The Beer Farmers
present

Will Thomas

Gone Phishin' / Attack of the Phish (something something phishing)

30th October, 15:40 GMT

#BeerCon2

$~WHOAMI

SECURITY RESEARCHER

CYBER THREAT INTELLIGENCE

MALWARE ANALYSIS

OSINT

THE MANY HATS CLUB

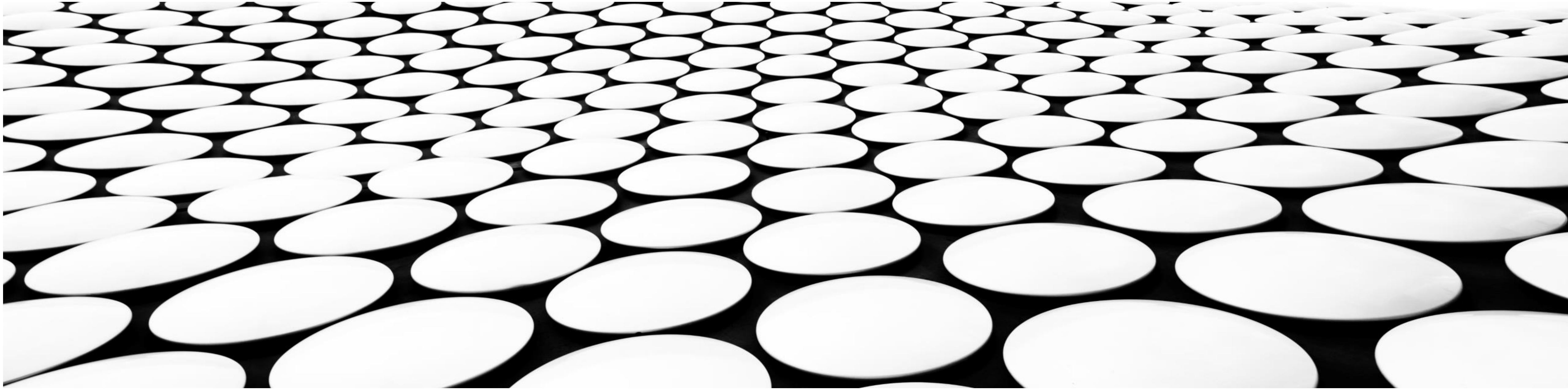
$~MAN

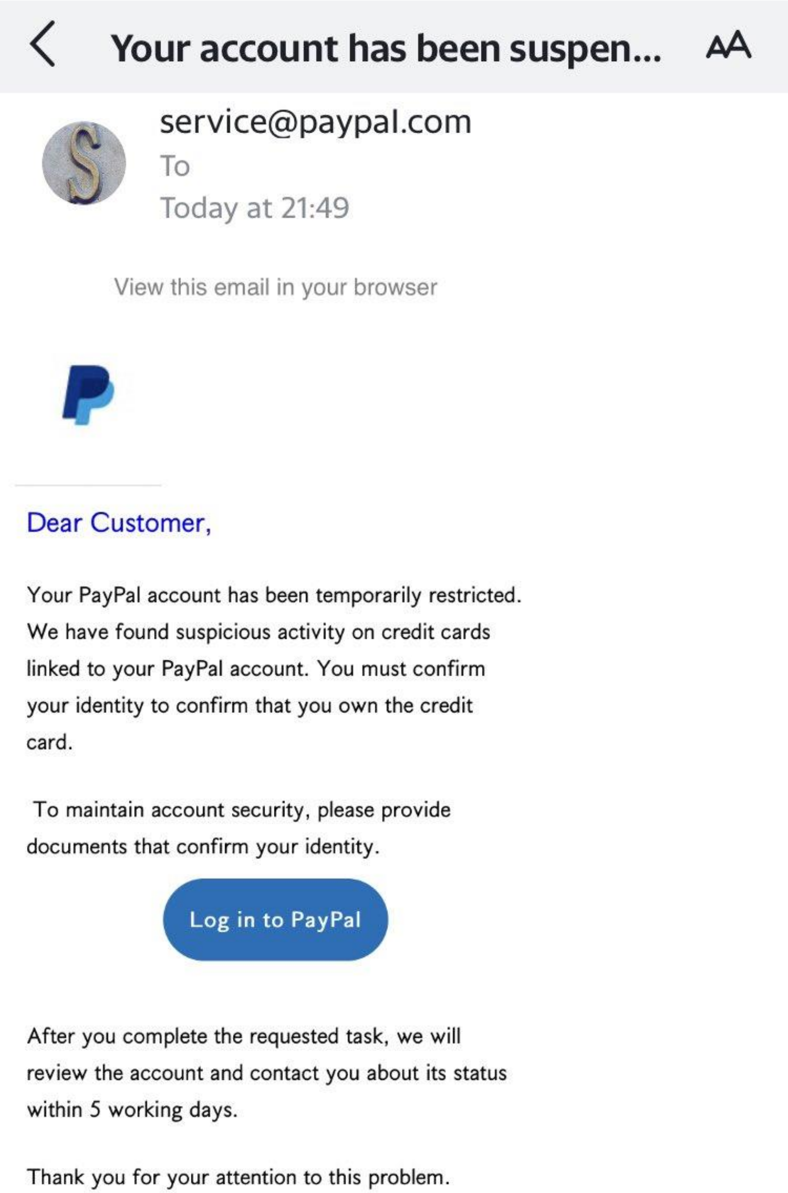
@BushidoToken

blog.bushidotoken.net

Moderator on The Many Hats Club

CTI League





Your account has been suspen...

service@paypal.com
To
Today at 21:49

View this email in your browser

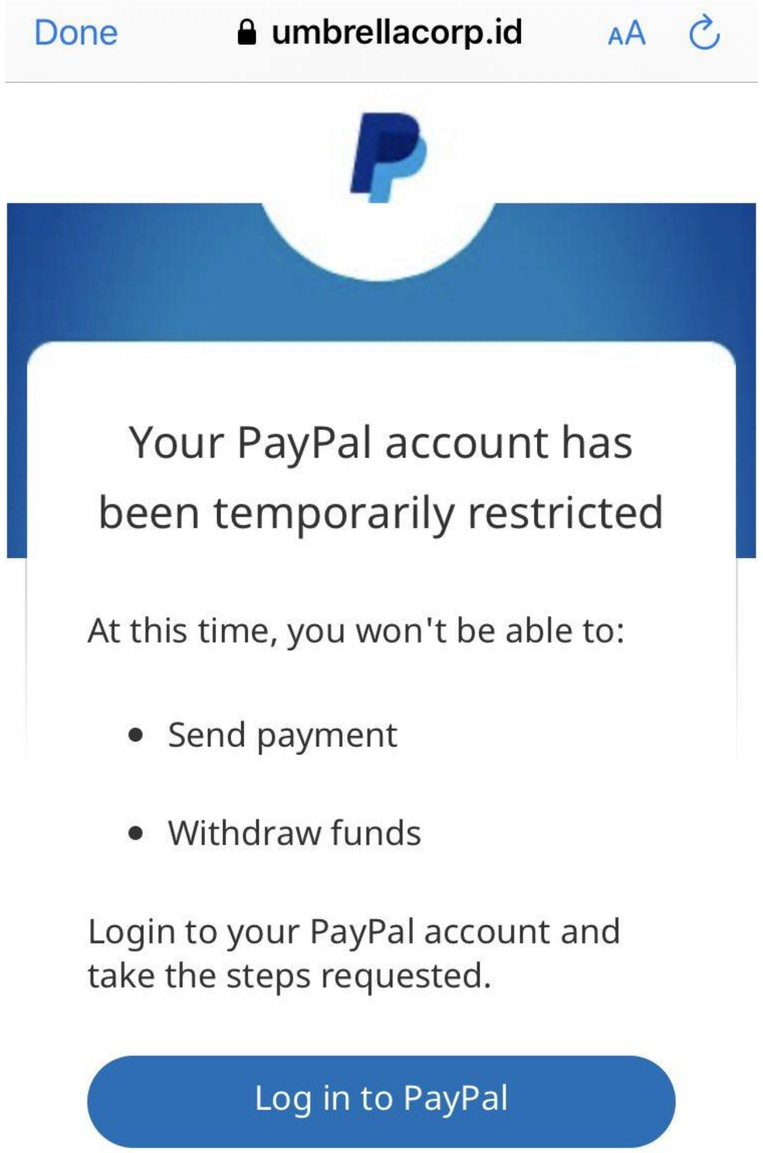
Dear Customer,

Your PayPal account has been temporarily restricted. We have found suspicious activity on credit cards linked to your PayPal account. You must confirm your identity to confirm that you own the credit card.

To maintain account security, please provide documents that confirm your identity.

After you complete the requested task, we will review the account and contact you about its status within 5 working days.

Thank you for your attention to this problem.

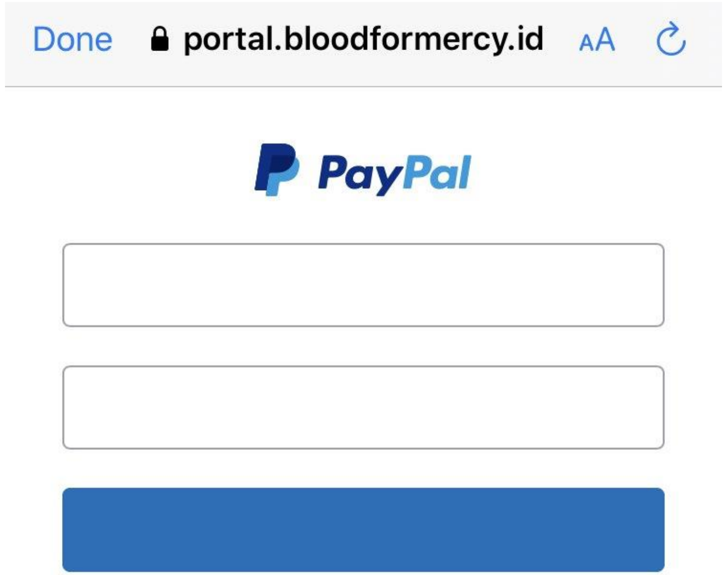


Your PayPal account has been temporarily restricted

At this time, you won't be able to:

- Send payment
- Withdraw funds

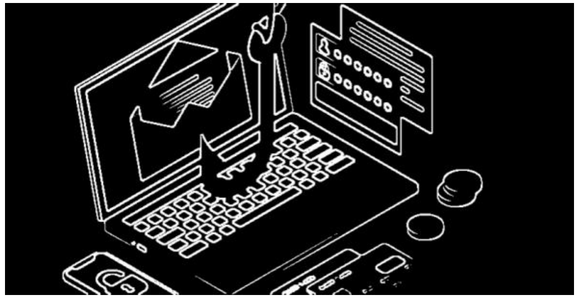
Login to your PayPal account and take the steps requested.



