Phishing • Spear Phishing • Business Email Compromise • Living Off the Land • CAPTCHA Phishing Attacks • Cryptocurrency Scams

2023 OpenText Cybersecurity Email Threat Report

Introduction

Attackers persistently adapted their email-based techniques throughout 2022, cycling through new and old tactics in the hopes of evading human and cyber security measures.

Phishing remains the dominant strategy — but attackers are introducing more nuances into their methods. For example, they are relying more heavily on living off the land (LotL), building messaging around trending topics, including cryptocurrency and Russia's invasion of Ukraine, and incorporating technology that users find reassuring, such as CAPTCHA and password-encrypted zip folders.

Although the aims of phishing campaigns vary, many are still being used to deploy malware, sometimes as a precursor to a ransomware attack. Microsoft's move against deploying macros in emails has forced malware users to diversify the file types they use. In less positive news, the notorious malware gang and software Emotet made an unwelcome return.

Based on reporting through OpenText Cybersecurity's Advanced Email Threat Protection (AETP), here's a review of email-based cyberattacks in 2022.

Phishing • Spear Phishing • Business Email Compromise • Living Off the Land • Call Back Phishing • Call Center Scams

Phishing

AETP quarantined nearly 7.3 billion emails that were classified as bulk spam, scams, and non-targeted phishing threats in 2022 — a 12.5% increase over 2021. As you can see below, this traffic hit its peak in March of 2021.

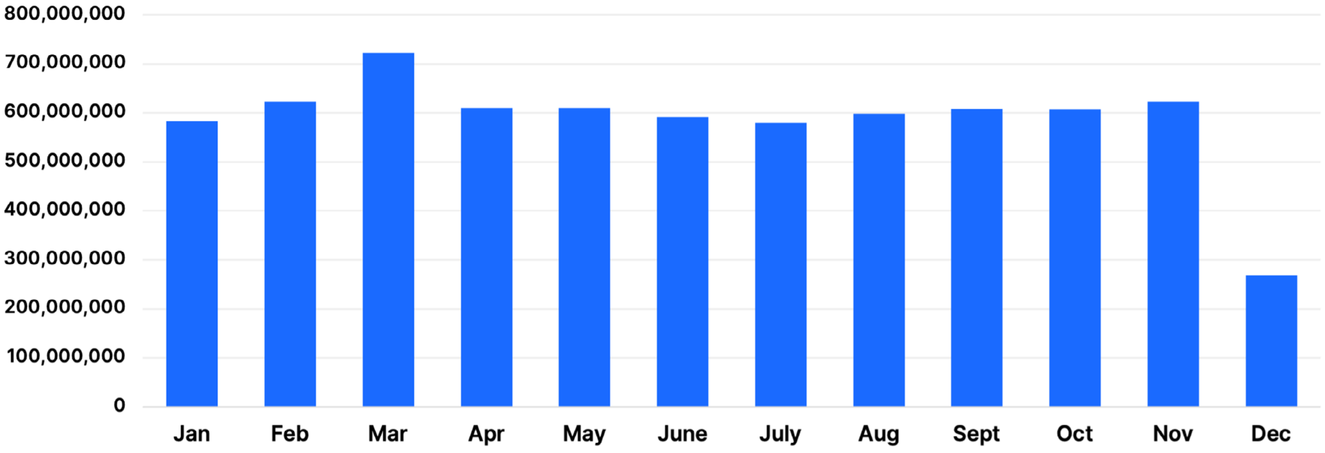


Figure 1: URL and text-based threats

Spear Phishing

Potentially even more concerning than this batch-blast approach are highly targeted attacks known as spear phishing. Attackers are increasingly adding layers of complexity, personalization, and obfuscation to their tactics to increase the likelihood of fooling end users. In 2022, we detected roughly 1.14 billion spear phishing attacks targeting businesses of all sizes, a 16.4% increase over 2021. Several factors, including the further proliferation and widespread availability of phishing tools, likely drove the increase.

Below is a chart depicting the monthly spear phishing traffic observed by our Advanced Email Threat Protection:

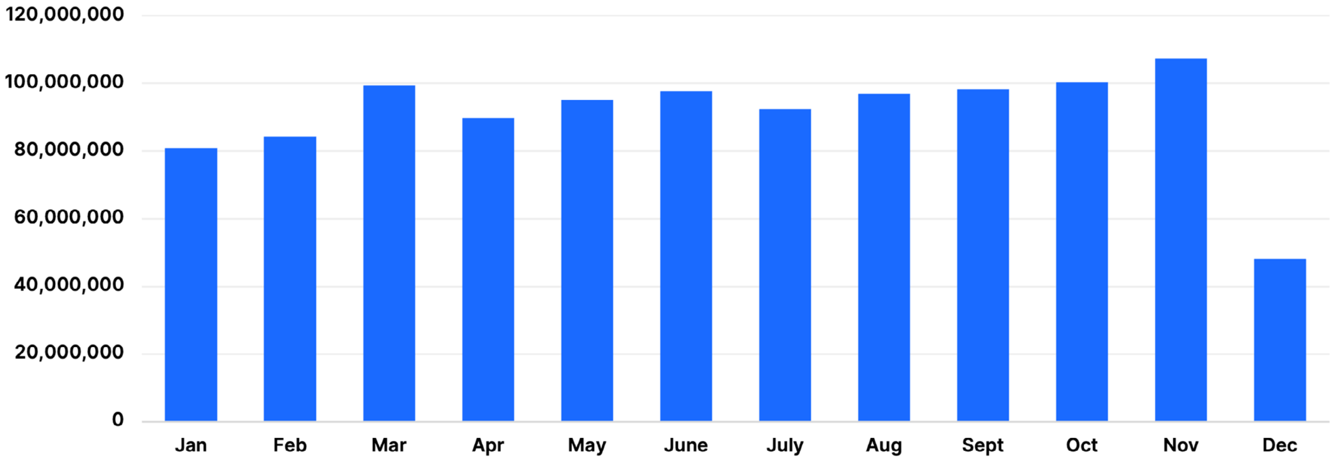
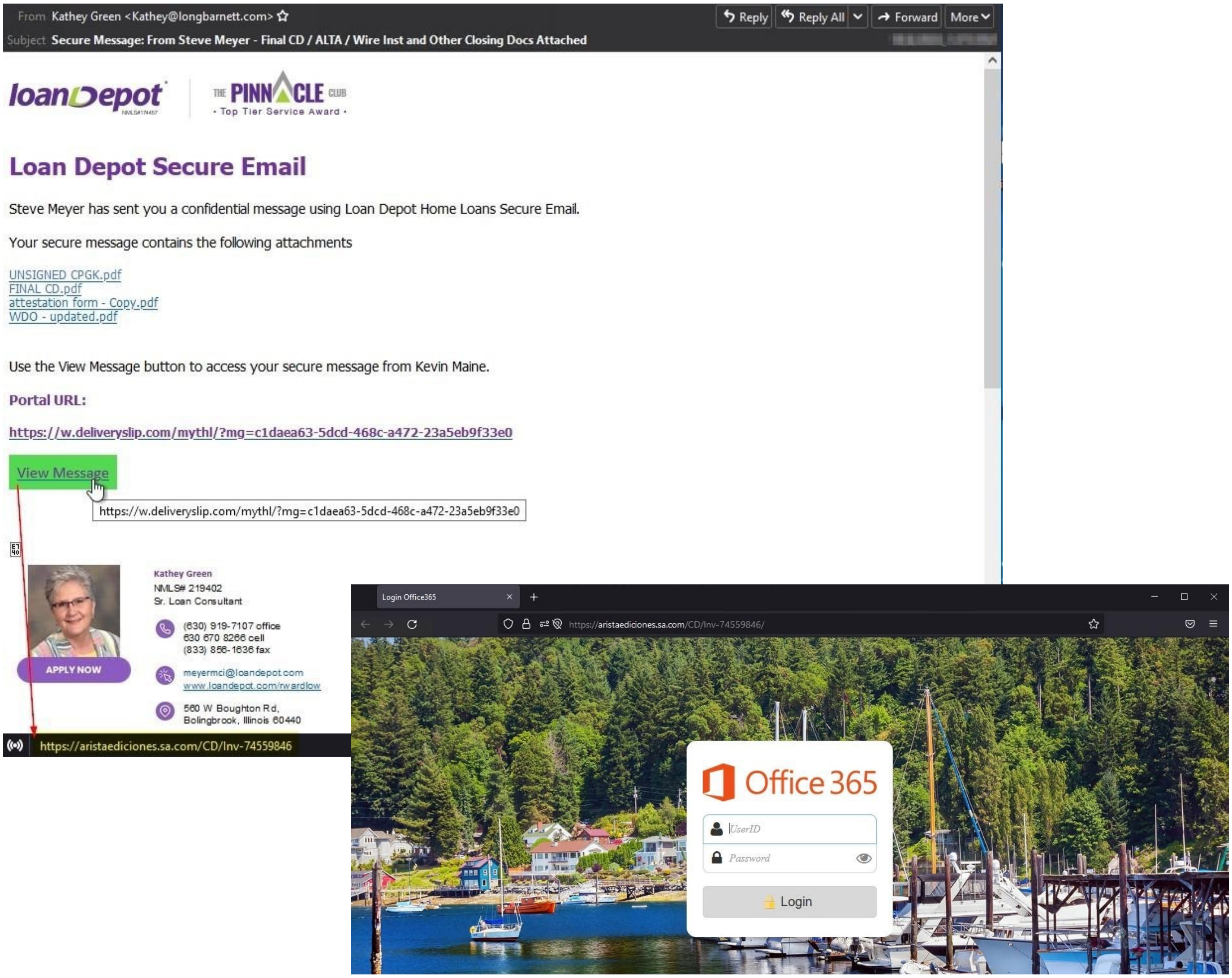


Figure 2: Spear Phishing Attacks

Business Email Compromise (BEC) Attacks

Perpetrators of business email compromise (BEC) attacks use spear phishing tactics to deceive victims into believing they're involved in a real business transaction, with the aim of convincing them to send sensitive account details or to wire money. A popular BEC technique involves registering a domain with a very similar name to a real company or creating one or more email addresses similar to those of real employees in the hopes that recipients of emails from these addresses won't notice the difference.

Compared to other types of phishing or malware attacks, BEC attacks potentially yield huge windfalls while requiring minimal time, money, and technical expertise. In a 2022 Congressional report, the FBI described business email compromise (BEC) attacks as "one of the fastest growing, most financially damaging internet-enabled crimes."[1] They pointed out that according to data from the Internet Crime Complaint Center (IC3), yearly losses attributable to these kinds of attacks had increased from $360 million in 2016 to over $2.4 billion in 2021.



From Kathey Green <Kathey@longbarnett.com>
Subject Secure Message: From Steve Meyer - Final CD / ALTA / Wire Inst and Other Closing Docs Attached [redacted]

Loan Depot Secure Email

Steve Meyer has sent you a confidential message using Loan Depot Home Loans Secure Email.

Your secure message contains the following attachments

UNSIGNED CPGK.pdf
FINAL CD.pdf
attestation form - Copy.pdf
WDO - updated.pdf

Use the View Message button to access your secure message from Kevin Maine.

Portal URL:

https://w.deliveryslip.com/mythl/?mg=c1daea63-5dcd-468c-a472-23a5eb9f33e0

https://w.deliveryslip.com/mythl/?mg=c1daea63-5dcd-468c-a472-23a5eb9f33e0

Kathey Green
NMLS# 219402
Sr. Loan Consultant

(630) 919-7107 office
630 670 8266 cell
(833) 856-1636 fax

meyermci@loandepot.com
www.loandepot.com/rwardlow

560 W Boughton Rd,
Bolingbrook, Illinois 60440

https://aristaediciones.sa.com/CD/Inv-74559846

Login Office365

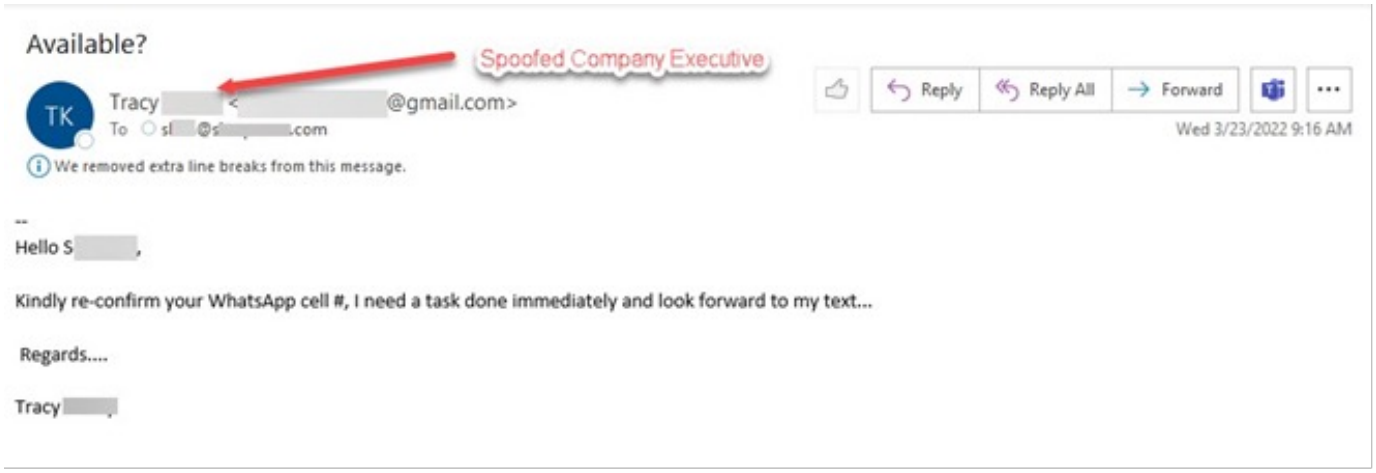
https://aristaediciones.sa.com/CD/Inv-74559846/

[1] https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view

This example shows a type of BEC attack called real estate wire fraud (REWF), in which perpetrators specifically target real estate transactions, often by pretending to be one of the parties involved. Here, the BEC attacker created a fake email from a real mortgage company loanDepot, including the final loan closing disclosures, wire instructions, and other related mortgage documents as attachments. They even created a signature with a photo. The link destination preview was designed to trick users by showing our Delivery Slip secure email service. However, the actual link was to a subdomain located at a Saudi Arabian TLD. Recipients who followed the link were directed to an Office 365-themed credential-harvesting site.

Channel Switching

Channel switching is a common BEC technique in which the attacker convinces the target to change from email to mobile communications in order to avoid email security filters. While most channel switching attacks involve moving to text messaging, attackers have also leveraged messaging apps, perhaps in response to more restrictive text filtering. In the example below, the attacker is posing as a company executive and attempting to convince their mark to channel switch to WhatsApp.



Available?

Spoofed Company Executive

Tracy [redacted] <[redacted]@gmail.com>

To sl[redacted]@s[redacted].com

Wed 3/23/2022 9:16 AM

We removed extra line breaks from this message.

--

Hello S[redacted],

Kindly re-confirm your WhatsApp cell #, I need a task done immediately and look forward to my text...

Regards....

Tracy [redacted]

Living Off the Land (LotL)

Over the last few years, phishing has become increasingly popular as a way to execute a type of cyberattack known as living off the land (LotL), in which attackers infiltrate a legitimate system and use its tools to mask and conduct malicious activities. Since these services are frequently used for legitimate purposes, they cannot be simply blocked outright in most cases and are harder for end users to detect.

Top 20 most abused services for malicious LotL links

1. **storage.googleapis.com (Google)**
2. **appspot.com (Google)**
3. **page.link (Google)**
4. **amazonaws.com (Amazon)**
5. **docs.google.com (Google)**
6. **windows.net (Microsoft)**
7. **cloudfront.net (Amazon)**
8. **blogspot.com (Google)**
9. **sendgrid.net (Twilio)**
10. **azurewebsites.net (Microsoft)**
11. **web.app (Google)**
12. **glitch.me (Fastly)**
13. **wetransfer.com (WeTransfer)**
14. **list-manage.com (Mailchimp / Intuit)**
15. **azureedge.net (Microsoft)**
16. **rebrand.ly (Rebrandly)**
17. **azure.com (Microsoft)**
18. **surveymonkey.com (Momentive)**
19. **my.sharepoint.com (Microsoft)**
20. **sites.google.com (Google)**

The following chart shows the frequency at which the top 10 most abused services were used in LotL attacks, broken down across each month of 2022. In 2022, these 10 services were invoked in 123 million phishing emails intended to launch LotL attacks.

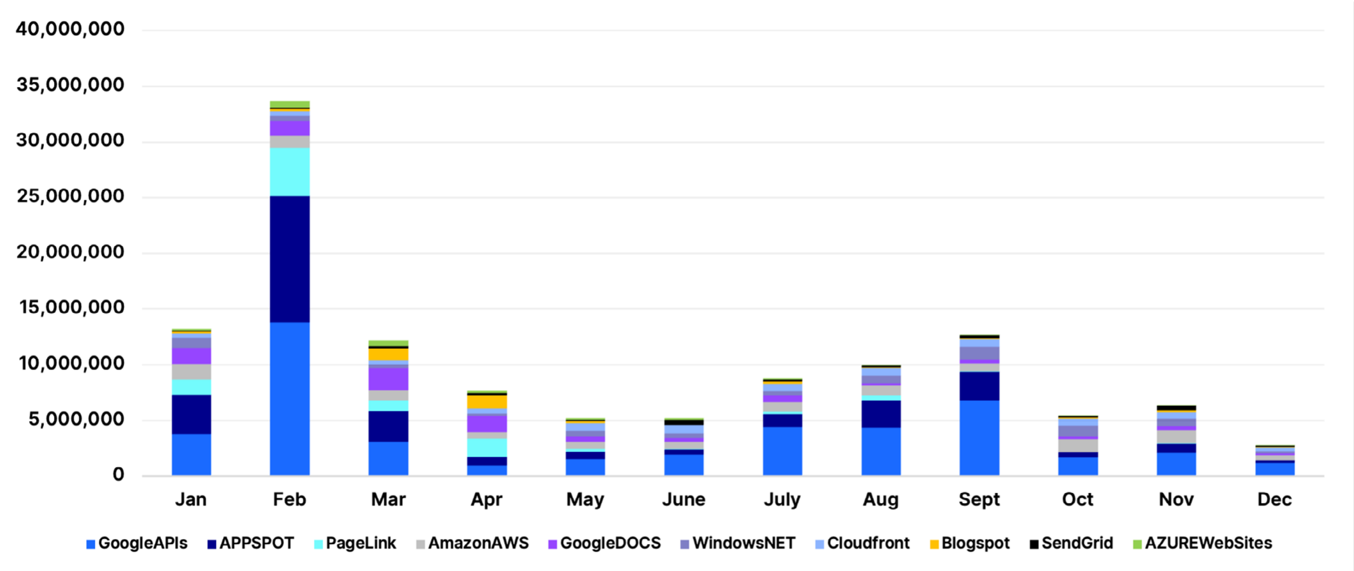
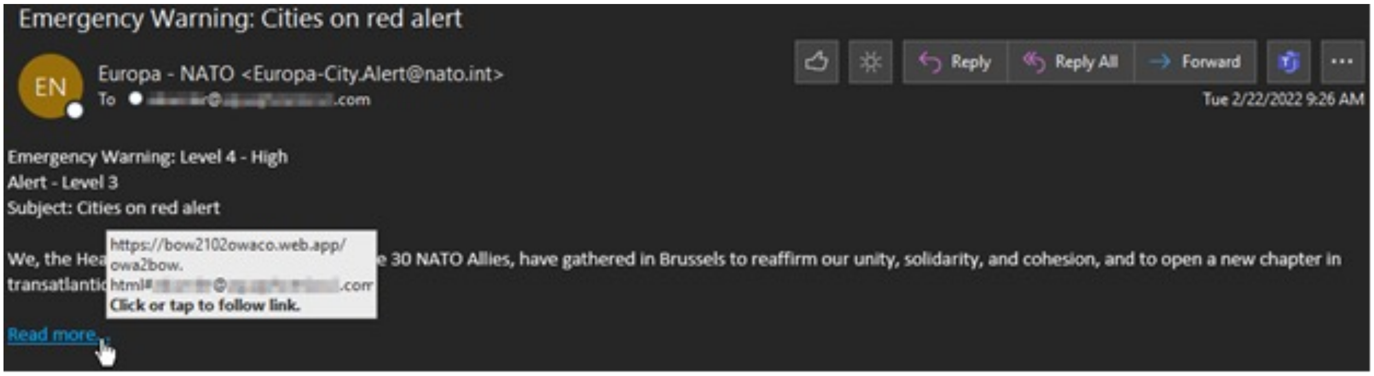


Figure 3: Top 10 abused services

Examples of LotL Phishing Attacks

Example A: Capitalizing on current events to pose as NATO

In February of 2022, a large LotL phishing campaign targeted customers with an emergency warning supposedly from NATO. The attacker was leveraging geopolitical events around Russia's pending invasion of Ukraine to urge recipients to click a Google link (.web.app) and "Read more."



