Project 1: Detecting Cyberattacks in Network Traffic Data

ChienLin Chen

900380

1. Ingesting the PCAP file

Using Wireshark to change the timestamp and converted it to csv file.

2. Methodology of Analyzing Traffic Pattern

2.1. Bonet Command & Control (C2)

There are **54** HTTP based C2 requests to C2 server “finalcortex.com”, and the URI strings **/snapbn/gate.php for POST** was used. The event started at **2020-06-19 00:55:21.316470** to **2020-06-19 00:58:00.085710**.

In order to find the C2 server IP address, “finalcortex.com” and “Protocol=DNS” were typed to find. DNS can translate the domain names to IPv4. From the Info field, we can say DNS IP address is 202.166.80.9 and the Botmaster is 202.166.84.165 because the Botmaster made standard query of “finalcortex.com” and DNS responses 31.192.109.167 for the C2 server IP address. When searching C2 server IP address and “Protocol=HTTP”, it showed that the Botmaster is communicated with the C2 server by identified the Source and Destination IP address. Attacker made 54 POST requests with /snapbn/gate.php path and C2 server response to the attacker “HTTP/1.1 200 OK (text/plain)” 54 times. The start and end time were noted down by “sort Time”.

2.2. SPAM

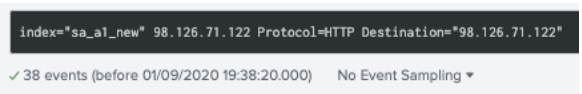
There are **214** email addresses have been targeted by the spam from **2020-06-19 00:55:23.278082** to **2020-06-19 01:01:12.900452.** The first and last recipient are **<nickandsonia@comcast.net>** and **<jberman1@gmail.com>** respectively.

By typing "RCPT | chart count by Info", we can get 214 distinct email addresses. The Protocol is SMTP which is used for electronic mail transmission. The source IP is the Botmaster's and the emails may send by bots. The start and end time were detected by "sort Time".

2.3. Click Fraud

There are **38** Click Fraud requests have been made to website www.generalamuse.com and the URI strings **/gen.php** were used. The event started at **2020-06-19 00:55:22.906077** to **2020-06-19 01:01:08.208700**.

Similar in the 2.1, the same attacker (Botmaster) asked same DNS for the www.generalamuse.com IP address by typing that URL and "Protocol=DNS". By looking at the DNS responses to attacker, the website IP address is 98.126.71.122. The number of requests and URI were found by searching "Protocol=HTTP" and "Destination=98.126.71.122". The attacker or maybe bots send 38 requests to this website and the URI is identified in the get path. The start and end time were detected by "sort Time".



2.4. IRC

There are **31** POST requests made by the infected machine and the IRC servers' IP addresses are showed below in the table:

58.42.247.143	60.173.109.42	61.17.216.4	61.17.216.86
61.17.216.92	61.17.216.94	61.150.114.216	61.167.116.133
61.177.120.254	88.250.200.14	184.106.213.57	200.171.4.222
202.112.126.218	211.157.110.34	217.34.4.225	218.189.208.34