THE STATE OF PHISHING

- Leveraging the Cloud
- Mass Credential Harvesting
- Capturing 2FA Tokens
- Free Malware
- Evasion

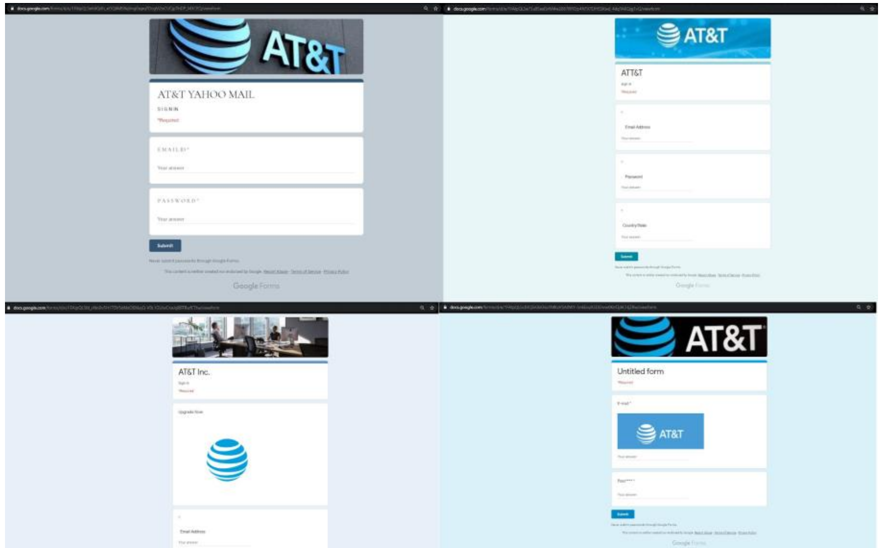
- Organised
- Phishing-as-a-Service
- Business Email Compromise
- Emotet Spam Botnet
- Mitigation & Prediction



LEVERAGING THE CLOUD

Google Docs

Google Forms



AT&T YAHOO MAIL

SIGN IN

*Required

EMAIL ID*

Your answer

PASSWORD*

Your answer

Submit

Google Forms

ATT&T

Email Address

Password

Country/State

Google Forms

AT&T Inc.

Upgrade Now

Email Address

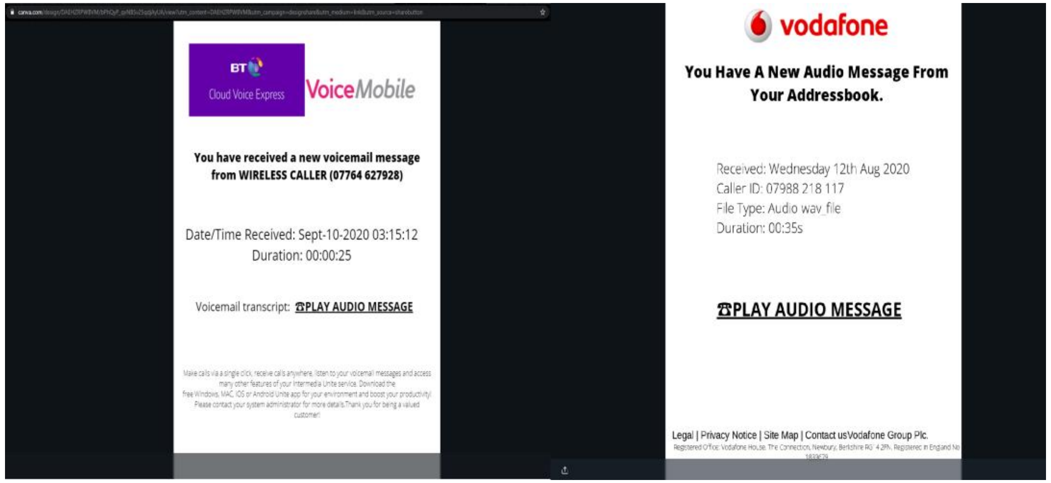
Untitled form

E-mail*

Pass****

Google Forms

Canva



BT Cloud Voice Express VoiceMobile

You have received a new voicemail message from WIRELESS CALLER (07764 627928)

Date/Time Received: Sept-10-2020 03:15:12

Duration: 00:00:25

Voicemail transcript: ☎PLAY AUDIO MESSAGE

Make calls via a single click, receive calls anywhere, listen to your voicemail messages and access many other features of your Intermedia Unite service. Download the free Windows, MAC, IOS or Android Unite app for your environment and boost your productivity! Please contact your system administrator for more details.Thank you for being a valued customer!

vodafone

You Have A New Audio Message From Your Addressbook.

Received: Wednesday 12th Aug 2020

Caller ID: 07988 218 117

File Type: Audio wav file

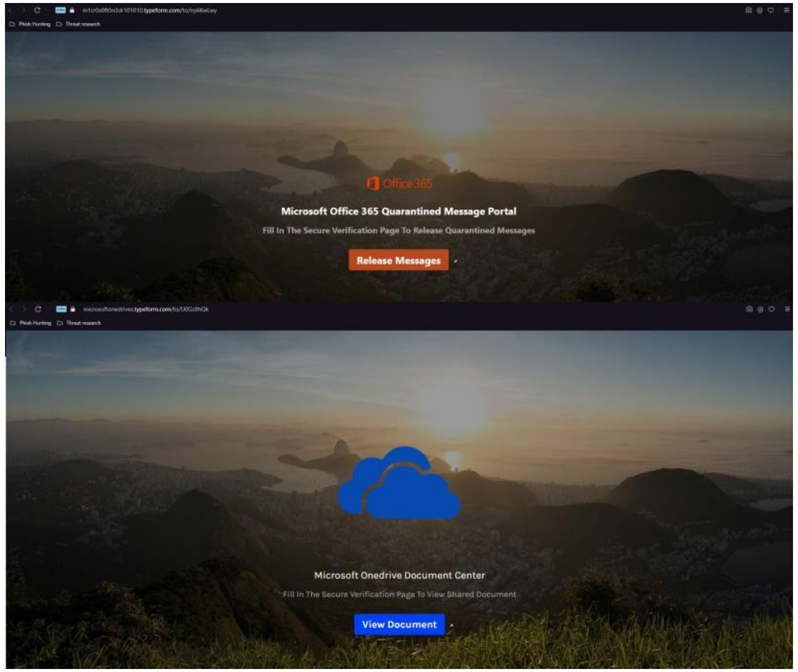
Duration: 00:35s

☎PLAY AUDIO MESSAGE

Legal | Privacy Notice | Site Map | Contact usVodafone Group Plc.

Registered Office: Vodafone House, The Connection, Newbury, Berkshire RG14 2FN. Registered in England No 1833679

Typeform



Office 365

Microsoft Office 365 Quarantined Message Portal

Fill In The Secure Verification Page To Release Quarantined Messages

Release Messages

microsoftonedrives.typeform.com/to/U0Gz8hQk

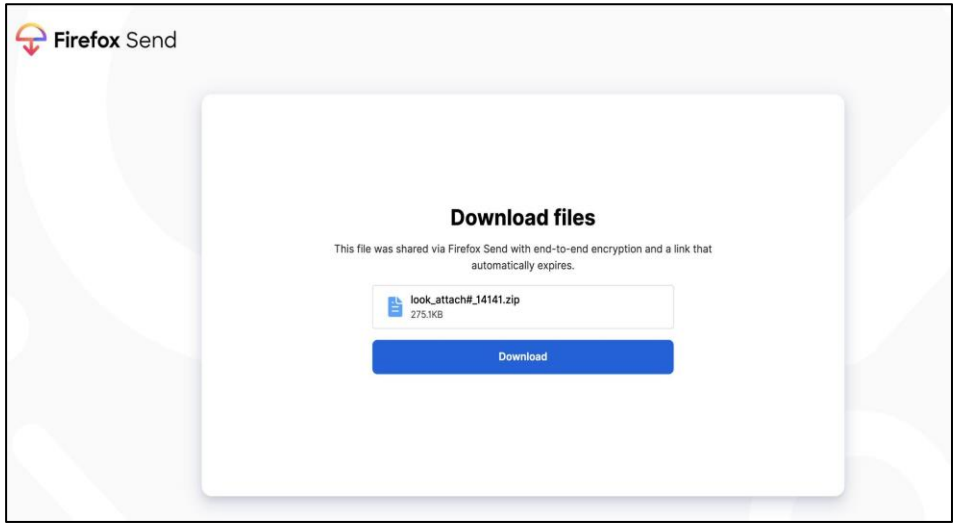
Phish Hunting Threat research

Microsoft Onedrive Document Center

Fill In The Secure Verification Page To View Shared Document

View Document

~~Firefox Send~~



Firefox Send

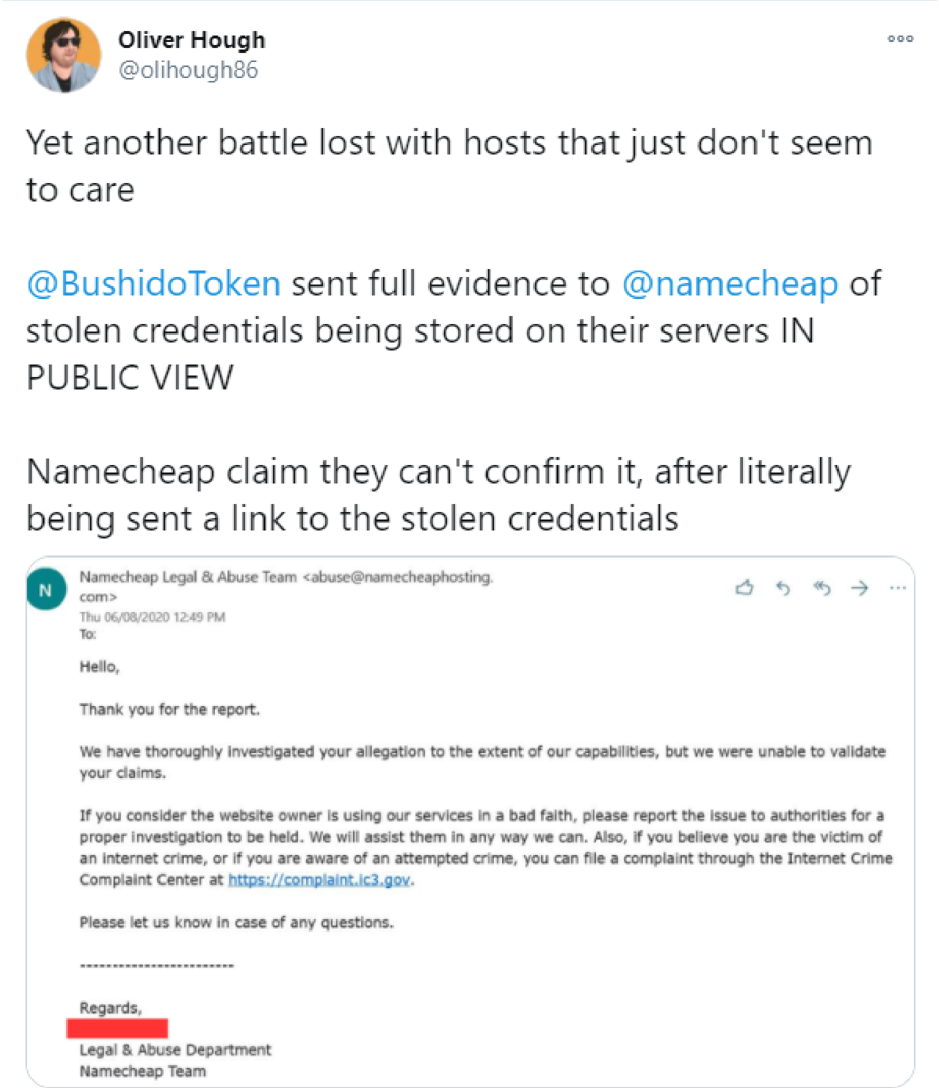
Download files

This file was shared via Firefox Send with end-to-end encryption and a link that automatically expires.

