PERCEPTION POINT™

2024 STATE OF PHISHING REPORT

Evasive Maneuvers

Table of Contents

Introduction

As the modern workspace undergoes a shift with the widespread adoption of email, collaboration apps, and web-based tools, employees' communication and productivity has been greatly enhanced. However, the increased usage of these new communication and SaaS apps has increased the organization's attack surface, exposing them to potential security breaches. According to recent studies, although email still remains the prime vector for cyber threats, the browser, which is the new main work app, is a fast growing attack vector.

The gravity of the situation becomes apparent when examining cybersecurity data from the past year, revealing that a staggering 91% of cyber attacks originate from email-based vectors. These attacks encompass a range of threats, including phishing attempts, malware delivery, and business email compromise (BEC) campaigns. The latter involves malicious actors impersonating coworkers or vendors, often seeking unauthorized fund transfers or changes to bank account information.

Phishing attacks are not new. They have been a persistent threat for over three decades. Originating with early attempts by attackers to impersonate AOL employees for credit card information, the landscape has evolved considerably. Traditionally, orchestrating a phishing campaign involved either creating a customized phishing template and disseminating it to the target audience or resorting to the Darknet to procure a phishing kit.

> Email is one of the most common ingress points into organizations for threat actors. As organizations have implemented email security solutions and trained employees to recognize email attacks, threat actors have pivoted to more advanced methods that bypass protections. They have also embraced artificial intelligence (AI) to make attacks more scalable and personalized while also less detectable.

Osterman Research, The Role of AI in Email Security 2023

The GenAI Factor

Generative artificial intelligence (GenAI) is changing the game for threat actors. Creating a phishing template with GenAI has been streamlined to a remarkable extent. Utilizing GenAI tools, threat actors can generate a sophisticated phishing template within a mere 20 to 30 seconds, seamlessly embedding malicious URLs or files. Moreover, GenAI can produce content that is almost indistinguishable from human-written texts, mimicking the sentiment and writing style of organizations and specific people. This evolution underscores the pressing need for organizations to fortify their defenses against the growing sophistication of email-based cyber threats in the contemporary era.

This report draws from research conducted by Perception Point's Incident Response team, focusing on three main themes:

1. Phishing Trends & Evasion Techniques
2. Post Account Takeover Tactics
3. A New Anti-Phishing Approach

The research included in this report offers valuable insights into current trends actively shaping the cybersecurity landscape, providing a tangible understanding of the ongoing evolution of cyber threats.

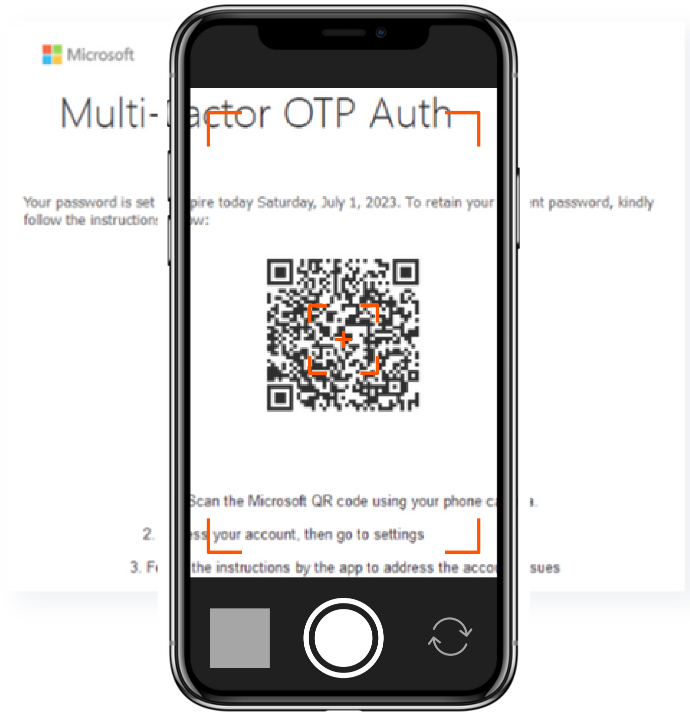
Phishing Trends & Evasive Techniques

In this section, we will review some of the advanced evasive maneuvers being used by threat actors. By examining text obfuscation and deceptive phishing techniques like "quishing" and 2-step phishing, we will shed light on the multifaceted arsenal at the disposal of attackers. This section will also present advanced browser-based threats, geofencing, manipulation of HTML files, phone scams, account takeover (ATO) attacks, and other methods employed by attackers to exploit security systems' vulnerabilities.

Quishing

When it comes to QR Code phishing, also known as "quishing," we have witnessed a staggering increase in occurrences throughout 2023. From just August 2023 to September 2023 alone, Perception Point detected a steep 427% increase in the use of malicious QR codes. This notable surge in numbers underscores the effectiveness of this technique for hackers.

The modus operandi involves redirecting individuals to a malicious page, such as a counterfeit Microsoft login page as seen below, or the like, upon scanning a QR code, thereby shifting the threat landscape to mobile devices.



Microsoft

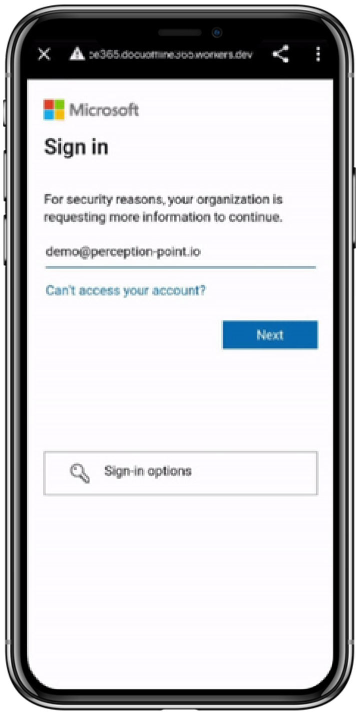
Multi-Factor OTP Auth

Your password is set …pire today Saturday, July 1, 2023. To retain your …nt password, kindly follow the instruction… …w:

Scan the Microsoft QR code using your phone c… …

2. …ss your account, then go to settings

3. F… the instructions by the app to address the acco… …sues



Microsoft

Sign in

For security reasons, your organization is requesting more information to continue.

demo@perception-point.io

Can't access your account?

Traditional email security systems like secure email gateways (SEGs) and even the most modern email security solutions scan for suspicious links in the email body of the message to prevent phishing attacks, but may overlook embedded URLs within images or file attachments. ***Most security solutions are unable to extract and dynamically scan links from QR codes which can be embedded within the email or in an attached file.***

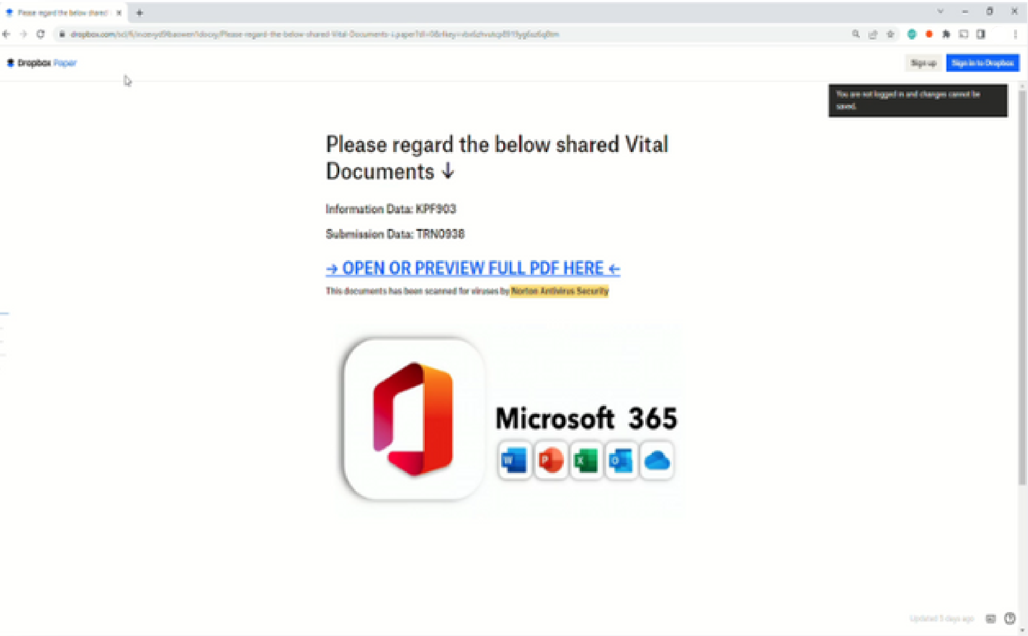
The escalating prevalence of this tactic prompts a critical question: Why are end users falling victim to QR code phishing? The ubiquity of this method suggests a lack of user awareness and familiarity with such deceptive practices. Therefore, when conducting phishing simulations, it is imperative to incorporate examples that mirror these real-world threats, as end users may not be well-versed in recognizing and avoiding quishing attempts.

