

Security Analysis Report 2018

COMP 707: PROJECT 2

Verosha Pillay

Student Number: 214539347



Terminology:

- IDPS: An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.
- Next Generation Firewall: A next-generation firewall (NGFW) is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by enforcing security policies at the application level, as well as at the port and protocol level.
- Patch: A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes or bug fixes, and improving the usability or performance.
- Spyware: is software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge.
- Adware: Adware, or "advertising-supported software", refers to any piece of software or application that displays advertisements, usually through pop-up or pop-under windows.
- Brute Force: Brute-Force attempt is an attempt by an Internet user attempting to gain unauthorized access to your server by way of connecting to it, and running a command which attempts multiple logins per second, using a dictionary file of common passwords, trying different combinations to see if they can gain access.
- Trojan: A program that contains hidden functionality, often posing as useful applications yet performing Spyware or Adware functions and facilitates unauthorized access to the user's computer system.
- BOTS: are also known as spiders, crawlers, and web bots. While they may be utilized to perform repetitive jobs, such as indexing a search engine, they often come in the form of malware. Malware bots are used to gain total control over a computer.

1. Introduction

A consulting firm that focuses on the government and energy sector required a security analyst report to analyse certain information, to be completed. A computer security incident is any attempted or successful unauthorized access, disclosure, or misuse of computing systems, data or networks, including hacking and theft.

The company noted that recently sensitive proprietary information appears to have been leaked from the organisation. The report will contain information to determine where/who/how the leak occurred as well as proposed methods on how to improve the security posture of the organisation.

2. Analysis of log files

2.1. Analyzed log files -segmented by user

Details: User 1

File Name: Antivirus_log_collection1

Date	Machine	Status	Action	Additional information
27/03/2018 15:04:36	RnD_USER1	Scan complete: WARNING Suspicious signature detected	Alert	Signature: edb9e045b8dc7bb0b549bdf28e55f3b5
28/03/2018 09:14:27	RnD_USER1	Alert: Antivirus is out of date		
28/03/2018 11:04:28	RnD_USER1	Scan complete: WARNING Suspicious signature detected	Alert	Signature: edb9e045b8dc7bb0b549bdf28e55f3b5
28/03/2018 15:04:36	RnD_USER1	Scan complete: WARNING Suspicious signature detected	Alert	Signature: edb9e045b8dc7bb0b549bdf28e55f3b5
29/03/2018 09:16:38	RnD_USER1	Alert: Antivirus is out of date		
29/03/2018 11:04:36	RnD_USER1	Scan complete: WARNING Suspicious signature detected	Alert	Signature: edb9e045b8dc7bb0b549bdf28e55f3b5
29/03/2018 15:04:36	RnD_USER1	Scan complete: WARNING Suspicious signature detected	Alert	Signature: edb9e045b8dc7bb0b549bdf28e55f3b5

Summary and notes of what was found in this log file

- User 1 had 5 scans done with his/her anti-virus in a span of 3 days. The 5 scans produced an alert for an unknown signature being detected. Signature files contain the latest list and behaviour of known.
- After the signature was detected, the anti-virus was out of date.
- User 1's anti-virus is out of date and has not yet being updated. Thus, leaving his/her computer open to regular threats by viruses
- Anti-virus programs release signature file updates regularly--sometimes daily, sometimes more often--because new viruses are being identified on a daily basis.
- User 1 needs to update anti-virus as it is best to configure your anti-virus program to automatically check for these signature updates in order for the anti-virus to be aware of this particular signature as I may be a potential threat.

Possible Security breach and Malware found

- After checking the suspected signature on IBM X-Force Exchange, it was found that this is a high risk Trojan virus (**Figure 2.1.1** shows a snapshot from IBM-Force Exchange and **Figure 2.1.2** and **2.1.3** show Collections found for this signature).
- A Trojan horse, or Trojan, is any malicious computer program which misleads users of its true intent. Trojan horse will fall under the category of spyware.
- A Trojan horse is to implement a "key logger" program. Such programs register which buttons and keys you press on your keyboard, and send a report of them to the hacker. Since there have been multiple brute force login attempts that the firewall has picked up and blocked (taken from the firewall logs1 file).
- Since User 1 failed to update his/her anti-virus this allowed for the Trojan to be possibly be installed on the system. Thus, this is a possible breach to be wary of and further monitor.
- The Trojan could corrupt very delicate data at the core of the company's operating system, causing everything from minor glitches to an operating system crash.

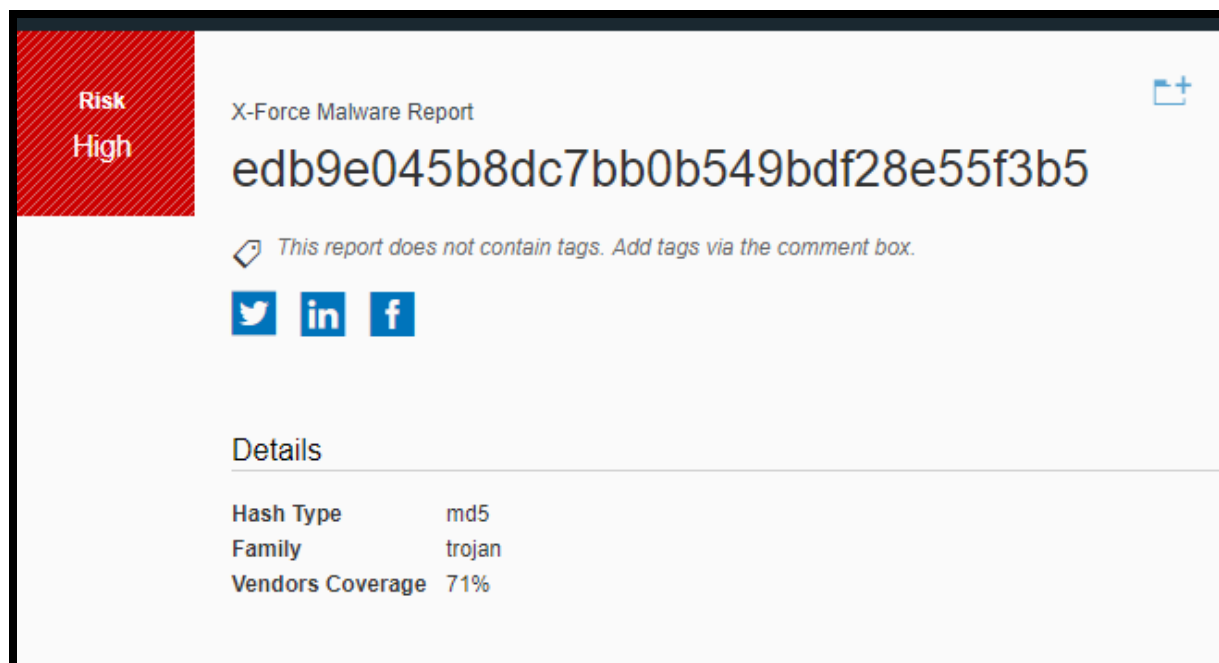


Figure 2.1.1: Snapshot of the signature “edb9e045b8dc7bb0b549bdf28e55f3b5” on IBM X-Force Exchange

0

▲

▼

Strider and Project Sauron

x-force espionage actor

Public Collection | 3 Followers | TLP: WHITE

Timeframe

- Attacks continue in August, 2016.
- Researchers have tracked this actor back to at least 2011.

Researchers recently disclosed a previously unreported threat actor called *Strider* or *Project Sauron*. For brevity and clarity, this report refers to the actor as Strider and their malware as Sauron. Strider represents a top notch adversary, and has operated without disclosure since at least 2011. They pursue espionage goals rather than harming or defrauding targets. In targeted countries, Strider compromises every key entity possible.

Strider goes to great lengths to avoid detection, as reflected in the TTPs listed below. Solid tradecraft and TTPs indicate considerable depth of experience, resources, and technical capability in Strider. Such zealous attention to detail often originates with actors intending to prosecute long-term campaigns, and perhaps a greater-than-usual sensitivity to detection. The stealth of this actor implies that the true scope of their operations could be larger than what has been detected and disclosed so far.

The rate at which Strider changes infrastructure and malware reduce the value of IP addresses and domain names as indicators of attack or compromise. We include them in this report mainly for completeness. In addition, Strider customizes the malicious implants so thoroughly that their hashes also have low value as indicators.

To support the memory-only preference in their attacks, Strider make their malware persistent on legitimate servers in the compromised network, such as domain controllers and software update servers. These legitimate servers then supply the memory-only infected hosts with malware, hiding the traffic among the legitimate demands on the server.

Strider shows a strong interest in cryptographic systems in use within victim networks. They appear to have specific, detailed technical knowledge of at least one such system (public reports do not identify it).

The wide variety of modules in Sauron's repertoire include exfiltration over numerous protocols, all engineered to appear benign and to submerge in legitimate traffic. The malware also makes extensive use of the DNS protocol for low-bandwidth meta-data exfiltration.

Figure 2.1.2: Snapshot of the suspected signature collection on IBM X-Force Exchange

Identifiers

- Strider (Symantec)
- Project Sauron (Kaspersky)

Known Campaigns

- Attacks focus on core organizations such as government, military, scientific research, telecommunications, and finance organizations.
- Publicly reported activities focus on just a few countries, notably Russia, China, Belgium, Sweden, Iran, and Rwanda.
- In targeted countries, Strider compromises every key entity possible.