Emergency Warning: Cities on red alert

Europa - NATO <Europa-City.Alert@nato.int>
To [redacted].com

Tue 2/22/2022 9:26 AM

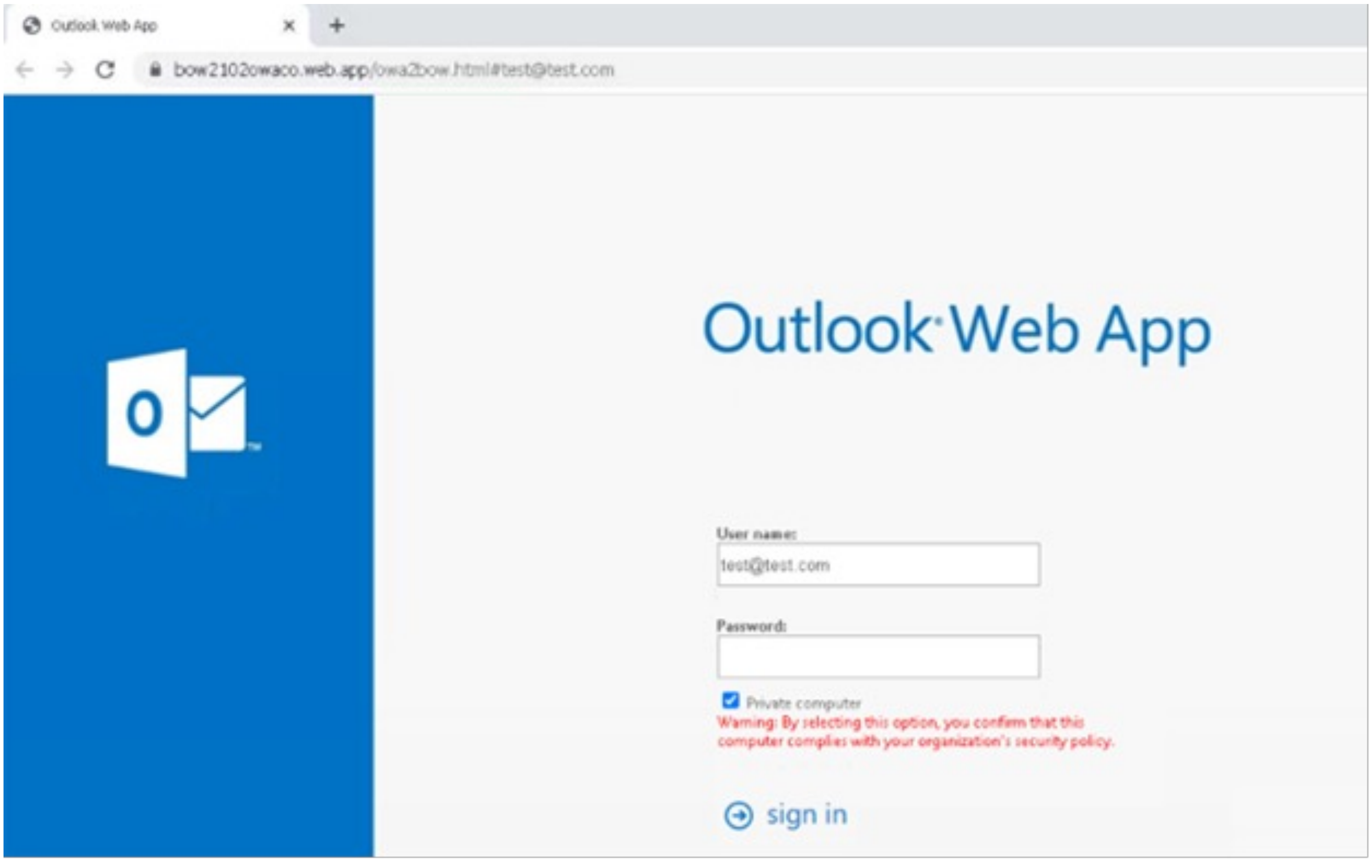
Emergency Warning: Level 4 - High
Alert - Level 3
Subject: Cities on red alert

We, the Hea… e 30 NATO Allies, have gathered in Brussels to reaffirm our unity, solidarity, and cohesion, and to open a new chapter in transatlanti…

https://bow2102owaco.web.app/owa2bow.html#[redacted].com
Click or tap to follow link.

Read more.

The link leads to a credential-harvesting page posing as Microsoft's OWA (Outlook Web App), hosted on the frequently abused Google App platform.



bow2102owaco.web.app/owa2bow.html#test@test.com

Outlook Web App

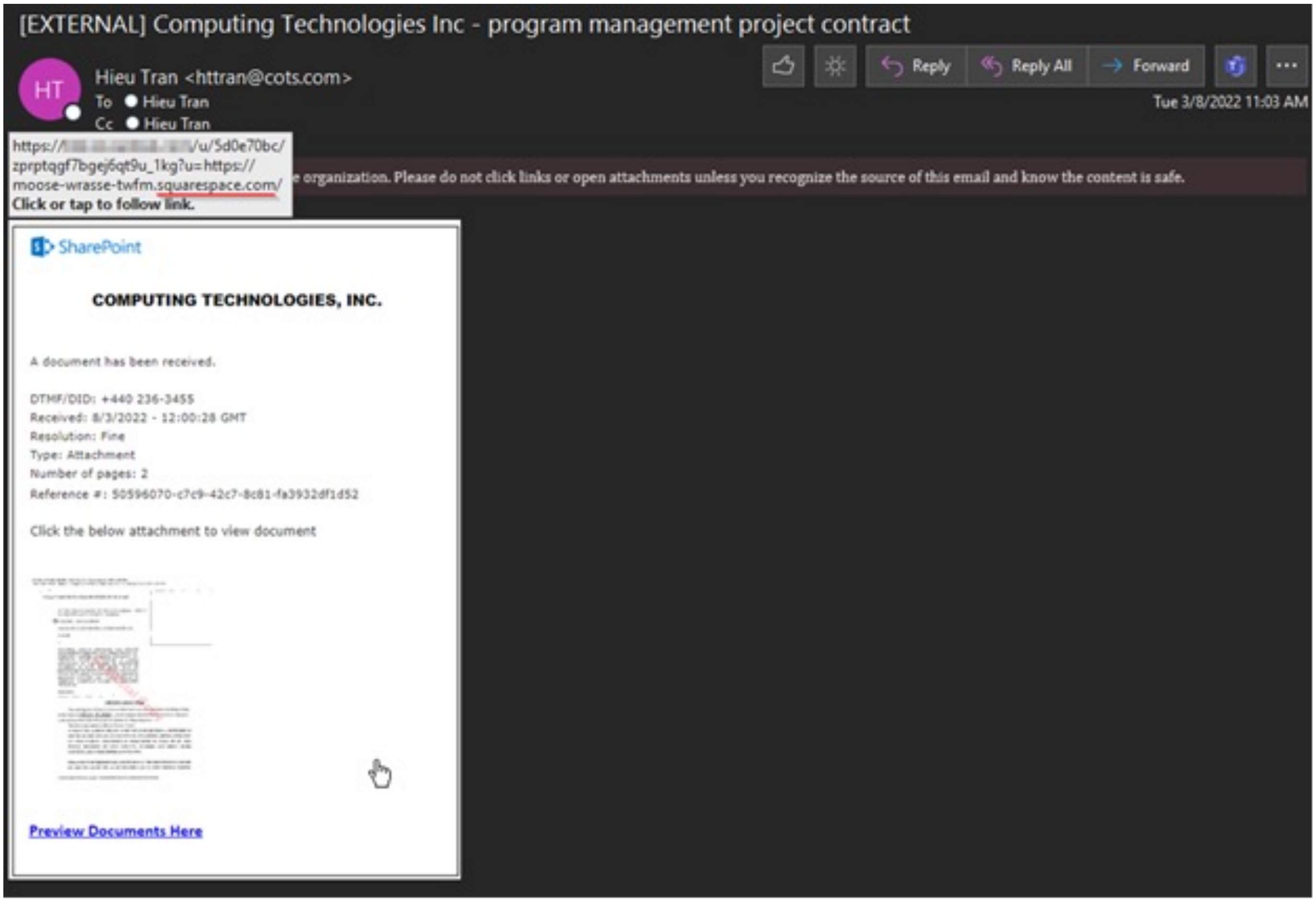
User name:
test@test.com

Password:

☑ Private computer
Warning: By selecting this option, you confirm that this computer complies with your organization's security policy.

Example B: Squarespace and Image Phishing

While not ranked in our top 20, the website-building and hosting company Squarespace, Inc. has also been used in LotL attacks. In this example, the attacker deliberately avoided using text in the body of the message as a way to escape detection by email filters, instead inserting an image with a hyperlink that led to a Microsoft Word-themed credential harvesting page.



[EXTERNAL] Computing Technologies Inc - program management project contract

Hieu Tran <httran@cots.com>
To ● Hieu Tran
Cc ● Hieu Tran

Tue 3/8/2022 11:03 AM

https://[redacted]/u/5d0e70bc/zprptqgf7bgej6qt9u_1kg?u=https://moose-wrasse-twfm.squarespace.com/
Click or tap to follow link.

e organization. Please do not click links or open attachments unless you recognize the source of this email and know the content is safe.

COMPUTING TECHNOLOGIES, INC.

A document has been received.

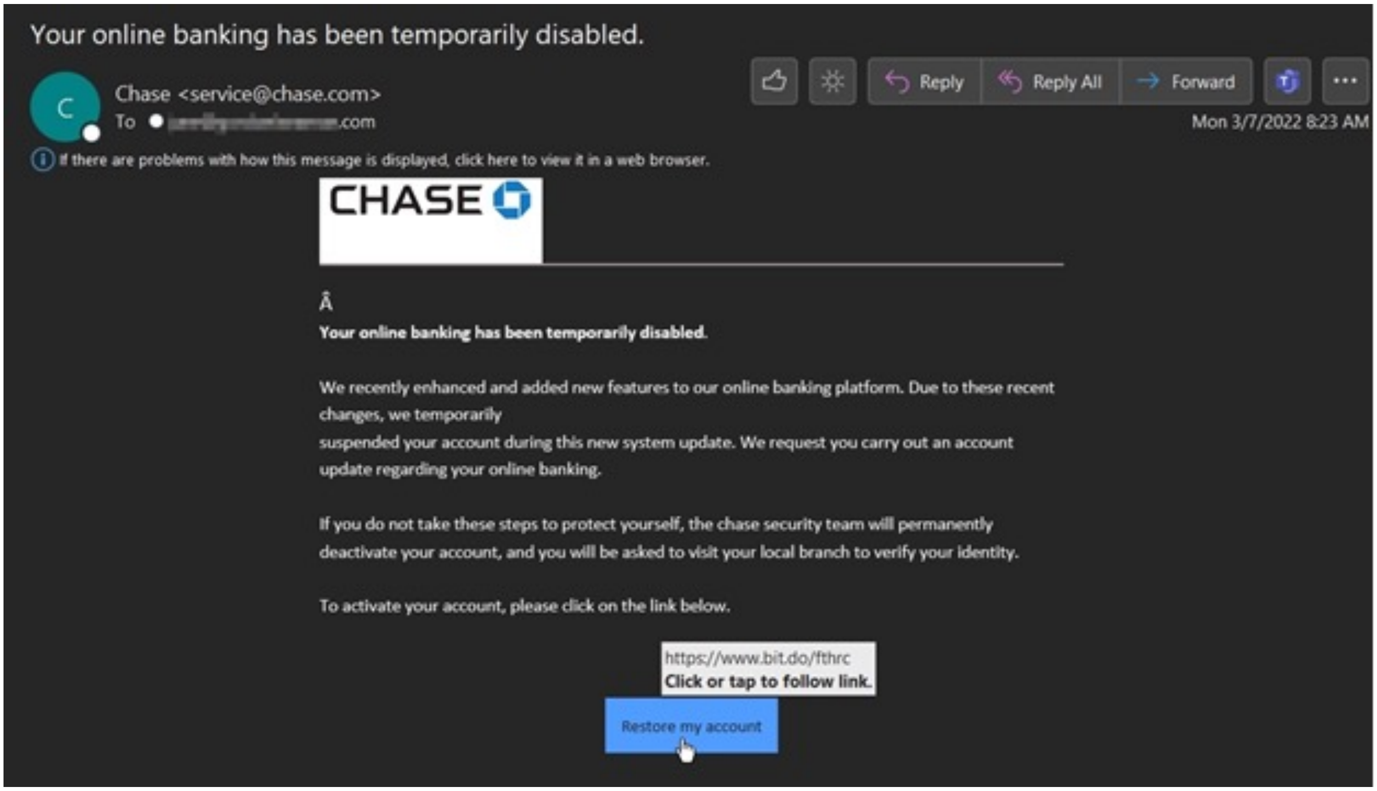
DTMF/DID: +440 236-3455
Received: 8/3/2022 - 12:00:28 GMT
Resolution: Fine
Type: Attachment
Number of pages: 2
Reference #: 50596070-c7c9-42c7-8c81-fa3932df1d52

Click the below attachment to view document

Preview Documents Here

Example C: Fake security update for Chase Bank

Banking-themed phishing attacks have been popular for years. A recent version that AETP filters captured purported to be a security update, letting the recipient know that their account had been temporarily disabled. To restore their account, the recipient was told to click on a bit[.]do shortened URL, which redirected them to a [.life] TLD hosting a corresponding Chase-themed credential harvesting page. In this example, not only is the attacker masking the ultimate destination of the link by using a shortener, bit[.]do also provides them with real-time click metrics, allowing them to monitor the progress of their attacks.



Your online banking has been temporarily disabled.

Chase <service@chase.com>
To [redacted].com

Mon 3/7/2022 8:23 AM

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

Â

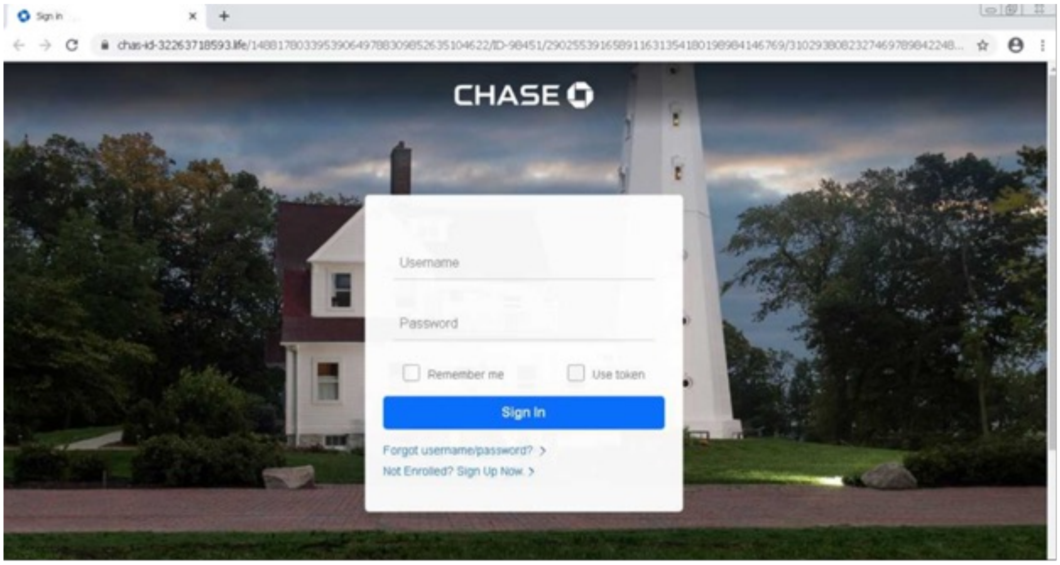
Your online banking has been temporarily disabled.

We recently enhanced and added new features to our online banking platform. Due to these recent changes, we temporarily
suspended your account during this new system update. We request you carry out an account update regarding your online banking.

If you do not take these steps to protect yourself, the chase security team will permanently deactivate your account, and you will be asked to visit your local branch to verify your identity.

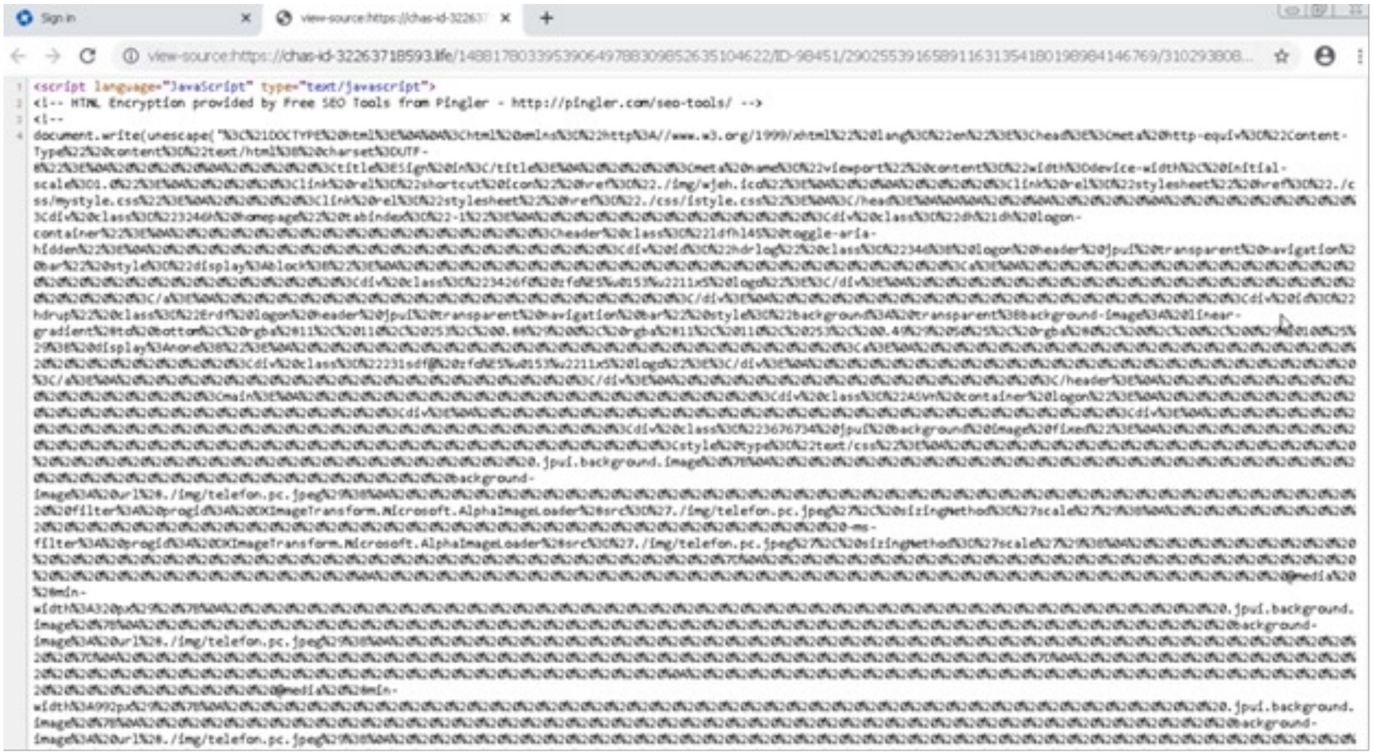
To activate your account, please click on the link below.

https://www.bit.do/fthrc
Click or tap to follow link.



chas-id-32263718593.life/148817803395390649788309852635104622/ID-98451/290255391658911631354180198984146769/3102938082327469789842248...

Analyzing the source code, we can see this threat actor utilized URL-encoded scripting to hide from web scanners. We have observed phishing actors increasingly using this tactic on phishing sites and within hyper-text markup file attachments. This example used a free tool provided by Pingler to encode this page.

