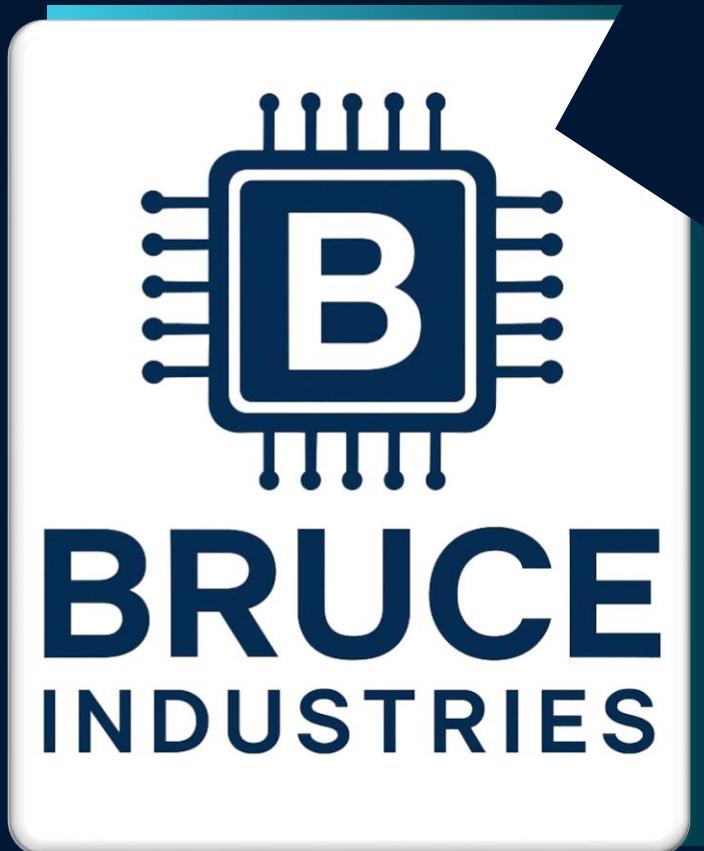


# Bruce Industries: Incident Response Focusing on Digital Forensics



# Organization Background



## Bruce Industries:

- A globally recognized and leading VLSI (Very-Large-Scale Integration) design and semiconductor manufacturing firm.
- With decades of innovation and excellence, the company specializes in evolving proprietary chip blueprints and pioneering microarchitecture designs.
- Serve as the advancements for next-generation of computing technologies.

To fight with the increasing threat of cyber-espionage and sensitive assets, company implemented TLS system also known as SSL proxy to inspect internal HTTPS traffic for some malware or data exfiltration.

# Incident Overview

Internal monitoring systems flagged unusual activity originating from a server used by the HR department.

The system was known to handle encrypted archives containing sensitive employee information.

The nature of the alerts prompted the security team to escalate the issue to Incident Response and Digital Forensics teams.

No immediate external breach was confirmed, but early signs warranted a closer look.



## Incident Response Planning

- 🔍 • **Identify** and confirm the security incident
  - 🚫 • **Contain** the threat to prevent further damage
  - ➖ • **Eradicate** malicious activity from affected systems
  - ⟳ • **Recover** systems and resume normal operations
  - 💡 • **Learn** from the incident to improve future defenses
- Here we're focusing more on Forensics side

```
lt@victim:~$ sudo passwd -l hr
passwd: user 'hr' does not exist
lt@victim:~$ sudo passwd -l hrmanager
passwd: password changed.
lt@victim:~$ sudo passwd -l faraz
passwd: password changed.
lt@victim:~$
```

```
lt@victim:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), deny (outgoing), disabled (routed)
New profiles: skip
lt@victim:~$
```

# Containment

- **Containment** is the process of **limiting the impact** of a security incident before it spreads further.

Disconnecting a compromised device from the network.

- Blocking malicious IP addresses or domains.
- Disabling user accounts such as HR account and IT admin of that machine.
- Redirecting traffic or changing firewall rules.

# Observed Exploitation Pattern



Initial access was gained through a web-based vulnerability introduced into the HR portal.



The attacker escalated privileges using misconfigured local permissions and accessed sensitive directories.



Final actions involved data exfiltration through a covert channel, bypassing traditional alerting mechanisms.



Packet captures and protocol analysis provided step-by-step evidence of the entire attack flow.



The investigation uncovered a multi-step exploitation process, each action building on the previous one.

# SQL Injection

\*ens160

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
53	108.037131488	10.200.0.91	91.189.91.49	HTTP	154	GET / [Information]
54	108.053052971	91.189.91.49	10.200.0.91	HTTP	255	HTTP/1.1 200 OK Content
70	128.265567460	10.200.0.129	10.200.0.91	HTTP	464	GET /employee_pro/ HTTP/1.1
72	128.266971206	10.200.0.91	10.200.0.129	HTTP	802	HTTP/1.1 200 OK (text/html)
74	128.389476328	10.200.0.129	10.200.0.91	HTTP	478	GET /favicon.ico HTTP/1.1
87	128.390939285	10.200.0.91	10.200.0.129	HTTP	2315	HTTP/1.1 200 OK
119	166.215755608	10.200.0.129	10.200.0.91	HTTP	646	POST /employee_pro/login.php HTTP/1.1 (application/x-www-form-urlencoded)
121	166.222112576	10.200.0.91	10.200.0.129	HTTP	479	HTTP/1.1 200 OK (text/html)
129	172.203756517	10.200.0.129	10.200.0.91	HTTP	550	GET /employee_pro/ HTTP/1.1
131	172.205069674	10.200.0.91	10.200.0.129	HTTP	368	HTTP/1.1 304 Not Modified
144	194.954665077	10.200.0.129	10.200.0.91	HTTP	675	POST /employee_pro/login.php HTTP/1.1 (application/x-www-form-urlencoded)
146	194.961148640	10.200.0.91	10.200.0.129	HTTP	483	HTTP/1.1 302 Found
148	194.969669449	10.200.0.129	10.200.0.91	HTTP	517	GET /employee_pro/upload.php HTTP/1.1
149	194.971311298	10.200.0.91	10.200.0.129	HTTP	830	HTTP/1.1 200 OK (text/html)

Accept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: 61\r\nOrigin: http://10.200.0.91\r\nConnection: keep-alive\r\nReferer: http://10.200.0.91/employee\_pro/\r\nCookie: PHPSESSID=d9nqrudet7ge2onjvanp8agqoc\r\nUpgrade-Insecure-Requests: 1\r\nPriority: u=0, i\r\n\r\n[Full request URI: http://10.200.0.91/employee\_pro/login.php]\r\n[HTTP request 1/2]\r\n[Response in frame: 146]\r\n[Next request in frame: 148]

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "username" = "' OR '1'='1"

Form item: "password" = "' OR '1'='1"