TTPs

- Initial infection vector still not known.
- Frequent infrastructure changes.
- Implants tailored very specifically to targets.
- Extremely modular malware with diffuse responsibilities.
- Memory only malware on most victimized hosts.
- Hiding malware withing a "Virtual File System" implemented inside the malicious binaries.
- Persistent implants on legitimate servers within the compromised network to provide the memory-only malware to hosts within the network.
- Infection of and exfiltration from air-gapped systems.
- Low profile exfiltration on a variety of protocols including DNS, SMTP, POP3, HTTP, FTP, and TFTP.
- Nearly universal use of strong encryption for command-and-control and exfiltration traffic.

Malware Used

- Sauron (Kaspersky)
- Remsec (Symantec)

Figure 2.1.3: Snapshot of the suspected signature collection on IBM X-Force Exchange

About Sauron Malware:

The Sauron malware presents an extremely fine grained modularity when compared to most malware. The core of the Sauron malware lies in a version of the Lau scripting engine modified to support Unicode text and strings. That core loads a variety of functional modules, as configured by its master. So far, researchers have identified more than fifty different modules in the suite. Given the stealth employed by Strider, more modules probably exist. The core implants are usually unique, with differing file sizes, names, and hashes, built individually for the target and tailored to the target's environment.

A standalone network sniffer module provides deep packet inspection of traffic on TCP, UDP, POP3, SMTP, FTP, VNC, SMB, HTTP, and TFTP, and possibly more.

Strider often deploys the Sauron malware by modifying existing software deployment scripts in the compromised network to also distribute and start the infiltrated malware.

File Name: Firewall logs1

Receive Time	Type	Threat/Content	Type	Source address	Destination address	Rule	Source User	Destination User	Application	Source Zone	Destination
2018/03/27	14:27	THREAT	spyware	172.20.10.31	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/27	15:27	THREAT	spyware	172.20.10.31	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/27	16:27	THREAT	spyware	172.20.10.31	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	08:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	09:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	10:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	11:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	12:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	14:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	15:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/28	16:27	THREAT	spyware	172.20.10.24	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	08:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	09:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	10:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	11:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	12:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	13:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	14:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	15:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block
2018/03/29	16:27	THREAT	spyware	172.20.10.14	185.78.64.121	Rule68	User1	unknown-tcp	INT, EXT, forward_to_log_storage	212410	59654, 443, tcp, Block

[illegible]

Summary and notes of what was found in this log file

- 19 logs were noted for this user.
- The IP source addresses used by user 1 were found to be: 172.20.10.31, 172.20.10.24 and 172.20.10.14.
- While the destination source was the same for every entry i.e. : 185.78.64.121
- After searching the Destination IP on IBM X-Force Exchange results showed 2 collections one of a “Botnet command and control server” and the other on “Strider and Project Sauron”(Figure 2.1.4 show these results)
- Threat/Content name which appeared was Command Control traffic which Describes when a compromised system is surreptitiously communicating with an attacker's remote server to receive malicious commands or infiltrate data. This should be taken note of and further investigated even though firewall has blocked any attempts.

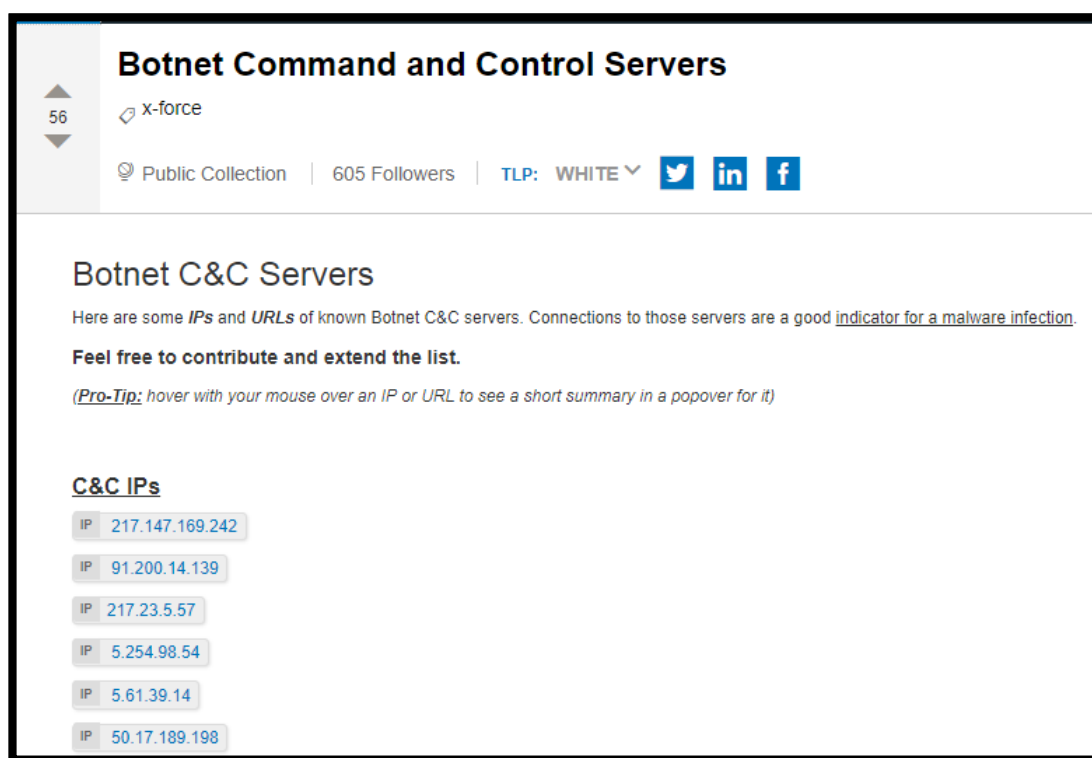


Figure 2.1.4: Showing results of destination address “185.78.64.121”

Possible Security breach and Malware found

- For every log entry the firewall found spyware as the threat entry. However, this was blocked by the firewall.
- User 1's anti-virus is not updated which would allow the spyware to be installed onto the system which may result in a breach.
- Spyware infects its victims through many different ways. The most common of these ways include drive-by download, P2P wreaks havoc, free software download, social engineering and vulnerability route.
- In the Web proxy log file, user 1 visited multiple sites and one website which was classified as spyware. When the user visits a website that pops up a window with a message like in order to properly view this website you must install this program. The FTP / HTTP Get request will initiate the download of the software onto the client machine. Installation will be performed by the user and during this installation they will be asked permission to install the malware as well as the software. This is another way of entry for the spyware picked up to be installed on the system.

Details: User 1

File Name: Web proxy logs1

```
36,2018/03/27,3:51:09 PM,User1,ACM.org,Allowed,14263,Research,None,0
39,2018/03/27,4:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
43,2018/03/27,4:57:42 PM,User1,gmail.com,Allowed,8166,Webmail,None,0
48,2018/03/28,7:59:42 AM,User1,gmail.com,Allowed,18051,Webmail,None,0
54,2018/03/28,8:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
55,2018/03/28,8:38:53 AM,User1,sabs.co.za,Allowed,12869,Government,None,0
57,2018/03/28,8:53:17 AM,User1,www.journals.elsevier.com/energy-research-and-social-science/,Allowed,17157,Research,None,0
62,2018/03/28,9:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
68,2018/03/28,10:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
73,2018/03/28,11:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
78,2018/03/28,12:02:53 PM,User1,gmail.com,Allowed,8166,Webmail,None,0
79,2018/03/28,12:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
82,2018/03/28,1:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
86,2018/03/28,2:09:01 PM,User1,linkedin.com,Allowed,16074,Social Media,None,0
89,2018/03/28,2:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
92,2018/03/28,3:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
93,2018/03/28,3:38:09 PM,User1,ieee.org,Allowed,14263,Research,None,0
98,2018/03/28,4:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
102,2018/03/28,4:57:42 PM,User1,gmail.com,Allowed,8166,Webmail,None,0
105,2018/03/29,7:53:19 AM,User1,google.co.za,Allowed,16074,Search Engine,None,0
111,2018/03/29,8:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
112,2018/03/29,8:46:17 AM,User1,ieee.org,Allowed,17157,Research,None,0
113,2018/03/29,8:46:53 AM,User1,ACM.org,Allowed,12869,Research,None,0
118,2018/03/29,9:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
122,2018/03/29,10:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
127,2018/03/29,11:29:16 AM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
128,2018/03/29,11:59:53 AM,User1,gmail.com,Allowed,8166,Webmail,None,0
131,2018/03/29,12:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
133,2018/03/29,1:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
137,2018/03/29,2:04:07 PM,User1,gmail.com,Allowed,8166,Webmail,None,0
139,2018/03/29,2:07:01 PM,User1,linkedin.com,Allowed,16074,Social Media,None,0
142,2018/03/29,2:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
146,2018/03/29,3:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
148,2018/03/29,3:51:09 PM,User1,ACM.org,Allowed,14263,Research,None,0
150,2018/03/29,4:29:16 PM,User1,flowershop22.110mb.com,Not allowed to browse this Malicious URL,246,Suspected Spyware or Adware,None,90
154,2018/03/29,4:57:42 PM,User1,gmail.com,Allowed,8166,Webmail,None,0
```

Summary and notes of what was found in this log file

- User 1 visits multiple sites such as Gmail, LinkedIn, and Google which were allowed for browsing.
- However, he/she visits a URL i.e. flowershop22.110mb.com which has been classified as Spyware or adware for the threat category.
- He/She has visited this site for the past 3 days from 2018/03/27 till the 2018/03/29 on multiple occasions in one day.