2-Step Phishing

The 2-step phishing technique has gained considerable traction among attackers. This term refers to how an additional step in the attack chain helps avoid detection. For example, a user will receive an email notifying them that their password has expired, which prompts them to click a link to reset the new password. This link redirects them to a usually legitimate hosting service, often utilized for website building, web hosting, or file sharing.

The nefarious twist lies in hackers embedding a hidden link within this authentic-looking website.

What distinguishes two-step phishing attacks is their wide-ranging scope, exploiting over 400 commonly used services. These include services like Salesforce, SharePoint, Adobe, and even public Jira tickets.



You are not logged in and changes cannot be saved.

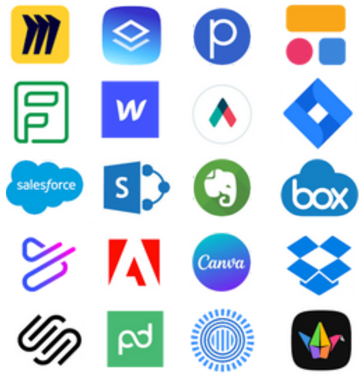
Please regard the below shared Vital Documents ↓

Information Data: KPF903

Submission Data: TRN0938

→ OPEN OR PREVIEW FULL PDF HERE ←

This documents has been scanned for viruses by Norton Anthivirus Security



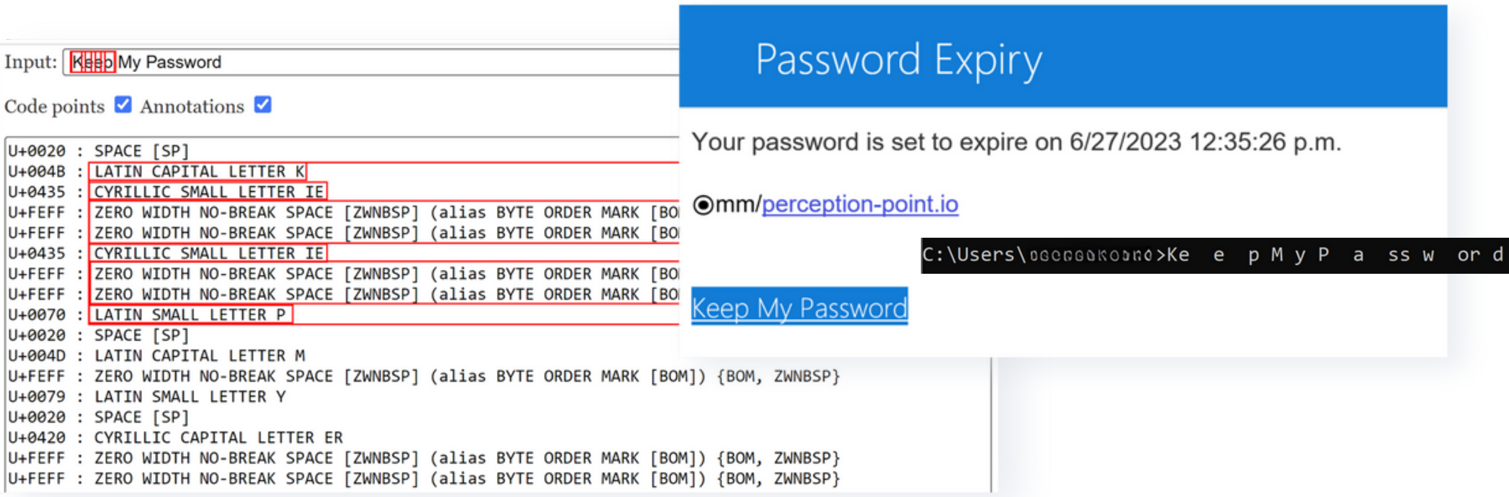
Hackers exploit the familiarity users have with these platforms, making it more likely for them to follow seemingly innocent links, assuming they are part of legitimate workflows. For instance, a developer might receive a link within a bug report, assuming it leads to relevant information, only to find themselves on a malicious login page.

Most of these attacks originate from legitimate vendors who had one or more of their accounts taken over by threat actors, or if the attacker is a legitimate user/owner of an account . Due to high sender reputation, allow-listing, and other policies, many email security solutions fail to detect these attacks. In addition, since most attackers use legitimate services as the first payload – most email security vendors fail to follow and detect the second malicious payload. Security solutions must simulate the user experience by recognizing the second link and "clicking" on it, in order to scan the second site and uncover its malicious intent.

Text Obfuscation

Text obfuscation attacks involve familiar phishing templates adopting a deceptive guise. These templates usually present as benign notifications like urging the user to update an expired password, seemingly appearing as ordinary text to the human eye. However, upon closer inspection, when copied and pasted into the command line, subtle irregularities emerge as suspicious spaces that are interspersed between the letters. A breakdown of the unicode reveals the sophisticated manipulation techniques employed by hackers used to evade traditional detection mechanisms.

Take, for instance, the letter 'K,' which, upon closer look, is revealed to be a combination of a Latin letter followed by an Cyrillic E-letter and succeeded by two non-break spaces—elements that HTML does not render visibly. ***This nuanced approach extends across various characters, transforming innocuous four-letter words into eight-letter counterparts, effectively evading static text filtering measures.*** This technique poses a challenge for outdated email security solutions, which fail to detect such attacks. For attackers well-versed in exploiting the limitations of legacy security measures, these tactics offer a convenient workaround.



Input: Keep My Password

Code points ☑ Annotations ☑

```
U+0020 : SPACE [SP]
U+004B : LATIN CAPITAL LETTER K
U+0435 : CYRILLIC SMALL LETTER IE
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BO
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BO
U+0435 : CYRILLIC SMALL LETTER IE
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BO
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BO
U+0070 : LATIN SMALL LETTER P
U+0020 : SPACE [SP]
U+004D : LATIN CAPITAL LETTER M
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BOM]) {BOM, ZWNBSP}
U+0079 : LATIN SMALL LETTER Y
U+0020 : SPACE [SP]
U+0420 : CYRILLIC CAPITAL LETTER ER
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BOM]) {BOM, ZWNBSP}
U+FEFF : ZERO WIDTH NO-BREAK SPACE [ZWNBSP] (alias BYTE ORDER MARK [BOM]) {BOM, ZWNBSP}
```

Password Expiry

Your password is set to expire on 6/27/2023 12:35:26 p.m.

◉mm/perception-point.io

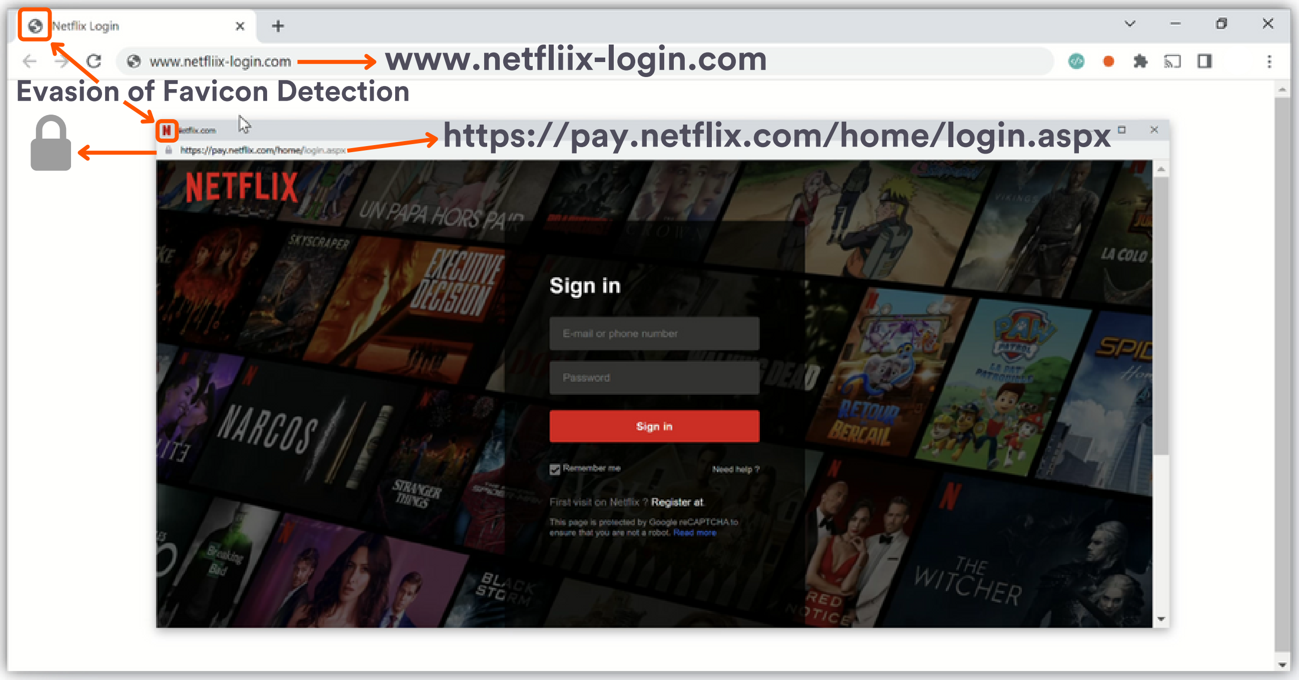
```
C:\Users\[illegible]>Ke  e  p M y P  a  ss w  or d
```

