E-BOOK

Cloud in the Crosshairs

How Cyber Criminals Exploit File-Sharing, Identity and Supply Chain Vulnerabilities in Microsoft 365

proofpoint.

Introduction

In the digital era, Microsoft 365 is an essential tool for getting work done. Unfortunately, its popularity has made it a prime target for cyber criminals. And while Microsoft 365 includes a host of native capabilities to stop cyber attacks, these tools are simply no match for today's sophisticated attacks.

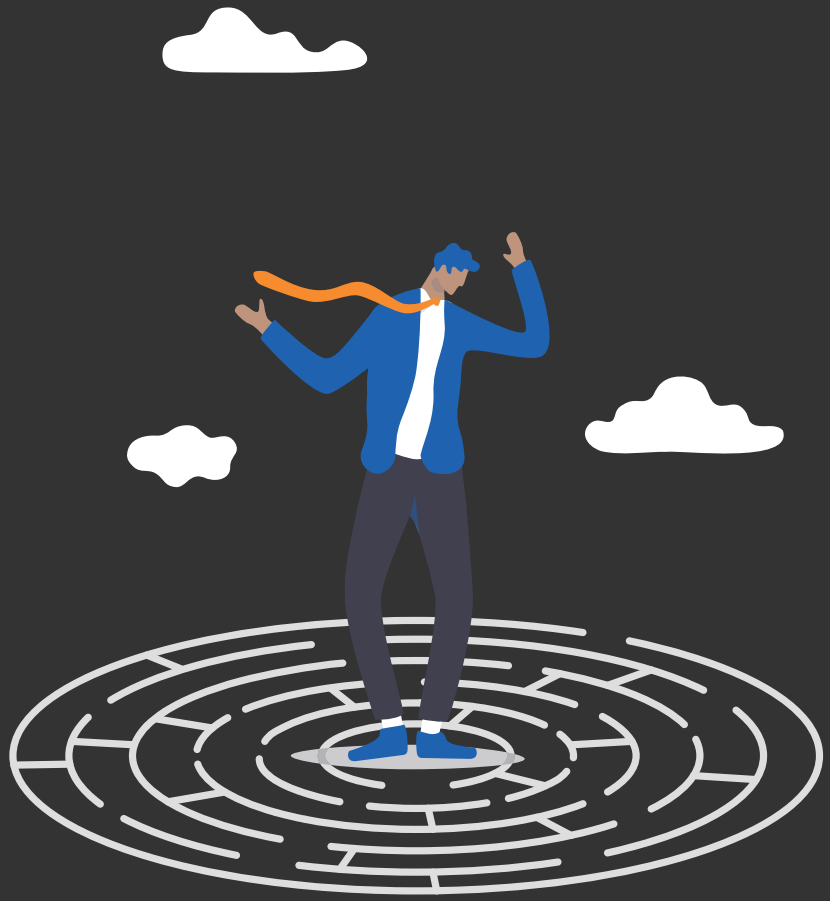
Every year, people-centric Microsoft 365 attacks cost organizations millions of dollars and cause frustration for security teams and users alike. It has gotten to the point that industry experts, like Gartner, agree that built-in tools for cloud should be augmented with third-party solutions.[1]

The reason built-in tools are no longer enough is simple: cyber criminals have become experts at targeting people. And this makes them increasingly difficult to stop.

Compromising users is usually the first step in a much larger series of events that happen when an organization is breached. Dubbed the "cyber attack chain," these events start with user compromise and progress to privilege abuse, data theft and more.

Steps in the cyber attack chain.

1 Gartner. Market Guide for Email Security. February 2023.



This e-book explores five types of people-centric attacks that give cyber criminals a foot in the door—and ultimately put organizations at risk for more serious breaches. They are very difficult to detect with Microsoft 365 capabilities alone.

1. Business Email Compromise (BEC)
2. Telephone-Oriented Attack Delivery (TOAD)
3. Weaponized File Sharing
4. Account Takeover
5. Compromised Supplier Accounts

Each section includes several examples that illustrate just how varied and inventive these attacks can be. They also show how almost anyone using Microsoft 365—without additional security—can become a victim of a skilled attacker.

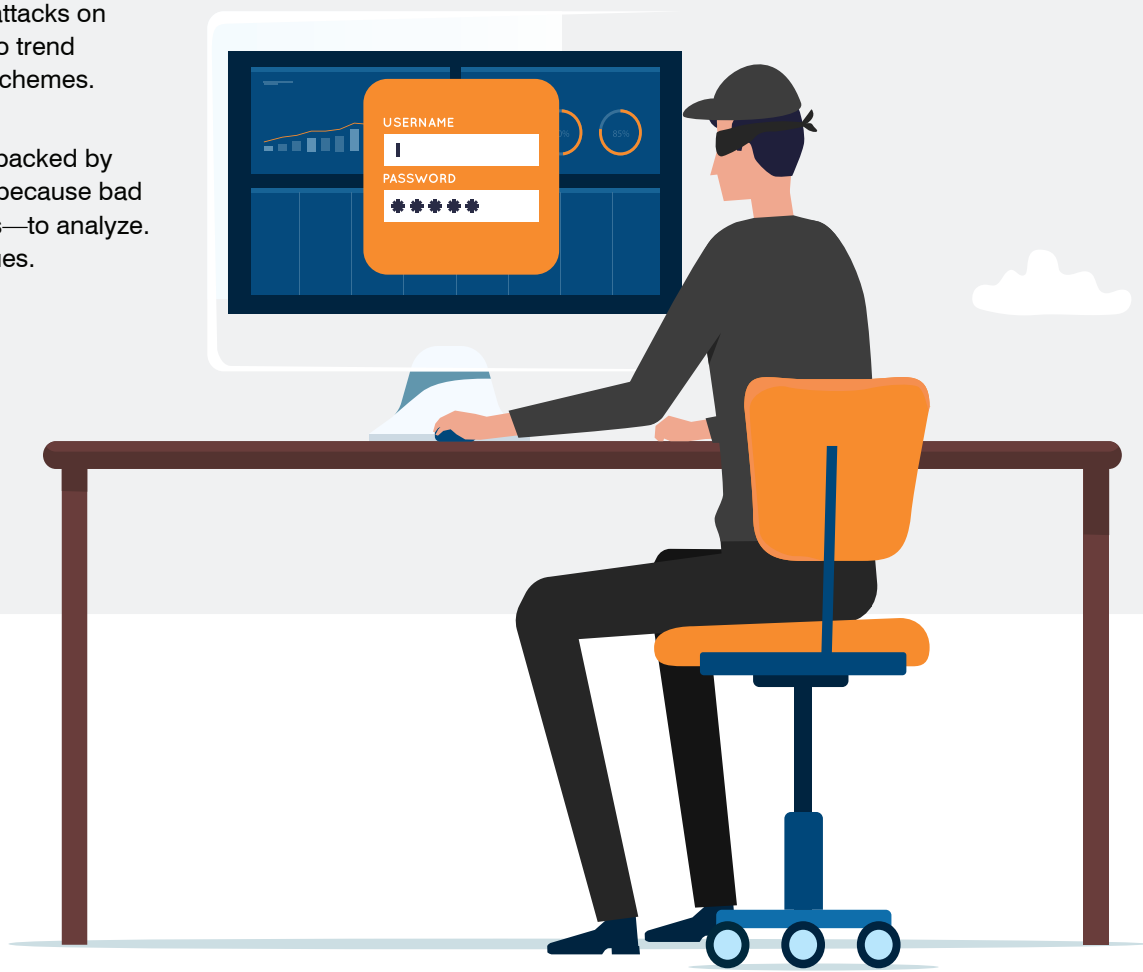
All of these examples are all real-world threats observed by Proofpoint in risk assessments we've done for organizations.