look_attach#_14141.zip
275.1KB

Download

MASS CREDENTIAL HARVESTING



Oliver Hough
@olihough86

Yet another battle lost with hosts that just don't seem to care

@BushidoToken sent full evidence to @namecheap of stolen credentials being stored on their servers IN PUBLIC VIEW

Namecheap claim they can't confirm it, after literally being sent a link to the stolen credentials

Namecheap Legal & Abuse Team <abuse@namecheaphosting.com>
Thu 06/08/2020 12:49 PM
To:

Hello,

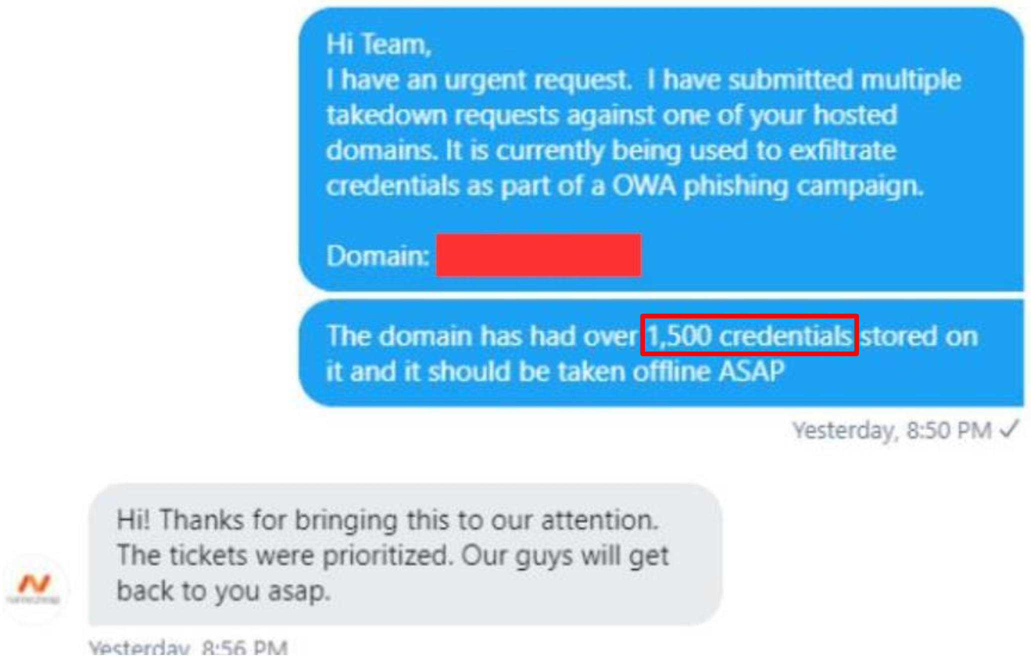
Thank you for the report.

We have thoroughly investigated your allegation to the extent of our capabilities, but we were unable to validate your claims.

If you consider the website owner is using our services in a bad faith, please report the issue to authorities for a proper investigation to be held. We will assist them in any way we can. Also, if you believe you are the victim of an internet crime, or if you are aware of an attempted crime, you can file a complaint through the Internet Crime Complaint Center at https://complaint.ic3.gov.

Please let us know in case of any questions.

Regards,
[redacted]
Legal & Abuse Department
Namecheap Team



Hi Team,
I have an urgent request. I have submitted multiple takedown requests against one of your hosted domains. It is currently being used to exfiltrate credentials as part of a OWA phishing campaign.

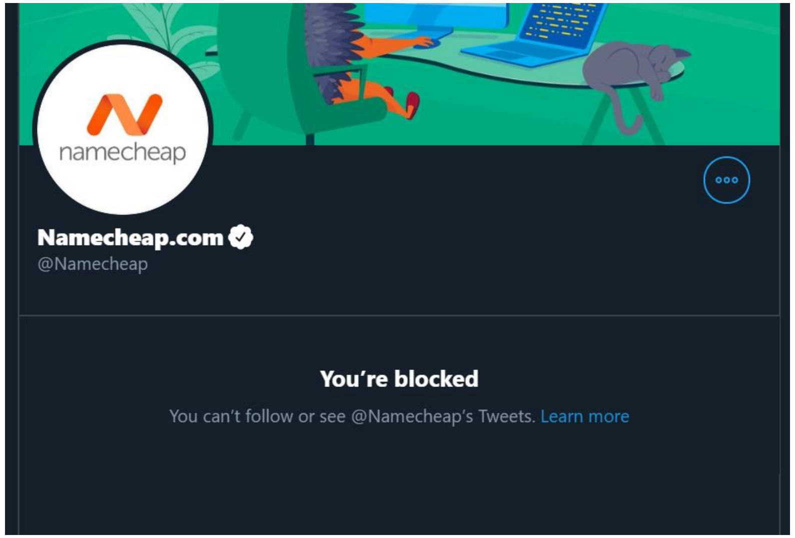
Domain: [redacted]

The domain has had over 1,500 credentials stored on it and it should be taken offline ASAP

Yesterday, 8:50 PM ✓

Hi! Thanks for bringing this to our attention. The tickets were prioritized. Our guys will get back to you asap.

Yesterday, 8:56 PM

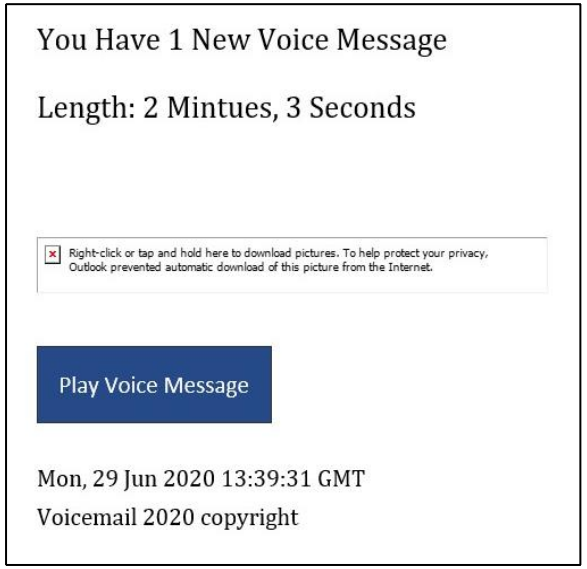


Namecheap.com ✓
@Namecheap

You're blocked

You can't follow or see @Namecheap's Tweets. Learn more

TWILIO SendGrid



You Have 1 New Voice Message

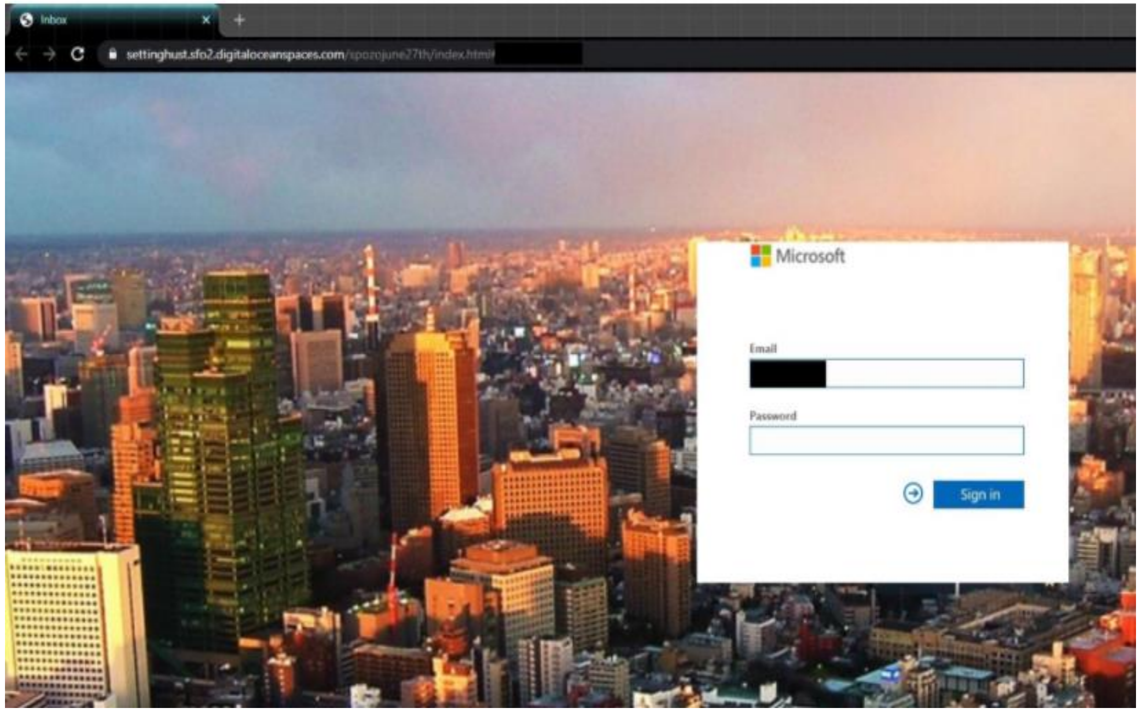
Length: 2 Mintues, 3 Seconds

☒ Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

Play Voice Message

Mon, 29 Jun 2020 13:39:31 GMT

Voicemail 2020 copyright



Inbox
settinghust.sfo2.digitaloceanspaces.com/spozojune27th/index.html# [redacted]
Microsoft
Email
Password
Sign in

Email: [redacted]

Other Domains used in this campaign:

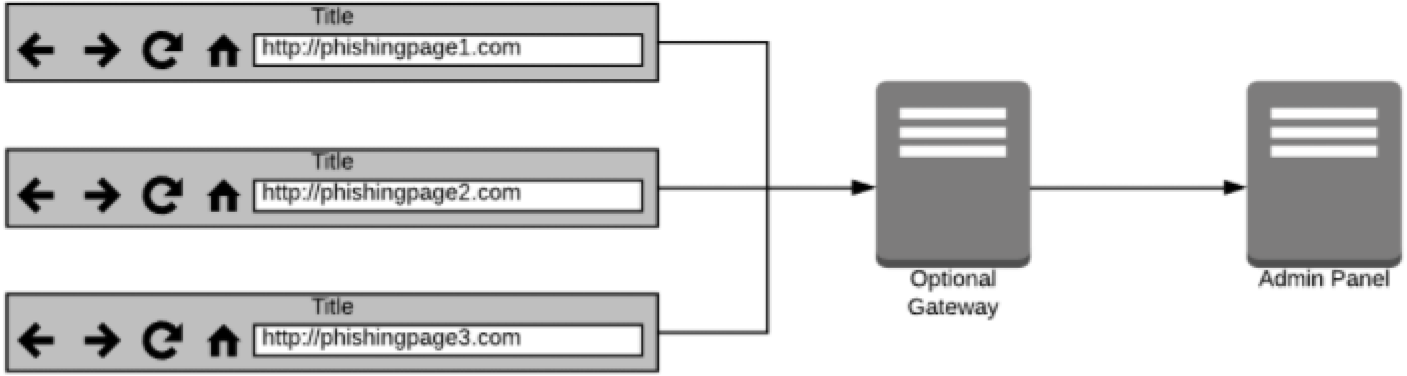
- erased-voice.sfo2.digitaloceanspaces[.]com
- checking-voicenote.sfo2.digitaloceanspaces[.]com
- voicenote-ringer.sfo2.digitaloceanspaces[.]com
- voicenote-caller.sfo2.digitaloceanspaces[.]com
- voice-marketing.sfo2.digitaloceanspaces[.]com
- vmail.sfo2.digitaloceanspaces[.]com