Browser in the Browser

In the past year, we have observed a novel attack involving a browser-based exploit that garnered considerable attention on LinkedIn and Twitter. In this attack, attackers leverage HTML and CSS code to craft an illusion within the browser, creating the appearance of a separate window opening within the user's own browser. The original domain is masked, but the injected URL mirrors a legitimate site, such as netflix.com, despite the fraudulent nature of the actual domain.

An attacker might impersonate a Netflix login page on the visible window, while the embedded URL seems legitimate because it displays "pay.netflix.com." What sets this approach apart is its ability to simulate an interactive browser within the browser. Users can move and resize the window, which enhances the deception. Exploiting the fact that many end users lack proper cybersecurity training, the attackers capitalize on users' reliance on visual cues like "HTTP" or "HTTPS" to assess website security. Despite appearances, the fraudulent site seems secure, leading unsuspecting users to unwittingly disclose sensitive credentials and credit card information.

This technique also evades favicon detection employed by security filters. Traditional security measures scrutinize the favicon of a website, flagging inconsistencies between the favicon and the domain as potential impersonation attempts. However, in this case, the absence of a favicon complicates detection. To combat such attacks effectively, it is imperative to have a security solution with strong visual detection capabilities.



Sign in

E-mail or phone number

Password

Sign in

☑ Remember me

Need help ?

First visit on Netflix ? Register at.

This page is protected by Google reCAPTCHA to ensure that you are not a robot. Read more

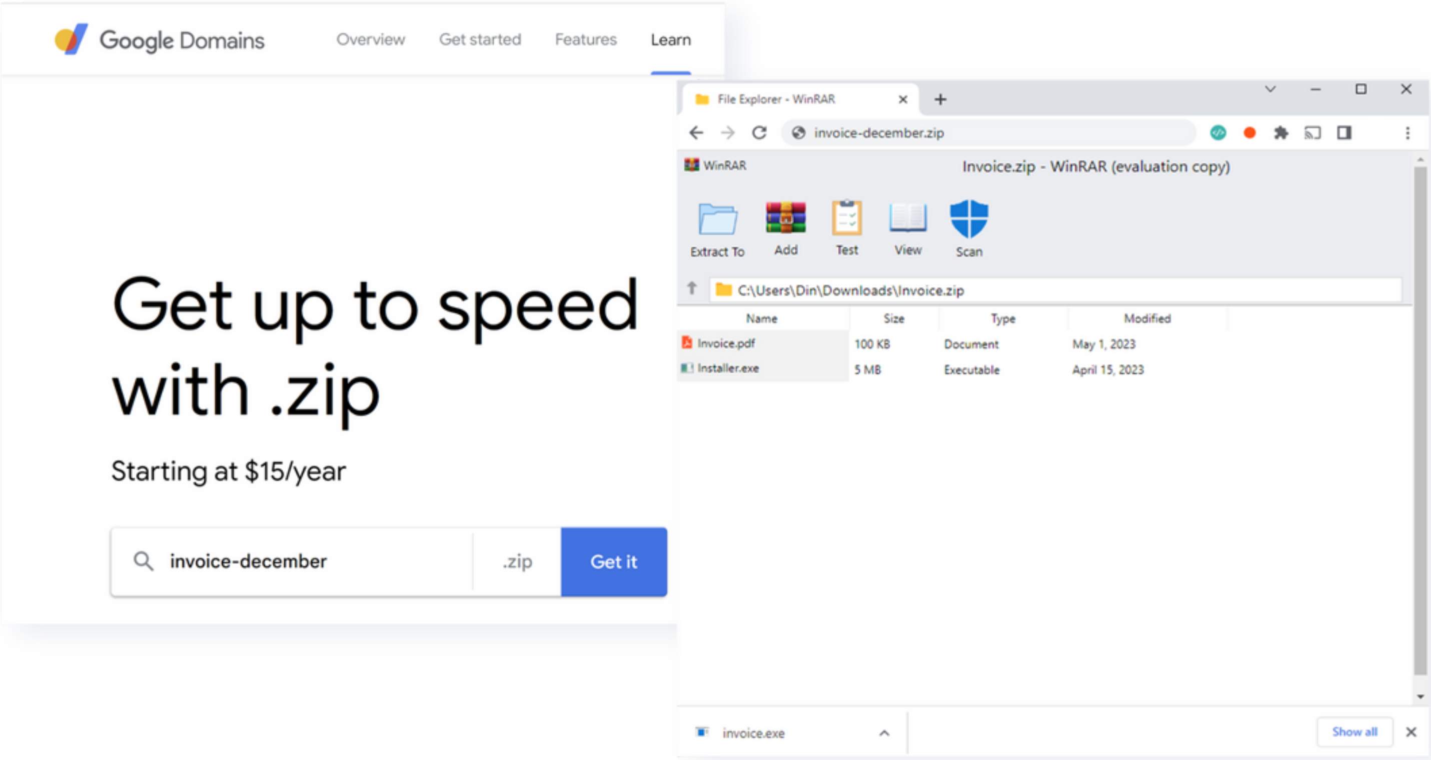
Netflix Login
www.netfliix-login.com
www.netfliix-login.com
Evasion of Favicon Detection
https://pay.netflix.com/home/login.aspx
NETFLIX

Archive in the Browser

Google's introduction of eight new Top-Level Domains (TLDs) this year, including ZIP, has brought about a distinctive cyber threat. Exploiting HTML and CSS techniques, attackers are manipulating browsers to create a façade that deceives end users into believing they are opening a file with WinZip directly within their browser. The cunning of this approach lies in its exploitation of the .zip domain which is an authentic domain, enabling attackers to bypass web crawlers effectively.

The attack entices users to click on a seemingly innocent link, such as "invoice pdf." However, instead of downloading a legitimate PDF file, users download an invoice EXE file and an information stealer malware onto their computers. With a single click, all the gathered information is transmitted to the hackers.

The challenge for security solutions to detect this type of attack lies in their resource limitations; many cannot scan every URL and button during web browsing.



Get up to speed with .zip

Starting at $15/year

invoice-december .zip Get it

Invoice.zip - WinRAR (evaluation copy)

