**1. Introduction**

To interduce this phishing attack that led to an installing of malware on a victim’s computer we were given two data types to investigate that may have triggered this attack. Those two data types are categorized into attachments and emails. The email data that we were given was a .txt file, a screenshot of the email with the virus, and a .csv file that contained multiple possible addresses that could have been linked to the attack. In the attachment folder we were given a .cab file, .src file, and a .tmp file. These files may contain possible benign with malware waiting to infect. Our goal is to find out where this attack may have come from and what possible malware could have caused this attack and how.

**2. E-mail investigation (with summary table)**

Analysis Questions 1-3

1. What country or countries were the messages sent to?

a. The countries that the messages were sent to were USA, Japan, Italy, Denmark, Austria, and the Netherlands.

2. What country or countries were the messages sent from?

b. The countries that the messages were sent from was the USA.

3. Which phishing techniques does the sender of the one complete message use?

c. This sender sent quit a unique phishing email that acted as if they were the bank freezing one’s account and telling them that they need to verify that the user is who they say they are. We can tell off the bat this is faked due to no company branding, company name, a spoofed email address that I wouldn’t trust, also an email about a frozen bank account and not a personal phone call is suspicious, also an attached file with that’s also the subject note.

|  |  |  |
| --- | --- | --- |
| **Server Hostname** | **Mail Server IP** | **Location of IP** |
| pc355053.ztv.ne.ip | 27.113 220 53 | Tsu, Japan |
| host82-70-static 96-5-b.business.telecomitalia.it | 5.96.70.82 | Schio, Italy |
| Unknown | Unknown | Unknown |
| (Denmark - EnergiMidt  Infrastruktur A/S) | 185.17.219.47 | Silkeborg, Denmark |
| static-195-130-60-95.ipcom.comunitel.net | 95.60 130.195 | Unknown  (checked multiple sources to find IP address and received nothing) |
| (United States - Cyberstreet) | 162.219 211.134 | USA |
| (Italy - Fastweb Mvno  Services) | 93.49.222.194 | Rome, Italy |
| yash-static-243.233.21.103.ya  shtel.co.in | 103.21.233.243 | Mysore, India |
| mail.sovso-stiozef.nl | 213.124.22.218 | Heerlen, Netherlands |
| 80-110-121-160.cgn.dynamic.  surfer.at | 80.110.121.160 | Vienna, Austria |
| mail.smclavoro.com | 89.96.220.230 | Turin, Italy |

**3. Attachment investigation (with summary table)**

Analysis Questions 4-6

4. What is a .cab file? Is it a likely benign filetype?

a. A .cab file is a Windows cabinet file that stores compressed archive files. Yes, it is very likely that a .cab file could be a benign filetype due to the contents that it may hold since it is a cabinet file type.

5. Were any of the attachment files benign? If so, what was their content and/or purpose?

a. Yes there was a benign file which was the D-57022RI-4035.cab file. This file contained a .src file that was scanned as a trojan horse malware. In the .src file there is a .rsrc file that is used to store graphics and text information that is usually ran on the Macintosh OS. These files were meant to collect text, data, and possible graphics of the infected user after they clicked on the link in the email.

6. Were any of the attachment files malware? If so, what is the name of the malware contained in them?

a. Yes, like stated above there was the .cab file that contained the malware storing it in the .src file inside of it. The name of this malware is Trojan/Win32.Gen.C687748 according to AegisLab AV.

|  |  |  |  |
| --- | --- | --- | --- |
| **Filetype** | **SHA1** | **Virus total ratio (from virustotal)** | **Malware Name** |
| .scr | 249ebfb5fb89e1ec4c3b396ca843bf59e857f8ac | 56/67 | AegisLab - Trojan/Win32.Gen.C687748 |
| .rtf | 8cbf720709c001a3ed8707cae4f1994a22a90e7c | 0/56 | Undetected |
| .cab | 278cb24c0ee4fa21df631fca722251181f6ca28d | 44/58 | AhnLab-V3 –  trojan/Generic.ASMalwS.D6B5D0 |

**4. Conclusion**

In conclusion, after looking at the email data we can conclude that the countries that the messages were sent from was the USA and they were reaching out or trying to attack were another spot in the USA, Japan, Italy, Denmark, Austria, and the Netherlands. We know where and to these messages were coming from due to the emails including their origin and destination addresses, subject, and attachment name from the file of .csv. We were able to find out a lot of this information through this one file and through IP addresses look up on the internet, such as whatismyipaddress.com. Once we knew where and to these emails were going our next step was looking into the attachments of what these phishing emails contained.

In this next section of the investigation, we were able to identify that in the attachment files there was a benign that contained a trojan horse. We first started by looking into the .cab file which through virustotal.com we found 44/58 malicious content that a lot of AV software read as a trojan horse. This was suspicious to me, so we decided to dig a little deeper. Keep in mind this .cab file was the file that was sent in the phishing attack and was the attachment to be clicked on by the victim. We were able to find out that the .cab file contains a hidden file of .src that stored the malware of the trojan horse and was able to read and store data, text, and images. We know this because of two reasons, one being in the .src file there was a .rsrc file that is used to store graphics and text information that is usually ran on the Macintosh OS which would make sense due to the dates these files were modified which was 1969. These files were meant to collect text, data, and possible graphics of the infected user after they clicked on the link in the email. We also know that this .src file contained malicious contents because once again when checked on virustotal there was a ratio of 56/67 total malware found, most reading that this was the trojan horse that was hidden. To conclude we were able to find out our main goals in this investigation which were to find out where this attack may have come from and what possible malware could have caused this attack and how.