Johnny Rivera

Dr. Walden

CIT 485

02/09/22

# Phishing Report

## Introduction

The citizens of the United Kingdom have been receiving numerous incoming phishing emails which led us to lead an investigation into their origins. The means to the investigation included viewing email headers, thoroughly inspecting the Comma-separated value (CSV) file, and utilizing the online virus detection tool Virus Total (VT). The main goal of this investigation is to find out the number of attackers and their intentions. This in turn will help us bring to light the phishing methods they use to avoid them.

## Email Investigation

Upon inspection of the collection of email through the means of image viewing and CSV file reading we were able to find the sending mail server hostname, IP address, Location, and the sender’s email.

Table 1. Email Investigation Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Sending Mail server hostname | Sending mail server IP | Location sent from | (Spoofed) Sender's Email |
| mail.smclavoro.com | **89.96.220.230** | **Italy, Europe** | [transaction@larynx.co.uk](mailto:transaction@larynx.co.uk) |
| 80-110-121-160.cgn.dynamic.surfer.at | **80.110.121.160** | **Austria, Europe** | [transaction@merti-diabetes.co.uk](mailto:transaction@merti-diabetes.co.uk) |
| mail.sovso-stjozef.nl | **213.124.22.218** | **Netherlands, Europe** | [transaction@merti-diabetes.co.uk](mailto:transaction@merti-diabetes.co.uk) |
| yash-static-243.233.21.103.yashtel.co.in | **103.21.233.243** | **India, Asia** | [sales@bimelearning.co.uk](mailto:sales@bimelearning.co.uk) |
| (Italy - Fastweb Mvno Sevices) | **93.49.222.193** | **Italy, Europe** | [purchase@motorbase.co.uk](mailto:purchase@motorbase.co.uk) |
| (United States - Cyberstreet) | **162.219.211.134** | **United States, North America** | [sale@ycoastco.ac.uk](mailto:sale@ycoastco.ac.uk) |
| static-195-130-60-95.ipcom.comunitel.net | **95.60.130.195** | **Spain, Europe** | [deal@ticketwiz.co.uk](mailto:deal@ticketwiz.co.uk) |
| (Denmark - EnergiMidt Infrastruktur A/S) | **185.17.219.47** | **Denmark, Europe** | [support@baulkinggrange.co.uk](mailto:support@baulkinggrange.co.uk) |
| Unknown | **Unknown** | **Unknown** | [commerce@envelop.co.uk](mailto:commerce@envelop.co.uk) |
| host82-70-static.96-5-b.business.telecomitalia.it | **5.96.70.82** | **Italy, Europe** | [payment@kmab.co.uk](mailto:payment@kmab.co.uk) |
| pc355053.ztv.ne.jp | **27.113.220.53** | **Japan, Asia** | [purchasing@soapoperanetwork.co.uk](mailto:purchasing@soapoperanetwork.co.uk) |

The data that we found in Table 1 led to us concluding that this attack was orchestrated by the same attacker using different mail servers and spoofed emails. Their main purpose was to target citizens in the United Kingdom into downloading files containing or being related to Trojan horses. Using a geolocating tool we were able to track down the location of the sending mail server that the attacker was using. The countries with which the attacker’s servers originated include Italy, Austria, Netherlands, India, Spain, Denmark, Japan, and The United States of America. The report also mentions the attacker’s mail server origin which is unknown but was also targeting the same victims. The methods in which the attacker used based on the emails and image detail that the victim’s bank account has been used for a transaction that never took place. They lured the victims into downloading the “Bank statement” so that they can inspect the so-called suspicious activity. Once the victim downloads the “Bank statement” the attacker can steal information, let themselves into the victim’s system, spy on their activity, or whatever the virus is programmed to do.

## Attachments Investigation

The data below was gathered using Virus Total and command-line tools to verify the filetype and SHA1 checksum. The SHA1 checksum is used to verify the integrity of the file and if it has been changed. The file extensions that were investigated included .cab, .rtf, .scr, and .tmp. The .scr file extension is used by windows for screen saver information including animations, graphic interfaces, and such. The .rtf file extension also known as rich text format is universally used for work-processed packages that are easier to read. The .tmp file extension also known as temporary files are used to store temporary information/program which can be used in the future. Lastly, .cab file extensions are used by windows to archive files which include their own embedded digital certificates. What are digital certificates? In short terms, they provide validity to the file’s identity.