C:\Users\Din\Downloads\Invoice.zip

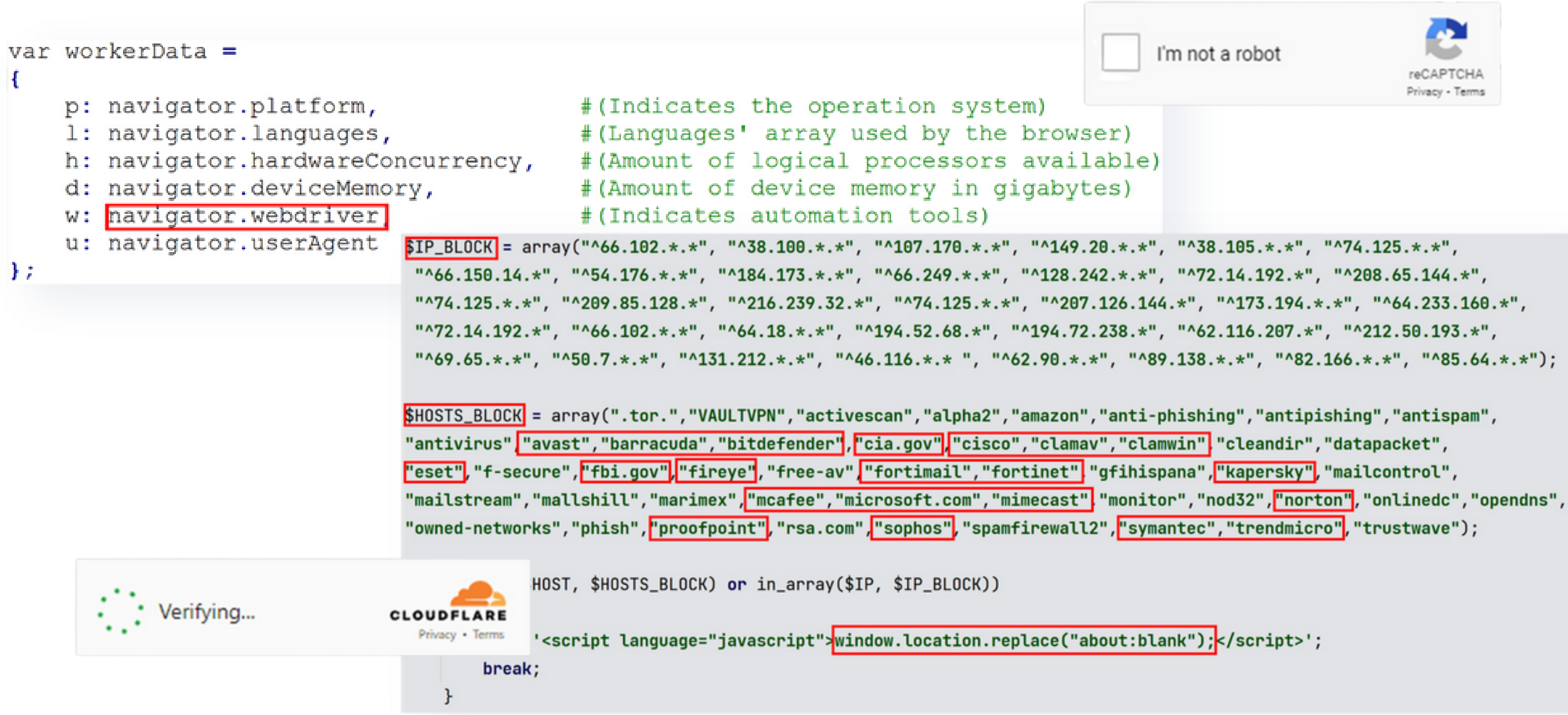
Name	Size	Type	Modified
Invoice.pdf	100 KB	Document	May 1, 2023
Installer.exe	5 MB	Executable	April 15, 2023

The archive in browser tactic strategically omits traditional indicators such as a download button or a "click here" prompt, which evades many security filters that typically inspect these elements. Consequently, security systems may provide a clean verdict because there are no buttons, no file downloads, and no incriminating actions identified. This not only grants the attacker a clean slate but also tricks the end user, who genuinely believes they opened a file within their browser's window. Moreover, the domain responsible for the attack gains an unintended boost in reputation by successfully bypassing the security system.

Captchas, Geofencing & Redirects

In a code-based tactic, hackers leverage CAPTCHAs, geofencing, and redirection to deceive security filters, creating an illusion of legitimacy while redirecting users to a different destination. In response to security measures like user agent block lists, IP block lists, VPN detection, and user interaction heuristics, hackers employ strategies to identify a system's browsing behavior and subsequently evade these hurdles.

The following example involves code utilizing the navigator web driver flag in Chrome. By detecting if the flag returns "true," hackers can determine if the system is using automation tools, remote debugging ports, or headless browsing. Headless browsing is particularly noteworthy as it expedites the retrieval of HTML and CSS code, making it more challenging for security solutions to promptly discern malicious intent.



```
var workerData =
{
    p: navigator.platform,              #(Indicates the operation system)
    l: navigator.languages,             #(Languages' array used by the browser)
    h: navigator.hardwareConcurrency,   #(Amount of logical processors available)
    d: navigator.deviceMemory,          #(Amount of device memory in gigabytes)
    w: navigator.webdriver              #(Indicates automation tools)
    u: navigator.userAgent
};
```

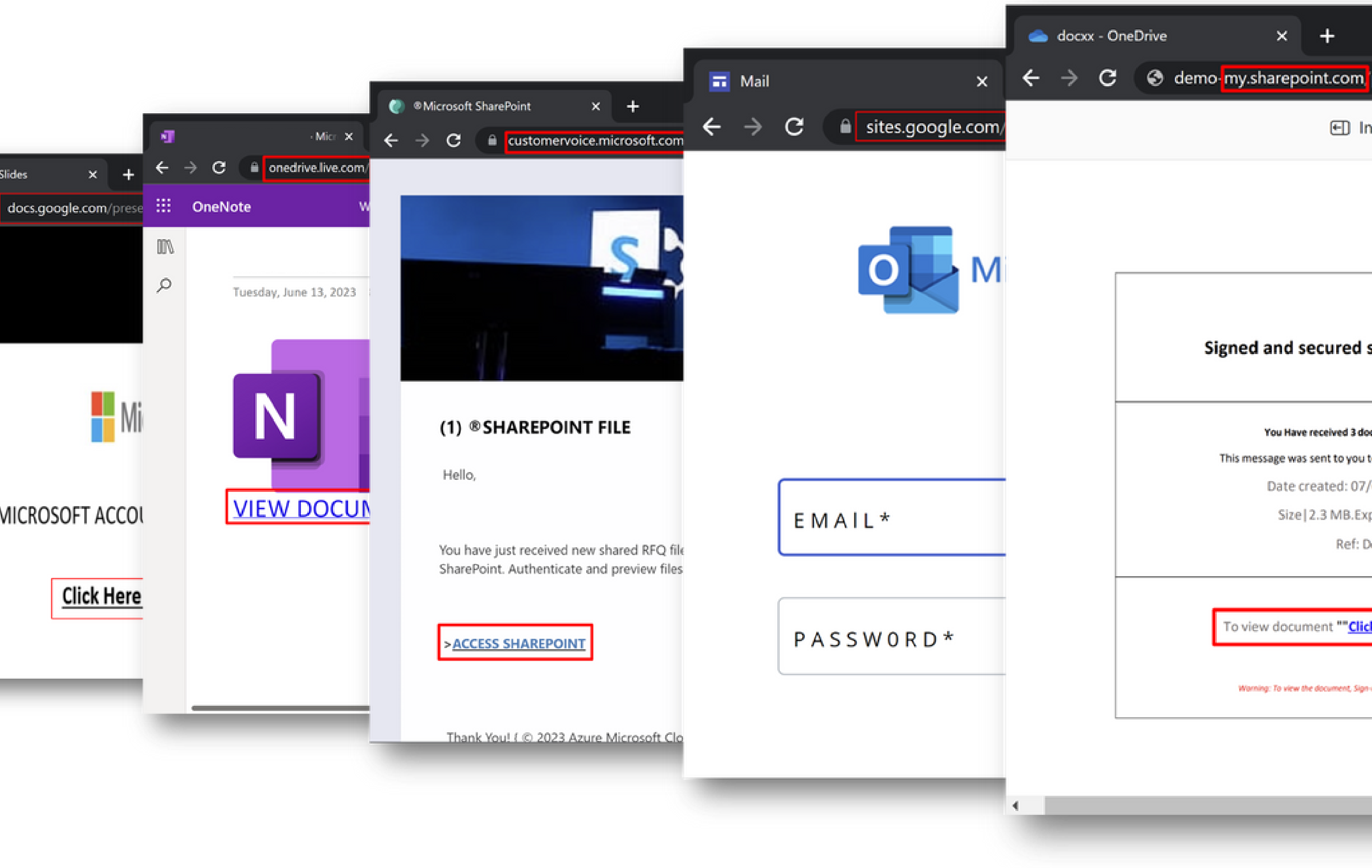
```
$IP_BLOCK = array("^66.102.*.*", "^38.100.*.*", "^107.170.*.*", "^149.20.*.*", "^38.105.*.*", "^74.125.*.*",
 "^66.150.14.*", "^54.176.*.*", "^184.173.*.*", "^66.249.*.*", "^128.242.*.*", "^72.14.192.*", "^208.65.144.*",
 "^74.125.*.*", "^209.85.128.*", "^216.239.32.*", "^74.125.*.*", "^207.126.144.*", "^173.194.*.*", "^64.233.160.*",
 "^72.14.192.*", "^66.102.*.*", "^64.18.*.*", "^194.52.68.*", "^194.72.238.*", "^62.116.207.*", "^212.50.193.*",
 "^69.65.*.*", "^50.7.*.*", "^131.212.*.*", "^46.116.*.* ", "^62.90.*.*", "^89.138.*.*", "^82.166.*.*", "^85.64.*.*");

$HOSTS_BLOCK = array(".tor.","VAULTVPN","activescan","alpha2","amazon","anti-phishing","antipishing","antispam",
"antivirus","avast","barracuda","bitdefender","cia.gov","cisco","clamav","clamwin","cleandir","datapacket",
"eset","f-secure","fbi.gov","fireye","free-av","fortimail","fortinet","gfihispana","kapersky","mailcontrol",
"mailstream","mallshill","marimex","mcafee","microsoft.com","mimecast","monitor","nod32","norton","onlinedc","opendns",
"owned-networks","phish","proofpoint","rsa.com","sophos","spamfirewall2","symantec","trendmicro","trustwave");

            HOST, $HOSTS_BLOCK) or in_array($IP, $IP_BLOCK))

            '<script language="javascript">window.location.replace("about:blank");</script>';
        break;
    }
```

