Fake Office 365 Used for Phishing Attacks on C-Suite Targets

trendmicro.com/en_us/research/21/a/fake-office-365-used-for-phishing-attacks-on-c-suite-targets.html

January 25, 2021

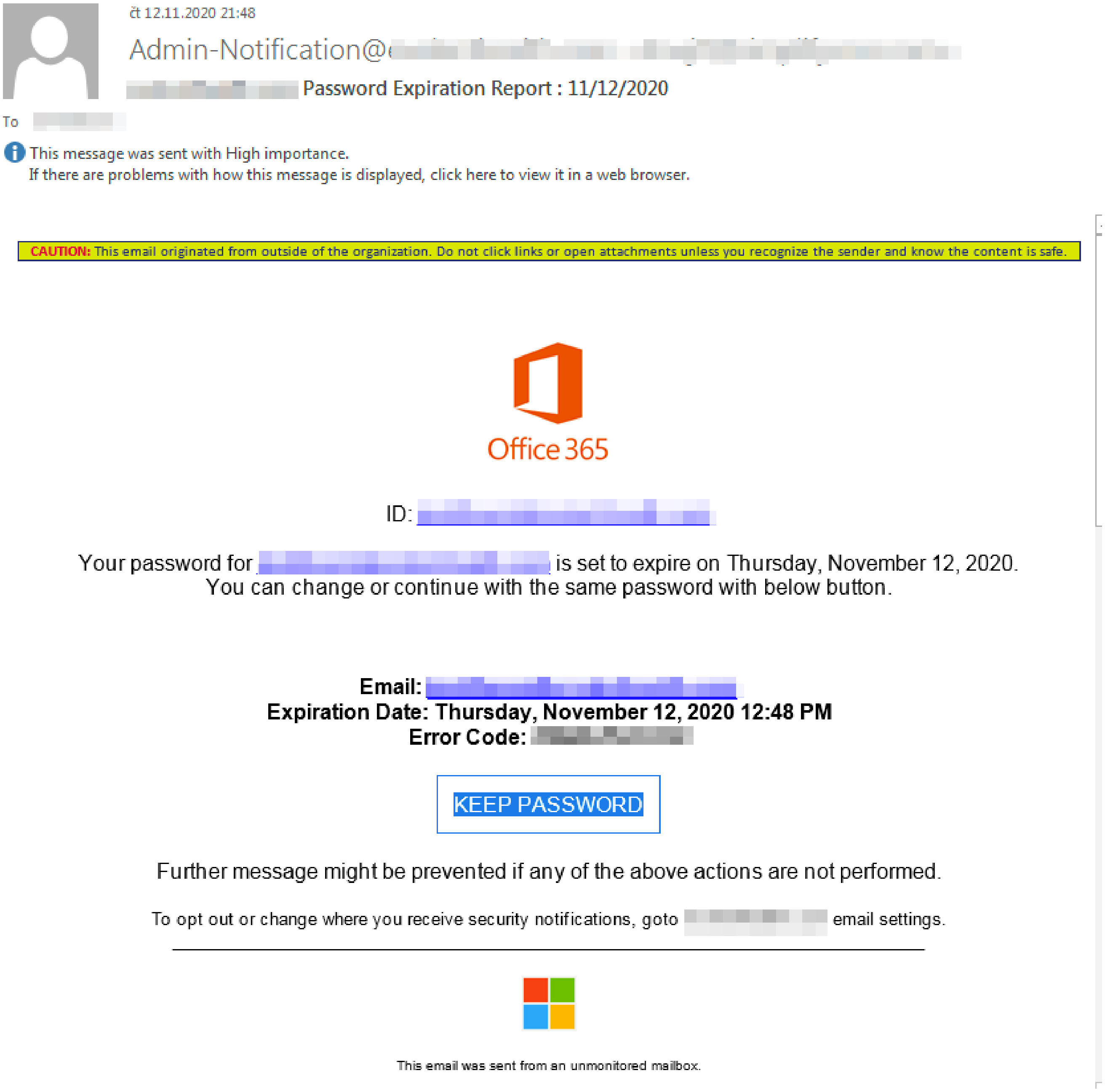
We have been following an evolving phishing campaign that targets high-ranking company executives since 2019, reusing compromised credentials and URLs to target more.

By: Matsukawa Bakuei, Marshall Chen, Vladimir Kropotov, Loseway Lu, Fyodor Yarochkin
January 25, 2021 Read time: (words)

We have been following an evolving phishing campaign that targets high-ranking company executives since May 2020. The attackers reuse compromised hosts for the phishing pages targeting organizations in the manufacturing, real estate, finance, government, and technological industries in several countries such as Japan, the United States, UK, Canada, Australia, and Europe. As of this writing, we found over 300 unique compromised URLs and 70 email addresses from eight compromised sites, including 40 legitimate emails of company CEOs, directors, owners, and founders, among other enterprise employee targets. We are now working with the respective authorities for further investigation.

Luring victims with compromised infrastructure

We observed the attackers targeting potential victims with emails containing fake Office 365 password expiration reports as lures. They prompt the targets to click the embedded link in the email if they want to continue using the same password; choosing the “Keep Password” option leads the user to the phishing page.



čt 12.11.2020 21:48

Admin-Notification@[redacted]

[redacted] Password Expiration Report : 11/12/2020

To [redacted]

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

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Office 365

ID: [redacted]

Your password for [redacted] is set to expire on Thursday, November 12, 2020.
You can change or continue with the same password with below button.

Email: [redacted]
Expiration Date: Thursday, November 12, 2020 12:48 PM
Error Code: [redacted]

KEEP PASSWORD

Further message might be prevented if any of the above actions are not performed.

To opt out or change where you receive security notifications, goto [redacted] email settings.

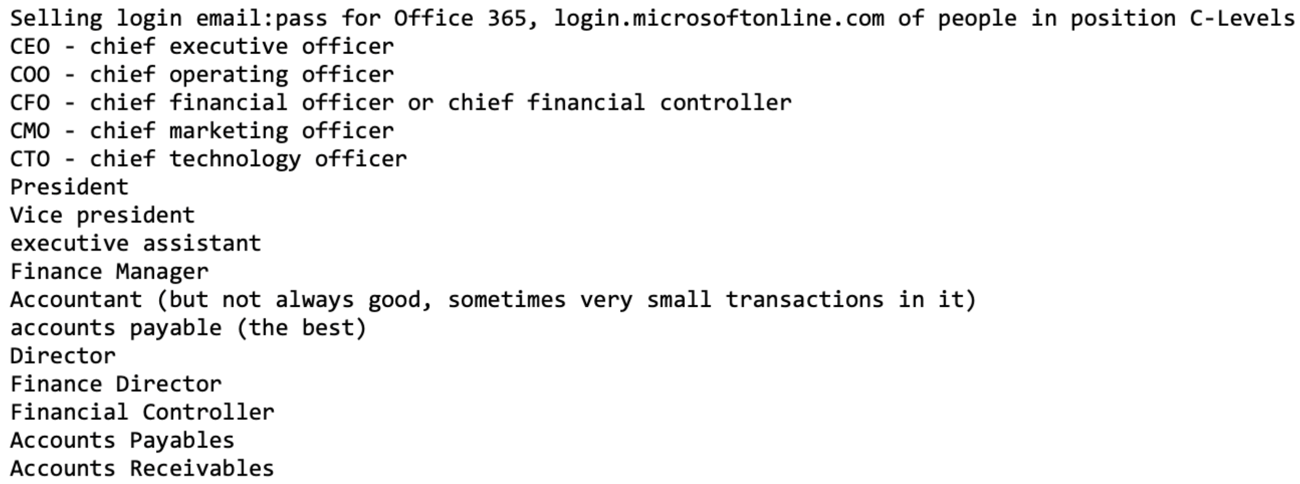
This email was sent from an unmonitored mailbox.

Figure 1. An MS Office365 password reset email and link is used as the phishing campaign lure.

The attackers are reusing compromised infrastructure and victims’ account credentials to host phishing pages and gain more victims, as briefly reported last year. The kit, which is available for sale, can validate the credentials’ details and accuracy once the victim interacts with the embedded link.

Related to this, during examination of underground activities we identified several advertisements by cybercriminals selling account credentials of CEOs, chief financial officers (CFOs), and finance department members, among others. Those posts were seen in multiple

English- and Russian-speaking forums, including an underground forum that seemingly matched with another user’s . Notably, all posts on the Russian-speaking forums were done in English and using recently registered accounts. We observed these users offering compromised MS Office 365 account credentials and the employees’ respective company positions.



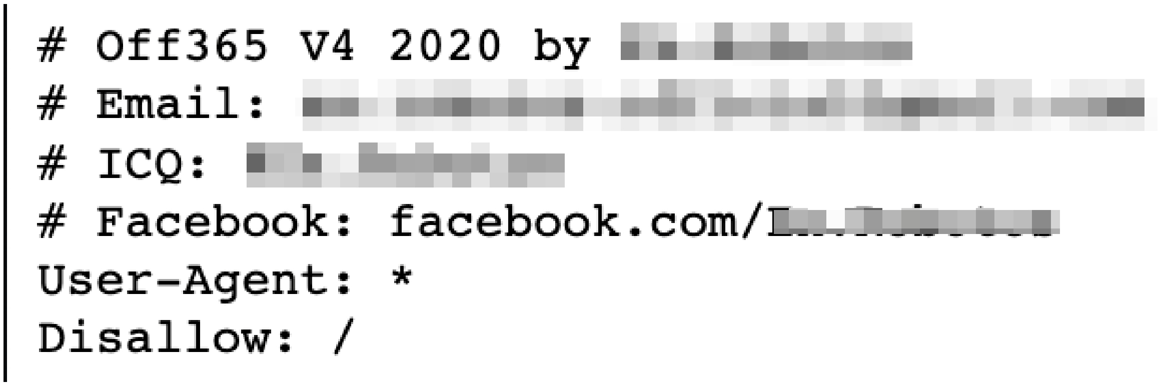
```
Selling login email:pass for Office 365, login.microsoftonline.com of people in position C-Levels
CEO - chief executive officer
COO - chief operating officer
CFO - chief financial officer or chief financial controller
CMO - chief marketing officer
CTO - chief technology officer
President
Vice president
executive assistant
Finance Manager
Accountant (but not always good, sometimes very small transactions in it)
accounts payable (the best)
Director
Finance Director
Financial Controller
Accounts Payables
Accounts Receivables
```

Figure 2. Underground forum message offering compromised account credentials.

Phishing kit

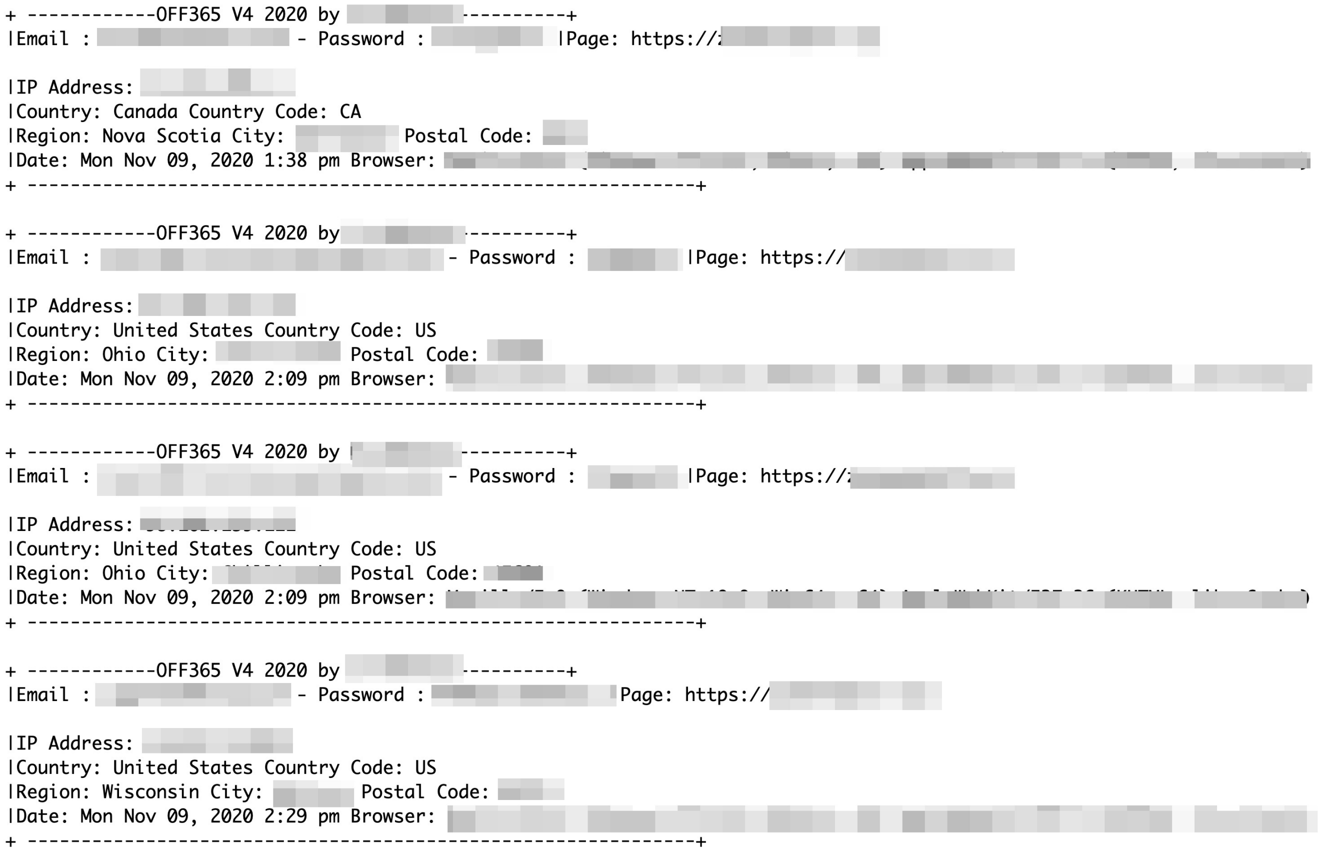
The campaign orchestrators used the same phishing kit during the campaigns. We observed that some of the sites that hosted the phishing kit were not configured properly. This exposed content of the directory, allowing the download of the phishing kit and associated log files without authentication. This also allowed us to get additional insights on the campaign and find evidence for potential attribution of the kits in their different deployment locations.

