Introduction to Network Forensics

Detecting exfiltration on a large finance corporation environment

Toolset, Document for students

1.0
JANUARY 2019

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use:

csirt-relations@enisa.europa.eu
PGP Key ID: 31E777EC 66B6052A
PGP Key Fingerprint: AAE2 1577 19C4 B3BE EDF7 0669 31E7 77EC 66B6 052A

For media enquiries about this paper, please use:

press@enisa.europa.eu.

ISBN: 978-92-9204-288-2, DOI: 10.2824/995110

Table of Contents

PARAMETER	DESCRIPTION	DURATION
Main Objective	Participants will set up their own lab environment, consisting of two virtual machines. For the first part of the exercise, basic VM images with preloaded files are provided. The installation and configuration process include: compiling software from the source, generating TLS/SSL certificate files, setting up the Certificate Authority, configuring web browser to recognise proxy server as CA and configuring proxy log analysis tool - SARG. The second part of the exercise will begin with participants receiving a firewall log. After analysis and comparing the results against MISP database, proxy server logs will be checked for: four infected hosts, exfiltrated database filenames, text storage site address and new malicious Command & Control server address. At the DNS part, participants will learn how to analyse provided BIND logs using popular Linux tools and simple scripts, and look for evidence of exfiltration against another technique.	
Targeted Audience	The exercise is dedicated to less-experienced CSIRT staff involved in network forensics. The exercise is expected to be also of value to more experienced CSIRT team members, involved in daily incident response.	
Total Duration	6.0 hours	
Time Schedule	Introduction to the exercise and tools overview	1 hour
	Setting up the environment	2 hours
	Log analysis	3 hours
	Introduction to DNS protocol	1 hour
	BIND log analysis	1 hour
Frequency	It is advised to organise this exercise when new team members join a CERT/CSIRT.	

1. What Will You Learn?

1.1 Detecting exfiltration on a large finance corporation environment

During the course of this exercise, participants will learn the basic concepts of the proxy server operation, and how inspecting the SSL traffic can aid forensic investigators. Students will also learn about the Malware Information Sharing Platform (MISP) and the role in can play in threat analysis.

By working with crafted firewall and proxy server logs, trainees will learn the basic approach to log analysis, get familiar with basic Linux command line tools and discover what kind of information can be extracted by combining them with MISP database.

Additionally, students will work with BIND logs learning about more concealed way of data exfiltration using DNS protocol. In this part, participants will analyse provided log files looking for evidence of data exfiltration with common Linux tools like grep and search for anomalous DNS queries. By working with simple Python script trainees will look for signs of data exfiltration logfiles using basic statistical analysis.

2. Introduction

2.1 Squid Proxy Server configuration

The two Virtual Machine images for the Squid Server and Squid Client can be downloaded here:

https://www.enisa.europa.eu/ftp/ENISA_INF_Squid_Server_5.2.ova
https://www.enisa.europa.eu/ftp/ENISA_INF_Squid_Client_5.2.ova

Both of them can be accessed using same credentials:

Credentials to the machine:

PARAMETER	VALUE
Username	squid
Password	squid

The exercise should be conducted using *squid* user account. If there is a need to access root account, the password is also **squid.**

First step is to compile the software from the source on the Squid Server machine. Source files have been preloaded to the **/home/squid/squid-3.5.27** folder.

Issuing these commands will install Squid and set the ownership to *squid* user:

```
cd squid-3.5.27

./configure --enable-ssl-crtd --with-openssl

sudo make && sudo make install

sudo chown squid:squid -R /usr/local/squid
```

PLEASE NOTE: compiling the software can take up to 10 minutes.

In order for Squid Server to able to inspect SSL traffic, it needs to act as a trusted Certificate Authority. For that purpose, a certificate needs to be generated:

```
mkdir /usr/local/squid/ssl_cert

cd /usr/local/squid/ssl_cert

openssl req -new -newkey rsa:4096 -sha256 -days 365 -nodes -x509 -extensions
v3_ca -keyout squid.pem  -out squid.pem

openssl x509 -in squid.pem -outform DER -out squid.der
```

No additional data needs to be provided during the creation of certificate.

Squid configuration file needs to be adjusted to activate the SSL inspection capabilities. The path to config file is **`/usr/local/squid/etc/squid.conf`**.

Line 59, containing the **`http_port 3128`** needs to be commented our or removed. At the end of file, these directives need to be added:

```
http_port 0.0.0.0:3128 ssl-bump cert=/usr/local/squid/ssl_cert/squid.pem
generate-host-certificates=on  dynamic_cert_mem_cache_size=4MB
sslcrtd_program /usr/local/squid/libexec/ssl_crtd -s /var/lib/ssl_db -M 4MB
acl step1 at_step SslBump1
acl exceptions ssl::server_name .10.1.1.1
ssl_bump splice exceptions
ssl_bump peek step1
ssl_bump bump all
```

SSL certificate database needs to be activated and its ownership changed to *squid* user:

```
sudo /usr/local/squid/libexec/ssl_crtd -c -s /var/lib/ssl_db -M 4MB
sudo chown squid:squid /var/lib/ssl_db
```

Squid software is activated by issuing the command:

```
/usr/local/squid/sbin/squid
```

If proxy server is up and running, netstat command will show that the machine is listening on port 3128:

```
netstat -plnt
```

```
squid@squid_server:/usr/local/squid/ssl_cert$ netstat -plnt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3128            0.0.0.0:*               LISTEN      11415/(squid-1)
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
squid@squid_server:/usr/local/squid/ssl_cert$
```

Figure 1. Netstat showing Squid proxy listening on port 3128

Below command will show a preview of proxy log file:

```
tail -f /usr/local/squid/var/logs/access.log
```

2.2 Squid Client configuration

CA needs to be imported to client's web browser. Previously generated file can be obtained by issuing the command:

```
scp squid@10.1.1.1:/usr/local/squid/ssl_cert/squid.der ~
```

Client comes preinstalled with Firefox browser. Certificate can be imported by navigating to the Settings and selecting *Privacy and Security => Certificates* option:

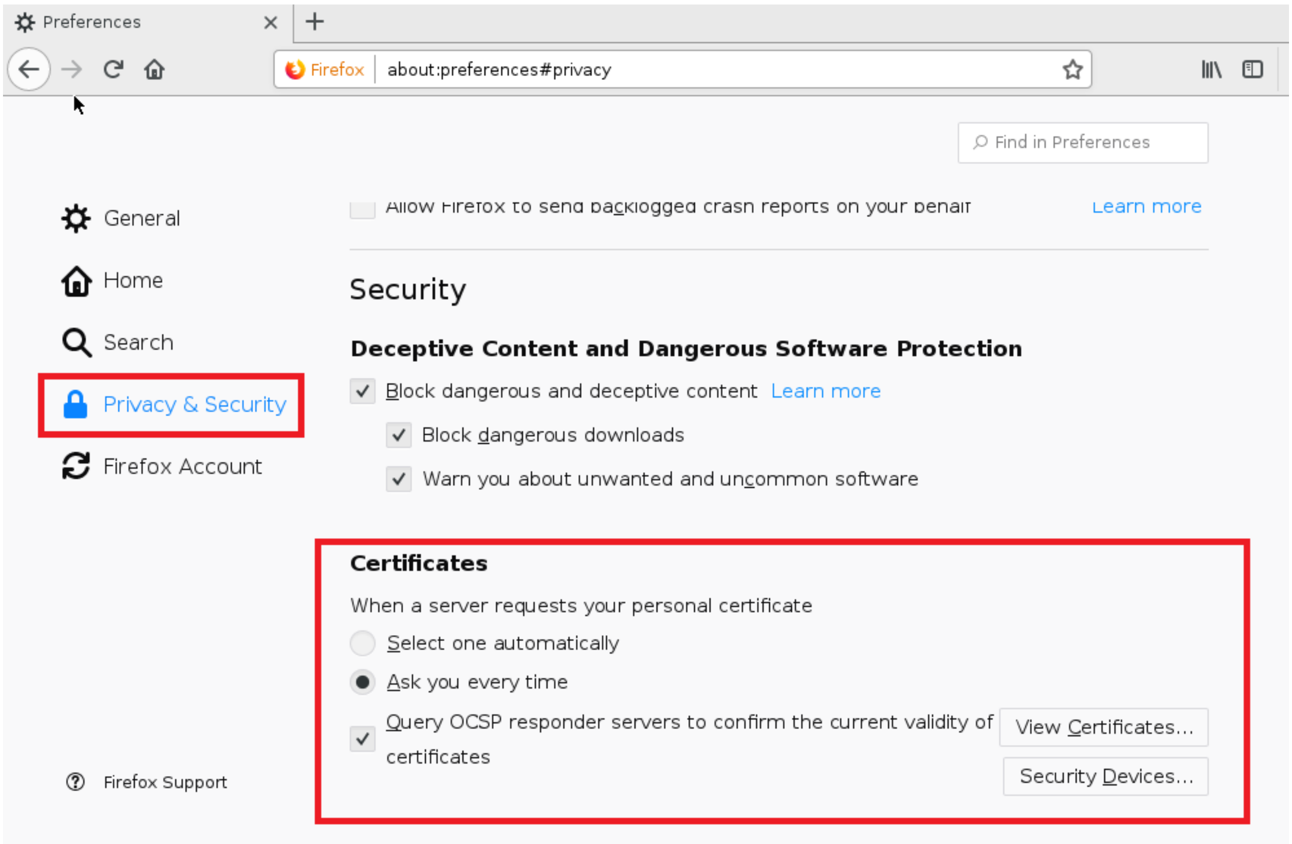


Figure 2. Firefox privacy and security settings

The *Authorities* tab allows to import the *.der file:

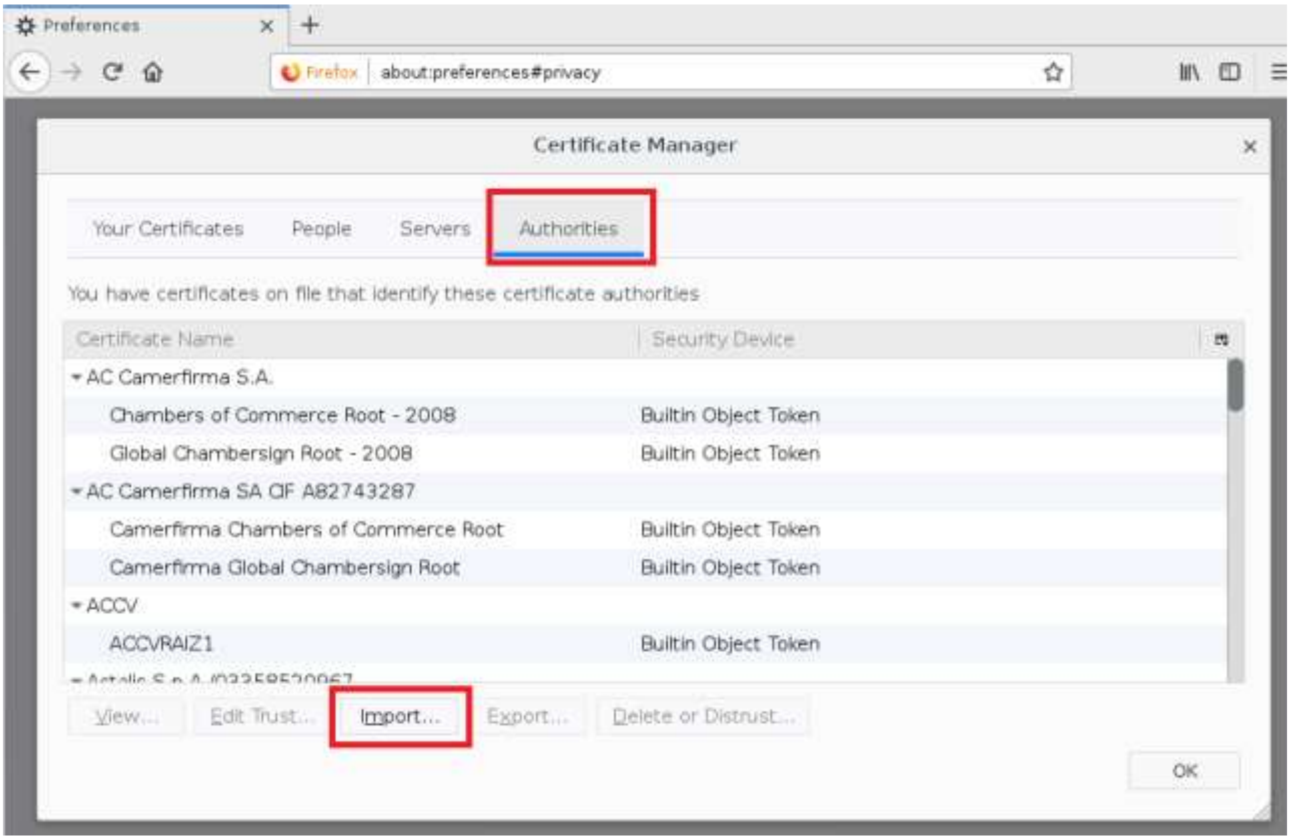


Figure 3. Firefox – importing CA file.