Hackers employ IP block lists and host block lists with targeted ranges and subnets, effectively blocking major security companies such as Barracuda, FireEye, Proofpoint, Mimecast, and others. Interestingly, these block lists extend to include host domains like cia.gov and fbi.gov, which prevent security researchers from reaching the final payload and dismantling C2 servers. ***The ultimate objective of these block lists is to redirect users to a blank page, allowing hackers to exploit the tendency of security filters to mark a blank or white page as clean, thereby securing a clean reputation.***

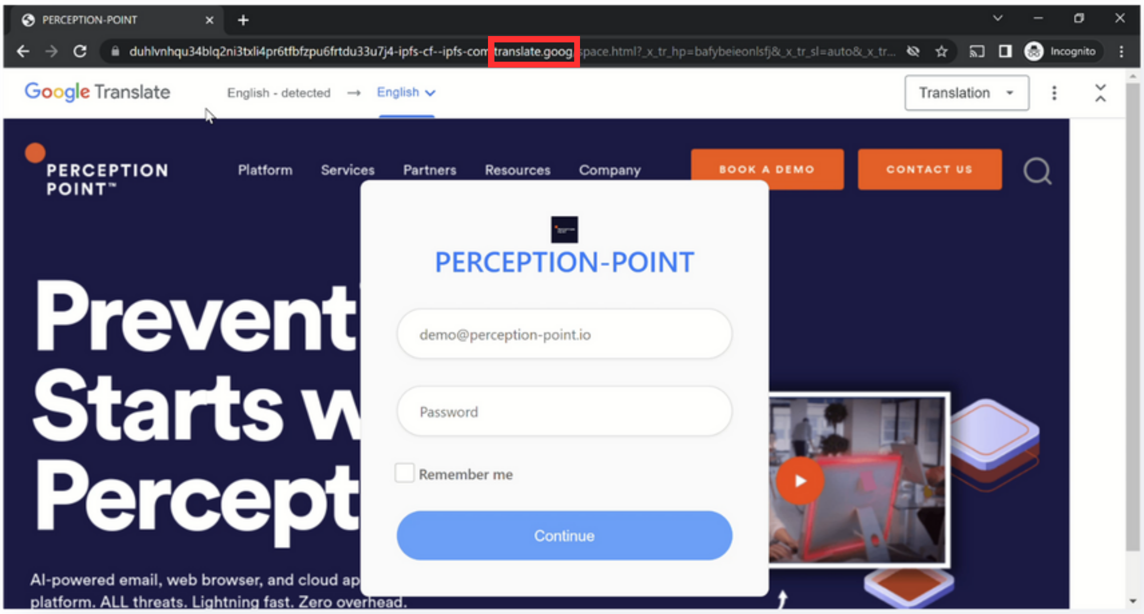
Attackers use this approach as a bypass, leveraging their ability to discern whether the system is automated or a genuine user, and ultimately enabling them to navigate around security measures effectively.

Microsoft & Google Services Abuse

In a phenomenon we refer to as the “allow-listing vulnerability,” attackers abuse Microsoft and Google services. Security analysts and engineers often add these services to allow lists, inadvertently creating a vulnerability that hackers exploit. Attacks include abuse of services like onedrive.com, customervoice.microsoft.com, and SharePoint within the Microsoft ecosystem. Similarly, Google services such as Google Docs, Google Sites, and, notably, Google Translate domains are exploited.



Perhaps most striking this past year was the misuse of Google Translate domains. Hackers leverage the reputation associated with Google Translate to host login pages, camouflaging their malicious intent. To demonstrate this, we created a fake login page impersonating Perception Point which is hosted on a Google Translate domain. The URL includes a parameter representing the recipient's address, allowing the website to dynamically adjust its appearance to mimic the targeted organization's website.



PERCEPTION-POINT

duhlvnhqu34blq2ni3txli4pr6tfbfzpu6frtdu33u7j4-ipfs-cf--ipfs-com.translate.goog/space.html?_x_tr_hp=bafybeieonlsfj&_x_tr_sl=auto&_x_tr...

PERCEPTION-POINT

demo@perception-point.io

Password

□ Remember me

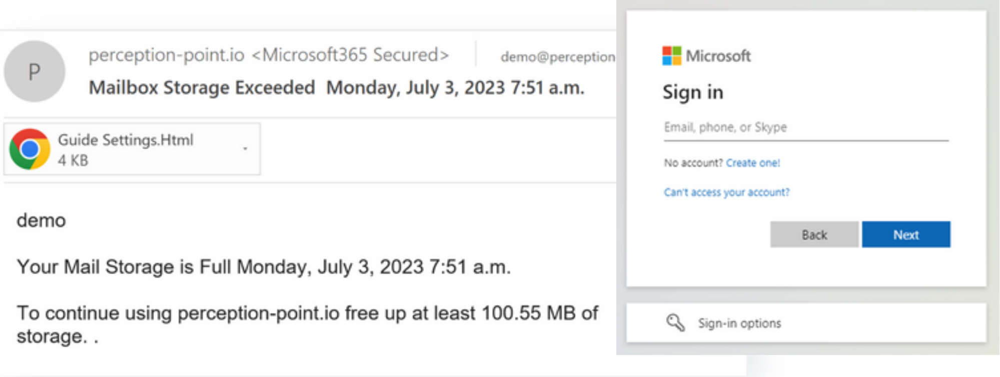
Continue

A unique aspect of this tactic is its versatility. By changing the language setting, hackers can easily target different audiences. For instance, switching the domain to microsoft.com enables the rapid creation of a new phishing campaign tailored to employees of Microsoft in a specific region, such as India.

Detecting these types of advanced phishing attempts requires vigilance. Security analysts should be on the lookout for login pages hosted on Google Translate domains, especially those that involve parameters indicating the recipient's address. These signs can serve as essential indicators for security professionals investigating phishing URLs.

Encoded HTML Files

The prevalence of encoded HTML files has surged, showcasing a concerning cyber threat trend. What sets this tactic apart is hackers' astute understanding that malicious URLs can quickly gain a bad reputation if detected. In contrast, files don't carry the same reputational baggage, allowing attackers to repeatedly send and distribute them without the same risk of incrimination.



perception-point.io <Microsoft365 Secured> demo@perception

Mailbox Storage Exceeded Monday, July 3, 2023 7:51 a.m.

Guide Settings.Html
4 KB

demo

Your Mail Storage is Full Monday, July 3, 2023 7:51 a.m.

To continue using perception-point.io free up at least 100.55 MB of storage. .

Microsoft

Sign in

Email, phone, or Skype

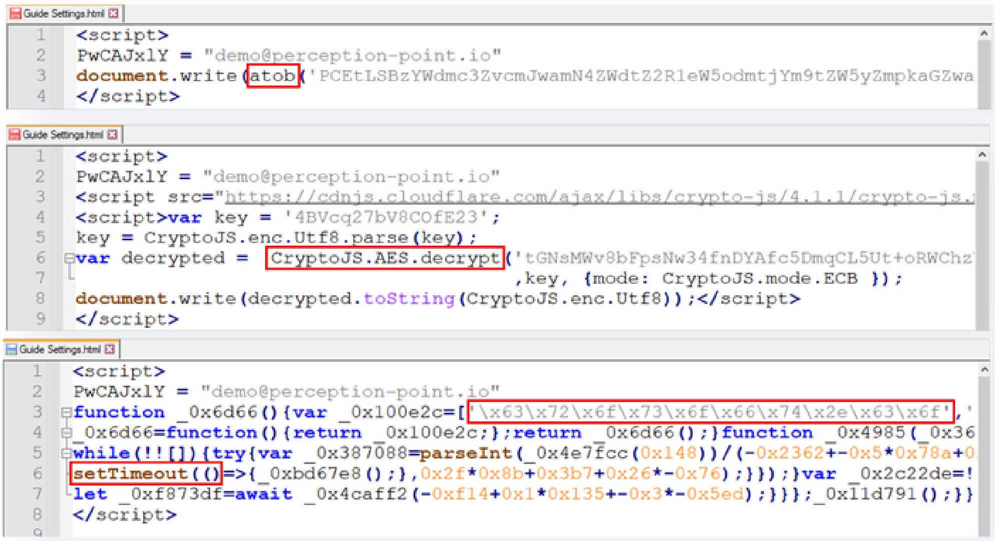
No account? Create one!