This discovery led us to believe that the kit developer’s previous projects served as precursor features that contributed to the Office 365 phishing kit versions subsequently sold in the underground. However, as we further examined the developer’s profile, we found odd behaviors that may warrant further technical and legal investigation.



```
# Off365 V4 2020 by [redacted]
# Email: [redacted]
# ICQ: [redacted]
# Facebook: facebook.com/[redacted]
User-Agent: *
Disallow: /
```

Figure 3. Potential attribution found in log files.



```
+ ------------OFF365 V4 2020 by [redacted]----------+
|Email : [redacted] - Password : [redacted] |Page: https://[redacted]

|IP Address: [redacted]
|Country: Canada Country Code: CA
|Region: Nova Scotia City: [redacted] Postal Code: [redacted]
|Date: Mon Nov 09, 2020 1:38 pm Browser: [redacted]
+ --------------------------------------------------------------+

+ ------------OFF365 V4 2020 by [redacted]----------+
|Email : [redacted] - Password : [redacted] |Page: https://[redacted]

|IP Address: [redacted]
|Country: United States Country Code: US
|Region: Ohio City: [redacted] Postal Code: [redacted]
|Date: Mon Nov 09, 2020 2:09 pm Browser: [redacted]
+ --------------------------------------------------------------+

+ ------------OFF365 V4 2020 by [redacted]----------+
|Email : [redacted] - Password : [redacted] |Page: https://[redacted]

|IP Address: [redacted]
|Country: United States Country Code: US
|Region: Ohio City: [redacted] Postal Code: [redacted]
|Date: Mon Nov 09, 2020 2:09 pm Browser: [redacted]
+ --------------------------------------------------------------+

+ ------------OFF365 V4 2020 by [redacted]----------+
|Email : [redacted] - Password : [redacted] Page: https://[redacted]

|IP Address: [redacted]
|Country: United States Country Code: US
|Region: Wisconsin City: [redacted] Postal Code: [redacted]
|Date: Mon Nov 09, 2020 2:29 pm Browser: [redacted]
+ --------------------------------------------------------------+
```

Figure 4. Improperly configured log files detailing the phishing sites to which the victims were redirected and their personally identifiable information (emails, passwords, city, and system information).

Emailing using third-party RDP

We looked at the email headers of the lure email samples, examined the SMTP headers, and found an interesting detail: most of the phishing emails were sent using a virtual private server (VPS) from FireVPS.

from FireVPS-RDP (XX.X.XXX.XX) by

from FireVPS-RDP (XXX.XXX.XX.XXX) by

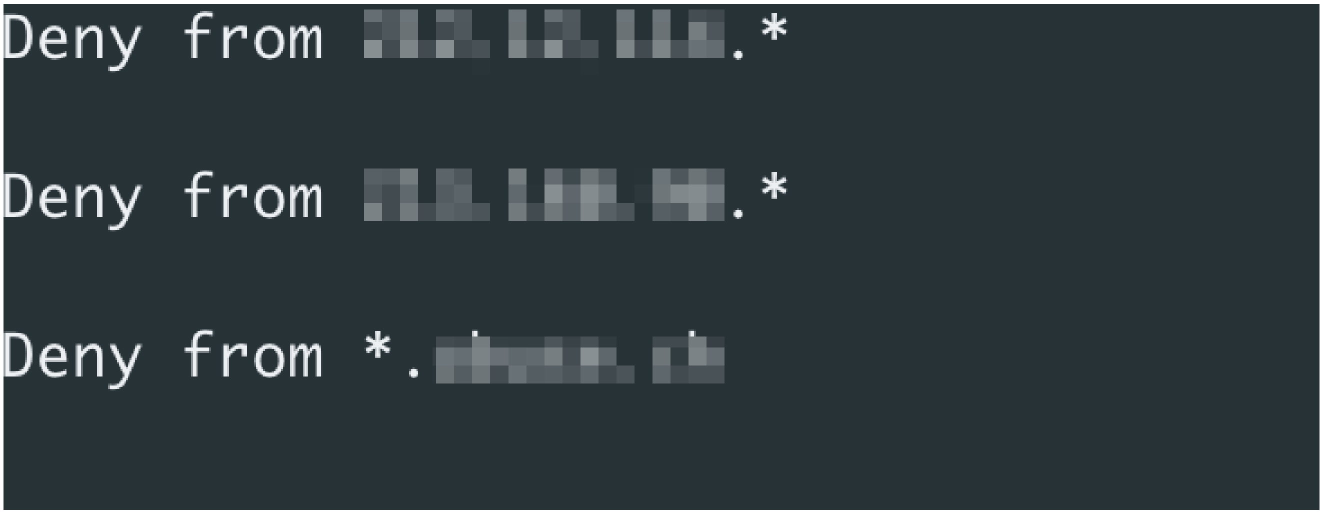
from FireVPS-RDP (XX.XXX.XXX.XX) by
OL1P279CA0064.NORP279.PROD.OUTLOOK.COM (2603:10a6:e10:15::15) with
Microsoft SMTP

FireVPS is a virtual private server (VPS) offering a range of Windows remote desktop protocol (RDP) plans for their respective customers. The emails sent to the victims are sent from the RDP service. We have alerted FireVPS of this and have yet to hear from them.

While scanning other email samples for emails sent from a FireVPS-RDP machine, we found similar phishing email templates and the URL that was sent to a financial department member also contained the recipient’s information and credentials. An online search revealed that the recipient’s profile and email address matched the accurate information listed on his LinkedIn account.

Phishing kit blocklist

We think the phishing kit developer spent considerable time compiling the blocklist included in the kit. It uses an extensive list of domain names and IP address ranges to ensure that access is blocked when accessed by security companies or large cloud providers. We assume the intention is to evade detection by security vendors as the list includes a number of antivirus companies; Google, Microsoft, VirusTotal, and a long list of other cybersecurity and technology companies, as well as public blocklisting sites.



```
Deny from [redacted].*

Deny from [redacted].*

Deny from *.[redacted]
```

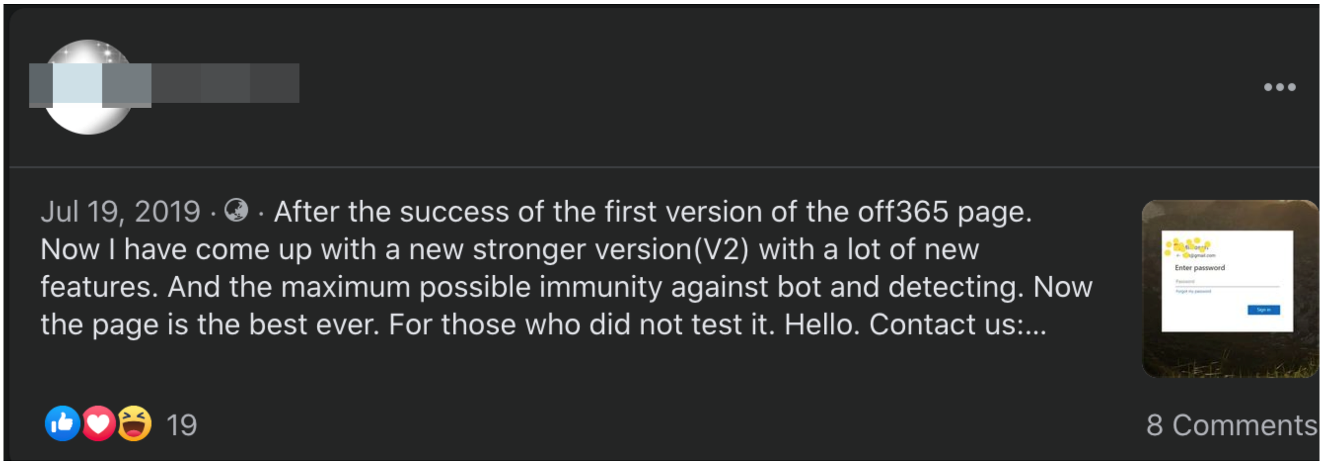
Figure 5. The phishing kit developer made an effort to add specific IP addresses to a blocklist evade detection.

Keeping this in mind, we find it ironic that the kit developer would take this much time to create a blocklist while actively marketing the kit on social network site(s).

Previous versions of the phishing kit

The phishing kit we observed in this campaign is the fourth iteration of the toolkit. Previous versions were noticed and are known to the cybersecurity community, since it was widely advertised in the underground and on social media.

According to the malware developer’s “business” Facebook page, the first version of the phishing kit was released on July 4, 2019, shortly followed by the second version (V2) 15 days after. The third version (V3) was not officially announced on the Facebook page but was observed to be in circulation and could be found through a simple online search.



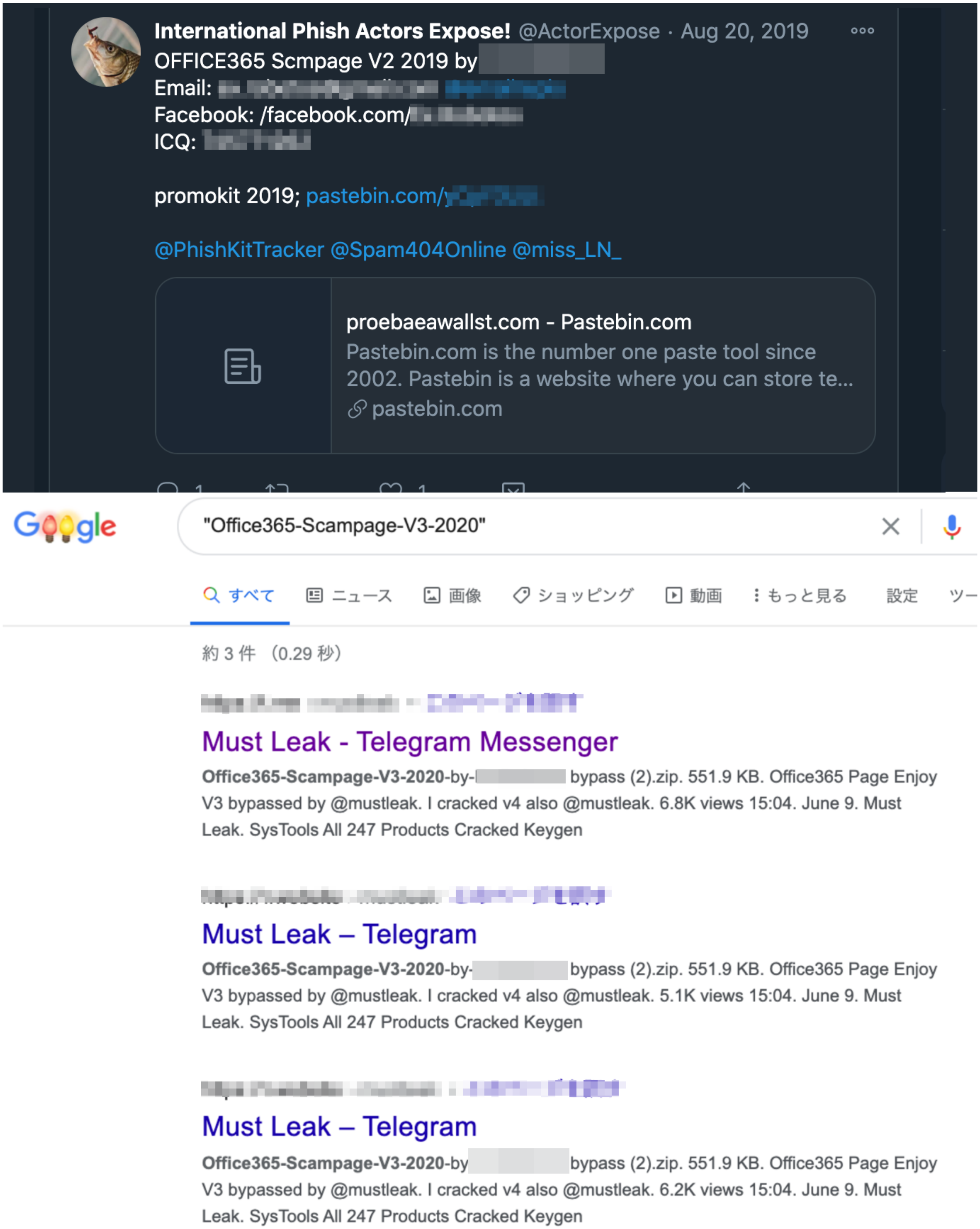
[redacted]

Jul 19, 2019 · · After the success of the first version of the off365 page. Now I have come up with a new stronger version(V2) with a lot of new features. And the maximum possible immunity against bot and detecting. Now the page is the best ever. For those who did not test it. Hello. Contact us:...