Pop-up window will appear, asking about the scope of certificate trust. *Trust this CA to identify websites* is sufficient for conducting this exercise:

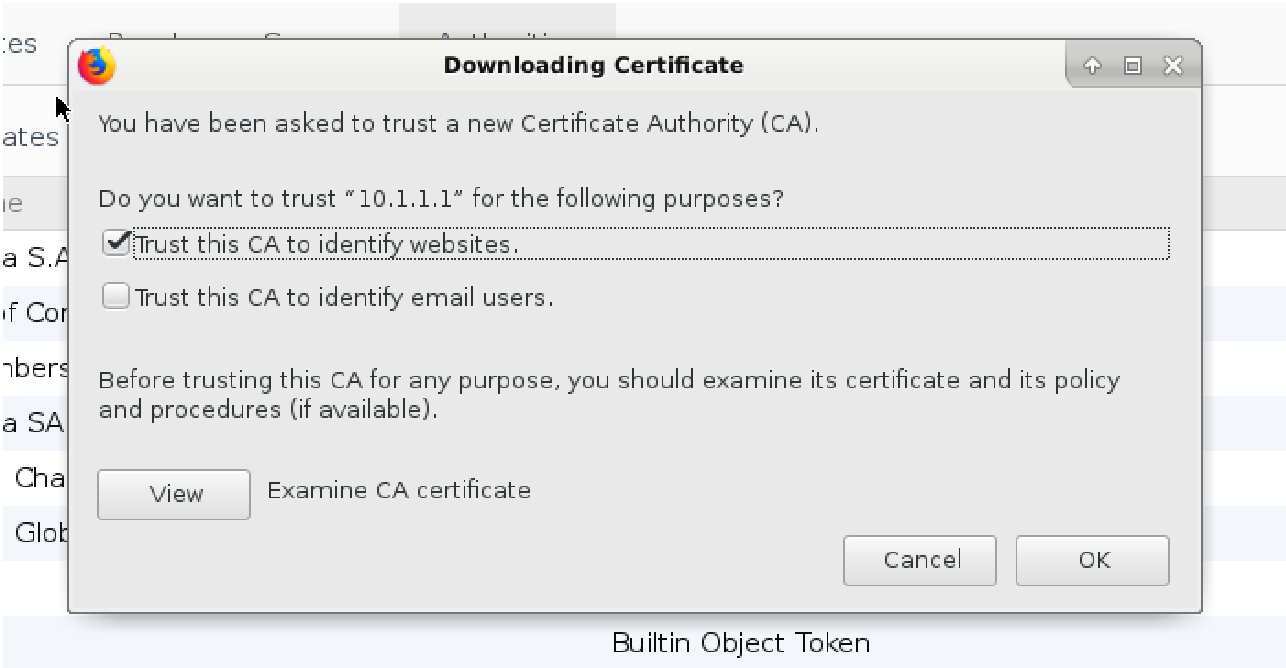


Figure 4. CA trust scope

CA certificate is in place, now the browser needs to be pointed to the address of the proxy server, so that all of the traffic goes through it. *Network Proxy* section can be found in *General* settings:

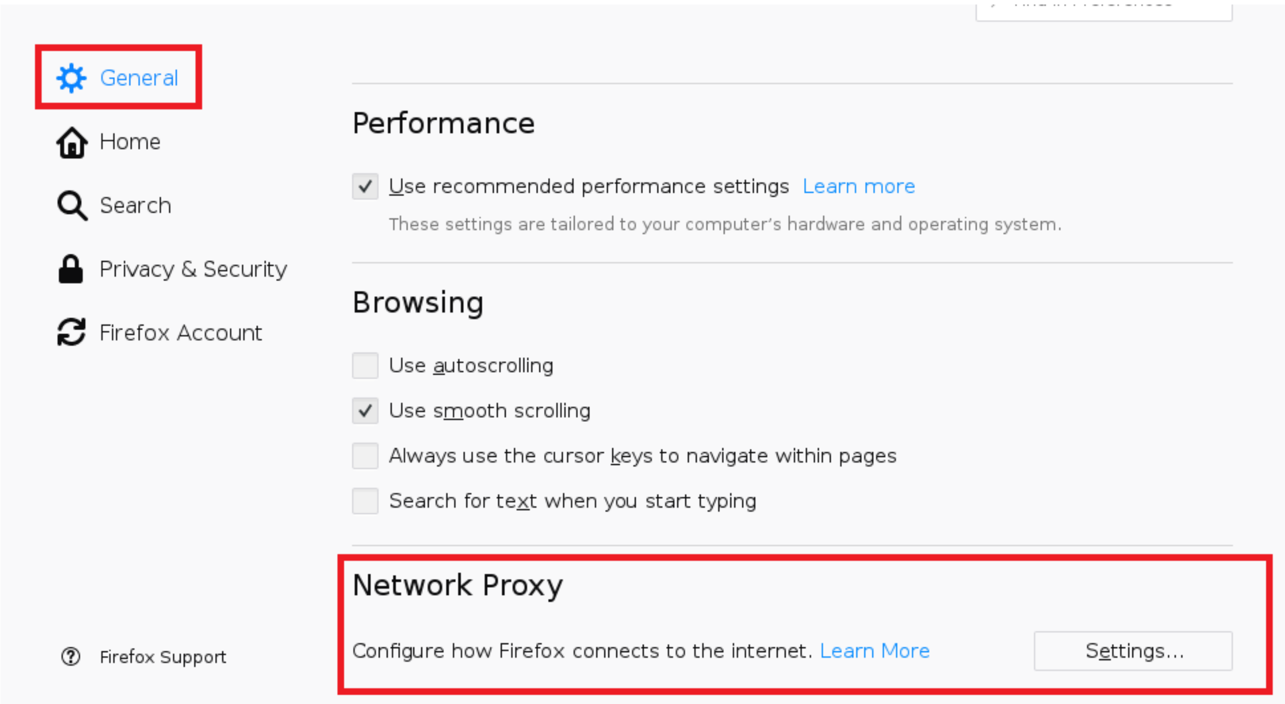


Figure 5. Firefox proxy settings

Squid Server IP address is statically set to 10.1.1.1, the port is 3128:

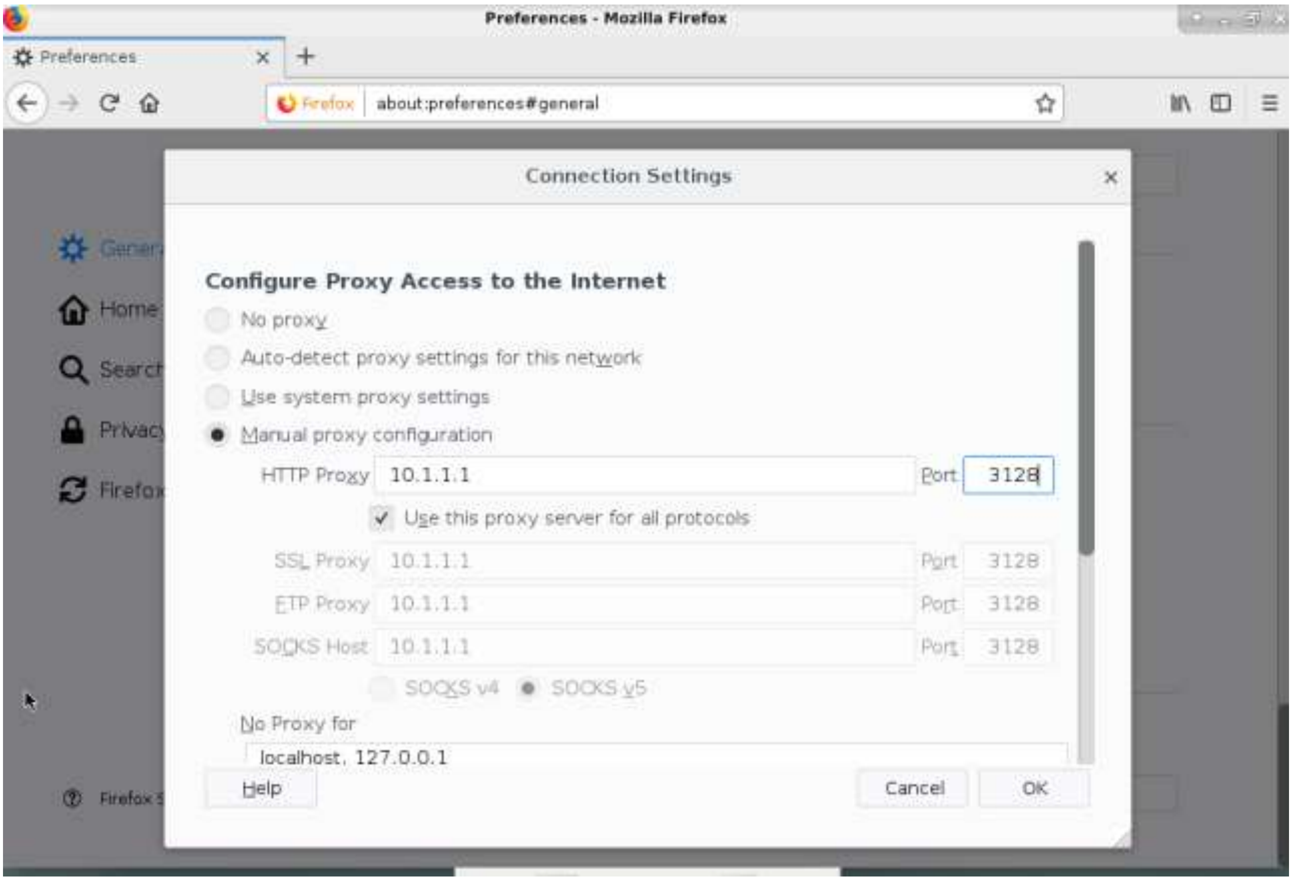


Figure 6. Proxy setting in Firefox

If client starts browsing the Internet, the *access.log* will begin to capture information about visited sites.

2.3 Squid Analysis Report Generator (SARG)

Sarg is a handy tool, designed specifically to work with Squid Software and it provides a quick view on the activity of all the machines in given network segment. It can be installed from the repository:

```
sudo apt install sarg
```

SARG operates on Squid's *access.log* file, so the path to the file needs to be provided in the configuration file **`etc/sarg/sarg.conf`** . Line 7 needs to be changed to:

```
/usr/local/squid/var/logs/access.log
```

Reports are generated by issuing the command:

```
sudo sarg -x
```

And accessed via web browser under the sarg.local address:

Figure 7. SARG web panel

3. Exercise Tasks

3.1 Network Traffic Analysis

Squid_client machine has been preloaded with two crafted log files that will be used in this part of exercise. Both are stored in **/home/squid/exercise_logs** directory:

- firewall.log – pfSense firewall log
- access.log – Squid proxy log

As a prerequisite, two additional commands need to be issued on the Squid_server VM:

```
sudo cp /root/access.log /usr/local/squid/var/logs/
sudo sarg -x
```

The analysis should start with firewall log file. Some basic statistical information can be obtained by issuing below commands:

```
wc -l firewall.log
```

Shows that the file has 7919 lines;

```
grep "block" firewall.log | wc -l
```

Shows that all of these 7919 lines are requests blocked by firewall

```
awk -F, '{print $17}' firewall.log | sort | uniq
```

Returns information about L4 protocols (and ICMP)

```
awk -F, '{print $17}' firewall.log | grep "tcp" | wc -l
awk -F, '{print $17}' firewall.log | grep "udp" | wc -l
awk -F, '{print $17}' firewall.log | grep "icmp" | wc -l
```

Will show how many requests correspond to each of the L4 protocols that has been used. The majority of traffic has been generated by TCP protocol.

```
awk -F, '{print $22}' firewall.log | sort | uniq -c | sort -n
```

Shows number of occurrences of ports that have been used by L4 protocols:

```
squid@squid_client:~$ awk -F, '{print $22}' firewall.log | sort | uniq -c | sort -n -r
   1264 443
    951 17500
    850 138
    657 23
    528 8610
    411 137
    297 7547
    291 8291
    158 80
    146 25
```

Figure 8. Most popular protocols

Below commands:

```
awk -F, '{print $19}' firewall.log | sort | uniq | wc -l
awk -F, '{print $20}' firewall.log | sort | uniq | wc -l
```

Will return the total number of unique IP source and destination addresses accordingly.

It is known from the scenario, that the data was exfiltrated to external service. This means that private IP address range can be excluded from the destination IP addresses. It is also known, that machines in this particular company operate in the 10.x.x.x IP address range. Below command:

```
awk -F, '{print $20}' firewall.log | grep -v "10.*" | sort | uniq | wc -l
```

Will return 136 unique IP addresses that do not belong to 10.x.x.x range. These addresses can be checked against MIPS database.

Local MISP instance can be accessed via web browser, the address is misp.local. User credentials are:

User: squid@example.com

Password: Password1234

PLEASE NOTE: Password is case sensitive

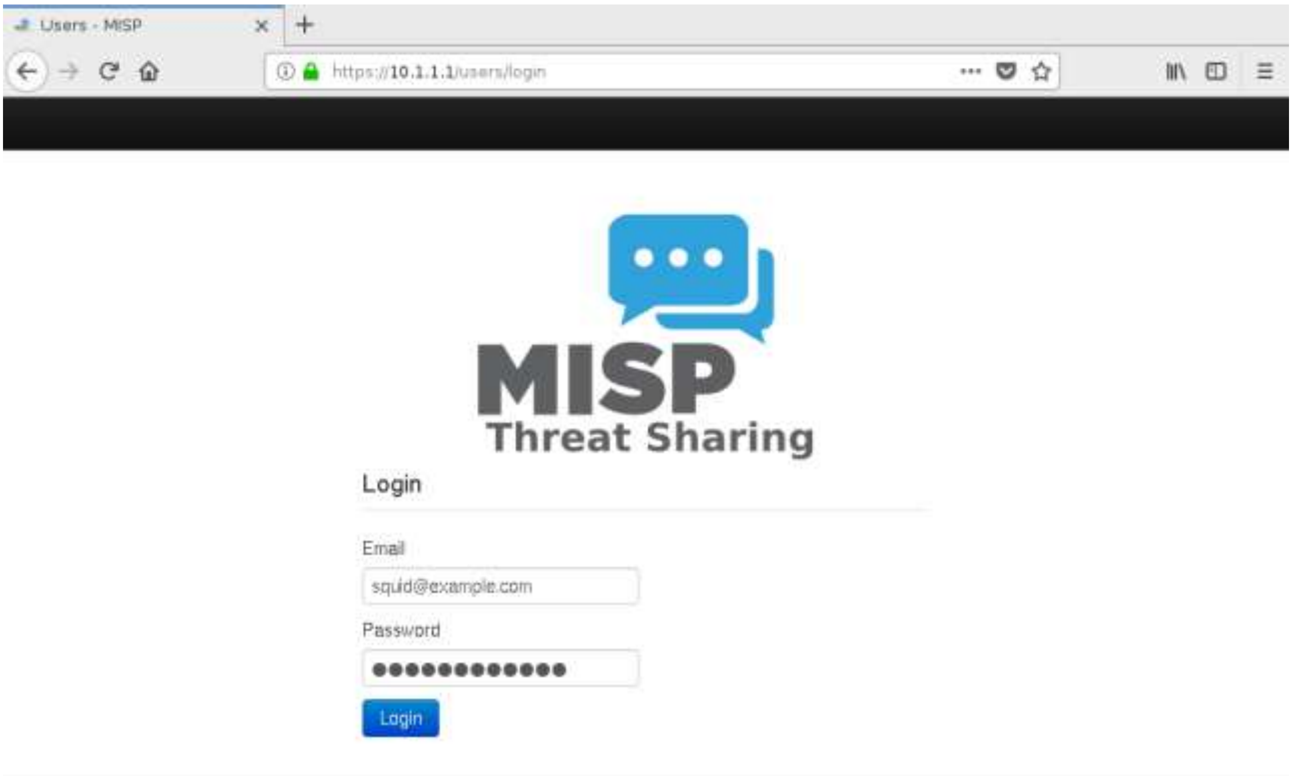


Figure 9. MISP login screen

All IP addresses can be checked by navigating to *Actions => Search Attributes:*

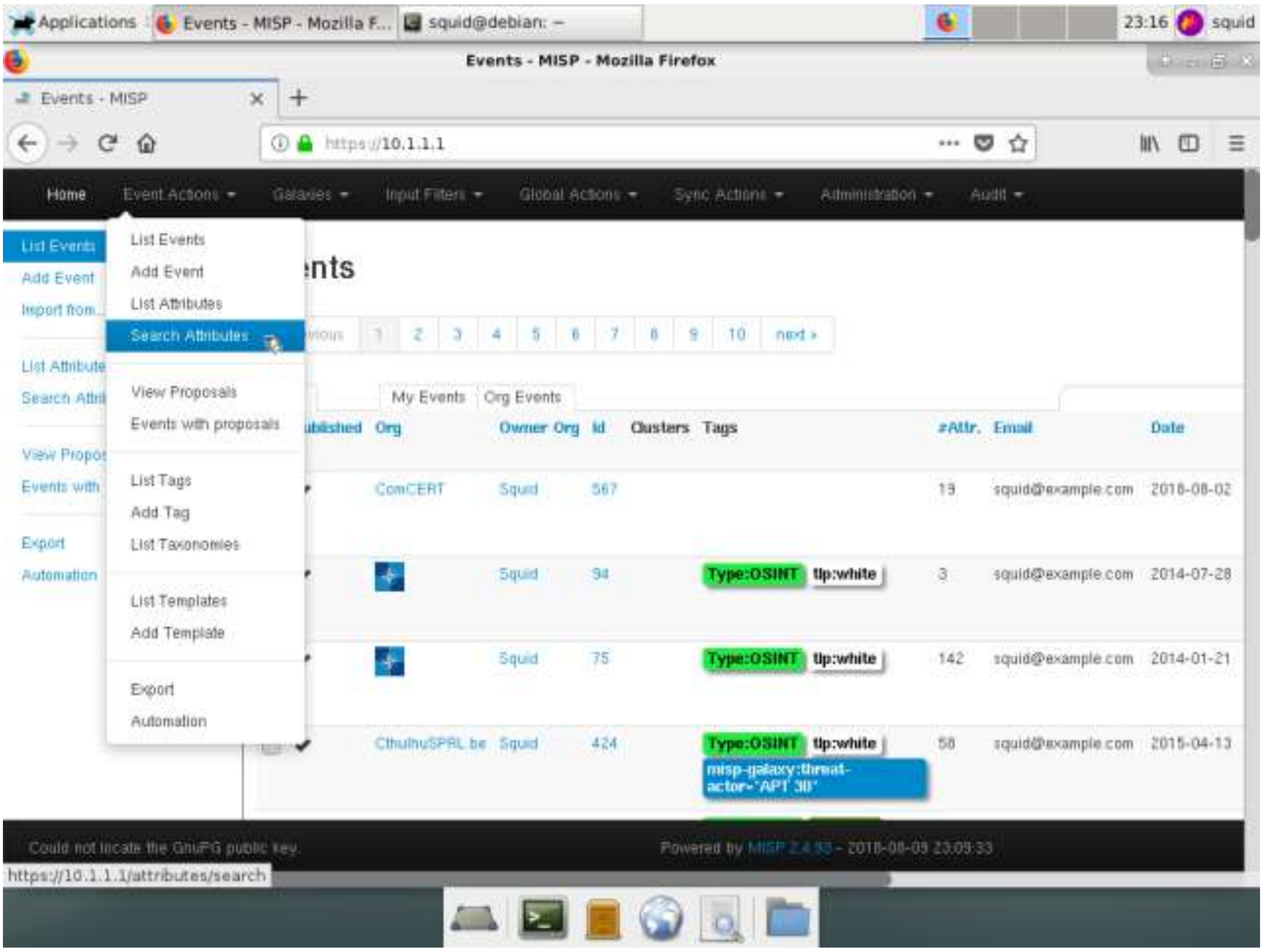


Figure 10. MISP Database with Options Menu

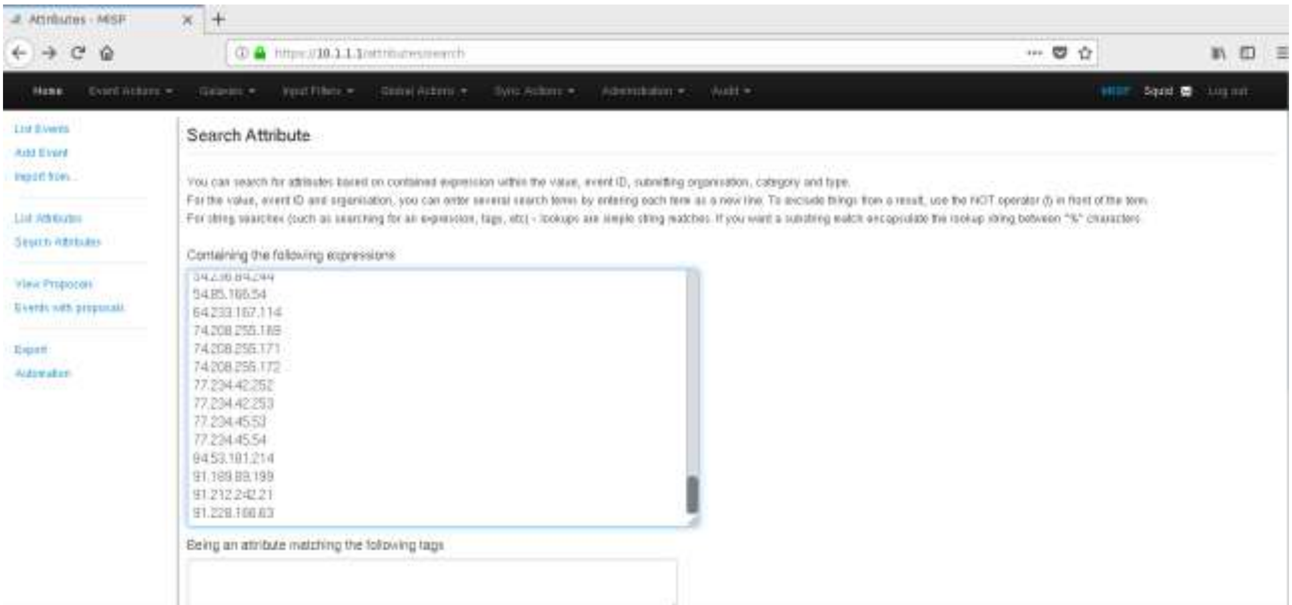


Figure 11. Search for Attributes

After clicking the *Search* button at the bottom of the page, this result can be seen:

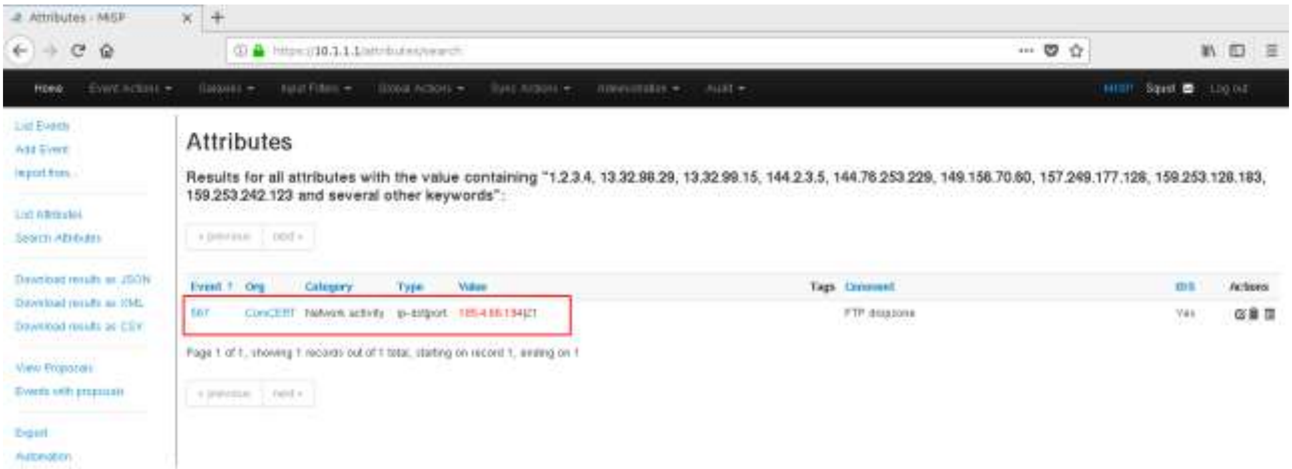


Figure 12. Match found in MISP

There is a match in MISP event number 567. IP Address 185.4.66.194 has been involved in some malicious activity. By clicking on the Event ID, additional information can be obtained.

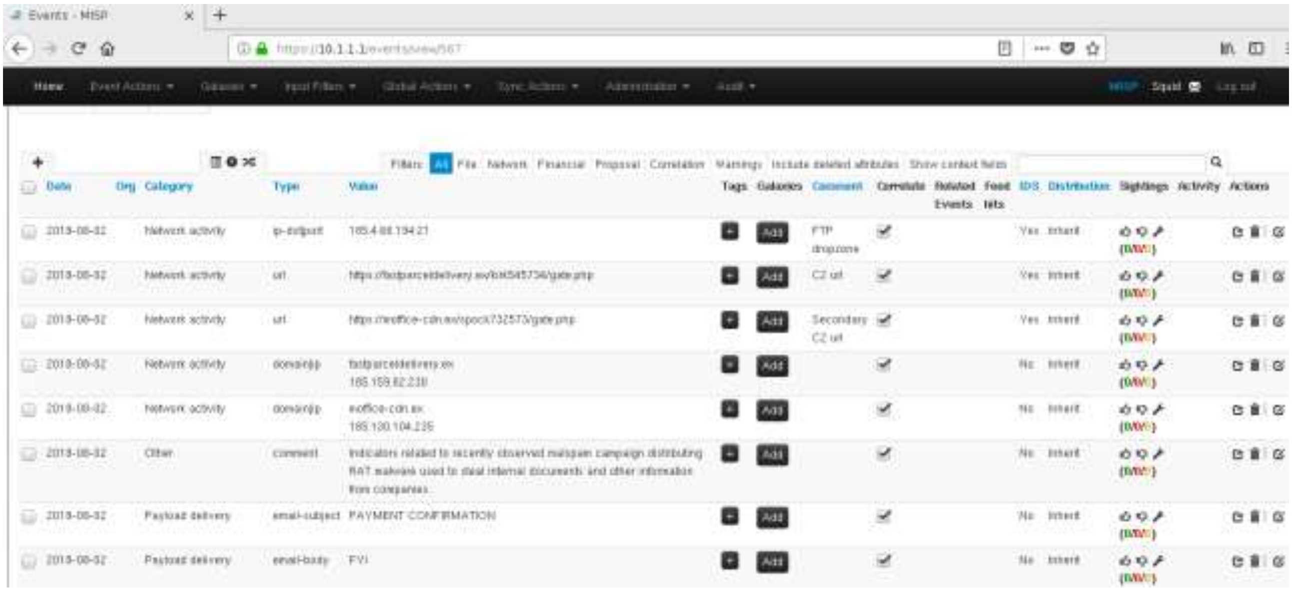


Figure 13. Collection of attributes belonging to Event 567

In the course of this exercise, C2 servers URL addresses as well as FTP host will be used:

- hxxps://fastparceldelivery[.]ex/kirk545734/gate.php
- hxxps://moffice-cdn[.]ex/spock732573/gate.php
- 185.4.66.194

PLEASE NOTE: in this particular scenario, the number of IP addresses is fairly low and can be easily processed by MISP in web panel. In cases, where there are many more IOCs to check, it is better to use MIPS's API.

IP address obtained from MISP can now be checked against firewall log to search for more information:

```
grep "185.4.66.194" firewall.log
```

```
squid@squid_client:~$ grep "185.4.66.194" firewall.log
Aug  3 10:53:42 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33722,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
Aug  3 10:53:43 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33723,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
Aug  3 10:53:45 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33724,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
Aug  3 10:53:49 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33725,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
Aug  3 10:53:57 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33726,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
Aug  3 10:54:13 fw0.mycompany.ex filterlog: 117,16777216,,1533225116,em1_vlan10,match,block,in,4,0x0,,64,33727,0,DF,6,tcp,60,10.0.10.202,185.4.66.194,33908,21,0,S,1316528098,,29200,,mss;sackOK;TS;nop;wscale
```

Figure 14. Connections to malicious IP address

From this query, it can be deduced that a connection attempt to a suspicious address was made on August the 3rd at 10:53:42. The source address was internal host 10.0.10.202, and the attempt was blocked by firewall. Destination IP was 185.4.66.194 on port 21, which suggests that this was an ftp connection attempt.

Firewall log analysis summary:

Total number of source IP addresses:	**1270**
Total number of destination IP Addresses:	**185**
IP Protocols that have been used:	**UDP, TCP and ICMP**
Well-known services that have been used:	**http, https. SSH, NetBIOS, smpt**
IP Address of the infected machine:	**10.0.10.202**
Malicious IP Address:	**185.4.66.194**
Time frame of the attack:	**10:53:42 – 10:54:13**

C2 server URLs. These can now be checked against Squid log file. The addresses are:

- hxxps://fastparceldelivery[.]ex/kirk545734/gate.php
- hxxps://moffice-cdn[.]ex/spock732573/gate.php

Since there are only two address to be checked, grep can be used:

```
grep https://fastparceldelivery.ex/kirk545734/gate.php access.log
grep https://moffice-cdn.ex/spock732573/gate.php access.log
```

First query yields no results, but the second one shows these log entries:

```
squid@squid_client:~$ grep https://moffice-cdn.ex/spock732573/gate.php access.log
1533282193.159    131 10.0.10.128 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533282673.159    131 10.0.10.111 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533283159.959    131 10.0.10.134 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533285883.559    131 10.0.10.128 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533286313.252    131 10.0.10.111 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533286733.759    131 10.0.10.134 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533289347.259    131 10.0.10.128 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
1533289773.929    131 10.0.10.111 TCP_MISS/200 35334 GET https://moffice-cdn.ex/spock732573/gate.php - HIER_DIRECT/185.130.104.235 text/html
```

Figure 15. Malicious domain found in Squid log

This indicates that some machines within the network have been infected with malware. Command:

```
grep https://moffice-cdn.ex/spock732573/gate.php access.log | awk '{print $3}'
| sort | uniq
```

Isolates three infected IP addresses: 10.0.10.111, 10.0.10.128, 10.0.10.134

```
squid@squid_client:~$ grep "https://moffice-cdn.ex/spock732573/gate.php" access.log | awk '{print $3}' | sort | uniq
10.0.10.111
10.0.10.128
10.0.10.134
```

Figure 16. IP addresses of infected hosts

Some more information can be easily obtained by looking through the SARG report. By navigating to sarg.local address, this report can be obtained:

SARG report for 2018 Aug 03

sarg.local/2018Aug03-2018Aug03/index.html

SARG Squid Analysis Report Generator

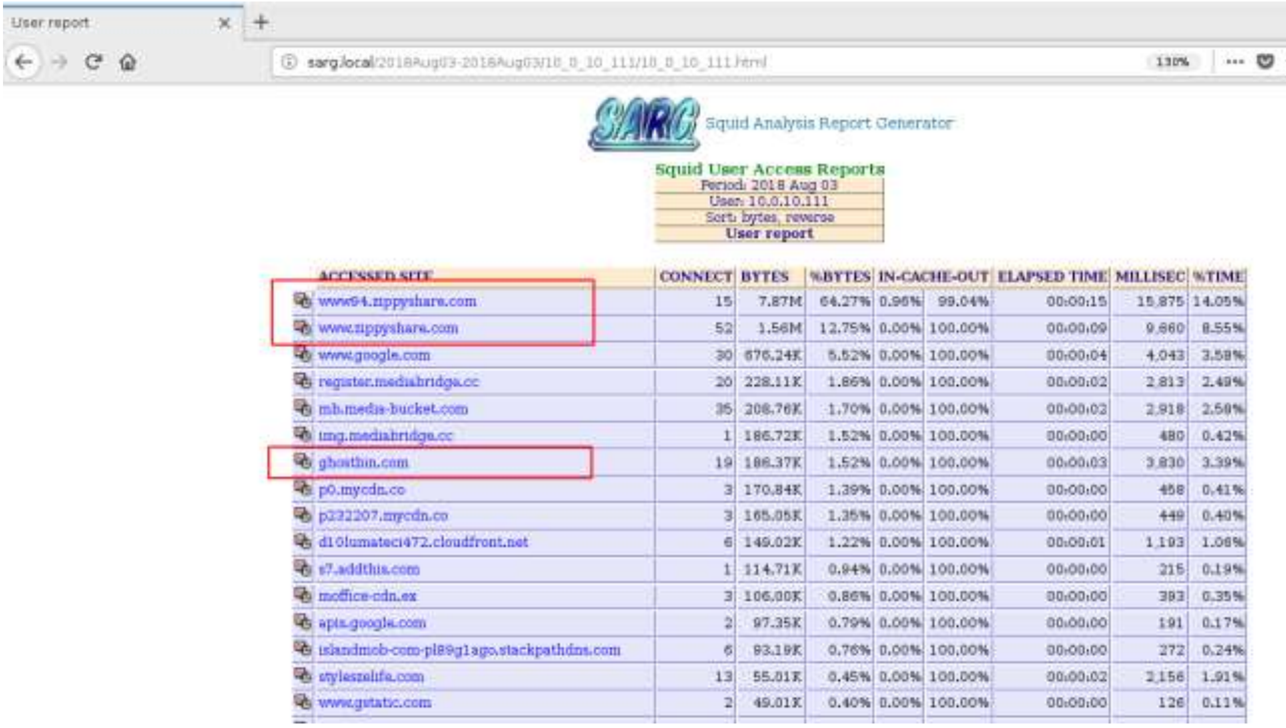
Squid User Access Reports
Period: 2018 Aug 03
Sort: bytes, reverse
Top users

Top sites
Sites & Users
Downloads

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1	10.0.10.101	72.15K	1.35G	14.24%	29.89%	70.11%	04:16:33	15,393,956	12.85%
2	10.0.10.166	58.12K	1.23G	12.94%	26.74%	73.26%	03:47:02	13,622,052	11.38%
3	10.0.10.205	61.92K	1.16G	12.23%	23.62%	76.38%	05:14:08	18,848,232	15.74%
4	10.0.10.184	55.23K	1.03G	10.91%	27.75%	72.25%	04:03:09	14,589,450	12.18%
5	10.0.10.172	55.23K	1.03G	10.91%	27.75%	72.25%	04:03:09	14,589,450	12.18%
6	10.0.10.173	48.06K	999.09M	10.50%	25.98%	74.02%	03:04:44	11,084,271	9.26%
7	10.0.10.102	48.79K	956.14M	10.05%	23.79%	76.21%	03:45:45	13,545,590	11.31%
8	10.0.10.119	40.63K	888.15M	9.33%	30.97%	69.03%	02:07:24	7,644,861	6.38%
9	10.0.10.152	38.92K	802.27M	8.43%	26.82%	73.18%	02:47:18	10,038,672	8.38%
10	10.0.10.151	361	17.46M	0.18%	3.46%	96.54%	00:01:56	116,669	0.10%
11	10.0.10.128	336	13.03M	0.14%	3.10%	96.90%	00:01:50	110,699	0.09%
12	10.0.10.111	461	12.26M	0.13%	0.61%	99.39%	00:01:52	112,977	0.09%
13	10.0.10.134	158	967.99K	0.01%	4.42%	95.58%	00:00:55	55,581	0.05%
	TOTAL	480.42K	9.51G		26.94%	73.06%	33:15:52	119,752,460	
	AVERAGE	36.95K	732.02M				02:33:31	9,211,727	

Figure 17. SARG shows logs from 3 Aug 2018

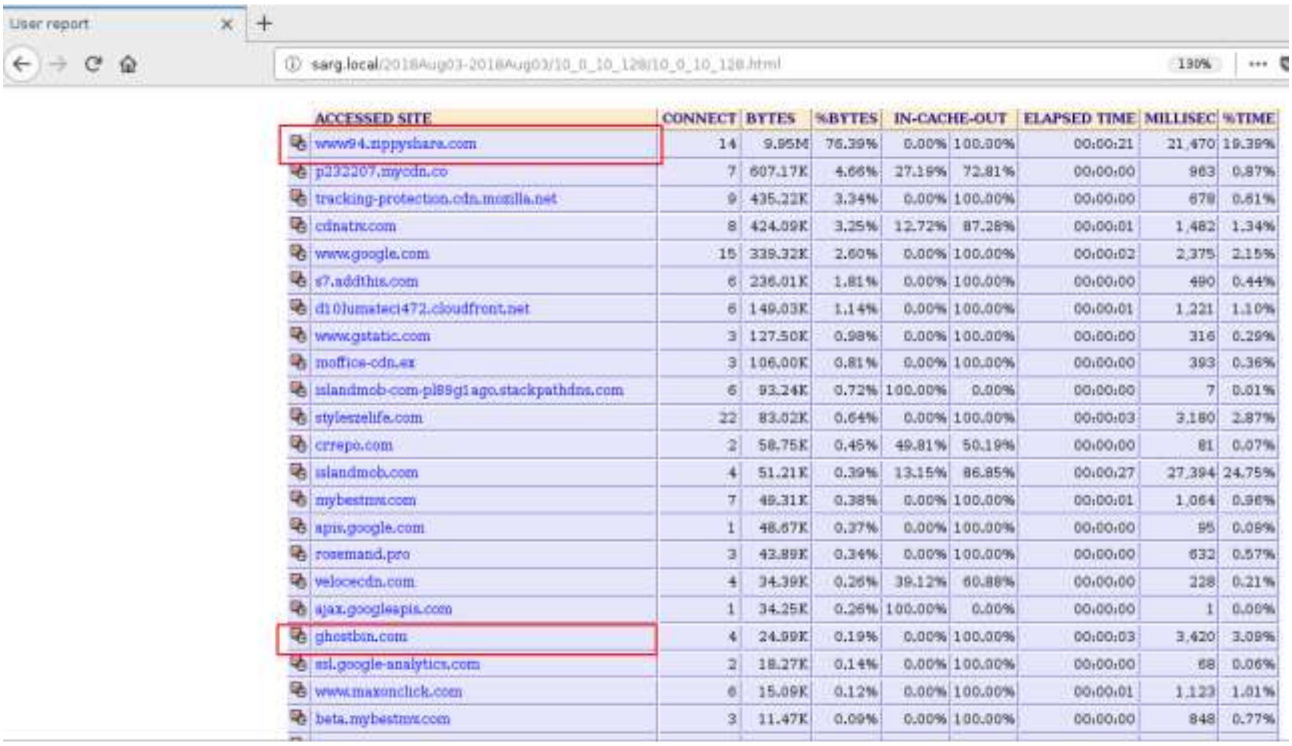
By browsing the activity of first infected machine, 10.0.10.111 it can be learned, that it visited services used for storing data online and pasting text data, namely Zippyshare and Ghostbin:



ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
www94.zippyshare.com	15	7.87M	64.27%	0.96%	99.04%	00:00:15	15,875	14.05%
www.zippyshare.com	52	1.56M	12.75%	0.00%	100.00%	00:00:09	9,660	8.55%
www.google.com	30	676.24K	5.52%	0.00%	100.00%	00:00:04	4,043	3.58%
register.mediabridge.cc	20	228.11K	1.86%	0.00%	100.00%	00:00:02	2,813	2.49%
mb.media-bucket.com	35	208.76K	1.70%	0.00%	100.00%	00:00:02	2,918	2.58%
img.mediabridge.cc	1	186.72K	1.52%	0.00%	100.00%	00:00:00	480	0.42%
ghosthin.com	19	186.37K	1.52%	0.00%	100.00%	00:00:03	3,830	3.39%
p0.mycdn.co	3	170.84K	1.39%	0.00%	100.00%	00:00:00	458	0.41%
p232207.mycdn.co	3	165.05K	1.35%	0.00%	100.00%	00:00:00	449	0.40%
d10lumateci472.cloudfront.net	6	149.02K	1.22%	0.00%	100.00%	00:00:01	1,193	1.06%
s7.addthis.com	1	114.71K	0.94%	0.00%	100.00%	00:00:00	215	0.19%
moffice-cdn.ex	3	106.00K	0.86%	0.00%	100.00%	00:00:00	393	0.35%
apis.google.com	2	97.35K	0.79%	0.00%	100.00%	00:00:00	191	0.17%
islandmob-com-pl89g1ago.stackpathdns.com	6	93.19K	0.76%	0.00%	100.00%	00:00:00	272	0.24%
styleszelife.com	13	55.01K	0.45%	0.00%	100.00%	00:00:02	2,156	1.91%
www.gstatic.com	2	49.01K	0.40%	0.00%	100.00%	00:00:00	126	0.11%

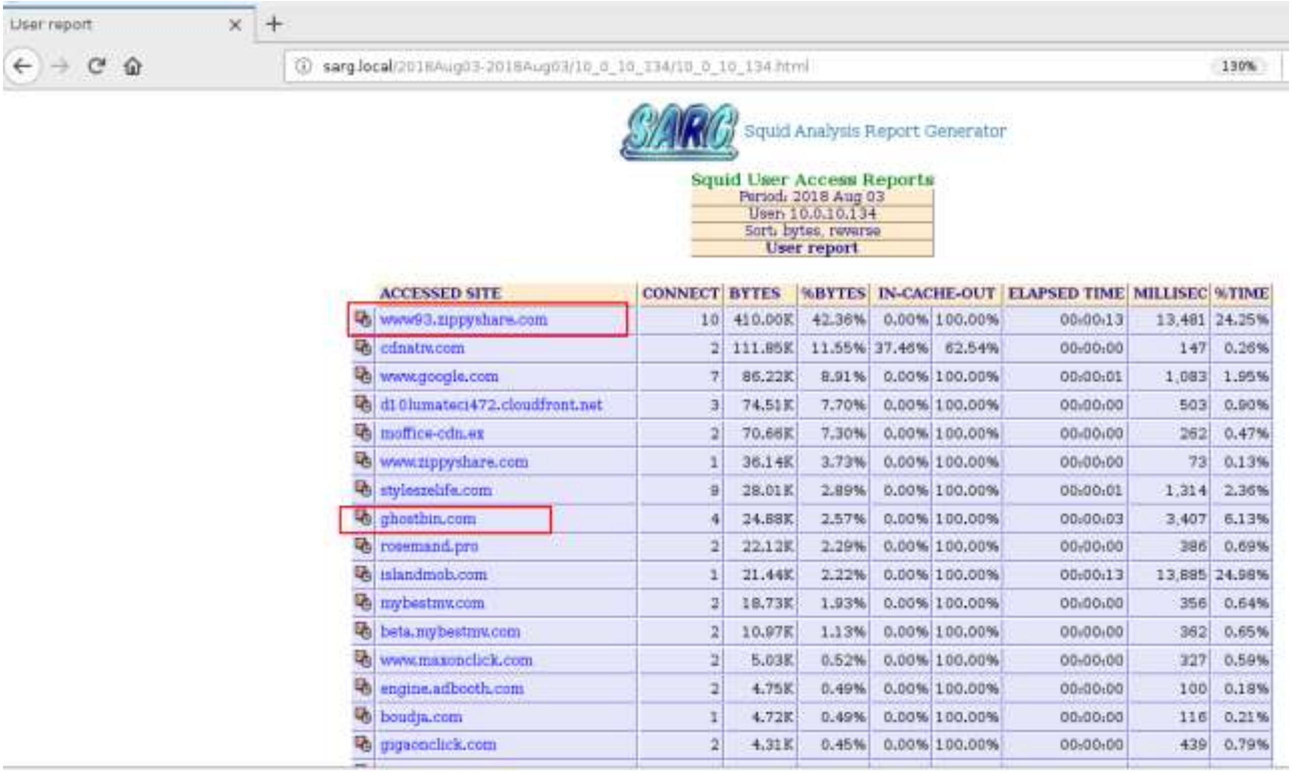
Figure 18. Host's 10.0.10.111 browsing history

Similar patterns can be observed by browsing the history of the remaining two infected hosts, 10.0.10.128 and 10.0.10.134:



ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
www94.zippyshare.com	14	9.95M	76.39%	0.00%	100.00%	00:00:21	21,470	19.39%
p232207.mycdn.co	7	607.17K	4.66%	27.19%	72.81%	00:00:00	963	0.87%
tracking-protection.cdn.mozilla.net	9	435.22K	3.34%	0.00%	100.00%	00:00:00	678	0.61%
cdnatrc.com	8	424.09K	3.25%	12.72%	87.28%	00:00:01	1,482	1.34%
www.google.com	15	339.32K	2.60%	0.00%	100.00%	00:00:02	2,375	2.15%
s7.addthis.com	6	236.01K	1.81%	0.00%	100.00%	00:00:00	490	0.44%
d10lumateci472.cloudfront.net	6	149.03K	1.14%	0.00%	100.00%	00:00:01	1,221	1.10%
www.gstatic.com	3	127.50K	0.98%	0.00%	100.00%	00:00:00	316	0.29%
moffice-cdn.ex	3	106.00K	0.81%	0.00%	100.00%	00:00:00	393	0.36%
islandmob-com-pl89g1ago.stackpathdns.com	6	93.24K	0.72%	100.00%	0.00%	00:00:00	7	0.01%
styleszelife.com	22	83.02K	0.64%	0.00%	100.00%	00:00:03	3,180	2.87%
crrepo.com	2	58.75K	0.45%	49.81%	50.19%	00:00:00	81	0.07%
islandmob.com	4	51.21K	0.39%	13.15%	86.85%	00:00:27	27,394	24.75%
mybestmx.com	7	49.31K	0.38%	0.00%	100.00%	00:00:01	1,064	0.96%
apis.google.com	1	48.67K	0.37%	0.00%	100.00%	00:00:00	95	0.09%
rosemand.pro	3	43.89K	0.34%	0.00%	100.00%	00:00:00	632	0.57%
velocecdn.com	4	34.39K	0.26%	39.12%	60.88%	00:00:00	228	0.21%
ajax.googleapis.com	1	34.25K	0.26%	100.00%	0.00%	00:00:00	1	0.00%
ghostbin.com	4	24.99K	0.19%	0.00%	100.00%	00:00:03	3,420	3.09%
ssl.google-analytics.com	2	18.27K	0.14%	0.00%	100.00%	00:00:00	68	0.06%
www.maxonclick.com	6	15.09K	0.12%	0.00%	100.00%	00:00:01	1,123	1.01%
beta.mybestmx.com	3	11.47K	0.09%	0.00%	100.00%	00:00:00	848	0.77%

Figure 19 Host's 10.0.10.1278 browsing history



Squid User Access Reports
Period: 2018 Aug 03
User: 10.0.10.134
Sort: bytes, reverse
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
www93.zippyshare.com	10	410.00K	42.36%	0.00%	100.00%	00:00:13	13,481	24.25%
cdnatv.com	2	111.85K	11.55%	37.46%	62.54%	00:00:00	147	0.26%
www.google.com	7	86.22K	8.91%	0.00%	100.00%	00:00:01	1,083	1.95%
d10lumateci472.cloudfront.net	3	74.51K	7.70%	0.00%	100.00%	00:00:00	503	0.90%
moffice-cdn.ex	2	70.66K	7.30%	0.00%	100.00%	00:00:00	262	0.47%
www.zippyshare.com	1	36.14K	3.73%	0.00%	100.00%	00:00:00	73	0.13%
styleszelife.com	9	28.01K	2.89%	0.00%	100.00%	00:00:01	1,314	2.36%
ghostbin.com	4	24.88K	2.57%	0.00%	100.00%	00:00:03	3,407	6.13%
rosemand.pro	2	22.12K	2.29%	0.00%	100.00%	00:00:00	386	0.69%
islandmob.com	1	21.44K	2.22%	0.00%	100.00%	00:00:13	13,885	24.98%
mybestmv.com	2	18.73K	1.93%	0.00%	100.00%	00:00:00	356	0.64%
beta.mybestmv.com	2	10.97K	1.13%	0.00%	100.00%	00:00:00	362	0.65%
www.maxonclick.com	2	5.03K	0.52%	0.00%	100.00%	00:00:00	327	0.59%
engine.adbooth.com	2	4.75K	0.49%	0.00%	100.00%	00:00:00	100	0.18%
boudja.com	1	4.72K	0.49%	0.00%	100.00%	00:00:00	116	0.21%
gigaonclick.com	2	4.31K	0.45%	0.00%	100.00%	00:00:00	439	0.79%

Figure 20. Host's 10.0.10.134 browsing history

This information can again be checked against Squid log to get some more detailed information.