221.207.141.60	

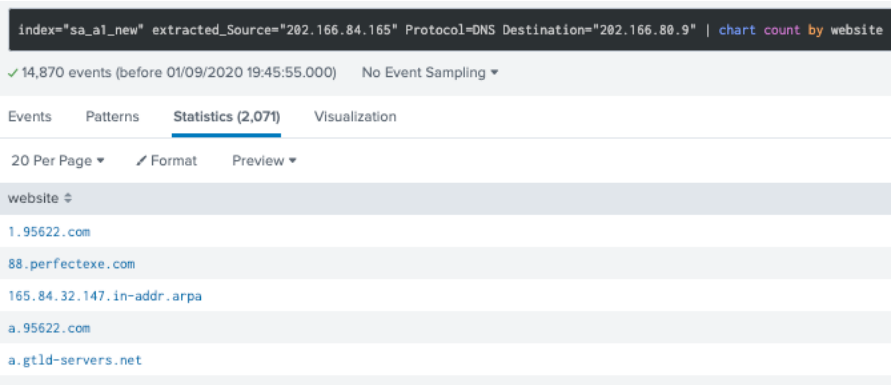
Table 1: IRC servers' IP addresses

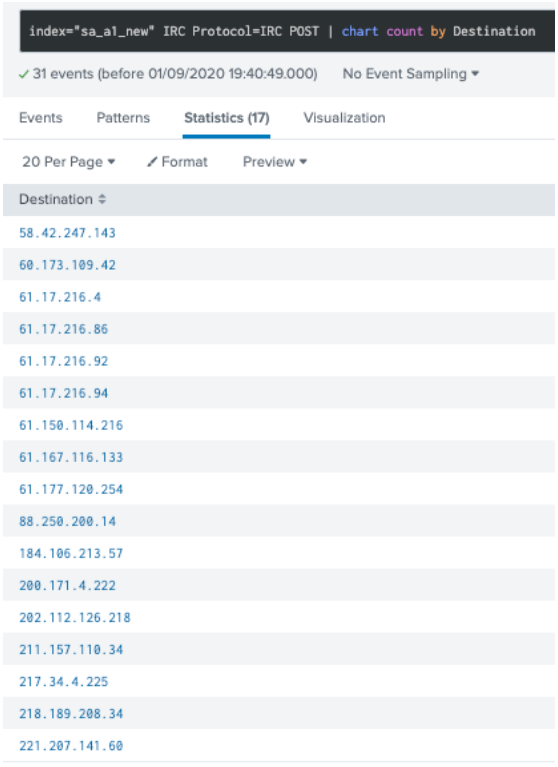
The event started at **2020-06-19 00:55:21.813824** to **2020-06-19 01:01:59.756180.**

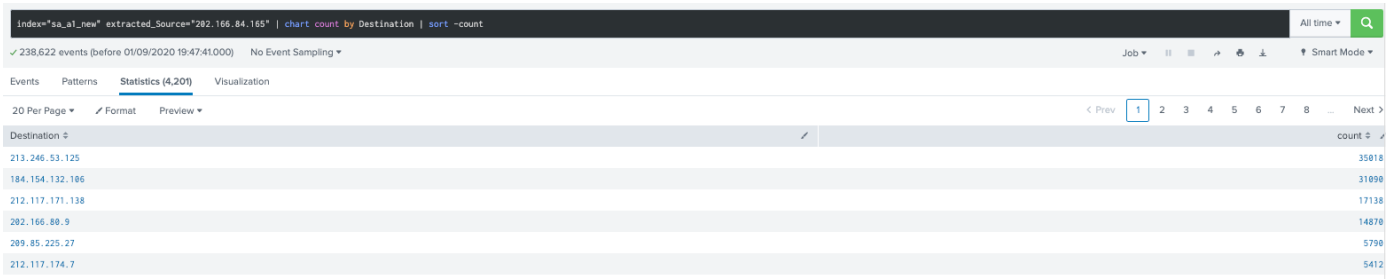
Number 31 was gotten by searching POST and Protocol=IRC. In addition, IRC servers, bots, were identified using Protocol=IRC and extracted_Source="202.166.84.165", which is the Botmaster IP address. All of these servers had gotten botmaster POST requests by further found by typing "chart count by Info". The start and end time were detected by "sort Time".

From the Info field in these POST requests with IRC protocol, it can be noted that it was aimed to start a DDoS attack to "212.117.171.138" with 17,138 events. The website is "sns.webmail.aol.com" by the sitedomain in HTTP GET request for botmaster login detail. All of these events have Botmaster IP address as extracted source. It started at 2020-06-19 00:55:21.822800 to 2020-06-19 01:02:09.482280.

The botnet starts DDoS for 2071 websites. The number is gotten from extracting the website field from the Botmaster's query to DNS. Botmaster start querying from 2020-06-19 00:55:19.399423 to 2020-06-19 01:02:09.684960. The largest number of attacking events was 35, 018 to "fgjikcfd.com" with IP address "213.246.53.125" from 2020-06-19 00:55:27.212684 to 2020-06-19 01:02:09.712928 and the second largest one was 31, 090 to "fgiiawee.com" with IP address "184.154.132.106" from 2020-06-19 00:55:22.262771 to 2020-06-19 01:01:56.692270.







3. Attack Narratives

From these four cases, it can be noticed that the Botnet architecture is centralized with IRC communication protocol. There is a botmaster with IP address “202.166.84.165”, C2 servers and bots. According to these four-start time, botmaster first choose the C2 servers, and then the bots interact with botmaster by running IRC services. From the start and end time of each case, it also matches that the centralized model can fast control the bots. Furthermore, the commands are pushed to bots. From the fourth situation of the source IP is equal to the botmaster’s. It implied that the bots were waiting for commands from botmaster. SPAM, Click fraud and DDoS attack also indicated the source IP are all same as botmaster, this meant bots run similar scripts from the botmaster.