SECTION 1

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) ranks as one of the costliest types of attacks on businesses of all sizes and across industries. Each year losses continue to trend higher. In 2022, the FBI found that businesses lost $2.7 billion from BEC schemes. That's $300 million more than 2021.

Many of today's BEC schemes are highly sophisticated, well-funded and backed by careful planning and research. They're also very difficult to detect. That's because bad actors don't send the usual payloads—malicious URLs or file attachments—to analyze. Instead, they rely on impersonation and other social engineering techniques.



2 FBI. 2022 Internet Crime Report. 2023.

Environment:
Microsoft 365

Threat Category:
Social Engineering

Attack Type:
Payroll redirect

Target:
Benefits Administrator

Payroll Redirect Attack

Payroll redirects are email fraud attacks that typically target employees working in finance, tax, payroll and human resources. In these attacks, threat actors aim to gain employee trust in an effort to change payment details and steal employee paychecks. Because they rely on social engineering tactics, they can be extremely hard to detect. Payroll redirects are considered a medium risk to businesses and organizations.

An example of a payroll redirect attack.

In this attack, a fraudster emailed a benefits administrator from a Gmail account pretending to be an employee who was requesting a change to their direct deposit paycheck to a new bank account. In this instance, the fraudster and victim were even allowed to exchange multiple messages. In evaluations and proof of concepts (POCs) conducted by Proofpoint, native Microsoft email security controls were unable to stop these types of attacks.

Environment:
Microsoft 365

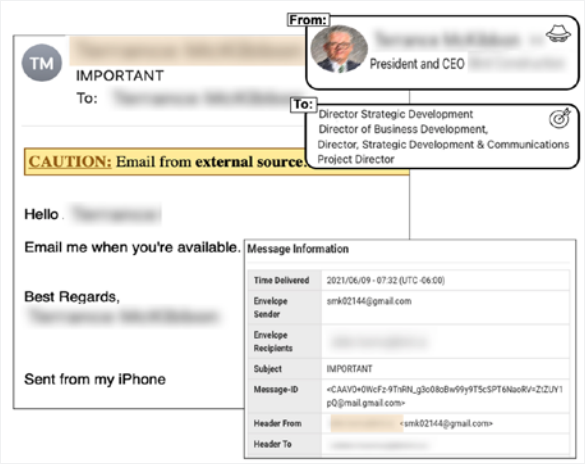
Threat Category:
Social Engineering

Attack Type:
Impersonation

Target:
Directors, Strategic and Business Development

Executive Impersonation Attack

When a bad actor successfully pretends to be an employee, the fraud can be costly for a business. But when they impersonate high-level executives, losses can be much more severe. In recent years, such attacks have risen drastically. Since March 2020, Proofpoint has seen email scammers impersonate more than 7,000 CEOs. More than half of Proofpoint customers have had at least one of their high-level executives' email accounts used in an attempted scam.



An example of an executive impersonation attack.

Here, an attacker emailed employees from a Gmail account, pretending to be a CEO who needed them to take follow-up action. If they had responded, the fraudster could have easily extracted data or financial rewards. In evaluations and POCs conducted by Proofpoint, native Microsoft email security controls were unable to stop these types of attacks.

Environment:
Microsoft 365

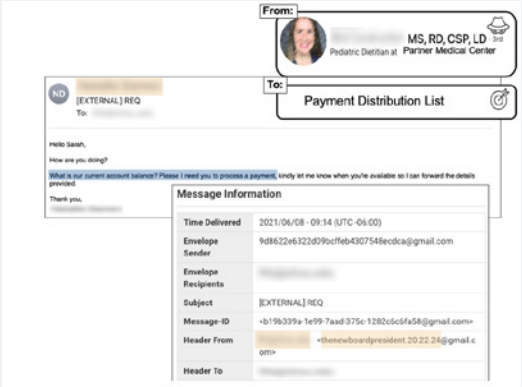
Threat Category:
Social Engineering

Attack Type:
Invoice Fraud

Target:
Finance Department

Supplier Invoicing Attack

Schemes that target consumers, like gift card fraud, characterize the vast number of BEC attacks. However, B2B-style BEC scams that target suppliers are highly targeted—so while they might be lower in volume, the financial losses from these attacks can be quite substantial. Proofpoint has stopped multiple supplier invoicing attempts where each incident could have cost millions of dollars. In these attacks, threat actors send fake invoices or new routing information so that payments are sent to a bank account controlled by them.



An example of supplier invoice fraud.