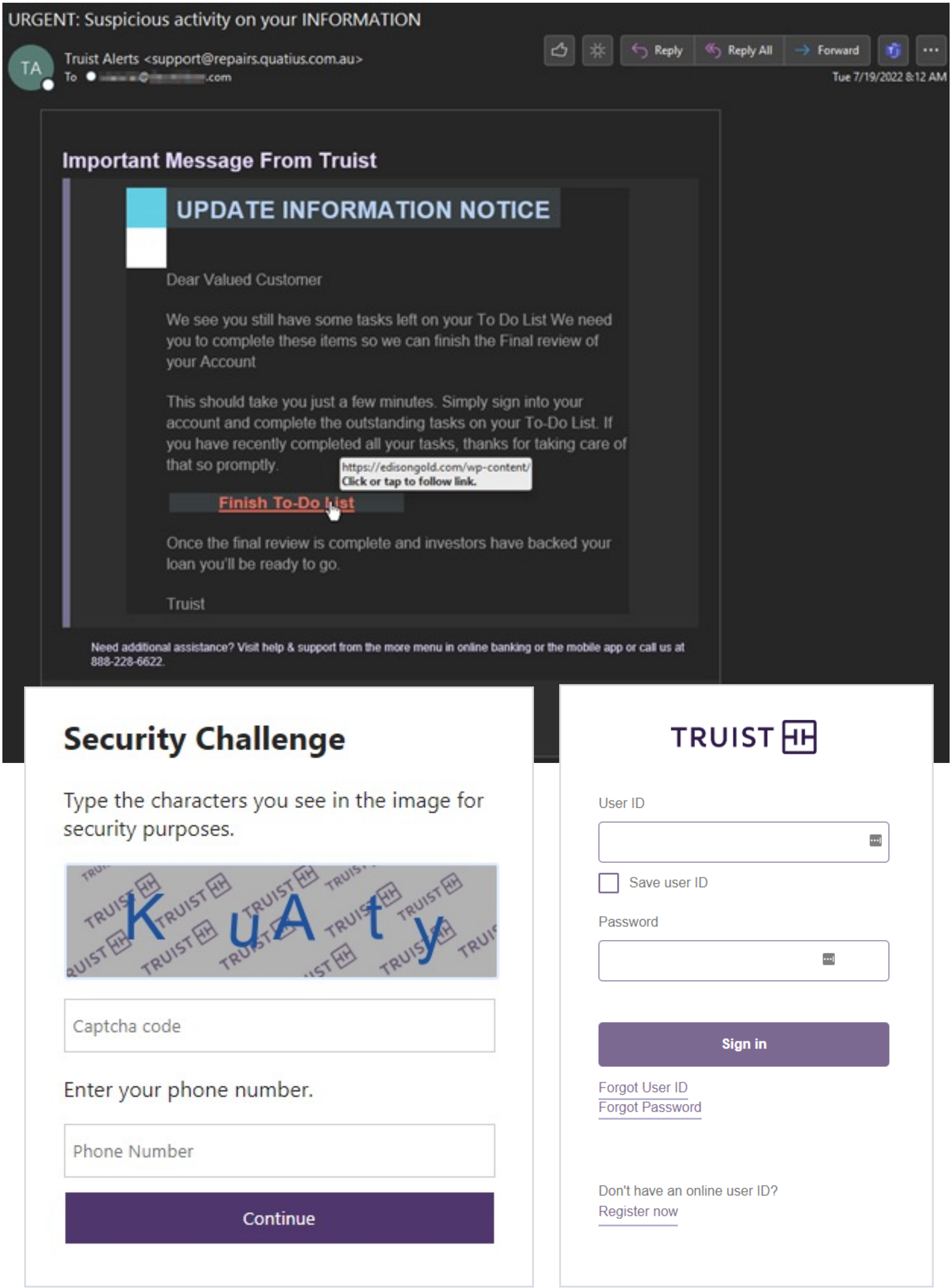

Sign in
view-source:https://chas-id-32263
view-source:https://chas-id-32263718593.life/148817803395390649788309852635104622/ID-98451/290255391658911631354180198984146769/310293808...

```
<script language="JavaScript" type="text/javascript">
<!-- HTML Encryption provided by Free SEO Tools from Pingler - http://pingler.com/seo-tools/ -->
<!--
document.write(unescape("%3C%21DOCTYPE%20html%3E%0A%0A%3Chtml%20xmlns%3D%22http%3A//www.w3.org/1999/xhtml%22%20lang%3D%22en%22%3E%3Chead%3E%3Cmeta%20http-equiv%3D%22Content-
Type%22%20content%3D%22text/html%3B%20charset%3DUTF-
8%22%3E%0A%20%20%20%20%0A%20%20%20%20%3Ctitle%3ESign%20in%3C/title%3E%0A%20%20%20%20%3Cmeta%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-
scale%3D1.0%22%3E%0A%20%20%20%20%3Clink%20rel%3D%22shortcut%20icon%22%20href%3D%22./img/wjeh.ico%22%3E%0A%20%20%0A%20%20%20%20%3Clink%20rel%3D%22stylesheet%22%20href%3D%22./c
ss/mystyle.css%22%3E%0A%20%20%20%20%3Clink%20rel%3D%22stylesheet%22%20href%3D%22./css/istyle.css%22%3E%0A%3C/head%3E%0A%0A%0A%20%20%0A%20%20%20%20%0A%20%20%20%20%20%20%20%20%
3Cdiv%20class%3D%22324dh%20homepage%22%20tabindex%3D%22-1%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cdiv%20class%3D%22dh%21dh%20logon-
container%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cheader%20class%3D%221dfh145%20toggle-aria-
hidden%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cdiv%20id%3D%22hdrlog%22%20class%3D%22346%3B%20logon%20header%20jpul%20transparent%20navigation%2
0bar%22%20style%3D%22display%3Ablock%3B%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Ca%3E%0A%20%20%20%20%20%20%20%20%20%20%20%2
[illegible]
hdrup%22%20class%3D%22Erdf%20logon%20header%20jpul%20transparent%20navigation%20bar%22%20style%3D%22background%3A%20transparent%3Bbackground-image%3A%20linear-
gradient%28to%20bottom%2C%20rgba%2811%2C%2011%2C%2025%2C%200.88%29%20%2C%20rgba%2811%2C%2011%2C%2025%2C%200.49%29%205%25%2C%20rgba%280%2C%200%2C%200%2C%200%29%20100%25%
[illegible]
```

CAPTCHA in Phishing Attacks

Attackers continue to integrate CAPTCHA technologies into their phishing attacks. Since security products like web scanners are not able to solve CAPTCHAs (as they are, in fact, a type of robot), they are prevented from accessing and scanning the next page, which attackers can therefore use to host threats. As a recognizable security tool, a CAPTCHA may also deceive end users by giving the page an air of credibility.

Phishing attackers used this technique to target financial corporation Truist in an expansive campaign disguised as suspicious activity alerts. Victims were sent an email that included a hyperlink labeled “Finish To-Do List.” This took the user to a page with a Truist-branded CAPTCHA and a box for a phone number — potentially another way to add credibility, and/or to capture the number to use in future mobile attacks. One the user entered the CAPTCHA code and phone number, they were taken to a Truist-branded credential-harvesting page.



URGENT: Suspicious activity on your INFORMATION

Truist Alerts <support@repairs.quatius.com.au>

To [redacted].com

Tue 7/19/2022 8:12 AM

Important Message From Truist

UPDATE INFORMATION NOTICE

Dear Valued Customer

We see you still have some tasks left on your To Do List We need you to complete these items so we can finish the Final review of your Account

This should take you just a few minutes. Simply sign into your account and complete the outstanding tasks on your To-Do List. If you have recently completed all your tasks, thanks for taking care of that so promptly.

https://edisongold.com/wp-content/
Click or tap to follow link.

Finish To-Do List

Once the final review is complete and investors have backed your loan you'll be ready to go.

Truist

Need additional assistance? Visit help & support from the more menu in online banking or the mobile app or call us at 888-228-6622.

Security Challenge

Type the characters you see in the image for security purposes.

Captcha code

Enter your phone number.

Phone Number

Continue

TRUIST

User ID

□ Save user ID

Password

Sign in

Forgot User ID
Forgot Password

Don't have an online user ID?
Register now

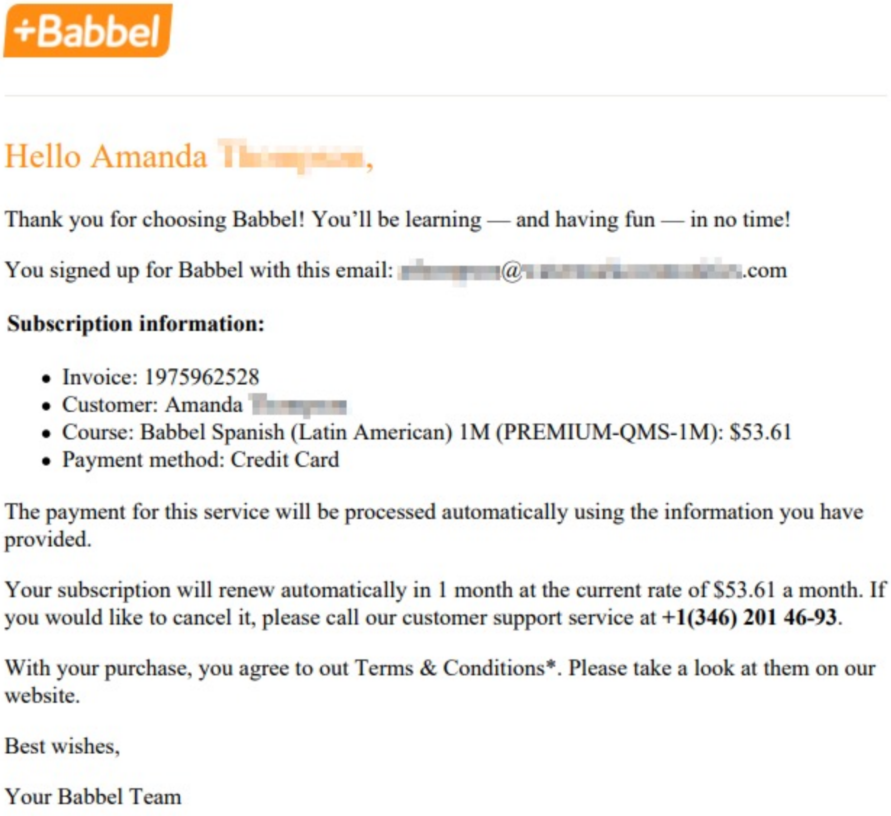
Callback Phishing/Call Center Scams

The ultimate aim of a callback phishing scheme is to gain remote access to the victim's computer and install software that allows the attacker to continually harvest sensitive information or demand a ransom.

Callback phishing typically begins with the perpetrator sending an email with a fake invoice directly attached or accessed through a link. The email states that a payment has been processed for a subscription to whichever service they are posing as and includes a number the recipient should call with any questions about the transaction. Common examples of services perpetrators imitate include online learning platform MasterClass, language learning software Babbel, and — ironically — McAfee, Norton, and Geek Squad, all of which are involved in computer security.

When the recipient of the email calls the number to query the charge, the scammer on the other end of the line tries to convince their target to allow them to establish a remote session. Once they are granted access to the end user's machine, they typically try to install remote access software.

In worst-case scenarios, attackers combine callback phishing with malware and ransomware. For example, the ransomware group Royal (which includes former members of the notorious Conti ransomware gang) have been observed using remote access to infect devices with Qakbot and Cobalt Strike, exfiltrating stolen data before deploying their ransomware payload.



Hello Amanda [redacted],

Thank you for choosing Babbel! You'll be learning — and having fun — in no time!

You signed up for Babbel with this email: [redacted]@[redacted].com

Subscription information:

- Invoice: 1975962528
- Customer: Amanda [redacted]
- Course: Babbel Spanish (Latin American) 1M (PREMIUM-QMS-1M): $53.61
- Payment method: Credit Card

The payment for this service will be processed automatically using the information you have provided.

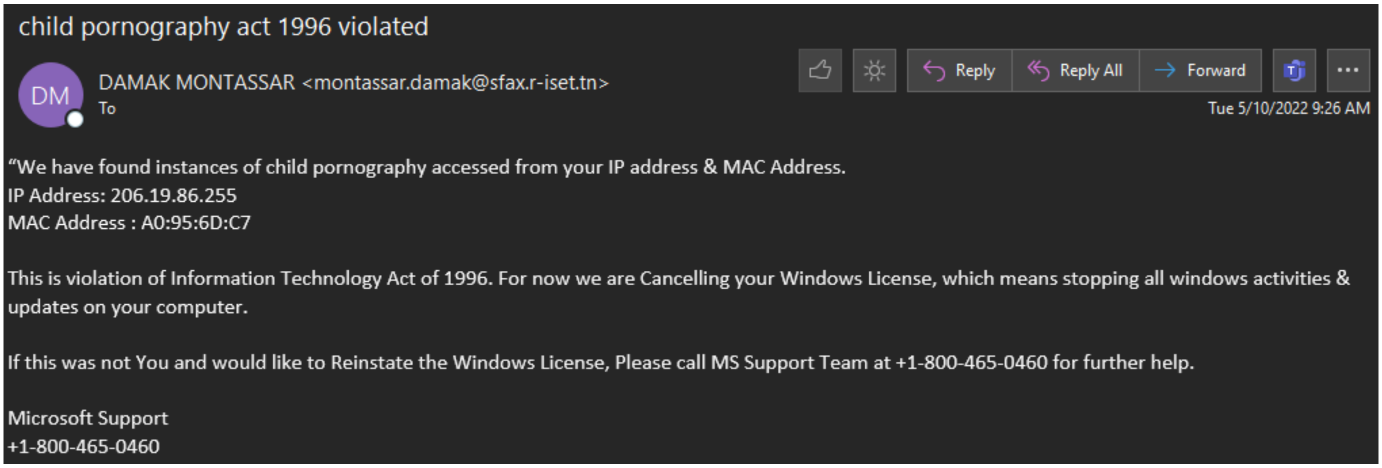
Your subscription will renew automatically in 1 month at the current rate of $53.61 a month. If you would like to cancel it, please call our customer support service at **+1(346) 201 46-93**.

With your purchase, you agree to out Terms & Conditions*. Please take a look at them on our website.

Best wishes,

Your Babbel Team

Another call center scam claimed that child pornography was accessed from the user's IP address, and they had therefore violated the Information Technology Act of 1996. This example included a fictitious IP and MAC address in an attempt to add authenticity.



child pornography act 1996 violated

DAMAK MONTASSAR <montassar.damak@sfax.r-iset.tn>
To

Tue 5/10/2022 9:26 AM

"We have found instances of child pornography accessed from your IP address & MAC Address.
IP Address: 206.19.86.255
MAC Address : A0:95:6D:C7

This is violation of Information Technology Act of 1996. For now we are Cancelling your Windows License, which means stopping all windows activities & updates on your computer.

If this was not You and would like to Reinstate the Windows License, Please call MS Support Team at +1-800-465-0460 for further help.

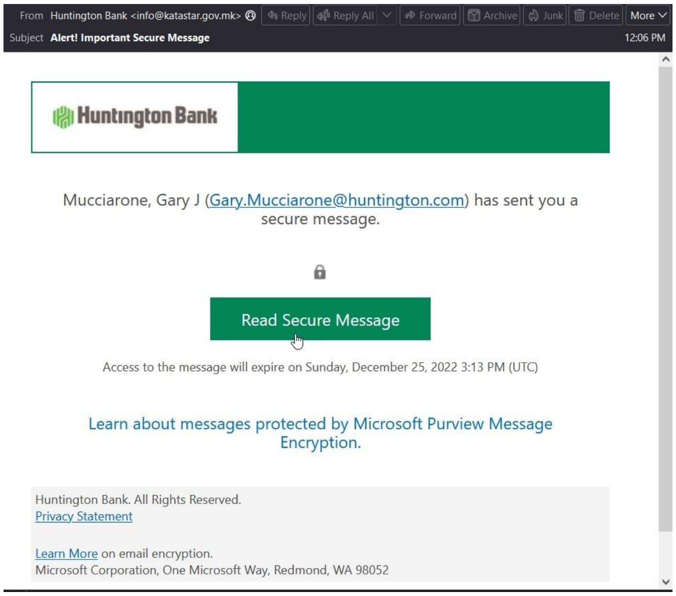
Microsoft Support
+1-800-465-0460

Clones

Since most attacks require the victim to believe that they're interacting with a legitimate service, attackers have increasingly tried cloning web pages and emails. This is often used in conjunction with other tactics like LotL and BEC.

The following example imitates a Microsoft-generated secure message from Huntington Bank. One noticeable feature is that it was sent from a North Macedonian government email account and server — an attempt to capitalize on their good reputation.

Once the user clicks on the link, they're directed to a webpage that contains a cloned Huntington online banking login designed to trick users into disclosing their account credentials.



From Huntington Bank <info@katastar.gov.mk>
Subject **Alert! Important Secure Message**
12:06 PM

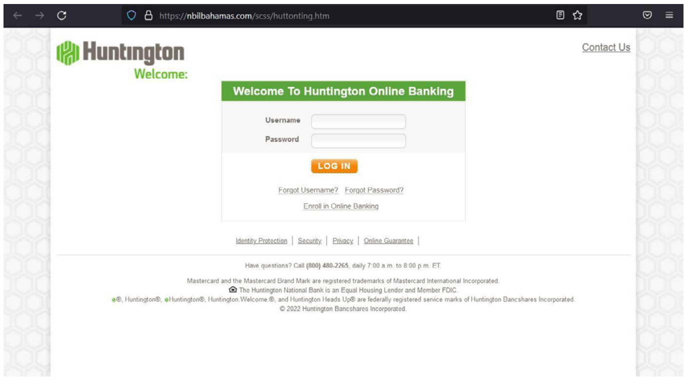
Mucciarone, Gary J (Gary.Mucciarone@huntington.com) has sent you a secure message.

Access to the message will expire on Sunday, December 25, 2022 3:13 PM (UTC)

Learn about messages protected by Microsoft Purview Message Encryption.

Huntington Bank. All Rights Reserved.
Privacy Statement

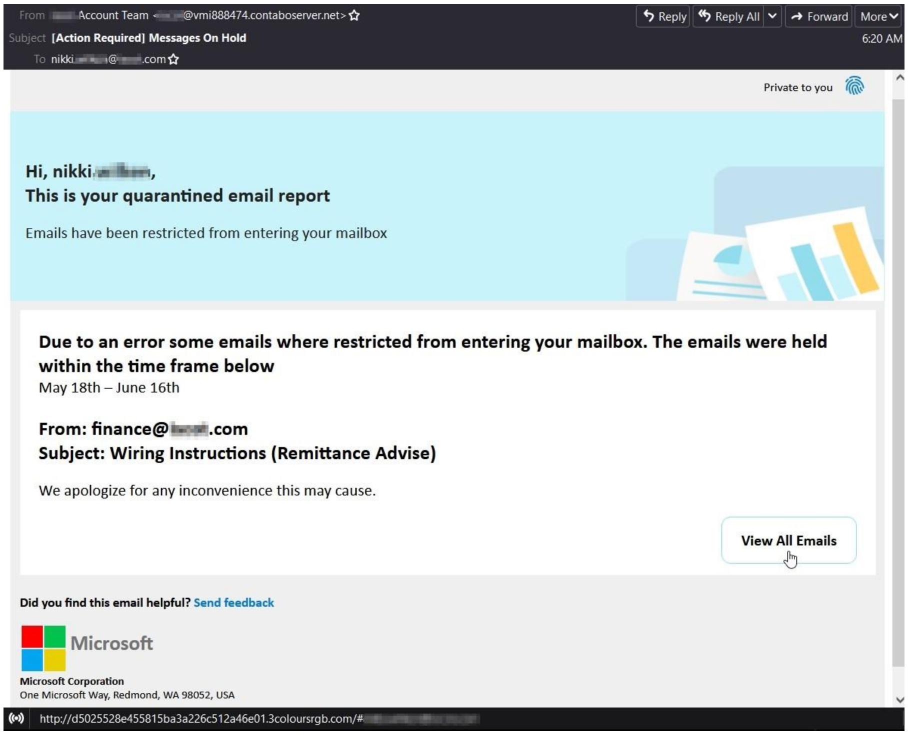
Learn More on email encryption.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052


Huntington
Welcome:
Contact Us
Welcome To Huntington Online Banking
Username
Password
LOG IN
Forgot Username? Forgot Password?
Enroll in Online Banking
Identity Protection | Security | Privacy | Online Guarantee |

https://nbilbahamas.com/scss/huttonting.htm

Have questions? Call (800) 480-2265, daily 7:00 a.m. to 8:00 p.m. ET.