Begin with the recruitment viewpoint of the Botnet Lifecycle, the computers that got infections might be before the botmaster start SPAM and Click fraud attacks. Because from the start time

of first and fourth are pretty close. Next, the interaction step is demonstrated in the first and the fourth cases. The former one was setting up a C2 channel for remote control and the latter one is showing that the infecting machines, bots, were gotten POST requests from the botmaster using IRC protocol for communication. The rest of the processes: Marketing and Attack execution cannot be summarized in these four cases. The attacker might do it for money motivation; nevertheless, it is hard to know other people mind or thinking. The attack executions are SPAM, Click fraud and DDoS judged from these occurrences.

The timeline for these four cases is showed in Figure 1. The end time was assumed to be when the last DDoS attack finished. There are 4,201 IP addresses had contacted with Botmaster. “202.166.80.9” is DNS. Botmaster query to this DNS for 2,071 websites might for C2 servers, Click fraud attack or DDoS attack. Furthermore, it also asked another query to other DNS. Therefore, there might be less than 1,800 bots in this botnet.

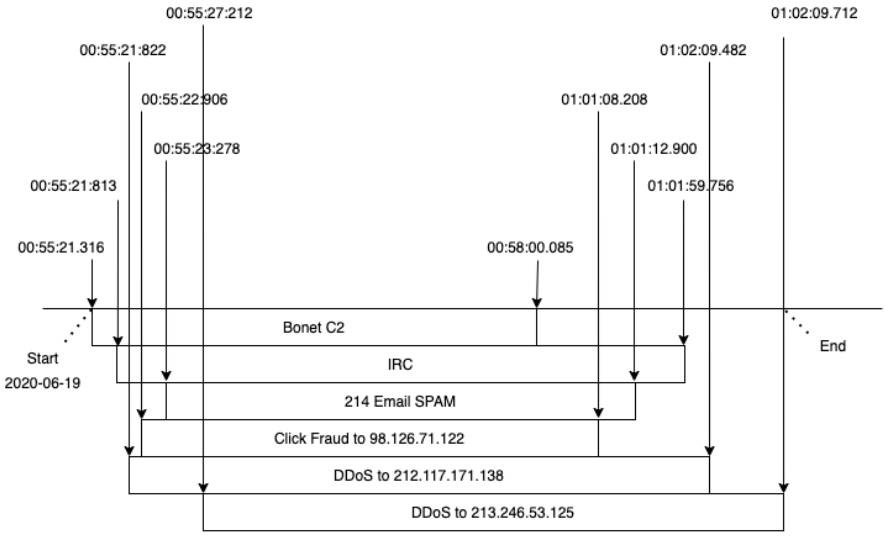


Figure 1: Attack Scenarios Timeline

4. Evaluation of Targeted Network Attacks Consequences

In the Confidentiality aspects in CIA triad in these four scenarios, those recipients of SPAM didn’t get supports from security controls because the data should be accessible only to its intended entities. Their email information was leaking to malicious entities. According to Integrity, the zombie computers controlment and falsify advertisement records by click fraud means lack of integrity provision. The former one didn’t meet this property as there were non-allowed individuals accessing their computer without permission to install malware, a remote access trojan or backdoor. The latter one provides inaccurate information for business decision making. DDoS can affect the availability principle because the information of the attacked servers will be unavailable for other users.

Furthermore, in the financial aspect, the disruption of DDoS can cost an enormous amount of extortion fee for availability of the server and the enterprises are responsible for 80% of SPAM emails (Timothy, Robert, Carl and David, 2006). In addition, these reusable personal sensitive details, emails in this case, can sale to several crime markets to gain money (Timothy, Robert, Carl and David, 2006). Without instant removal of the click fraud bots, a large amount of money for paying per click advertisement has to transfer to these fake entities (Brendan, Jingying, Albert & Ron, 2013).

5. Attack Scenarios Patterns

Given a small range of time, in this case, from 2020-06-19 00:55:19.383465 to 2020-06-19 01:02:09.742832 there are 238, 622 events was sent by 202.166.84.165. Therefore, this IP address is very suspicious. Then, detected of the Destination sent by this source, there was a huge number of events to some IP addresses; therefore, a DDoS attack can be assumed. In order to find out what servers had been attacked; DNS protocol was selected to do the analysis because the domain names need to be translated. To check which are C2 servers or Click fraud attack, selection of HTTP protocol is required. After checking these destinations, it can show that from Botmaster IP addresses was sending same content of GET/POST requests to them. To identify between C2 servers and server under Click fraud attack is by the content of the request. Since there is IRC protocol presented, botnet on IRC service for communication can be expected and find out Botmaster POST requests commands to IRC servers. There are also events using SMPT protocol to several destinations in a short time; therefore, an email SPAM attack was conducted. The summarization is below in table 2.