0190 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 d...Content-Len  
01a0 68 3a 20 36 31 0d 0a 4f 72 69 67 69 6e 3a 20 68 h: 61..0 rigin:  
01b0 74 74 70 3a 2f 2f 31 30 2e 32 30 30 2e 30 2e 39 ttp://10.200.6  
01c0 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 1..Conne ction:  
01d0 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 eep-aliv e..Ref  
01e0 65 72 3a 20 68 74 74 70 3a 2f 2f 31 30 2e 32 30 er: http://10.  
01f0 30 2e 30 2e 39 31 2f 65 6d 70 6c 6f 79 65 65 5f 0.0.91/e mploye  
0200 70 72 6f 2f 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 pro/..Co okie:  
0210 50 53 45 53 53 49 44 3d 64 39 6e 71 72 75 64 65 PSESSID=d9nqr  
0220 74 37 67 65 32 6f 6e 6a 76 61 6e 70 38 61 67 71 t7ge2onj vanp8a  
0230 6f 63 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 oc..Upgr ade-I  
0240 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests:  
0250 0d 0a 50 72 69 6f 72 69 74 79 3a 20 75 3d 30 2c ..Priori ty: u  
0260 20 69 0d 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 25 i...us ername  
0270 32 37 2b 4f 52 2b 25 32 37 31 25 32 37 25 33 44 27+OR+%2 71%279  
0280 25 32 37 31 26 70 61 73 73 77 6f 72 64 3d 25 32 %271&pas sword:  
0290 37 2b 4f 52 2b 25 32 37 31 25 32 37 25 33 44 25 7+OR+%27 1%2763  
02a0 32 37 31 271

Text item (text), 30 bytes

Packets: 167 · Displayed: 14 (8.4%)

Profile: Default

# RFI File Upload

Wireshark 1.6.0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
54	108.053052971	91.189.91.49	10.200.0.91	HTTP	255	HTTP/1.1 204 No Content
70	128.265567460	10.200.0.129	10.200.0.91	HTTP	464	GET /employee_pro/ HTTP/1.1
72	128.266971206	10.200.0.91	10.200.0.129	HTTP	802	HTTP/1.1 200 OK (text/html)
74	128.389476328	10.200.0.129	10.200.0.91	HTTP	478	GET /favicon.ico HTTP/1.1
87	128.390939285	10.200.0.91	10.200.0.129	HTTP	2315	HTTP/1.1 200 OK
119	166.215755608	10.200.0.129	10.200.0.91	HTTP	646	POST /employee_pro/login.php HTTP/1.1 (application/x-www-form-urlencoded)
121	166.222112576	10.200.0.91	10.200.0.129	HTTP	479	HTTP/1.1 200 OK (text/html)
129	172.203756517	10.200.0.129	10.200.0.91	HTTP	550	GET /employee_pro/ HTTP/1.1
131	172.205069674	10.200.0.91	10.200.0.129	HTTP	368	HTTP/1.1 304 Not Modified
144	194.954665077	10.200.0.129	10.200.0.91	HTTP	675	POST /employee_pro/login.php HTTP/1.1 (application/x-www-form-urlencoded)
146	194.961148640	10.200.0.91	10.200.0.129	HTTP	483	HTTP/1.1 302 Found
148	194.969669449	10.200.0.129	10.200.0.91	HTTP	517	GET /employee_pro/upload.php HTTP/1.1
149	194.971311298	10.200.0.91	10.200.0.129	HTTP	830	HTTP/1.1 200 OK (text/html)
203	378.746326840	10.200.0.129	10.200.0.91	HTTP	725	POST /employee_pro/upload.php HTTP/1.1 (application/x-php)
205	378.753596888	10.200.0.91	10.200.0.129	HTTP	880	HTTP/1.1 200 OK (text/html)
217	408.100472425	10.200.0.91	185.125.190.98	HTTP	154	GET / HTTP/1.1
218	408.186256436	185.125.190.98	10.200.0.91	HTTP	251	HTTP/1.1 204 No Content

Line-based text data: text/html (17 lines)

```
\n<!DOCTYPE html>\n<html lang="en">\n<head>\n    <meta charset="UTF-8">\n    <title>Upload a File</title>\n</head>\n<body>\n    <h2>Upload a File</h2>\n    <form action="upload.php" method="POST" enctype="multipart/form-data">\n        <input type="file" name="fileUpload" required><br><br>\n        <button type="submit" name="submit">Upload</button>\n\n    \n    The file php-reverse-shell.php has been uploaded.</body>\n</html>\n\n
```