Victim Organisations:

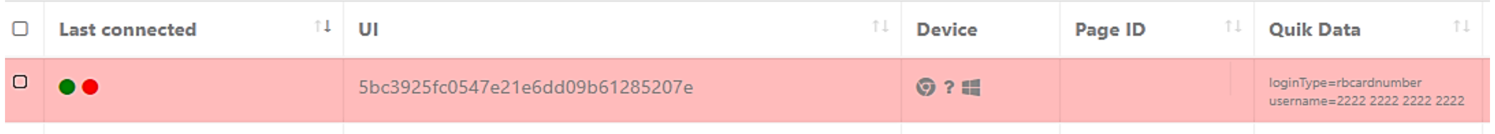
- UK Law Enforcement and the National Health Service
- Government Employees from UK, Australia, Canada, New Zealand, and the US
- Telecoms, Energy, Professional Services, Aviation, and more.
- Stolen Data: email addresses, passwords, IPv4, and geo-location.
- 1,500 credentials

CAPTURING TWO-FACTOR AUTHENTICATION (2FA)

INFRASTRUCTURE:

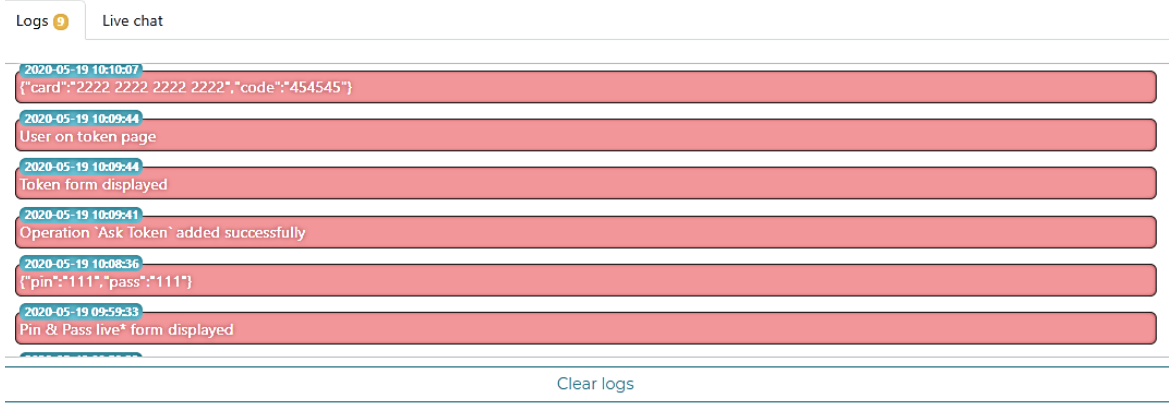


LIVE NOTIFICATIONS:

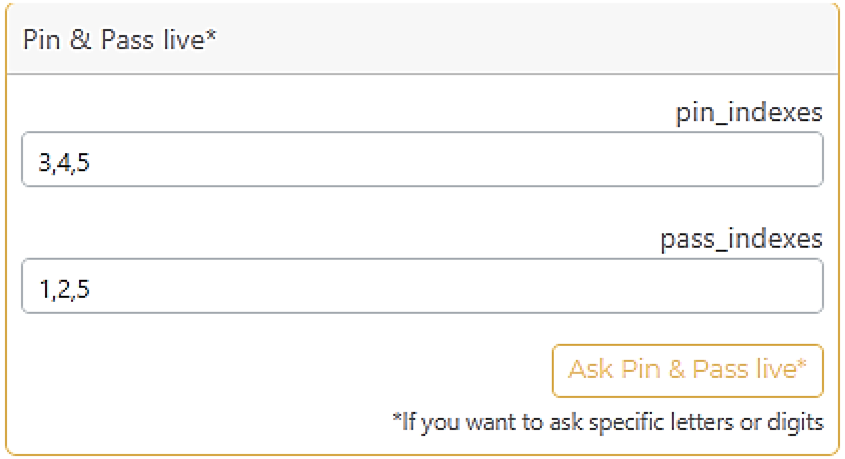


□	Last connected ↑↓	UI ↑↓	Device	Page ID ↑↓	Quik Data ↑↓
□	● ●	5bc3925fc0547e21e6dd09b61285207e	?		loginType=rbcardnumber username=2222 2222 2222 2222

DYNAMIC DATA:



```
2020-05-19 10:10:07
{"card":"2222 2222 2222 2222","code":"454545"}
2020-05-19 10:09:44
User on token page
2020-05-19 10:09:44
Token form displayed
2020-05-19 10:09:41
Operation `Ask Token` added successfully
2020-05-19 10:08:36
{"pin":"111","pass":"111"}
2020-05-19 09:59:33
Pin & Pass live* form displayed
```

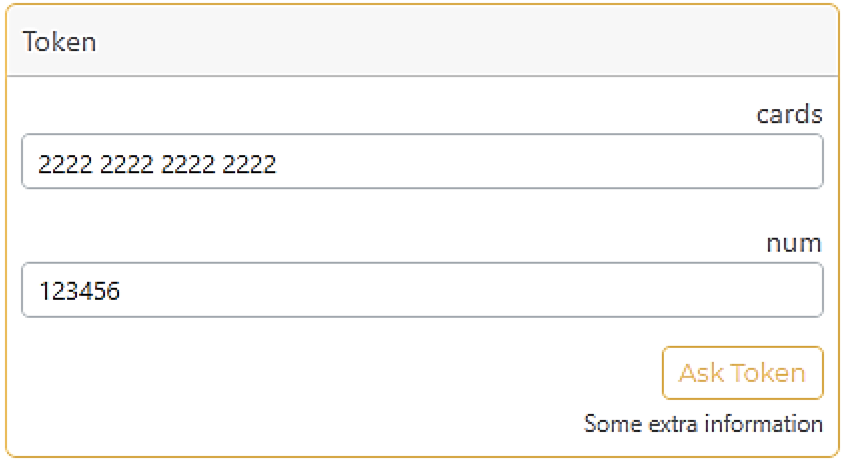


Pin & Pass live*

pin_indexes: 3,4,5

pass_indexes: 1,2,5

*If you want to ask specific letters or digits



Token

cards: 2222 2222 2222 2222

num: 123456

Some extra information

FREE MALWARE HOSTING

[redacted] Re: Consignment Notification: You have A Package With Us

DG
DHL GLOBAL EXPRESS INC <service@dhl.com>
To [redacted]

Greetings,

FYI

Your consignment have been booked via DHL EXPRESS is scheduled for delivery on July 7th.

But your shipment address is missing please kindly review the shipping details attached to confirm if every information is correct to enable us dispatch.

Attached is the shipping document for clearing and reference purposes

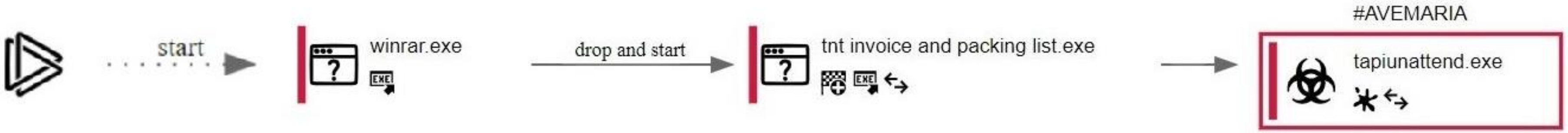
If you would like to find out about the many ways DHL helps you to track your shipment, or if you would like to know more about the services provided by DHL, simply connect to www.dhl.com and select your location at any time.

Best Regards,

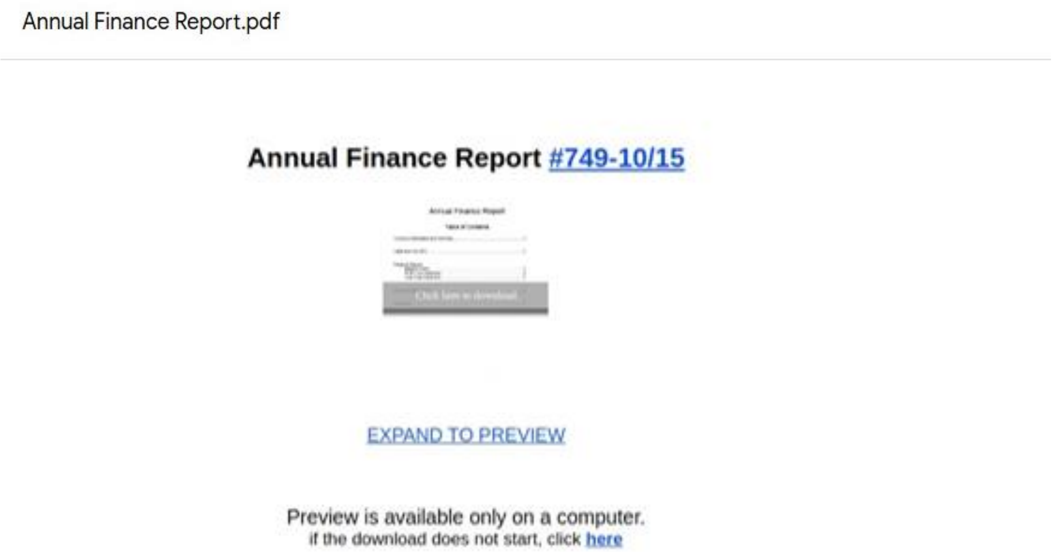
Naveed Castro | Dispatch Manager - Business Development & Marketing
DHL Global Forwarding.
DHL EXPRESS (GLOBAL), INC

DISCORD

https://cdn.discordapp.com/attachments/{ChannelID}/{AttachmentID}/example.exe



TWILIO SendGrid → Google Docs → aws Basecamp → BazarLoader

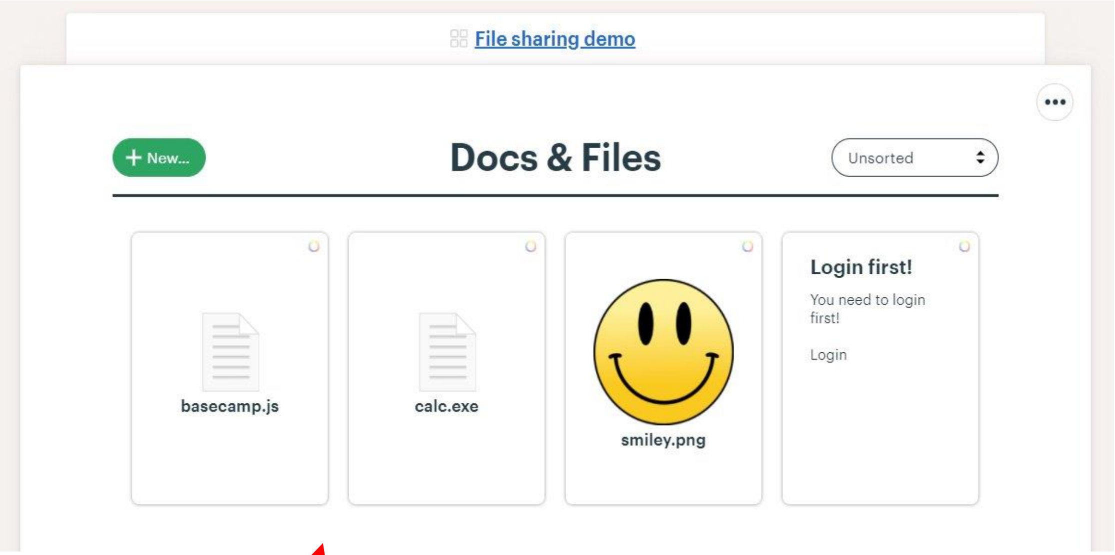


Annual Finance Report.pdf

Annual Finance Report #749-10/15

EXPAND TO PREVIEW

Preview is available only on a computer.
If the download does not start, click here



File sharing demo

Docs & Files

Login first!