Possible Security breach and Malware found

- Malware found was spyware or adware.
- Possibly due to anti-virus not being updated.
- flowershop22.110mb.com: This URL takes you to a website which allows you to copy the hostname i.e. : flowershop22.110mb.com which is commonly used as a target for communicating with malware, hosting malware or acting as a vector for attacking targets in watering hole attacks.
- This is a secondary domain name from a primary domain name i.e.: all the secondary domains share the same primary domain hence “.110mb.com”
- This hostname picked up on IBM’s X-Force Exchange and has been categorized as malware with a high risk level of 10 (Screenshots of this are provided below in **figure 2.1.5 and 2.1.6**).
- This is malware that the company should definitely be concerned about.
- Results from IBM X-Force Exchange show that this spyware breach may have come from a group called Strider. Strider uses an advanced piece of software known as Remsec which contains a number of stealth features that help it to avoid detection. Several of its components are in the form of executable blobs (Binary Large Objects), which are more difficult for traditional antivirus software to detect.

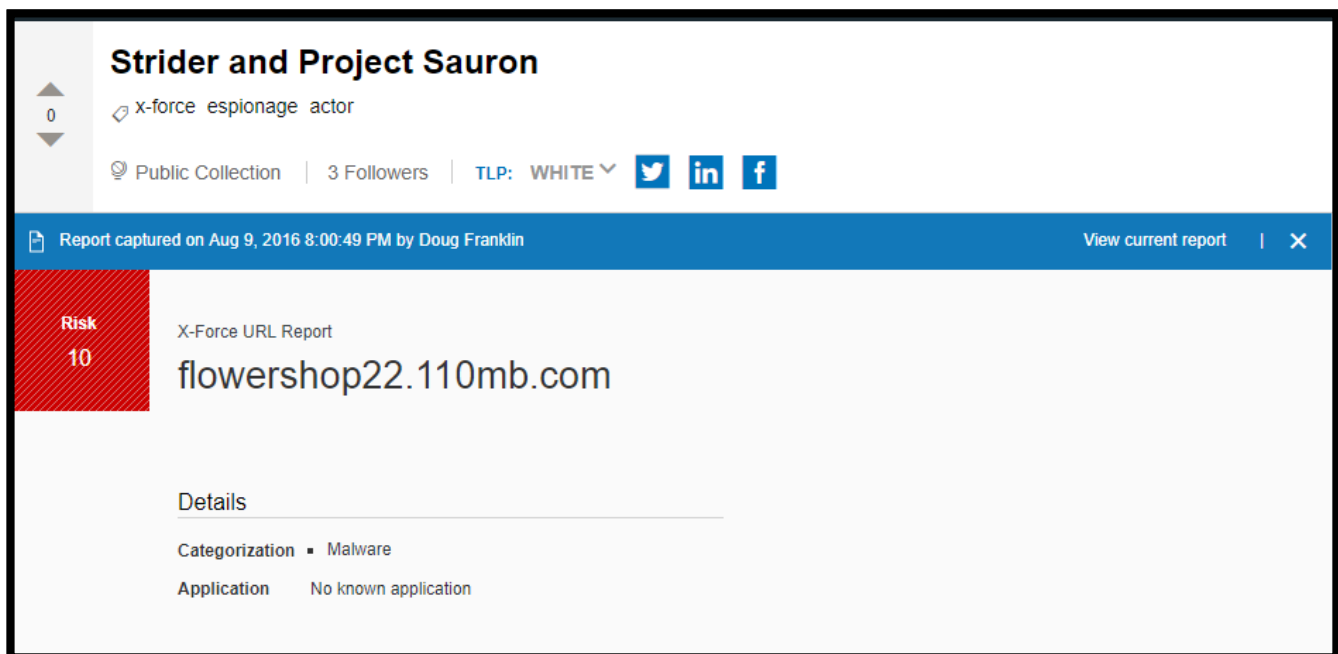


Figure 2.1.5: Snapshot 1 of flowershop22.110mb.com on IBM X-Force exchange

The screenshot shows the IBM X-Force Exchange interface. At the top, there's a search bar with the text 'Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...'. Below the search bar, the collection name 'Strider and Project Sauron' is displayed, along with a tag 'x-force espionage actor'. The collection is a 'Public Collection' with '3 Followers' and a 'TLP: WHITE' classification. There are social media icons for Twitter, LinkedIn, and Facebook. Below this, a table lists 3 malware entries:

Family	MD5 hash	Date
MWF TR/BHO.Gen	MAL ED5B29587FC8BCE1042DDDB118AE2483	Jul 19, 2009 12:17 AM
MWF Win.Trojan.Bho-2499	MAL C46579290C6A4450ABEFB2BBCBC9C721	Jul 11, 2009 2:24 AM
MWF Trojan.Spy-202	MAL 0EEE6A2FEC304BC52B837CC70A0794ED	Feb 21, 2009 9:39 AM

Figure 2.1.6: Snapshot 2 of flowershop22.110mb.com on IBM X-Force exchange

Strider and Project Sauron

A previously unknown group called Strider has been conducting cyber espionage-style attacks against selected targets in Russia, China, Sweden, and Belgium. Strider has been highly selective in its choice of targets and, to date, Symantec has found evidence of infections in 36 computers across seven separate organizations. The group uses an advanced piece of malware known as Remsec (Backdoor. Remsec) to conduct its attacks. Remsec is a stealthy tool that appears to be primarily designed for spying purposes.

Details: User 2

File Name: Antivirus_log_collection1

Date	Machine	Status	Action	Additional information
27/03/2018 15:05:12	RnD_USER2	Scan complete: WARNING Suspicious signature detected	Alert	Signature: db07e1740152e09610ea826655d27e8d
28/03/2018 09:16:16	RnD_USER2	Alert: Antivirus is out of date		
28/03/2018 11:04:47	RnD_USER2	Scan complete: WARNING Suspicious signature detected	Alert	Signature: db07e1740152e09610ea826655d27e8d
28/03/2018 15:05:12	RnD_USER2	Scan complete: WARNING Suspicious signature detected	Alert	Signature: db07e1740152e09610ea826655d27e8d
29/03/2018 09:17:27	RnD_USER2	Alert: Antivirus is out of date		
29/03/2018 11:04:12	RnD_USER2	Scan complete: WARNING Suspicious signature detected	Alert	Signature: db07e1740152e09610ea826655d27e8d
29/03/2018 15:05:12	RnD_USER2	Scan complete: WARNING Suspicious signature detected	Alert	Signature: db07e1740152e09610ea826655d27e8d

Summary and notes of what was found in this log file

- User 2 results were the same as User 1 for this file.
- User 2 had 5 scans done with his/her anti-virus in a span of 3 days. The 5 scans produced an alert for an unknown signature being detected. Signature files contain the latest list and behaviour of known.
- User 2's anti-virus is out of date and has not yet being updated. Thus, leaving his/her computer and system open to regular threats by viruses.
- Signature found by anti-virus : "db07e1740152e09610ea826655d27e8d"

Possible Security breach and Malware found

- Signature files contain the latest list and behaviour of known.
- Anti-virus programs release signature file updates regularly--sometimes daily, sometimes more often--because new viruses are being identified on a daily basis.
- Thus, it is important that user 2 needs to update anti-virus as it is best to configure your anti-virus program to automatically check for these signature updates in order for the anti-virus to be aware if this particular signature is a potential threat.
- The unknown signature is found to be a high risk spyware, Trojan, virus.(Screenshot shown below **Figure 2.1.7**)

➤

- IBM X-Force Exchange found 2 collections for this signature one of which is called “Dragonfly Energy Sector Attacks” (Shown in **figure 2.1.8**)
- **Dragonfly Energy Sector Attacks:** The Dragonfly group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so.
- Thus, this is another possible breach.
- Indicating further from user 1 and user 2 results that thus far the system has high chance of potential spyware installed on it.

The screenshot displays a malware report interface. On the left, a red box with a diagonal pattern contains the text 'Risk High'. The main content area is titled 'X-Force Malware Report' and features a large MD5 hash: 'db07e1740152e09610ea826655d27e8d'. Below the hash, a note states: 'This report does not contain tags. Add tags via the comment box.' There are three social media icons (Twitter, LinkedIn, Facebook) below the note. A section titled 'Details' is separated by a horizontal line. Below this line, the following information is listed: 'Hash Type' is 'md5', 'Family' is 'heuristic, spyware, tool, trojan', and 'Vendors Coverage' is '61%'.

Hash Type	md5
Family	heuristic, spyware, tool, trojan
Vendors Coverage	61%




Figure 2.1.7: Results of the suspected signature on IBM X-Force Exchange

0

Dragonfly - Energy Sector Attacks

X-force

Public Collection | 11 Followers | TLP: WHITE



Dragonfly - Energy Sector Attacks

Time Frame

- Since this past May, threat actors have identified as targeting organizations and government entities in the nuclear, energy, aviation, water, and manufacturing sectors. This campaign is still ongoing, and threat actors are actively pursuing their ultimate objectives over a long-term campaign. The FBI and Department of Homeland Security recently released a report over the weekend, providing detailed information on this advanced persistent threat that included indicators of compromise, other technical information about the APT adversaries' actions, and details about the compromised victims' networks. The US-CERT has issued an Alert (Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, TA17-293A) as a result of this release of information. Proventia customers have a signature, HTTP_Post_Dragonfly_CnC, that provides protection against Dragonfly.