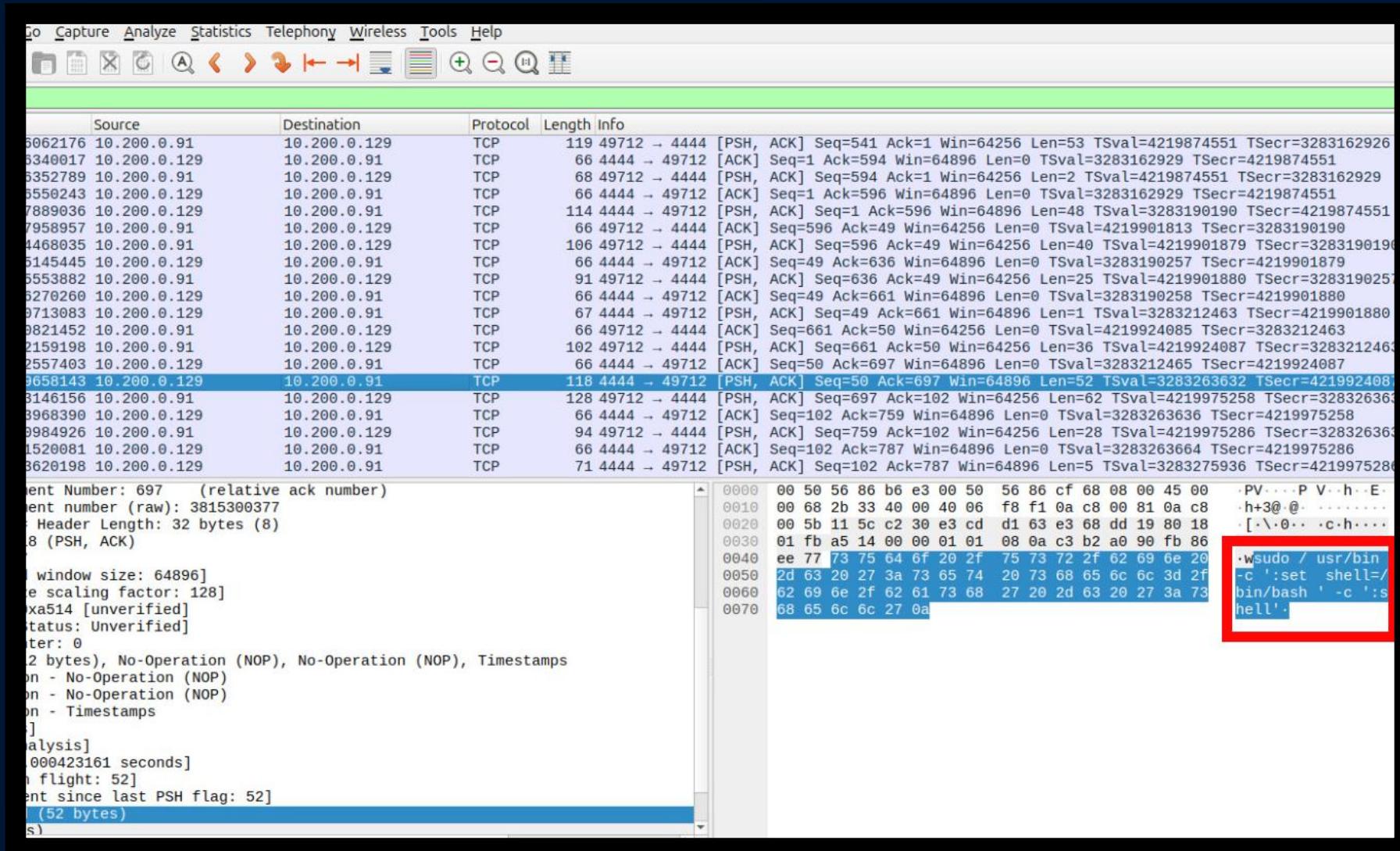
0250 20 46 69 6c 65 3c 2f 68 32 3e 0a 20 20 20 20 20 3c File</h 2>\n0260 66 6f 72 6d 20 61 63 74 69 6f 6e 3d 22 75 70 6c form act ion="u\n0270 6f 61 64 2e 70 68 70 22 20 6d 65 74 68 6f 64 3d oad.php" metho\n0280 22 50 4f 53 54 22 20 65 6e 63 74 79 70 65 3d 22 "POST" e nctype=\n0290 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 multipar t/form\n02a0 61 74 61 22 3e 0a 20 20 20 20 20 20 20 20 3c 69\n02b0 6e 70 75 74 20 74 79 70 65 3d 22 66 69 6c 65 22\n02c0 20 6e 61 6d 65 3d 22 66 69 6c 65 55 70 6c 6f 61\n02d0 64 22 20 72 65 71 75 69 72 65 64 3e 3c 62 72 3e\n02e0 3c 62 72 3e 0a 20 20 20 20 20 20 20 3c 62 75\n02f0 74 74 6f 6e 20 74 79 70 65 3d 22 73 75 62 6d 69\n0300 74 22 20 6e 61 6d 65 3d 22 73 75 62 6d 69 74 22\n0310 3e 55 70 6c 6f 61 64 3c 2f 62 75 74 74 6f 6e 3e\n0320 0a 20 20 20 3c 2f 66 6f 72 6d 3e 0a 0a 54 68\n0330 65 20 66 69 6c 65 20 70 68 70 2d 72 65 76 65 72\n0340 73 65 2d 73 68 65 6c 6c 2e 70 68 70 20 68 61 73\n0350 20 62 65 65 6e 20 75 70 6c 6f 61 64 65 64 2e 3c\n0360 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0a e file p hp-re\n\nThe file php-reverse-shell.php has been uploaded.\n\n

Text item (text), 57 bytes

Packets: 227 · Displayed: 18 (7.9%)

Profile: Default

# Exploiting VIM sudo vulnerability



# Root Access at Victim Machine

Source	Protocol	Length	Destination	Info
770178898 10.200.0.91	TCP	139	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1095 Ack=171 Win=64256 Len=73 TSval=4220045505 TSecr=32833
770502587 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=171 Ack=1168 Win=64896 Len=0 TSval=3283333883 TSecr=4220045505
810718241 10.200.0.91	TCP	108	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1168 Ack=171 Win=64256 Len=42 TSval=4220045545 TSecr=32833
811322399 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=171 Ack=1210 Win=64896 Len=0 TSval=3283333923 TSecr=4220045545
750877758 10.200.0.129	TCP	72	10.200.0.91	4444 → 49712 [PSH, ACK] Seq=171 Ack=1210 Win=64896 Len=6 TSval=3283430863 TSecr=422004
753314658 10.200.0.91	TCP	80	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1210 Ack=177 Win=64256 Len=14 TSval=4220142488 TSecr=32834
753924493 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=177 Ack=1224 Win=64896 Len=0 TSval=3283430866 TSecr=4220142488
758514856 10.200.0.91	TCP	709	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1224 Ack=177 Win=64256 Len=643 TSval=4220142493 TSecr=3283
758898217 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=177 Ack=1867 Win=64256 Len=0 TSval=3283430871 TSecr=4220142493
759729345 10.200.0.91	TCP	108	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1867 Ack=177 Win=64256 Len=42 TSval=4220142494 TSecr=32834
760019498 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=177 Ack=1909 Win=64256 Len=0 TSval=3283430872 TSecr=4220142494
321547838 10.200.0.129	TCP	85	10.200.0.91	4444 → 49712 [PSH, ACK] Seq=177 Ack=1909 Win=64256 Len=19 TSval=3283442434 TSecr=42201
323242168 10.200.0.91	TCP	95	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1909 Ack=196 Win=64256 Len=29 TSval=4220154058 TSecr=32834
323639308 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=196 Ack=1938 Win=64256 Len=0 TSval=3283442436 TSecr=4220154058
323661200 10.200.0.91	TCP	136	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=1938 Ack=196 Win=64256 Len=70 TSval=4220154058 TSecr=32834
323907656 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=196 Ack=2008 Win=64256 Len=0 TSval=3283442436 TSecr=4220154058
6.9187227... 10.200.0.129	TCP	85	10.200.0.91	4444 → 49712 [PSH, ACK] Seq=196 Ack=2008 Win=64256 Len=19 TSval=3283531031 TSecr=42201
6.9210524... 10.200.0.91	TCP	165	10.200.0.129	49712 → 4444 [PSH, ACK] Seq=2008 Ack=215 Win=64256 Len=99 TSval=4220242656 TSecr=32835
6.9215207... 10.200.0.129	TCP	66	10.200.0.91	4444 → 49712 [ACK] Seq=215 Ack=2107 Win=64256 Len=0 TSval=3283531034 TSecr=4220242656

8 bytes on wire (64 bits), 108 bytes captured (864 bits) on interface ens3  
Src: VMware\_86:b6:e3 (00:50:56:86:b6:e3), Dst: VMware\_86:cf:68 (00:50:56:86:c9:68)  
Protocol Version 4, Src: 10.200.0.91, Dst: 10.200.0.129  
Control Protocol, Src Port: 49712, Dst Port: 4444, Seq: 1867, Ack: 177, Len: 42  
: 49712  
Port: 4444  
ex: 15]  
on completeness: Incomplete, DATA (15)]  
t Len: 42]  
umber: 1867 (relative sequence number)  
mber (raw): 3815301547  
nce Number: 1909 (relative sequence number)]  
ent Number: 177 (relative ack number)  
ent number (raw): 3821916642  
Header Length: 32 bytes (8)  
8 (PSH, ACK)  
  
window size: 64256]  
e scaling factor: 128]  
x16bc [unverified]  
status: Unverified]