Mastercard and the Mastercard Brand Mark are registered trademarks of Mastercard International Incorporated.
The Huntington National Bank is an Equal Housing Lender and Member FDIC.
®, Huntington®, Huntington®, Huntington.Welcome.®, and Huntington Heads Up® are federally registered service marks of Huntington Bancshares Incorporated.
© 2022 Huntington Bancshares Incorporated.



From [redacted]Account Team <[redacted]@vmi888474.contaboserver.net>
Subject [Action Required] Messages On Hold
To nikki.[redacted]@[redacted].com

6:20 AM

Hi, nikki.[redacted],
This is your quarantined email report

Emails have been restricted from entering your mailbox

Due to an error some emails where restricted from entering your mailbox. The emails were held within the time frame below
May 18th – June 16th

From: finance@[redacted].com
Subject: Wiring Instructions (Remittance Advise)

We apologize for any inconvenience this may cause.

Did you find this email helpful? Send feedback

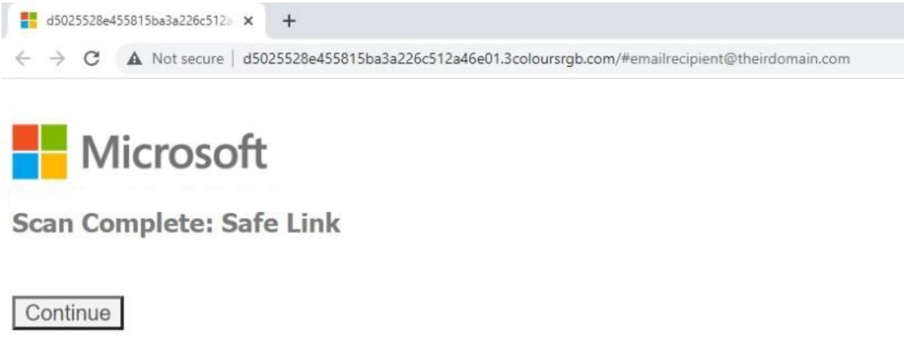
Microsoft

Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA

http://d5025528e455815ba3a226c512a46e01.3coloursrgb.com/#[redacted]

One of the more convincing cloned messages posed as a Microsoft quarantined email report. This threat actor commonly uses VPS servers for their phishing campaigns: this one originated from a Contabo server, a German cloud provider which offers both VPS and dedicated servers.

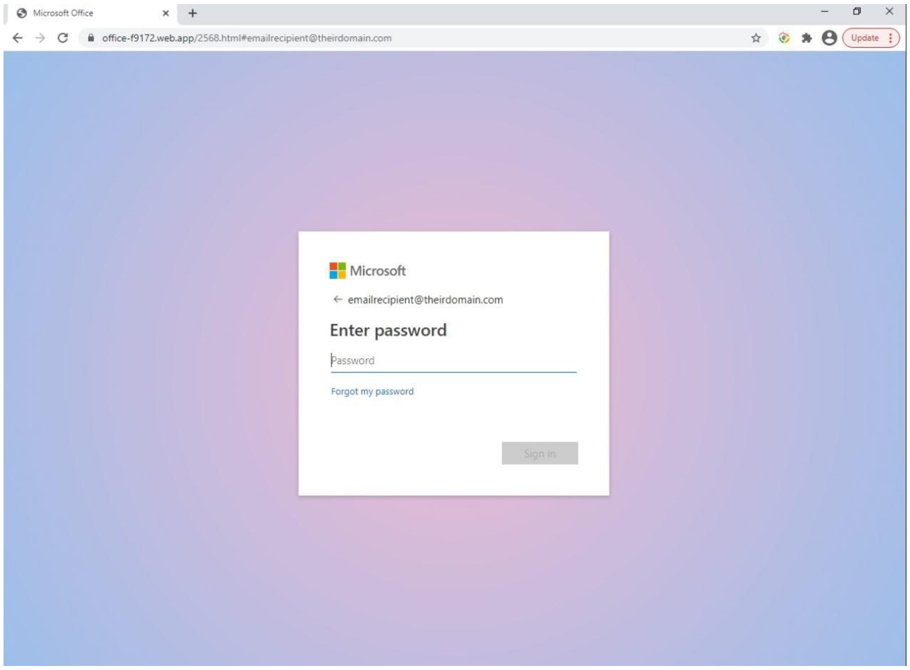
The message pretended to alert the recipient to a quarantined email with the subject “Wiring Instructions (Remittance Advise [sic])” and included a hyperlinked button marked “View All Emails.”



d5025528e455815ba3a226c512a46e01.3coloursrgb.com/#emailrecipient@theirdomain.com

Scan Complete: Safe Link

If the user clicked the button, they were directed to a similarly themed site that claimed to conduct a security scan. Of course, the fake scan declared the link to be safe.



office-f9172.web.app/2568.html#emailrecipient@theirdomain.com

← emailrecipient@theirdomain.com

Enter password

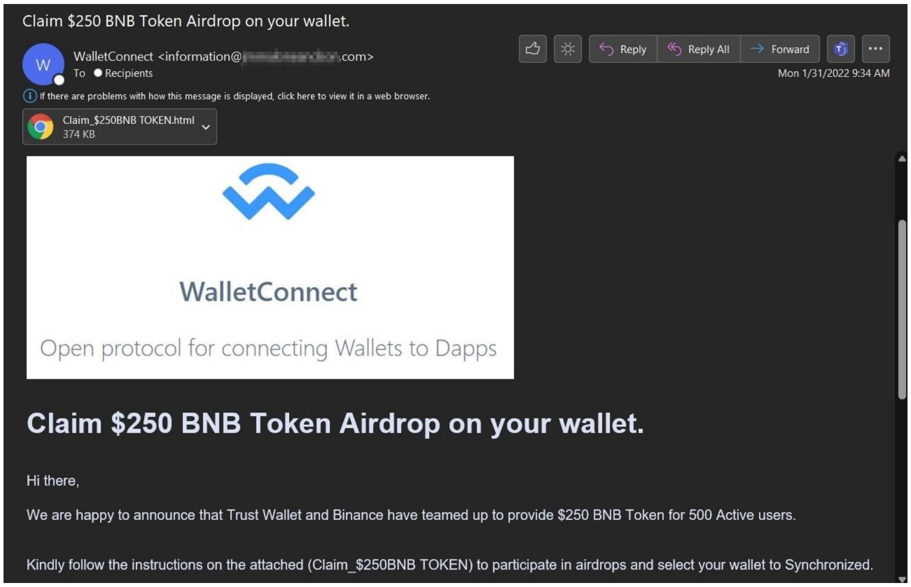
After clicking the “Continue” button, the user would be sent to a Microsoft-themed credential-harvesting site located on Google Firebase (web[.]app). This is one of the platforms most commonly used for phishing attacks.

Cryptocurrency • Crypto-based Phishing • Cryto Scams • Bitcoin • Ethereum • NFTs

Cryptocurrency Scams

Cryptocurrency Scams

Unsurprisingly, cryptocurrency-related phishing scams tend to increase in popularity when crypto prices are rising. The following example purported to be WalletConnect, offering users a way to connect their wallet to decentralized apps. The message instructed the recipient to open an [.]html attachment in order to claim $250 in Binance Coin (BNB) and synchronize their wallet.



Claim $250 BNB Token Airdrop on your wallet.

WalletConnect <information@[redacted].com>
To ● Recipients
Mon 1/31/2022 9:34 AM

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

Claim_$250BNB TOKEN.html
374 KB

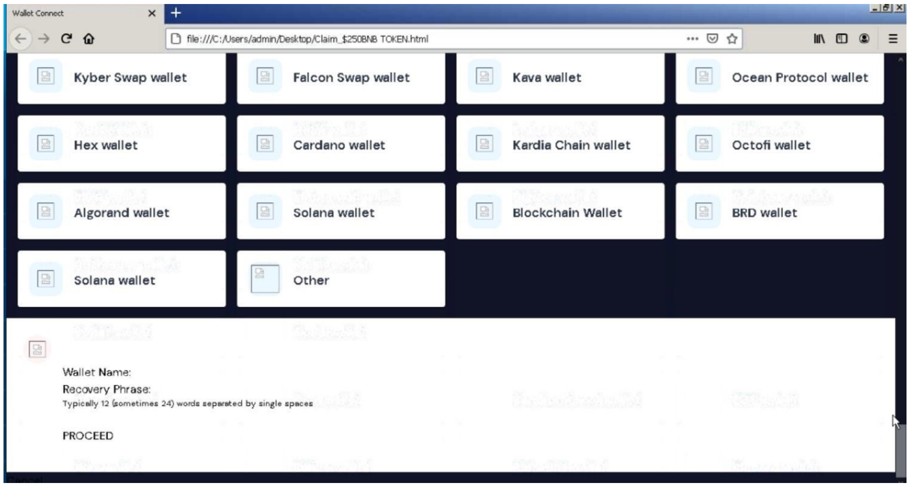
Claim $250 BNB Token Airdrop on your wallet.

Hi there,

We are happy to announce that Trust Wallet and Binance have teamed up to provide $250 BNB Token for 500 Active users.

Kindly follow the instructions on the attached (Claim_$250BNB TOKEN) to participate in airdrops and select your wallet to Synchronized.

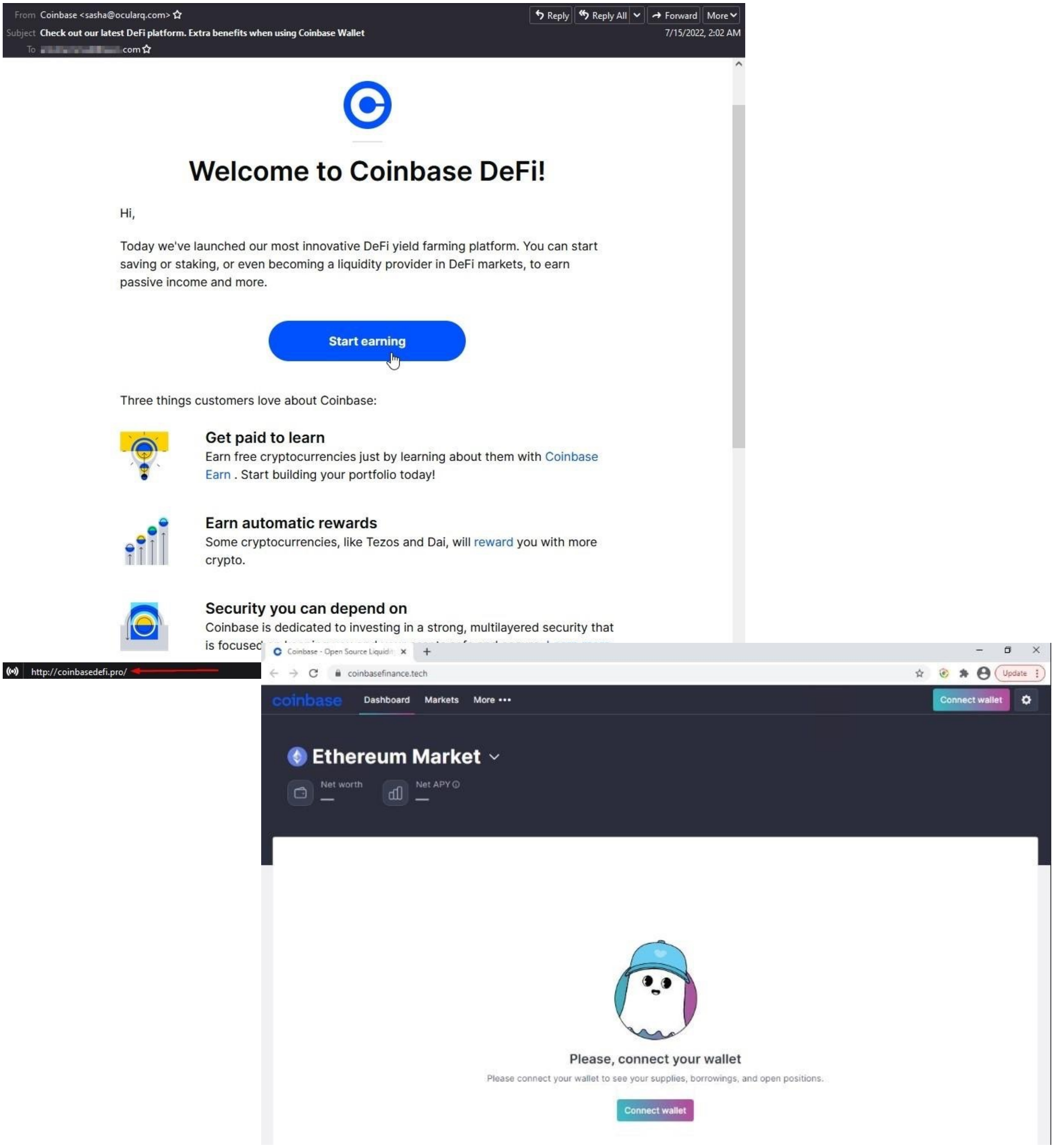
If the recipient opened the attachment, they were presented with a selection of different crypto wallets they could supposedly synchronize using WalletConnect. At the bottom of the file, there's a space for the user's wallet name and recovery phrase. Also known as a seed phrase, the recovery phrase is a private key for the wallet that uses a series of words rather than numbers. Turning it over would give the attacker control of the wallet.



file:///C:/Users/admin/Desktop/Claim_$250BNB TOKEN.html

Wallet Name:
Recovery Phrase:
Typically 12 (sometimes 24) words separated by single spaces

In another example, the attacker posed as popular crypto exchange platform Coinbase and attempted to dupe users into granting them access to their crypto holdings. This campaign used a Coinbase DeFi yield farming email as the lure. However, the link in the email led to the illegitimate site coinbasedefi[.]pro. If the user clicked the URL, they were redirected to coinbasefinance[.]tech — a cloned copy of the real Coinbase site — which prompted the user to connect their wallet. From there, the attacker would be able to transfer the holdings to their own wallet.



From Coinbase <sasha@ocularq.com>

Subject Check out our latest DeFi platform. Extra benefits when using Coinbase Wallet

To [redacted]com

7/15/2022, 2:02 AM

Welcome to Coinbase DeFi!

Hi,

Today we've launched our most innovative DeFi yield farming platform. You can start saving or staking, or even becoming a liquidity provider in DeFi markets, to earn passive income and more.

Three things customers love about Coinbase:

Get paid to learn
Earn free cryptocurrencies just by learning about them with Coinbase Earn . Start building your portfolio today!

Earn automatic rewards
Some cryptocurrencies, like Tezos and Dai, will reward you with more crypto.

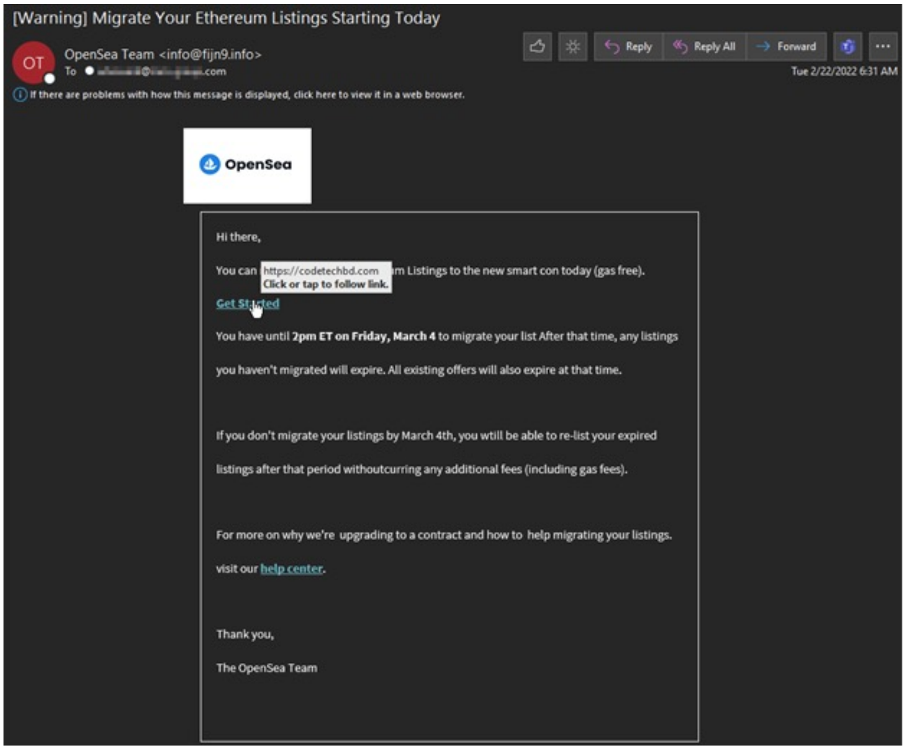
Security you can depend on
Coinbase is dedicated to investing in a strong, multilayered security that is focused

http://coinbasedefi.pro/

Please, connect your wallet

Please connect your wallet to see your supplies, borrowings, and open positions.

One crypto scam took advantage of NFT marketplace OpenSea's contract migrations and upgrade announcement. During this migration — between February 18 to 25, 2022 — these attackers swindled millions of dollars in Ethereum by spoofing OpenSea's migration announcement email.



[Warning] Migrate Your Ethereum Listings Starting Today

OpenSea Team <info@fijn9.info>
To [redacted].com
Tue 2/22/2022 6:31 AM

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

Hi there,

You can https://codetechbd.com Click or tap to follow link. m Listings to the new smart con today (gas free).

Get Started

You have until **2pm ET on Friday, March 4** to migrate your list After that time, any listings you haven't migrated will expire. All existing offers will also expire at that time.

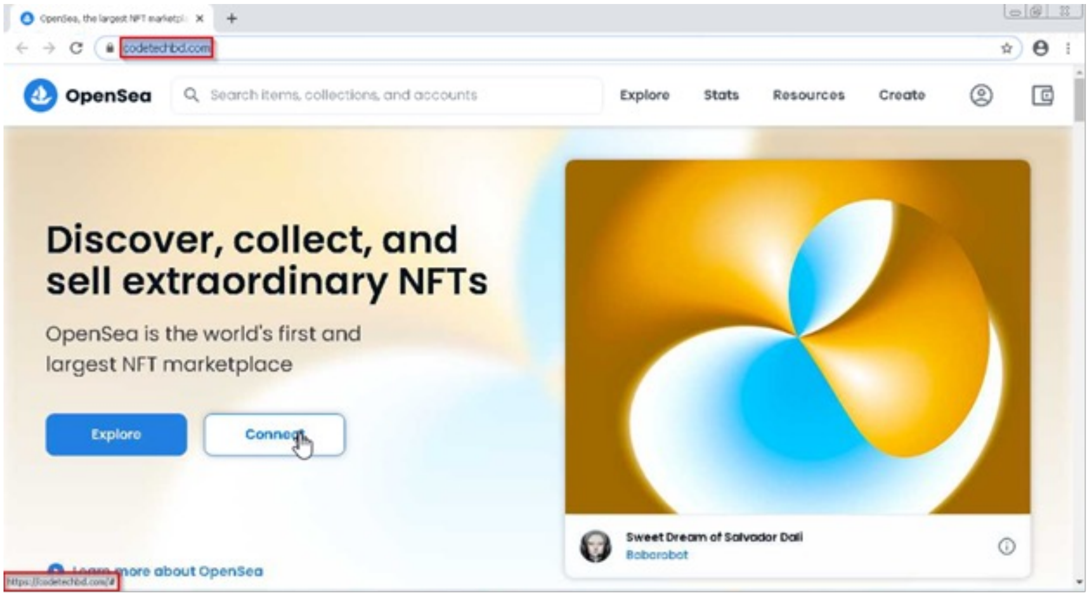
If you don't migrate your listings by March 4th, you wtill be able to re-list your expired listings after that period withoutcurring any additional fees (including gas fees).

For more on why we're upgrading to a contract and how to help migrating your listings. visit our help center.

Thank you,

The OpenSea Team

Recipients who clicked "Get Started" were taken to a clone of OpenSea's home page, where they were prompted with two buttons labeled "Explore" and "Connect." These both opened a prompt asking the victim to authenticate their crypto wallet, connecting it to the attacker.