Industry

Targeting organizations and government entities in the following sectors:

- nuclear
- energy
- aviation
- water
- manufacturing

Attack Type

- open-source reconnaissance
- spear-phishing emails (from compromised legitimate accounts)
- watering-hole domains
- host-based exploitation
- industrial control system (ICS) infrastructure targeting
- ongoing credential gathering

Figure 2.1.8: Results of the suspected signature on IBM X-Force Exchange Collection for Dragonfly

Receive Time	Type	Threat/Content Type	Source address	Destination address	Rule	Source User	Destination User	Application	Source Zone	Destination Zone
2018/03/27 14:18	THREAT	spyware	172.20.10.24	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/27 15:18	THREAT	spyware	172.20.10.24	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/27 16:18	THREAT	spyware	172.20.10.24	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/27 16:18	THREAT	spyware	172.20.10.24	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 08:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 09:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 10:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 11:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 12:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 14:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 15:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/28 16:18	THREAT	spyware	172.20.10.12	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 08:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 09:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 10:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 11:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 12:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 13:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 14:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 15:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block
2018/03/29 16:18	THREAT	spyware	172.20.10.21	184.154.150.66	Rule68	User2	unknown-tcp	INT,EXT,forward_to_log_storage	212410	59654,443,tcp,Block

[illegible]

- 20 logs were noted for this user.
- The IP source addresses used by user 1 were found to be: 172.20.10.24, 172.20.10.12 and 172.20.10.21.
- While the destination source was the same for every entry i.e. : 184.154.150.66
- Threat/Content name which appeared was Command Control traffic which describes when a compromised system is surreptitiously communicating with an attacker's remote server to receive malicious commands or exfiltrate data. This should be taken note of and further investigated even though firewall has blocked any attempts.

Possible Security breach and Malware found

- For every log entry the firewall found spyware as the threat entry this was however blocked by the firewall.
 - User 2 visits many sites (cross referenced from the log file web proxy logs1), any of which could have had pop-up messages and links to install the spyware.
-

Details: User 2

File Name: Web proxy logs1

```
2,2018/03/27,7:59:42 AM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
9,2018/03/27,8:59:46 AM,User2,www.journals.elsevier.com/energy-research-and-social-science/,Allowed,17157,Research,None,0
10,2018/03/27,9:01:14 AM,User2,phys.org,Allowed,24268,Research,None,0
16,2018/03/27,10:31:14 AM,User2,sabs.co.za,Allowed,12869,Government,None,0
20,2018/03/27,12:03:24 PM,User2,linkedin.com,Allowed,16074,Social Media,None,0
26,2018/03/27,2:06:41 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
28,2018/03/27,2:08:51 PM,User2,facebook.com,Allowed,24268,Social Media,None,0
33,2018/03/27,3:26:47 PM,User2,ieee.org,Allowed,12831,Research,None,0
40,2018/03/27,4:48:24 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
45,2018/03/27,4:59:37 PM,User2,linkedin.com,Allowed,16074,Social Media,None,0
47,2018/03/28,7:57:24 AM,User2,yahoo-mail.com,Allowed,16074,Webmail,None,0
56,2018/03/28,8:47:46 AM,User2,www.journals.elsevier.com/energy-research-and-social-science/,Allowed,17157,Research,None,0
60,2018/03/28,9:14:14 AM,User2,saiee.org.za,Allowed,24268,Research,None,0
67,2018/03/28,10:24:14 AM,User2,ACM.org,Allowed,12869,Research,None,0
76,2018/03/28,11:57:24 AM,User2,linkedin.com,Allowed,16074,Social Media,None,0
85,2018/03/28,2:06:51 PM,User2,facebook.com,Allowed,24268,Social Media,None,0
88,2018/03/28,2:17:41 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
94,2018/03/28,3:46:47 PM,User2,phys.org,Allowed,12831,Research,None,0
99,2018/03/28,4:48:24 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
104,2018/03/28,5:02:36 PM,User2,linkedin.com,Allowed,16074,Social Media,None,0
106,2018/03/29,7:59:42 AM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
115,2018/03/29,8:59:46 AM,User2,www.journals.elsevier.com/energy-research-and-social-science/,Allowed,17157,Research,None,0
116,2018/03/29,9:01:14 AM,User2,phys.org,Allowed,24268,Research,None,0
123,2018/03/29,10:31:14 AM,User2,sabs.co.za,Allowed,12869,Government,None,0
129,2018/03/29,12:03:24 PM,User2,linkedin.com,Allowed,16074,Social Media,None,0
138,2018/03/29,2:06:41 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
140,2018/03/29,2:08:51 PM,User2,facebook.com,Allowed,24268,Social Media,None,0
145,2018/03/29,3:26:47 PM,User2,ieee.org,Allowed,12831,Research,None,0
151,2018/03/29,4:48:24 PM,User2,yahoo-mail.com,Allowed,18051,Webmail,None,0
156,2018/03/29,4:59:37 PM,User2,linkedin.com,Allowed,16074,Social Media,None,0
```

Summary and notes of what was found in this log file

- User 2 has a total of 30 web proxy logs.
- He/She has visited multiple websites i.e.: yahoo-mail.com, linkedin.com, facebook.com, phys.org, www.journals.elsevier.com/energy-research-and-social-science, ieee.org, ACM.org and saiee.org.za all of which have been allowed.
- No suspicious activities for user 2 have been found for this log file.

Details: User 3

File Name: Antivirus_log_collection1

Date	Machine	Status	Action	Additional information
27/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
28/03/2018 09:19:16	PA_USER3	Alert: Antivirus is out of date		
28/03/2018 11:04:36	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
28/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
29/03/2018 09:18:19	PA_USER3	Alert: Antivirus is out of date		
29/03/2018 11:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
29/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	

Summary and notes of what was found in this log file

- User 3 had 5 scans done with his/her anti-virus in a span of 3 days.
- The 5 scans produced an alert for a suspicious file suspected to be a generic Trojan
- File of the suspected Trojan is Snappy_bird.swf. **Figure 2.1.9** shows a snapshot of User 3's anti-virus log file records.
- Snappy bird is a free game which is available on the app store.

Possible Security breach and Malware found

- Malware found was a Trojan which is a type of spyware.
- Downloading Snappy bird may be a way for malicious software to be installed into the system. Due to the game possibly containing a Trojan horse.
- User 3's anti-virus is out of date and has not yet being updated. Thus, leaving his/her computer open to the Trojan which has been found by the anti-virus.
- User 3 needs to update anti-virus as it is best to configure your anti-virus program to automatically check for these updates in order for the anti-virus to be aware of any new threats that have been found.

Date	Machine	Status	Action	Additional information
27/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
28/03/2018 09:19:16	PA_USER3	Alert: Antivirus is out of date		
28/03/2018 11:04:36	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
28/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
29/03/2018 09:18:19	PA_USER3	Alert: Antivirus is out of date		
29/03/2018 11:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	
29/03/2018 15:04:47	PA_USER3	Scan complete: WARNING Suspicious file detected: Generic Trojan Alert	File: /browser/temp/Snappy_bird.swf	

Figure 2.1.9: Snapshot of User 3's anti-virus log records.

File Name: Firewall log1

[illegible][illegible]

Summary and notes of what was found in this log file

- 21 log records were noted for this user 3. For every log entry the firewall found spyware as the threat entry.
- A suspicious DNS query was picked up by the firewall as (generic:www.gyd900yhllcfci.info)
- gyd900yhllcfci.info has been found to be a domain name. It has been used an email address @ceo gyd900yhllcfci.info.
- The firewall provided an alert for this DNS query.
- The IP source addresses used by user 3 were found to be : 172.20.10.18, 172.20.10.17 and 172.20.10.19
- While the destination source was the same for every entry i.e. : 41.57.15.146 should be taken note of and further investigated even though firewall has blocked any attempts.

Possible Security breach and Malware found

- This domain name could be used for phishing.
- Phishing involves sending email messages that seem to come from trustworthy sources, such as banking entities, but attempt to harvest confidential user data. In order to do so, they usually include a link that, if accessed, takes the user to a fake website. By doing this, users believe they are interacting with a trustworthy website, enter the information requested, which finally ends up in the hands of the fraudster.

Details: User 3

File Name: Web proxy logs1

```
3, 2018/03/27, 8:02:49 AM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
4, 2018/03/27, 8:07:04 AM, User3, linkedin.com, Allowed, 8051, Social Media, None, 0
5, 2018/03/27, 8:07:04 AM, User3, twitter.com, Allowed, 8166, Social Media, None, 0
11, 2018/03/27, 9:28:04 AM, User3, pinterest.com, Allowed, 27935, Social Media, None, 0
15, 2018/03/27, 10:28:04 AM, User3, youtube.com/search?cat-videos, Allowed, 147082, Videos, None, 0
22, 2018/03/27, 1:36:24 PM, User3, funnyflashgames.com, Allowed, 74952, General Browsing, None, 0
24, 2018/03/27, 1:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
31, 2018/03/27, 2:54:41 PM, User3, vimeo.com/funny_videos, Allowed, 179852, Videos, None, 0
32, 2018/03/27, 2:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
35, 2018/03/27, 3:46:14 PM, User3, netflix.com, Allowed, 426397, Videos, None, 0
37, 2018/03/27, 3:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
42, 2018/03/27, 4:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
44, 2018/03/27, 4:59:16 PM, User3, linkedin.com, Allowed, 16074, Social Media, None, 0
46, 2018/03/27, 5:02:36 PM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
49, 2018/03/28, 8:04:49 AM, User3, twitter.com, Allowed, 8166, Social Media, None, 0
50, 2018/03/28, 8:06:04 AM, User3, pinterest.com, Allowed, 27935, Social Media, None, 0
51, 2018/03/28, 8:09:04 AM, User3, linkedin.com, Allowed, 8051, Social Media, None, 0
59, 2018/03/28, 8:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
61, 2018/03/28, 9:18:04 AM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
65, 2018/03/28, 9:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
69, 2018/03/28, 10:31:04 AM, User3, funnyflashgames.com, Allowed, 147082, General Browsing, None, 0
71, 2018/03/28, 10:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
74, 2018/03/28, 11:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
75, 2018/03/28, 11:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
80, 2018/03/28, 12:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
81, 2018/03/28, 1:26:24 PM, User3, youtube.com/search?funny_videos, Allowed, 74952, General Browsing, None, 0
84, 2018/03/28, 1:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
90, 2018/03/28, 2:54:41 PM, User3, showmax.co.za, Allowed, 179852, Videos, None, 0
```

```
91, 2018/03/28, 2:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
95, 2018/03/28, 3:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
101, 2018/03/28, 4:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
103, 2018/03/28, 4:59:37 PM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
107, 2018/03/29, 8:02:49 AM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
108, 2018/03/29, 8:07:04 AM, User3, linkedin.com, Allowed, 8051, Social Media, None, 0
109, 2018/03/29, 8:07:04 AM, User3, twitter.com, Allowed, 8166, Social Media, None, 0
114, 2018/03/29, 8:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
117, 2018/03/29, 9:28:04 AM, User3, pinterest.com, Allowed, 27935, Social Media, None, 0
120, 2018/03/29, 9:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
121, 2018/03/29, 10:28:04 AM, User3, youtube.com/search?cat-videos, Allowed, 147082, Videos, None, 0
```