0000 00 50 56 86 cf 68 00 50 56 86 b6 e3 08 00 45 00 ·PV·h P V...E·  
0010 00 5e 87 9a 40 00 40 06 9c 94 0a c8 00 5b 0a c8 ^@ @ .[...]  
0020 00 81 c2 30 11 5c e3 68 e1 ab e3 cd d1 e2 80 18 ..0.\h.....  
0030 01 f6 16 bc 00 00 01 01 08 0a fb 8a 43 9e c3 b5 ..[?200 4h ]0;ro  
0040 2d d7 1b 5b 3f 32 30 30 34 68 1b 5d 30 3b 72 6f ot@victi m: /-roo  
0050 6f 74 40 76 69 63 74 69 6d 3a 20 2f 07 72 6f 6f t@victim :#  
0060 74 40 76 69 63 74 69 6d 3a 2f 23 20

# Attacker Reconnaissance Within HR Directory

Wireshark Screenshot showing network traffic analysis for an HTTP session. The packet list displays numerous TCP connections between various IP addresses and port 129. The details and bytes panes provide specific information about a selected packet, including source and destination ports, sequence numbers, and payload content. A red box highlights a portion of the payload bytes.

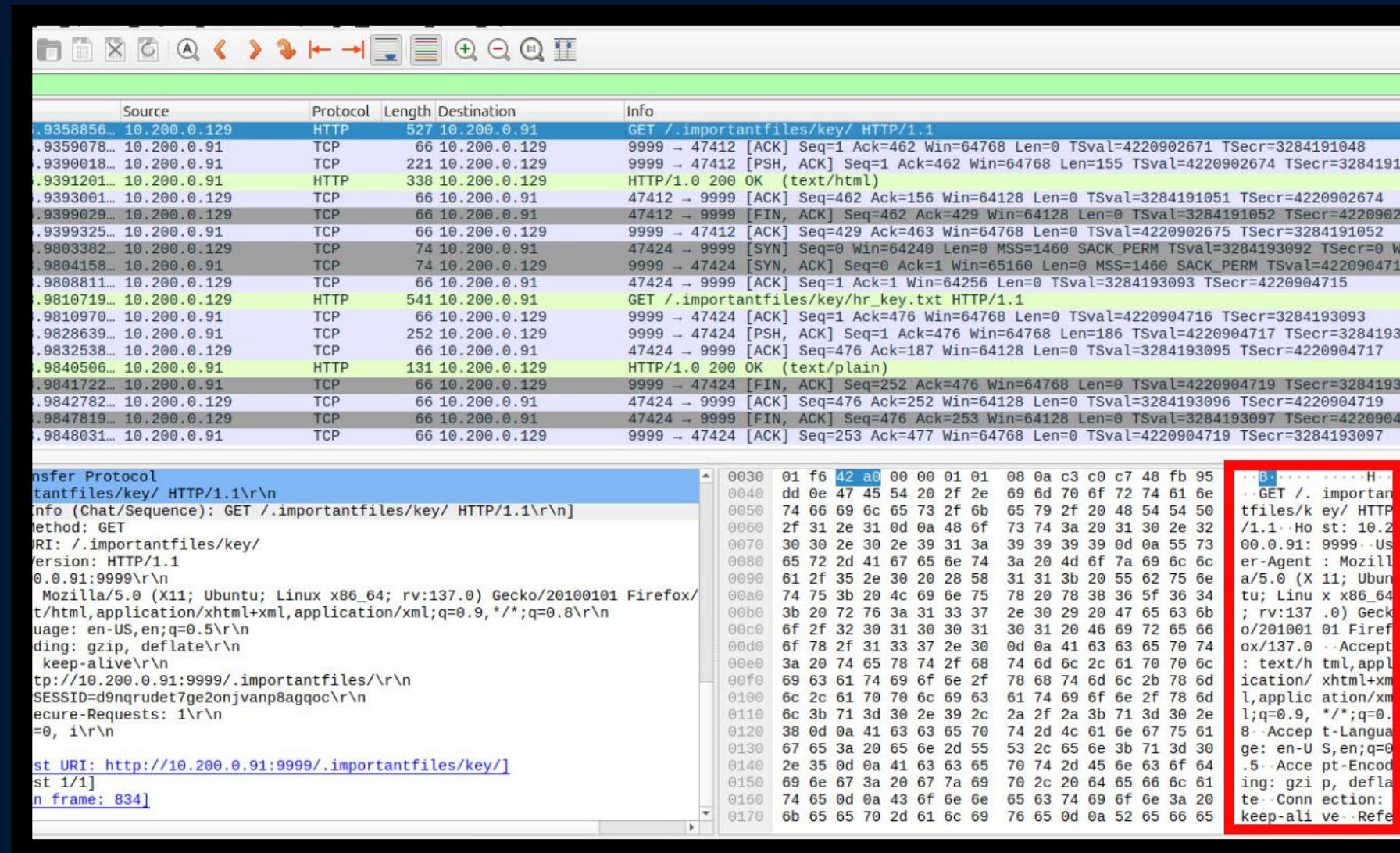
Selected packet details:

- Source: 10.200.0.91
- Protocol: TCP
- Length: 136
- Destination: 10.200.0.129
- Info: 49712 → 4444 [PSH, ACK] Seq=1938 Ack=196 Win=64256 Len=70 TSval=4220154058 TSecr=32834
- Info: 4444 → 49712 [ACK] Seq=196 Ack=2008 Win=64256 Len=0 TSval=3283442436 TSecr=4220154058
- Info: 4444 → 49712 [PSH, ACK] Seq=196 Ack=2008 Win=64256 Len=19 TSval=3283531031 TSecr=4220154058
- Info: 49712 → 4444 [PSH, ACK] Seq=2008 Ack=215 Win=64256 Len=99 TSval=4220242656 TSecr=3283531031
- Info: 4444 → 49712 [ACK] Seq=215 Ack=2107 Win=64256 Len=0 TSval=3283531034 TSecr=4220242656
- Info: 4444 → 49712 [PSH, ACK] Seq=215 Ack=2107 Win=64256 Len=3 TSval=3283678464 TSecr=4220242656
- Info: 49712 → 4444 [PSH, ACK] Seq=2107 Ack=218 Win=64256 Len=13 TSval=4220390089 TSecr=3283678464
- Info: 4444 → 49712 [ACK] Seq=218 Ack=2120 Win=64256 Len=0 TSval=3283678467 TSecr=4220390089
- Info: 49712 → 4444 [PSH, ACK] Seq=2120 Ack=218 Win=64256 Len=263 TSval=4220390100 TSecr=3283678467
- Info: 4444 → 49712 [ACK] Seq=218 Ack=2383 Win=64000 Len=0 TSval=3283678478 TSecr=4220390100
- Info: 4444 → 49712 [PSH, ACK] Seq=218 Ack=2383 Win=64000 Len=7 TSval=3283682750 TSecr=4220390100
- Info: 49712 → 4444 [PSH, ACK] Seq=2383 Ack=225 Win=64256 Len=17 TSval=4220394374 TSecr=3283682750
- Info: 4444 → 49712 [ACK] Seq=225 Ack=2400 Win=64000 Len=0 TSval=3283682752 TSecr=4220394374
- Info: 49712 → 4444 [PSH, ACK] Seq=2400 Ack=225 Win=64256 Len=1400 TSval=4220394386 TSecr=3283682752
- Info: 4444 → 49712 [ACK] Seq=225 Ack=3800 Win=67072 Len=0 TSval=3283682764 TSecr=4220394386
- Info: 49712 → 4444 [PSH, ACK] Seq=3800 Ack=225 Win=64256 Len=258 TSval=4220394387 TSecr=3283682764
- Info: 4444 → 49712 [ACK] Seq=225 Ack=4058 Win=69888 Len=0 TSval=3283682765 TSecr=4220394387
- Info: 49712 → 4444 [PSH, ACK] Seq=4058 Ack=225 Win=64256 Len=70 TSval=4220394387 TSecr=3283682765
- Info: 4444 → 49712 [ACK] Seq=225 Ack=4128 Win=69888 Len=0 TSval=3283682765 TSecr=4220394387