Can't access your account?

Back Next

Sign-in options

Examining the code reveals the complexity and sophistication employed by hackers to bypass security measures. In one example, Perception Point researchers observed a three-step process, in which the initial code utilized the document(.)write(atob) in the Base64 code. Upon decoding, the attackers introduced AES encryption, adding an extra layer of complexity. Subsequent decryption led to the identification of the final malicious payload.



```
<script>
PwCAJxlY = "demo@perception-point.io"
document.write(atob('PCEtLSBzYWdmc3ZvcmJwamN4ZWdtZ2R1eW5odmtjYm9tZW5yZmpkaGZwa
</script>
```

```
<script>
PwCAJxlY = "demo@perception-point.io"
<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.
<script>var key = '4BVcq27bV8COfE23';
key = CryptoJS.enc.Utf8.parse(key);
var decrypted = CryptoJS.AES.decrypt('tGNsMWv8bFpsNw34fnDYAfc5DmqCL5Ut+oRWChz
                                      ,key, {mode: CryptoJS.mode.ECB });
document.write(decrypted.toString(CryptoJS.enc.Utf8));</script>
</script>
```

```
<script>
PwCAJxlY = "demo@perception-point.io"
function _0x6d66(){var _0x100e2c=['\x63\x72\x6f\x73\x6f\x66\x74\x2e\x63\x6f','
_0x6d66=function(){return _0x100e2c;};return _0x6d66();}function _0x4985(_0x36
while(!![]){try{var _0x387088=parseInt(_0x4e7fcc(0x148))/(-0x2362+-0x5*0x78a+0
setTimeout(()=>{_0xbd67e8();},0x2f*0x8b+0x3b7+0x26*-0x76);}});}var _0x2c22de=!
let _0xf873df=await _0x4caff2(-0xf14+0x1*0x135+-0x3*-0x5ed);}}};_0x11d791();}}
</script>
```

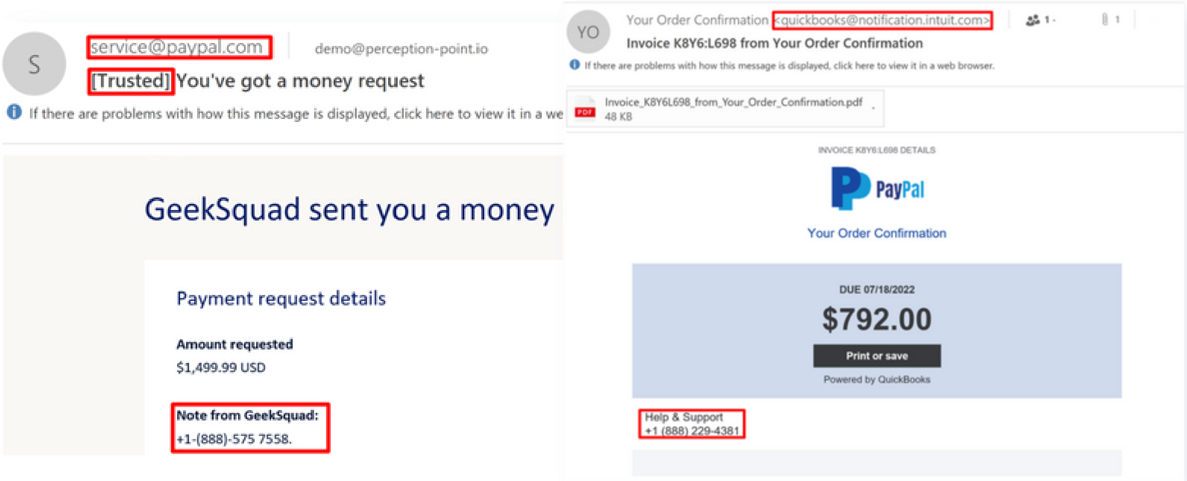
An additional layer of evasion involves the strategic use of the set timeout function. Recognizing the time constraints of security solutions during file analysis (typically within 5 to 7 seconds), hackers employ a set timeout for 10 seconds or more, effectively evading traditional dynamic scanning measures.

The key takeaway from this trend is the importance of caution when encountering encoded HTML files, encrypted HTML files, or any form of obfuscation within JavaScript code. Security analysts should remain attuned to these nuanced techniques, as attackers continue to evolve and adapt to exploit vulnerabilities in both static and dynamic scanning processes.

Phone Scams

Phone scams have evolved beyond generic credit card phishing schemes, with hackers now employing fake renewal alerts to lure unsuspecting victims. These scams often impersonate well-known services such as McAfee, Norton, PayPal, and others, creating an air of legitimacy. When individuals call the numbers provided in these fake invoices, they are connected to call centers typically located in India. In extensive investigations involving over 50 calls to different numbers, Perception Point researchers discovered that scammers are creating over 1,000 templates each month.

The ultimate aim of these phone scams is to gain control over the endpoint. By impersonating services that individuals use on a regular basis, the scammers exploit the inherent trust associated with familiar brands. For instance, if an invoice appears to be from a service like PayPal, QuickBooks, or Intuit, individuals are more likely to make the call to verify its authenticity. This approach capitalizes on the absence of malicious URLs or files, with users making the initial contact themselves.



S service@paypal.com | demo@perception-point.io

[Trusted] You've got a money request

If there are problems with how this message is displayed, click here to view it in a we

GeekSquad sent you a money

Payment request details

Amount requested
$1,499.99 USD

Note from GeekSquad:
+1-(888)-575 7558.

YO Your Order Confirmation <quickbooks@notification.intuit.com>

Invoice K8Y6:L698 from Your Order Confirmation

If there are problems with how this message is displayed, click here to view it in a web browser.

Invoice_K8Y6L698_from_Your_Order_Confirmation.pdf
48 KB

INVOICE K8Y6:L698 DETAILS

PayPal

Your Order Confirmation

DUE 07/18/2022

$792.00

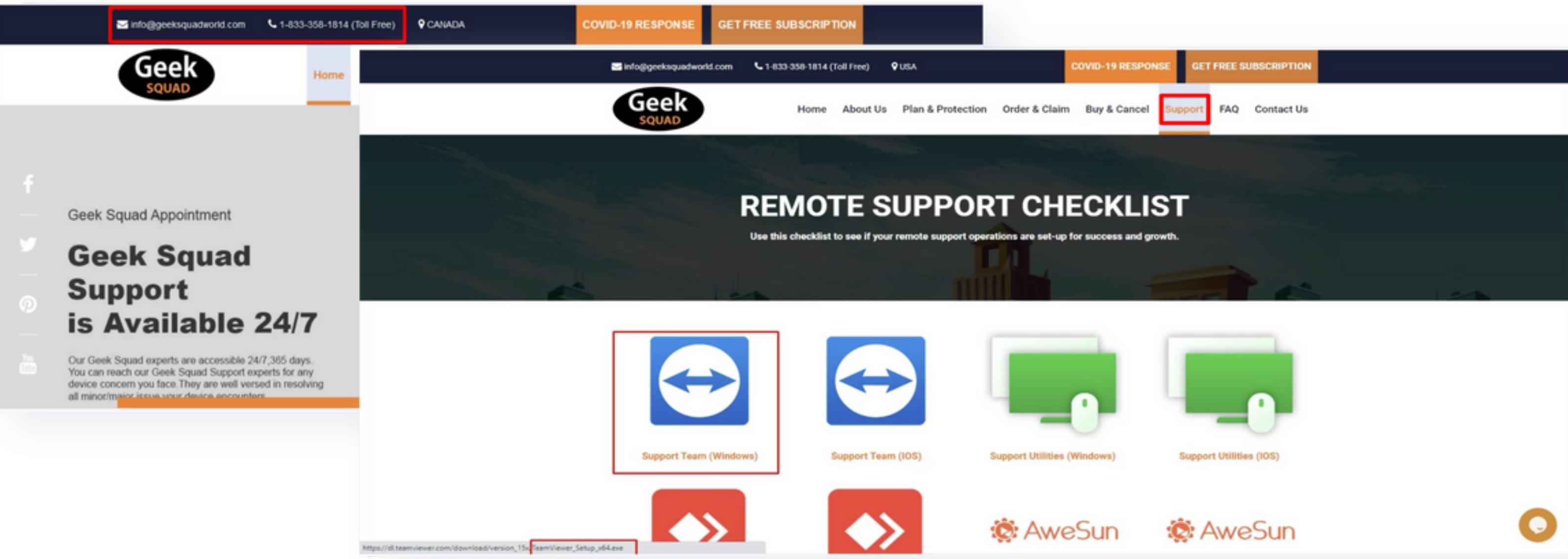
Print or save

Powered by QuickBooks

Help & Support
+1 (888) 229-4381

In the example presented below, you can see an excellent impersonation of Geek Squad, a service offered by Best Buy. The attackers create a lookalike domain, geesquadword(.)com, complete with a fake phone number. The victim calls the call center representative who then directs them to the fake website, where they are instructed to download TeamViewer under the guise of technical support. This interaction allows the scammers access to victims' laptops, enabling them to download additional payloads, such as information stealers, without relying on traditional email-based methods.

