Real-Time Honeypot Forensic Investigation on a German Organized Crime Network

GIAC (GCIA) Gold Certification

Author: Karim Lalji (GSE #246), karimlalji1@gmail.com
Advisor: Dr. Johannes Ullrich

Accepted: May 18, 2020

Abstract

German police raided a military-grade NATO bunker in the fall of 2019, believed to have been associated with a dark web hosting operation supporting a variety of cybercrimes. The organized crime group has gone by the aliases of CyberBunker, ZYZtm, and Calibour (Dannewitz, 2019). While most of the group's assets were seized during the initial raid, the IP address space remained and was later sold to Legaco Networks. Before being shut down, Legaco Networks temporarily redirected the traffic to the SANS Internet Storm Center honeypots for examination. The intention behind this examination was to identify malicious traffic patterns or evidence of illegal activity to assist the information security community in understanding the techniques of a known adversary. Analysis of the network traffic revealed substantial residual botnet activity, phishing sites, ad networks, pornography, and evidence of potential Denial of Service (DoS) attacks. The investigation uncovered a possible instance of Gaudox Malware, IRC botnets, and a wide variety of reconnaissance activities related to Mirai variant IoT exploits. A survey of the network activity has been provided with an emphasis on potential botnet activity and Command and Control (C&C) communication.
1. Introduction

In September 2019, German police arrested several individuals in connection with a dark web hosting operation which resided in a military-grade facility located inside a cold-war era NATO bunker in Traben-Trarbach, approximately 100 miles outside Frankfurt, Germany. The adversary group is commonly referred to as CyberBunker, ZYZtm, and Calibour (Dannewitz, 2019). The raid of the 13,000 square meter property was undertaken by 650 armed police officers, including GSG9 (an elite tactical unit within the German Federal Police) on foot and in helicopters.

According to a press release by the State Central Cybercrime Attorney General Office, over 2 petabytes of data were seized including servers, mobile phones, hard drives, laptops, external storage, documents and cash. One of the sites, C3B3ROB, seized by the state criminal police listed over 6000 darknet sites linked to fraudulent bitcoin lotteries, narcotics marketplaces (with millions of Euros in net transactions), weapons, counterfeit money, stolen credit cards, murder orders, and child sexual abuse images (Attorney General Koblenz, 2020). The organization has also been suspected of chemical warfare and providing electronic control systems for weapons (Dannewitz, 2019). Several of the individuals connected to CyberBunker are currently undergoing criminal trials in Germany. To help pay for legal expenses, the individuals behind CyberBunker sold the IP address space to Legaco Networks B.V. Due to a long-standing relationship between the SANS Internet Storm Center and individuals at Legaco Networks, the traffic from this malicious address space was temporarily redirected to the SANS honeypots for analysis.

This traffic redirection aims to study the behavior of the adversary group to determine what types of attack traffic are still visible on these networks. Since the raid of the bunker was approximately six months before the time of this writing, there is a strong possibility that components of the malicious traffic have reduced or stopped. However, signs of data exfiltration from previously compromised hosts, signatures for known botnets, as well as phishing sites and malicious ad hosts still remain.

In addition to examining current trends, studying the network traffic from a known adversary group helps the information community understand the methods used
for exploitation, covert communication, and data exfiltration to protect networks against future attacks.

2. Traffic Overview

The traffic redirection began on April 15, 2020, and included the following three subnets: 185.103.72.0/22, 185.35.136.0/22, 91.209.12.0/24. The initial capture rate was slightly sporadic, presumably due to the traffic redirection from Legaco Networks taking a short time to finalize. By April 16, 2020, the honeypot was seeing a steady stream of traffic.

The data analysis windows were between April 16-20, 2020, April 26, 2020, and April 28, 2020, resulting in 7 days’ worth of traffic. Due to the very high volume of data on these networks, and considering over 2000 IPs were in scope for the analysis, a sampling approach had to be taken. The traffic analyzed consisted of a randomized 4-hour chunk of data from each of the seven days except for April 16 and April 17, which had samples of 11 hours and 6 hours, respectively.

I/O statistics were extracted for each full-hour duration of available data, to identify notable deviations, by obtaining both the number of frames and the number of bytes from the PCAPs. The following graph depicts the I/O statistics from the sample data analyzed with the Y-Axis representing frames and bytes, and the X-Axis representing each 1-hour (3600 seconds) period on the particular day.

![Traffic I/O Statistics](image-url)

Figure 1 (Traffic I/O Statistics)

Karim Lalji
As shown in Figure 1, while there are some spikes in traffic, the fluctuations aren't very drastic. The numeric values in the graphic above are scaled to illustrate patterns. The raw data was extracted using TShark from the collected PCAPs at hourly intervals. The byte values above are divided by 1 million (producing Megabytes), and the frames are divided by 10,000 for a clear visual ratio relative to the number of bytes. The average data transfer rate for the sample set was 1.89 Mbps (Megabits/sec) and 0.29 FPS (Frames/sec).

High-level IP statistics show that a subset of hosts account for a large portion of the total traffic. The top-25 IPs based on the number of bytes, as well as the top-25 TCP ports based on the number of connections are listed in Appendix A and Appendix B. These IP and port statistics have been provided from the perspective of the subnets which are presumed to belong to CyberBunker. In other words, incoming traffic refers to data bytes being sent to the CyberBunker subnets, potentially as a result of residual C&C traffic, whereas outgoing traffic refers to data bytes sent out from those subnets.

Not surprisingly, Port 80 (HTTP) and Port 443 (HTTPS) were the top TCP ports in the sampled connection data. However, the sections to follow will showcase that not all of this communication can be attributed to classic web traffic, but rather, botnet check-ins and other potentially malicious activities that contribute to the disproportionate size.

In addition to obtaining the top IP addresses based on the number of incoming and outgoing bytes, geolocation data was also extracted from the top-25 IP addresses to get a general understanding of where in the world traffic is flowing and by what density. The following image (Figure 2) represents a heatmap from the top-25 largest IP connections, based on byte count, either receiving data from the CyberBunker subnets (left) or sending data to the CyberBunker subnets (right). This high-level heatmap illustrates traffic patterns from the data set where the CyberBunker networks are listed as either the source or destination IPs; additional context, however, should be obtained before drawing conclusions about malicious activity. Many of these connections likely do not result from traditionally initiated requests by client IPs, but rather are the result of previous compromises, automated check-ins and command and control traffic.