Selected packet bytes:

```
0000  00 50 56 86 cf 68 00 50 56 86 b6 e3 08 00 45 00 -PV...h.PV....E
0010  00 7a 87 a3 40 00 40 06 9c 6f 0a c8 00 5b 0a c8 -z@.o...[...
0020  00 81 c2 30 11 5c e3 68 ea 3a e3 cd d2 12 80 18 ...0.\h:.....
0030  01 f6 16 d8 00 00 01 01 08 0a fb 8e 1b 93 c3 b9 ...
0040  05 cd 1b 5b 3f 32 30 30 34 68 1b 5d 30 3b 72 6f ...
0050  6f 74 40 76 69 63 74 69 6d 3a 20 2f 68 6f 6d 65 ...
0060  2f 68 72 6d 61 6e 61 67 65 72 07 72 6f 6f 74 40 ...
0070  76 69 63 74 69 6d 3a 2f 68 6f 6d 65 2f 68 72 6d ...
0080  61 6e 61 67 65 72 23 20 ...[?200 4h ]0;root@victi m: /home/.../hrmanager#
```

# Attacker exfiltrating data through Python Server



What's Next?

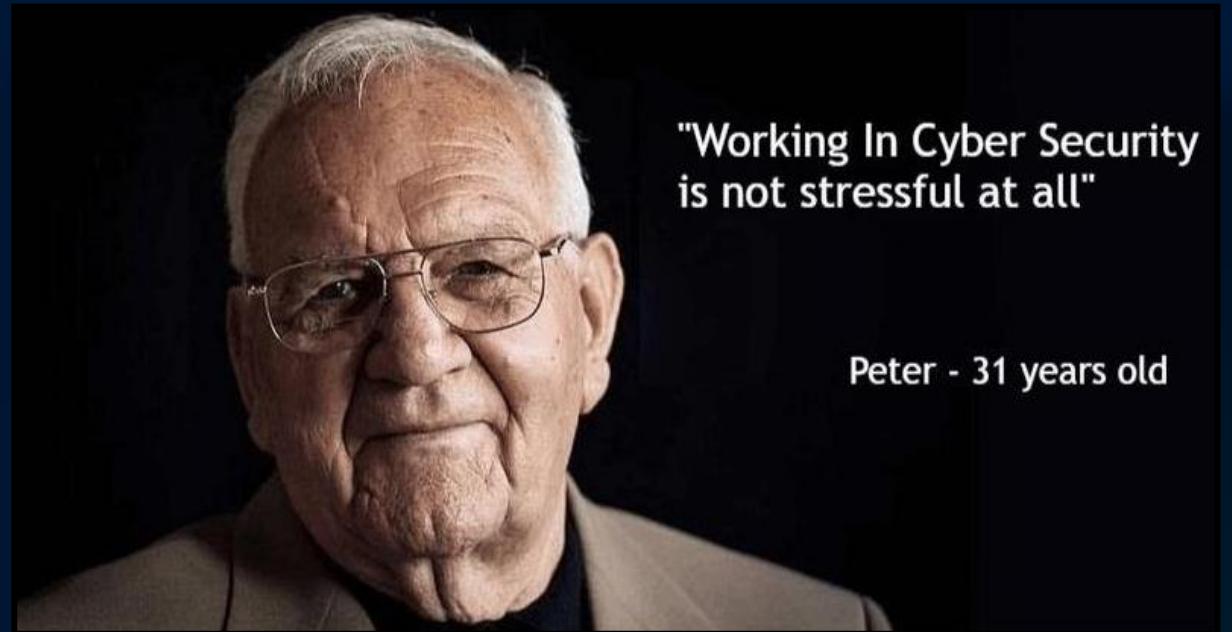
Lessons  
Learned?

Any Questions?





Peter – 20 years  
old



"Working In Cyber Security  
is not stressful at all"

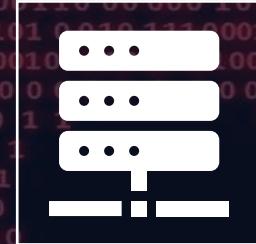
Peter - 31 years old

Peter with data

# Red Flags in Vulnerability Pattern



During initial analysis, forensic investigators observed a suspicious pattern



Multiple critical vulnerabilities were present on the same system:

SQL Injection in HR web portal

Remote File Inclusion (RFI) upload capability

Privilege escalation via sudo misconfiguration (vim NOPASSWD for daemon)

This combination felt unusual and intentional, not accidental.