This approach to delivering malware leverages trust and the absence of malicious elements in the initial contact, making it more challenging for users to discern the scam.



info@geeksquadworld.com 1-833-358-1814 (Toll Free) CANADA

Geek Squad Appointment

Geek Squad Support is Available 24/7

Our Geek Squad experts are accessible 24/7,365 days. You can reach our Geek Squad Support experts for any device concern you face. They are well versed in resolving all minor/major issue your device encounters

info@geeksquadworld.com 1-833-358-1814 (Toll Free) USA

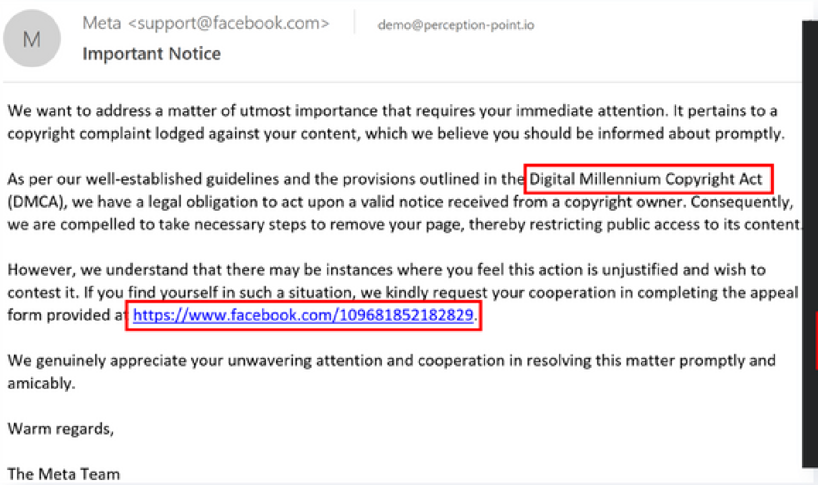
REMOTE SUPPORT CHECKLIST

Use this checklist to see if your remote support operations are set-up for success and growth.

https://dl.teamviewer.com/download/version_15x/TeamViewer_Setup_x64.exe

Social Media Posts

The abuse of social media platforms, including LinkedIn, Facebook, and Twitter (now X), is a growing concern as attackers employ increasingly sophisticated tactics. A notable example involves a phishing attempt disguised as an email from support@facebook(.)com. The email contains a seemingly legitimate Facebook URL that redirects the user to a Facebook group called "DMCA form." Upon entering the group, the user receives a notification claiming a policy violation, prompting them to fill out a form within 48 hours to avoid account shutdown.



M

Meta <support@facebook.com> | demo@perception-point.io

Important Notice

We want to address a matter of utmost importance that requires your immediate attention. It pertains to a copyright complaint lodged against your content, which we believe you should be informed about promptly.

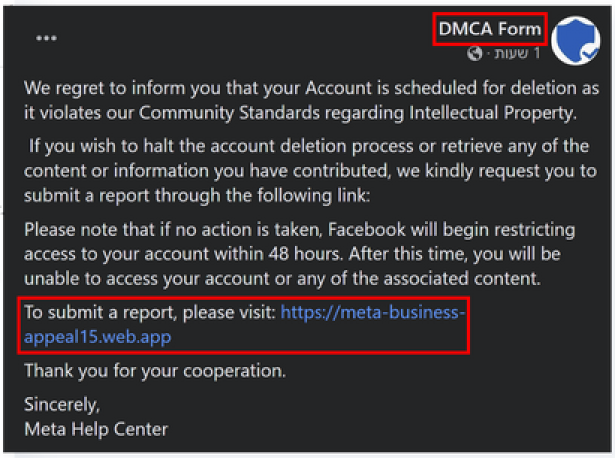
As per our well-established guidelines and the provisions outlined in the Digital Millennium Copyright Act (DMCA), we have a legal obligation to act upon a valid notice received from a copyright owner. Consequently, we are compelled to take necessary steps to remove your page, thereby restricting public access to its content.

However, we understand that there may be instances where you feel this action is unjustified and wish to contest it. If you find yourself in such a situation, we kindly request your cooperation in completing the appeal form provided at https://www.facebook.com/109681852182829.

We genuinely appreciate your unwavering attention and cooperation in resolving this matter promptly and amicably.

Warm regards,

The Meta Team



DMCA Form

1 שעות ·

We regret to inform you that your Account is scheduled for deletion as it violates our Community Standards regarding Intellectual Property.

If you wish to halt the account deletion process or retrieve any of the content or information you have contributed, we kindly request you to submit a report through the following link:

Please note that if no action is taken, Facebook will begin restricting access to your account within 48 hours. After this time, you will be unable to access your account or any of the associated content.

To submit a report, please visit: https://meta-business-appeal15.web.app

Thank you for your cooperation.

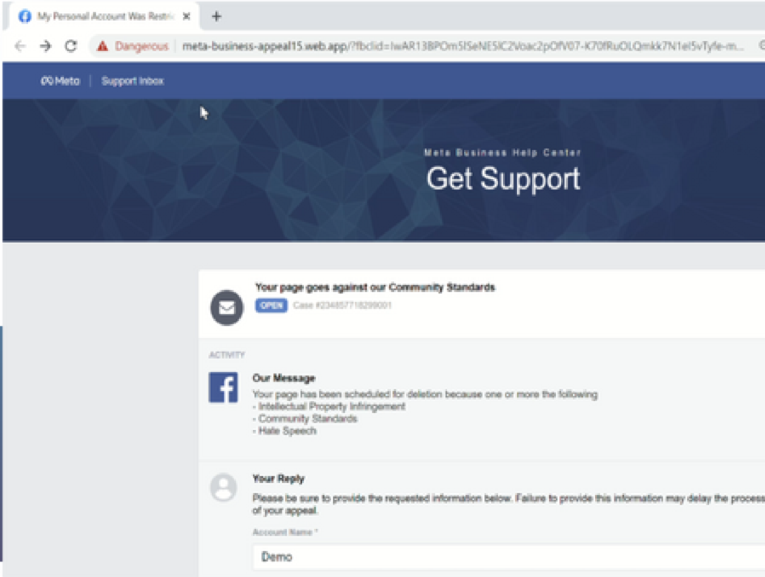
Sincerely,
Meta Help Center

The malicious URL embedded in the form redirects the user to a web application that convincingly mimics the Facebook interface. This spoofed page includes a familiar design and font, creating an environment that can easily deceive unsuspecting users. Once the user submits the form, the application displays a GIF impersonating Meta, finally asking the user to enter their password.

The shift towards attempting to steal social media passwords reflects attackers' understanding that individuals often reuse passwords across multiple platforms. Acquiring access to a LinkedIn account, for instance, could potentially grant access to a user's broader online presence, including work-related applications.

> Organizations use more than six types of tools for communication and collaboration. There is a growing reliance on cloud collaboration apps and web browsers for employee productivity and collaboration with external parties.

Osterman Research, The Rise of Cyber Threats Against Email, Browsers and Emerging Cloud-Based Channels



My Personal Account Was Restri

Dangerous | meta-business-appeal15.web.app/?fbclid=IwAR13BPOm5ISeNESIC2Voac2pOfV07-K70fRuOLQmkk7N1el5vTyfe-m...

Meta Business Help Center

Get Support

Your page goes against our Community Standards

OPEN Case #234857718299001

ACTIVITY

Our Message

Your page has been scheduled for deletion because one or more the following
- Intellectual Property Infringement
- Community Standards
- Hate Speech

Your Reply

Please be sure to provide the requested information below. Failure to provide this information may delay the process of your appeal.

Account Name *

Demo

Account Takeover

Understanding the intricacies of account takeover is crucial in comprehending the evolving landscape of cyber threats. The process typically involves a series of steps:

1 **Generate Phishing Email**

An attacker initiates the process by creating a phishing email. This could be done using tools like ChatGPT, custom-built solutions, or by purchasing resources from the Darknet.