Karim Lalji
An interesting observation in both scenarios is that South America, specifically Brazil, accounts for the highest data density in both directions. Based on this heatmap, North American locations such as the United States and Canada appear to have a more notable footprint as source hosts in the sample set with the CyberBunker subnets as destinations. This geographic pattern could be attributed to either content hosted by the CyberBunker group being accessed in larger volumes by Western countries (for example due to previous phishing campaigns or hosted content) or due to more widespread exploitation of hosts resulting in frequent botnet check-ins and C&C traffic.

3. Malicious Traffic Samples

The SANS honeypot contained a network sniffer, Apache web server instances on both TCP ports 80 and 443, a VSFTPD server, and an IPTables firewall. The IPTables rules on the honeypot also redirected port 80 and 443 traffic to ports 30080 and 30443, respectively. The analysis data consisted of PCAP files, Apache web server logs, VSFTPD logs, and IPTables logs. Legaco Networks permitted SANS to examine and report on all the traffic aside from email-based communication – no server on the honeypot listened on TCP port 25.

The general observation from the sample traffic points to a large amount of botnet communication. Some of the behavioral indicators suggest well-known malware/botnets, while others are not as clear. A cautionary note to consider is that the traffic examined

Karim Lalji
contains only a portion of the big picture, such as a compromised bot's check-in with a C&C server as an HTTP request. In most cases, the initial exploit or foothold attempt, which is often necessary for a full analysis, isn't visible in the sample. Analyzing these requests provides strong indications about network activity, but does not necessarily yield conclusive results. Additionally, the adversary group's arrests took place six months before this analysis, increasing the likelihood of a reduction in active illegal traffic in the period leading up to this examination.

Large amounts of "background noise" expected on most networks were filtered out to assist in focusing the analysis activities. Events explicitly filtered out from further analysis included port scanning, web directory brute forcing (e.g., DirBuster), SQL injection discovery, DNS zone transfer attempts, VoIP scans (primarily with SIPVicious), Telnet, SSH, FTP, and web-form brute force login attempts. Several of these events can be attributed to internet-wide scans that are not specific to the IP address space under examination.

The primary goal of this exercise was to identify any residual evidence of compromised hosts or botnet activity by attempting to discover devices that may be "calling home" to a C&C server instead of reconnaissance activities likely to be a result of automation or script kiddies.

3.1. IRC over Port 80 - Potential C2 Communication

The honeypot redirected all port 80 and port 443 traffic to an installed Apache instance for log collection. A cursory look at the Apache access logs for port 80 traffic resulted in immediately visible anomalous behavior. Several entries in the Apache log files contain requests from internet-bound hosts with IRC traffic logged as HTTP by Apache. An example of one of these requests is shown below:

187.208.118.97 - [26/Apr/2020:06:37:44 +0000] "USER DESKTOPF30TQO7_601B909E_PEDRO 571347 878568 33657\n" 400 0 "-" "-"

Over 4 million requests, similar to the one noted above are contained in the Apache access logs within the time analysis window. Based on the initial view, it appears

Karim Lalji
as though hosts are looking for an IRC server over HTTP on port 80 destined primarily for the 185.35.136.0/22 subnet.

These requests are easily identifiable with the word "USER" in place of the HTTP request method in the Apache logs. The parameters following contain random numeric sequences preceded by a string that appears to be a computer name. The hosts listed in Table 1 below show the distribution of a subset of requests from Zeek's http.log formatted with either "USER", "NICK" or "JOIN" as the HTTP request method.

<table>
<thead>
<tr>
<th>Count</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>248813</td>
<td>185.35.137.80</td>
</tr>
<tr>
<td>63274</td>
<td>185.35.137.72</td>
</tr>
<tr>
<td>50702</td>
<td>185.35.139.241</td>
</tr>
<tr>
<td>11743</td>
<td>185.35.139.240</td>
</tr>
<tr>
<td>1998</td>
<td>185.35.137.71</td>
</tr>
<tr>
<td>1</td>
<td>91.209.12.22</td>
</tr>
<tr>
<td>1</td>
<td>185.35.139.221</td>
</tr>
</tbody>
</table>

Table 1 (IRC on Port 80 Destination IPs)

The Apache logs only provide a source IP, resulting in Zeek logs being leveraged to provide insight into the destination IPs. Each of the destination IP addresses listed is within the scope of the subnets belonging to the CyberBunker group. Assembling one of these TCP streams in Wireshark reveals the following format:

![Figure 3 (IRC TCP Tream)](image)
The destination server responds with a 400 Bad Request error code, which is expected since the request is not valid HTTP. However, the NICK and JOIN commands in the second HTTP request within this TCP stream indicates that the traffic is very likely attempting to leverage the IRC protocol.

Close to 2000 unique computer names and over 7000 unique source IPs that follow a similar request pattern are present in the traffic sample collected. Figure 4 below represents a short snapshot of Zeek’s http.log file showcasing the frequency and random nature of the traffic.

Another pattern observed which indicates that this traffic is unlikely to be human-generated, relates to the time interval between requests. The time intervals are clearly shown in the following Excel output (Figure 5), with a single traffic pattern isolated for clarity. The IP listed is presumed to be a "victim" (at this point under the current assumptions) connecting outbound to the attacker or C&C server.

Karim Lalji
Figure 5 (Isolated IRC Traffic Pattern)

As shown, the time between requests is exactly 1min and 30sec, aside from a couple of deviations, assumed to be attributed to network latency or TCP retransmissions. This type of traffic pattern is generally too precise to be human-generated. Based on the behavior of this traffic, it is highly likely to be a result of an IRC botnet, which has traditionally been a popular technique used by adversaries. The assumption is that these "bots" are configured to use an inconspicuous port such as HTTP for C&C communication, which was logged by Apache after the redirection by Legaco Networks began routing this traffic toward the honeypot where a web server resided on port 80.

The analysis thus far shows that the portion following the computer name could be C&C traffic. The numeric bytes were decoded in various formats, including decimal, ASCII, Byte-Wise XOR, UTF, and Hex in English, German, Dutch and Latin languages in an attempt to find patterns in the output that could be attributed to malicious use. These attempts did not yield any meaningful results.