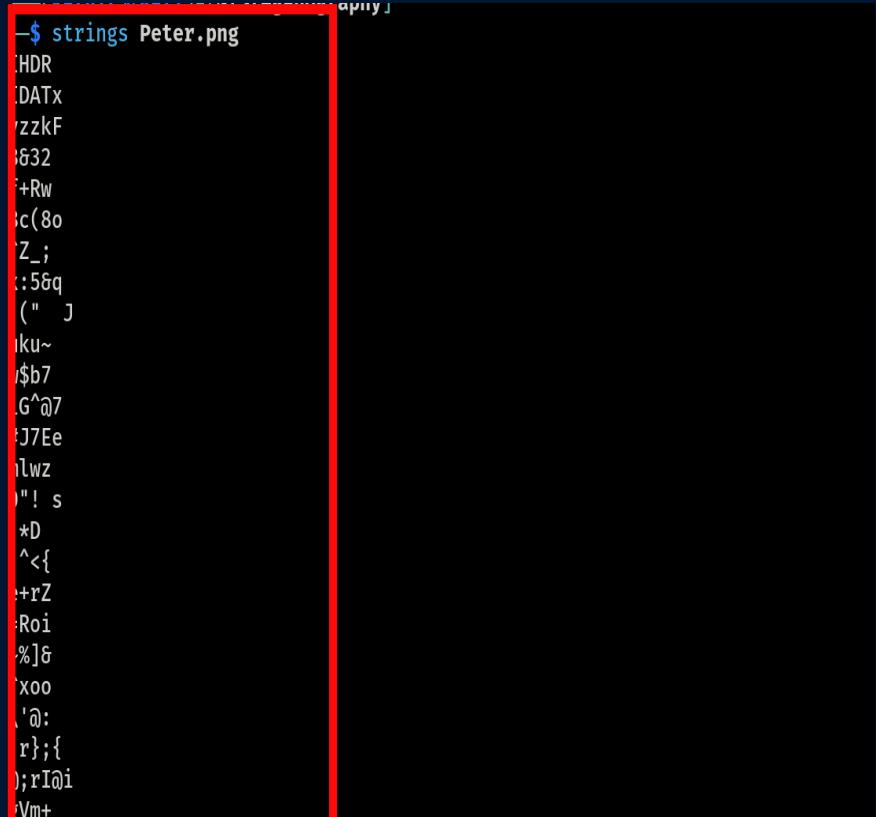


Decision was made to perform deep-dive forensic analysis on the full disk image of the machine to identify potential insider involvement.

Truths are yet to be uncovered...

# Steganography techniques found

```
$ strings Peter.png
```



```
[HDR
DATX
zzkF
&32
+Rw
c(80
Z_;
::5&q
(" J
iku~
$b7
.G^@7
J7Ee
lwz
!" s
*D
^<{
+rZ
:Roi
%]g
xoo
`@:
r};{
);rI@i
\m+
```

```
(kathir㉿Kali)-[~/Steganography]
$ python3 Steganography.py

Steganography found and extracting the message:

Employee ID,Full Name,SSN
EID1023,James McKenzie,694-22-7813
EID1024,Alexis Knight,106-99-8878
EID1025,Brittany Johnson,159-77-7857
EID1026,Haley Harris,843-12-2686
EID1027,Samantha Savage,136-74-4273
EID1028,Melinda Torres,309-94-4515
EID1029,Emily Watkins,531-93-8018
EID1030,Michele Smith,204-91-3129
EID1031,Sean Petty,552-57-2208
EID1032,Amy Moyer,392-93-2615
EID1033,Jennifer Fleming,290-41-7920
EID1034,Laura Pierce,587-84-2329
EID1035,Katherine Ortiz,402-62-6303
EID1036,Cynthia Marshall,164-35-6683
EID1037,Charles Rivera,835-86-6188
EID1038,Theodore Smith,324-87-4168
EID1039,Vanessa Nguyen,754-51-2792
EID1040,Bobby Wood MD,152-51-8169
EID1041,Scott Garcia,116-86-7795
EID1042,Victor Reilly DVM,830-91-7003
EID1043,Timothy Barron,765-16-1321
```

# Steganography techniques found in Faraz directory

While analyzing Faraz's user directory from the disk image

Investigators discovered **suspicious image files**

One image was confirmed to contain **hidden SPII (SSNs and employee data)** using **steganographic techniques**

This immediately raised concern:

Why was sensitive HR data embedded inside media files?

Who had access to both HR data and stego tools?

To confirm **how and when** the data was accessed:

The team began reviewing **authentication logs** (`/var/log/auth.log`)

Auth log review focused on:

Sudo sessions

User switches (su)

Access timestamps to `/home/hrmanager`



*Wait a minute, who are you?*

```
2025-04-15T00:00:57.405323-04:00 victim sudo: hrmanager : TTY=pts/0 ; PWD=/home/hrmanager ; USER=root ; COMMAND=/usr/sbin/usermod -aG sudo faraz
2025-04-15T00:00:57.455370-04:00 victim usermod[47226]: add 'faraz' to group 'sudo'
2025-04-15T00:00:57.456161-04:00 victim usermod[47226]: add 'faraz' to shadow group 'sudo'
```

## Privilege escalation

```
2025-04-15T00:33:07.643585-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/ls -a /home/hrmanager/.importantfiles/key
2025-04-15T00:33:07.646674-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:34:27.571117-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/.importantfiles/key/hr_key.txt /home/faraz/Documents/interesting.txt
2025-04-15T00:34:27.572997-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:35:44.944016-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents ; USER=root ; COMMAND=/usr/bin/ls -a /home/hrmanager/.importantfiles/
2025-04-15T00:35:44.947034-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:36:43.828156-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/.importantfiles/ssn_data.enc /home/faraz/Documents/very interesting.enc
```

## Encryption key extraction

```
2025-04-15T00:43:02.093297-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/Documents/.confidential/.secret.tar.xz.gpg /home/faraz/Documents/others
2025-04-15T00:43:02.098157-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:43:53.521806-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/mv .secret.tar.xz.gpg easy.tar.xz.gpg
```

## Encrypted file extraction

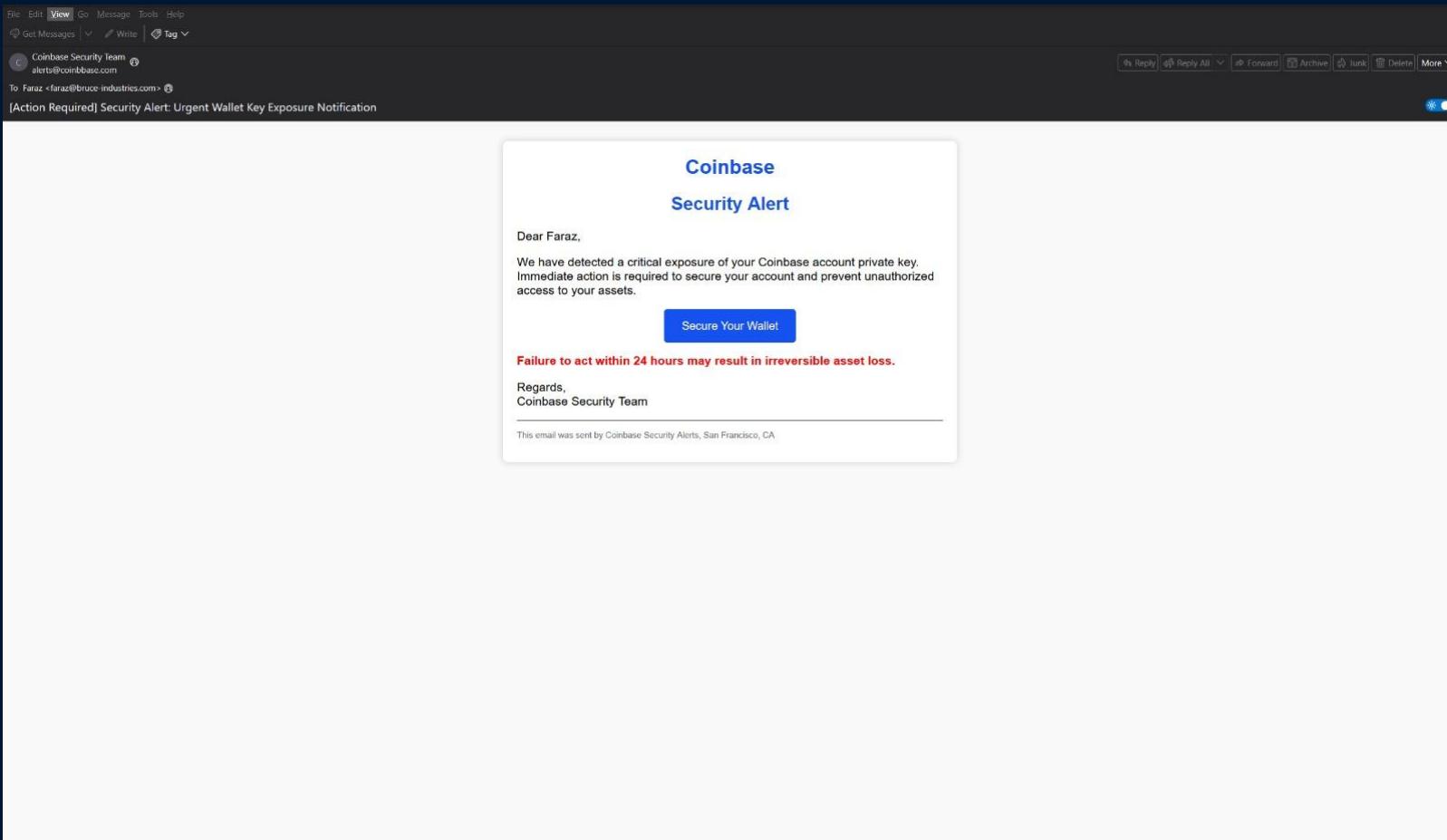
```
2025-04-15T00:55:12.173872-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/cat /home/hrmanager/.local/share/Trash/files/deletethis.txt
2025-04-15T00:55:12.176116-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:55:54.924706-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/gpg --decrypt easy.tar.xz.gpg
2025-04-15T00:55:54.927821-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:56:20.202052-04:00 victim sudo: faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/gpg --decrypt easy.tar.xz.gpg
```