19

8 Comments

Figure 6. Malware developer advertising the second version of the fake Office365 phishing kit on his social media page.



International Phish Actors Expose! @ActorExpose · Aug 20, 2019

OFFICE365 Scmpage V2 2019 by [redacted]
Email: [redacted]
Facebook: /facebook.com/[redacted]
ICQ: [redacted]

promokit 2019; pastebin.com/[redacted]

@PhishKitTracker @Spam404Online @miss_LN_

proebaeawallst.com - Pastebin.com
Pastebin.com is the number one paste tool since 2002. Pastebin is a website where you can store te...
pastebin.com

"Office365-Scampage-V3-2020"

約 3 件 （0.29 秒）

[redacted]
Must Leak - Telegram Messenger
Office365-Scampage-V3-2020-by-[redacted] bypass (2).zip. 551.9 KB. Office365 Page Enjoy V3 bypassed by @mustleak. I cracked v4 also @mustleak. 6.8K views 15:04. June 9. Must Leak. SysTools All 247 Products Cracked Keygen

[redacted]
Must Leak – Telegram
Office365-Scampage-V3-2020-by-[redacted] bypass (2).zip. 551.9 KB. Office365 Page Enjoy V3 bypassed by @mustleak. I cracked v4 also @mustleak. 5.1K views 15:04. June 9. Must Leak. SysTools All 247 Products Cracked Keygen

[redacted]
Must Leak – Telegram
Office365-Scampage-V3-2020-by[redacted] bypass (2).zip. 551.9 KB. Office365 Page Enjoy V3 bypassed by @mustleak. I cracked v4 also @mustleak. 6.2K views 15:04. June 9. Must Leak. SysTools All 247 Products Cracked Keygen

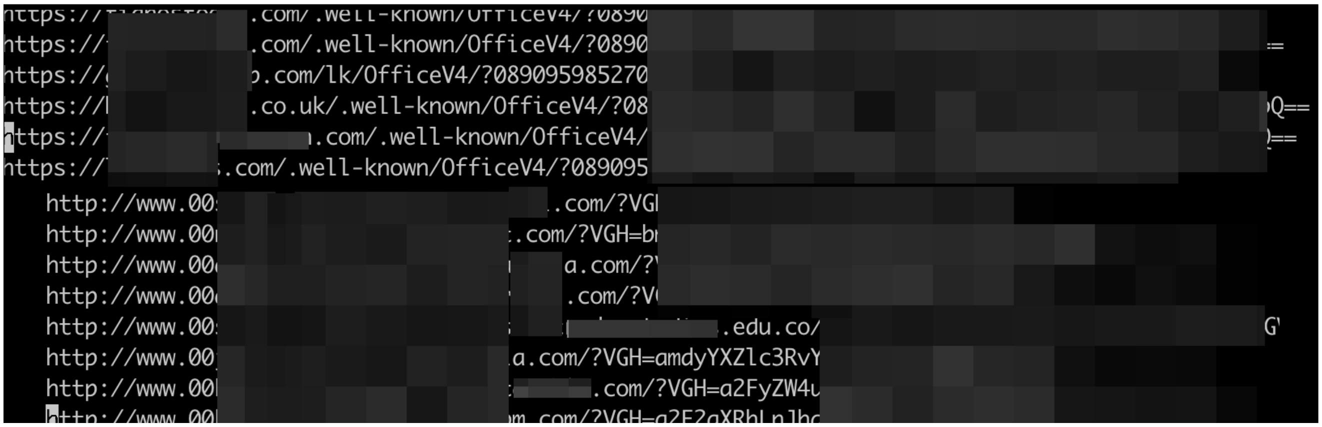
Figure 7. V2 and V3 of the phishing kit were reported in previous months and known among cybersecurity researchers.

Most of the lure’s content theme focuses on prompting the victims to keep their current passwords. A look at the campaigns' pattern shows that the first layer of the phishing link includes the recipient’s email domain in the compromised URLs' subdomain, followed by the

Base64 encoded string of the recipient's email. (The email does not always have to be base64 encoded, we also have seen landing pages with email being included in plaintext).

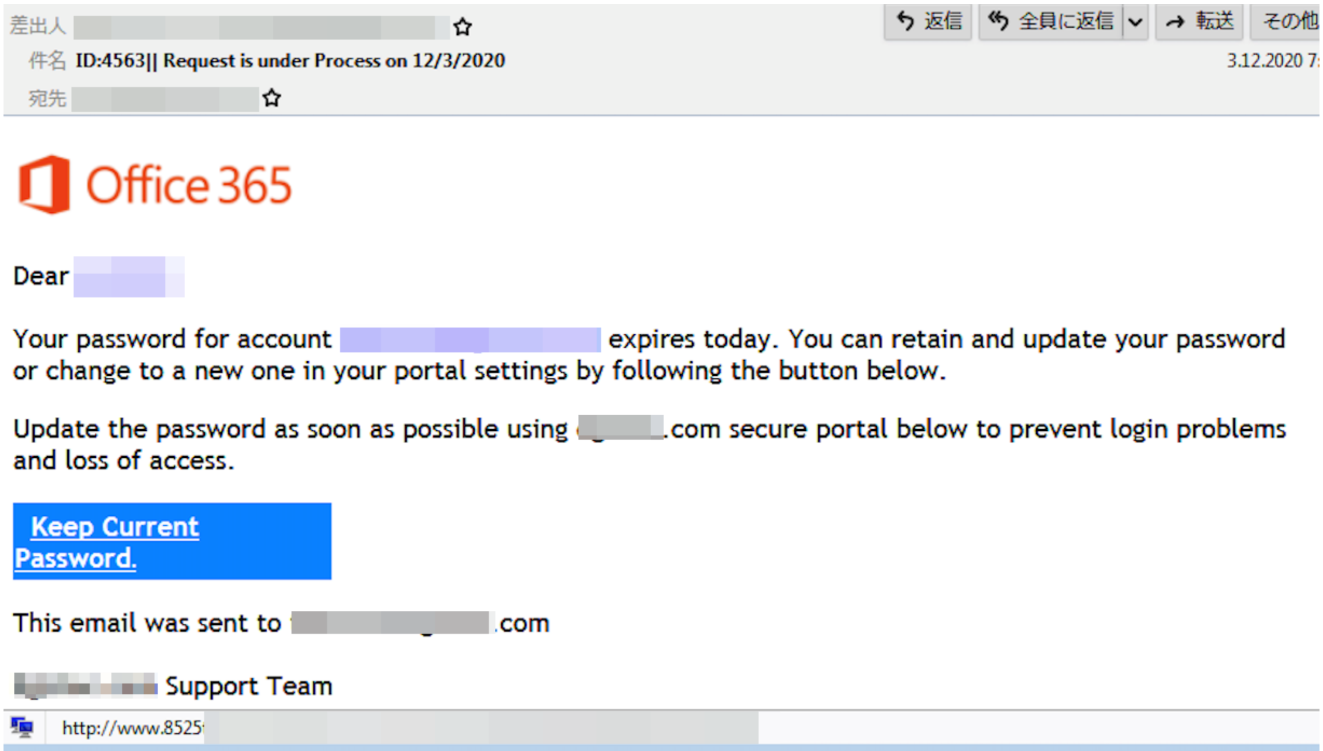
As the user chooses the link to keep their password, they are redirected to the phishing pages. We noticed that the current version the compromised URLs' landing pages started including the keyword "OfficeV4" in August.

By September, the victims' domain names were still included, but the prefixes were changed from "sg" to "pl," "00," and/or "ag." In another development in October, the victim's names were being included in the subdomain instead of the respective domain names.



```
https://[redacted].com/.well-known/OfficeV4/?0890[redacted]
https://[redacted].com/.well-known/OfficeV4/?0890[redacted]==
https://[redacted]o.com/lk/OfficeV4/?089095985270[redacted]
https://l[redacted].co.uk/.well-known/OfficeV4/?08[redacted]Q==
https://[redacted]n.com/.well-known/OfficeV4/[redacted]==
https://[redacted].com/.well-known/OfficeV4/?089095[redacted]
    http://www.00[redacted].com/?VG[redacted]
    http://www.00[redacted].com/?VGH=b[redacted]
    http://www.00[redacted]a.com/?[redacted]
    http://www.00[redacted].com/?V[redacted]
    http://www.00[redacted].edu.co/[redacted]G'
    http://www.00[redacted]a.com/?VGH=amdyYXZlc3RvY[redacted]
    http://www.00[redacted].com/?VGH=a2FyZW4u[redacted]
    http://www.00[redacted]om.com/?VGH=a2F2aXRhLnJhc[redacted]
```

Figure 8. Tracking part of the campaigns' domain developments



差出人 [redacted] ☆

件名 ID:4563|| Request is under Process on 12/3/2020

3.12.2020 7:

宛先 [redacted] ☆

Office 365

Dear [redacted]

Your password for account [redacted] expires today. You can retain and update your password or change to a new one in your portal settings by following the button below.

Update the password as soon as possible using [redacted].com secure portal below to prevent login problems and loss of access.

Keep Current Password.

This email was sent to [redacted].com

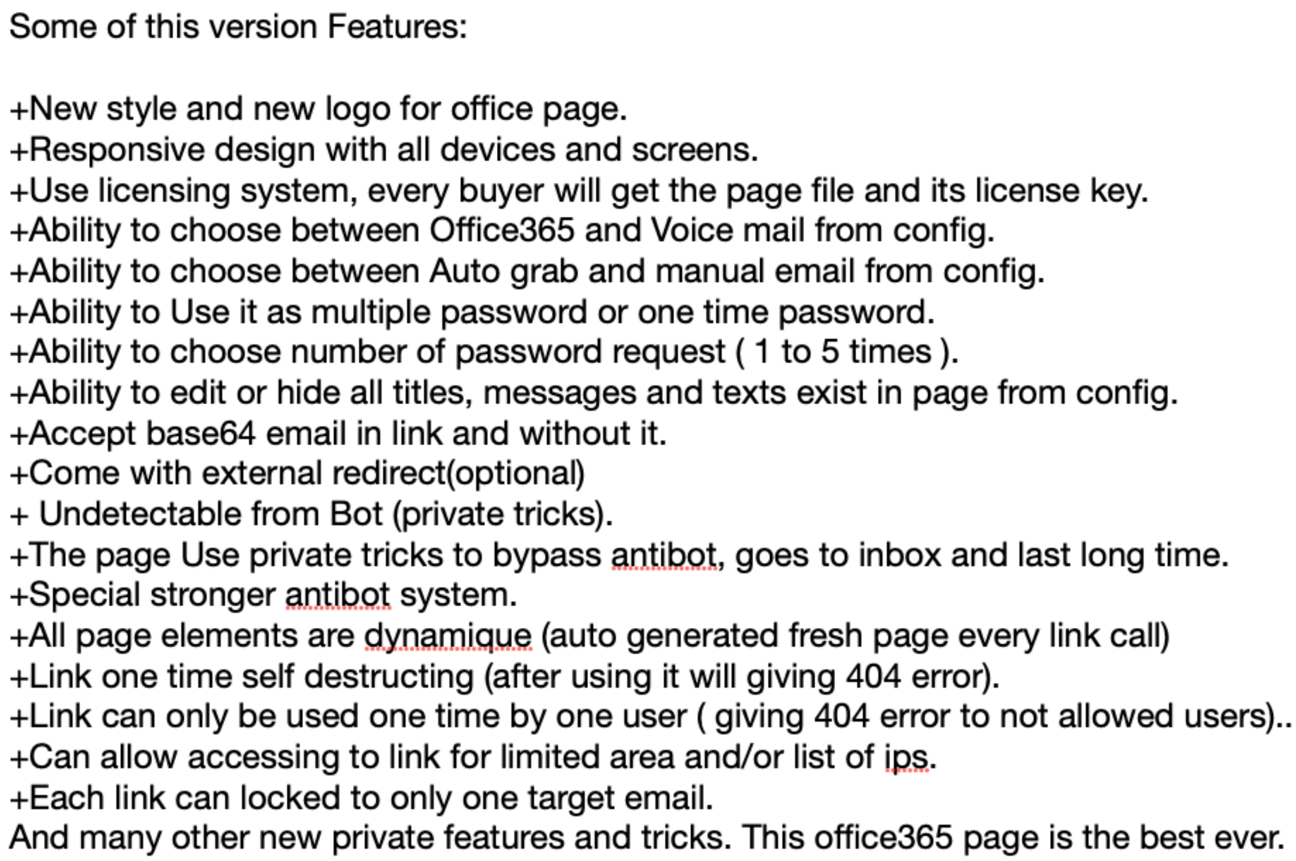
[redacted] Support Team

http://www.8525[redacted]

Figure 9. A common theme for all the versions: Messages that prompt the victim to click on the embedded link to keep their current password.