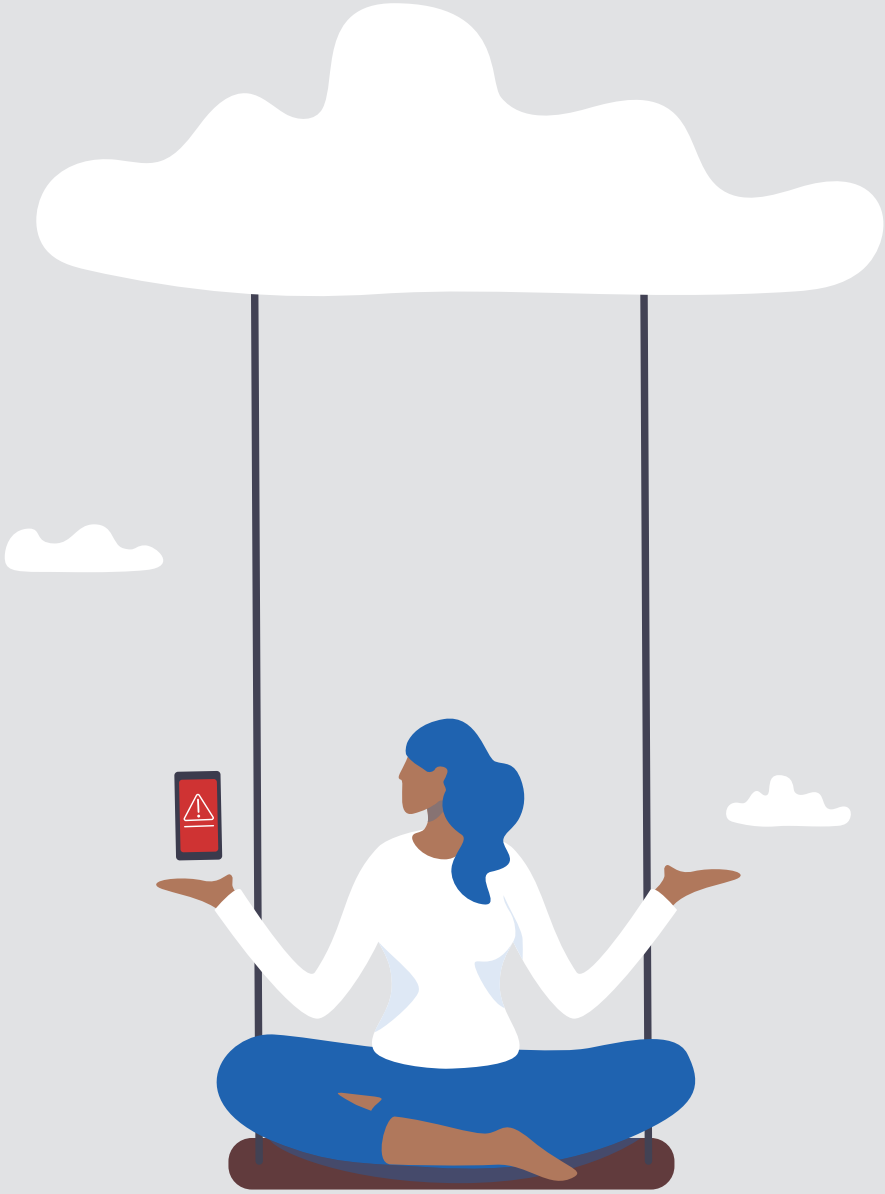
In this case, the attacker pretended to be a former employee now working at a partner organization that needed its payment processed. Sent to the finance department with a Gmail account, this message got past native Microsoft email security controls.

Often, bad actors use Gmail or other free email services when they're attempting this type of fraud. That's because it helps them to bypass email authentication checks like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Attackers may also send malicious URLs or attachments to help them gain access to financial information or other high-value data.

SECTION 2

TELEPHONE-ORIENTED ATTACK DELIVERY

In a telephone-oriented attack delivery (TOAD) attack, a target receives a message that typically contains a fake invoice or alert. The message also contains a customer service number to contact with questions or to correct an error. If the target calls the number, they find themselves on the line with a threat actor. At peak, Proofpoint saw over 13 million TOAD messages sent per month in 2022. This number has been steadily rising since the technique first appeared in 2021.[3]



Environment:
Microsoft 365

Threat Category:
Social Engineering

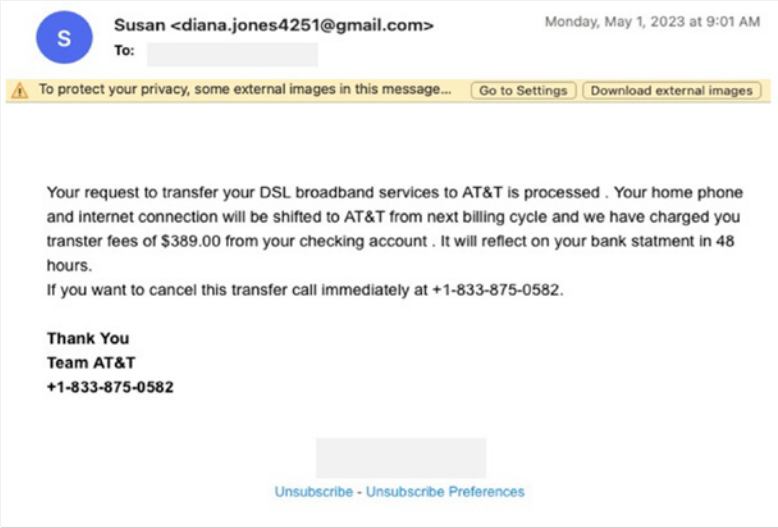
Attack Type:
TOAD

Target:
Microsoft 365 User

TOAD Threat

Email fraud supported by call center customer service agents is prolific and profitable. In many cases, victims lose tens of thousands of dollars stolen directly from their bank accounts. A reported 68.4 million Americans lost $39.5 billion to phone fraud attacks between 2021 and 2022.[4]

There are two types of call center threat activity regularly observed by Proofpoint. One uses free, legitimate remote assistance software to steal money. The second uses malware disguised as a document to compromise a computer and can lead to follow-on malware.



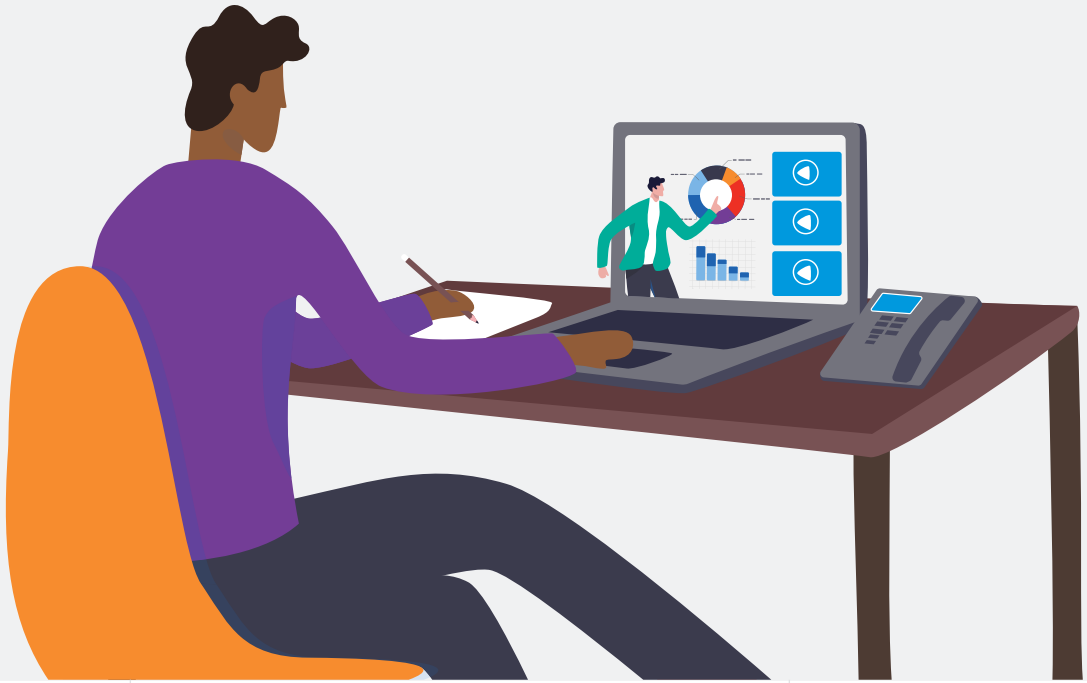
An example of a TOAD attack.