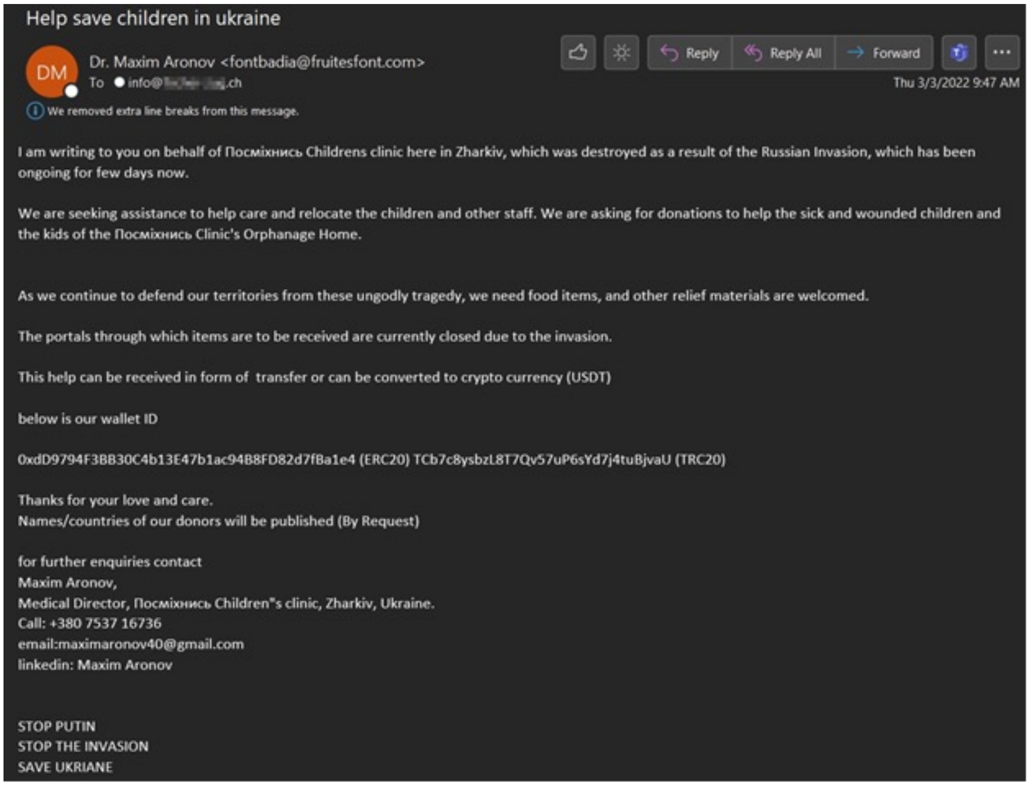


Discover, collect, and sell extraordinary NFTs

OpenSea is the world's first and largest NFT marketplace

Crypto-Based Phishing Attacks Leveraging Current Events

As the OpenSea example shows, scammers always attempt to monetize major news and world events. Russia's invasion of Ukraine was no exception. The following examples show attackers attempting to solicit Bitcoin or Ethereum "donations" they claim will go to help victims of the war. In this first example, the sender attempts to masquerade as a children's clinic to obtain Ethereum.



Help save children in ukraine

Dr. Maxim Aronov <fontbadia@fruitesfont.com>
To info@[redacted].ch
Thu 3/3/2022 9:47 AM

I am writing to you on behalf of Посміхнись Childrens clinic here in Zharkiv, which was destroyed as a result of the Russian Invasion, which has been ongoing for few days now.

We are seeking assistance to help care and relocate the children and other staff. We are asking for donations to help the sick and wounded children and the kids of the Посміхнись Clinic's Orphanage Home.

As we continue to defend our territories from these ungodly tragedy, we need food items, and other relief materials are welcomed.

The portals through which items are to be received are currently closed due to the invasion.

This help can be received in form of transfer or can be converted to crypto currency (USDT)

below is our wallet ID

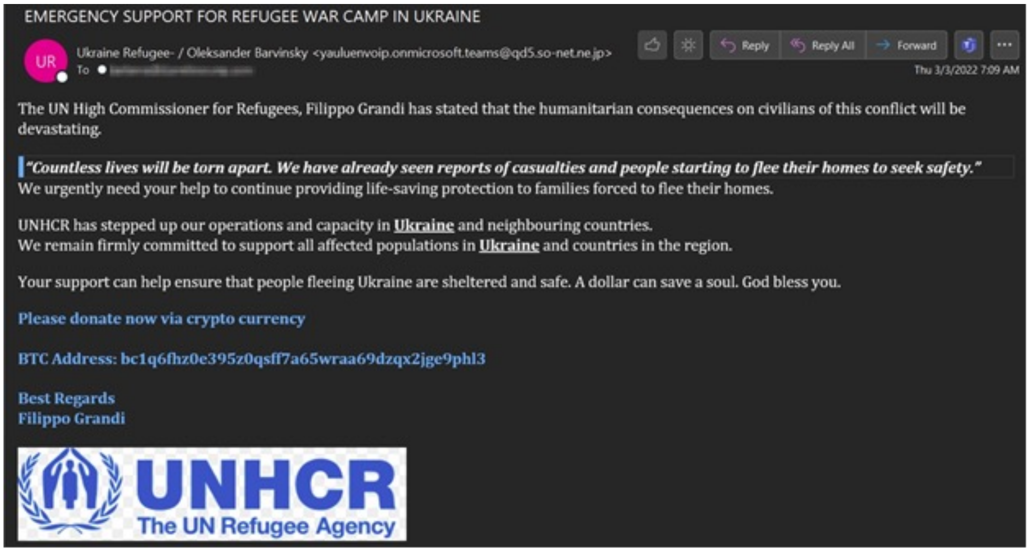
0xdD9794F3BB30C4b13E47b1ac94B8FD82d7fBa1e4 (ERC20) TCb7c8ysbzL8T7Qv57uP6sYd7j4tuBjvaU (TRC20)

Thanks for your love and care.
Names/countries of our donors will be published (By Request)

for further enquiries contact
Maxim Aronov,
Medical Director, Посміхнись Children"s clinic, Zharkiv, Ukraine.
Call: +380 7537 16736
email:maximaronov40@gmail.com
linkedin: Maxim Aronov

STOP PUTIN
STOP THE INVASION
SAVE UKRIANE

Another attacker posed as the United Nations High Commissioner for Refugees (UNHCR) — a legitimate agency. It asked for emergency Bitcoin donations to support Ukrainian refugees.



EMERGENCY SUPPORT FOR REFUGEE WAR CAMP IN UKRAINE

Ukraine Refugee- / Oleksander Barvinsky <yauluenvoip.onmicrosoft.teams@qd5.so-net.ne.jp>
To [redacted]
Thu 3/3/2022 7:09 AM

The UN High Commissioner for Refugees, Filippo Grandi has stated that the humanitarian consequences on civilians of this conflict will be devastating.

> ***"Countless lives will be torn apart. We have already seen reports of casualties and people starting to flee their homes to seek safety."***

We urgently need your help to continue providing life-saving protection to families forced to flee their homes.

UNHCR has stepped up our operations and capacity in **Ukraine** and neighbouring countries.
We remain firmly committed to support all affected populations in **Ukraine** and countries in the region.

Your support can help ensure that people fleeing Ukraine are sheltered and safe. A dollar can save a soul. God bless you.

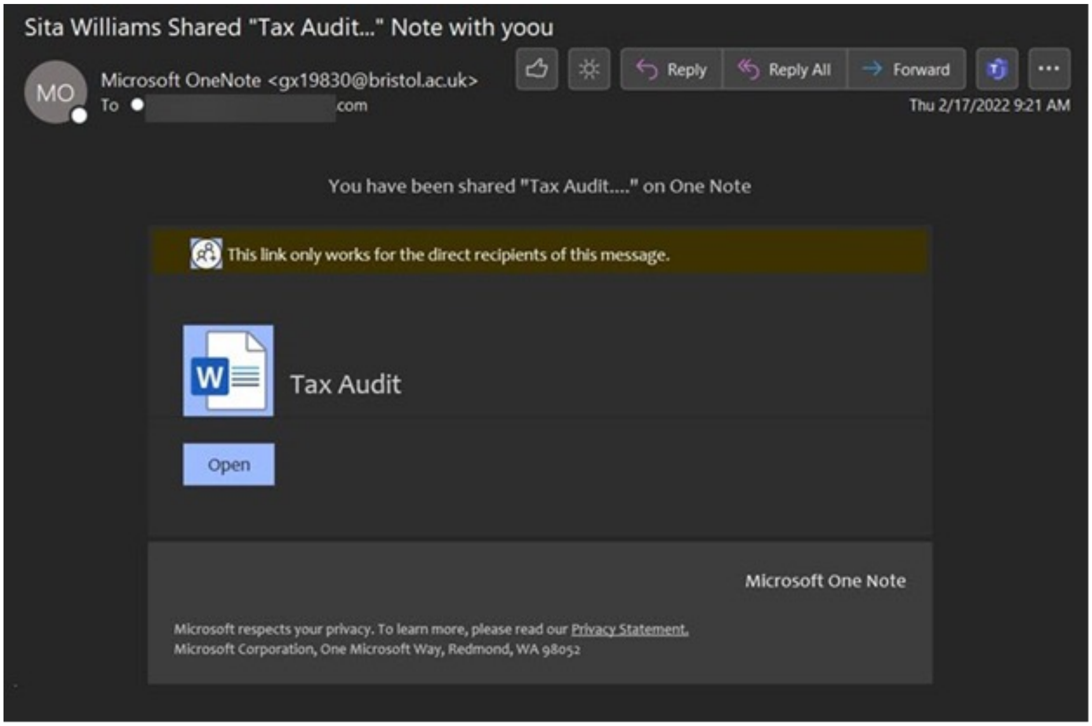
Please donate now via crypto currency

BTC Address: bc1q6fhz0e395z0qsff7a65wraa69dzqx2jge9phl3

Best Regards
Filippo Grandi

Tax-Themed Phishing

In addition to developing news stories, attackers also weaponize annual events. The weeks leading up to the U.S. tax-filing deadline — on or within a few days of April 15 — always see a spike in phishing attacks, and 2022 was no different. One attacker sent a fake Microsoft OneNote document with a tax audit theme.



Sita Williams Shared "Tax Audit..." Note with yoou

Microsoft OneNote <gx19830@bristol.ac.uk>
To [redacted].com

Thu 2/17/2022 9:21 AM

You have been shared "Tax Audit...." on One Note

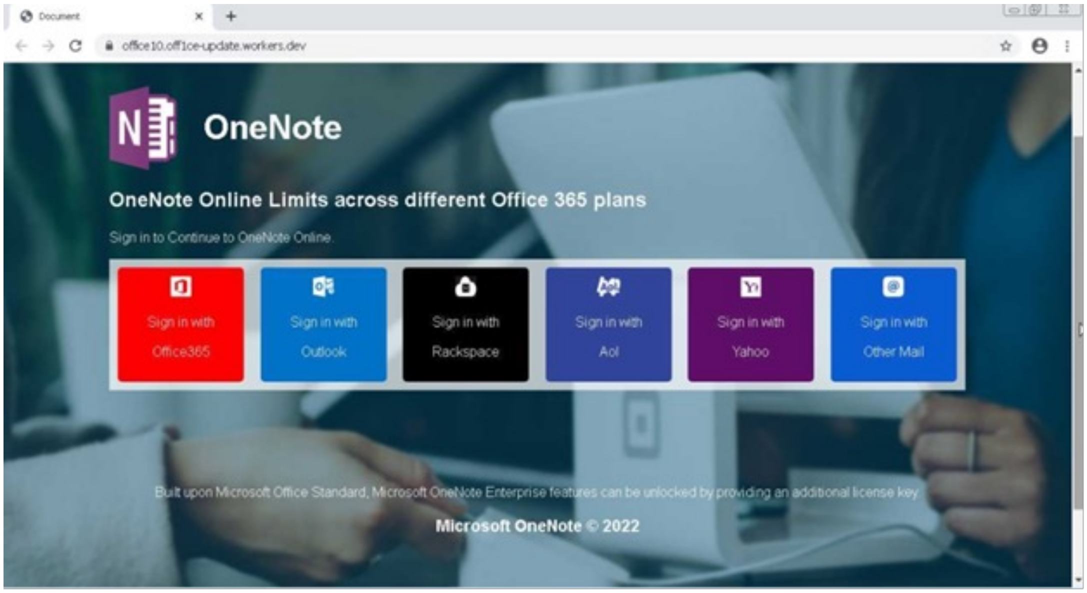
This link only works for the direct recipients of this message.

Tax Audit

Microsoft One Note

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Upon clicking, the user would be redirected to a phishing site soliciting credentials hosted on Cloudflare's (workers[.]dev) service. This service allows for up to 100,000 free requests per day along with a subdomain, such as the one in this example, office10.off1ce-update.workers[.]dev.



office10.off1ce-update.workers.dev

OneNote

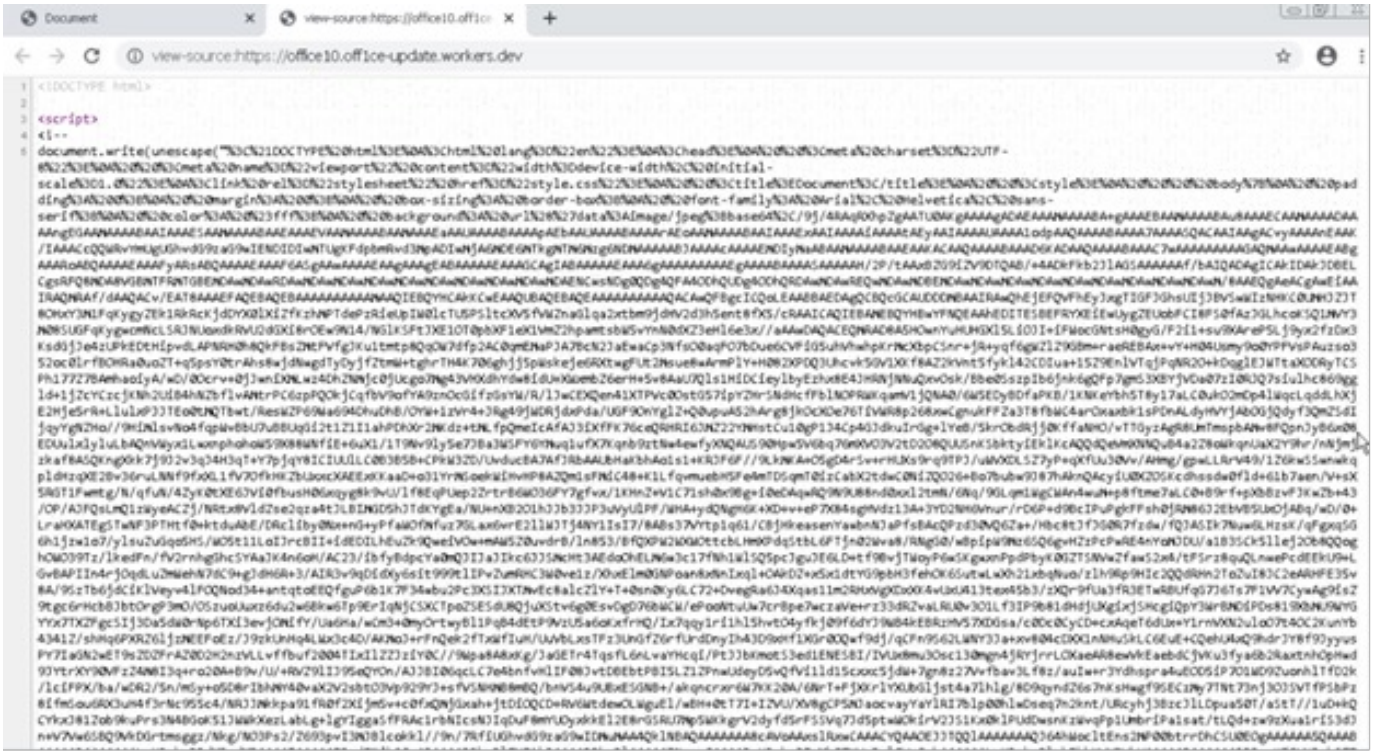
OneNote Online Limits across different Office 365 plans

Sign in to Continue to OneNote Online.

Built upon Microsoft Office Standard, Microsoft OneNote Enterprise features can be unlocked by providing an additional license key.

Microsoft OneNote © 2022

Looking at the source code, we can see that this attacker used a combination of URL encoding and base64 for their JavaScript in an attempt at obfuscation — hiding from web bots and scanners that might detect the malicious script in plain text.



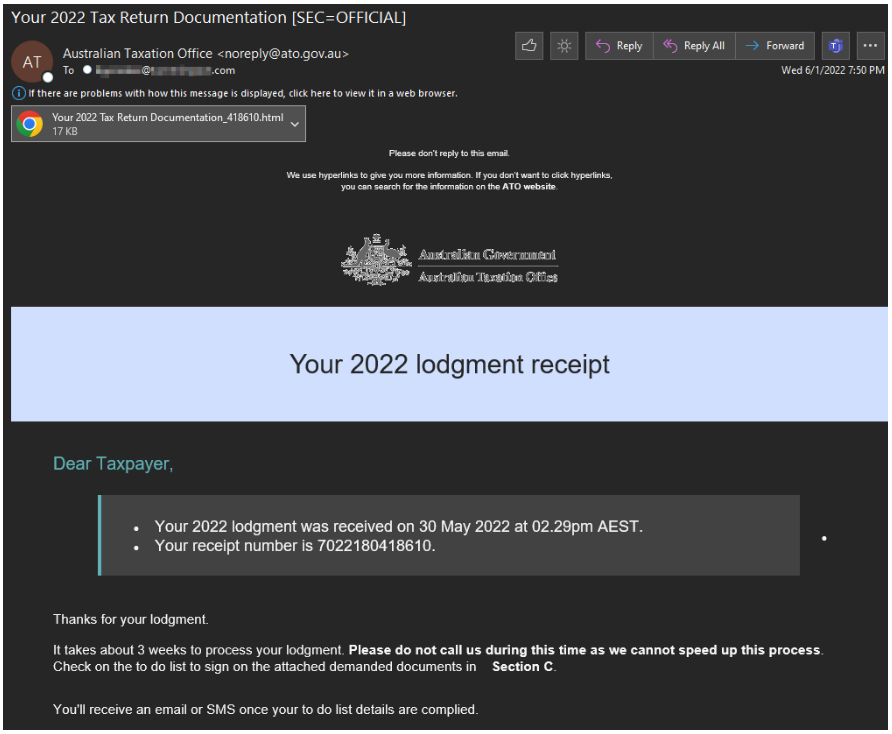
Document
view-source:https://office10.offic
view-source:https://office10.off1ce-update.workers.dev

```
<!DOCTYPE html>

<script>
<!--
document.write(unescape("%3C%21DOCTYPE%20html%3E%0A%3Chtml%20lang%3D%22en%22%3E%0A%3Chead%3E%0A%20%20%3Cmeta%20charset%3D%22UTF-
8%22%3E%0A%20%20%3Cmeta%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-
scale%3D1.0%22%3E%0A%3Clink%20rel%3D%22stylesheet%22%20href%3D%22style.css%22%3E%0A%20%20%3Ctitle%3EDocument%3C/title%3E%0A%20%20%3Cstyle%3E%0A%20%20%20%20body%7B%0A%20%20pad
ding%3A%200%3B%0A%20%20margin%3A%200%3B%0A%20%20box-sizing%3A%20border-box%3B%0A%20%20font-family%3A%20Arial%2C%20Helvetica%2C%20sans-
serif%3B%0A%20%20color%3A%20%23fff%3B%0A%20%20background%3A%20url%28%27data%3Aimage/jpeg%3Bbase64%2C/9j/4AAQ
```

[illegible]

We occasionally capture malicious messages originating from and/or abusing government networking infrastructure. For example, we encountered an Australian phishing campaign that actually originated from the official Australian Taxation Office (ATO) servers. All the links in the email led to the official ato.gov.au website — but an attached HTML file led to a credential-harvesting page with a Microsoft-branded login.



Your 2022 Tax Return Documentation [SEC=OFFICIAL]

AT Australian Taxation Office <noreply@ato.gov.au>
To [redacted]

Wed 6/1/2022 7:50 PM

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

Your 2022 Tax Return Documentation_418610.html
17 KB

Please don't reply to this email.

We use hyperlinks to give you more information. If you don't want to click hyperlinks, you can search for the information on the **ATO website**.