You need to login first!

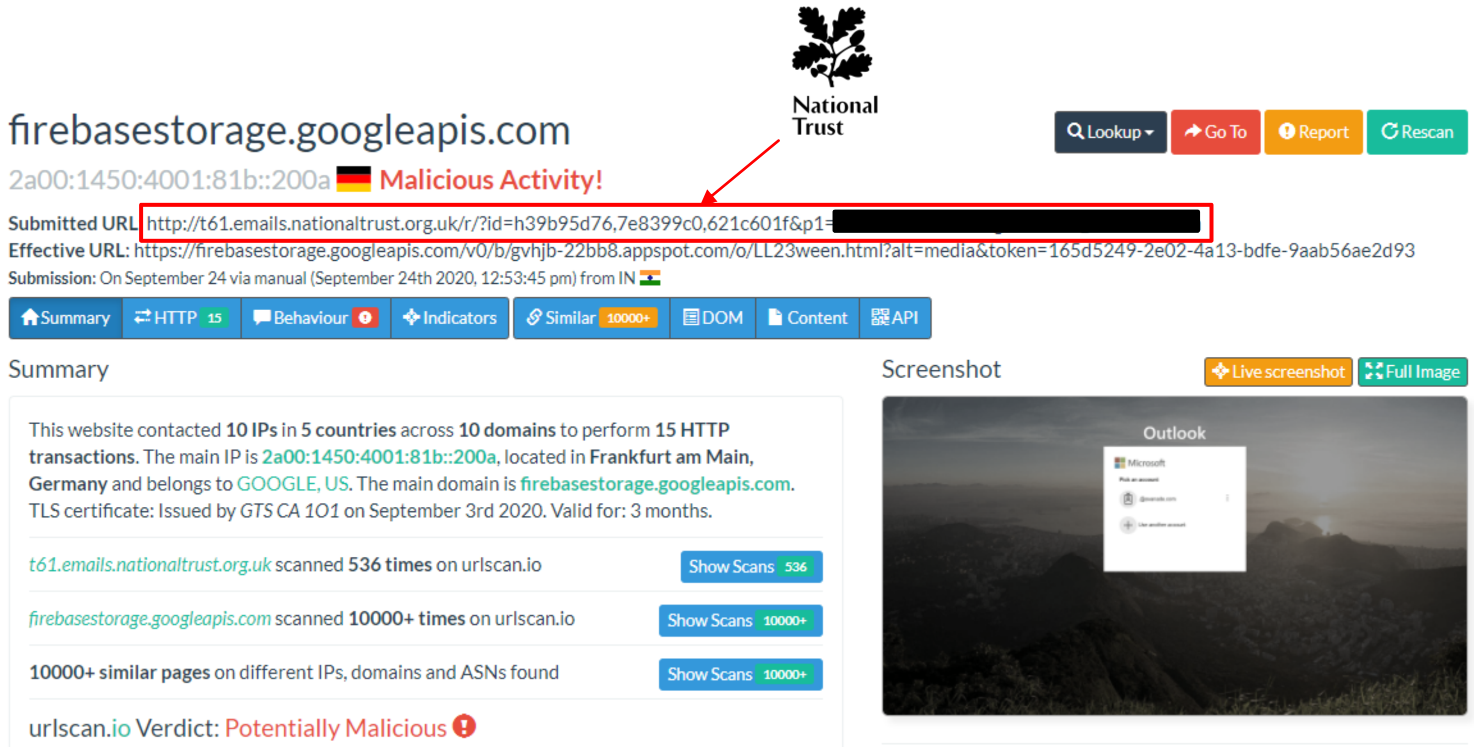
Login

hxxps://public.3.basecamp[.]com/p/6WvTkPssC6sxWf7qM1jMhLiY/upload/download/Review_Report15-10.exe

TWILIO SendGrid → Google Docs → aws Trello → BazarLoader

hxxps://trello-attachments.s3.amazonaws[.]com/5f9178701d651c5c6cc82707/5f91bab7cfea9309f8ed1c77/0dbd0d26d1185530a7813a7ab0567594/Report-Review22-10.exe

EVASION



National Trust

firebasestorage.googleapis.com

2a00:1450:4001:81b::200a Malicious Activity!

Submitted URL http://t61.emails.nationaltrust.org.uk/r/?id=h39b95d76,7e8399c0,621c601f&p1=[redacted]

Effective URL: https://firebasestorage.googleapis.com/v0/b/gvhjb-22bb8.appspot.com/o/LL23ween.html?alt=media&token=165d5249-2e02-4a13-bdfe-9aab56ae2d93

Submission: On September 24 via manual (September 24th 2020, 12:53:45 pm) from IN

Summary

This website contacted **10 IPs** in **5 countries** across **10 domains** to perform **15 HTTP transactions**. The main IP is 2a00:1450:4001:81b::200a, located in **Frankfurt am Main, Germany** and belongs to GOOGLE, US. The main domain is firebasestorage.googleapis.com. TLS certificate: Issued by *GTS CA 1O1* on September 3rd 2020. Valid for: 3 months.

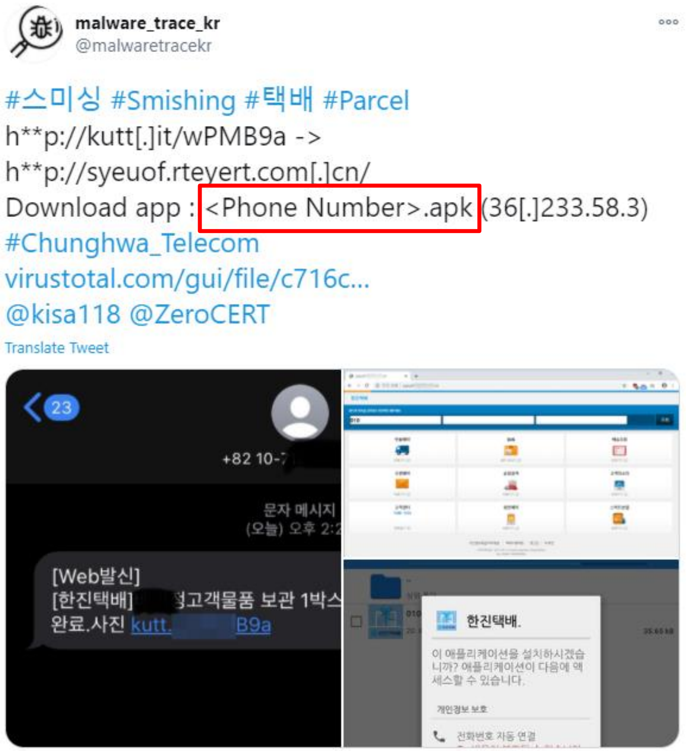
t61.emails.nationaltrust.org.uk scanned **536 times** on urlscan.io — Show Scans 536

firebasestorage.googleapis.com scanned **10000+ times** on urlscan.io — Show Scans 10000+

10000+ similar pages on different IPs, domains and ASNs found — Show Scans 10000+

urlscan.io Verdict: Potentially Malicious

Screenshot



malware_trace_kr
@malwaretracekr

#스미싱 #Smishing #택배 #Parcel
h**p://kutt[.]it/wPMB9a ->
h**p://syeuof.rteyert.com[.]cn/
Download app : <Phone Number>.apk (36[.]233.58.3)
#Chunghwa_Telecom
virustotal.com/gui/file/c716c...
@kisa118 @ZeroCERT

Translate Tweet

+82 10-7[redacted]

문자 메시지
(오늘) 오후 2:2

[Web발신]
[한진택배] [redacted]렇고객물품 보관 1박스
완료.사진 kutt.[redacted]B9a

한진택배.

이 애플리케이션을 설치하시겠습니까? 애플리케이션이 다음에 액세스할 수 있습니다.

개인정보 보호

전화번호 자동 연결

https://

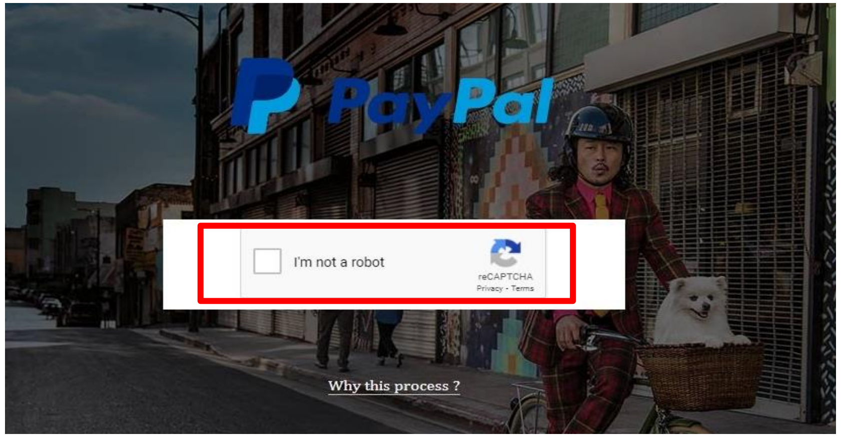
Let's Encrypt

SECURED BY SECTIGO

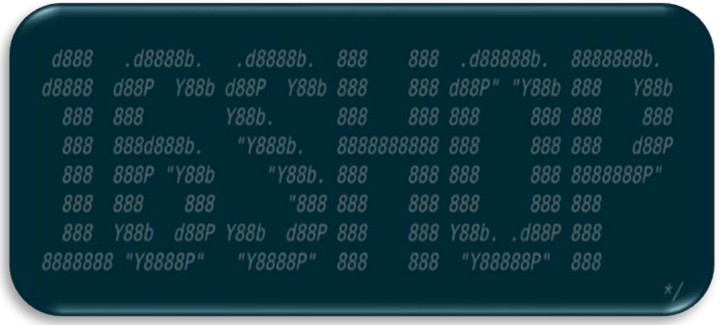
.secure-pay.