Communication with Zippyshare can be investigated by issuing the command:

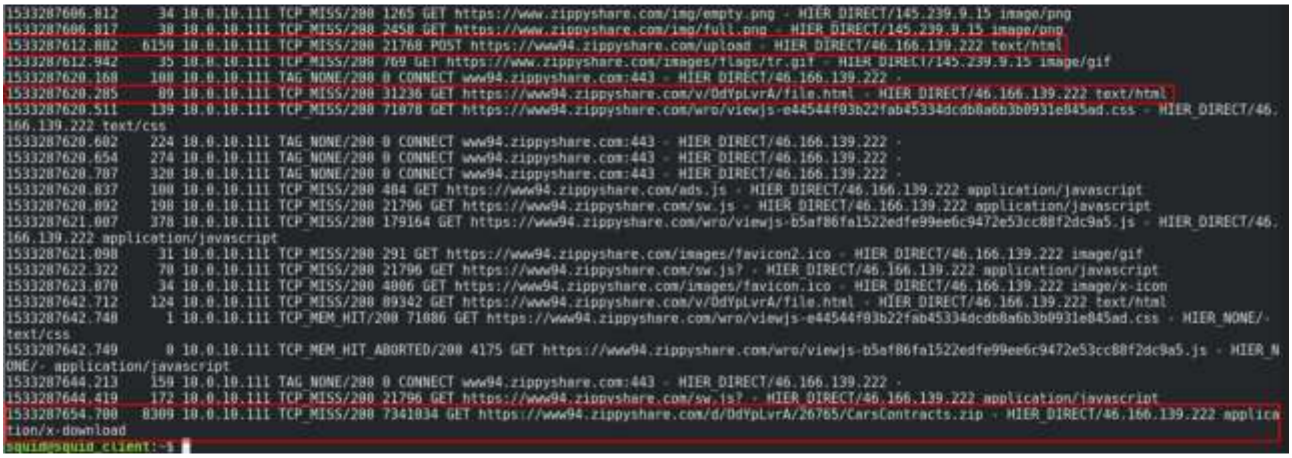
```
grep "zippyshare.com" access.log
```

```
1533289088.610     93 10.0.10.134 TAG_NONE/200 0 CONNECT www.zippyshare.com:443 - HIER_DIRECT/145.239.9.15 -
1533289088.712     73 10.0.10.134 TCP_MISS/200 36148 GET https://www.zippyshare.com/ - HIER_DIRECT/145.239.9.15 text/html
1533289096.585    310 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289096.679     34 10.0.10.134 TCP_MISS/200 257 OPTIONS https://www93.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 -
1533289109.360  12679 10.0.10.134 TCP_MISS/200 21739 POST https://www93.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 text/html
1533289113.504    103 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.772    127 10.0.10.134 TCP_MISS/200 89391 GET https://www93.zippyshare.com/v/zm0at8N3/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289113.899     96 10.0.10.134 TCP_MISS/200 71078 GET https://www93.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.
166.139.222 text/css
1533289113.917    114 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.924    119 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.946    117 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289114.092     94 10.0.10.134 TCP_MISS/200 21796 GET https://www93.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289114.094     32 10.0.10.134 TCP_MISS/200 484 GET https://www93.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289114.327    270 10.0.10.134 TCP_MISS/200 179164 GET https://www93.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.
166.139.222 application/javascript
1533289114.377     45 10.0.10.134 TCP_MISS/200 291 GET https://www93.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289115.758     33 10.0.10.134 TCP_MISS/200 4086 GET https://www93.zippyshare.com/images/favicon.ico - HIER_DIRECT/46.166.139.222 image/x-icon
1533289117.620     71 10.0.10.134 TCP_MISS/200 21796 GET https://www93.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533289682.146    116 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.299    123 10.0.10.128 TCP_MISS/200 89418 GET https://www94.zippyshare.com/v/OdYpLvrA/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289682.578    100 10.0.10.128 TCP_MISS/200 71078 GET https://www94.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.
166.139.222 text/css
1533289682.592    113 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.599    118 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.623    132 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.764     34 10.0.10.128 TCP_MISS/200 484 GET https://www94.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289682.801     74 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289683.066    383 10.0.10.128 TCP_MISS/200 179164 GET https://www94.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.
166.139.222 application/javascript
1533289683.147     45 10.0.10.128 TCP_MISS/200 366 GET https://www94.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289684.192     47 10.0.10.128 TCP_MISS/200 366 GET https://www94.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289686.895    112 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289687.055    130 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533289693.989    106 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289694.066     36 10.0.10.128 TCP_MISS/200 257 OPTIONS https://www94.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 -
1533289701.829   7761 10.0.10.128 TCP_MISS/200 21726 POST https://www94.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 text/html
1533289706.243     96 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289706.422    145 10.0.10.128 TCP_MISS/200 90285 GET https://www94.zippyshare.com/v/NitWfpnd/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289707.648     67 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533289710.441     33 10.0.10.128 TCP_MISS/304 207 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 -
1533289743.073    128 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289755.599  12492 10.0.10.128 TCP_MISS/200 9438168 GET https://www94.zippyshare.com/d/NitWfpnd/7275/Clients.zip - HIER_DIRECT/46.166.139.222 application/x-
download
squid@squid_client:~$
```

Figure 21. Zippshare.com traffic log

To make the log more readable, the results can be narrowed down to show a single host:

```
grep "zippyshare.com" access.log | grep 10.0.10.111
```



```
1533287606.812     34 10.0.10.111 TCP_MISS/200 1265 GET https://www.zippyshare.com/img/empty.png - HIER_DIRECT/145.239.9.15 image/png
1533287606.817     38 10.0.10.111 TCP_MISS/200 2458 GET https://www.zippyshare.com/img/full.png - HIER_DIRECT/145.239.9.15 image/png
1533287612.882   6159 10.0.10.111 TCP_MISS/200 21768 POST https://www94.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 text/html
1533287612.942     35 10.0.10.111 TCP_MISS/200 769 GET https://www.zippyshare.com/images/flags/tr.gif - HIER_DIRECT/145.239.9.15 image/gif
1533287620.168    108 10.0.10.111 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533287620.285     89 10.0.10.111 TCP_MISS/200 31236 GET https://www94.zippyshare.com/v/OdYpLvrA/file.html - HIER_DIRECT/46.166.139.222 text/html
1533287620.511    139 10.0.10.111 TCP_MISS/200 71078 GET https://www94.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.
166.139.222 text/css
1533287620.602    224 10.0.10.111 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533287620.654    274 10.0.10.111 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533287620.707    320 10.0.10.111 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533287620.837    100 10.0.10.111 TCP_MISS/200 484 GET https://www94.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.222 application/javascript
1533287620.892    198 10.0.10.111 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.222 application/javascript
1533287621.007    378 10.0.10.111 TCP_MISS/200 179164 GET https://www94.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.
166.139.222 application/javascript
1533287621.098     31 10.0.10.111 TCP_MISS/200 291 GET https://www94.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533287622.322     70 10.0.10.111 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533287623.070     34 10.0.10.111 TCP_MISS/200 4086 GET https://www94.zippyshare.com/images/favicon.ico - HIER_DIRECT/46.166.139.222 image/x-icon
1533287642.712    124 10.0.10.111 TCP_MISS/200 89342 GET https://www94.zippyshare.com/v/OdYpLvrA/file.html - HIER_DIRECT/46.166.139.222 text/html
1533287642.748      1 10.0.10.111 TCP_MEM_HIT/200 71086 GET https://www94.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_NONE/-
text/css
1533287642.749      0 10.0.10.111 TCP_MEM_HIT_ABORTED/200 4175 GET https://www94.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_N
ONE/- application/javascript
1533287644.213    159 10.0.10.111 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533287644.419    172 10.0.10.111 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533287654.700   8309 10.0.10.111 TCP_MISS/200 7341034 GET https://www94.zippyshare.com/d/OdYpLvrA/26765/CarsContracts.zip - HIER_DIRECT/46.166.139.222 applica
tion/x-download
squid@squid_client:~$
```

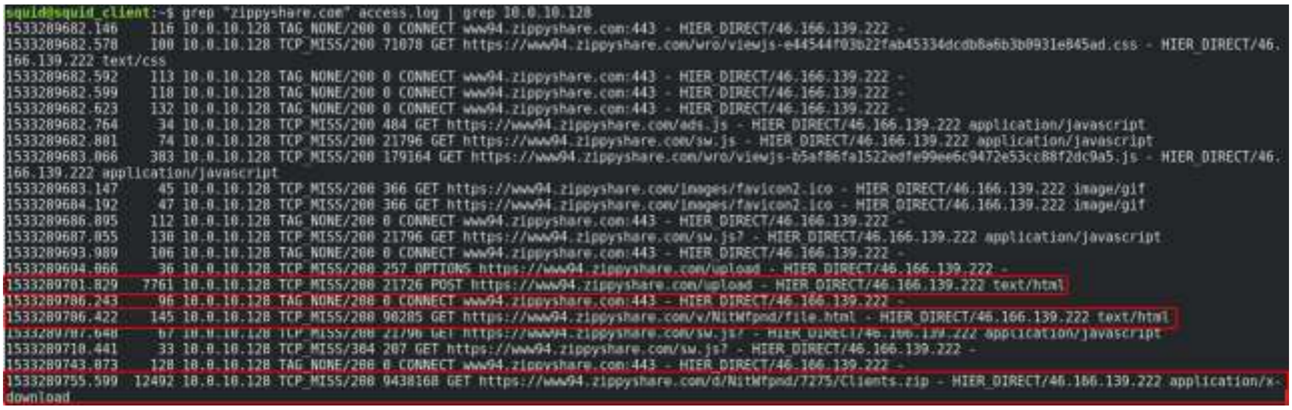
Figure 22. Zippyshare.com traffic from 10.0.10.111 host

From these results, it can be read that:

- POST request has been made to zippyshare.com
- There is a distinct link pointing to a file on Zippyshare: hxxts://www94.zippyshare[.]com/v/OdYpLvrA/file.html
- GET request has been issued for a file called CarsContract.zip

Remaining hosts can be checked using the same approach:

```
grep "zippyshare.com" access.log | grep 10.0.10.128
```

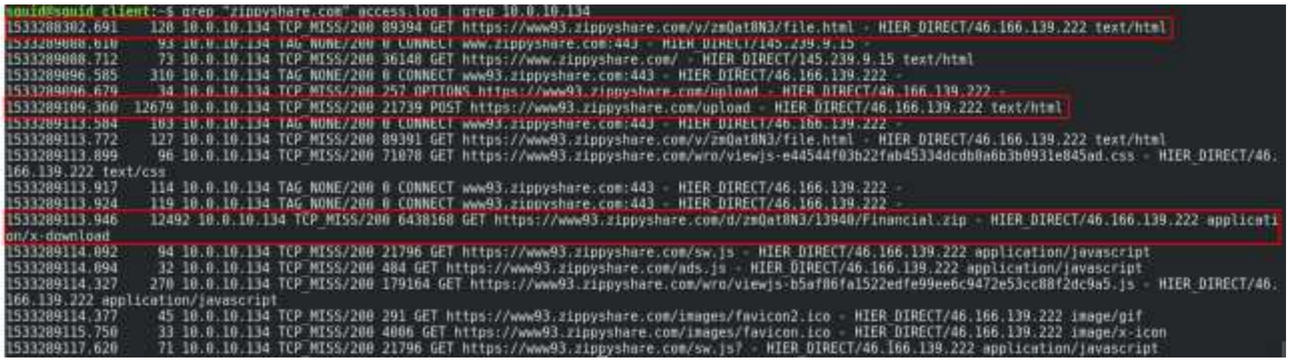


```
squid@squid_client:~$ grep "zippyshare.com" access.log | grep 10.0.10.128
1533289682.146    116 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.578    100 10.0.10.128 TCP_MISS/200 71078 GET https://www94.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.166.139.222 text/css
1533289682.592    113 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.599    118 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.623    132 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289682.764     34 10.0.10.128 TCP_MISS/200 484 GET https://www94.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289682.801     74 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289683.066    383 10.0.10.128 TCP_MISS/200 179164 GET https://www94.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289683.147     45 10.0.10.128 TCP_MISS/200 366 GET https://www94.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289684.192     47 10.0.10.128 TCP_MISS/200 366 GET https://www94.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289686.895    112 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289687.055    130 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533289693.989    106 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289694.066     36 10.0.10.128 TCP_MISS/200 257 OPTIONS https://www94.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 -
1533289701.829   7761 10.0.10.128 TCP_MISS/200 21726 POST https://www94.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 text/html
1533289786.243     96 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289786.422    145 10.0.10.128 TCP_MISS/200 90285 GET https://www94.zippyshare.com/v/NitWfpnd/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289787.648     67 10.0.10.128 TCP_MISS/200 21796 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
1533289710.441     33 10.0.10.128 TCP_MISS/304 207 GET https://www94.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 -
1533289743.873    128 10.0.10.128 TAG_NONE/200 0 CONNECT www94.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289755.599  12492 10.0.10.128 TCP_MISS/200 9438168 GET https://www94.zippyshare.com/d/NitWfpnd/7275/Clients.zip - HIER_DIRECT/46.166.139.222 application/x-download
```