Notable features of the latest phishing kit

Aside from the blocklist, V4’s other features supposedly make the detection of this kit harder. Among them the capability to detect bot scanning or crawling attempts, and provide alternative content when bots are detected. Below are some of the features of V4 as listed by the kit developer on his Facebook page.

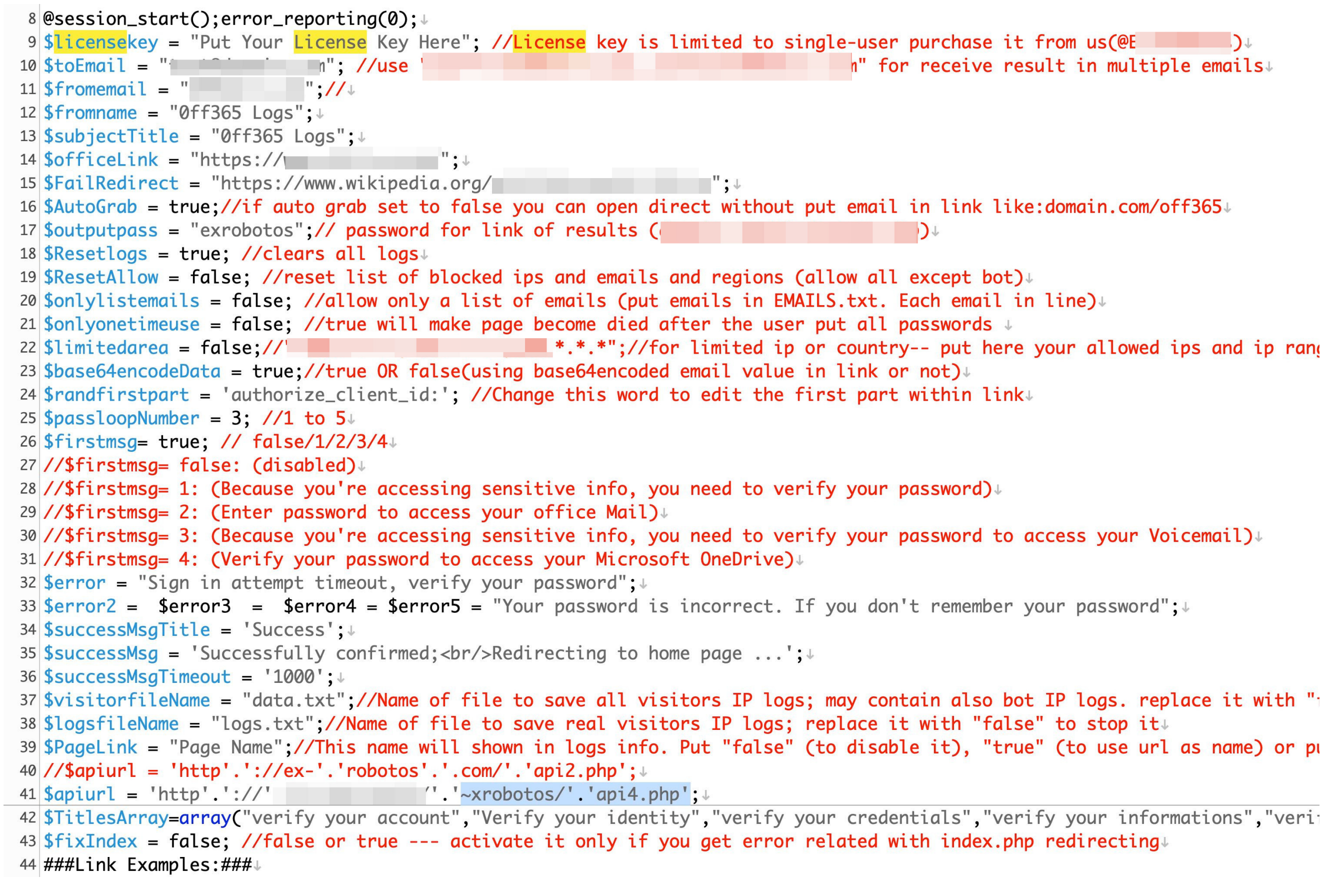


Some of this version Features:

+New style and new logo for office page.
+Responsive design with all devices and screens.
+Use licensing system, every buyer will get the page file and its license key.
+Ability to choose between Office365 and Voice mail from config.
+Ability to choose between Auto grab and manual email from config.
+Ability to Use it as multiple password or one time password.
+Ability to choose number of password request (1 to 5 times).
+Ability to edit or hide all titles, messages and texts exist in page from config.
+Accept base64 email in link and without it.
+Come with external redirect(optional)
+ Undetectable from Bot (private tricks).
+The page Use private tricks to bypass antibot, goes to inbox and last long time.
+Special stronger antibot system.
+All page elements are dynamique (auto generated fresh page every link call)
+Link one time self destructing (after using it will giving 404 error).
+Link can only be used one time by one user (giving 404 error to not allowed users)..
+Can allow accessing to link for limited area and/or list of ips.
+Each link can locked to only one target email.
And many other new private features and tricks. This office365 page is the best ever.

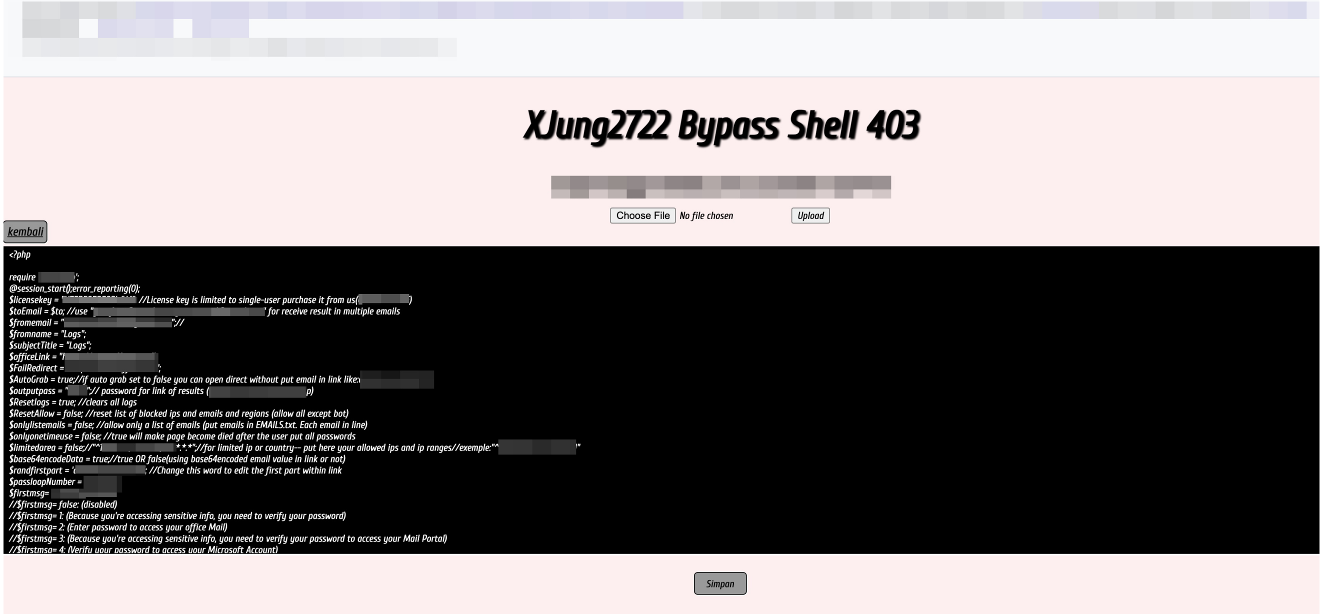
Figure 10. Features of the Office365 V4 phishing kit, as posted on social media.

Furthermore, the phishing kit is sold with a license, and the obfuscated PHP script calls back to the developer’s system to verify the license’s validity. The phishing page calls back to the license server to check the license key's availability, and a URL/IP to access the license server is seen in config.PHP. Interestingly, config.PHP file is readable on an actual phishing site and contains the license key and the email address in it.



```
@session_start();error_reporting(0);
$licensekey = "Put Your License Key Here"; //License key is limited to single-user purchase it from us(@[redacted])
$toEmail = "[redacted]"; //use '[redacted]" for receive result in multiple emails
$fromemail = "[redacted]";//
$fromname = "0ff365 Logs";
$subjectTitle = "0ff365 Logs";
$officeLink = "https://[redacted]";
$FailRedirect = "https://www.wikipedia.org/[redacted]";
$AutoGrab = true;//if auto grab set to false you can open direct without put email in link like:domain.com/off365
$outputpass = "exrobotos";// password for link of results ([redacted])
$Resetlogs = true; //clears all logs
$ResetAllow = false; //reset list of blocked ips and emails and regions (allow all except bot)
$onlylistemails = false; //allow only a list of emails (put emails in EMAILS.txt. Each email in line)
$onlyonetimeuse = false; //true will make page become died after the user put all passwords 
$limitedarea = false;//'[redacted]*.*.*";//for limited ip or country-- put here your allowed ips and ip rang
$base64encodeData = true;//true OR false(using base64encoded email value in link or not)
$randfirstpart = 'authorize_client_id:'; //Change this word to edit the first part within link
$passloopNumber = 3; //1 to 5
$firstmsg= true; // false/1/2/3/4
//$firstmsg= false: (disabled)
//$firstmsg= 1: (Because you're accessing sensitive info, you need to verify your password)
//$firstmsg= 2: (Enter password to access your office Mail)
//$firstmsg= 3: (Because you're accessing sensitive info, you need to verify your password to access your Voicemail)
//$firstmsg= 4: (Verify your password to access your Microsoft OneDrive)
$error = "Sign in attempt timeout, verify your password";
$error2 =  $error3  =  $error4 = $error5 = "Your password is incorrect. If you don't remember your password";
$successMsgTitle = 'Success';
$successMsg = 'Successfully confirmed;<br/>Redirecting to home page ...';
$successMsgTimeout = '1000';
$visitorfileName = "data.txt";//Name of file to save all visitors IP logs; may contain also bot IP logs. replace it with "
$logsfileName = "logs.txt";//Name of file to save real visitors IP logs; replace it with "false" to stop it
$PageLink = "Page Name";//This name will shown in logs info. Put "false" (to disable it), "true" (to use url as name) or pu
//$apiurl = 'http'.'://ex-'.'robotos'.'.com/'.'api2.php';
$apiurl = 'http'.'://'[redacted]'.'~xrobotos/'.'api4.php';
$TitlesArray=array("verify your account","Verify your identity","verify your credentials","verify your informations","veri
$fixIndex = false; //false or true --- activate it only if you get error related with index.php redirecting
###Link Examples:###
```