namecheap

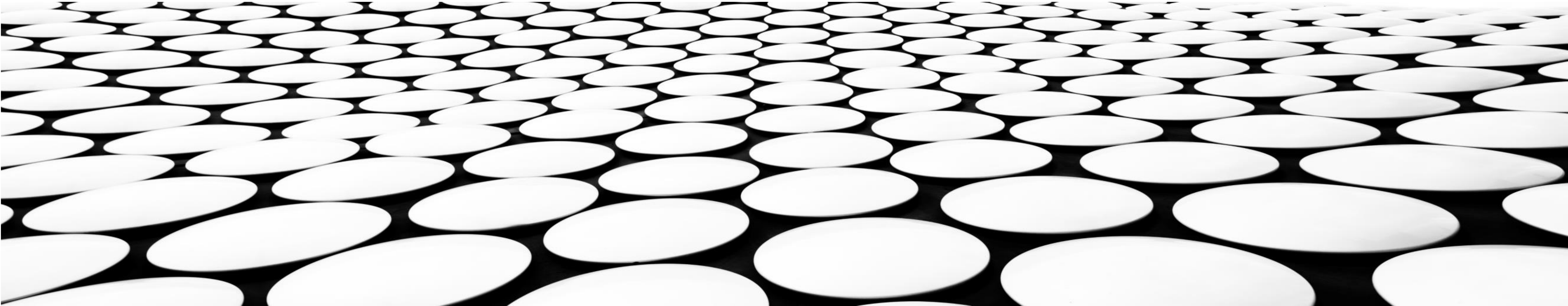
Alibaba Group
阿里巴巴集团



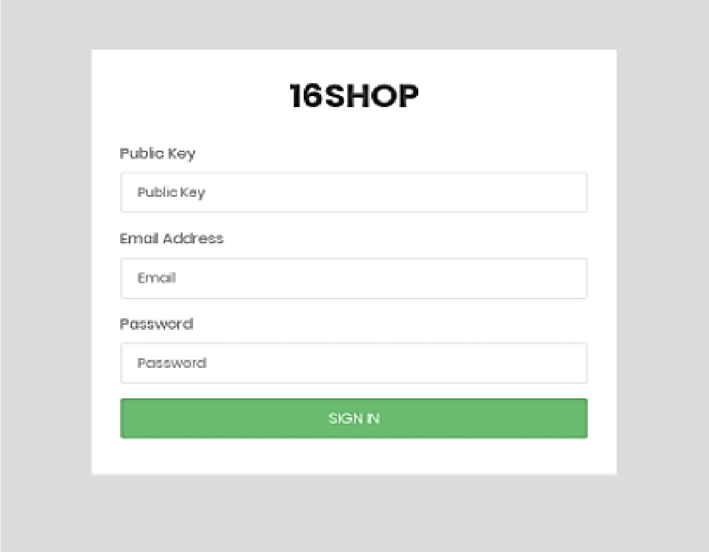
ORGANISED CYBERCRIME



```
 d888    .d8888b.   .d8888b.  888    888  .d88888b.  8888888b. 
d8888   d88P  Y88b d88P  Y88b 888    888 d88P" "Y88b 888   Y88b
  888   888        Y88b.      888    888 888     888 888    888
  888   888d888b.   "Y888b.   8888888888 888     888 888   d88P
  888   888P "Y88b     "Y88b. 888    888 888     888 8888888P" 
  888   888    888       "888 888    888 888     888 888       
  888   Y88b  d88P Y88b  d88P 888    888 Y88b. .d88P 888       
8888888  "Y8888P"   "Y8888P"  888    888  "Y88888P"  888       
                                                            */
```



PHISHING-AS-A-SERVICE



16SHOP

Public Key

Public Key

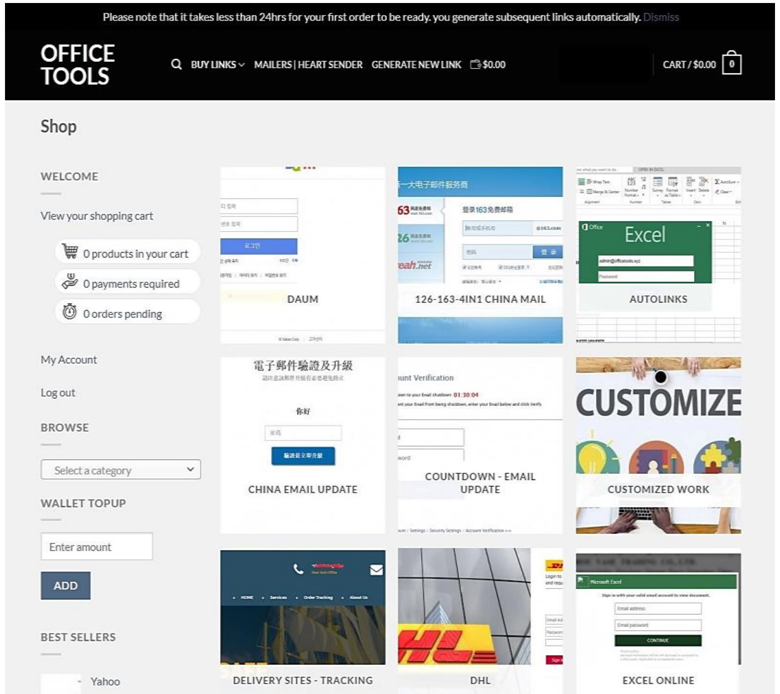
Email Address

Email

Password

Password

SIGN IN



Please note that it takes less than 24hrs for your first order to be ready. you generate subsequent links automatically. Dismiss

OFFICE TOOLS

BUY LINKS | MAILERS | HEART SENDER | GENERATE NEW LINK | $0.00 | CART / $0.00 | 0

Shop

WELCOME

View your shopping cart

- 0 products in your cart
- 0 payments required
- 0 orders pending

My Account

Log out

BROWSE

Select a category

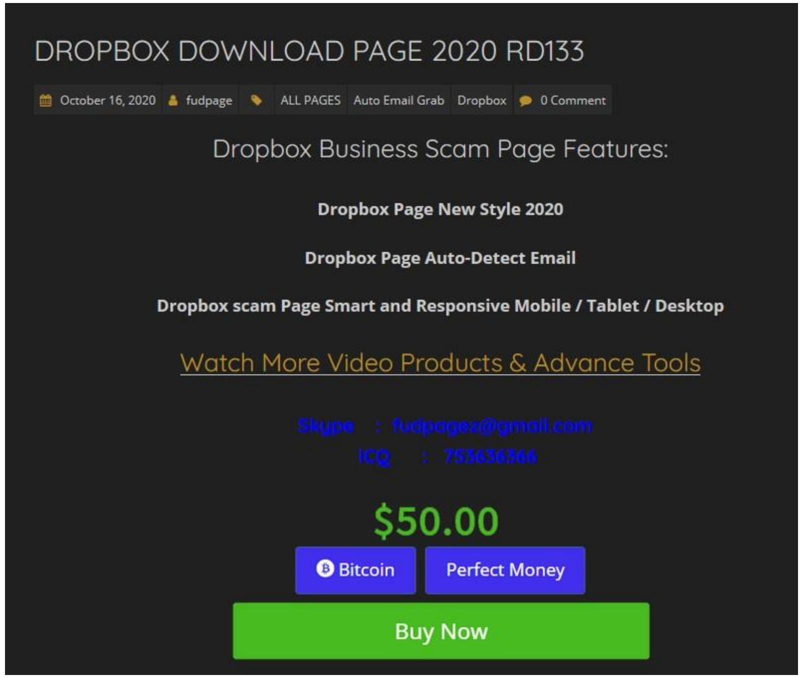
WALLET TOPUP

Enter amount

ADD

BEST SELLERS

Yahoo



DROPBOX DOWNLOAD PAGE 2020 RD133

October 16, 2020 | fudpage | ALL PAGES | Auto Email Grab | Dropbox | 0 Comment

Dropbox Business Scam Page Features:

Dropbox Page New Style 2020

Dropbox Page Auto-Detect Email

Dropbox scam Page Smart and Responsive Mobile / Tablet / Desktop

Watch More Video Products & Advance Tools

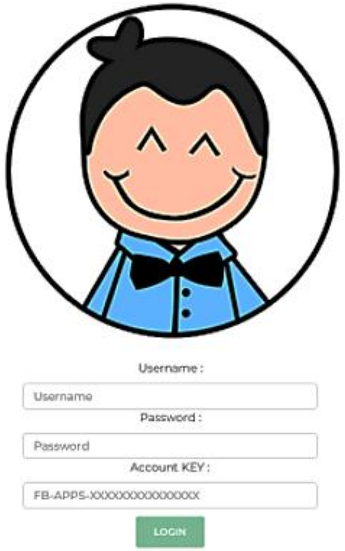
Skype : fudpagez@gmail.com

ICQ : 753636366

$50.00

Bitcoin | Perfect Money

Buy Now



Username :

Username

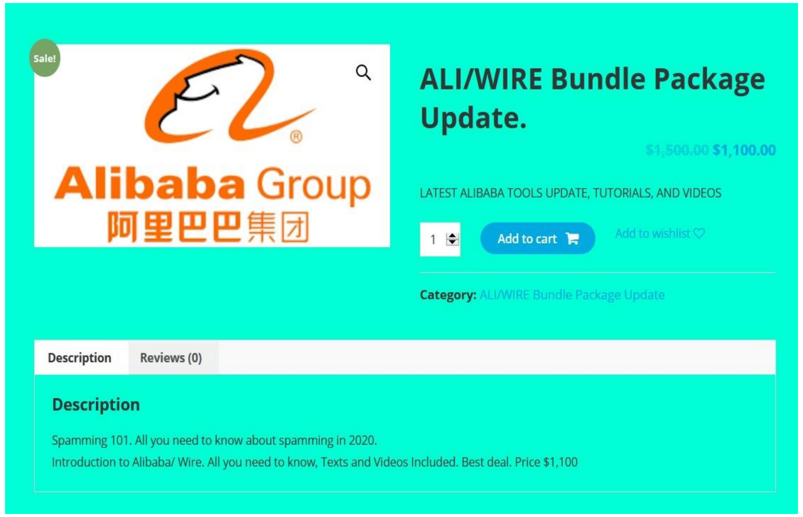
Password :

Password

Account KEY :

FB-APPS-XXXXXXXXXXXXXXX

LOGIN



ALI/WIRE Bundle Package Update.

~~$1,500.00~~ $1,100.00

LATEST ALIBABA TOOLS UPDATE, TUTORIALS, AND VIDEOS

1 | Add to cart | Add to wishlist ♡

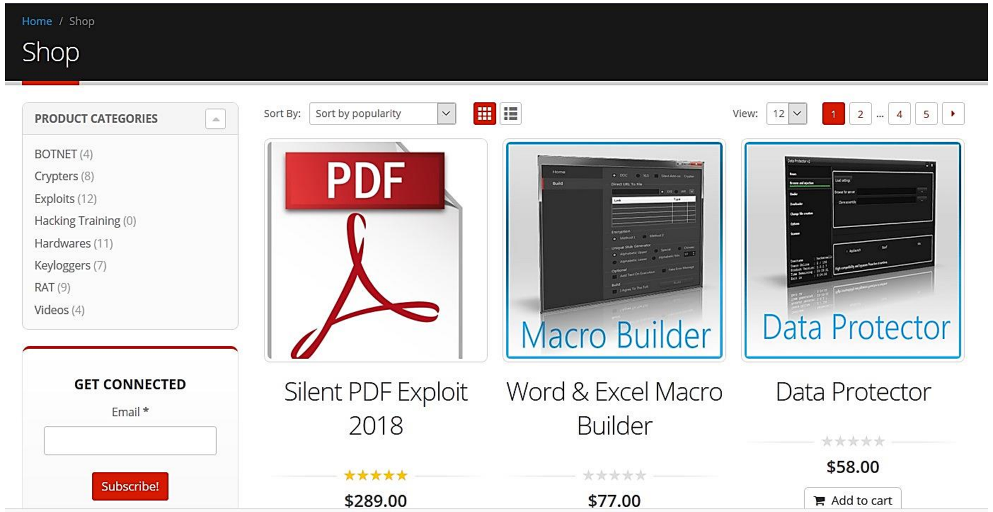
Category: ALI/WIRE Bundle Package Update

Description | Reviews (0)

Description

Spamming 101. All you need to know about spamming in 2020.

Introduction to Alibaba/ Wire. All you need to know, Texts and Videos Included. Best deal. Price $1,100



Home / Shop

Shop

PRODUCT CATEGORIES

- BOTNET (4)
- Crypters (8)
- Exploits (12)
- Hacking Training (0)
- Hardwares (11)
- Keyloggers (7)
- RAT (9)
- Videos (4)

GET CONNECTED

Email *

Subscribe!