3.2. Encrypted Inbound HTTP – Potential Gaudox Botnet

Filtering the traffic by the largest TCP connections based on the number of bytes pointed to several thousand HTTP POST requests made to a PHP application. While this would often not be considered unusual, there are a few unique factors that warranted further investigation. These include: data sent to the PHP application with an HTTP
POST at consistent intervals, HTTP POST data appearing to be binary rather than text-based, and most interestingly, the binary data exhibiting behavior consistent with encryption. The general pattern observed is somewhat typical for well-known botnets.

During the initial analysis, a 4-hour window of PCAP data was carved from the honeypot on April 16, 2020 as a sample. Running SiLK’s rwfilter and rwstat commands to determine the largest TCP connections, based on the number of bytes, revealed the following connections:

![Figure 6 (Largest TCP Connections by Byte Count)](image)

The initial analysis showcased several internet-bound hosts making large outbound connections to two of the CyberBunker IP addresses over port 80. The top TCP connection from the SiLK data shown above, containing the most significant number of bytes, was then carved out and isolated from the primary PCAP data. The carved PCAP data revealed several HTTP POST requests to an endpoint called /smelly/order.php.

![Figure 7 (Wireshark Capture of the Largest TCP Connection)](image)

Karim Lalji
The timestamps in Figure 7 above (normalized to UTC) indicate outbound requests every 00:05:05 (5min and 5sec), aside from an odd deviation, likely due to network latency or congestion. This consistent time interval led to an assumption of automated traffic. Following the first TCP stream from the Figure 7 Wireshark capture above showcases an HTTP POST request which is not text-based:

![TCP Stream Image]

**Figure 8 (HTTP Post TCP Stream)**

There is a strong possibility that the data is encrypted based on an entropy analysis of the resulting contents. The following image showcases a high likelihood of encrypted data with an entropy of 7.99 based on the Shannon scale.

![Entropy Image]

Karim Lalji
Additionally, the image to the left shows a histogram bar chart based on byte frequency. The highly sporadic byte distribution also points to a likelihood of encryption.

The Apache web server logs from the full sample contained 39,439 requests for "/smelly/order.php" – of those, 33,725 were destined for 185.35.138.142, and 5,714 were destined for 185.35.138.142, both of which are contained within the address space belonging to CyberBunker. Additionally, all 39,439 requests had an identical User-Agent of “Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0” despite the requests being generated by 33 different source IPs - this is highly unlikely under normal circumstances.

At the time of this writing, neither of the destination IPs listed above resolve to valid hostnames. However, the following passive DNS records show recently associated hostnames. Passive DNS records dating back to 2017 and 2016 were recorded but removed from this output.

<table>
<thead>
<tr>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-03-07 20:16:35</td>
<td>2020-05-11 9:01:07</td>
<td>188</td>
<td>haveno.name</td>
</tr>
</tbody>
</table>

Table 2 (Passive DNS Records)

Data Source: https://my.farsightsecurity.com/user/jullrich@sans.edu/

These passive DNS records show that two hosts were active until very recently, and potentially continue to be active. Both of the hosts last seen in May of 2020 resolve to 185.35.138.175.

Karim Lalji
Initial review of this traffic pointed to signs that were consistent with Beta Bot, a popular and freely available botnet used for Crypto mining, DDoS, and various other malicious purposes. It often said to spread through malicious Microsoft Office documents as the vector in which the User-Mode (Ring 3) rootkit is injected (Faouzi, 2015). The traffic initially appeared to be consistent with Beta Bot due to the C&C check-in following the pattern of “some_path/order.php”.

Additionally, Beta Bot version 1.7 has several variants, including Neurevt, which leverages encrypted HTTP payloads using XOR and RC4. The key to decrypting the payload is contained within the configuration portion of the original malicious executable (Heppner, "Sophos - Betabot Configuration Data Extraction"), which is inaccessible in the network traffic examined.

However, web-based botnet check-ins often utilize consistent idioms, with a default endpoint of order.php being a common pattern. As an extra layer of examination, the binary bytes posted to the order.php endpoint in the carved PCAP file were exported to disk. Binary comparison of five randomly chosen files showcases that the first several bytes of each file are identical, indicating some type of configuration header or reference data.

As shown in Figure 8 below, the portion of the file where bytes begin to differ starts at 0x0000820, in all cases. Attempts to retrieve common patterns with simple transformations such as XOR brute-forcing were attempted unsuccessfully; however, if methods similar to BetaBot (RC4 and XOR) are used then there is likely an asymmetric encryption key packed into the original Windows executable used to infect the host. Without this key, obtaining further information from only the web payload would be challenging.

Karim Lalji
The smaller carved PCAP representing a single conversation was run through Snort IDS with the Emerging Threats ruleset added to snort.conf resulting in the following output:

```
138 [1:2018359:1] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 2
```