2 **Send Phishing Email**

The crafted phishing email is then sent to the victim's mailbox, exploiting social engineering techniques to increase the likelihood of the victim falling for the attack.

3 **Victim Opens Email**

The victim interacts with the phishing email, opening it.

4 **Victim Enters Credentials**

The victim clicks on the URL provided, unknowingly entering their credentials into a fake login window.

5 **Attacker Gains Credentials**

The attacker successfully retrieves the entered credentials, now having unauthorized access to the victim's mailbox.

6 **Attacker Logs Into Victim's Mailbox**

7 **Define Malicious Inbox Rules**

With control over the victim's mailbox, the attacker defines new malicious inbox rules. These rules are used to automate the next steps in the attack.

8 **Deliver Malicious Payloads**

The attacker exploits the compromised mailbox to deliver malicious payloads. This can include phishing attacks, malware, or business email compromise attacks.

9 **Known Contacts**

Using known contacts, the attacker is able to compromise more mailboxes, which are used to send massive phishing campaigns, leading to a significant increase of compromised mailboxes used in such attacks.

10 **Recursive Phishing**

The term "recursive phishing" is used to describe the attacker's strategy of leveraging the victim's mailbox to perpetuate the attack. This creates a never-ending loop as the attacker continues to expand their database by infecting known contacts.

The prevalence of this account takeover technique has seen a staggering 500% increase over the past year, emphasizing the effectiveness and persistence of attackers in exploiting compromised mailboxes for widespread phishing campaigns.

A critical component of any ATO attack involves Step #7: Define Malicious Inbox Rules. To detect and mitigate the impact of such breaches, there are a few key indicators investigators should consider. These indicators help identify suspicious activities and potential threats. They include:

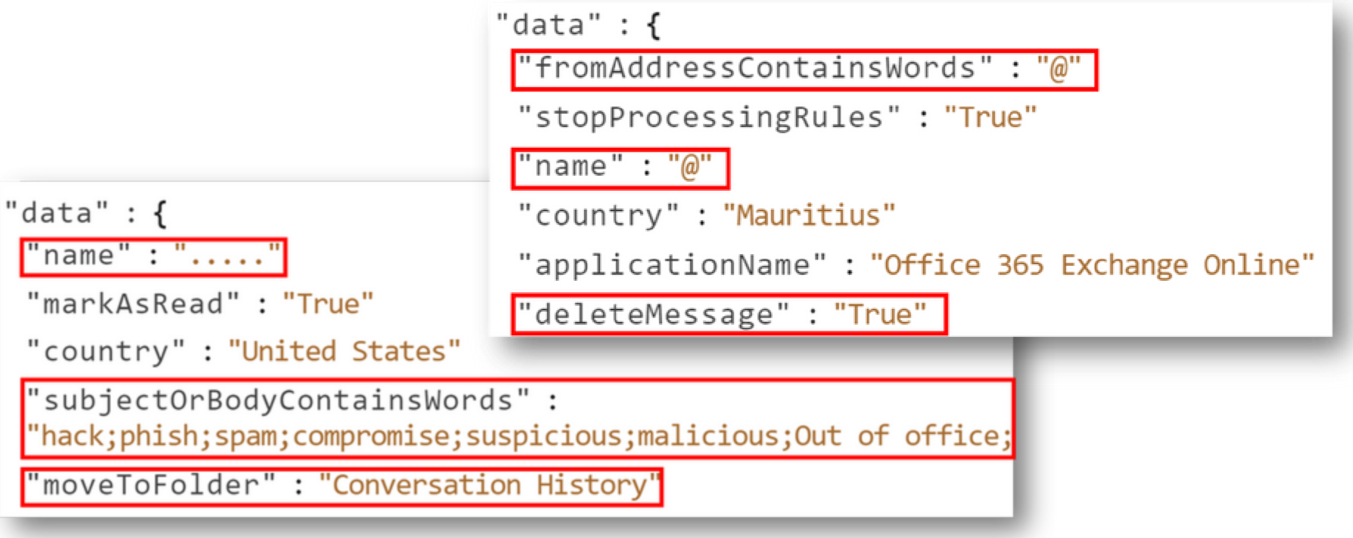
A. Suspicious Logins

Examine the login details, including IP addresses and the originating country, to identify unusual or suspicious activity. Login audit logs can provide valuable information in this regard.

B. Inbox Rules

1. Suspicious Indicators: Look for rules that exhibit suspicious characteristics, including:
   a. Rule names
   b. Delete actions
   c. Move actions
   d. Suspicious text filtering, like “subjectOrBodyContainsWords” or “fromAddressContainsWords”
2. Forwarding Rules: Identify rules that forward emails outside the organization, as this could be a red flag.

Attackers create rules to divert or delete emails that could reveal their presence in the compromised mailbox. This is one way that attackers employ evasion techniques within the defined rules. For instance, an attacker might set up rules to move or delete messages containing terms like "hack," "phish," "spam," "compromised," or "out of office." This helps them maintain covert access to the compromised mailbox without alerting the victim.



```
"data" : {
 "fromAddressContainsWords" : "@"
 "stopProcessingRules" : "True"
 "name" : "@"
 "country" : "Mauritius"
 "applicationName" : "Office 365 Exchange Online"
 "deleteMessage" : "True"
```

```
"data" : {
 "name" : "....."
 "markAsRead" : "True"
 "country" : "United States"
 "subjectOrBodyContainsWords" :
 "hack;phish;spam;compromise;suspicious;malicious;Out of office;
 "moveToFolder" : "Conversation History"
```

A New Anti-Phishing Approach

In response to the escalating sophistication of phishing attacks, we advise implementing a layered method that leverages email security, collaboration application security, and browser security, so organizations can holistically and efficiently protect end users.

Perception Point's Advanced Threat Prevention solutions provide organizations with enterprise-grade security for the modern workspace. The solutions combine the highest detection accuracy on the market powered by patented anti-evasion and AI technology, with an all-included Incident Response service. The fully-managed incident response service analyzes and remediates threats, handles on-demand investigations, manages false-positives and creates algorithms on-the-fly to rapidly address new, emerging attacks.

Advanced Email Security is a modern Integrated Cloud Email Security (ICES) solution, that uniquely dynamically scans 100% of content (including embedded text, files, and URLs) in an average of 15 seconds to prevent malicious emails from ever reaching the user's inbox. Its next-gen sandbox technology leverages patented CPU-level technology, detecting attacks at the exploit phase – pre-malware release – for more accurate and near-real time advanced attack zero-day threat prevention.

The result is unparalleled detection and response that not only prevents the most advanced phishing attacks, but also spam, BEC, ATO, malware, ransomware, and Zero-day threats.

This solution can also replace or augment Microsoft's native defenses for OneDrive, SharePoint, and Teams with next-gen detection of all incoming threats including unknown attacks and advanced evasion techniques that bypass Microsoft EOP and Defender.

In addition to email security and cloud app security, organizations should also consider enterprise browser security. With the advent of web extensions, a new paradigm in browser security is developing, surpassing traditional enterprise and isolated browsers. Perception Point's Advanced Browser Security boasts remarkable detection capabilities, primarily dynamic scanning within the browser environment. By closely monitoring end-user actions, it can identify malicious behaviors, including phishing pages and web vulnerabilities. The addition of browser-based detection addresses non-email threats, recognizing that phishing can manifest through various channels like SMS, WhatsApp, Discord, and Telegram.

Browser security can also play a crucial role in account takeover investigations, offering insights into services used and mapping login activities. This capability aids in identifying compromised accounts, addressing password reuse, and enhancing overall security awareness. Additionally, enforcing policies becomes more robust as these extensions allow organizations to define and apply web browser-specific policies, mitigating potential risks and internal threats.

Perception Point's Advanced Browser Security adds enterprise-grade security to standard web browsers (Chrome, Edge, Safari, etc.) fusing advanced threat detection with browser-level governance and DLP controls. The solution provides organizations of all sizes with unprecedented ability to detect, prevent and remediate any browser threat, internal and external, while maintaining user productivity and native browsing experience.

Organizations should adopt a layered security approach to comprehensively protect end users and counter evolving cyber threats. Doing so not only ensures efficiency by minimizing redundancy in threat detection and incident response but also addresses the dynamic nature of phishing techniques, contributing to a resilient cybersecurity posture.

About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection and response to all attacks across email, cloud collaboration channels, and web browsers. The solution's natively integrated incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, Zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing content-borne attacks across their email and cloud collaboration channels with Perception Point.

Visit us: www.perception-point.io
Contact us: info@perception-point.io