4 Truecaller. U.S. Spam & Scam Report. 2022.

In a typical call center attack, a user receives a message that needs to be dealt with urgently, like the email above. Often, the message includes some type of receipt for a large purchase and appears to be sent by a legitimate company. The recipient is instructed to call a number in the email to cancel the transaction or dispute their purchase.

If the user calls the phone number in the email, a customer service representative will verbally guide the user to visit a website or mobile app store. Proofpoint researchers have seen a range of next steps, including guiding victims to download malware, transfer money or enable remote access.

Microsoft misses these messages because they don't include payloads or malicious URLs.



SECTION 3

WEAPONIZED FILE SHARING

Weaponized file-sharing attacks are one of the most common types of URL-based attacks. Proofpoint internal threat data shows that URLs account for three-quarters of cyber threats overall. And file-sharing URLs used in more than 50% of these attacks.

Because users inherently trust and use services like Microsoft OneDrive and Microsoft SharePoint, bad actors frequently use these links. Microsoft is in a unique position when it comes to these attacks. Not only does it inadvertently host these malicious files, but it also allows them to pass through its email security solutions.

In 2021, we found that more than 45 million URL-based threats sent to our customers had malicious content hosted by Microsoft.

Environment:
Microsoft 365

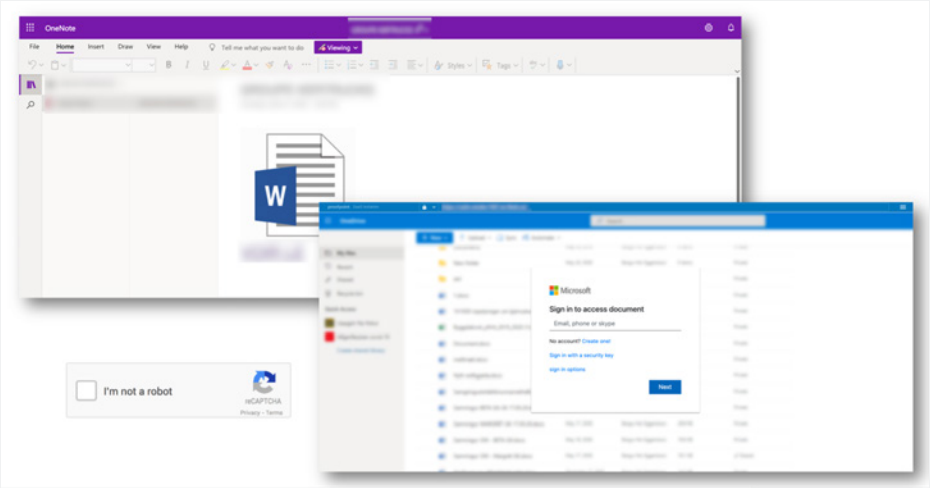
Threat Category:
URL-Based File-Sharing

Attack Type:
Credential Phishing

Target:
Shared Mailbox Users

OneNote Credential Phishing

Bad actors have increased their use of CAPTCHA by 50 times year over year, according to Proofpoint data.[5] In these attacks, bad actors try to steal user credentials by sending them links to fake documents. When users click on these links, they're presented with a CAPTCHA. After they check the CAPTCHA box, they're taken to a fake Microsoft page where they're asked to enter their credentials.



An example of a Microsoft OneNote page with a link to a fake Word document.

5 Proofpoint. Human Factor Report. 2022.

In this example, an attacker pretended to be a third-party vendor who was submitting a work request to a telecom company's shared mailbox. The attacker's goal was to get mailbox users to hand over their credentials by sending them a link to a fake Word document that presented them with a CAPTCHA. Sent through OneDrive, the link to the malicious page bypassed native Microsoft security controls.

Remarkably, even after it was condemned by Proofpoint, the OneDrive page was still live a month later. This is only one of the millions of abused file-sharing pages that impersonate the Microsoft brand every month.

Environment:
Microsoft 365

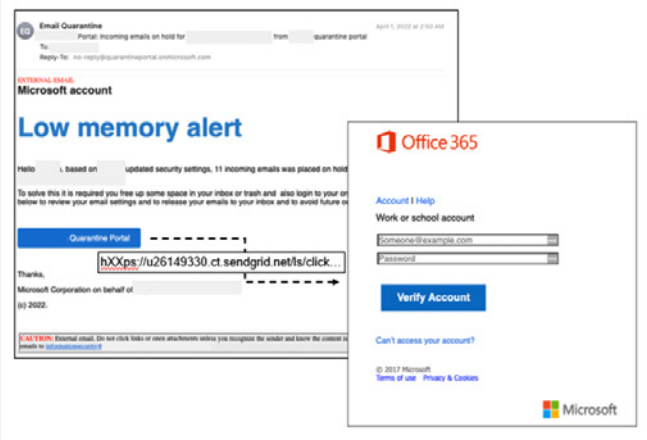
Threat Category:
Legitimate Cloud Service Abuse

Attack Type:
Credential Phishing

Target:
Microsoft 365 user

Legitimate Cloud Services Abuse Credential Phishing

Microsoft 365 credential theft is a common tactic used by threat actors to compromise users' accounts. Once inside their victim's account, attackers are able to learn details that enable them to send very convincing messages. As a result, they are able to steal valuable data and siphon funds.



An example of credential theft imitating the Microsoft brand, hosted on a legitimate cloud service site.

In this example, the attacker used SendGrid as a host and sent their message from a spoofed Microsoft domain (onmicrosoft.com) to make it appear legitimate. At the bottom of the message, they even made it seem as though Microsoft Corporation was a signee on behalf of the organization.

