, is recommended as a best practice for email security. It is essential as hackers continue to target and find ways to bypass the layers of protection included in the service by the service provider.

About Check Point Harmony Email & Collaboration

Check Point's Harmony Email and Collaboration Security (HEC) platform is the only security solution that can prevent malicious content from reaching a user's inbox. HEC operates "Inline," meaning that the platform scans all emails and attachments before they get a user's account. The platform scans for potentially malicious content using AI and Machine Learning algorithms, alerts SOC staff when an issue is found, and quarantines the harmful content.

Check Point's unique architecture allows it to learn from the specific emails that Microsoft misses. These are often highly targeted attacks explicitly designed to bypass Microsoft's protections. HEC's email security architecture sits behind Microsoft. When Microsoft blocks an attack, the attack is blocked, entirely stopped. When it doesn't, however, HEC sits between it and the inbox, giving a final analysis. Our AI has the unique ability to be trained on these specific, sophisticated, and evasive attacks.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com