Australian Government
Australian Taxation Office

Your 2022 lodgment receipt

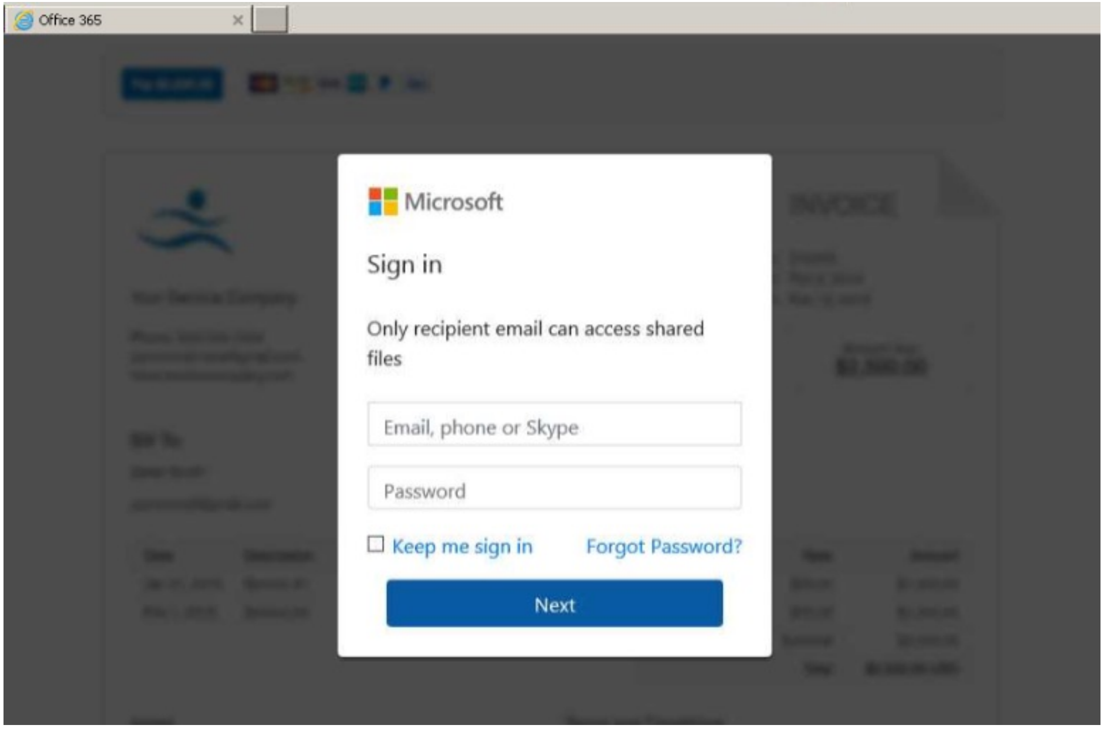
Dear Taxpayer,

- Your 2022 lodgment was received on 30 May 2022 at 02.29pm AEST.
- Your receipt number is 7022180418610.

Thanks for your lodgment.

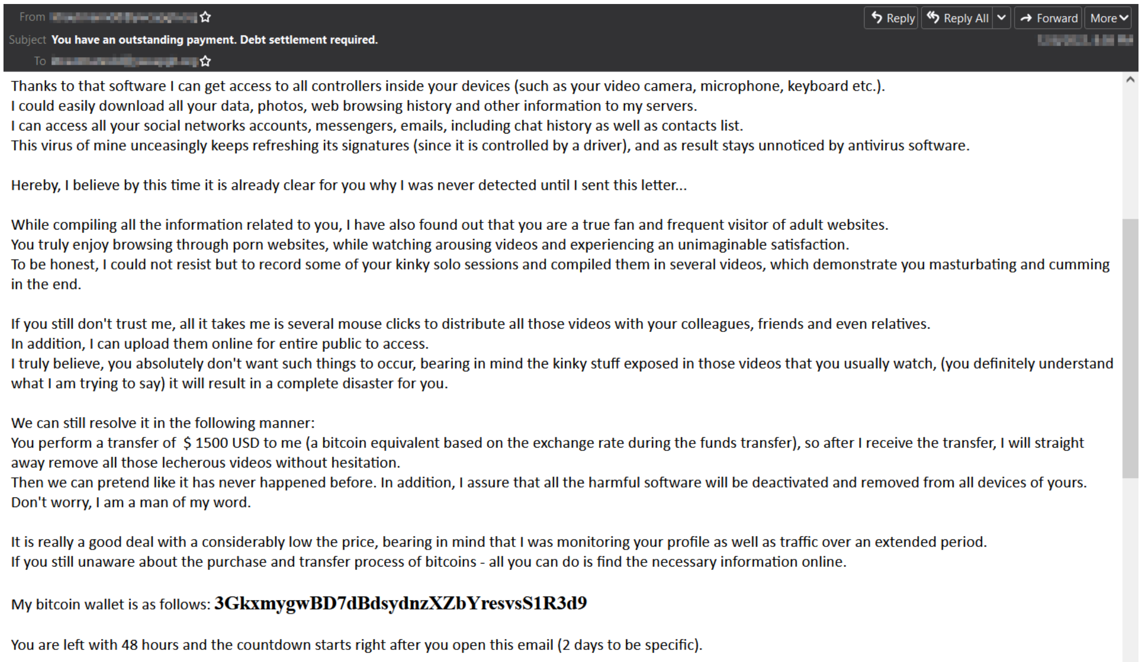
It takes about 3 weeks to process your lodgment. **Please do not call us during this time as we cannot speed up this process.**
Check on the to do list to sign on the attached demanded documents in **Section C**.

You'll receive an email or SMS once your to do list details are complied.



Sextortion

The portmanteau “sextortion” refers to attacks in which perpetrators threaten to publish explicit images or videos of their victim unless the victim sends money or more sexual content. Although these phishing attacks take place across many platforms, email-based examples typically involve attackers claiming to have installed malware on the victim’s system that recorded them through their own webcam. They usually demand payment in Bitcoin.



From [redacted]
Subject **You have an outstanding payment. Debt settlement required.**
To [redacted]
[redacted]

Thanks to that software I can get access to all controllers inside your devices (such as your video camera, microphone, keyboard etc.).
I could easily download all your data, photos, web browsing history and other information to my servers.
I can access all your social networks accounts, messengers, emails, including chat history as well as contacts list.
This virus of mine unceasingly keeps refreshing its signatures (since it is controlled by a driver), and as result stays unnoticed by antivirus software.

Hereby, I believe by this time it is already clear for you why I was never detected until I sent this letter...

While compiling all the information related to you, I have also found out that you are a true fan and frequent visitor of adult websites.
You truly enjoy browsing through porn websites, while watching arousing videos and experiencing an unimaginable satisfaction.
To be honest, I could not resist but to record some of your kinky solo sessions and compiled them in several videos, which demonstrate you masturbating and cumming in the end.

If you still don't trust me, all it takes me is several mouse clicks to distribute all those videos with your colleagues, friends and even relatives.
In addition, I can upload them online for entire public to access.
I truly believe, you absolutely don't want such things to occur, bearing in mind the kinky stuff exposed in those videos that you usually watch, (you definitely understand what I am trying to say) it will result in a complete disaster for you.

We can still resolve it in the following manner:
You perform a transfer of $ 1500 USD to me (a bitcoin equivalent based on the exchange rate during the funds transfer), so after I receive the transfer, I will straight away remove all those lecherous videos without hesitation.
Then we can pretend like it has never happened before. In addition, I assure that all the harmful software will be deactivated and removed from all devices of yours.
Don't worry, I am a man of my word.

It is really a good deal with a considerably low the price, bearing in mind that I was monitoring your profile as well as traffic over an extended period.
If you still unaware about the purchase and transfer process of bitcoins - all you can do is find the necessary information online.

My bitcoin wallet is as follows: **3GkxmygwBD7dBdsydnzXZbYresvsS1R3d9**

You are left with 48 hours and the countdown starts right after you open this email (2 days to be specific).

Email-based Threats • Remote Access Trojan • Notorius Malwares • Emotet • Qakbot/Qbot • IcedID

Malware

Top Malware Threats

In 2022, our Advanced Email Threat Protection detected and quarantined over 165 million emails with malware attachments — a 3.41% increase over 2021. Volumes peaked early in the year, before Microsoft implemented stricter default settings in April, a move that pushed more attackers to shift to URL-based techniques.

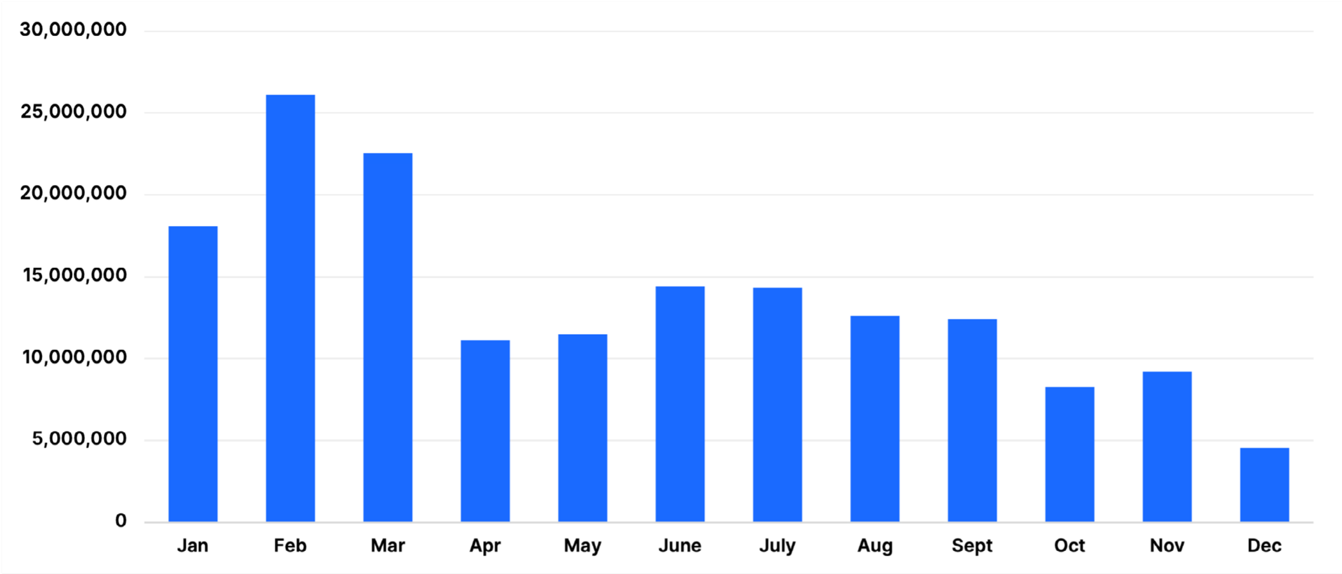


Figure 4: Attached malware

As of 2021, the United States remained the top origin location for email-based malware attacks.

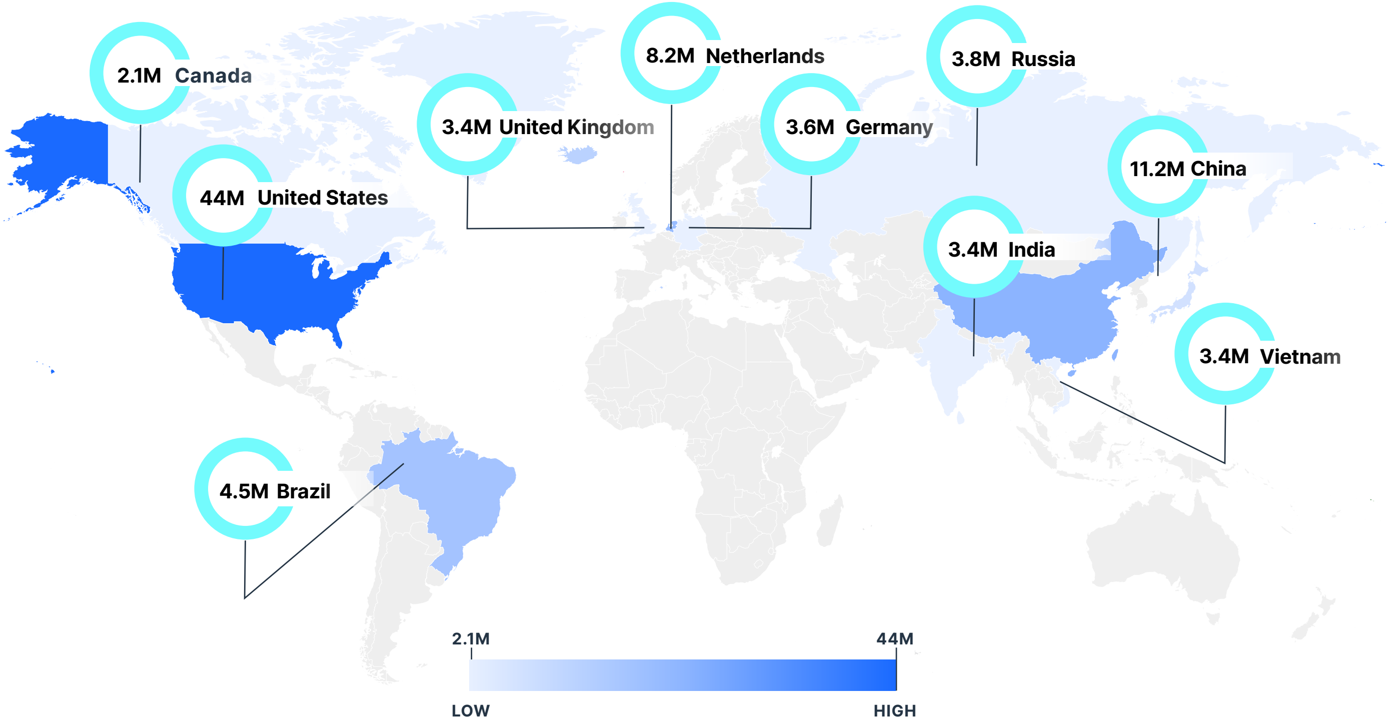


Figure 5: Top 10 malware attack country of origin (in millions)

In 2021, .xls (Excel spreadsheet) files were by far the most prevalent file type used for malware delivery. However, .xls use declined significantly throughout 2022, while the combined use of .htm and .html attachments increased by double digits over the prior year. In 2022, archive files were also popular mediums for malware, with usage increasing roughly 80% over 2021. The content of those archives varied greatly, but there was a substantial uptick of virtual disc file types within the ZIP archives, such as .img & .iso.

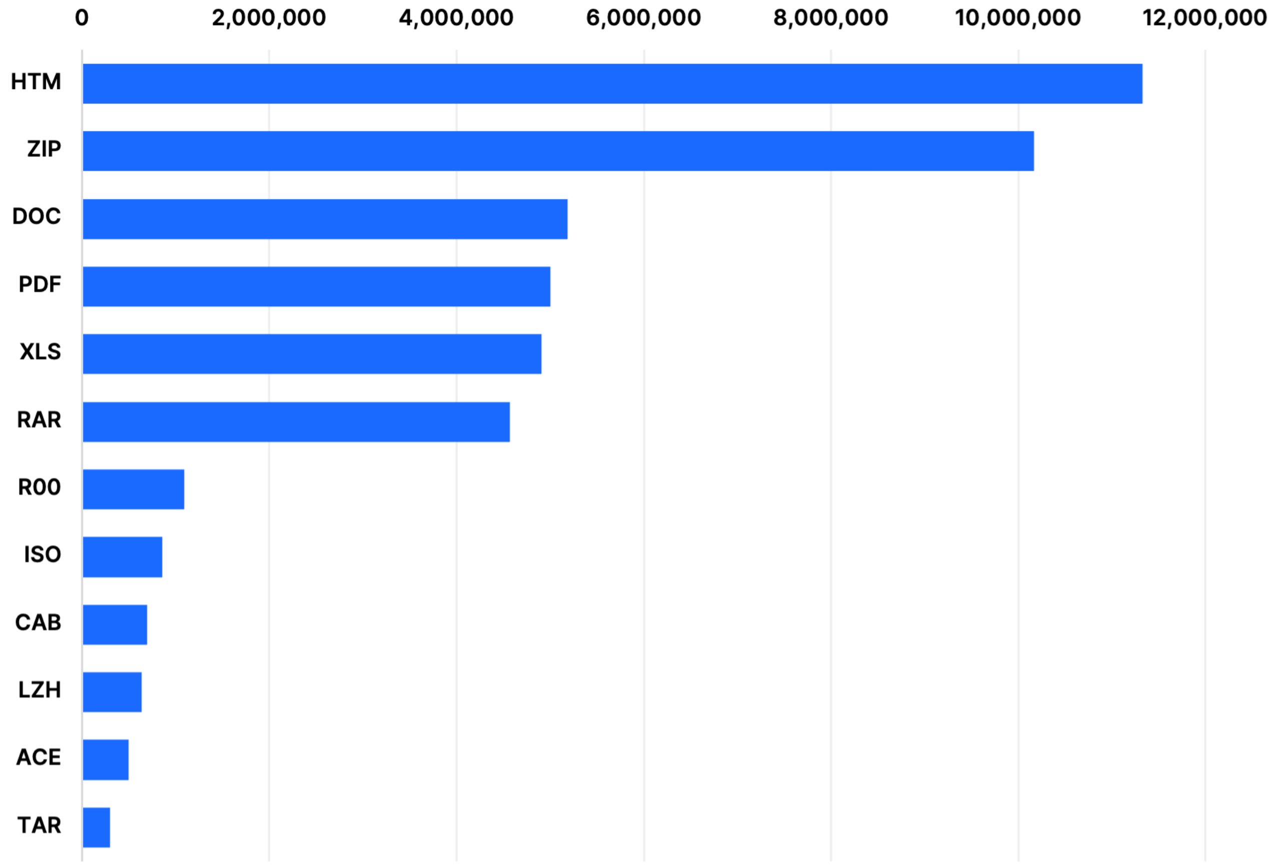
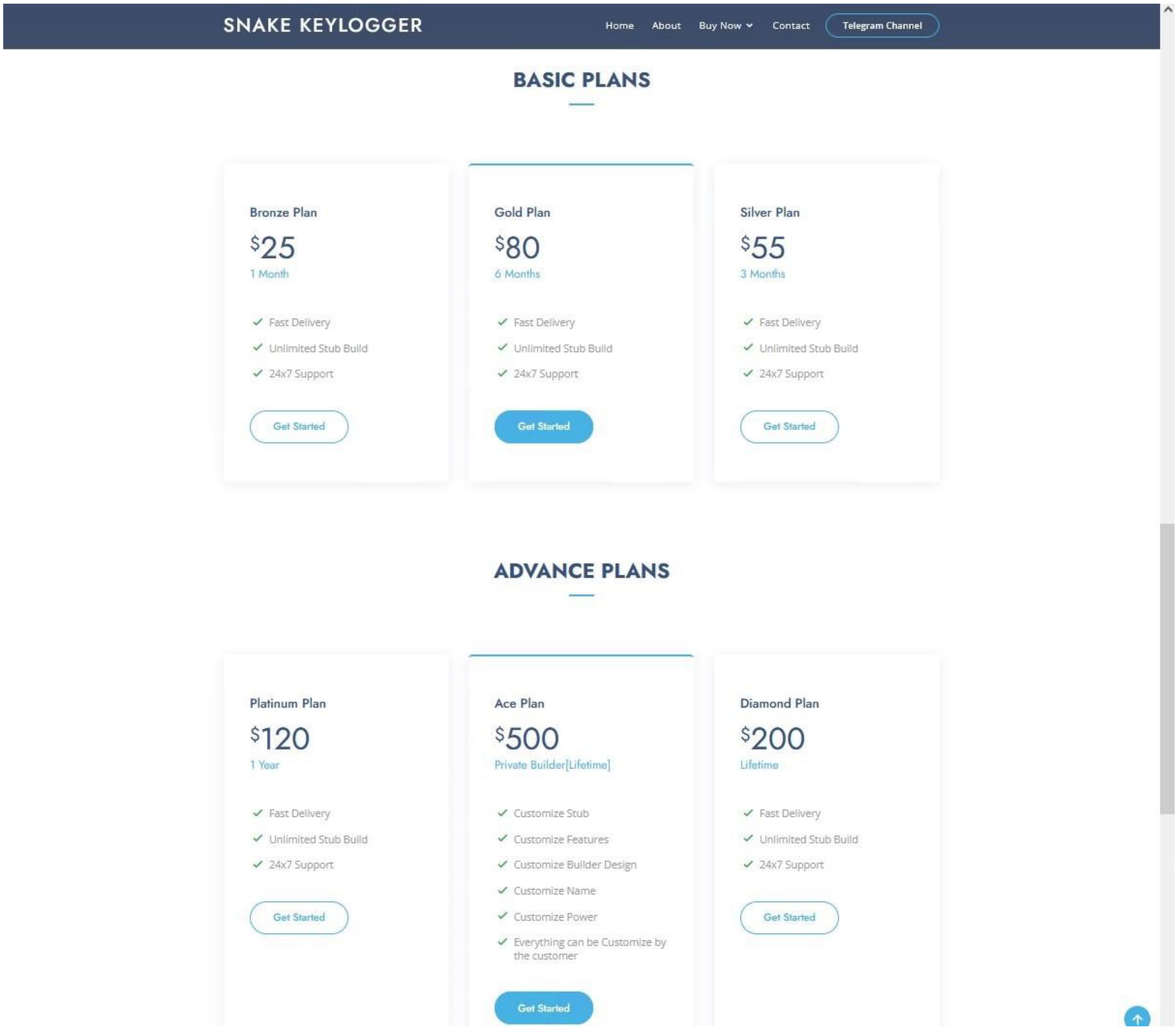


Figure 6: Malware attachment by file type

Next, we will look at some of the most popular malware families we observed throughout the year and some techniques malicious actors employed to manipulate end users into facilitating their attacks.