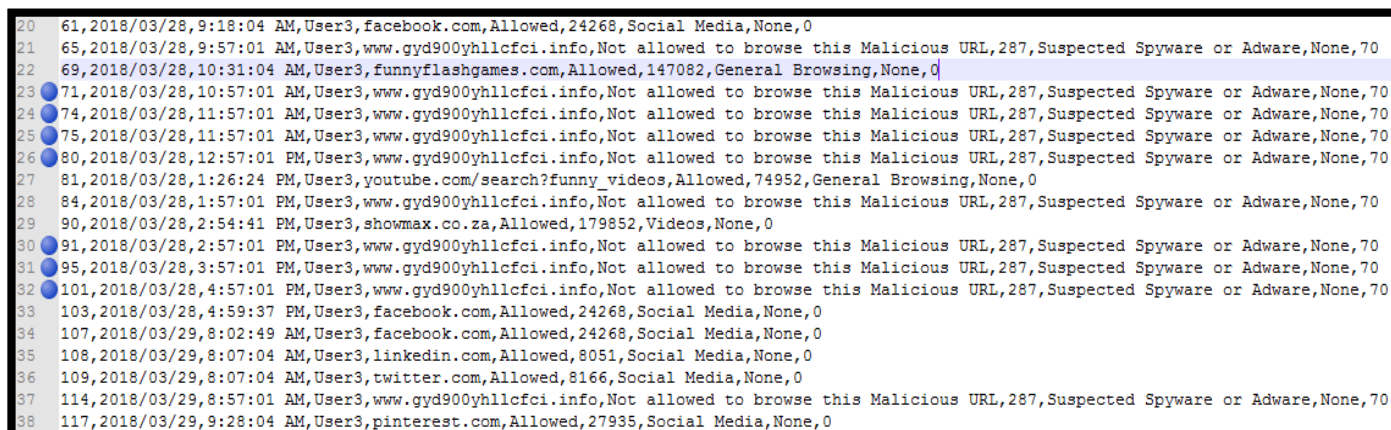
```
125, 2018/03/29, 10:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
132, 2018/03/29, 12:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
134, 2018/03/29, 1:36:24 PM, User3, funnyflashgames.com, Allowed, 74952, General Browsing, None, 0
136, 2018/03/29, 1:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
143, 2018/03/29, 2:54:41 PM, User3, vimeo.com/funny_videos, Allowed, 179852, Videos, None, 0
144, 2018/03/29, 2:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
147, 2018/03/29, 3:46:14 PM, User3, netflix.com, Allowed, 426397, Videos, None, 0
149, 2018/03/29, 3:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
153, 2018/03/29, 4:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
155, 2018/03/29, 4:59:16 PM, User3, linkedin.com, Allowed, 16074, Social Media, None, 0
157, 2018/03/29, 5:02:36 PM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
```

Summary and notes of what was found in this log file

- User 3 visits gyd900yhllcfci.info which has been classified as suspected Spyware or adware for the threat category
- He/She has visited this site for the past 3 days from 2018/03/27 till the 2018/03/29 on multiple occasions in one day.
- He/She attempts to go on gyd900yhllcfci.info 5 times on the 2018/03/28 with a small time gap in between (screenshot of this is shown below in **figure 2.1.10**)

Possible Security breach and Malware found

- Malware found to be spyware or adware.
- This is a breach that may have resulted from the user going on this website which provided this domain name and clicking on a link to use the domain name.



The screenshot displays a list of browser history entries. The entries are numbered on the left margin from 20 to 38. Each entry contains a timestamp, the user name 'User3', the website visited, the browser's decision (Allowed or Not allowed), and a threat classification. Several entries show visits to 'www.gyd900yhllcfci.info', which is consistently classified as a 'Malicious URL' and 'Suspected Spyware or Adware'. Other entries show visits to legitimate sites like 'facebook.com', 'funnyflashgames.com', and 'youtube.com'.

20	61, 2018/03/28, 9:18:04 AM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
21	65, 2018/03/28, 9:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
22	69, 2018/03/28, 10:31:04 AM, User3, funnyflashgames.com, Allowed, 147082, General Browsing, None, 0
23	71, 2018/03/28, 10:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
24	74, 2018/03/28, 11:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
25	75, 2018/03/28, 11:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
26	80, 2018/03/28, 12:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
27	81, 2018/03/28, 1:26:24 PM, User3, youtube.com/search?funny_videos, Allowed, 74952, General Browsing, None, 0
28	84, 2018/03/28, 1:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
29	90, 2018/03/28, 2:54:41 PM, User3, showmax.co.za, Allowed, 179852, Videos, None, 0
30	91, 2018/03/28, 2:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
31	95, 2018/03/28, 3:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
32	101, 2018/03/28, 4:57:01 PM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
33	103, 2018/03/28, 4:59:37 PM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
34	107, 2018/03/29, 8:02:49 AM, User3, facebook.com, Allowed, 24268, Social Media, None, 0
35	108, 2018/03/29, 8:07:04 AM, User3, linkedin.com, Allowed, 8051, Social Media, None, 0
36	109, 2018/03/29, 8:07:04 AM, User3, twitter.com, Allowed, 8166, Social Media, None, 0
37	114, 2018/03/29, 8:57:01 AM, User3, www.gyd900yhllcfci.info, Not allowed to browse this Malicious URL, 287, Suspected Spyware or Adware, None, 70
38	117, 2018/03/29, 9:28:04 AM, User3, pinterest.com, Allowed, 27935, Social Media, None, 0

Figure 2.1.10 : Screenshot of User 3's browsing history times for gyd900yhllcfci.info on the 2018/03/28.

Details: User 4

File Name: Antivirus_log_collection1

Date	Machine	Status	Action	Additional information
28/03/2018 09:17:08	RnD_USER4	Status: OK		
28/03/2018 11:04:12	RnD_USER4	Scan complete: no detections		
28/03/2018 15:04:28	RnD_USER4	Scan complete: no detections		
29/03/2018 09:19:03	RnD_USER4	Status: OK		
29/03/2018 11:04:28	RnD_USER4	Scan complete: no detections		
29/03/2018 15:04:28	RnD_USER4	Scan complete: no detections		

Summary and notes of what was found in this log file

- User 4 anti-virus is up to date.
- All scans done found no suspicious activity.
- Anti-virus status is "OK"

Details: User 4

File Name: Firewall log1

- No logs recorded for user 4

Details: User 4

File Name: Web proxy logs1

```
6,2018/03/27,8:24:36 AM,User4,hotmail.com,Allowed,8159,Webmail,None,0
12,2018/03/27,9:47:24 AM,User4,www.thebalancecareers.com/what-to-do-when-you-hate-your-job-2060644,Allowed,8159,General Browsing,None,0
13,2018/03/27,9:49:47 AM,User4,ndoherty.com/job-hate/,Allowed,3579,General Browsing,None,0
14,2018/03/27,9:57:41 AM,User4,onlinegambling.com,Allowed,17157,General Browsing,None,0
17,2018/03/27,10:53:24 AM,User4,wikileaks.org,Allowed,8159,General Browsing,None,0
18,2018/03/27,11:14:53 AM,User4,anonofficial.com,Allowed,16074,General Browsing,None,0
21,2018/03/27,12:07:46 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
23,2018/03/27,1:42:36 PM,User4,how-to.com/win-at-online-gambling,Allowed,14751,General Browsing,None,0
29,2018/03/27,2:16:24 PM,User4,how-to.com/make-money,Allowed,8159,General Browsing,None,0
38,2018/03/27,4:01:58 PM,User4,self-help.com/how-to-get-rich-quick/,Allowed,8159,General Browsing,None,0
41,2018/03/27,4:49:16 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
52,2018/03/28,8:14:36 AM,User4,hotmail.com,Allowed,8159,Webmail,None,0
53,2018/03/28,8:16:24 AM,User4,wikileaks.org,Allowed,8159,General Browsing,None,0
58,2018/03/28,8:53:36 AM,User4,anonofficial.com,Allowed,16074,General Browsing,None,0
63,2018/03/28,9:36:24 AM,User4,how-to.com/steal-company-secrets,Allowed,8159,General Browsing,None,0
64,2018/03/28,9:42:47 AM,User4,how-to.com/anonymous-emails,Allowed,3579,General Browsing,None,0
66,2018/03/28,9:57:41 AM,User4,en.wikipedia.org/wiki/The_Anarchist_Cookbook,Allowed,17157,General Browsing,None,0
70,2018/03/28,10:46:24 AM,User4,wikileaks.org,Allowed,8159,General Browsing,None,0
72,2018/03/28,11:21:53 AM,User4,anonofficial.com,Allowed,16074,General Browsing,None,0
77,2018/03/28,12:01:46 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
83,2018/03/28,1:47:36 PM,User4,anonofficial.com,Allowed,14751,General Browsing,None,0
87,2018/03/28,2:16:24 PM,User4,anonymous-mail.com,Allowed,8159,General Browsing,None,0
96,2018/03/28,4:01:58 PM,User4,how-to.com/anonymous-emails,Allowed,3579,General Browsing,None,0
97,2018/03/28,4:06:42 PM,User4,how-to.com/steal-company-secrets,Allowed,8159,General Browsing,None,0
100,2018/03/28,4:49:16 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
110,2018/03/29,8:24:36 AM,User4,hotmail.com,Allowed,8159,Webmail,None,0
119,2018/03/29,9:47:24 AM,User4,anonymous-mail.com,Allowed,2649573,General Browsing,None,0
124,2018/03/29,10:53:24 AM,User4,wikileaks.org,Allowed,8159,General Browsing,None,0
126,2018/03/29,11:14:53 AM,User4,anonofficial.com,Allowed,16074,General Browsing,None,0
130,2018/03/29,12:07:46 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
135,2018/03/29,1:42:36 PM,User4,www.textfiles.com/anarchy/JOLLYROGER/,Allowed,1463,General Browsing,None,0
141,2018/03/29,2:16:24 PM,User4,anonymous-mail.com,Allowed,1357342,General Browsing,None,0
152,2018/03/29,4:49:16 PM,User4,hotmail.com,Allowed,8159,Webmail,None,0
```