What's notable is here is that when threat actors use legitimate cloud services, their attacks often go undetected by Microsoft. The reason they get through comes down to how Microsoft handles links. Microsoft Safe Links does not have predictive sandboxing at the time users click. Instead, it relies on reputation, which means it is incapable of detecting never-before-seen threats that originate from legitimate cloud and file-sharing services.

SECTION 4

ACCOUNT TAKEOVER

Account takeover attacks are a common tactic for threat actors. In these attacks, a threat actor steals a user's account credentials so that they can assume their corporate identity. A single set of credentials is highly valuable to attackers because it can be used to access email, document storage and other single sign-on services. With so much access, the effects of a successful attack can be severe. Organizations lost an average of $6.2 million annually from cloud account compromises in 2021.[6] And these attacks are on the rise. In 2022, Verizon found that credential theft took place in 76% of social engineering attacks.[7]

6 Ponemon Institute. Ponemon Report: Cost of Cloud Compromise and Shadow IT. 2021.
7 Verizon. Data Breach Investigations Report. 2023.

Environment:
Microsoft 365

Threat Category:
URL-Based

Attack Type:
Credential Theft

Target:
Customer Service Department

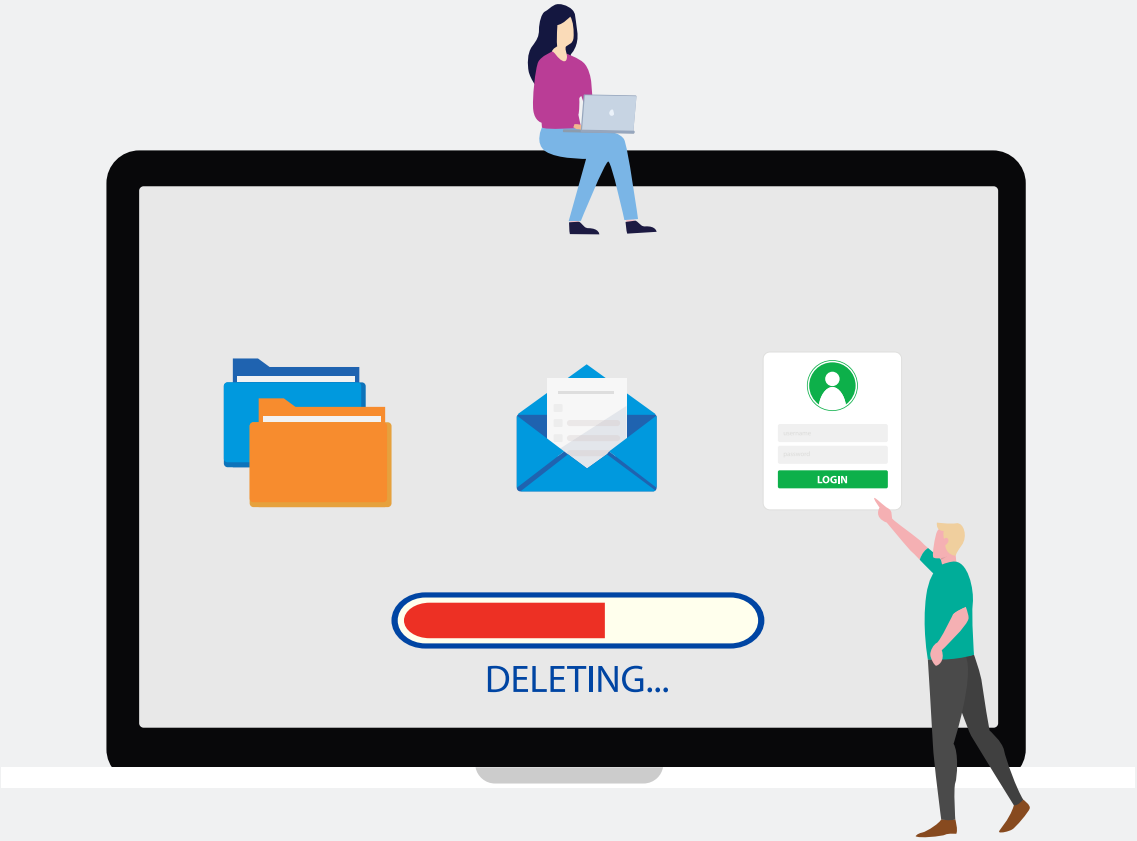
Microsoft 365 Credential Harvest Attack

Many credential attacks use the same tactic—they imitate Microsoft in order to get past Microsoft's own perimeter defenses. Abusing familiarity and trust in major brands is one of the simplest forms of social engineering. Microsoft is an overwhelming favorite when it comes to brand abuse. Proofpoint research shows that Microsoft occupied four of the top five positions for abused brands across all threats in 2022.[8]

An example of a credential harvest attack.

8 Proofpoint. Human Factor Report. 2023.

This attempt at credential theft got past native Microsoft email security controls. The attacker sent a message to a customer support center employee pretending to be a member of IT support staff. To appear genuine, the attacker's message included a recognizable display name and Microsoft branding. Proofpoint often sees bad actors use a legitimate URL (in this case, sendgrid.net) to bypass Microsoft URL scanning defenses.



Environment:
Microsoft 365

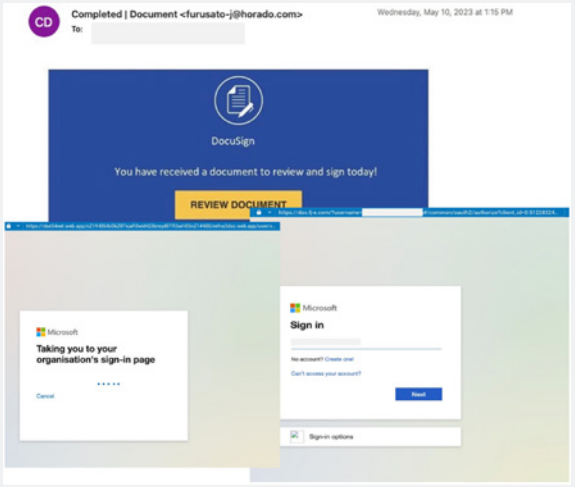
Threat Category:
MFA Collection

Attack Type:
Credential Phishing

Target:
Microsoft 365 User

MFA-Enabled Phishing

Multifactor authentication (MFA) can no longer be counted on to stop account takeover. Attackers are increasingly adept at getting around it. At peak, Proofpoint research found that MFA bypass accounted for more than a million messages per month in 2022.[9]



An example of MFA-enabled phishing with a URL that redirects to a lookalike Microsoft login page..