Sort By: Sort by popularity

View: 12 | 1 | 2 | ... | 4 | 5

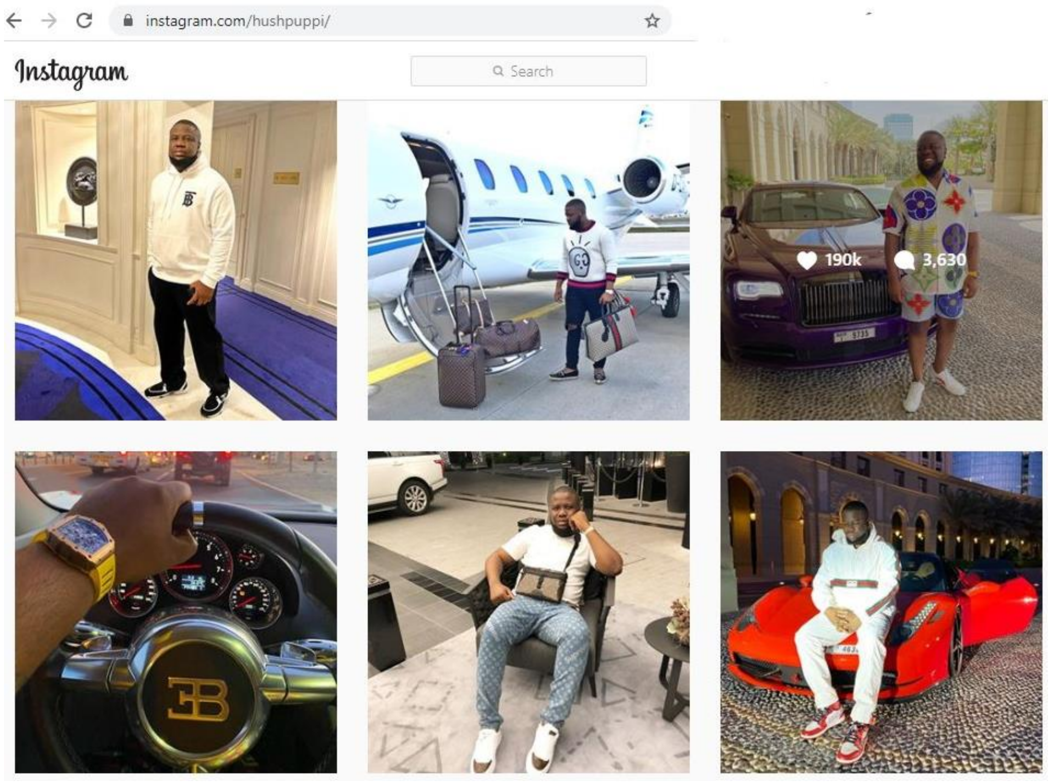
Silent PDF Exploit 2018 ★★★★★ $289.00

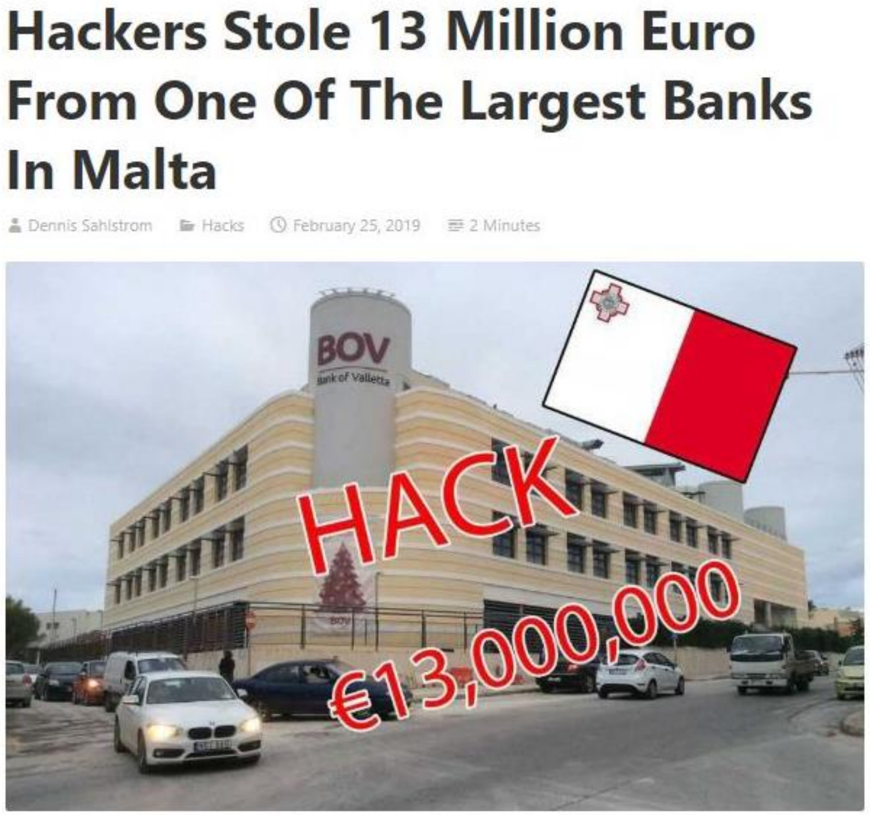
Word & Excel Macro Builder ★★★★★ $77.00

Data Protector ★★★★★ $58.00 Add to cart

BUSINESS EMAIL COMPROMISE

- Ray Hushpuppi, a Dubai-based Nigerian BEC scammer, was arrested by Dubai police in June 2020, in a case called **Operation Fox Hunt 2**.
- Responsible for stealing millions of USD via BEC attacks against large enterprises, such as *a* US law firm, a foreign bank, and an English Premier League football club.





Hackers Stole 13 Million Euro From One Of The Largest Banks In Malta

Dennis Sahlstrom   Hacks   February 25, 2019   2 Minutes

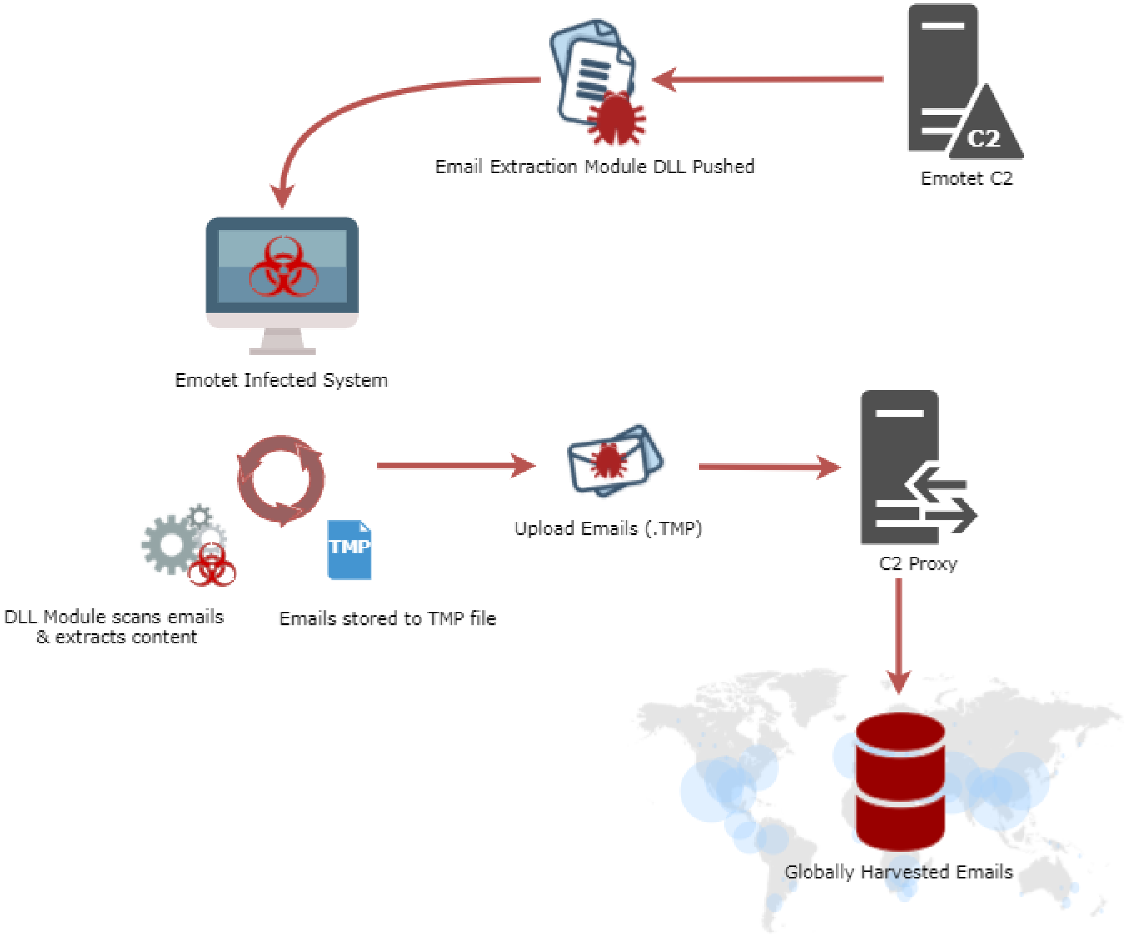
- The **Hushpuppi Indictment** revealed how BEC scammers work with Russian cybercriminal gangs, such as **FIN7,** to launder stolen funds from elaborate bank heists.