While a single triggered IDS rule isn’t sufficient in drawing a conclusion about the traffic, some of the indicators present a high likelihood of being related to the Guadox Trojan, as highlighted in the contents of the triggered Snort Emerging Threats signature rule below:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN W32/Gaudox Checkin"; flow:to_server,established; content:"o.php"); fast_pattern:25,20; http_header; content:"User-Agent|Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0|Accept; Referer|Content-Type|application/x-www-form-urlencoded|Accept""); http_header; content:""Accept"; http_header; content:""Referer"; http_header; pcre:"/\x7e\n/Ps"; pcre:"/\.$U"; metadata: former_category MALWARE; reference:md5,5d662258fd506b87dc5d3f8f6c2f784; classtype:trojan-activity; sid:2022505; rev:3; metadata:created_at 2016_02_11, updated_at 2019_10_23;)
```

The Gaudox signature content above showcases a few consistencies with the traffic sample, including the User-Agent used to issue requests, the default check-in endpoint of order.php (the Snort rule only looks for a PHP extension since the actual

Karim Lalji
filename can be customized), and the HTTP Content-Type of application/x-www.form-urlencoded.

Gaudox is a Win32 User-Mode (Ring 3) rootkit used for botnets and has many behavioral characteristics consistent with the popular Beta Bot. While the behavior seen in these captures is highly consistent with Gaudox, the network traffic only contains the botnet’s C&C check-in component with an encrypted web payload that follows a very similar pattern to the indicators of Gaudox. Extracting the original exploit executable for further analysis or obtaining additional Indicators of Compromise (IOC’s) from the captured traffic was not possible. This would require the initial exploit attempt to be captured.

Figure 10 below shows a public Gaudox malware detonation using app.any.run – the permalink to this analysis is: https://app.any.run/tasks/fd92ee80-bc1b-4fb9-bdfa-6b16437c6b93/ - Screenshots are provided under the assumption that these sandbox analyses will expire at some point and will no longer be accessible.

![Gaudox Malware Detonation](https://app.any.run/tasks/fd92ee80-bc1b-4fb9-bdfa-6b16437c6b93/)

Figure 10 (Gaudox Malware Detonation)

Note the exploitation path taking advantage of explorer.exe, sys32.exe, and dllhost.exe. It’s also apparent that regular check-ins for order.php are taking place.

Karim Lalji
Further analysis by the sandbox service shows the binary web content as a GNU Privacy Guard keyring, adding to the initial assumptions about encrypted data sent over HTTP.

The TrID tool used by the sandbox service, as shown in Figure 11, was run against several of the order.php files obtained from the network capture; however, the file type could not be identified likely due to a modified configuration. The HTTP request shown above has a very similar style and appearance to the analyzed data shown from the CyberBunker PCAP, despite being completely independent.

The following images were taken from a hacker blog and showcase some of the detailed configuration settings for the Guadox Bot ("[Update]Gaudox - HTTP Bot (1.1.0.1): C++/ASM: Ring3 Rootkit: Watchdog: Antis: Stable", 2016).

The following images show selected screenshots from the Gaudox configuration, each consistent with the behavior observed in the captured traffic. This includes a default knock interval of 5 minutes, HTTP check-in paths with the default endpoint of "order.php", and anti-analysis settings. The author of the blog also describes the encrypted nature of the outbound HTTP check-in to subvert Man-in-the-Middle (MiTM) forensic measures.

Karim Lalji
Screenshots from the blog have been provided under the assumption that the post will be taken down at some point.

### 3.3. Encrypted HTTP – Unknown Base64 Data

Other instances of HTTP communication also raised some suspicion. The following Wireshark capture summary shows a single carved out communication between two hosts on April 16, 2020. The source IP appears to be initiating an outbound HTTP POST request every 2 minutes for approximately 4 hours and 30 minutes with the destination network in the CyberBunker scope.

The image to the left shows the default Knock Interval for Gaudox set to 5 minutes which is highly consistent with the observed behavior of 5 minutes and 5 seconds in the traffic captures.

The image to the left shows the “Path” setting containing a default “order.php” endpoint and a port of 80, both of which are consistent with the captured traffic.

The options shown here are presumed to be more relevant to the initial exploit executable. However, they showcase the functionality built into Gaudox, such as encryption and anti-analysis, in an attempt to thwart discovery.

Karim Lalji
Following the first TCP stream from Figure 12 above shows the data being submitted to the destination server as a collection of Base-64 encoded strings.

These encoded strings do not simply decode into ASCII text despite several attempts to leverage various character encodings, languages, and compression schemes. CyberChef indicated potential Chinese characters when attempting to identify possible languages, which, when decoded, constructed valid words, but produced a linguistic composition that was not comprehensible.

Table: Decode_text('UTF-16BE (128)')

<table>
<thead>
<tr>
<th>Chinese</th>
<th>Japanese</th>
<th>Valid UTF8</th>
<th>Entropy: 5.08</th>
</tr>
</thead>
<tbody>
<tr>
<td>危険なバッグウイルス侵害、暗号化された各種セキュリティの問題</td>
<td>危険なバッグウイルス侵害、暗号化された各種セキュリティの問題</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Karim Lalji
The assumption is that the data is either encrypted or encoded in an unknown format. However, due to the consistent time intervals and HTTP POST data not following conventional mechanisms (submission of parameters in a web form), it is reasonable to infer some type of C2 communication is present.

### 3.4. Phishing and Ad Sites

As might be expected, various phishing sites, ad sites, and URLs that appeared to be malicious (simply by appearance) were logged on the network. The current scope did not involve in-depth analysis into the different phishing attacks with success or failure rates, but rather to obtain additional high-level data on the types of web traffic observed.

Appendix C provides some high-level metrics on the top 50 domains from both web server logs and captured DNS queries. While some of these domains are considered normal, others have a highly suspicious appearance. The web server logs were obtained from Apache and the DNS queries were obtained from Zeek’s dns.log files.

Several sites in the Apache access logs appear to be related to bank phishing such as 266 hits for bank66[dot]com and 4 hits for r0yalbankrbc[dot]com (presumably used as a decoy for RBC Royal Bank). DNS queries in dns.log from Zeek show queries for 525,102 unique domains that contain the word “PayPal”. There are 960,893 unique domains in total within the analysis period resulting in almost 55% of all the unique DNS queries being related to hosts containing the term “PayPal”. Very few of these domains appear to be legitimately affiliated with PayPal and are instead assumed to be used for the intention of phishing, for example, [random subdomain].paypall-password[dot]com.

Another phishing site to note included several requests for the domain appleserviceauthentication.com.juetagsdeas.org. This domain continues to receive active hits at the time of this writing. DIG queries on both the Fully Qualified Domain Name (FQDN) and the host name returns an NXDOMAIN response. However, urlscan.io revealed the associated IP address of 185.35.138.158, which is within the CyberBunker subnets, in addition to identifying 54 other domains associated to the same IP address that appear to be phishing related. Urlscan.io also contains cached screenshots of previous sites hosted by this IP. Although a screen capture was not available for the domain name

Karim Lalji
seen in the honeypots log files, screenshots for several other domains hosted by the same IP address are available. Figure 19 shows a cached screenshot for the domain name `psrepair.3utilities.com` hosted by the same IP.

![Figure 19](https://urlscan.io/result/477546d6-659c-4395-bb50-901a5e0d4c0b/compare)

**Figure 19** (Phishing Landing Page - Chase Bank)

Image Source: https://urlscan.io/result/477546d6-659c-4395-bb50-901a5e0d4c0b/compare

Figure 19 shows a suspected phishing landing page (presumably for credential harvesting) for Chase Bank. Urlscan.io also provided a score of 100 and has flagged the domain as phishing. Figure 20 below also shows a phishing example for Apple ID:

![Figure 20](https://urlscan.io/result/2ea1908c-c30f-4b42-85bc-c28cda30413f)

**Figure 16** (Phishing Landing Page - Apple ID)

Image source: https://urlscan.io/result/2ea1908c-c30f-4b42-85bc-c28cda30413f

Karim Lalji
While the destination landing page appears to be Apple, the following IP/ASN path shows that the initial host resides in the suspect network. A valid hypothesis could include a credential harvesting webpage which then redirects to the “real” Apple ID login. This path shows the initial redirection (depicted with the orange arrow) taking place from the malicious IP identified by the AS of ZYZTM:

```
Figure 17 (URL Redirection Path for Apple ID Landing Page)
```

Image Source: https://urlscan.io/result/2ea1908c-c30f-4b42-85bf-c28da30413f

The following output showcases the various source IP addresses that accessed the destination web host (apple-serviceauthentication.com.juetagsdeas.org) noted in the log files. The country and ISP data has also been included (based on WHOIS databases). User-Agent strings showcase that only a small percentage of these requests actually originate from Apple devices.

```
Figure 18 (Access Logs for Apple Landing Page)
```

Karim Lalji
There are also a large number of pornographic site hits, which is expected and considered a normal part of internet traffic. However, a cursory examination was also undertaken to identify adult websites of a more inappropriate or illicit in nature (for instance, related to minors or animals), by referencing a few known domain blacklists. While the number of hits in these categories were minimal, there were a few occurrences of pornographic hostnames in the DNS logs that appeared to involve animals. A client IP address of 177.200 (located in Brazil) attempted DNS resolution of dog-porn-vids.us at 185.35.138.159 over UDP:53 at 1587104620.335057 (Friday, April 17, 2020 6:23:40.335 AM GMT). The site was not directly accessed due to the assumed content. Running the queried hostname through urlscan.io identified multiple redirects with a final destination host of: http://cpxtri[dot]com/

Figure 19 (Illicit Website Redirection Path)

Image Source: https://urlscan.io/result/601860da-3497-4c3c-abb8-b4f66f7d2151

The live screenshot feature indicated that the content of this website is indeed what the hostname suggests. Additional references to the site have not been provided due to the disturbing content.

These website checks should not be considered exhaustive or complete as the domain lists used to identify illicit hosts are freely available on the internet and may not contain a fully comprehensive set of websites.

As an additional point of reference, the following hosts were seen in the web server and DNS logs which had domain names directly related to the adversary group under the known identities, which are “CyberBunker”, “ZYZtm” and “Calibour”.

Karim Lalji
The following entries appeared in the Apache web server logs in order, according to the number of occurrences:

1. cyberbunker.com (5065)
2. zyztm.com (328)
3. www.zyztm.com (233)
4. cyberbunker.com:30080 (6)
5. cyberbunker.com:30443 (4)
6. cyberbunker.com:80 (3)
7. asimov.zyztm.com (2)
8. zyztm.softether.net (1)
9. ZYZTM.COM (1)

The following entries appeared as DNS queries within the Zeek logs in order, according to the number of occurrences:

1. mail.calibour.com (114069)
2. voip.calibour.com (38960)
3. calibour.com (35239)
4. _sips._tcp.voip.calibour.com (14727)
5. vpn.calibour.com (449)
6. pass.calibour.com (246)
7. everest.calibour.com (219)
8. auth.calibour.com (197)
9. sip.calibour.com (193)
10. gitlab.calibour.com (188)
11. monitor.calibour.com (162)
12. jabber.calibour.com (150)
13. planning.calibour.com (149)
14. rundeck.calibour.com (147)
15. release.calibour.com (146)
16. chat.calibour.com (143)
17. _sip._udp.calibour.com (141)
18. unused.calibour.com (136)
19. chef.calibour.com (134)
20. autoconfig.calibour.com (130)
21. registry.gitlab.calibour.com (123)
22. _dmarc.calibour.com (83)
23. _matrix._tcp.voip.calibour.com (79)
24. _udp.calibour.com (56)
25. _matrix._tcp.sip.calibour.com (40)
26. _matrix._tcp.vpn.calibour.com (39)
27. www.calibour.com (26)
28. default._bimi.calibour.com (20)
29. _tcp.mail.calibour.com (18)
30. _25._tcp.mail.calibour.com (18)
31. boy.calibour.com (12)
32. _587._tcp.mail.calibour.com (12)
33. _465._tcp.mail.calibour.com (12)
34. studentn3.calibour.com (7)
35. silencer.calibour.com (6)
36. cust1.frontend.ha.calibour.com (4)
37. nlf-018.calibour.com (3)
38. chef.cloud.calibour.com (2)
39. abuse.calibour.com (2)
40. _sip._udp.voip.calibour.com (1)
41. _sip._udp.sip.calibour.com (1)

Karim Lalji
There were also a large number of requests for a specific ad hosting site in the web server logs, which consisted of getmyads.com (17753), www.getmyads.com (9846), and traffic.getmyads.com (3649).

Some of these ad requests appear to contain other URL’s within the HTTP request’s query parameter, and are potentially tied to phishing campaigns. A small excerpt of the Apache access.log is provided to showcase the format and frequency (based on timestamps) of these requests:

```
172.69.70.108 www.getmyads.com - - [16/Apr/2020:09:26:41 +0000] "GET //?q=www.sewing-world.ru HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.206 www.getmyads.com - - [16/Apr/2020:09:26:42 +0000] "GET //?q=www.sex-tjejer.com HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.141 www.getmyads.com - - [16/Apr/2020:09:26:44 +0000] "GET //?q=www.sexhotxxx.com HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.164 www.getmyads.com - - [16/Apr/2020:09:26:46 +0000] "GET //?q=www.sextoyclub.com HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.150 www.getmyads.com - - [16/Apr/2020:09:26:50 +0000] "GET //?q=www.sexykontakty.cz HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.168 www.getmyads.com - - [16/Apr/2020:09:26:48 +0000] "GET //?q=www.sexytales.org HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.154 www.getmyads.com - - [16/Apr/2020:09:26:51 +0000] "GET //?q=www.sfanytime.com HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"