Figure 11. Checking the license’s validity via PHP



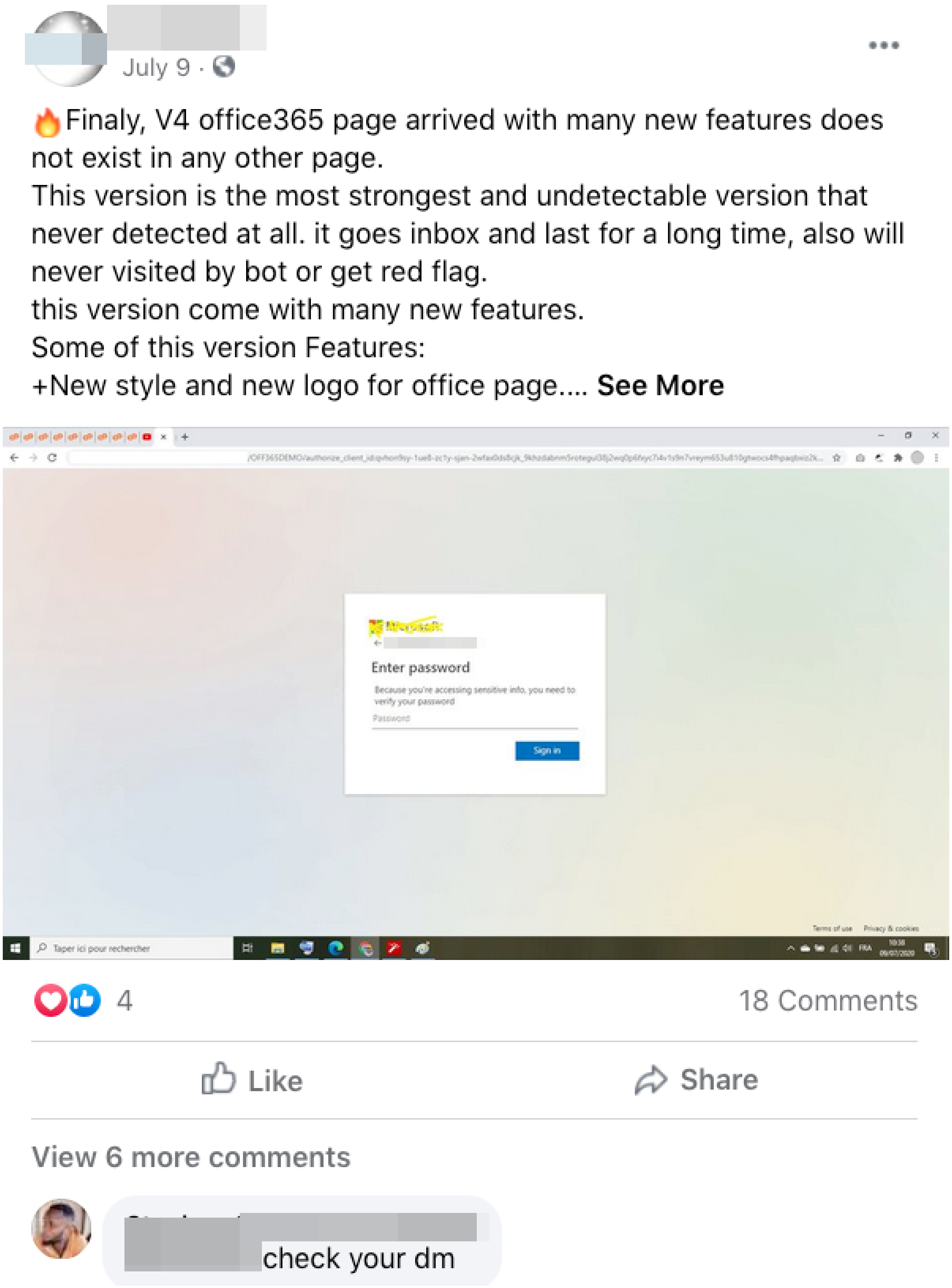
```
<?php

require [redacted]';
@session_start();error_reporting(0);
$licensekey = [redacted] //License key is limited to single-user purchase it from us([redacted])
$toEmail = $to; //use "[redacted]' for receive result in multiple emails
$fromemail = "[redacted]";//
$fromname = "Logs";
$subjectTitle = "Logs";
$officeLink = "[redacted]
$FailRedirect = [redacted];
$AutoGrab = true;//if auto grab set to false you can open direct without put email in link like:[redacted]
$outputpass = "[redacted]";// password for link of results ([redacted]p)
$Resetlogs = true; //clears all logs
$ResetAllow = false; //reset list of blocked ips and emails and regions (allow all except bot)
$onlylistemails = false; //allow only a list of emails (put emails in EMAILS.txt. Each email in line)
$onlyonetimeuse = false; //true will make page become died after the user put all passwords
$limitedarea = false;//"^[redacted]*.*.*";//for limited ip or country-- put here your allowed ips and ip ranges//exemple:"^[redacted]"
$base64encodeData = true;//true OR false(using base64encoded email value in link or not)
$randfirstpart = '[redacted]; //Change this word to edit the first part within link
$passloopNumber = [redacted]
$firstmsg= [redacted]
//$firstmsg= false: (disabled)
//$firstmsg= 1: (Because you're accessing sensitive info, you need to verify your password)
//$firstmsg= 2: (Enter password to access your office Mail)
//$firstmsg= 3: (Because you're accessing sensitive info, you need to verify your password to access your Mail Portal)
//$firstmsg= 4: (Verify your password to access your Microsoft Account)
```

Figure 12. Config file readable on the phishing site

We continue to study the features of this phishing campaign to track the current and potential developments this routine may further include, and to anticipate the changes in its evasion techniques.

Tracking the kit developer

The alleged developer of Office365 announced the V4 phishing kit’s availability on their “business” Facebook page in mid-2020.



[redacted]
July 9 ·

🔥Finaly, V4 office365 page arrived with many new features does not exist in any other page.
This version is the most strongest and undetectable version that never detected at all. it goes inbox and last for a long time, also will never visited by bot or get red flag.
this version come with many new features.
Some of this version Features:
+New style and new logo for office page.... **See More**

[redacted]

Enter password

Because you're accessing sensitive info, you need to verify your password

Password

Sign in

4

18 Comments

Like

Share

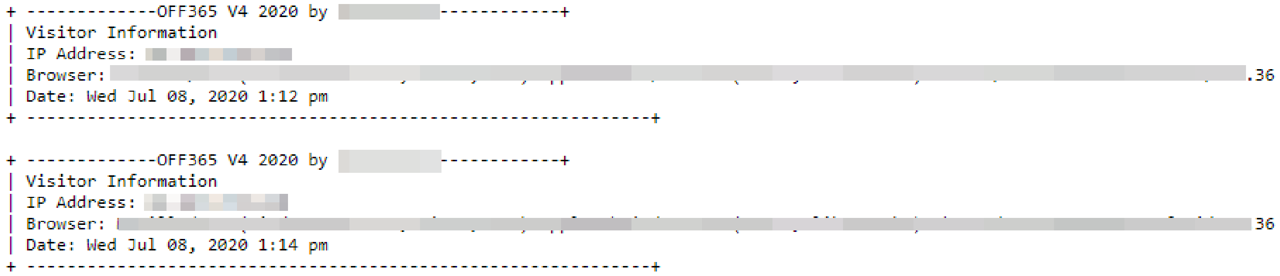
View 6 more comments

[redacted] check your dm

Figure

13. The potential developer of the phishing kit announcing its availability on their business Facebook page.

We also observed logs of test traffic from the phishing kit one day before the announcement of V4, wherein almost all logs recorded were from different IP addresses from Morocco.



```
+ -------------OFF365 V4 2020 by [redacted]------------+
| Visitor Information
| IP Address: [redacted]
| Browser: [redacted].36
| Date: Wed Jul 08, 2020 1:12 pm
+ -------------------------------------------------------------+

+ -------------OFF365 V4 2020 by [redacted]------------+
| Visitor Information
| IP Address: [redacted]
| Browser: [redacted]36
| Date: Wed Jul 08, 2020 1:14 pm
+ -------------------------------------------------------------+
```

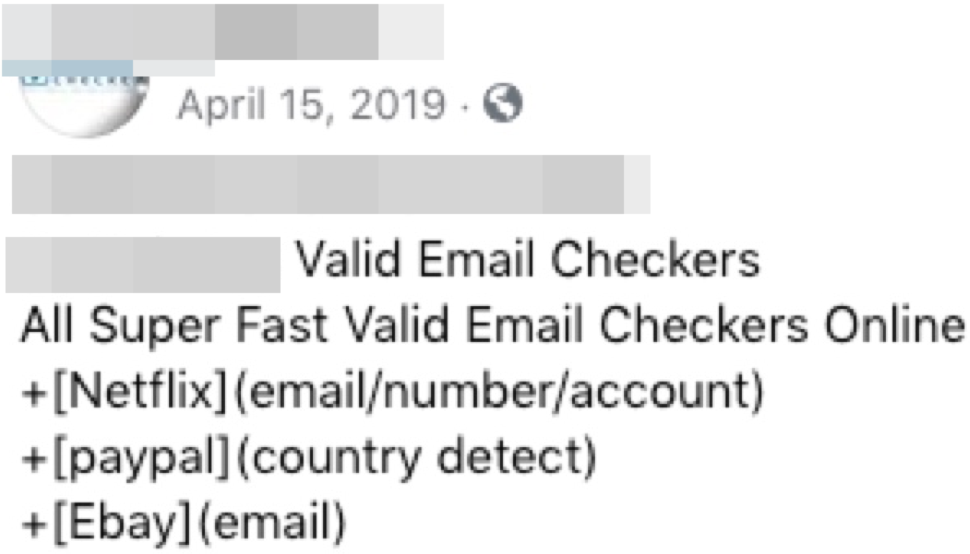
Figure 14. Access logs allowed us to determine the IP addresses used the day before the announcement. The top five IP addresses used were tracked to Morocco.

Several days after the announcement of the V4's availability, we found an email lure sample; a look at the details of the header revealed that it matched the phishing samples we saw in November and December.

Subject: ID:4563|| Request is under Process on Friday, July 17, 2020

Received: FireVPS-RDP (XX.X.XXX.XX) by VI1PR08CA0138.eurprd08.prod.outlook.com (2603:10a6:800:d5::16) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id XX.XX.XXXX.XX via Frontend Transport; Fri, 17 Jul 2020 16:46:44 +0000……

Looking further at the previous posts in the account also revealed announcements that claimed the user responsible for the fake Office 365 versions as the developer of other credential harvesting kits. While no longer available, the latter kit was capable of rapidly verifying the validity of email addresses; it could have been a predecessor project that potentially contributed to the features of the phishing kit versions sold. Based on other posts on the actor's social media page, this user also continues to sell harvested credentials aside from the phishing kit itself.



[redacted]

April 15, 2019 ·

[redacted]

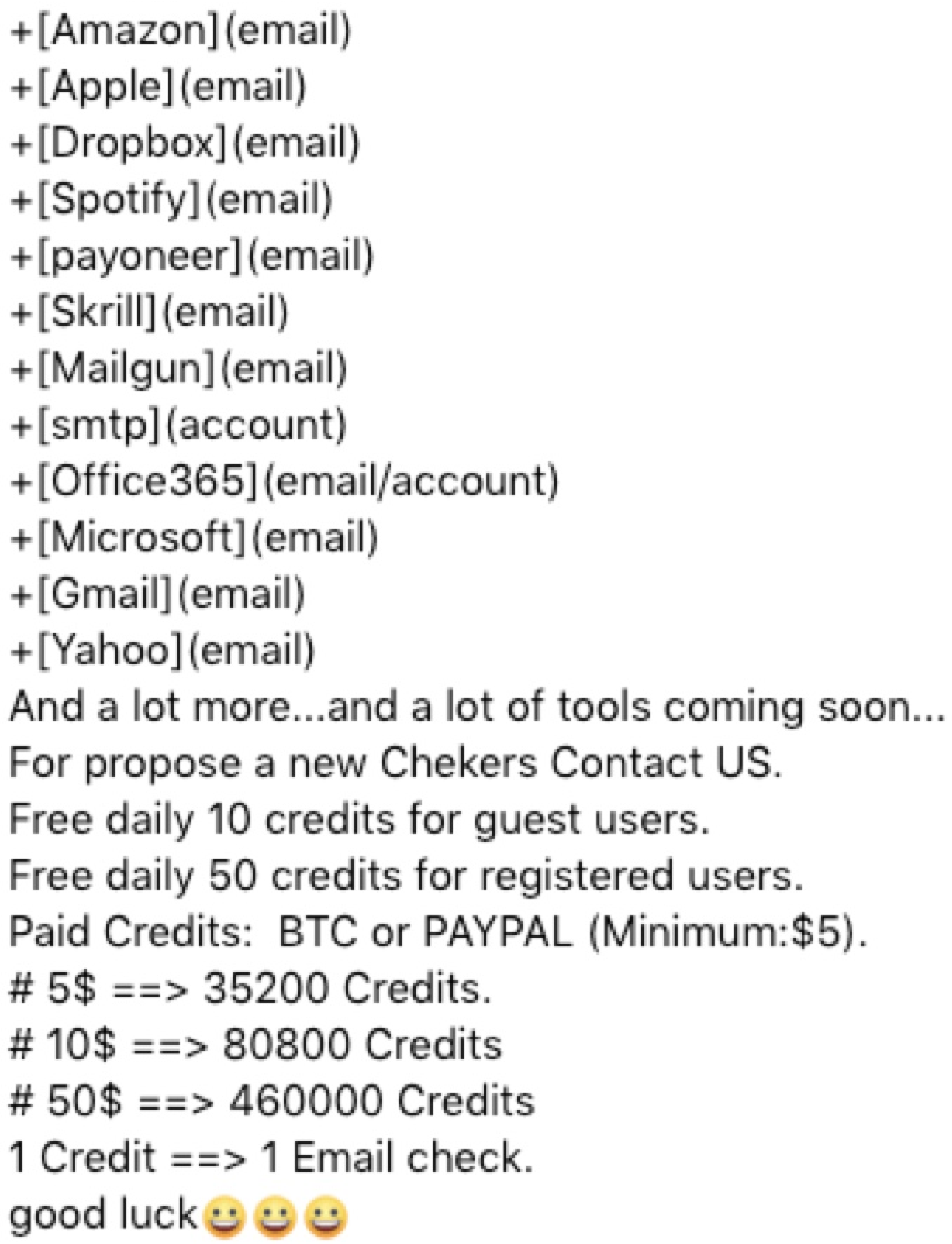
[redacted] Valid Email Checkers

All Super Fast Valid Email Checkers Online

+[Netflix](email/number/account)