Figure 23. Zippyshare.com traffic from 10.0.10.128 host

There is a distinct link: hxxts://www94.zippyshare[.]com/v/NitWfpnd/file.html and GET request for a file called Clients.zip

```
grep "zippyshare.com" access.log | grep 10.0.10.134
```



```
squid@squid_client:~$ grep "zippyshare.com" access.log | grep 10.0.10.134
1533288302.691    120 10.0.10.134 TCP_MISS/200 89394 GET https://www93.zippyshare.com/v/zmQat8N3/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289088.610     93 10.0.10.134 TAG_NONE/200 0 CONNECT www.zippyshare.com:443 - HIER_DIRECT/145.239.9.15 -
1533289088.712     73 10.0.10.134 TCP_MISS/200 36148 GET https://www.zippyshare.com/ - HIER_DIRECT/145.239.9.15 text/html
1533289096.585    310 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289096.679     34 10.0.10.134 TCP_MISS/200 257 OPTIONS https://www93.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 -
1533289109.360  12679 10.0.10.134 TCP_MISS/200 21739 POST https://www93.zippyshare.com/upload - HIER_DIRECT/46.166.139.222 text/html
1533289113.584    103 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.772    127 10.0.10.134 TCP_MISS/200 89391 GET https://www93.zippyshare.com/v/zmQat8N3/file.html - HIER_DIRECT/46.166.139.222 text/html
1533289113.899     96 10.0.10.134 TCP_MISS/200 71078 GET https://www93.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.166.139.222 text/css
1533289113.917    114 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.924    119 10.0.10.134 TAG_NONE/200 0 CONNECT www93.zippyshare.com:443 - HIER_DIRECT/46.166.139.222 -
1533289113.946  12492 10.0.10.134 TCP_MISS/200 6438168 GET https://www93.zippyshare.com/d/zmQat8N3/13940/Financial.zip - HIER_DIRECT/46.166.139.222 application/x-download
1533289114.092     94 10.0.10.134 TCP_MISS/200 21796 GET https://www93.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289114.094     32 10.0.10.134 TCP_MISS/200 484 GET https://www93.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289114.327    270 10.0.10.134 TCP_MISS/200 179164 GET https://www93.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.166.139.222 application/javascript
1533289114.377     45 10.0.10.134 TCP_MISS/200 291 GET https://www93.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.222 image/gif
1533289115.750     33 10.0.10.134 TCP_MISS/200 4086 GET https://www93.zippyshare.com/images/favicon.ico - HIER_DIRECT/46.166.139.222 image/x-icon
1533289117.620     71 10.0.10.134 TCP_MISS/200 21796 GET https://www93.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.222 application/javascript
```

Figure24. Zippyshare.com traffic from 10.0.10.134

There is a distinct link: hxxts://www93.zippyshare[.]com/v/zmQat8N3/file.html and GET request for a file called Financial.zip

The other suspicious service found in the browsing history is Ghostbin. Access.log might be storing some useful information:

```
grep "ghostbin" access.log
```

```
squid@squid_client:~$ grep "ghostbin" access.log
1533287628.862 165 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287628.940 49 10.0.10.111 TCP_MISS/503 8582 GET https://ghostbin.com/ - HIER_DIRECT/104.27.142.50 text/html
1533287629.146 131 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287629.188 135 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287629.271 55 10.0.10.111 TCP_MISS/200 7766 GET https://ghostbin.com/favicon.ico - HIER_DIRECT/104.27.142.50 image/vnd.microsoft.icon
1533287629.719 539 10.0.10.111 TCP_MISS/200 7762 GET https://ghostbin.com/favicon.ico - HIER_DIRECT/104.27.142.50 image/vnd.microsoft.icon
1533287633.069 45 10.0.10.111 TCP_MISS/302 637 GET https://ghostbin.com/cdn-cgi/l/chk_jschl? - HIER_DIRECT/104.27.142.50 text/html
1533287633.583 490 10.0.10.111 TCP_MISS/200 2441 GET https://ghostbin.com/ - HIER_DIRECT/104.27.142.50 text/html
1533287633.683 56 10.0.10.111 TCP_MISS/200 9019 GET https://ghostbin.com/css/lib.min.d251b95d.css - HIER_DIRECT/104.27.142.50 text/css
1533287633.711 84 10.0.10.111 TCP_MISS/200 2654 GET https://ghostbin.com/css/application.min.b99ea92e.css - HIER_DIRECT/104.27.142.50 text/css
1533287633.759 130 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287633.765 134 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287633.765 136 10.0.10.111 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533287633.880 53 10.0.10.111 TCP_MISS/200 3577 GET https://ghostbin.com/js/application.min.91933291.js - HIER_DIRECT/104.27.142.50 application/javascript
1533287633.887 52 10.0.10.111 TCP_MISS/200 1121 GET https://ghostbin.com/css/theme.min.77312fb0.css - HIER_DIRECT/104.27.142.50 text/css
1533287633.923 111 10.0.10.111 TCP_MISS/200 43327 GET https://ghostbin.com/js/lib.min.002a0da2.js - HIER_DIRECT/104.27.142.50 application/javascript
1533287634.051 65 10.0.10.111 TCP_MISS/200 17453 GET https://ghostbin.com/fonts/lmsans10-regular-webfont.woff - HIER_DIRECT/104.27.142.50 application/font-woff
1533287634.054 67 10.0.10.111 TCP_MISS/200 20045 GET https://ghostbin.com/fonts/lmsans10-bold-webfont.woff - HIER_DIRECT/104.27.142.50 application/font-woff
1533287634.061 78 10.0.10.111 TCP_MISS/200 6376 GET https://ghostbin.com/fonts/fontello.woff? - HIER_DIRECT/104.27.142.50 application/font-woff
1533287634.090 109 10.0.10.111 TCP_MISS/200 34657 GET https://ghostbin.com/fonts/envy_code_r-webfont.woff - HIER_DIRECT/104.27.142.50 application/font-woff
1533287634.248 49 10.0.10.111 TCP_MISS/200 6422 GET https://ghostbin.com/ghostbin-icon152.png - HIER_DIRECT/104.27.142.50 image/png
1533287634.501 490 10.0.10.111 TCP_MISS/200 4541 GET https://ghostbin.com/languages.json - HIER_DIRECT/104.27.142.50 application/json
1533287634.593 51 10.0.10.111 TCP_MISS/200 1228 GET https://ghostbin.com/select2.png - HIER_DIRECT/104.27.142.50 image/png
1533287643.234 507 10.0.10.111 TCP_MISS/200 7799 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.142.50 text/html
1533288335.483 152 10.0.10.151 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.143.50 -
1533288336.027 509 10.0.10.151 TCP_MISS/200 7797 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.143.50 text/html
1533288347.771 564 10.0.10.151 TCP_MISS/200 7411 GET https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.143.50 text/html
1533288357.849 1252 10.0.10.151 TCP_MISS/303 469 POST https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.143.50 text/plain
1533288358.377 496 10.0.10.151 TCP_MISS/200 8242 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.143.50 text/html
1533289113.393 176 10.0.10.134 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533289113.967 543 10.0.10.134 TCP_MISS/200 8230 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.142.50 text/html
1533289116.776 491 10.0.10.134 TCP_MISS/200 7898 GET https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.142.50 text/html
1533289132.952 1772 10.0.10.134 TCP_MISS/303 469 POST https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.142.50 text/plain
1533289133.572 601 10.0.10.134 TCP_MISS/200 8293 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.142.50 text/html
1533289712.228 164 10.0.10.128 TAG_NONE/200 0 CONNECT ghostbin.com:443 - HIER_DIRECT/104.27.142.50 -
1533289712.881 622 10.0.10.128 TCP_MISS/200 8293 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.142.50 text/html
1533289714.683 602 10.0.10.128 TCP_MISS/200 7937 GET https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.142.50 text/html
1533289730.647 1591 10.0.10.128 TCP_MISS/303 469 POST https://ghostbin.com/paste/n4d3g/edit - HIER_DIRECT/104.27.142.50 text/plain
1533289731.258 605 10.0.10.128 TCP_MISS/200 8294 GET https://ghostbin.com/paste/n4d3g - HIER_DIRECT/104.27.142.50 text/html
```

Figure 25. Ghostbin traffic

This logs show numerous requests being sent to the address hxxps//ghostbin[.]com/paste/n4d3g. It can also be noted, that it appears that there are some new IP addresses belonging to private range. All IP addresses that are reaching out to this address can be found by issuing the following command:

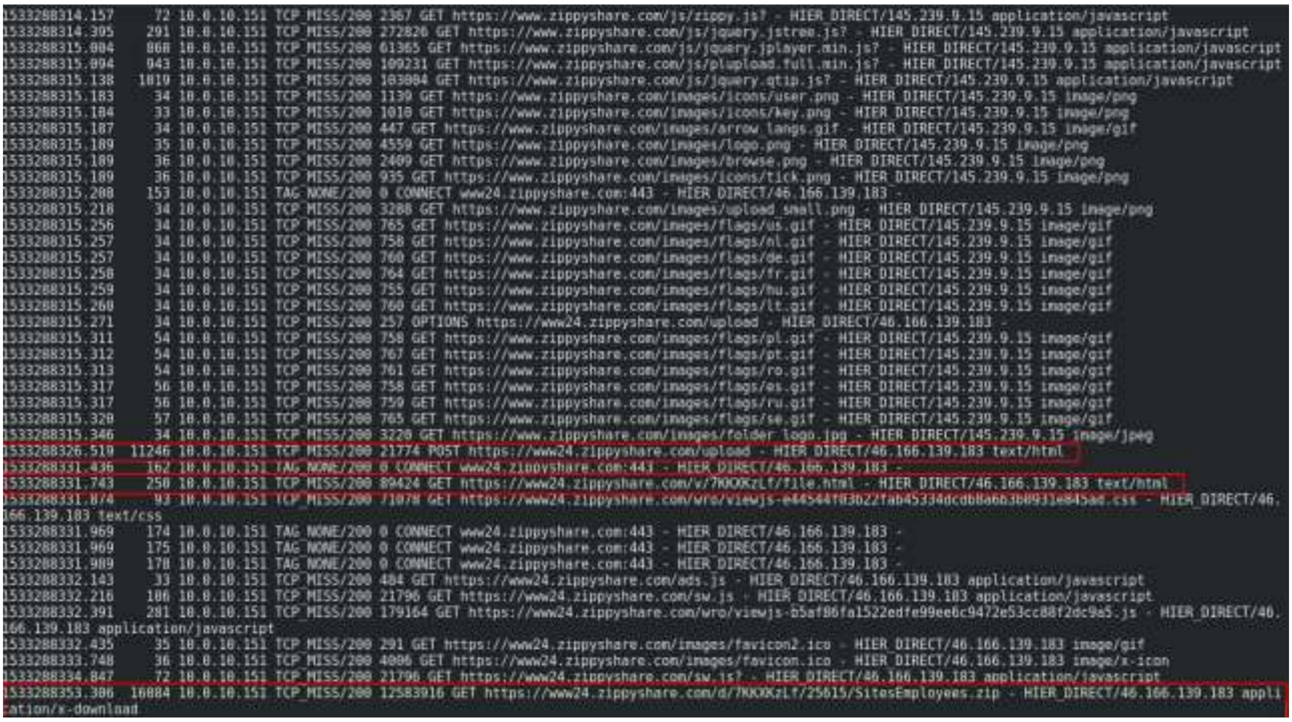
```
grep "ghostbin" access.log | awk '{print $3}' | sort | uniq
```

```
squid@squid_client:~$ grep "ghostbin" access.log | awk '{print $3}' | sort | uniq
10.0.10.111
10.0.10.128
10.0.10.134
10.0.10.151
```