172.69.174 www.getmyads.com - - [16/Apr/2020:09:26:52 +0000] "GET //?q=www.naij.com HTTP/1.1" 200 643 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"
```

Note the predominant User-Agent of MJ12bot/v1.4.8. The MJ12Bot belongs to Majestic-12, and is supposed to be a harmless bot created for the purpose of building a search engine. Many user reports on the internet suggest a malicious intent contrary to Majestic’s claim due to an inordinate number of requests that occupy website resources, along with a lack of adherence to disallow rules in robots.txt (Suba, "MJ12bot – Blocking the Parasites", 2016).
Additionally, a second prevalent (and more legitimate) use case for these ad hosts appears to be as an integration within a website’s workflow as shown below:

```
173.245.54.180 getmyads.com [22/Apr/2020:08:39:01 +0000] "GET /signature/90683/3f43bb85b7cd77f0b4fa3ccbe1f9cc56/en/468x60.jpg HTTP/1.1" "https://mx.world/verify_account.php?c=4d68641c7d6354866396a9dada2a9f"

162.128.249 getmyads.com [24/Apr/2020:11:21:08 +0000] "GET /signature/90683/3f43bb85b7cd77f0b4fa3ccbe1f9cc56/en/468x60.jpg HTTP/1.1" "https://mx.world/memberoffice.php"

141.101.76.41 getmyads.com [24/Apr/2020:13:33:31 +0000] "GET /signature/90683/3f43bb85b7cd77f0b4fa3ccbe1f9cc56/en/468x60.jpg HTTP/1.1" "http://mx.world/mxw_surfing.php"

162.192.99 getmyads.com [24/Apr/2020:15:50:05 +0000] "GET /signature/90683/3f43bb85b7cd77f0b4fa3ccbe1f9cc56/en/468x60.jpg HTTP/1.1" "http://mx.world/mxw_ptcads.php"