+[paypal](country detect)

+[Ebay](email)



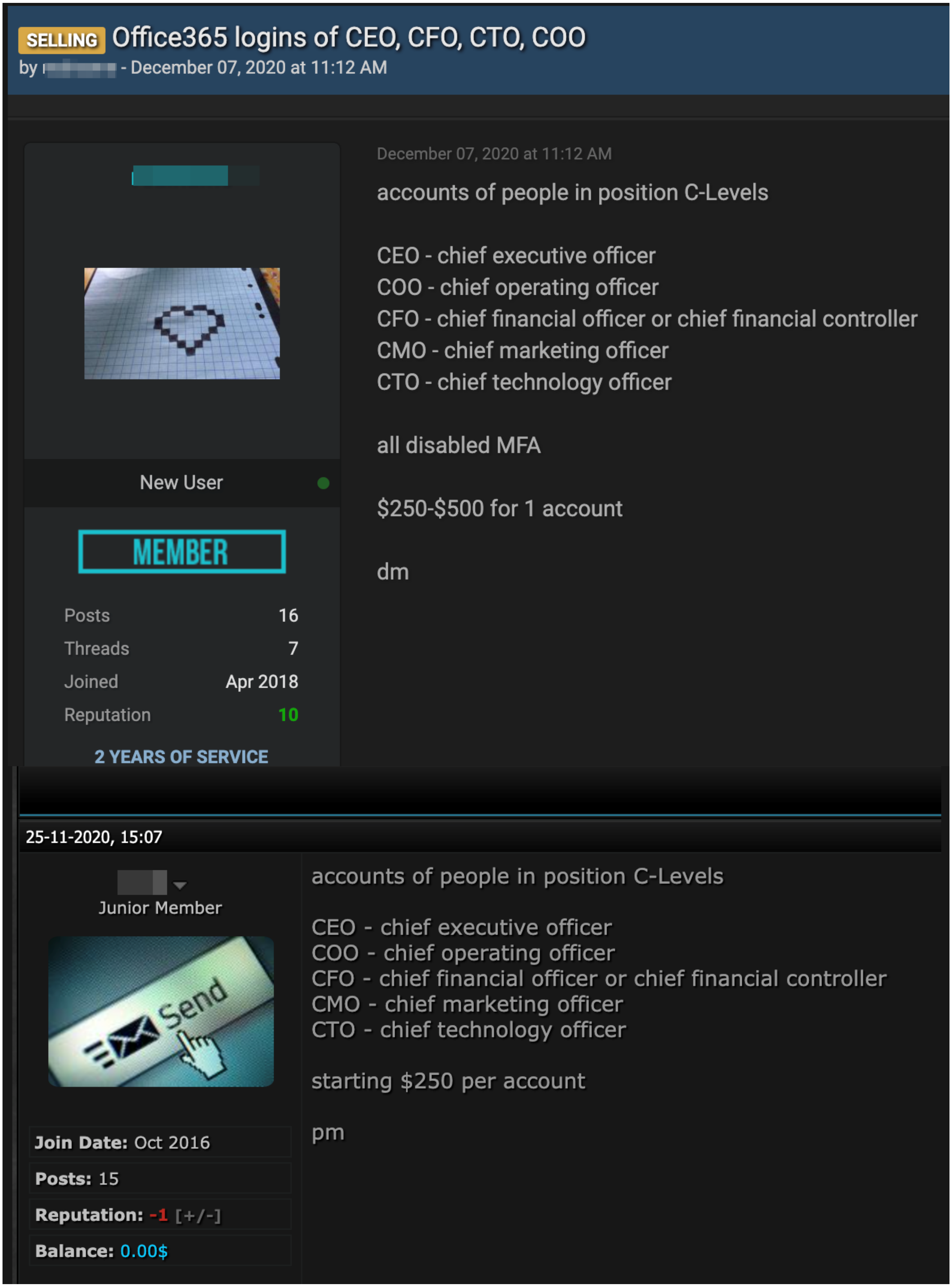
+[Amazon](email)
+[Apple](email)
+[Dropbox](email)
+[Spotify](email)
+[payoneer](email)
+[Skrill](email)
+[Mailgun](email)
+[smtp](account)
+[Office365](email/account)
+[Microsoft](email)
+[Gmail](email)
+[Yahoo](email)
And a lot more...and a lot of tools coming soon...
For propose a new Chekers Contact US.
Free daily 10 credits for guest users.
Free daily 50 credits for registered users.
Paid Credits: BTC or PAYPAL (Minimum:$5).
5$ ==> 35200 Credits.
10$ ==> 80800 Credits
50$ ==> 460000 Credits
1 Credit ==> 1 Email check.
good luck😀😀😀

Figure 15. The malware actor’s previous project with features that are similar to some of the current phishing kit’s features

We were able to match the cybercriminal’s business Facebook page to personal pages while scanning for information online. We have informed the appropriate authorities of these details for this investigation.

Possible link to online sellers of C-level accounts

There are numerous users in underground forums selling C-Level accounts. We identified these user handles as sellers of some relevant C-level accounts across different forums, pricing these credentials ranging from $250 to $500.



SELLING Office365 logins of CEO, CFO, CTO, COO

by [redacted] - December 07, 2020 at 11:12 AM

[redacted]

New User

MEMBER

Posts	16
Threads	7
Joined	Apr 2018
Reputation	10

2 YEARS OF SERVICE

December 07, 2020 at 11:12 AM

accounts of people in position C-Levels

CEO - chief executive officer
COO - chief operating officer
CFO - chief financial officer or chief financial controller
CMO - chief marketing officer
CTO - chief technology officer

all disabled MFA

$250-$500 for 1 account

dm

25-11-2020, 15:07

[redacted]

Junior Member

Join Date: Oct 2016

Posts: 15

Reputation: -1 [+/-]

Balance: 0.00$

accounts of people in position C-Levels

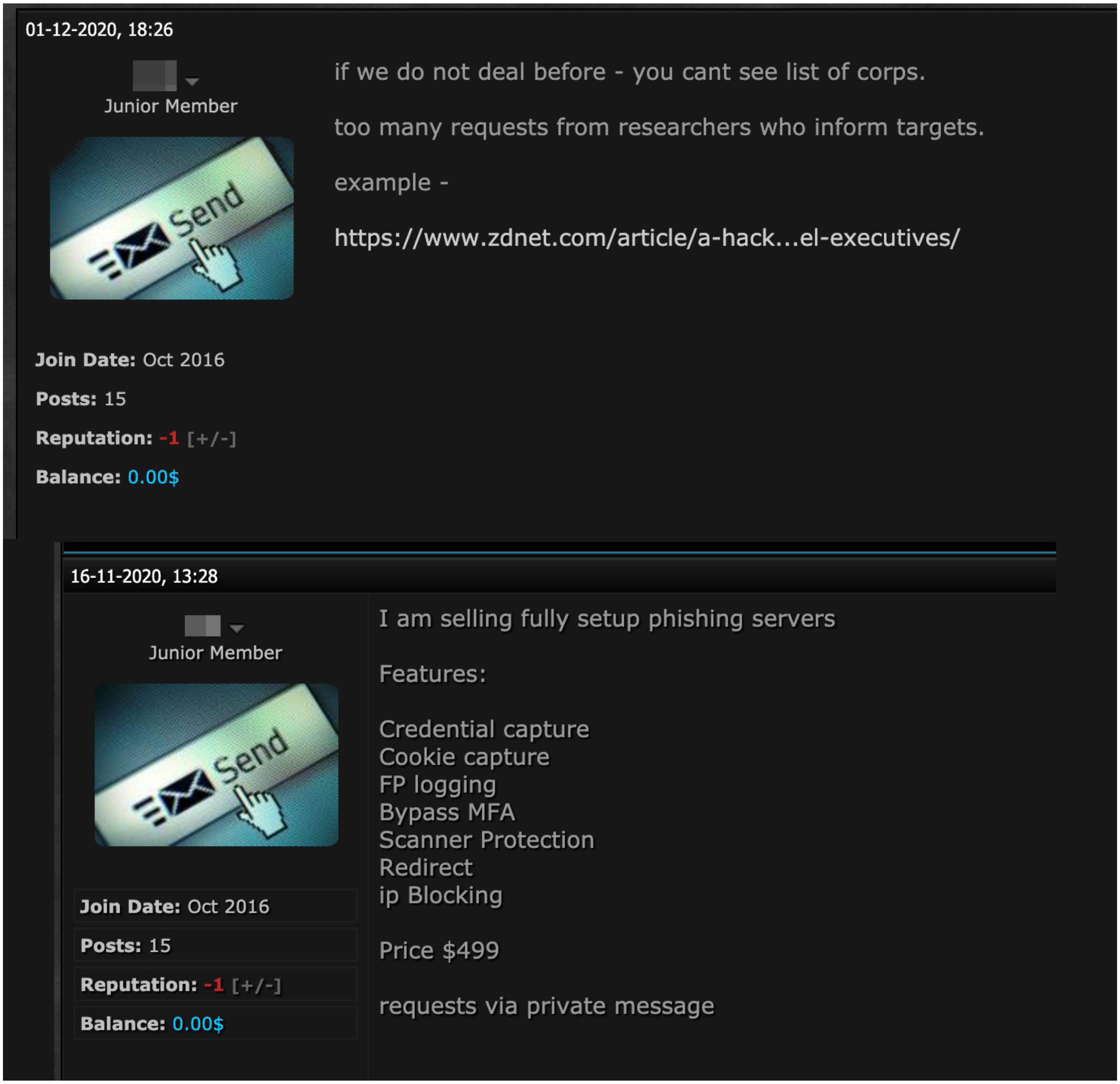
CEO - chief executive officer
COO - chief operating officer
CFO - chief financial officer or chief financial controller
CMO - chief marketing officer
CTO - chief technology officer

starting $250 per account

pm

Figure 16. Some sellers of company executives’ compromised credentials in underground forums

We found it interesting that the user mentioned the published article regarding selling C-level credentials and requests to deal only with users or customers he had previous transactions with. New customers are automatically prohibited from viewing the list of affected companies and credentials. The user also sells a phishing routine targeting servers and identifies its features such as cookie capture and multi-factor authentication bypass. Interestingly, the same handle sells both; the tool for credential harvesting and (two) collected accounts are priced approximately the same, similar to the alleged phishing kit developer's offers on social media.



01-12-2020, 18:26

[redacted]

Junior Member

Join Date: Oct 2016

Posts: 15

Reputation: -1 [+/-]

Balance: 0.00$

if we do not deal before - you cant see list of corps.

too many requests from researchers who inform targets.

example -

https://www.zdnet.com/article/a-hack...el-executives/

16-11-2020, 13:28

[redacted]

Junior Member

Join Date: Oct 2016

Posts: 15

Reputation: -1 [+/-]

Balance: 0.00$

I am selling fully setup phishing servers

Features:

Credential capture
Cookie capture
FP logging
Bypass MFA
Scanner Protection
Redirect
ip Blocking

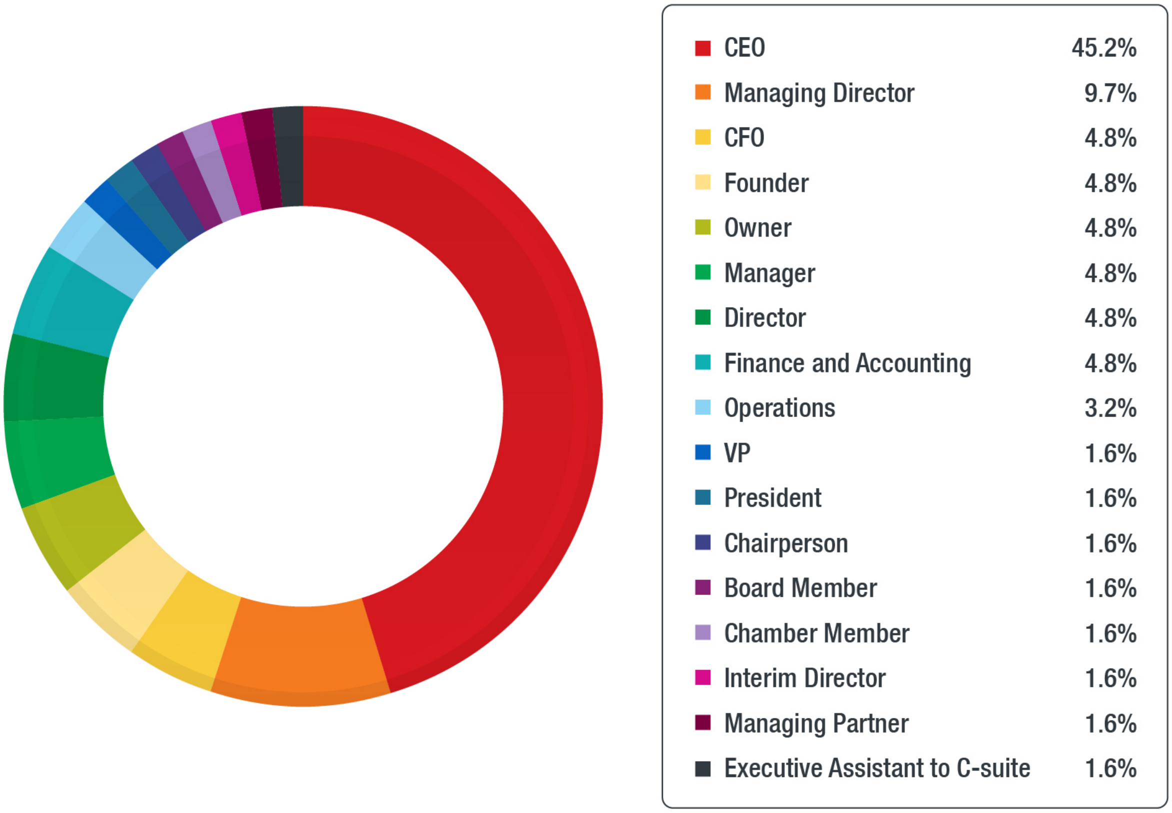
Price $499

requests via private message

Figure 17. Underground seller issuing a disclaimer on who he will transact with (above), and another post selling a phishing malware (below).