Summary and notes of what was found in this log file

- User 4 visits multiple websites which were allowed.
- However, User 4 search results were suspicious and should be seen as a possible threats
- A table(**Table 2.1.1**) shown below of the suspicious searches for user 4.
- User 4 is definitely someone who should be further investigated
- He/She maybe be the cause of the previously mentioned potential malware found on the system.

URL	What was searched by User 4	About the website
www.thebalancecareers.com	what-to-do-when-you-hate-your-job-	Job website for searching and researching different job opportunities.
ndoherty.com	job-hate	Website which teaches people how to make a living online.
onlinegambling.com	Online gambling	Website which shows people different locations to play at and teaches them how to improve their gambling skills.
wikileaks.org	-	WikiLeaks is an international non-profit organization that publishes secret information, <u>news leaks</u> , ^[5] and classified media provided by anonymous <u>sources</u> .
how-to.com	win-at-online-gambling	Website which shows easy step by step illustrations of how to do things.
how-to.com	make-money	Website which shows easy step by step illustrations of how to do things.
self-help.com	how-to-get-rich-quick	Financial service help website
anonofficial.com	-	Anonymous official website. Anonymous is a decentralized international hacktivist group that is widely known for its various DDOS cyber-attacks against several governments
how-to.com	steal-company-secrets	Website which shows easy step by step illustrations of how to do things.
how-to.com	anonymous-emails	Website which shows easy step by step illustrations of how to do things.
wikipedia.org	The_Anarchist_Cookbook	A book that contains instructions for the manufacture of <u>explosives</u> , rudimentary telecommunications <u>phreaking</u> devices, and related weapons, as well as instructions for home manufacturing of illicit drugs, including <u>LSD</u> .
http://anonymous-mail.com/	Send anonymous emails	Website which allows someone to send anonymous emails.
www.textfiles.com	anarchy/JOLLYROGER	Website which provides text files with instructions on how to make explosives, hacking tutorials etc.(screenshot shown below in figure 2.1.11)

Table 2.1.1: Showing User 4 Web proxy searches

Filename	Size	Description of the Textfile
000.jrc	9337	Introduction by The Jolly Roger
001.jrc	4984	Counterfeiting Money
002.jrc	8400	Credit Card Fraud
003.jrc	3055	Making Plastic Explosives from Bleach
004.jrc	1607	Picking Master Locks
005.jrc	6608	The Arts of Lockpicking I
006.jrc	2680	The Arts of Lockpicking II
007.jrc	1677	Solidox Bombs
008.jrc	7058	High Tech Revenge.jrc The Beigebox (NEW Revision 2.0)
009.jrc	928	CO2 Bombs
010.jrc	2622	Thermite Bombs
011.jrc	910	Touch Explosives
012.jrc	1389	Letter Bombs
013.jrc	721	Paint Bombs
014.jrc	1356	Ways to send a car to HELL
015.jrc	1215	Do ya hate school?
016.jrc	787	Phone related vandalism
017.jrc	2432	Highway police radar jamming
018.jrc	431	Smoke Bombs
019.jrc	654	Mail Box Bombs
020.jrc	454	Hotwiring cars
021.jrc	400	Napalm
022.jrc	450	Fertilizer Bomb
023.jrc	553	Tennis Ball Bomb

Figure 2.1.11: Anarchy and Explosives: Jolly Roger's Cookbook

Notes:

- User 4 is definitely someone to keep an eye on for potential breaches.
- He/She seems to be having financial problems and is willing to go to extensive lengths in order to make money.
- From user 4's searches, it is evident that he/she hates their job and is keen on selling company secrets to make some money as well as possibly cause havoc and harm to the company by some drastic means(seen in **figure 2.1.11**)

2.2. Analyzed log files-segmented by IP Addresses

File Name: Firewall logs1

1. Summary for Unknown User Source IP Address: **148.251.177.114**

- Recorded 24 times
- Firewall provided an “Alert” action.
- DMZ present by firewall for the 24 records which is a physical or logical sub network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
- On the 2018/03/27 08:45 the Firewall blocked a an attempt made brute force login attempt
- SSH User Authentication Brute Force Attempt - If a session has the same source and destination but triggers our child signature, 31914, 20 times in 60 seconds, we call it is a brute force attack. The child signature, 31914 is alert on every connection on ssh server.
- Firewall picked this up as a vulnerability to the system.
- On the 2018/03/27 08:46 the Firewall picked up another vulnerability which was 2 HTTP SQL Injection Attempts.
- However, the Firewall blocked this attempt.
- On the 2018/03/27 08:47 another SSH User Authentication Brute Force Attempt was made.
- In a span of 3 min 2 brute force attempts were made and a SQL inject attempt.
- Screenshot of Source IP Address: 148.251.177.114 results on IBM X-Force Exchange shown in **figure 2.2.1**
- This IP is known for bot-net member activity, devices using this IP are definitely infected and take part in DDoS attacks and port scanning spam sending etc. Hence, this is a potential breach.

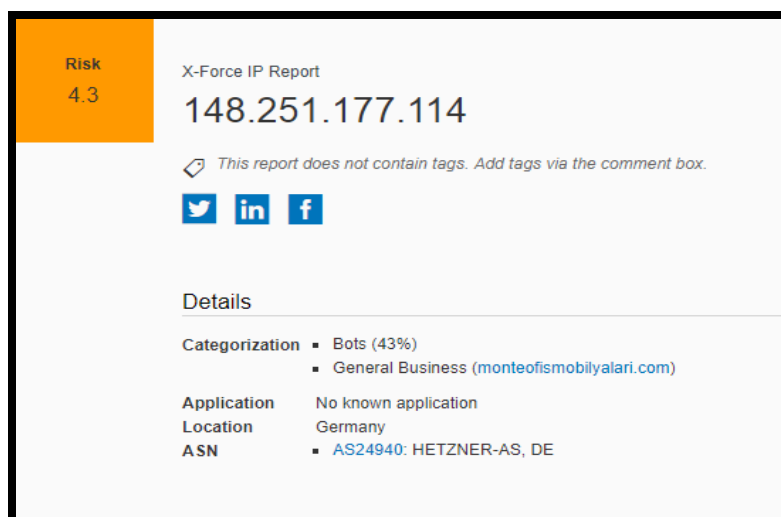


figure 2.2.1 : showing the results of the source IP Address: 148.251.177.114 on IBM X-Force Exchange

Possible Security breach and Malware found

- As seen in figure 2.2.1 the malware found is BOTS
- Malicious bots are defined as self-propagating malware that infects its host and connects back to a central server(s). The server functions as a “command and control center” for a botnet, or a network of compromised computers and similar devices. Malicious bots have the “worm-like ability to self-propagate,” and can also:
 - Gather passwords
 - Log keystrokes
 - Obtain financial information
 - Relay spam
 - Capture and analyse packets
 - Launch DoS attacks
 - Open back doors on the infected computer
 - Exploit back doors opened by viruses and worms
- Source Country for these attempts is listed as Germany. In IBM X-force Exchange Germany used this IP for botnet member activities.
- User for which this IP address is being used is unknown.
- There have been multiple brute force attempts made using this IP address which definitely calls for concern. Hence, a possible breach.

2. Summary for Unknown User Source IP Address: 222.186.129.104

- 28 records logged for this source IP address.
- All records have a DMZ present.
- This IP address was checked on IBM X-Force Exchange and resulted in no suspicious activity associated with it.
- On the 2018/03/29 the firewall picked up 3 vulnerabilities which included 2 brute force attempts and one SQL injection. However, this was blocked by the Firewall.