Source IP Address	Protocol	Port	Destination IP Address	Attack
(Identified by which was sending a large flow in a small period of time)	SMPT	587	Victims	SPAM
	HTTP	80		Click fraud
	TCP	Many		DDoS

Table 2: Attack Scenarios Patterns

6. Countermeasures

To prevent data leaking or controlment of victim computers for the target network, permission, authentication and access control list can protect some confidentiality because only authorized users are able to access the resources and information. The use of checksum and firewall may provide integrity by checking the data was modified or not and reject suspicious IP address (Josh, 2020). Implementing IPS systems and firewall or backing up, replicated data and computers can reduce the harms of DDoS availability (Kim, 2017). Instant detection and fast recovery may not make attack consequence worse.

It is a centralized push-based command and control botnet architecture running on IRC protocol according to the previous statements. Botmaster control bots via C2 channels; hence, the discovering and elimination of C2 severs can let the botnet be ineffective. For the first

attack scenario, it showed the botmaster sent HTTP POST request to C2 server and gate.php is one of sensitive names that are usually interact with suspicious domain (Tyler, 2014, p. 12). In addition, botmaster also query DNS about the C2 server IP address several times. If we can combine these two patterns, we may find out who are C2 servers.

From the attack scenarios, we can predict that the bots may exist an arbitrary time before they were used for attacks. Maryam, Alireza and Sureswaran (2009, p270) suggest using DNS detection to find out where C2 server is located since bots will send DNS query about C2 server in order to start the connection with it. Hence, after we know where the C2 server is, bots address can also be revealed. In our situation, we will have to check back some time ago because only botmaster's IP address is showed contacting DNS in this short time range.

In addition, anomaly detection can be used as a passive networking traffic detection and analyzing for botnet. Timothy, Robert, Carl and David (2006) detect the bandwidth, duration and packet timing to do anomaly detection of botnet after filtering normal traffics. Then they classified and cluster groups of them in correlation and topological information to find common abnormal communication patterns and hubs. We can adopt the patterns from discussion 5 that the data flow will appear similar to the case for one botmaster interact to many bots on IRC protocol. Guofei, Junjie and Wenke (2008) used Botsniffer as network-based anomaly detection of spatial-temporal correlation and similarity to identify C2 server and infected host. The topology information can find out from IP addresses, for example, the botmaster "202.166.84.165" make comparable large DNS query to "202.166.80.9" than other ones.

Botnet using IRC channel have characteristics that a single controller is issuing commands and all the observers see those in a specific time. They recommend detecting botnet by examining on IRC port 6667 for chat sessions and string content (Timothy, Robert, Carl and David, 2006, p196). This situation can be seen on scenarios 4 where the contents of POST request are same, and the source IP address are all from botmaster. Investigating IRC protocol may ease the damage of the botnet.

To detect or block the packets from a suspicious IP source address is a way to mitigate the risk of attacks. Maryam, Alireza and Sureswaran (2009, p270) suggest making use of reactive cyber security solution, an intrusion detection system (IDS) such as Snort to detect signatures of known botnets. What's more, Brendan, Jingying, Albert and Ron (2013) recommend using IP blacklist from public domain provider to prevent SPAM and Click fraud. They also proposed detection of the high frequency of user click, rejecting cookie and particular keyword repeatedly click.

7. Conclusion

Botnet pose a significant influence threats to cyber security. These bots can be used to implement several attacks parallel during a short period of time. The harms of SPAM, Click fraud, DDoS are massive to the target network. In order to prevent the loss of CIA triad in the future, passive networking traffic detection countermeasures for this attack were discussed.

8. Reference

Maryam, F, Alireza, S & Sureswaran, R 2009, A Survey of Botnet and Botnet Detection, IEEE Xplore, p. 268-272.

Tyler Cui, 2014, An Approach to Detect Malware Call-Home Activities, SANS Institute, p. 12-13.

Hossein, Z, Azizah, M 2009, Botnet Command and Control Mechanisms, IEEE Xplore, 2009.151, p. 564-566.

Timothy, S, Robert, W, Carl, L & David, L 2006, Detecting Botnets with Tight Command and Control, IEEE Xplore, p. 195-201.

Guofei, G, Junjie, Z & Wenke, L 2008, BotSniffer: Detecting Command and Control Channels in Network Traffic, Wright State University Computer Science and Engineering Faculty Publication.

Brendan, K, Jingying Z, Albert, R & Ron, M 2013, Click Fraud Detection with Bot Signatures. IEEE Xplore, p. 146-150.

Kim, C 2017, All About the CIA Triad, viewed 1th September 2020, < https://blogs.blackberry.com/en/2017/11/all-about-the-cia-triad>

Josh, F, 2020, The CIA triad: Definition, components and examples, viewed 1th September 2020, < https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>