This attack bypassed native Microsoft security controls by looking like a DocuSign page with a link for the user's signature. Instead of taking the user to DocuSign, the URL redirects to a lookalike Microsoft login page.

To carry out this attack, the threat actor used EvilProxy, which is a phishing framework that uses a reverse proxy to customize landing pages for each recipient and collect credentials and bypass MFA protection. The kit is relatively new and is available for sale on exploit forums. Once MFA is collected, it provides persistent access to an account even with a password reset.

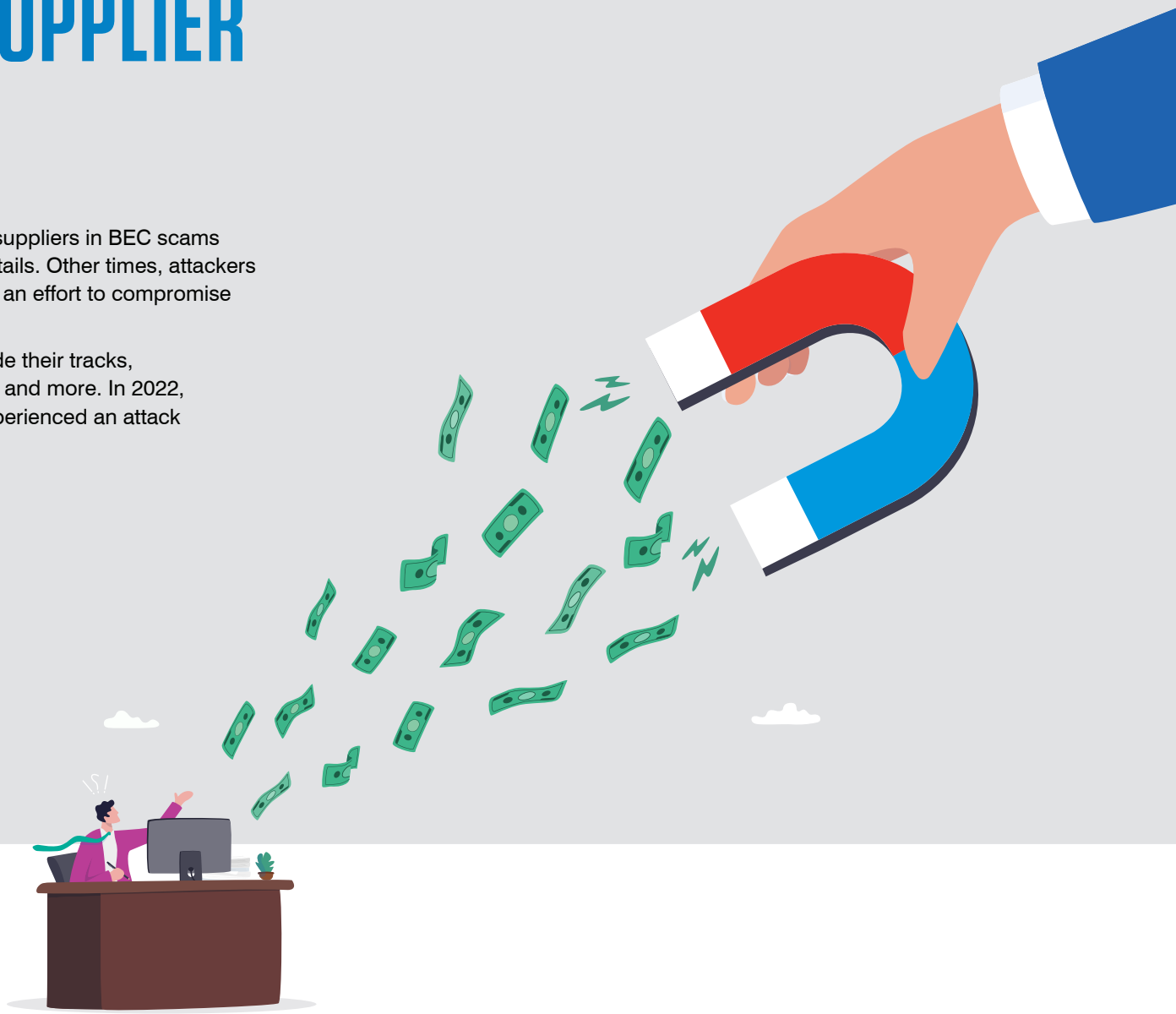
9 Proofpoint. Human Factor Report. 2023.

SECTION 5

COMPROMISED SUPPLIER ACCOUNTS

As already discussed, threat actors often impersonate suppliers in BEC scams to submit fake invoices or change account payment details. Other times, attackers compromise suppliers and other trusted third parties in an effort to compromise your employee's accounts or steal money and data.

Once inside your network, they create email rules to hide their tracks, access intellectual property, change payment accounts and more. In 2022, a staggering 69% of organizations across the globe experienced an attack that started in their supply chain.[10]



10 Proofpoint. State of the Phish Report. 2023.

Environment:
Microsoft 365

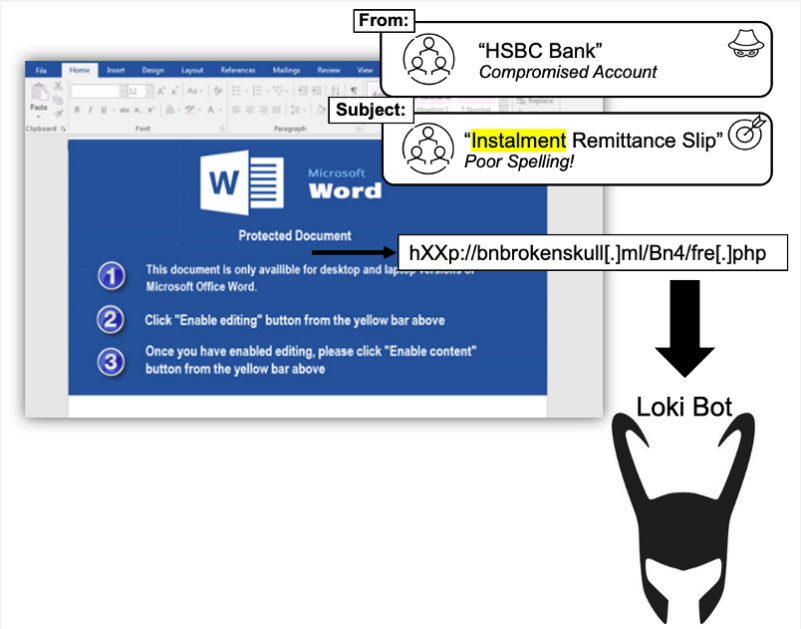
Threat Category:
URL-Based

Attack Type:
Downloader

Target:
Hidden via BCC in Email

Malicious Attachment Threat

One way to get inside a network is to use malware. Recently, Proofpoint did an internal analysis of data on nearly 4,600 businesses. We found that 85% of these businesses experienced supplier-based email attacks over a seven-day period that ended January 31, 2023. Malware was involved in about 13% of these attacks.[11]