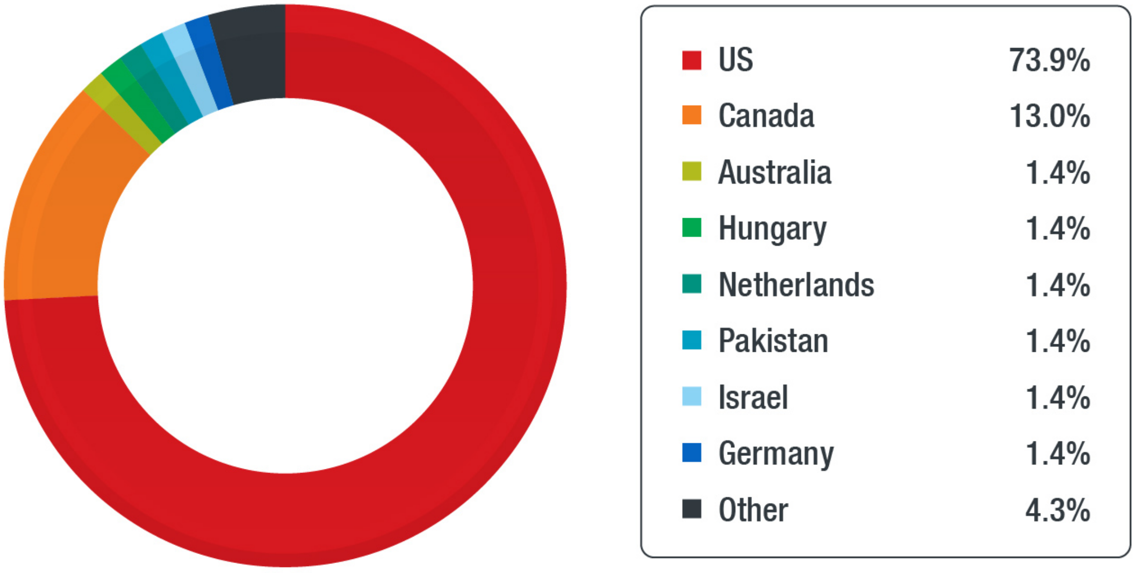
Potential targets and victims' data

Analysis of the data from the misconfigured sites' collected log files revealed that the stolen credentials came from eight compromised phishing sites hosting the malicious Office 365 V4 kit as of this writing. We found each site to be possibly made by different phishers for different phishing campaigns of varying scale and scope. One campaign targeted only company CEOs, presidents, and founders in the US, while another campaign targeted directors and managers from various countries such as the US, UK, Canada, Hungary, the Netherlands, and Israel. In addition, it appeared that the phishers mostly collected targeted email addresses from LinkedIn.



©2021 TREND MICRO

Figure 18. Victims' company positions identified from LinkedIn



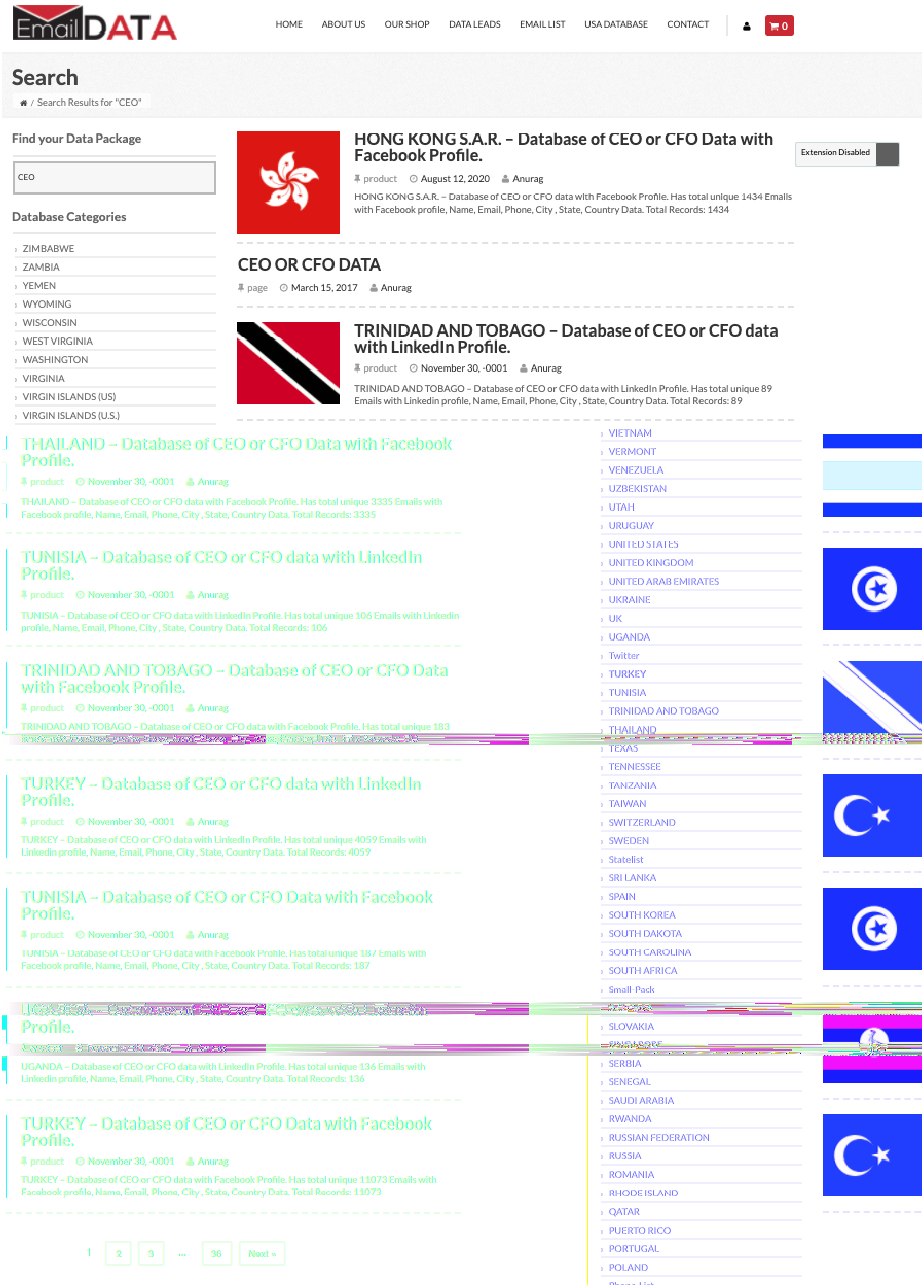
©2021 TREND MICRO

Figure 19. Country distribution of victims

Based on the data distribution, CEOs in the US are obviously the main targets of the threat actors that use the Office 365 V4 phishing kit. In the underground markets, CEO email address lists are often sold and bought for the purpose of conducting additional phishing attacks, gaining access to sensitive information or conducting other social engineering attacks, such as business email compromise (BEC) and impersonation.

A look at different underground forums and pages also revealed specific offers for compromised credentials which are categorized according to year, industry, company position, and social media platform credentials. In addition, the forum messages were written in English, even in non-English forums such as those catering to Russian-speaking users and groups. While not uncommon, the accounts were notably created to post those specific messages selling the data and phishing kit to potential customers. This is emphasized in one forum where the actor bought an account for use in one of the forums just to sell data.

To start a target list, there are a number of platforms available that sell lists of CFO/CEO emails, Facebook profiles and more, categorized by region and country. The attackers could have purchased target lists from one of these websites.



Search

/ Search Results for "CEO"

Find your Data Package

CEO

Database Categories

- ZIMBABWE
- ZAMBIA
- YEMEN
- WYOMING
- WISCONSIN
- WEST VIRGINIA
- WASHINGTON
- VIRGINIA
- VIRGIN ISLANDS (US)
- VIRGIN ISLANDS (U.S.)
- VIETNAM
- VERMONT
- VENEZUELA
- UZBEKISTAN
- UTAH
- URUGUAY
- UNITED STATES
- UNITED KINGDOM
- UNITED ARAB EMIRATES
- UKRAINE
- UK
- UGANDA
- Twitter
- TURKEY
- TUNISIA
- TRINIDAD AND TOBAGO
- THAILAND
- TEXAS
- TENNESSEE
- TANZANIA
- TAIWAN
- SWITZERLAND
- SWEDEN
- Statelist
- SRI LANKA
- SPAIN
- SOUTH KOREA
- SOUTH DAKOTA
- SOUTH CAROLINA
- SOUTH AFRICA
- Small-Pack
- SLOVENIA
- SLOVAKIA
- SINGAPORE
- SERBIA
- SENEGAL
- SAUDI ARABIA
- RWANDA
- RUSSIAN FEDERATION
- RUSSIA
- ROMANIA
- RHODE ISLAND
- QATAR
- PUERTO RICO
- PORTUGAL
- POLAND
- Phone-List

Extension Disabled

HONG KONG S.A.R. – Database of CEO or CFO Data with Facebook Profile.

product August 12, 2020 Anurag

HONG KONG S.A.R. – Database of CEO or CFO data with Facebook Profile. Has total unique 1434 Emails with Facebook profile, Name, Email, Phone, City , State, Country Data. Total Records: 1434

CEO OR CFO DATA

page March 15, 2017 Anurag

TRINIDAD AND TOBAGO – Database of CEO or CFO data with LinkedIn Profile.

product November 30, -0001 Anurag

TRINIDAD AND TOBAGO – Database of CEO or CFO data with LinkedIn Profile. Has total unique 89 Emails with Linkedin profile, Name, Email, Phone, City , State, Country Data. Total Records: 89

THAILAND – Database of CEO or CFO Data with Facebook Profile.

product November 30, -0001 Anurag

THAILAND – Database of CEO or CFO data with Facebook Profile. Has total unique 3335 Emails with Facebook profile, Name, Email, Phone, City , State, Country Data. Total Records: 3335

TUNISIA – Database of CEO or CFO data with LinkedIn Profile.

product November 30, -0001 Anurag

TUNISIA – Database of CEO or CFO data with LinkedIn Profile. Has total unique 106 Emails with Linkedin profile, Name, Email, Phone, City , State, Country Data. Total Records: 106

TRINIDAD AND TOBAGO – Database of CEO or CFO Data with Facebook Profile.

product November 30, -0001 Anurag

TRINIDAD AND TOBAGO – Database of CEO or CFO data with Facebook Profile. Has total unique 183 Emails with Facebook profile, Name, Email, Phone, City , State, Country Data. Total Records: 183

TURKEY – Database of CEO or CFO data with LinkedIn Profile.

product November 30, -0001 Anurag

TURKEY – Database of CEO or CFO data with LinkedIn Profile. Has total unique 4059 Emails with Linkedin profile, Name, Email, Phone, City , State, Country Data. Total Records: 4059

TUNISIA – Database of CEO or CFO Data with Facebook Profile.

product November 30, -0001 Anurag

TUNISIA – Database of CEO or CFO data with Facebook Profile. Has total unique 187 Emails with Facebook profile, Name, Email, Phone, City , State, Country Data. Total Records: 187

UGANDA – Database of CEO or CFO data with LinkedIn Profile.