3. Summary for Unknown User Source IP Address: 46.29.161.175

- 30 records logged for this IP address.
- 2 SSH User authentication brute force attempts found and blocked by the firewall.
- HTTP SQL Injection Attempt found and blocked by the firewall.
- SQL Injection Attempt Found and blocked by firewall.
- HTTP SSH User authentication brute force attempt found and blocked by the firewall.
- These attempts all have the source country as Russia.
- Results shown below of Source IP 46.29.161.175 in **Figure 2.2.2 and 2.2.3**

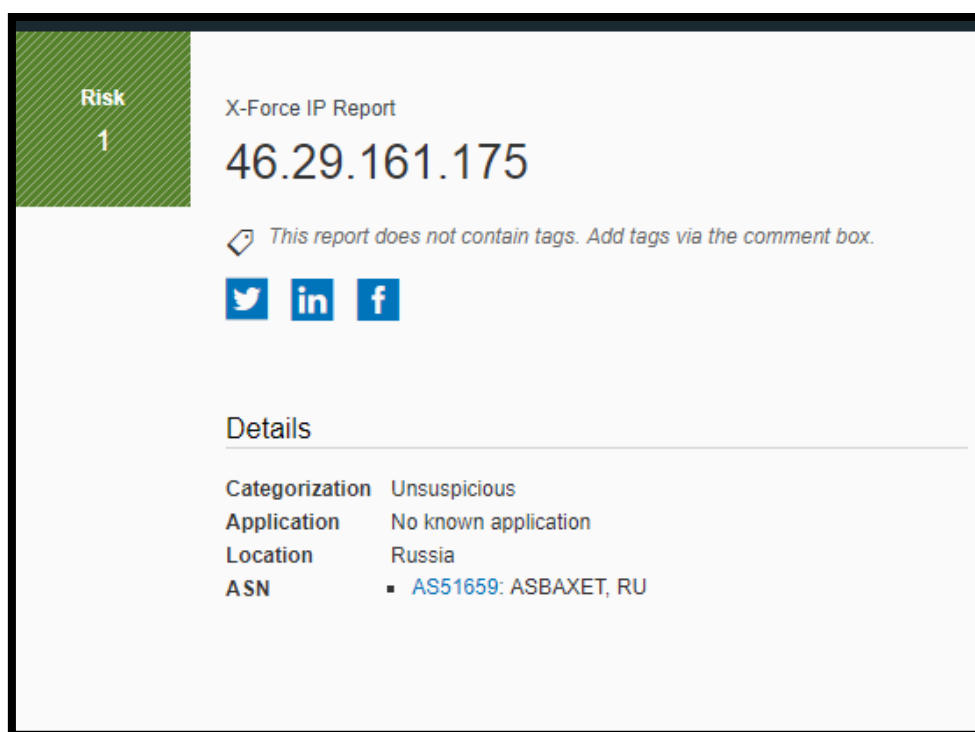


Figure 2.2.2: Showing results for IP “46.29.161.175” on IBM X-Force Exchange

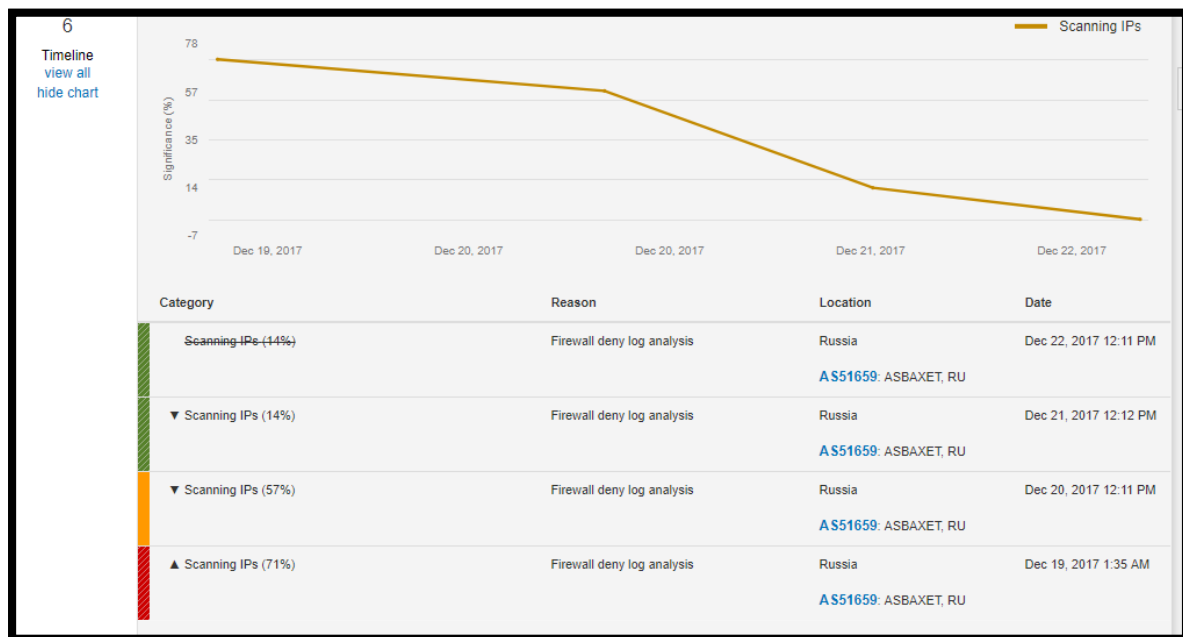


Figure 2.2.3: Showing results for IP “46.29.161.175” on IBM X-Force Exchange

Possible Security breach and Malware found

- This IP has a risk level of 1 and was found in **Russia** for illegally scanning networks for vulnerabilities.
- Possible breach using this IP address as the source country for previously mentioned attempts is listed for Russia.
- There are definitely illegal scans being conducted on the network.

4. Summary for Unknown User Source IP Address: 185.56.82.56

- One record found of this source IP
- Firewall logged this as an alert.
- Host sweep scan was done.
- Screenshot of results from IBM X-Force Exchange shown below(Figure 2.2.4)

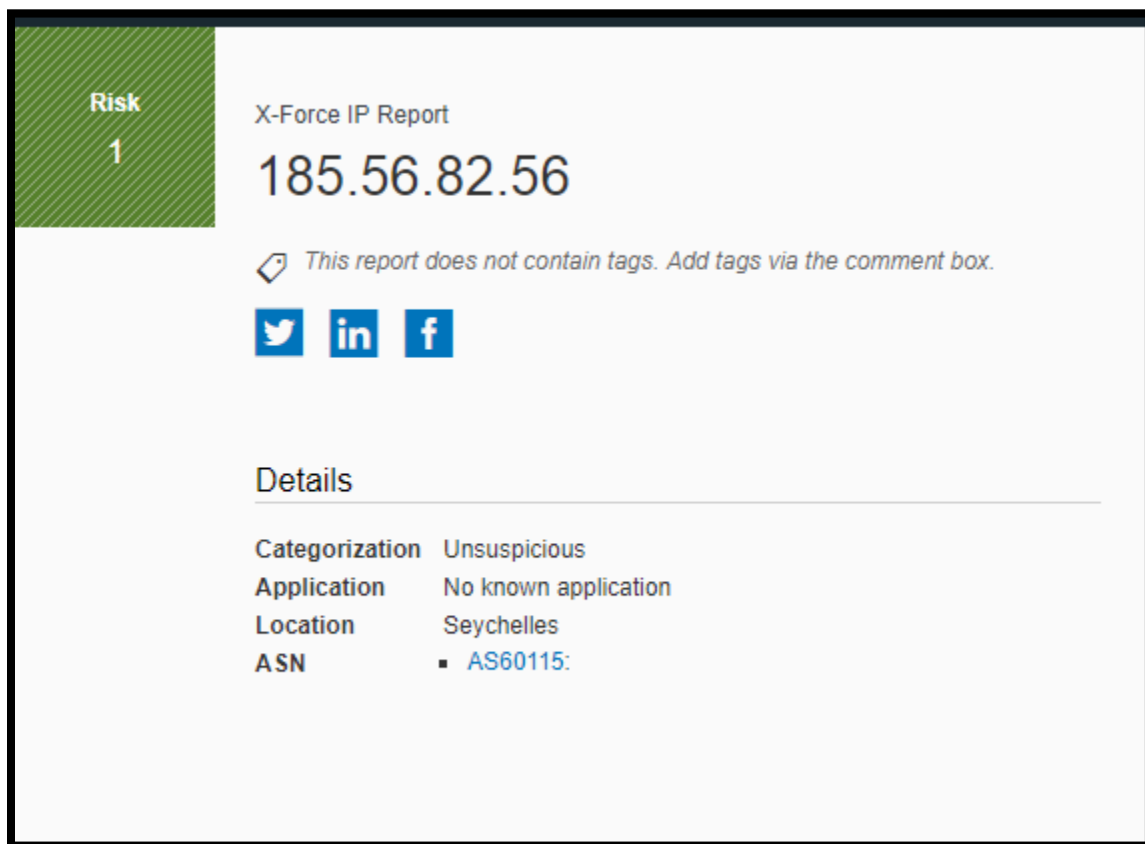
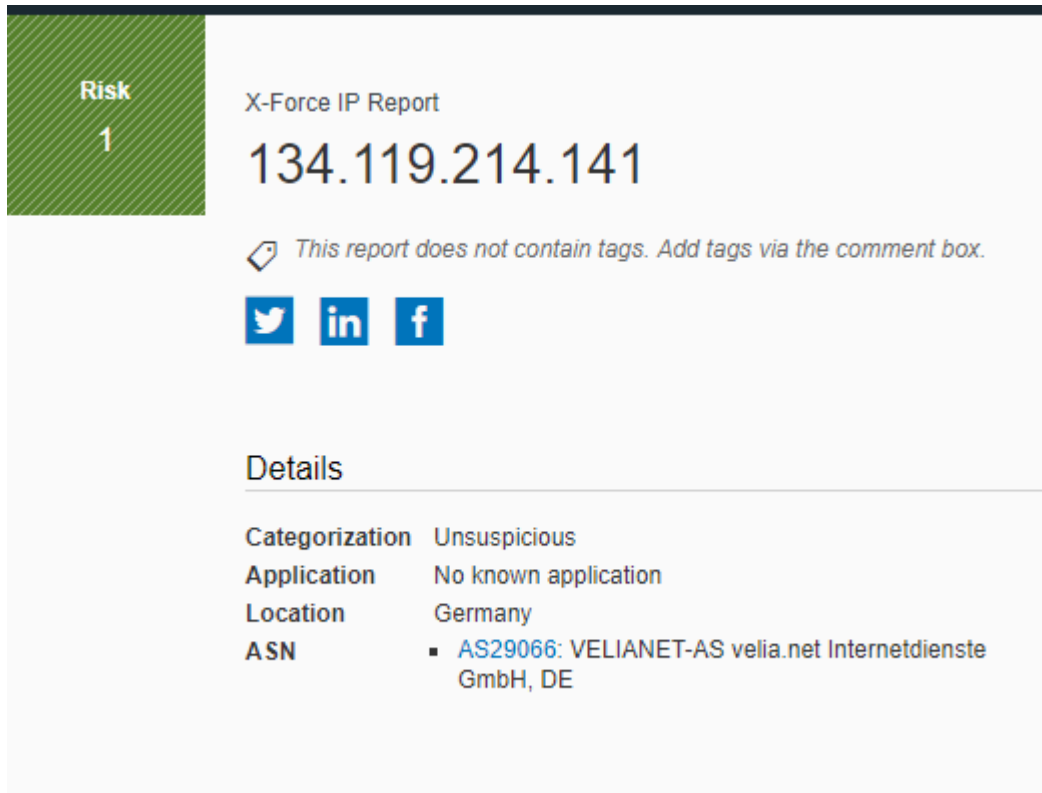