Figure 26. Ghostbin uniq IP addresses

The result shows four IP addresses, while there were previously discovered only three that were communicating with malicious C2 server. Taking a closer look at the 10.0.10.151 might show more information:

```
grep "zippyshare.com" access.log | grep "10.0.10.151"
```



```
1533288314.157     72 10.0.10.151 TCP_MISS/200 2367 GET https://www.zippyshare.com/js/zippy.js? - HIER_DIRECT/145.239.9.15 application/javascript
1533288314.305    291 10.0.10.151 TCP_MISS/200 272826 GET https://www.zippyshare.com/js/jquery.jstree.js? - HIER_DIRECT/145.239.9.15 application/javascript
1533288315.004    868 10.0.10.151 TCP_MISS/200 61365 GET https://www.zippyshare.com/js/jquery.jplayer.min.js? - HIER_DIRECT/145.239.9.15 application/javascript
1533288315.094    943 10.0.10.151 TCP_MISS/200 109231 GET https://www.zippyshare.com/js/plupload.full.min.js? - HIER_DIRECT/145.239.9.15 application/javascript
1533288315.138   1019 10.0.10.151 TCP_MISS/200 103004 GET https://www.zippyshare.com/js/jquery.qtip.js? - HIER_DIRECT/145.239.9.15 application/javascript
1533288315.183     34 10.0.10.151 TCP_MISS/200 1139 GET https://www.zippyshare.com/images/icons/user.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.184     33 10.0.10.151 TCP_MISS/200 1010 GET https://www.zippyshare.com/images/icons/key.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.187     34 10.0.10.151 TCP_MISS/200 447 GET https://www.zippyshare.com/images/arrow_langs.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.189     35 10.0.10.151 TCP_MISS/200 4559 GET https://www.zippyshare.com/images/logo.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.189     36 10.0.10.151 TCP_MISS/200 2409 GET https://www.zippyshare.com/images/browse.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.189     36 10.0.10.151 TCP_MISS/200 935 GET https://www.zippyshare.com/images/icons/tick.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.208    153 10.0.10.151 TAG_NONE/200 0 CONNECT www24.zippyshare.com:443 - HIER_DIRECT/46.166.139.183 -
1533288315.218     34 10.0.10.151 TCP_MISS/200 3288 GET https://www.zippyshare.com/images/upload_small.png - HIER_DIRECT/145.239.9.15 image/png
1533288315.256     34 10.0.10.151 TCP_MISS/200 765 GET https://www.zippyshare.com/images/flags/us.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.257     34 10.0.10.151 TCP_MISS/200 758 GET https://www.zippyshare.com/images/flags/nl.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.257     34 10.0.10.151 TCP_MISS/200 760 GET https://www.zippyshare.com/images/flags/de.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.258     34 10.0.10.151 TCP_MISS/200 764 GET https://www.zippyshare.com/images/flags/fr.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.259     34 10.0.10.151 TCP_MISS/200 755 GET https://www.zippyshare.com/images/flags/hu.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.260     34 10.0.10.151 TCP_MISS/200 760 GET https://www.zippyshare.com/images/flags/lt.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.271     34 10.0.10.151 TCP_MISS/200 257 OPTIONS https://www24.zippyshare.com/upload - HIER_DIRECT/46.166.139.183 -
1533288315.311     54 10.0.10.151 TCP_MISS/200 758 GET https://www.zippyshare.com/images/flags/pl.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.312     54 10.0.10.151 TCP_MISS/200 767 GET https://www.zippyshare.com/images/flags/pt.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.313     54 10.0.10.151 TCP_MISS/200 761 GET https://www.zippyshare.com/images/flags/ro.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.317     56 10.0.10.151 TCP_MISS/200 758 GET https://www.zippyshare.com/images/flags/es.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.317     56 10.0.10.151 TCP_MISS/200 759 GET https://www.zippyshare.com/images/flags/ru.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.320     57 10.0.10.151 TCP_MISS/200 765 GET https://www.zippyshare.com/images/flags/se.gif - HIER_DIRECT/145.239.9.15 image/gif
1533288315.346     34 10.0.10.151 TCP_MISS/200 3220 GET https://www.zippyshare.com/images/folder_logo.jpg - HIER_DIRECT/145.239.9.15 image/jpeg
1533288326.519  11246 10.0.10.151 TCP_MISS/200 21774 POST https://www24.zippyshare.com/upload - HIER_DIRECT/46.166.139.183 text/html
1533288331.436    162 10.0.10.151 TAG_NONE/200 0 CONNECT www24.zippyshare.com:443 - HIER_DIRECT/46.166.139.183 -
1533288331.743    250 10.0.10.151 TCP_MISS/200 89424 GET https://www24.zippyshare.com/v/7KKXKzLf/file.html - HIER_DIRECT/46.166.139.183 text/html
1533288331.874     93 10.0.10.151 TCP_MISS/200 71078 GET https://www24.zippyshare.com/wro/viewjs-e44544f03b22fab45334dcdb8a6b3b0931e845ad.css - HIER_DIRECT/46.166.139.183 text/css
1533288331.969    174 10.0.10.151 TAG_NONE/200 0 CONNECT www24.zippyshare.com:443 - HIER_DIRECT/46.166.139.183 -
1533288331.969    175 10.0.10.151 TAG_NONE/200 0 CONNECT www24.zippyshare.com:443 - HIER_DIRECT/46.166.139.183 -
1533288331.989    178 10.0.10.151 TAG_NONE/200 0 CONNECT www24.zippyshare.com:443 - HIER_DIRECT/46.166.139.183 -
1533288332.143     33 10.0.10.151 TCP_MISS/200 484 GET https://www24.zippyshare.com/ads.js - HIER_DIRECT/46.166.139.183 application/javascript
1533288332.216    106 10.0.10.151 TCP_MISS/200 21796 GET https://www24.zippyshare.com/sw.js - HIER_DIRECT/46.166.139.183 application/javascript
1533288332.391    281 10.0.10.151 TCP_MISS/200 179164 GET https://www24.zippyshare.com/wro/viewjs-b5af86fa1522edfe99ee6c9472e53cc88f2dc9a5.js - HIER_DIRECT/46.166.139.183 application/javascript
1533288332.435     35 10.0.10.151 TCP_MISS/200 291 GET https://www24.zippyshare.com/images/favicon2.ico - HIER_DIRECT/46.166.139.183 image/gif
1533288333.748     36 10.0.10.151 TCP_MISS/200 4006 GET https://www24.zippyshare.com/images/favicon.ico - HIER_DIRECT/46.166.139.183 image/x-icon
1533288334.847     72 10.0.10.151 TCP_MISS/200 21796 GET https://www24.zippyshare.com/sw.js? - HIER_DIRECT/46.166.139.183 application/javascript
1533288353.386  16884 10.0.10.151 TCP_MISS/200 12583916 GET https://www24.zippyshare.com/d/7KKXKzLf/25615/SitesEmployees.zip - HIER_DIRECT/46.166.139.183 application/x-download
```

Figure 27. Host 10.0.10.151 traffic

There is a distinct link: hxxts://www94.zippyshare[.]com/v/7KKXKzLf/file.html and GET request for a file called SitesEmployees.zip. This follows the pattern observed on other infected machines. The fact that this machine was not discovered earlier should raise the suspicion that some IOCs might be still left undiscovered.

Two C2 addresses obtained from MISP were:

- hxxps://fastparceldelivery[.]ex/kirk545734/gate.php
- hxxps://moffice-cdn[.]ex/spock732573/gate.php

The address seems to be too random to weed out another one from the log file, except the last part „**gate.php**" which seems constant. After applying this logic:

```
grep "10.0.10.151" access.log | grep "gate.php"
```

```
squid@squid_client:~$ grep "10.0.10.151" access.log | grep gate.php
1533281912.249    131 10.0.10.151 TCP_MISS/200 35334 GET https://city-bistro.ex/picard323456/gate.php - HIER_DIRECT/185.159.82.58 text/html
1533285496.432    131 10.0.10.151 TCP_MISS/200 35334 GET https://city-bistro.ex/picard323456/gate.php - HIER_DIRECT/185.159.82.58 text/html
```

Figure 28. New C2 server

New C2 address is discovered: : hxxps://city-bistro[.]ex/picard323456/gate.php

3.2 Detecting data exfiltration over DNS

For the purpose of this exercise, logfiles were prepared reflecting common corporate network configuration, where all request coming from corporate network workstations are processed and logged by a local forwarding DNS server running BIND.

All log files prepared for this exercise can be found at **`/home/bind/exercise_logs/dns`** directory on **`Squid_client`** virtual machine. Python script bind_stats.py is located at **`/home/bind/tools.`**

Task 1 – basic detection based on logs size and count

First steps should start with basic statistic, using standard Linux tools.

First go to **`/home/bind/exercise_logs/dns`** and check number of available log files:

```
# ls -l
```

There are 6 logs provided, 5 with the size of 25MB and one with 15MB being the latest.

Assuming standard network activity 5 logs with similar size should have similar number of log entries:

Check the number of log entries:

```
# wc -l bind.log.*
```

```
 154700 bind.log.0
 204964 bind.log.1
 150327 bind.log.2
 208247 bind.log.3
 237499 bind.log.4
 247461 bind.log.5
1203198 total
```

Figure 29. Difference in number of records in log file

The output of the above command shows, that bind.log.2 has only 150327 lines, where number of lines is equal to number of DNS queries.

With this knowledge, analysis can be started with bind.log.2 file looking for long label names:

```
# egrep "[a-zA-Z0-9]{40,63}" bind.log.2 | wc -l
# 3
```

Above egrep command returns 3 lines containing queries with labels in range of 40 – 63 characters.

These queries can be viewed by removing wc – l from previous command:

```
egrep "[a-zA-Z0-9]{40,63}" bind.log.2
```

```
13-Aug-2018 12:53:10.216 client 10.0.10.119#61671: query: aaqjzks4scrkxevy7vnbruqip4iyg4pdfzi7pxdtavwym7o3.17xzd4gfuygmp4
zyxeevcwcn73mlxg3fdzu6aj4rjumtrnvm.23m3c7k5kvg3uufmozfxbqj2izaa7nm6v5dq.probe.performance.dropbox.com IN A + (10.0.10.2)
13-Aug-2018 12:53:10.296 client 10.0.10.119#61671: query: aaqjzks4scrkxevy7vnbruqip4iyg4pdfzi7pxdtavwym7o3.17xzd4gfuygmp4
zyxeevcwcn73mlxg3fdzu6aj4rjumtrnvm.23m3c7k5kvg3uufmozfxbqj2izaa7nm6v5dq.probe.performance.dropbox.com IN A + (10.0.10.2)
13-Aug-2018 15:44:40.871 client 10.0.10.140#51427: query: aaqmq3ocjqyma7tdfvjkfkcxb2zgzpag2judaq673jfue7eg.k7qk7udukzc7in
jumkzqrjdkgscuks3sfdgwgcjq6t2zycwc.3gthoci6mau753khgmuewikaibu4sedktg7q.probe.performance.dropbox.com IN A + (10.0.10.2)
```

Figure 30. Legitimate service queries

Dropbox is legitimate service, yet queries are longer than usual.

With two following commands, it can compared if Dropbox queries are responsible for difference in queries count:

```
# grep dropbox bind.log.2 | wc -l
# 1048
# grep dropbox bind.log.5 | wc -l
# 3340
```

bind.log.5 has 3 times as many Dropbox queries yet its total line count is significantly higher, so it can be assumed that Dropbox isn't responsible for this difference.

It is common for DNS exfiltration techniques to use as many characters as possible, so regex can be modified to include them:

```
# egrep "[a-zA-Z0-9\\]{30,63}" bind.log.2 | wc -l | uniq
# 17981
```

Just this number gives basis for further investigation and checking those queries:

```
# egrep "[a-zA-Z0-9\\]{40,63}" bind.log.2 | uniq > suspicious.queries
# less suspicious.queries
```

```
12-Aug-2018 20:25:53.915 client 10.0.10.19#42044: query: 0a2ae\197\197ICH\251a\223J\204u\211V\236\243Yr\234I\238w\250\199
\208WJO\195\2132W\204\244\214L\204\226\225s\206I2\191E\194\224\248E\214\232\235F\192\253\197\224\224.\214\227H\216Ux\210\
189tgi6\214\196o\224\222\188jfmpE\2239k\200g7\2377\234in\235Ktk2M\206\217\233\227G\207QZd\212S\205\229\232m\204x.lu\198\2
00\197\197xW\197s\230\234\213FNk\192\222\246\221g\253\233H\202Lw\226\242y\206\217G\191\2114\239\224\227\189\249\193\208\2
24\252O\206A\211Ct\223\193Kg\250\195.mf\208vd\228\231\2539\226\236C\193\2140B3\213\231\2162\213\234RF\189\240KueE\241\226
\223DZjcm\192v3\247\2384I\247PKCY\235W0Txc.\223\230hwkZ1.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:53.980 client 10.0.10.19#42044: query: 0beaf\211\218\227\230\221\231\217\198K\191\2370\211\253Cf\217\24
8\253\208\203o\188dt\245\246\197lVN\226\196\234O\2526d\238\1907\253u\231\23068QKk8\229jYJ\224\189.l\193\221\217uEB\216\24
1YCy\216\247\195\204IoDH\213\239\194\197tSJlW\231\228S\234\205\240\211\205\238\190\219\205\239T\202GU\196\1993\208I58\247
\232\213X.\208XR\250\214\197\193\240\190y\206\2297\223\212\243W\229\228u\201\248\211\227Zzj\251\215\217\228\213\214s\230Q
qB4\217\192\192D3\209\247\222m\214YB\237\222Uw\197j.\197\204szw5\211\247\244im\242\218E\242L\207fH\206\237\252CT\203h\243
\215\208\241\222R\240\242y\200\250cqQ\197\226\234\219jn\215\209\214\226oK\229r\247\229K.l\204I7\197\228P.example.xyz IN N
ULL +E (10.0.10.2)
12-Aug-2018 20:25:54.040 client 10.0.10.19#42044: query: 0bmbgM\2371\248I18h\210\196\200\205\239\198\189q\193e\207\189\23
8\233\234jS\199Y\213P\208\245ZN\196\199\225\193K\224z\215W\208\243d\244MT\225\194\219\200\223R\2144\198.09a\2091\223\239\
190\213r\213mFp\200\218\193\209g\210A\189Y\200J9H\211\222\220J\249X\188\207e\248\204U\194gX\221\215\210TyQbIv\2494\2132q\
196.\224ga\211\205UYgI\228\207D\208\250V\195\192\229\213\196MH\252a.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:54.102 client 10.0.10.19#42044: query: 0efah82\190w\238sJ\249aabacuqe1\189\227\242abag\221\200yk\193\23
5\193\190\210E\2377\226\190\198Q\201Nh\219\192\223up\191Gcag\243W\241a.aaqiGv\208\198\221w\238i\205\244S\231\214\252P8\25
3\2071Y\216iV\236M\231\212\212IG\206\189\210L\200T\238\240\236\243\220n\189Ni\222\236J\225\213S\2497.\216\221\242Hb\1997j
\209Sy\222\220\189\230\210sCu\202\247t\201\250a\196\1966\188\201\236\245\209H\245bu\236I\201\201\24806Vda\232\217U\214h\2
08\225h\251\220.\228\230h\249\226\208\212\242\191\217K\208\225X5\234Yo\188Q\2457\194\243f4\242U\2322jFamk\191nxn\250\222o
r\230x\207\251\2045Nf\246\234Mc\249\191.\2211Bi\217\224T.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:54.162 client 10.0.10.19#42044: query: 0enai0\213\212\228X\214c\218\2429\216U6e\212\192\242\201\192FPj\
suspicious.queries
```

Figure 11. Log entries indicating DNS data exfiltration

Resulting file contains all of 17981 lines, consisting of generated labels in domain example.xyz:

```
# ls -lh | awk '{print $5" "$9}'
```

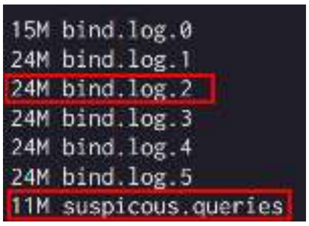


Figure 32. Excerpt of log for analysis

Additionally, it weights 11MB out of 25MB of total log size, which clearly indicate data exfiltration.

It is possible to generate some more statistics and check for higher than usual number of queries for NULL, TXT, CNAME and other unusual records:

```
# egrep "IN TXT" bind.log.1 | wc -l
# egrep "IN CNAME" bind.log.1 | wc -l
```

Additional exercises:

Logs were generated using two tools giving slightly different output.

- find first sign of data exfiltration
- create timeline of attacker steps
- explain why exfiltration took place at certain time of day

TASK2 – anomaly detection approach

In this exercise, a free python script[1] is used to perform quick quantitative analysis:

```
# cd /home/bind/tools
# ./bind_stats.py ../exercise_logs/dns/bind.log.0
```

For ease of use, the script can be copied to the logs directory.

Simply running the script with log file name as argument will display a number of metrics. Additional statistics can be obtained with optional parameters (full list of parameters can be shown issuing **`bind_stats.py -h`** command).

Existence of queries for very long domain names

As pointed out in previous chapters, the rise of usage of generated queries used by legitimated providers makes it more difficult to distinguish suspicious activity by looking at some of query properties like label length.

For example, log query used by Dropbox service for analytics purpose fulfils almost all criteria for DNS exfiltration: multiple computationally generated label names, each 48 characters long with a total length of 164 characters:

[1] https://github.com/Matty9191/bind-query-log-statistics

```
Top  100  longest DNS names requested:
aaskepmwk4rdoeb6ld3jz4mucl7bzye5lbcvi63zs4hznis7.ajrm6xykeg45jhsrgs7ixp55kfpzek36xrkducqnsfxym3an.miihv3sn56mxrhd4ue7cbeu
puf3c2zejgsta.probe.performance.dropbox.com
00e9e64bac87773782f7c9275c19248597ac0ad39ac5899a33-apidata.googleusercontent.com
dmp-eupro-haproxyd-16fgltvm0s4xx-617771131.eu-central-1.elb.amazonaws.com
p2-alvf6jmxtkhpk-rsrppwayqyfre74m-554751-i1-v6exp3.v4.metric.gstatic.com
```

Figure 33. Long DNS query for legitimate services

As comparison query generated by dnscat2 is presented, with only difference of length and base domain name:

```
Top  100  longest DNS names requested:
2ffb01cc2dc3d502fa86c8004123cf21cfacc035dd005f035c7e842a4127.56a1a9bf15063a8e1611cbd846a39b78f2277e68d3ad7e8f6c5b154a2cf4
.e69d93bf13fd66741bced47d9136353678cf14ec539bb32ab6e2409924a2.75b66e5ecf182c98a01e7e18e42989fda27ea06c1dd026.example.xyz
```

Figure 34. Long DNS query indicating DNS exfiltration

This can be remediated, by use of a trusted domain list, for which such long queries would be ignored.