Remote Access Trojan (RAT) Attacks

As in previous years, the most commonly used malware attachments in 2022 were readily available malware-as-a-service (MaaS) products such as remote access Trojans (RATs) and info-stealers. Recognizable names included Agent Tesla, Formbook, Ave Maria (Warzone), ASYNCRAT, NJRAT, Adwind, Quasar, Remcos, and Nanocore2. The image below shows different MaaS plan options for the Snake Keylogger, with licenses available for varying price points based on how long they last (ranging from one month to a lifetime) and the services and features included.



BASIC PLANS

Bronze Plan
$25
1 Month
- ✓ Fast Delivery
- ✓ Unlimited Stub Build
- ✓ 24x7 Support

Gold Plan
$80
6 Months
- ✓ Fast Delivery
- ✓ Unlimited Stub Build
- ✓ 24x7 Support

Silver Plan
$55
3 Months
- ✓ Fast Delivery
- ✓ Unlimited Stub Build
- ✓ 24x7 Support

ADVANCE PLANS

Platinum Plan
$120
1 Year
- ✓ Fast Delivery
- ✓ Unlimited Stub Build
- ✓ 24x7 Support

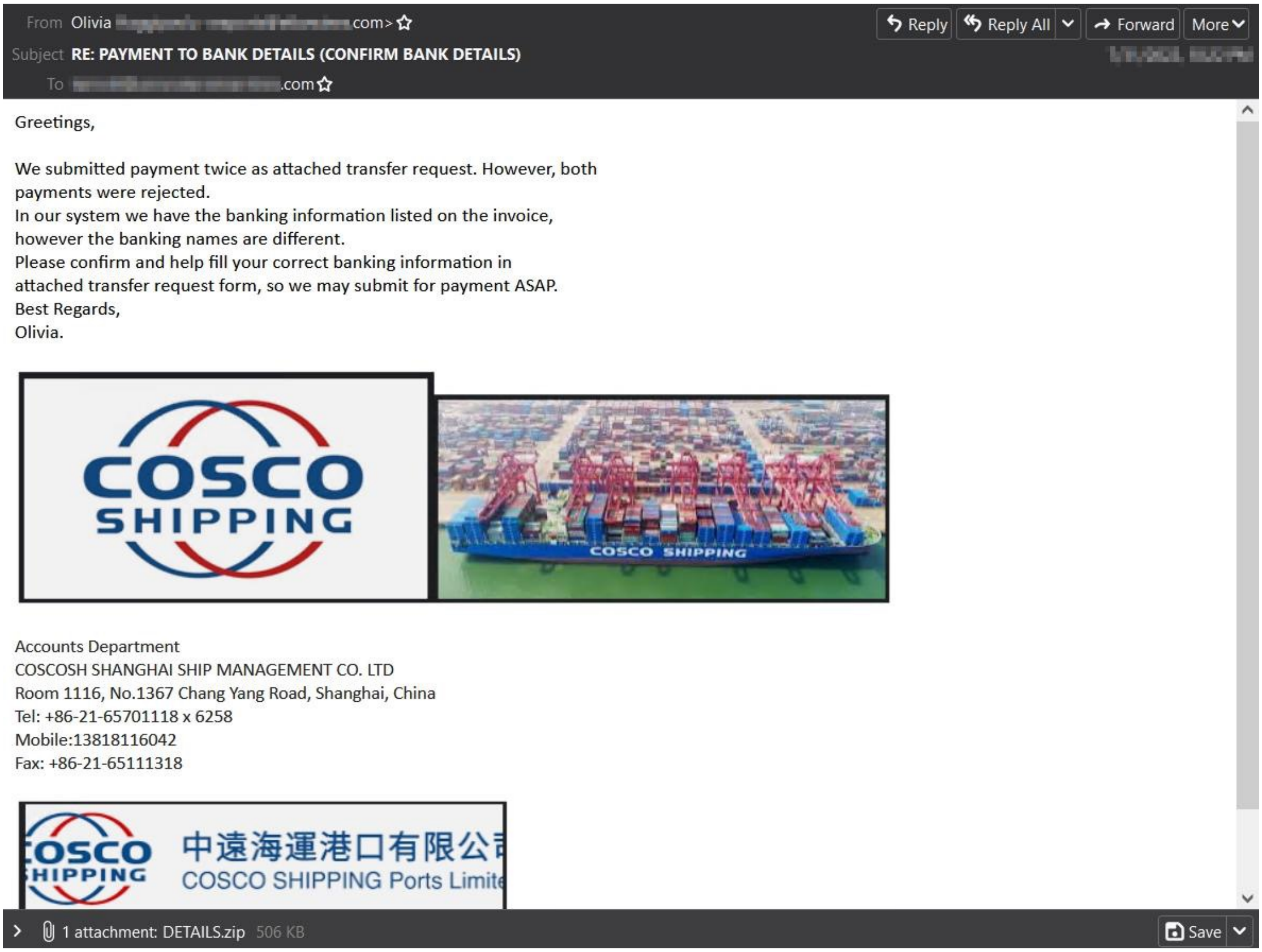
Ace Plan
$500
Private Builder[Lifetime]
- ✓ Customize Stub
- ✓ Customize Features
- ✓ Customize Builder Design
- ✓ Customize Name
- ✓ Customize Power
- ✓ Everything can be Customize by the customer

Diamond Plan
$200
Lifetime
- ✓ Fast Delivery
- ✓ Unlimited Stub Build
- ✓ 24x7 Support

Examples of Email-Based Malware Attacks

Example A: Imitating Cosco Shipping

We quarantined a large number of RAT attacks targeting the shipping industry in 2022. In one incident, the attackers attempted to imitate Cosco Shipping. They created an email stating that payments submitted for a shipment had been rejected and urging the recipient to confirm the correct banking information in the attached transfer request form. However, the attached .zip archive file contained only an executable file that initiated the Formbook infection chain.



From Olivia [redacted].com>

Subject **RE: PAYMENT TO BANK DETAILS (CONFIRM BANK DETAILS)**

[redacted]

To [redacted].com

Greetings,

We submitted payment twice as attached transfer request. However, both
payments were rejected.
In our system we have the banking information listed on the invoice,
however the banking names are different.
Please confirm and help fill your correct banking information in
attached transfer request form, so we may submit for payment ASAP.
Best Regards,
Olivia.

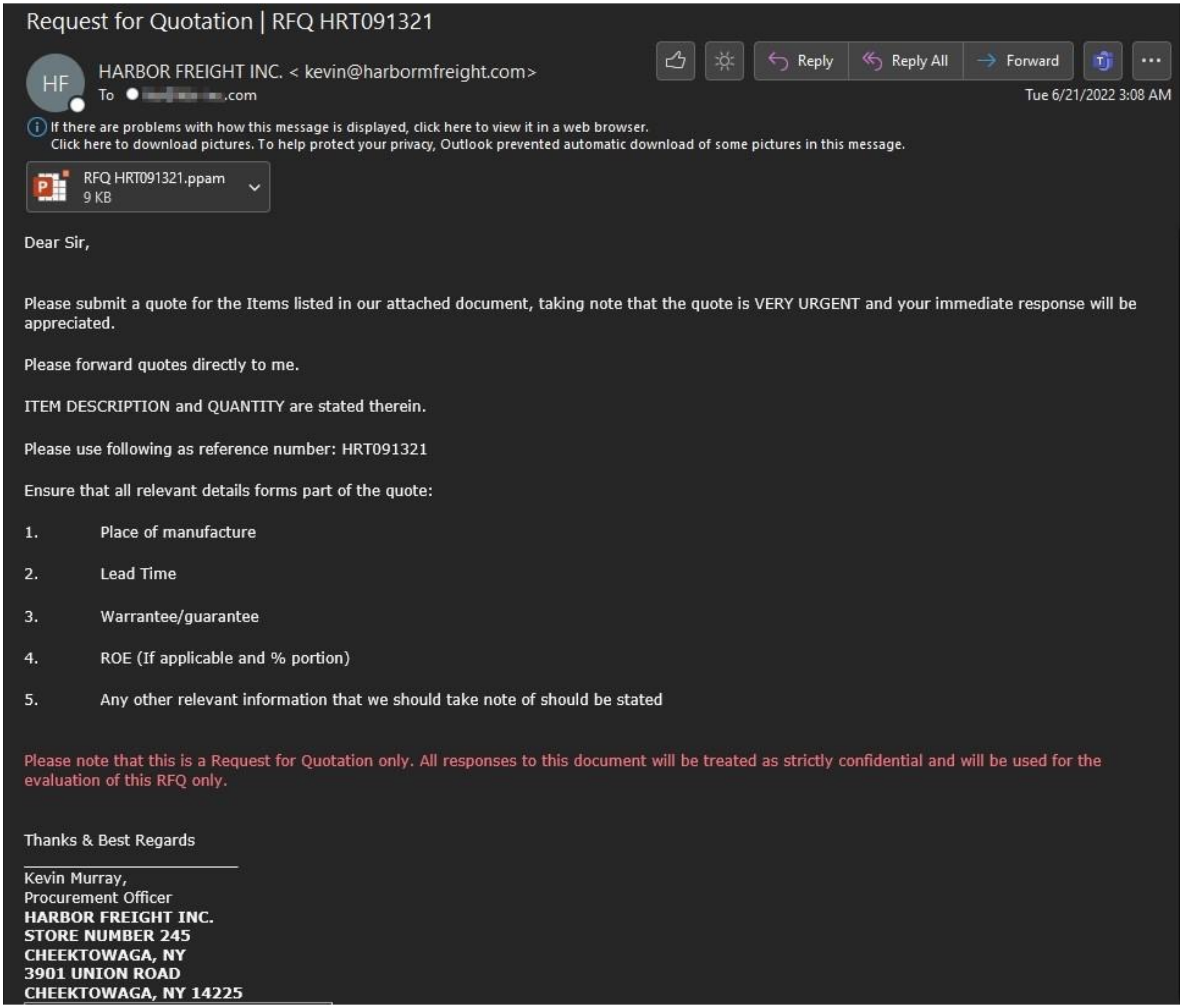
Accounts Department
COSCOSH SHANGHAI SHIP MANAGEMENT CO. LTD
Room 1116, No.1367 Chang Yang Road, Shanghai, China
Tel: +86-21-65701118 x 6258
Mobile:13818116042
Fax: +86-21-65111318

中遠海運港口有限公司
COSCO SHIPPING Ports Limite

1 attachment: DETAILS.zip 506 KB

Example B: Fale Harbor Freight Request for Quote (RFQ)

The cybercrime group we refer to as Master X uses PowerPoint malware loaders to conduct attacks. One of their campaigns posed as tool and equipment retailer Harbor Freight. The email appeared to be a request for quote (RFQ), with the aim of convincing the recipient to open the macro-enabled PowerPoint file (.ppam). The macro would automatically execute upon closing the file to kick off the infection chain. Master X prefers to live off the land, abusing legitimate services to host their attacks. This one reached out to Atlassian's Bitbucket source code repo service, enabling it to retrieve the Agent Tesla remote access Trojan payload.



Request for Quotation | RFQ HRT091321

HARBOR FREIGHT INC. < kevin@harbormfreight.com>
To [redacted].com
Tue 6/21/2022 3:08 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Sir,

Please submit a quote for the Items listed in our attached document, taking note that the quote is VERY URGENT and your immediate response will be appreciated.

Please forward quotes directly to me.

ITEM DESCRIPTION and QUANTITY are stated therein.

Please use following as reference number: HRT091321

Ensure that all relevant details forms part of the quote:

1. Place of manufacture
2. Lead Time
3. Warrantee/guarantee
4. ROE (If applicable and % portion)
5. Any other relevant information that we should take note of should be stated

Please note that this is a Request for Quotation only. All responses to this document will be treated as strictly confidential and will be used for the evaluation of this RFQ only.

Thanks & Best Regards

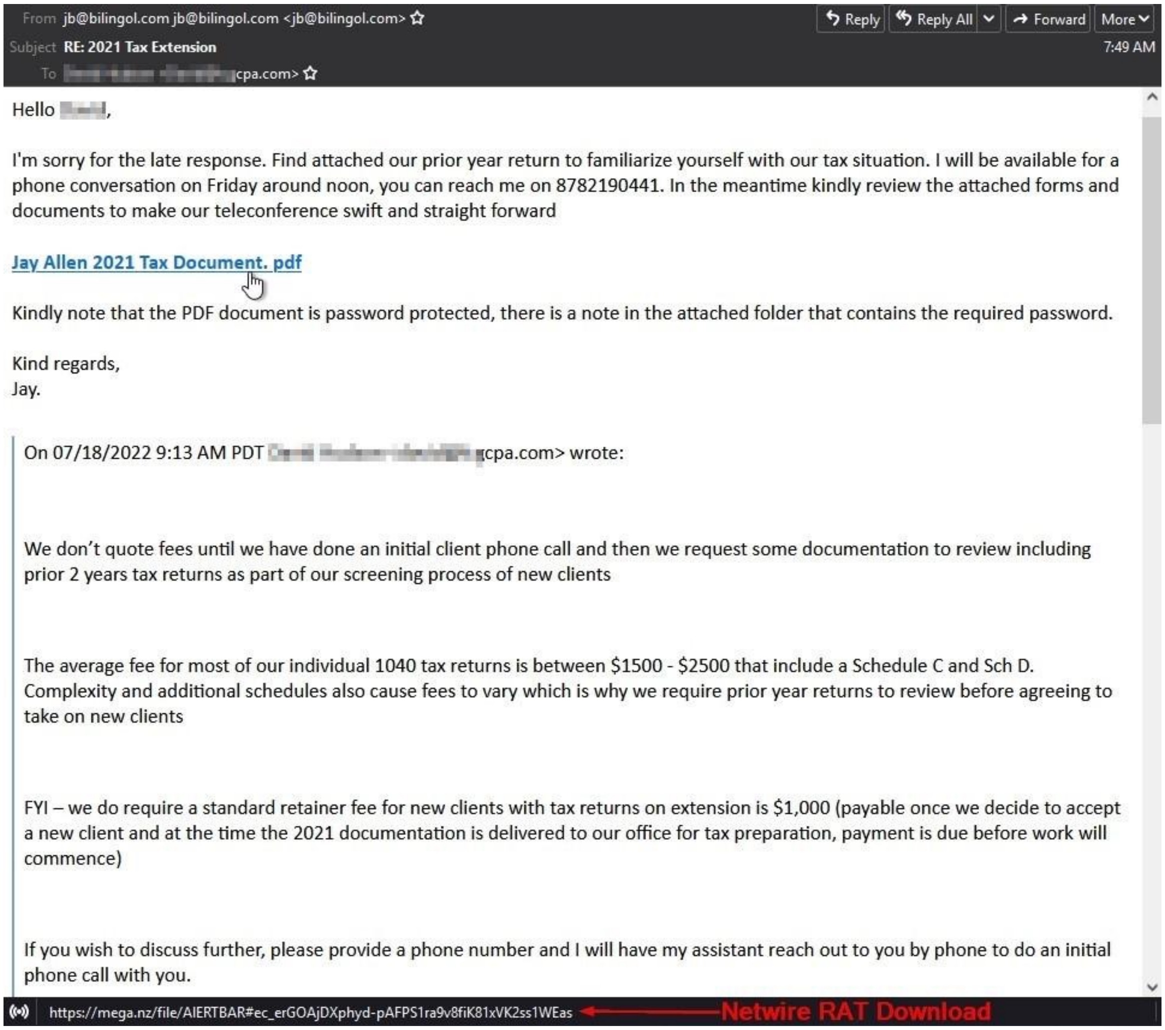
Kevin Murray,
Procurement Officer
HARBOR FREIGHT INC.
STORE NUMBER 245
CHEEKTOWAGA, NY
3901 UNION ROAD
CHEEKTOWAGA, NY 14225

Example C: Targeting Tax Firms

Attackers often use malware attachments to execute business email compromise (BEC) attacks. For example, a trend we've noticed over the last couple of years has seen attackers targeting chartered public accountants (CPAs) and law firms with BEC attacks that use malware. (We've even been able to turn the scam back against some of these actors.)

The attacker starts by sending a few emails containing realistic tax questions. After some back-and-forth, having gained the victim's trust, they follow up by sending malware disguised as documents they claim are tax files for the recipient to download and review.

A recent example contained a link to the mega[.]nz file sharing service that downloads an .iso (disc image) file. Inside this example was an encrypted "2021 Tax Documents" PDF, along with a supposed password file to open the PDF. However, the password file was designed to retrieve and execute the Netwire RAT payload that would download from Pastebin.



From jb@bilingol.com jb@bilingol.com <jb@bilingol.com> ☆
Subject RE: 2021 Tax Extension
7:49 AM
To [redacted]cpa.com> ☆

Hello [redacted],

I'm sorry for the late response. Find attached our prior year return to familiarize yourself with our tax situation. I will be available for a phone conversation on Friday around noon, you can reach me on 8782190441. In the meantime kindly review the attached forms and documents to make our teleconference swift and straight forward

Jay Allen 2021 Tax Document. pdf

Kindly note that the PDF document is password protected, there is a note in the attached folder that contains the required password.

Kind regards,
Jay.

> On 07/18/2022 9:13 AM PDT [redacted]cpa.com> wrote:
>
> We don't quote fees until we have done an initial client phone call and then we request some documentation to review including prior 2 years tax returns as part of our screening process of new clients
>
> The average fee for most of our individual 1040 tax returns is between $1500 - $2500 that include a Schedule C and Sch D. Complexity and additional schedules also cause fees to vary which is why we require prior year returns to review before agreeing to take on new clients
>
> FYI – we do require a standard retainer fee for new clients with tax returns on extension is $1,000 (payable once we decide to accept a new client and at the time the 2021 documentation is delivered to our office for tax preparation, payment is due before work will commence)
>
> If you wish to discuss further, please provide a phone number and I will have my assistant reach out to you by phone to do an initial phone call with you.