Figure 2.2.4 : Results of IP “185.56.82.56 “

5. Summary for Unknown User Source IP Address: 134.119.214.141

- One record found of this source IP
- This IP has been identified as illegally scanning networks for vulnerabilities.
- Firewall logged this as an alert.
- Host sweep scan was done.
- Screenshot of results from IBM X-Force Exchange shown below(Figure 2.2.5 and 2.2.6)



The screenshot shows the IBM X-Force IP Report interface. On the left, a green box displays 'Risk 1'. The main header reads 'X-Force IP Report' followed by the IP address '134.119.214.141'. Below this, a message states: 'This report does not contain tags. Add tags via the comment box.' There are social media icons for Twitter, LinkedIn, and Facebook. A 'Details' section is expanded, showing the following information:

Categorization	Unsuspicious
Application	No known application
Location	Germany
ASN	AS29066: VELIANET-AS velia.net Internetdienste GmbH, DE

Figure 2.2.5: Showing results of IP “134.119.214.141” on IBM X-Force Exchange

▼ Scanning IPs (71%)	Firewall deny log analysis	Germany	Jan 13, 2018 12:21 PM
AS29066: VELIANET-AS velia.net Internetdienste GmbH, DE			
▼ Scanning IPs (86%)	Firewall deny log analysis	Germany	Jan 12, 2018 12:19 PM
AS29066: VELIANET-AS velia.net Internetdienste GmbH, DE			
▲ Scanning IPs (100%)	Firewall deny log analysis	Germany	Jan 3, 2018 7:37 AM
AS29066: VELIANET-AS velia.net Internetdienste GmbH, DE			

Figure 2.2.6: Showing results of IP “134.119.214.141” on IBM X-Force Exchange

Checking IP Addresses by User:

User 1:

1. Summary for Source IP Address 1: **172.20.10.31**
 - No suspicious activity found using this IP
2. Summary for Source IP Address 2: **172.20.10.24**
 - No suspicious activity found using this IP
3. Summary for Source IP Address 3: **172.20.10.14**
 - No suspicious activity found using this IP

User 2:

1. Summary for Source IP Address 1: **172.20.10.24**
 - No suspicious activity found using this IP
2. Summary for Source IP Address 2: **172.20.10.12**
 - No suspicious activity found using this IP
3. Summary for Source IP Address 3 : **172.20.10.21**
 - No suspicious activity found using this IP

User 3:

1. Summary for Source IP Address 1: **172.20.10.18**
 - No suspicious activity found using this IP
- 2 Summary for Source IP Address 2: **172.20.10.17**
 - No suspicious activity found using this IP
3. Summary for Source IP Address 3: **172.20.10.19**
 - No suspicious activity found using this IP

User 4: No firewall records found for user 4

2.3. Summary and Conclusion of Analysis

The person most likely for leaking sensitive proprietary information from the organisation is User 4.

Evidence supporting the above statement:

- On the 2018/03/27 User 4 search results reveal that he/she hates their job. Moments later He/She visits the “Anonymous official website” (Shown in **Table 2.1.** of Web Proxy logs1 file)
- On the same day User 4 web proxy results also reveal User 4 is having some financial struggles and he is in desperate need to make money.(Shown in **Table 2.1.1.**,entries reflecting gambling and how to make money)
- User 4 does a search on the 2018/03/28 on how to steal company secrets (Shown in **Table 2.1.1**). At this point he could have possibly found something online on how to steal company secrets as his next search reflects him going back onto the official “Anonymous” website. Straight after visiting the “Anonymous” website he then visits a Wikipedia and reads about “The Anarchist Cookbook” (Description of this book can be found in **Table 2.1.1**)
- User 4 then looks up ways to send anonymous emails (shown in **Table 2.1.1**) and straight after he once again searches how to steal company secrets. We can deduce he has already found an idea and is searching for alternative ways to steal secrets or he hasn’t found anything yet and he is still searching for methods to possess and possibly sell company secrets.
- There is a chance that user 4 wants to steal company secrets to Anonymous in order to make some money. This will benefit him in seeing the company suffer as he/she isn’t satisfied with his job as well as earn him some cash.
- He/She visits the JollyRoger website (description mentioned in **Table 2.1.1**) which reveals he has found a site which can help him with his cause.
- On 2018/03/28 at 2:16:24 PM User 4 goes on anonymous mail and possibly sends an anonymous email. On the 2018/03/27 at 14:27 PM User 1 firewall records pick up a spyware which an external IP Address “185.78.64.121” which when searched on IBM X-Force Exchange revealed this a possible Botnet.(Shown in Figure 2.1.4). User 4 could have sent a spam email with a dangerous website.
- While trying to attempt to steal company secrets he/she may have exposed the entire system to vulnerabilities which appear for other users such as viruses, spyware and a Trojan horse. Furthermore, allowing major groups such as Anonymous and Strider to gain access and further sabotage and exploit the company.

3. Assessment of Network Diagram

3.1. Identified Security Issues

- Only one Firewall present in network diagram design: In a topology with a single firewall serving both internal and external users (LAN and WAN), it acts as a shared resource for these two zones. Due to limited computing power, a denial of service attack on the firewall from WAN can disrupt services on the LAN. The existing single main firewall may identify external threats passing through the perimeter firewalls, but its positioning in the network means it will be unable to identify or block viruses, hackers and similar threats moving laterally throughout the network (i.e. East-to-West). This lateral traffic could be data flows between the departmental networks, between your devices and live environments, or across your WAN from other offices.
- Firewall rules and policies: The current rules and policies can be regularly updated to properly handle network traffic. Moreover, since this is a work environment, social media sites, online flash games sites and so on should be blocked by the firewall. Further, regular checking could be done to continuously block and new suspicious websites.
- No DMZ around internal network: Hackers and malicious intruders can attempt as well as succeed to access the organization's externally facing assets rather. Thus, having free rein to attack its in-house data and servers.
- The current use of a single external firewall will suffice for the protection of the network, given that the DMZ has its own internal firewall implemented and as well as the Internal Network.
- Anti-malware agents: Anti-virus programs release signature file updates regularly--sometimes daily, sometimes more often--because new viruses are being identified on a daily basis. Since the anti-viruses weren't being updated by users-this put the entire system at risk.

3.2. Redesign of the Network Diagram

- Add another firewall to the Network diagram: In a topology with two firewalls, you protect internal services on the LAN from denial of service attacks on the perimeter firewall. The Internal Network Firewall (INFW) securely segments the network whilst simultaneously screening for unusual traffic, indications of compromise and other anomalous behaviour.
- Add a DMZ around the internal network: Protecting the internal network with a DMZ will protect your servers from the local intranet and your intranet from your publicly accessible servers. This is done by making each portion of your network sit on different IP networks. There are many different ways to design a network with a DMZ. Two of the most basic methods are with a single firewall, also known as the three legged model, and with dual firewalls. These architectures can be expanded to create very complex architectures depending on the network requirement. The most secure approach is to use two firewalls to create a DMZ. The first firewall (also called the "front-end" firewall) must be configured to allow traffic destined to the DMZ only. The second firewall (also called "back-end" firewall) only allows traffic from the DMZ to the internal network. This setup is considered more secure since two devices would need to be compromised. There is even more protection if the two firewalls are provided by two different vendors, because it makes it less likely that both devices suffer from the same security vulnerabilities.
- Add network agents to the internal network as well as around the servers :
 - This will deliver information about the current software state;
 - sends and receives administrative commands;
 - synchronizes the configuration information;
 - sends the information about events on client hosts to the Server;
 - provides functionality of the update agent.
- Anti-malware agents should be installed onto the user machines and along with a reliable antivirus which does an automatic update of its virus signature database, which was a weakness of the current network.
- Patching and updates : should be done regularly and not be given an option to postpone for too long since there are always new and custom virus signatures that come out so servers and user machines continuously need to be kept up to date with these. Moreover, the versions of software used on the user machine should be updated regularly as older versions sometimes contain unclose bugs which can potentially be used as a vulnerability exploit.