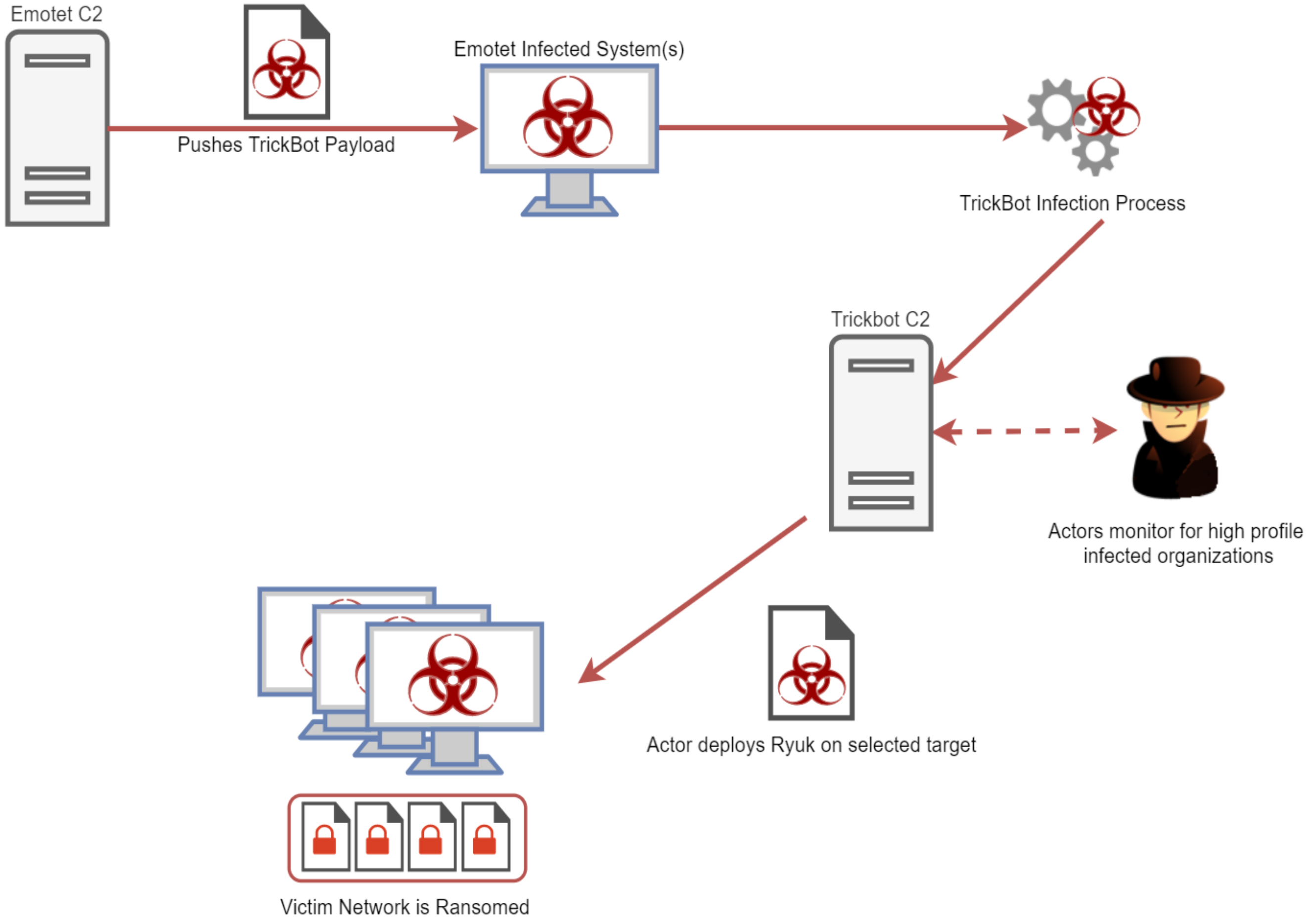
>

MUMMY SPIDER

EMOTET SPAM BOTNET

WIZARD SPIDER

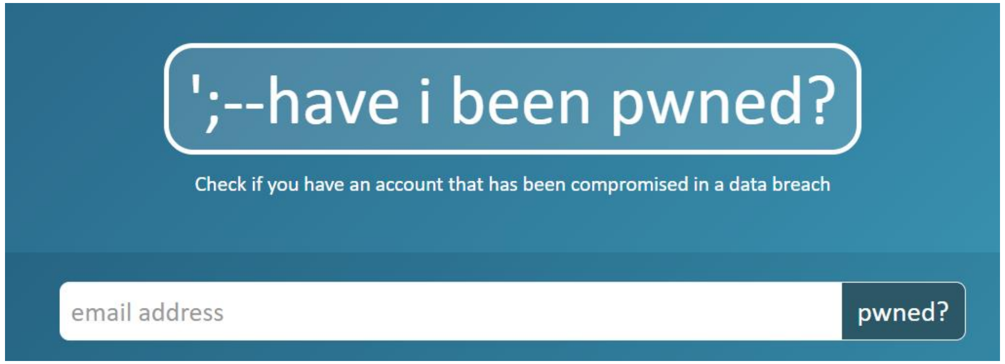

Email Extraction Module DLL Pushed
C2
Emotet C2
Emotet Infected System
DLL Module scans emails & extracts content
TMP
Emails stored to TMP file
Upload Emails (.TMP)
C2 Proxy
Globally Harvested Emails


Emotet C2
Pushes TrickBot Payload
Emotet Infected System(s)
TrickBot Infection Process
Trickbot C2
Actors monitor for high profile infected organizations
Actor deploys Ryuk on selected target
Victim Network is Ransomed

MITIGATION

- MFA/2FA – Prevents compromise if credentials are stolen
- Block List – Add malicious domains to protection systems
- Takedown Requests – Identify the host/registrar and submit a takedown
- Password Security – Password Resets / Password Formula
- Anti-Malware Best Practices – Updated Software, Logging, and Isolate Infected Systems
- Simulation – Red Team tests to identify weaknesses
- Awareness Training – Onboarding security training & simple to report something
- Email Forwarding Rules – Usually the first thing an attacker will setup (so check them!)

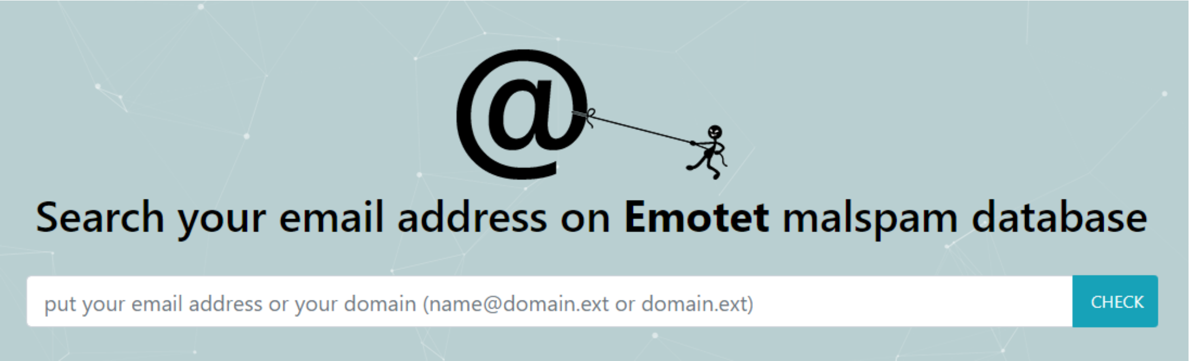
haveibeenpwned.com



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

haveibeenemotet.com



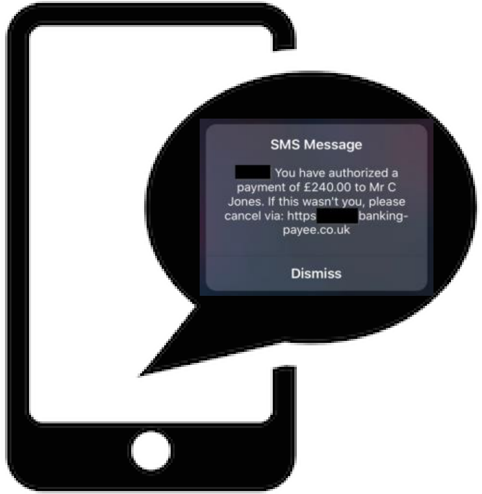
Search your email address on **Emotet** malspam database

put your email address or your domain (name@domain.ext or domain.ext)
CHECK

PREDICTIONS

- SMiShing – Traditional Phishing will eventually be overtaken by SMiShing
- TTPs – Upgraded and deployed in new geographies

- Collaborative Applications – Email comms now done on Teams & Slack + Zoom & WebEx
- Increased Losses – In 2019, the FBI's IC3 received 23,775 BEC complaints with adjusted losses of over **$1.7 billion**.



SMS Message

[redacted] You have authorized a payment of £240.00 to Mr C Jones. If this wasn't you, please cancel via: https[redacted]banking-payee.co.uk

Dismiss

FEDERAL BUREAU OF INVESTIGATION

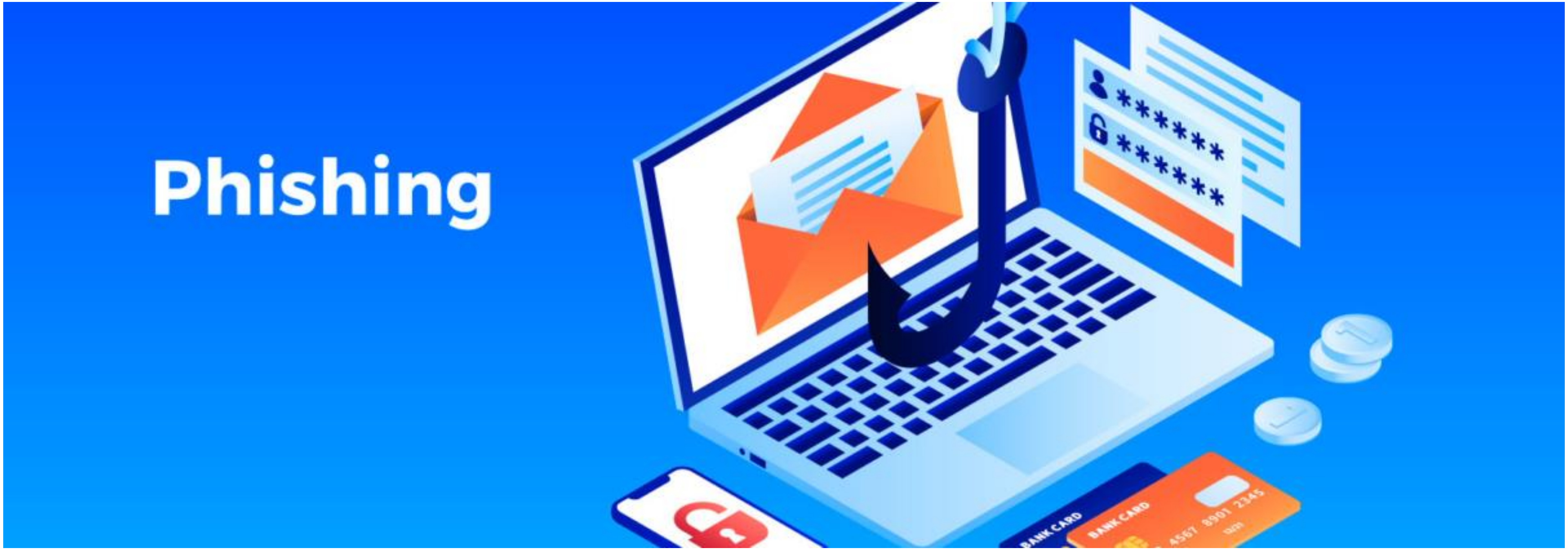
IC3

INTERNET CRIME COMPLAINT CENTER

Cisco webex

zoom

THANK YOU!



REFERENCES

- https://www.cyjax.com/2020/08/20/credential-harvesting-campaigns-target-governments-and-cybersecurity-companies/
- https://www.cyjax.com/2020/07/14/two-factor-fail-analysis-of-a-modern-phishing-kit/
- https://www.cyjax.com/2020/07/17/spam-campaign-using-discord-to-host-malware/
- https://blog.bushidotoken.net/2020/09/intelligence-analysis-report-attacks.html
- https://blog.bushidotoken.net/2020/05/gone-phishing.html
- https://blog.bushidotoken.net/2020/10/analysing-phishing-c-server.html
- https://phishunt.io/community/
- https://urlscan.io/search/#domain%3Anationaltrust.org.uk
- https://twitter.com/olihough86/status/1291347834650886145
- https://twitter.com/ian_kenefick/status/1319332152283115525
- https://twitter.com/ffforward/status/1318558802099273730
- https://twitter.com/malwaretracekr/status/1255805990865268736
- https://trends.netcraft.com/cybercrime/hosters
- https://trends.netcraft.com/cybercrime/certificate_authorities
- https://www.hornetsecurity.com/en/security-information/emotet-update-increases-downloads/
- https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return
- https://securityboulevard.com/2020/07/hushpuppi-and-mr-woodbery-bec-scammers-welcome-to-chicago/
- https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars
- https://us-cert.cisa.gov/ncas/alerts/TA18-201A
- https://paste.cryptolaemus.com/
- https://twitter.com/Cryptolaemus1
- https://pdf.ic3.gov/2019_IC3Report.pdf