[illegible]

UGANDA – Database of CEO or CFO data with LinkedIn Profile. Has total unique 136 Emails with Linkedin profile, Name, Email, Phone, City , State, Country Data. Total Records: 136

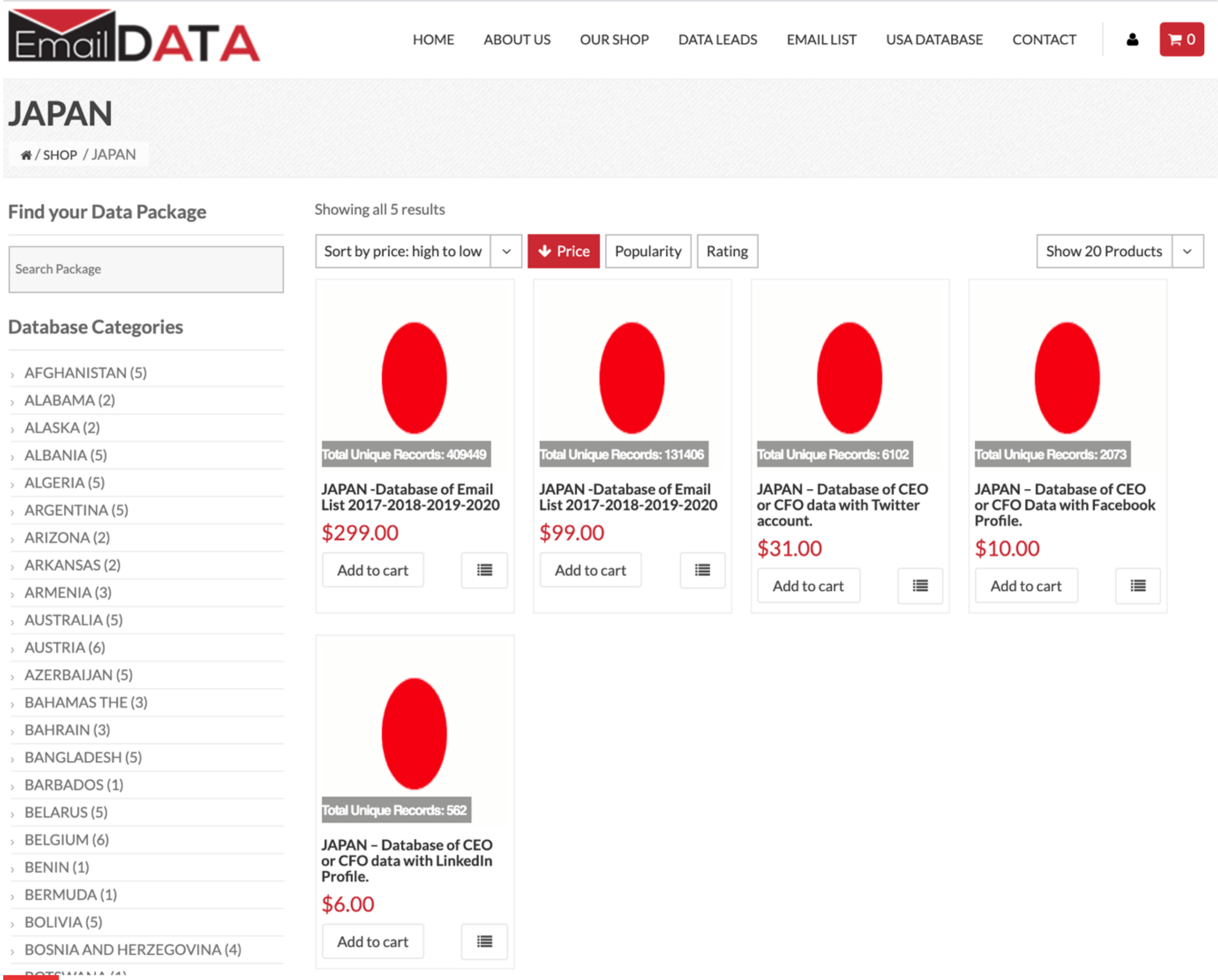
TURKEY – Database of CEO or CFO Data with Facebook Profile.

product November 30, -0001 Anurag

TURKEY – Database of CEO or CFO data with Facebook Profile. Has total unique 11073 Emails with Facebook profile, Name, Email, Phone, City , State, Country Data. Total Records: 11073

1 2 3 … 36 Next »

Figure 20. A marketing website offering CEO/CFO email and Facebook page lists



JAPAN

/ SHOP / JAPAN

Find your Data Package

Search Package

Database Categories

- AFGHANISTAN (5)
- ALABAMA (2)
- ALASKA (2)
- ALBANIA (5)
- ALGERIA (5)
- ARGENTINA (5)
- ARIZONA (2)
- ARKANSAS (2)
- ARMENIA (3)
- AUSTRALIA (5)
- AUSTRIA (6)
- AZERBAIJAN (5)
- BAHAMAS THE (3)
- BAHRAIN (3)
- BANGLADESH (5)
- BARBADOS (1)
- BELARUS (5)
- BELGIUM (6)
- BENIN (1)
- BERMUDA (1)
- BOLIVIA (5)
- BOSNIA AND HERZEGOVINA (4)

Showing all 5 results

Sort by price: high to low | ↓ Price | Popularity | Rating | Show 20 Products

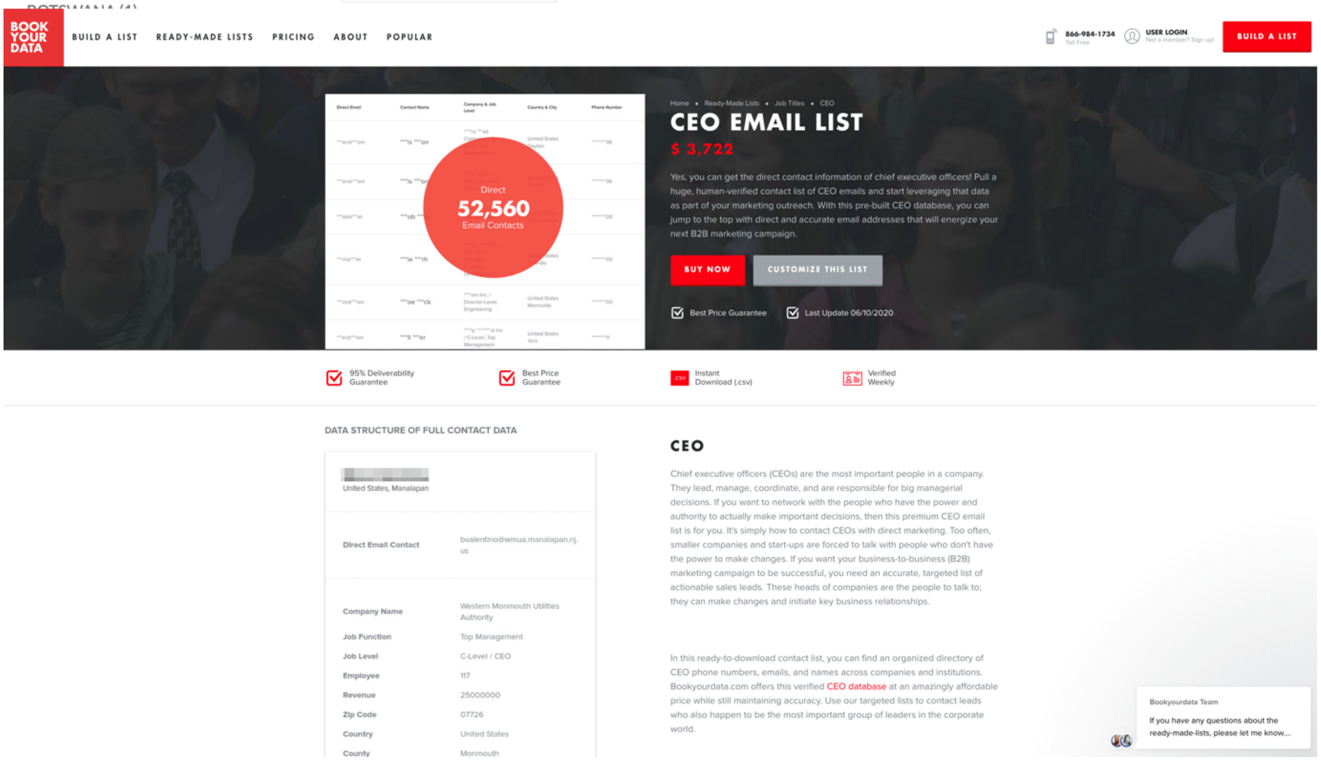
Total Unique Records: 409449
JAPAN -Database of Email List 2017-2018-2019-2020
$299.00
Add to cart

Total Unique Records: 131406
JAPAN -Database of Email List 2017-2018-2019-2020
$99.00
Add to cart

Total Unique Records: 6102
JAPAN – Database of CEO or CFO data with Twitter account.
$31.00
Add to cart

Total Unique Records: 2073
JAPAN – Database of CEO or CFO Data with Facebook Profile.
$10.00
Add to cart

Total Unique Records: 562
JAPAN – Database of CEO or CFO data with LinkedIn Profile.
$6.00
Add to cart



Direct Email	Contact Name	Company & Job Level	Country & City	Phone Number
ondom	***is ***on	***ra ***ad [illegible]	United States Dayton	********36
ondom	***is ***on	[illegible]	[illegible]	********36
obdet	***ob ***	[illegible]	[illegible]	********00
hdet	***ie ***rh	[illegible]	United States [illegible]	********00
ckdom	***oe ***ck	***om Inc. / Director-Level, Engineering	United States Morrisville	********00
erdom	***ll ***er	***ly ********al Inc / C-Level, Top Management	United States York	********tt

Direct
52,560
Email Contacts

Home • Ready-Made Lists • Job Titles • CEO

CEO EMAIL LIST

$ 3,722

Yes, you can get the direct contact information of chief executive officers! Pull a huge, human-verified contact list of CEO emails and start leveraging that data as part of your marketing outreach. With this pre-built CEO database, you can jump to the top with direct and accurate email addresses that will energize your next B2B marketing campaign.

BUY NOW | CUSTOMIZE THIS LIST

☑ Best Price Guarantee ☑ Last Update 06/10/2020

☑ 95% Deliverability Guarantee
☑ Best Price Guarantee
.csv Instant Download (.csv)
Verified Weekly

DATA STRUCTURE OF FULL CONTACT DATA

[redacted]
United States, Manalapan

Direct Email Contact	bvalentino@wmua.manalapan.nj.us
Company Name	Western Monmouth Utilities Authority
Job Function	Top Management
Job Level	C-Level / CEO
Employee	117
Revenue	25000000
Zip Code	07726
Country	United States
County	Monmouth

CEO

Chief executive officers (CEOs) are the most important people in a company. They lead, manage, coordinate, and are responsible for big managerial decisions. If you want to network with the people who have the power and authority to actually make important decisions, then this premium CEO email list is for you. It's simply how to contact CEOs with direct marketing. Too often, smaller companies and start-ups are forced to talk with people who don't have the power to make changes. If you want your business-to-business (B2B) marketing campaign to be successful, you need an accurate, targeted list of actionable sales leads. These heads of companies are the people to talk to; they can make changes and initiate key business relationships.

In this ready-to-download contact list, you can find an organized directory of CEO phone numbers, emails, and names across companies and institutions. Bookyourdata.com offers this verified CEO database at an amazingly affordable price while still maintaining accuracy. Use our targeted lists to contact leads who also happen to be the most important group of leaders in the corporate world.

Bookyourdata Team
If you have any questions about the ready-made-lists, please let me know....

Figure 21. A marketing website offering lists for Japan sorted by year, company position, and

social media platform

Conclusion

Phishing attacks and attackers often target employees — usually the weakest link in an organization’s security chain. As seen in this particular campaign, the attackers target high profile employees who may not be as technically or cybersecurity savvy, and may be more likely to be deceived into clicking on malicious links. By selectively targeting C-level employees, the attacker significantly increases the value of obtained credentials as they could lead to further access to sensitive personal and organizational information, and used in other attacks.

The scale and accuracy of the emails and credentials show that the attacker possesses an accurate dataset of victims and potential targets. While the attacker could have simply compiled the emails from the targeted organizations’ websites, they went a step further to validate these to make sure it complements data collected from the public domain.

While organizations are aware and wary of the information they include in public-facing websites and platforms, their respective employees should be constantly reminded to be mindful of the details they disclose on personal pages. These can be easily used against them for attacks using social engineering techniques. All employees, regardless of company rank, should exercise caution when reviewing and acting on email prompts for specific actions, especially from unknown sources.

Considering this, legitimate service providers and vendors will never ask individual consumers and enterprise users for details such as account access credentials, and especially not to retain dated passwords. These details are susceptible to abuse among unauthorized and malicious individuals and are left for customization by vendors to respective security and IT teams following organizational policies.

Indicators of Compromise (IoCs)

Please click on the link to find our list of IoCs.