Unusual DNS records

One of the approaches for DNS exfiltration is to use queries for other types of addresses than A or AAAA addresses. Examples of such types might be TXT, MX, CNAME, NULL queries[2]. Consequently, large amounts of queries for records of such types coming from corporate workstations should be investigated further.

```
Total DNS_QUERIES processed : 154700
  A     records requested : 102236
  AAAA  records requested : 52376
  SRV   records requested : 75
  TXT   records requested : 13

Top  100  DNS names requested:
  ntp.org : 54135
  microsoft.com : 12914
  google.com : 12605
  facebook.com : 6055
  yahoo.com : 3775
  fbcdn.net : 3061
  doubleclick.net : 2958
  googleapis.com : 2655
  gstatic.com : 2372
  edu.pl : 1807
  akamaiedge.net : 1754
  redcdn.pl : 1592
  eset.com : 1334
  google-analytics.com : 1285
  twitter.com : 1256
  avast.com : 1179
  googlesyndication.com : 1119
  twimg.com : 1048
  mozilla.com : 1017
  amazonaws.com : 965
  google.pl : 964
```

```
Total DNS_QUERIES processed : 208247
  A     records requested : 128999
  AAAA  records requested : 71668
  NULL  records requested : 7491
  SRV   records requested : 83
  TXT   records requested : 6

Top  100  DNS names requested:
  ntp.org : 94032
  microsoft.com : 21323
  google.com : 13324
  example.xyz : 7491
  yahoo.com : 6467
  facebook.com : 5456
  edu.pl : 3109
  fbcdn.net : 2601
  doubleclick.net : 2472
  eset.com : 2143
  twitter.com : 2027
  gstatic.com : 1743
  cux.io : 1648
  windowsupdate.com : 1633
  googleapis.com : 1333
  akamaiedge.net : 1285
  twimg.com : 1054
  amazonaws.com : 990
  googlevideo.com : 962
  cloudfront.net : 881
```

Figure 35. Comparison of statistics for clean logs (left) and suspicious queries with NULL records (right)

It is worth checking what queries associated with NULL records were send with grep command:

```
# grep "NULL" bind.log.3 | less
```

---

[2] IANA (2018b), https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4

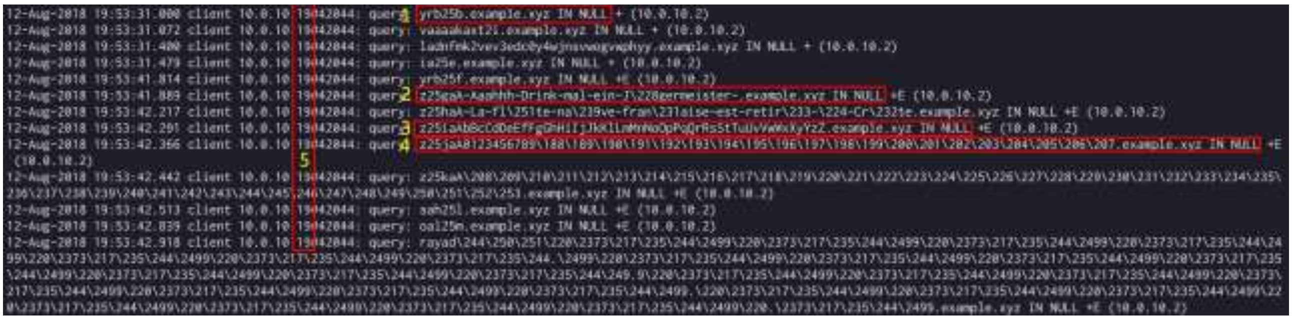


Figure 36. Checking queries associated with NULL records

In the output of the grep command shown in above figure, fragment of queries generated by iodine are shown, representing the start of a session. Data is sent compressed with gzip and encoded with Base32, Base64 or Base128, depending on DNS relay server configuration. Lines marked 1-4 show automatic discovery of accepted characters, label length and optimal encoding.[3] In this example, all queries were sent by the same host 10.0.10.19 – marked with 5.

Unusual popularity of previously unknown domain

When obscure and previously unknown domain becomes frequently queried, it might be the sign of some viral AD campaign or popular link being shared. However, when DNS records associated with query are rather unusual, logs should be inspected for signs of data exfiltration, especially when all those queries come from a single or a small number of workstation(s).

```
# ./bind_stats.py ../exercise_logs/dns/bind.log.5
```

```
Total DNS_QUERIES processed : 247461
  A     records requested : 167511
  AAAA  records requested : 75979
  TXT   records requested : 1288
  MX    records requested : 1239
  CNAME records requested : 1204
  SRV   records requested : 240

Top  100  DNS names requested:
  ntp.org : 102478
  microsoft.com : 24671
  google.com : 20559
  yahoo.com : 7096
  edu.pl : 4739
  example.xyz : 3718
  dropbox.com : 3270
  googleapis.com : 2930
  gstatic.com : 2656
  doubleclick.net : 2588
```

Figure 37. Queries for rare DNS records coming from client workstations

```
# grep "example.xyz" bind.log.5
```

[3] https://github.com/yarrick/iodine

```
04-Aug-2018 19:34:16.562 client 10.0.10.19#37574: query: 504d018b5cbca62defa76e00295ee4a8cffab468a5d8723d236e332d7719.378
10c7630f993860779734c295ec176b7abb8d76f424fe2dd5f47501234.8ebc55cafdc17186cc4bdc6555d1aa4dfa117a7158deda118210be1397da.2a
94dd74b2ffeeb4edab6f403c6a6406370da6b68f3639.example.xyz IN MX + (10.0.10.2)
04-Aug-2018 19:34:16.631 client 10.0.10.19#37574: query: 285c018b5c9ac0a36e5813002a531c824f3c98165e2a8d5fab5996ef7d75.ada
1177e774a752974111b918509ca54eed93d83af2b91ee9706682ab5b5.b206bc05d40445473343dc9b46db1ae5da06499eab0d4c75a360f50e207d.c7
7bddc5eb85df4088e658404b70d82bc0f77b9d1fb4cd.example.xyz IN CNAME + (10.0.10.2)
04-Aug-2018 19:34:16.712 client 10.0.10.19#37574: query: 028c018b5ceb15a2c855c7002babee67449f0932be8600f8a83afc6a59ce.414
07367284daf880abad71734a3deac4bd05092719327dd6801680f812c.eed2ec585a20969571ea5fc17447d5c415f5663b78b3dd81297477105 0c6.5c
0c0f2700e562bad7ed1990e32f41a58dc6aef7a38d03.example.xyz IN TXT + (10.0.10.2)
```

Figure 38. Excerpt from logs with MX, CNAME and TXT records

In a corporate network with centrally managed environment, MX records would mostly be used by the local mail server. Similarly, the most common uses for TXT records are also associated with mail: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Email). Information about fluctuations in service specific DNS records cannot only be valuable to DNS exfiltration detection, but also service misconfiguration.

High number of queries from single client

Any unexpected rise of traffic generated by client workstation should be analysed when it comes to DNS protocol as it may indicate malware infection or data exfiltration attempt.

```
# ./bind_stats.py ../exercise_logs/dns/bind.log.0
# ./bind_stats.py ../exercise_logs/dns/logs/bind.log.2
```

```
Top 100 DNS clients:        Top 100 DNS clients:
  10.0.10.125 :  54313        10.0.10.125 :  49292
  10.0.10.162 :  24698        10.0.10.162 :  25774
  10.0.10.71 :  14843         10.0.10.19 :  17982
  10.0.10.204 :  12358        10.0.10.20 :  10628
  10.0.10.20 :  11577         10.0.10.71 :  10463
  10.0.10.108 :  4290         10.0.10.204 :  5972
  10.0.10.23 :  3402          10.0.10.155 :  3864
  10.0.10.72 :  3347          10.0.10.119 :  3714
  10.0.10.155 :  3133         10.0.10.108 :  3072
  10.0.10.196 :  2677         10.0.10.23 :  3029
```

Figure 39. Usually quiet workstation appears on the top of the DNS clients list

The figure above is the output of previous two commands and shows that the most active client on the network is 10.0.10.125. This can be further compared with other log files. Closer examination of logs shows that its queries are associated with NTP (Network Time Protocol) service:

```
# grep "10.0.10.162" bind.log.2 | less
```

```
12-Aug-2018 20:25:55.342 client 10.0.10.125#59781: query: 2.debian.pool.ntp.org IN A + (10.0.10.2)
12-Aug-2018 20:25:55.343 client 10.0.10.125#59781: query: 2.debian.pool.ntp.org IN AAAA + (10.0.10.2)
12-Aug-2018 20:26:00.346 client 10.0.10.125#59781: query: 2.debian.pool.ntp.org IN A + (10.0.10.2)
12-Aug-2018 20:26:00.346 client 10.0.10.125#59781: query: 2.debian.pool.ntp.org IN AAAA + (10.0.10.2)
12-Aug-2018 20:26:05.347 client 10.0.10.125#49215: query: 3.debian.pool.ntp.org IN A + (10.0.10.2)
12-Aug-2018 20:26:05.347 client 10.0.10.125#49215: query: 3.debian.pool.ntp.org IN AAAA + (10.0.10.2)
```

Figure 40. NTP related DNS traffic

What draws attention is appearance of computer with IP 10.0.10.19 as third most active.

This can be compared with other statistics like number of queries, record types and domains queried:

```
# ./bind_stats.py ../exercise_logs/dns/bind.log.2
```

```
Total DNS_QUERIES processed : 150327
  A      records requested : 88604
  AAAA   records requested : 43633
  NULL   records requested : 17982
  SRV    records requested : 91
  TXT    records requested : 17

Top  100  DNS names requested:
  ntp.org : 49442
  example.xyz : 17982
  microsoft.com : 12193
  google.com : 10721
  facebook.com : 5244
  yahoo.com : 3433
  fbcdn.net : 2826
  doubleclick.net : 1877
  edu.pl : 1634
  gstatic.com : 1538
  twitter.com : 1460
```

Figure 41. Number of requests for NULL records correlated with suspicious domain

```
# grep "10.0.10.19" bind.log.2 | less
```

```
12-Aug-2018 20:25:53.915 client 10.0.10.19#42044: query: 0a2ae\197\197ICH\251a\223J\204u\211V\236\243Yr\234I\238w\250\199\
208WJO\195\2132W\204\244\214L\204\226\225s\206I2\191E\194\224\248E\214\232\235F\192\253\197\224\224.\214\227H\216Ux\210\18
9tgi6\214\196o\224\222\188jfmpE\2239k\200g7\2377\234in\235Ktk2M\206\217\233\227G\207QZd\212S\205\229\232m\204x.lu\198\200\
197\197xW\197s\230\234\213FNk\192\222\246\221g\253\233H\202Lw\226\242y\206\217G\191\2114\239\224\227\189\249\193\208\224\2
52O\206A\211Ct\223\193Kg\250\195.mf\208vd\228\231\2539\226\236C\193\2140B3\213\231\2162\213\234RF\189\240KueE\241\226\223D
Zjcm\192v3\247\2384I\247PKCY\235W0Txc.\223\230hwkZ1.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:53.980 client 10.0.10.19#42044: query: 0beaf\211\218\227\230\221\231\217\198K\191\2370\211\253Cf\217\248
\253\208\203o\188dt\245\246\197lVN\226\196\234O\2526d\238\1907\253u\231\23068QKk8\229jYJ\224\189.l\193\221\217uEB\216\241Y
Cy\216\247\195\204IoDH\213\239\194\197tSJlW\231\228S\234\205\240\211\205\238\190\219\205\239T\202GU\196\1993\208I58\247\23
2\213X.\208XR\250\214\197\193\240\190y\206\2297\223\212\243W\229\228u\201\248\211\227Zzj\251\215\217\228\213\214s\230QqB4\
217\192\192D3\209\247\222m\214YB\237\222Uw\197j.\197\204szw5\211\247\244im\242\218E\242L\207fH\206\237\252CT\203h\243\215\
208\241\222R\240\242y\200\250cqQ\197\226\234\219jn\215\209\214\226oK\229r\247\229K.l\204I7\197\228P.example.xyz IN NULL +E
```

Figure 42. DNS exfiltration attempt

In typical corporate environments, many fluctuations in DNS traffic coming from client workstations can be attributed to human interaction. It is a good practice to determine how many DNS request come from typical client and track any deviations.

3.3 Tools used in this use-case

- Squid proxy: http://www.squid-cache.org/
- SARG: https://sourceforge.net/projects/sarg/
- MISP: http://www.misp-project.org/
- bind-query-log-statistics.py script was used with custom modifications to provide some additional metrics: https://github.com/Matty9191/bind-query-log-statistics
- iodine: https://github.com/yarrick/iodine
- dnscat2: https://github.com/iagox86/dnscat2

4. Glossary and References

4.1 Glossary

ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
C&C	Command and Control (Server)
CLI	Command Line Interfaces
COTP	Connection Oriented Transport Protocol
GUI	Graphical User Interface
ICS	Industrial Control Systems
IGMP	Internet Group Management Protocol
ISO 27001	International Organization for Standardization
LLDP	Link Local Discovery Protocol
LLMNR	Link Local Multicast Name Resolution
PCAP	Packet CAPture
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
TPKT	Packet format used to transport OSI TPDUs over TCP
TPDU	(OSI) Transport Protocol Data Uni
UDP	User Datagram Protocol
VNC	Virtual Network Computing

4.2 References

Bejtlich, R. (2013), *The Practice of Network Security Monitoring – Understanding Incident Detection and Response*, No Starch Press, 2013, ISBN-13:1-59327-509-9

Davidoff, S. and Ham, J. (2012), *Network Forensics: Tracking Hackers through Cyberspace*, Prentice Hall, 2012, ISBN-10: 0-13-256471-8

Elz, R. and Bush, R. (1997), *RFC 2181: Clarifications to the DNS Specification,* July 1997, https://tools.ietf.org/html/rfc2181 (last accessed on October 7th, 2018)

Farnham, G. (2013), *Detecting DNS Tunneling*, SANS Institute, February 2013, https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152 (last accessed on October 7th, 2018)

IANA (2018), *Domain Name System (DNS) Parameters,* September 2018, https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4 (last accessed on October 10th, 2018)

Squid-cache.org (n.d.), O*fficial Squid project site*, http://www.squid-cache.org (last accessed on October 7th, 2018)

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-288-2
DOI: 10.2824/995110