172.168.141.29 getmyads.com [24/Apr/2020:17:57:16 +0000] "GET /signature/90683/3f43bb85b7cd77f0b4fa3ccbe1f9cc56/en/468x60.jpg HTTP/1.1" "https://mx.world/register.php?r=srinivas65"
```

The ad site appears to be the result of an HTTP referral from another site (mx.world, in this case) with a JPG file unique to that site as the destination endpoint. The JPG could not be extracted from the PCAP data to determine its purpose or to confirm any additional malicious use cases.

### 3.5. Large TCP Retransmissions

High-level NetFlow analysis with SiLK revealed some very large (based on byte count) connections in the network. The following output from rwstats shows the largest TCP connections from April 16-19, 2020 (inclusive), based on the number of bytes that are initiated outbound from an internet-connected host and destined for IP addresses within the CyberBunker subnets. As shown in Figure 15, these large connections are all initiated by a single source IP to destination hosts in the 185.35.136.0/22 network.

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Bytes</th>
<th>%Bytes</th>
<th>Cumul %</th>
</tr>
</thead>
<tbody>
<tr>
<td>178.1232</td>
<td>165.35.136.201</td>
<td>21</td>
<td>21</td>
<td>687480</td>
<td>0.37%</td>
<td>0.37%</td>
</tr>
<tr>
<td>178.1232</td>
<td>165.35.136.59</td>
<td>21</td>
<td>21</td>
<td>657480</td>
<td>0.37%</td>
<td>0.74%</td>
</tr>
<tr>
<td>178.1232</td>
<td>165.35.136.138</td>
<td>21</td>
<td>21</td>
<td>6423760</td>
<td>0.37%</td>
<td>2.25%</td>
</tr>
<tr>
<td>178.1232</td>
<td>185.35.136.206</td>
<td>21</td>
<td>21</td>
<td>6393640</td>
<td>0.37%</td>
<td>2.94%</td>
</tr>
<tr>
<td>178.1232</td>
<td>185.35.137.164</td>
<td>21</td>
<td>21</td>
<td>6258080</td>
<td>0.37%</td>
<td>3.65%</td>
</tr>
</tbody>
</table>

**Figure 20 (Largest TCP Connections by Byte Count)**

Figure 16 below shows some additional statistics from rwfilter for the top connection with the largest number of bytes. This command was primarily executed to

Karim Lalji
obtain the sTime and eTime values so that the TCP stream could be isolated from the larger PCAP.

Figure 21 (rwfilter Statistics for the Largest TCP Connection)

Extracting the connection noted in Figure 16 from the larger PCAP data and analyzing it in Wireshark showed a large number of TCP retransmissions (just over 171,000) with no payload data and different sequence numbers. Each sequence number is retransmitted either precisely 242 or 241 times.

Another interesting characteristic was the presence of the TCP urgent pointer in each of the retransmitted packets. In all 171,000 packets, the URG pointer is set to 256, ruling out a potential covert channel that leverages this specific TCP header value.

Figure 22 (Wireshark Excerpt of TCP Retransmissions)

The behavior seen likely indicates an error in crafted communication or a portion of a reflected Denial of Service (DoS) attack.

Figure 23 (Wireshark TCP Retransmission Urgent Pointer)

Karim Lalji
### 3.6. Mirai Variant Router Exploits

A large number of URL's discovered in the web server logs match patterns that are similar to a variety of well-known router exploits, many of which are classified as Mirai variants. While several different malware signatures could exist in the sample set, the high-volume of data under analysis resulted in the examination of only the most frequently occurring examples. Individual devices were not examined for successful exploitation; however, the general observation is that a majority of the logged URL's can be attributed to reconnaissance activities attempting to discover vulnerable devices to exploit.

While these known Miria variants haven’t been specifically attributed to the CyberBunker group, the widespread botnet activity already identified in the address space of the adversary group suggested that an overview of further potential bot activity would be useful. A high-level survey of the most frequently occurring behaviors associated with known IoT botnets has been highlighted for the period following the traffic redirection from Legaco Networks B.V.

#### 3.6.1. Hoaxcalls DDoS IoT Botnet

A vulnerability released in February 2020 with the identifier CVE-2020-5722 has been actively exploited in the wild by Hoaxcalls, an IoT DDoS botnet variant based on source code from the Tsunami and Gafgyt botnets (Hsu, Zhang, Zhang, & Nigam, 2020). This vulnerability impacts Grandstream and Draytek Vigor devices, and as outlined by NVD in the vulnerability disclosure, “allow[s] remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI” (“NVD - CVE-2020-8515 Detail", 2020).

The following URL hits were seen in the honeypot’s web server logs attempting to access a mainfunction.cgi endpoint:

<table>
<thead>
<tr>
<th>Count</th>
<th>URI Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>73766</td>
<td>/cgi-bin/mainfunction.cgi</td>
</tr>
</tbody>
</table>
| 25435 | /cgi-bin/mainfunction.cgi?action=login&keyPath=%27%0A/bin/sh%{IFS}-c%{IFS} |--
|       | 'cd%{IFS}/tmp;%{IFS}rm%{IFS}-rf%{IFS}arm7;%{IFS}busybox%{IFS}wget%{IFS}http://19ce033f.ngrok.io/arm7;%{IFS}chmod%{IFS}777%{IFS}arm7;%{IFS}./arm7='%0A%27&loginUser=a&loginPwd=a |
The second two URL endpoints are very similar, aside from a different destination host in the embedded ‘wget’ command. Although there are several exploits used by variants of Hoaxcalls, a research paper by Radware published on April 22, 2020 indicated that the URL patterns seen above are consistent with attempts to exploit CVE-2020-8515. Additionally, the paper outlined that these botnets utilize a common User-Agent pattern containing the string “XTC” ("Radware ERT Threat Alert Evolution of Hoaxcalls April 22nd ", 2020).

Extracting the User-Agent from the web server logs for requests containing ‘/cgi-bin/mainfunction.cgi’ yield results consistent with the expected User-Agent string outlined by Radware (left). Additionally, a public proof of concept (POC) exploit for DrayTek Vigor devices was released on March 31, 2020 on Packet Storm ("DrayTek Vigor2960 / Vigor3900 / Vigor300B Remote Command Execution", 2020).

Palo Alto Networks noted a sudden increase in exploitation traffic soon after the POC was released, stating that “this vulnerability was employed by a new DDoS botnet for propagation” (Hsu, Zhang, Zhang, & Nigam, 2020). This is further verified by a graph from CVE Stalker (right) showcasing traffic patterns specific to CVE-2020-8515, demonstrating a notable spike during the first few days of April. The timing of these attacks and release of the exploit is consistent with the analysis window of the examined CyberBunker traffic. However,
according to the dates noted in the traffic graph above, the most notable spikes appear a few weeks prior to this analysis.

3.6.2. **NetLink GPON Router – Polaris Botnet**

Another variant of the XTC botnet discussed previously is known as the Polaris botnet, which attempts to discover vulnerable devices using the /boaform/admin/formPing URL endpoint. This specific URL is tied to a Netlink GPON Router 1.0.11 remote code execution vulnerability. The exploit Proof of Concept (POC) code was published on exploit-db on March 17, 2020 (EDB-ID:48225) however, there is currently no assigned CVE as the vulnerability is still relatively new at the time of this writing. These botnets also leverage an older vulnerability in GPON routers utilizing CVE-2018-10562 and CVE-2018-10561 with a URL pattern on /GponForm/diag_Form?images/.

The following table shows instances of URL’s matching these patterns within the analysis data:

<table>
<thead>
<tr>
<th>Count</th>
<th>URI Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>17120</td>
<td>POST /boaform/admin/formPing</td>
</tr>
<tr>
<td>3303</td>
<td>POST /GponForm/diag_Form?images/</td>
</tr>
<tr>
<td>137</td>
<td>GET /boaform/admin/formPing</td>
</tr>
<tr>
<td>73</td>
<td>GET /boaform/admin/formPing?target_addr=;cd</td>