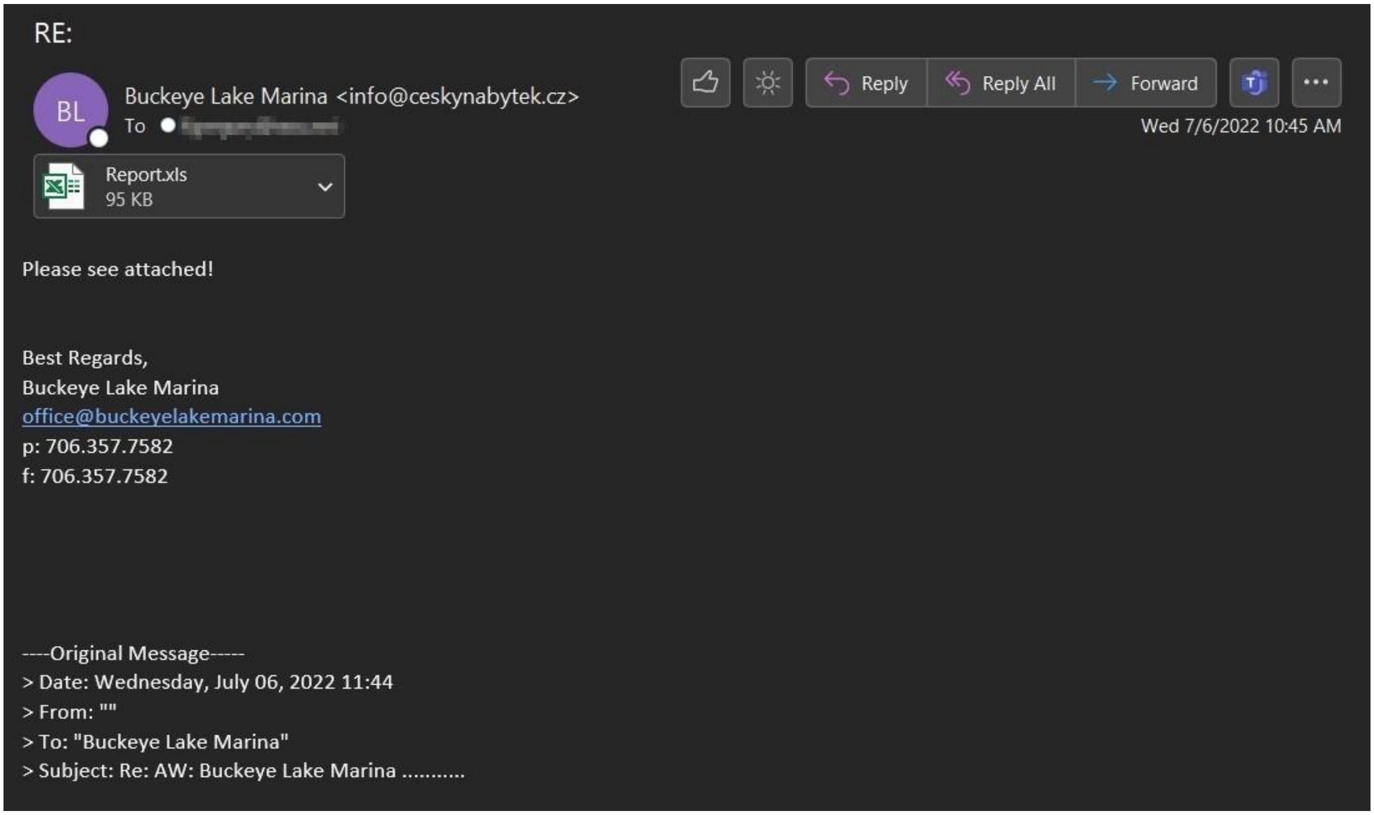
https://mega.nz/file/AIERTBAR#ec_erGOAjDXphyd-pAFPS1ra9v8fiK81xVK2ss1WEas

Notorious Malwares

Emotet

The Emotet malware gang has been considered one of the most prolific and dangerous operators since it was first detected in 2014. In an Emotet attack, a Cobalt Strike beacon is typically deployed on the compromised machine, creating an opportunity for ransomware gangs such as Conti, Quantum, or BlackCat. In March, Bleeping Computer reported that Emotet had infected 130,000 systems in 179 countries since it re-emerged in November 2021, when Trickbot began reseeding it. Emotet attacks appeared in multiple languages in 2022, including Italian, German, Japanese, Spanish, Portuguese, and English.

As in previous years, Emotet users continued to rely on conversation hijacking attacks (CHAs), replying to messages from compromised victims' contacts in the hope that the recipient would trust and open the attachment. They often kept the body of the replies very simple, such as "Please see attached!"



RE:

Buckeye Lake Marina <info@ceskynabytek.cz>
To [redacted]

Wed 7/6/2022 10:45 AM

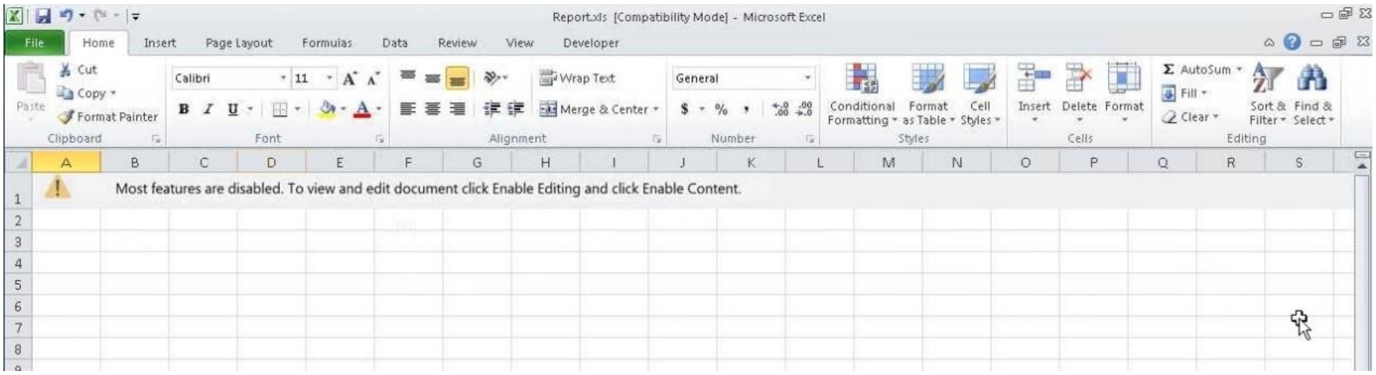
Report.xls
95 KB

Please see attached!

Best Regards,
Buckeye Lake Marina
office@buckeyelakemarina.com
p: 706.357.7582
f: 706.357.7582

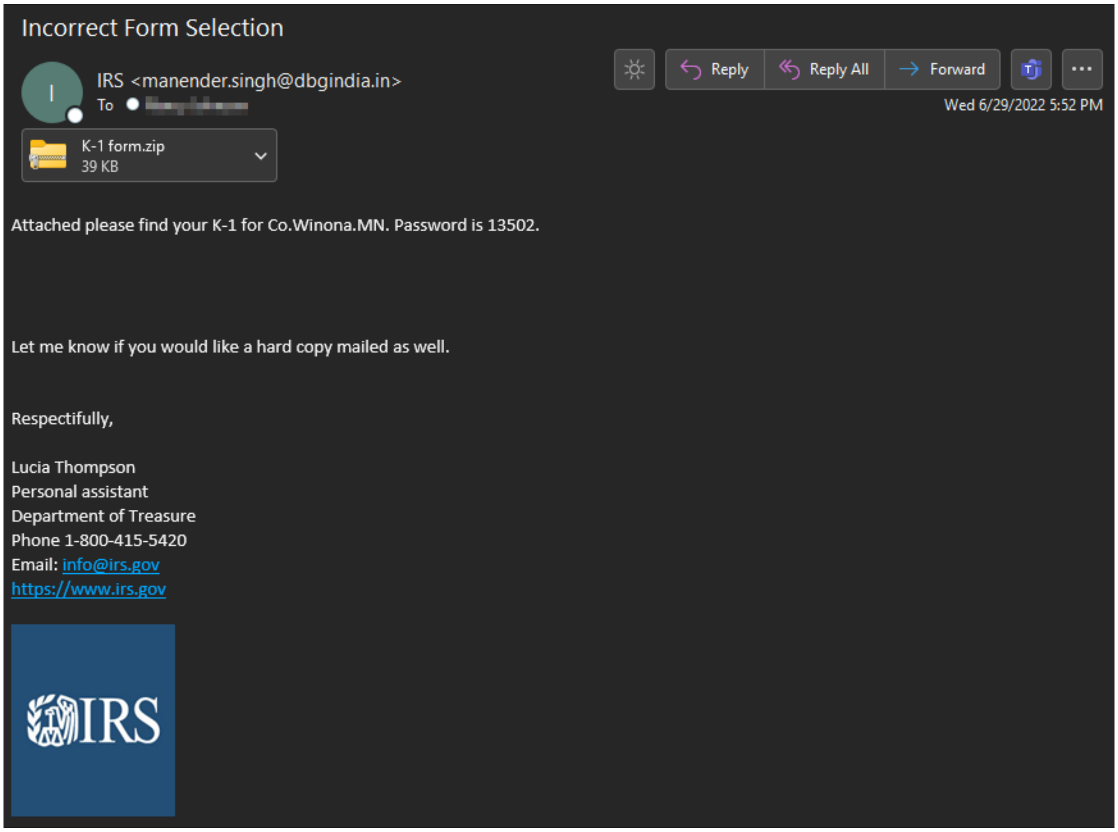
----Original Message-----
> Date: Wednesday, July 06, 2022 11:44
> From: ""
> To: "Buckeye Lake Marina"
> Subject: Re: AW: Buckeye Lake Marina ....

If the recipient opened the attachment, they were greeted with a simple message in the Excel worksheet that stated: “Most features are disabled. To view and edit document, click Enable Editing and click Enable Content.” Clicking these would disable Microsoft’s protected view and allow the macro to execute the Emotet payload modules. Users should be extremely suspicious of any file that asks them to disable security features such as this.



Most features are disabled. To view and edit document click Enable Editing and click Enable Content.

Another Emotet campaign we captured used password-protected encrypted ZIPs containing malicious XLS files. For example, the attackers sent an email posing as the Internal Revenue Service (IRS) with a subject line claiming that the recipient had selected the wrong tax form. They attached a fictitious K-1 form and included a password in the email body.



Incorrect Form Selection

IRS <manender.singh@dbgindia.in>
To [redacted]

Wed 6/29/2022 5:52 PM

K-1 form.zip
39 KB

Attached please find your K-1 for Co.Winona.MN. Password is 13502.

Let me know if you would like a hard copy mailed as well.

Respectfully,

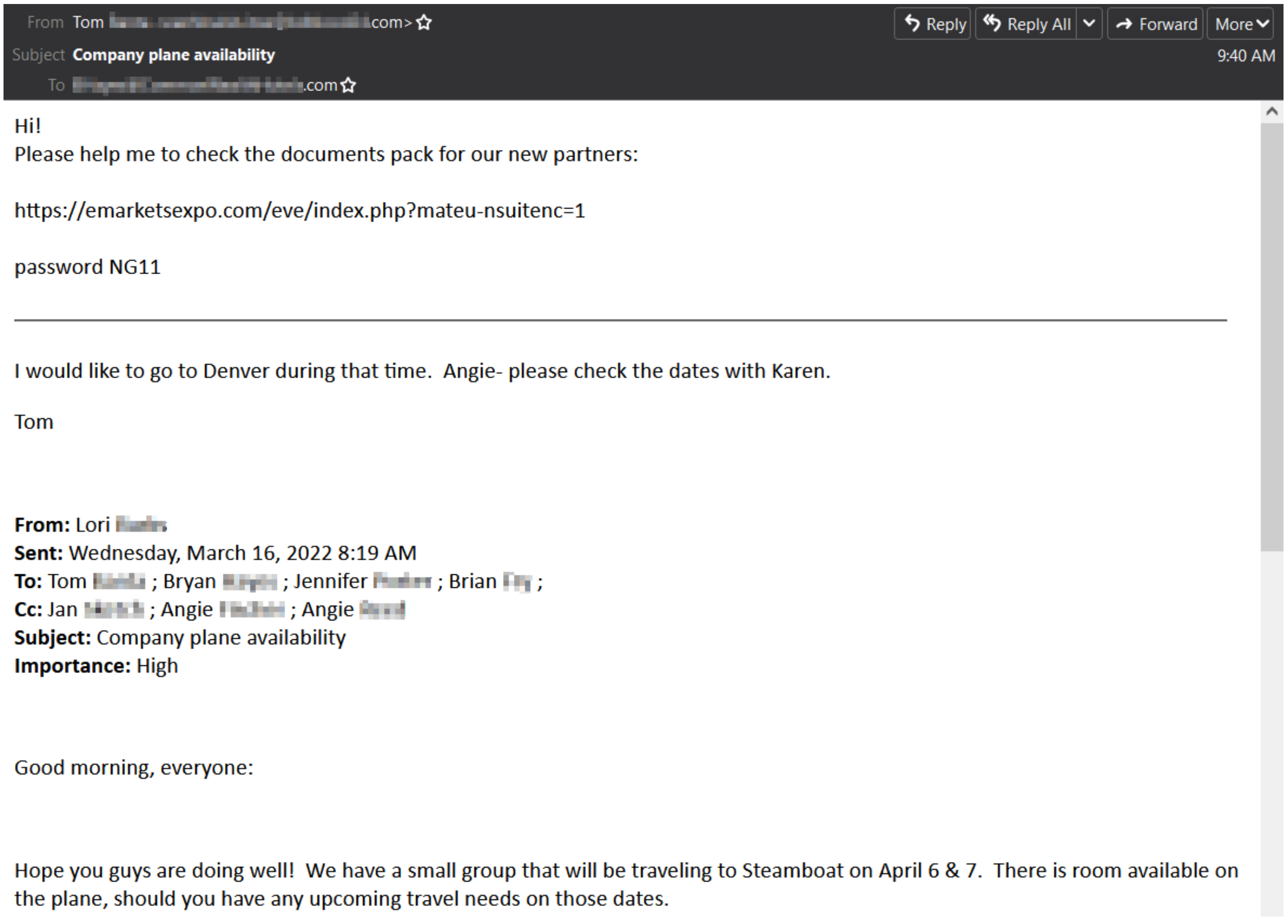
Lucia Thompson
Personal assistant
Department of Treasure
Phone 1-800-415-5420
Email: info@irs.gov
https://www.irs.gov

Qakbot/Qbot

While RATs continue to make up most malware attacks, Qakbot/Qbot is one of the most destructive and convincing types of email attacks. As with Emotet, it’s usually followed up with a CobaltStrike attack, priming it for ransomware operations.

Some of the most convincing and aggressive attacks of 2022 were sent by an actor who is tracked under the identifier TA577 and known as “TR” based on their Qakbot affiliate tag. In a typical attack, they use Qakbot to scrape trusted email conversations that they can respond to — the same MO as Emotet. TA577 is known to sell access to compromised accounts to ransomware groups such as Conti and Black Basta, the latter of whom has been linked to FIN7/Carbanak, a Russian APT group responsible for some of the most sophisticated and highest-profile attacks in the world. Over the past decade, they have stolen over $1.2 billion USD.

TA577 recently changed the infection chain in the following CHA campaign to use a URL that isn’t hyperlinked in the message. It requires the victim to copy and paste it in a browser to initiate the download of an encrypted zip file that requires the password from the body of the message. Upon extraction, the zip contains an .img archive that contains a visual basic script that retrieves the Qakbot payload.



From Tom [redacted].com> ☆
Subject **Company plane availability**
To [redacted].com ☆
9:40 AM

Hi!
Please help me to check the documents pack for our new partners:

https://emarketsexpo.com/eve/index.php?mateu-nsuitenc=1

password NG11

I would like to go to Denver during that time. Angie- please check the dates with Karen.

Tom

From: Lori [redacted]
Sent: Wednesday, March 16, 2022 8:19 AM
To: Tom [redacted] ; Bryan [redacted] ; Jennifer [redacted] ; Brian [redacted] ;
Cc: Jan [redacted] ; Angie [redacted] ; Angie [redacted]
Subject: Company plane availability
Importance: High

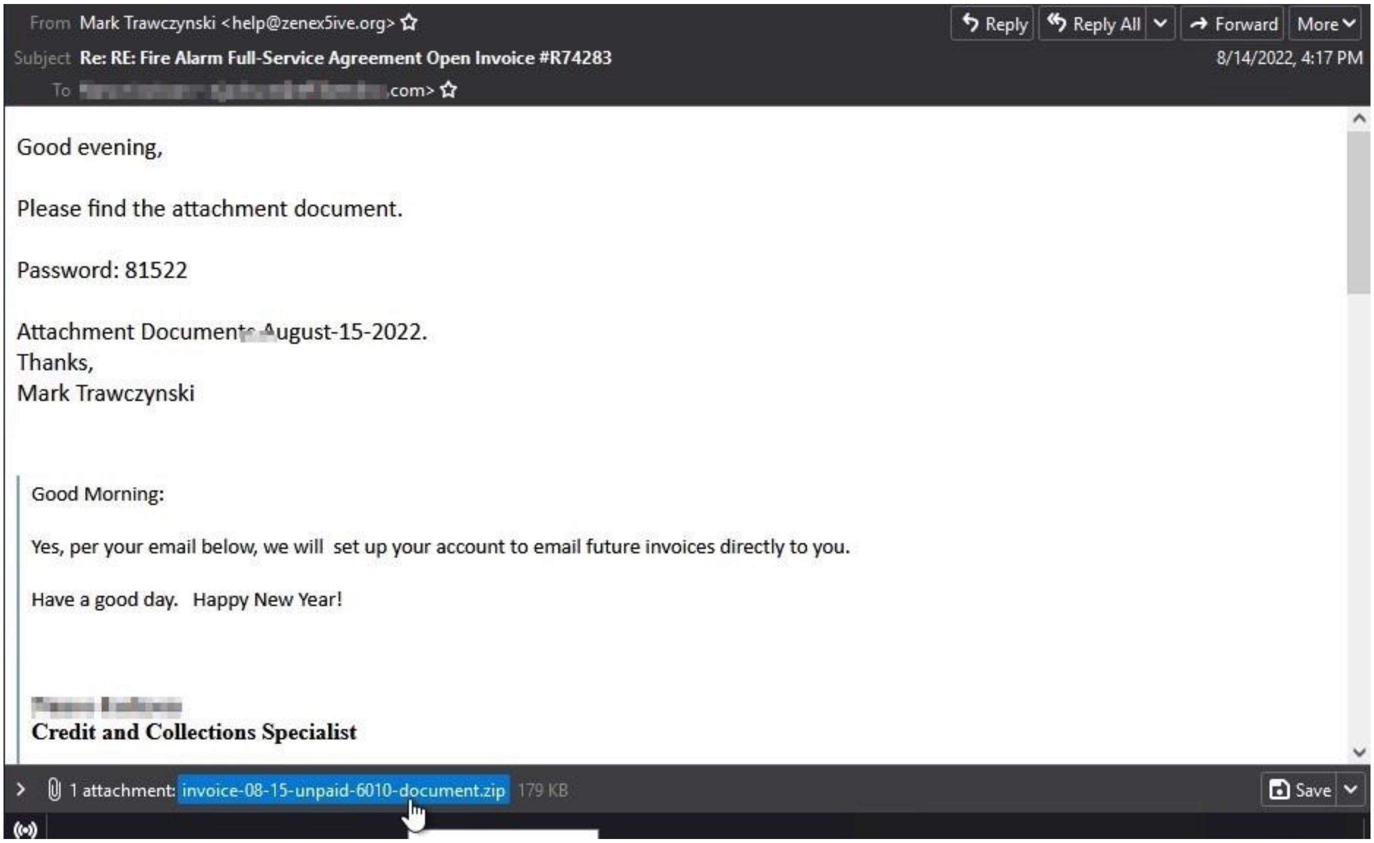
Good morning, everyone:

Hope you guys are doing well! We have a small group that will be traveling to Steamboat on April 6 & 7. There is room available on the plane, should you have any upcoming travel needs on those dates.

IcedID

The actors behind the IcedID modular banking Trojan remained active in 2022, even though their activities were often overshadowed by higher volume campaigns from Emotet and Qakbot actors using similar techniques. Multiple threat actors used IcedID as brokers through which they could sell access to victims' accounts to ransomware operators such as Conti. Given this activity, it remained a top email threat in 2022 and will continue to be so in 2023.

For years we've been capturing IcedID CHAs. In this recent example, they are replying to a conversation with an encrypted zip file and the password to open it in the body of the email. Receiving this kind of message with no context should be a red flag — but sending it from a trusted contact as part of an established conversation makes it more convincing to even well-trained users. This attack also uses an .iso file within the zip in order to bypass mark-of-the-web security controls and execute the IcedID payload without warning to the user.



From Mark Trawczynski <help@zenex5ive.org>
Subject Re: RE: Fire Alarm Full-Service Agreement Open Invoice #R74283
8/14/2022, 4:17 PM
To [redacted].com>

Good evening,

Please find the attachment document.

Password: 81522

Attachment Document[redacted]August-15-2022.
Thanks,
Mark Trawczynski

> Good Morning:
>
> Yes, per your email below, we will set up your account to email future invoices directly to you.
>
> Have a good day. Happy New Year!
>
> [redacted]
> **Credit and Collections Specialist**

1 attachment: invoice-08-15-unpaid-6010-document.zip 179 KB

Email-based Threats • Remote Access Trojan • Notorius Malwares • Emotet • Qakbot/Qbot • IcedID

Conclusion

Email has long been considered a cybersecurity hot spot — and the trends we saw in 2022 justify these concerns. Attackers recognize that email serves as a direct link to end users. Many of their tactics rely on convincing those users that the link or attachment they've received is safe and genuine, when in fact, it gains the attackers' access to their system, other accounts, and sensitive information.

Combatting email attacks requires cybersecurity and human awareness. Email filters can pick up on and quarantine suspicious messages, and cyber training teaches people not to automatically trust any email they receive. It's important that they verify email addresses, attachments, and links, report hacked accounts, and follow strong password policies.

Attackers adapt their tactics to suit changing changing technology and societal trends. By monitoring their behavior, we can react to and defend against their strategies.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.