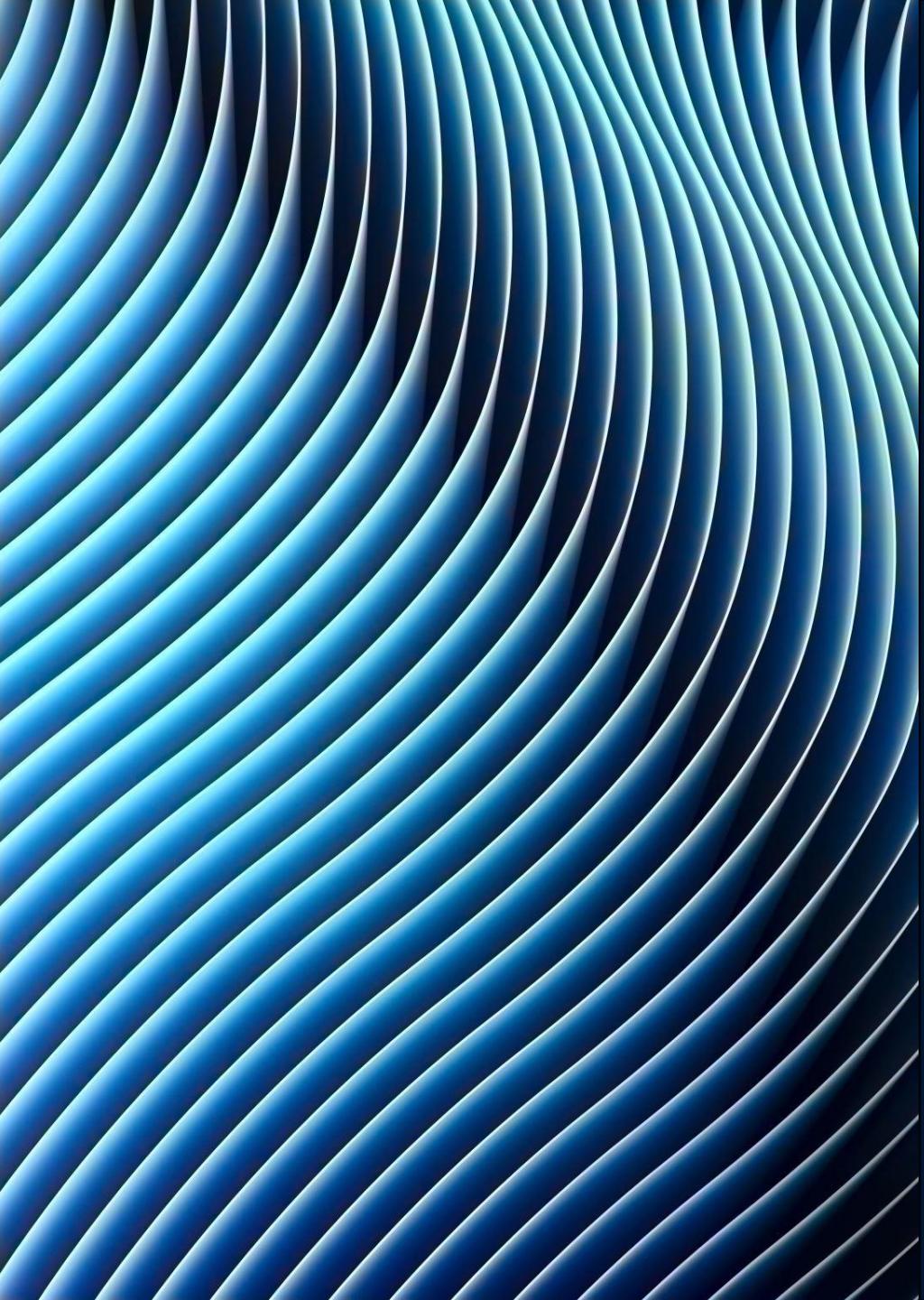
## Decryption

# Phishing Email Never reported: A Turning Point in the Case

- During the investigation, a **phishing email** was found in Faraz's inbox:
- Received from alerts@coinbbase.com (typo squatted domain)
- Posed as a security alert from Coinbase
- **Faraz never reported this email** to the security team
- Contained a **link to a fake website** with threatening instructions to Faraz
- This became a **critical red flag**:
- Showed lack of compliance with phishing awareness protocols
- Suggested **possible cooperation** or intentional negligence
- The email became a **key pivot point** in shifting Faraz's role from victim to potential insider

# Initial mail received from Coinbase





The phishing email included a link to:  
[https://www.coin  
base.com-  
security-  
alerts.com/](https://www.coinbase.com-security-alerts.com/)



To avoid interaction with a live malicious server, the team used a **safe, automated screenshot tool** to analyze the link's destination