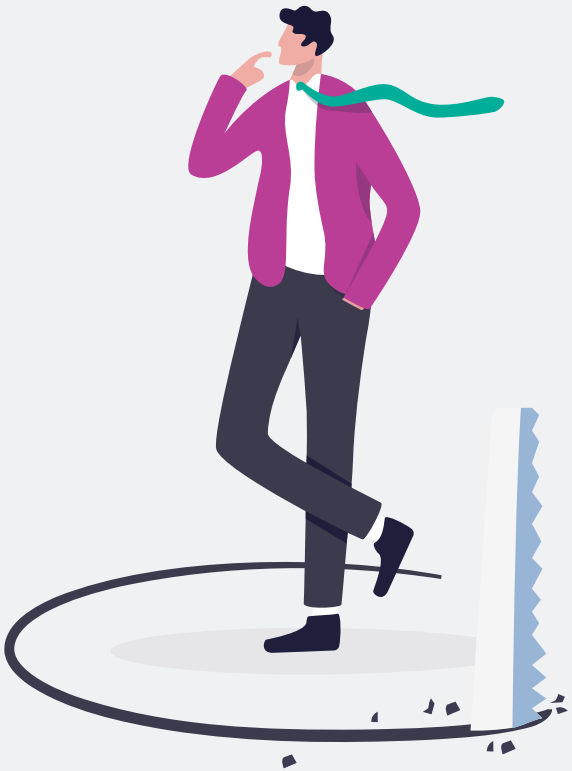


An example of a Loki Bot attack.

11 Proofpoint. "Hidden Risk: How to Recognize and Prevent Supply Chain Attacks." April 2023.

This attack was sent from a compromised email account at a global bank. Inside the message was a link to a Word document that exploited various Equation Editor vulnerabilities to download Loki Bot—a bot that can steal passwords from browsers, FTP/SSH applications and email accounts.

Microsoft missed this attack because the message was sent from a legitimate domain, so static reputation analysis didn't identify it as malicious. The message also passed SPF authentication. And the malicious payload used sandbox evasion and file obfuscation techniques.



Environment:
Microsoft 365

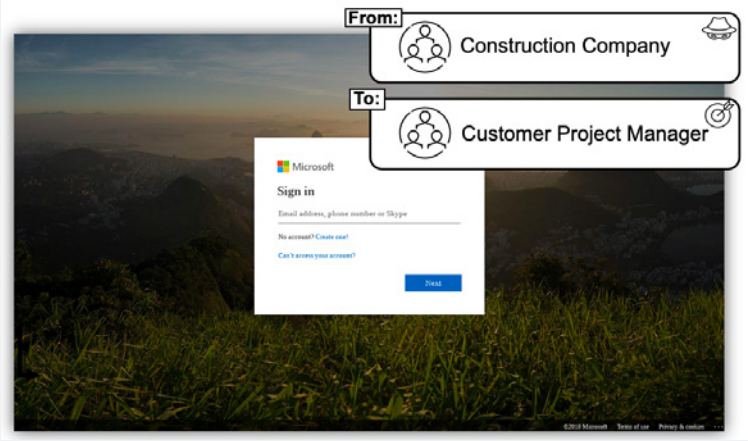
Threat Category:
URL-Based

Attack Type:
Credential Phishing

Target:
Customer Project Manager

Credential Phishing Threat

Threat actors also abuse compromised supplier accounts to steal user credentials. And in these cases, the outcome can be even more damaging. Unfortunately, users often freely engage with these threats because—even on close inspection—these messages appear to be legitimate as they're sent from a legitimate domain.



This credential page mimics a Microsoft 365 login.

The attack above was sent from a compromised account that belongs to a legitimate construction company. This account regularly emails a project manager who is one of its customers. The malicious email contained a URL that linked to a page that mimicked the Microsoft brand in order to harvest Microsoft 365 credentials.

This threat was delivered to the project manager's inbox for several reasons. For starters, Microsoft's reputation scan often does not detect new malicious URLs—even when they impersonate the Microsoft brand. Also, this message was sent from a legitimate supplier's domain, so Microsoft's static reputation analysis would not flag the sender as malicious. The envelope did not trigger obvious spoof use cases.

Environment:
Microsoft 365

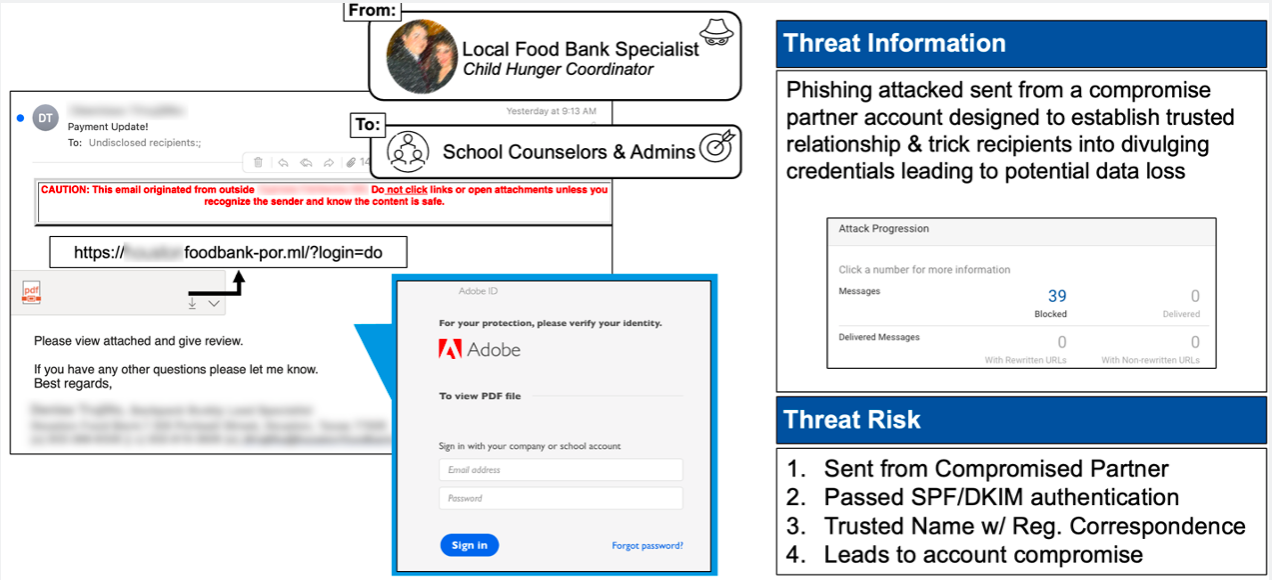
Threat Category:
Attachment-Based, Containing URL-Based Threat