Table 2. File Names

|  |
| --- |
| File Name |
| D-57022RI-4035.cab |
| D-57022RI-4035.rtf |
| D-57022RI-4035.scr |
| temp\_cab\_2557436.cab |
| ~WRS{17C4D294-5B95-4F11-B819-029421E9A922}.tmp |
| ~WRS{66763477-E1A2-43A5-9778-EB2B8B2EA2DE}.tmp |

In most cases you would trust these files since they seem harmless, benign, but some of them like the ones provided below can be dangerous. The file investigation in Table 3 shows the results of the files from Table 2 mentioned above in descending order.

Table 3. Attachment Investigation using Virus Total

|  |  |  |  |
| --- | --- | --- | --- |
| Filetype | SHA1 checksum | VT ratio | Malware Name |
| CAB *(.cab)* | **278cb24c0ee4fa21df631fca722251181f6ca28d** | **44/58** | **Trojan/Generic.ASMalwS.D6B5D0** |
| Rich Text Format *(.rtf)* | **8cbf720709c001a3ed8707cae4f1994a22a90e7c** | **0/56** | **Benign** |
| Win32EXE  *(.scr)* | **249ebfb5fb89e1ec4c3b396ca843bf59e857f8ac** | **56/67** | **Trojan/Win32.Yakes** |
| CAB (.cab) | **3cf8292d82c8e12cbefe6965494e0e5a84052a93** | **0/59** | **Benign** |
| UKNOWN *(.tmp)* | **bcda595a00e4c6fad0935d514e49e1aae23c570e** | **0/59** | **Benign** |
| UKNOWN *(.tmp)* | **dbb111419c704f116efa8e72471dd83e86e49677** | **0/56** | **Benign** |

In Table 3 lists the Malware name or mention if it was a benign file. The files that were found to be malware upfront were the CAB and Win32EXE files which were reported to be Trojan viruses. On the surface some of those files were harmless but upon further investigation, they had some sort of connection with other malicious programs. Table 4 shows the relations that the .tmp, .cab, and .rtf files had which were reported to be harmless.

Table 4. Related Malware Investigation with Virus Total

|  |  |  |
| --- | --- | --- |
| Filetype | Related Malware Name & Type | VT ratio |
| Format *(.rtf)* | **Trojan/Win32.Yakes (RAR)** | **39/61** |
| CAB (.cab) | **Trojan/Win32.Yakes (RAR)** | **39/61** |
| UKNOWN *(.tmp)* | **Trojan/Win32.Yakes (RAR)** | **39/61** |
| UKNOWN *(.tmp)* | **Trojan/Generic.ASMalwS.39E4AC (Win32 EXE)** | **63/69** |

The related malware name for the three out of the four files was the same which could detail that the attacker was either trying to target multiple victims at once or that they are not that skilled. The attacker would most likely be a “script kiddie” where they would just use the attack script developed by another hacker. That is the most likely cause why the code was the same for most of these attacks, they would just copy and reuse the same virus.

## Conclusion

In conclusion, the investigation on these phishing emails led us to discover a lot of information about the attacker and their goal. To start off the conclusion that the attack was orchestrated by one attacker would be the time of the emails, these emails were all sent minutes after each other for an hour. This hour would be filled with them setting up emails and viruses to be sent out to various victims. The country which they were targeting was the United Kingdom (UK) since the emails that were sent had UK domains. The countries in which the attacker used a mail server to send these phishing attempts include Italy, Austria, Netherlands, India, Spain, Denmark, Japan, and The United States of America. These locations were found using a geolocation lookup with the mail server’s IP. The phishing technique that the attacker used was Deceptive Phishing, this was concluded after looking at the email text which had the attacker impersonating that victim’s bank alert system. The email had some issues with the formatting at the start and had a vague subject title. The text also had some grammatical issues when addressing how long the victim’s bank account would be “frozen”. They attached the .cab file in the email for the victim to download, and in most cases given the data it was malicious. CAB filetypes on their own are secure since they are just archives which have been digitally certified by windows, in this case, the files were tinkered with and made to believe that they were benign. This was determined by the VT ratio which on low had a rating of 39/61 and a high of 63/69 including the related malicious malware when the file was said to be benign. The attachments which were said to be harmless included temp\_cab\_2557436.cab which was related to a Trojan Virus as it being the child of that Virus. The file would run but would call upon its parent process to start, the Trojan, in this case, then the attacker would still get access to the victim’s computer. The name of these Trojans was in most cases the same and the VT score was repeating on some which led to us concluding that they would copy other attacker’s scripts to use in the phishing attacks. This also meant that the Trojan the attacker used is named “Trojan/Win32.Yakes” and is malicious given the average 46 VT rating. Using all the data summarized previously we can conclude that the files attached to these emails are malicious and should not be downloaded by the receivers in the UK.