The screenshot revealed



A **fake Coinbase-branded webpage**



A threatening message directed at Faraz



Demands to follow future instructions, including vulnerability injection



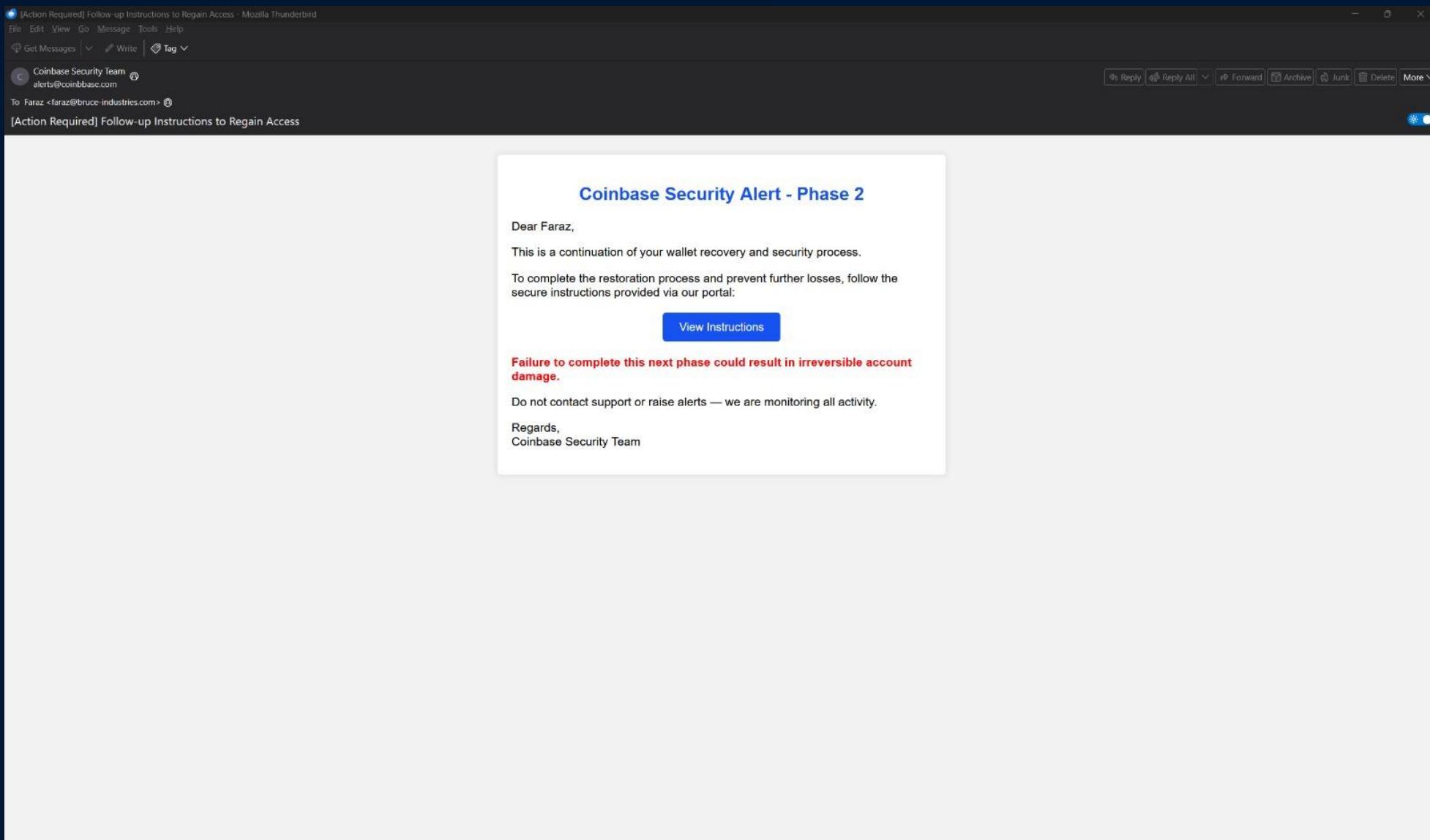
This confirmed that the email was part of a **coercive phishing campaign**, contributing to Faraz's compromised behavior

# The message for Faraz is

coinbase

Cryptocurrencies Individuals Businesses Institutions Developers Company Sign in Sign up

# Second phishing mail



# Instructions given in second mail

coinbase

Cryptocurrencies Individuals Businesses Institutions Developers Company Sign in Sign up



Hey Faraz,

### Final Instructions

This is your next step to avoid permanent loss:

- Introduce a **Remote File Inclusion (RFI)** vulnerability into the HR portal you are managing.
- Ensure the portal also has a **SQL Injection** vulnerability available for remote querying.
- Modify the sudoers configuration to add **NOPASSWD for vim** under the daemon account hosting the website.
- Make these changes discreetly without raising suspicion.
- Don't be dumb enough to exfiltrate data from your account, your organization has TLS interception, so you'll get caught easily.

**⚠ Remember: Any alert to the security team will trigger the permanent loss of your 2 BTC and expose your activities.**

Future instructions will be communicated through this secure channel only.

Just follow instructions — or lose everything.

- After the **first phishing email**, Faraz:
  - Accessed sensitive HR data
  - Transferred it into his **own user account**
  - Attempted to hide it using **steganography techniques**
  - However, due to the organization's **TLS interception**, Faraz realized:
    - His traffic could be monitored
    - Direct data exfiltration from his account would expose him as an insider
  - Shortly after the **second phishing email**, his behavior changed:
    - Timeline aligned perfectly with these events
    - **Stopped using his account** for further actions
    - Followed the attacker's next set of instructions
      - **Planted vulnerabilities** (SQLi, RFI) in the HR portal
      - Modified sudoers to allow NOPASSWD privilege escalation for the daemon user
      - Acted more like a **facilitator**, not a direct exfiltrator
      - It was unknown who was the one instructing Faraz...yet

# Final Remarks

Faraz received a malicious email which was not reported

Evidence shows Faraz intentionally vandalized the HR portal

It was unknown who was the one instructing Faraz...yet

Allowed for an unauthorized individual to export sensitive information



lafuddyduddy

# Disclosure



After the investigation is complete, the CISO reveals the incident was a controlled simulation

TLS interception resulted in unintentional decryption of Faraz's Coinbase wallet  
CISO saw this as a training opportunity



Assess the teams under real pressure and psychological stress, also to assess the effectiveness of Forensics team.



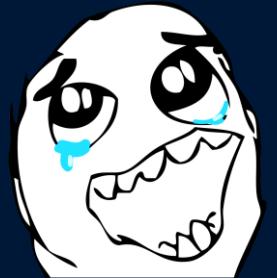
CISO seized 1 bitcoin of Faraz as a Penalty

A stylized illustration of a man with dark hair and sunglasses, wearing a grey suit and tie, standing with his arms outstretched wide. He is positioned in front of a background of a digital city with numerous small buildings and a large, jagged mountain-like structure on the right. Below him, the word "ABSOLUTE" is written in large, blocky, black and white pixelated letters, followed by "INJECTION" in a similar style below it.

ABSOLUTE  
INJECTION

Faraz was not harmed  
during this project (I was)

---



Thanks Prof. Dominic Sellitto, CISSP for providing two Virtual Machines



# Thank You

Let us know if you have any questions!!!