Attack Type:
Credential Phishing

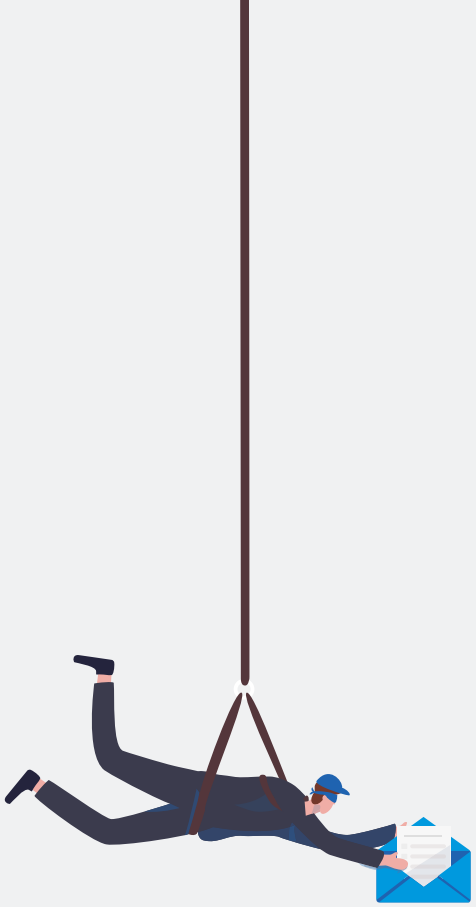
Target:
School Counselors and Administrators

Embedded URL Attack

Not all threat actors target Microsoft 365. With the growth in cloud apps, it's often easier to abuse cloud accounts that have less protection than Microsoft 365. To improve the likelihood that their victim will activate an attack, a threat actor will send a message from a partner's compromised account.



This credential page mimics an Adobe software login.



This credential harvest attack was sent from the compromised account of a legitimate partner that the user regularly emails. As shown above, a link inside the message sends the user to a page that mimics the Adobe brand in an attempt to harvest the user's software credentials.

Microsoft did not stop the attack for several reasons. Firstly, it was sent by a legitimate partner's account, so it passed SPF/DKIM authentication. And because there was regular correspondence with this account, it was considered a trusted name, so it passed Microsoft's static reputation scoring.

Also, the threat actor was able to evade sandboxing by putting the malicious payload (URL) within the attachment and not the email itself. The URL was not detected by Microsoft's reputation scan, which can miss new malicious URLs.

Environment:
Microsoft 365

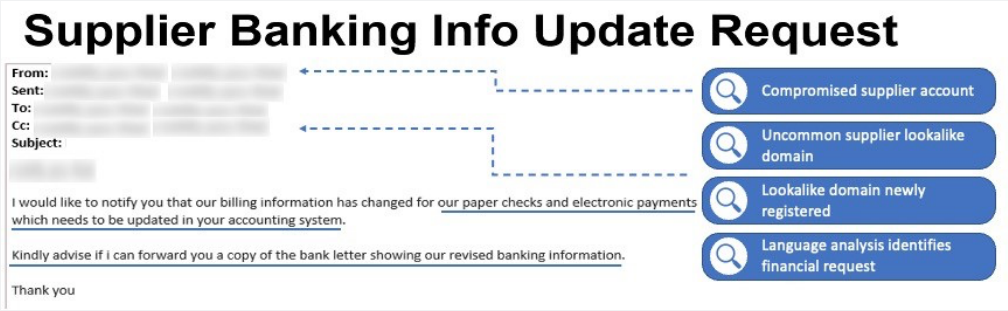
Threat Category:
Social Engineering, Compromised Supplier Account

Attack Type:
Invoice Fraud

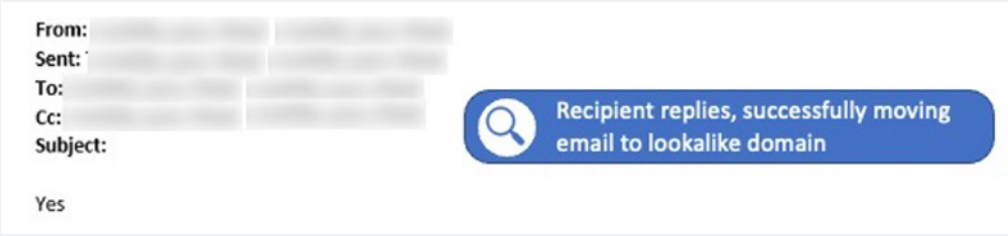
Target:
Account Executive Staff

Supplier Impersonation Threat

People are more likely to respond to a malicious email when it looks like it comes from someone they know. When one of these attacks is sent by a seemingly legitimate supplier, it becomes even more dangerous.



This was the attacker's initial email.



This was the customer's response, which was sent to a lookalike domain.

The initial message was received by a global retailer from a legitimate supplier's account. The sender requested an update to their payment information. But what seemed like a routine request was malicious, as the sender's account had been compromised. The attacker was trying to redirect response emails to a newly registered lookalike domain with an aim to intercept sensitive information and divert funds.

Microsoft did not stop this threat was because it was sent by a legitimate client, so it passed SPF/DKIM authentication. And because there was regular correspondence with this account, it was considered a trusted name, so it passed Microsoft's static reputation scoring.

CONCLUSION

When it comes to keeping your organization secure, Microsoft 365's built-in security features are a good starting point. But as threats multiply and evolve, you need other layers of security.

Cyber attackers no longer depend on siloed techniques. Instead, they mix and match advanced tactics to exploit people. They also look for relationships that can be leveraged, trust that can be abused and access that can be exploited. That's why stopping them requires a multilayered, people-centric approach that spans the entire attack chain.

To learn more about how Proofpoint can enhance your Microsoft 365 native security and protect your people from advanced cyber attacks, visit proofpoint.com.

Why Proofpoint

Every day, we analyze more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

We are trusted by more than:

- **75%** OF THE FORTUNE 100
- **60%** OF THE FORTUNE 1000
- **30%** OF THE FORTUNE GLOBAL 2000

- **8,000** ENTERPRISES
- **200,000** SMALL BUSINESSES

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0503-003-01-04 08/23