</tr>
<tr>
<td>4</td>
<td>POST /boaform/admin/formPing?target_addr=;'+payload+='%20/&amp;waninf=1 INTERNET_R VID 154</td>
</tr>
</tbody>
</table>

**Table 3 (Polaris Botnet URL’s)**

For all 17,120 URL endpoints with an HTTP POST to boaform/admin/formPing the User-Agent string is conveniently set to “polaris botnet”. Additionally, all 3,303 occurrences with the HTTP POST to /GponForm/diag_Form?images/ have a User-Agent string of “Hello, World”.

These URL patterns and User-Agents were also seen and identified by the SANS Internet Storm Center on March 21, 2020 (Bruneau, "Honeypot - Scanning and Targeting Devices & Services - SANS Internet Storm Center", 2020).

Karim Lalji
3.6.3. ThinkPHP RCE Router Exploits

Several URL patterns in the Apache logs are consistent with a remote code execution vulnerability in ThinkPHP affecting versions 5.0 and 5.1. The vulnerability was fixed in versions 5.0.23 and 5.1.31. TrendMicro identified these signatures as a Mirai variant called Yowai. 3,571 occurrences of the following URL were discovered in the Apache logs within the time analysis window:

GET/index.php?s=%2f%69%6e%64%65%78%2f%5c%74%68%69%6e%6b%5c%61%70%70%2f%69%6e%76%6f%6b%65%66%75%6e%63%74%69%6f%6e%function=%63%61%6c%6c%5f%75%73%65%72%5f%66%75%6e%63%5f%61%72%72%61%79&function=%63%61%6c%6c%5f%75%73%65%72%5f%66%75%6e%63%5f%61%72%72%61%79&vars[0]=%6d%45&vars[1]=%48%65%6c%6c%6f%54%68%69%6e%6b%50%48%50

When the URL is decoded, the following request is the result:

GET/index.php?s=/index/	hink\app\invokefunction&function=call_user_func_array &vars[0]=md5&vars[1]=HelloThinkPHP

F5 Labs performed an analysis on this IoT botnet variant and identified a reconnaissance campaign which was used to identify devices that are vulnerable, and that leverages URLs very similar to the one noted above (Segal, "Threat Actors Rapidly Adopt New ThinkPHP RCE Exploit to Spread IoT Malware and Deploy Remote Shells", 2018). Two other relevant URL’s in this category are as follows:

- 3472 GET /index.php?s=/module/action/param1/${@die(md5(HelloThinkPHP))}
- 3529 GET /index.php/module/action/param1/${@die(md5(HelloThinkPHP))}

As shown above approximately 3,500 URLs for each discovery attempt were found in the honeypot’s web server logs.

4. Conclusion

Analysis of the seized CyberBunker networks provided reasonable insight into a variety of potential botnet and command and control activities. The findings should be taken with some degree of caution when attempting to draw conclusions due to only a portion of the traffic being available for analysis. Further investigation would most likely

Karim Lalji
yield additional results and discoveries. Due to the large data set, investigative activities
needed to be focused in specific areas while also leveraging a sampling approach.

As a general observation, previously compromised hosts are continuing to "call
home" to C&C servers within the IP address space belonging to CyberBunker and could
also be sending exfiltrated data back to adversary groups. Potential phishing and ad
networks are continuing to receive traffic, either as a result of active campaigns, but more
likely due to residual instructions from previously compromised hosts. There is also a
small amount of evidence pointing to DNS hosting of illicit pornography which
prospective owners of the IP address space may wish to investigate further to ensure
illegal content is no longer being accessed.

In order to protect the privacy of hosts that are assumed to be compromised,
identifying characteristics such as source IP addresses or hostnames that can identify an
internet-bound user have been partially redacted. Additionally, only high-level details
about the analyzed data have been provided. Where appropriate, additional artifacts
including raw data can be shared with researchers.
References


Karim Lalji
Exploit to Spread IoT Malware and Deploy Remote Shells. Retrieved from

https://topfreelancer.co.uk/blog/mj12bot-blocking-the-parasites/

General, A. (2020, April 7). Landeszentralstelle Cybercrime der Generalstaatsanwaltschaft Koblenz erhebt Anklage gegen acht Tatverdächtige im Verfahren gegen die Betreiber des "Cyberbunkers". Retrieved from
4.1. Appendix A – Top IP Address (Bytes)

The following table provides high-level statistics on the top-25 IP addresses based on the number of bytes. The directionality (in/out) are referenced based on the perspective of the CyberBunker subnets. Bytes (Out) refers to bytes sent out from the CyberBunker subnet to a destination IP. Bytes (In), conversely, refers to bytes received by the CyberBunker subnets from a source IP.

<table>
<thead>
<tr>
<th>Destination IP</th>
<th>Bytes (Out)</th>
<th>Source IP</th>
<th>Bytes (In)</th>
</tr>
</thead>
<tbody>
<tr>
<td>189.89.133.190</td>
<td>4919373</td>
<td>189.89.133.190</td>
<td>9848124</td>
</tr>
<tr>
<td>201.4.167.162</td>
<td>374084</td>
<td>34.102.197.176</td>
<td>6488961</td>
</tr>
<tr>
<td>189.107.246.251</td>
<td>359776</td>
<td>179.106.151.75</td>
<td>6423259</td>
</tr>
<tr>
<td>187.127.171.50</td>
<td>305146</td>
<td>201.184.118.114</td>
<td>6267081</td>
</tr>
<tr>
<td>179.127.197.22</td>
<td>166196</td>
<td>178.217.188.232</td>
<td>4895134</td>
</tr>
<tr>
<td>187.127.166.133</td>
<td>150947</td>
<td>177.72.3.62</td>
<td>4219110</td>
</tr>
<tr>
<td>179.182.87.240</td>
<td>119147</td>
<td>34.98.123.114</td>
<td>2906034</td>
</tr>
<tr>
<td>80.82.65.60</td>
<td>102568</td>
<td>192.223.24.250</td>
<td>2521593</td>
</tr>
<tr>
<td>89.248.168.221</td>
<td>102439</td>
<td>185.156.73.42</td>
<td>1699446</td>
</tr>
<tr>
<td>185.143.223.81</td>
<td>102419</td>
<td>80.82.65.60</td>
<td>1190861</td>
</tr>
<tr>
<td>194.26.29.213</td>
<td>94521</td>
<td>89.248.168.221</td>
<td>1180988</td>
</tr>
<tr>
<td>194.26.29.114</td>
<td>93789</td>
<td>177.12.44.228</td>
<td>1062855</td>
</tr>
<tr>
<td>45.251.59.178</td>
<td>93668</td>
<td>185.143.223.81</td>
<td>899721</td>
</tr>
<tr>
<td>194.26.29.210</td>
<td>91251</td>
<td>92.118.37.95</td>
<td>648149</td>
</tr>
<tr>
<td>194.26.29.212</td>
<td>89941</td>
<td>194.26.29.213</td>
<td>549475</td>
</tr>
<tr>
<td>189.126.64.158</td>
<td>89856</td>
<td>194.26.29.114</td>
<td>545213</td>
</tr>
<tr>
<td>189.168.101.130</td>
<td>86463</td>
<td>194.26.29.210</td>
<td>539951</td>
</tr>
<tr>
<td>45.141.84.15</td>
<td>86163</td>
<td>194.26.29.212</td>
<td>535867</td>
</tr>
<tr>
<td>185.103.153.176</td>
<td>82583</td>
<td>187.36.198.199</td>
<td>531560</td>
</tr>
<tr>
<td>185.103.248.146</td>
<td>81651</td>
<td>72.43.255.68</td>
<td>384790</td>
</tr>
<tr>
<td>91.209.234.200</td>
<td>19898</td>
<td>12.146.238.57</td>
<td>198154</td>
</tr>
<tr>
<td>91.209.157.22</td>
<td>15747</td>
<td>80.82.64.210</td>
<td>107708</td>
</tr>
<tr>
<td>111.59.93.76</td>
<td>14625</td>
<td>205.205.150.21</td>
<td>70352</td>
</tr>
<tr>
<td>91.209.157.34</td>
<td>14308</td>
<td>14.135.120.21</td>
<td>52006</td>
</tr>
<tr>
<td>185.156.73.42</td>
<td>10167</td>
<td>202.83.172.43</td>
<td>49380</td>
</tr>
</tbody>
</table>

Data Source: SiLK rwfilter and rwstat
### 4.2. Appendix B – Top TCP Ports (Count)

The following table provides high-level statistics on the top-25 TCP ports based on the number of connections. The directionality (SRC/DST) are referenced based on the perspective of the CyberBunker networks. TCP Port (OUT) header refers to connections initiated from within the CyberBunker networks along with the destination port of the receiver. The TCP Port (IN) header refers to connections initiated to one of the CyberBunker networks along with the destination port used by the sender.

<table>
<thead>
<tr>
<th>TCP Port (OUT)</th>
<th>Count</th>
<th>TCP Port (IN)</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>26372</td>
<td>2401477</td>
<td>51315</td>
</tr>
<tr>
<td>443</td>
<td>11324</td>
<td>961228</td>
<td>47150</td>
</tr>
<tr>
<td>32767</td>
<td>7249</td>
<td>543198</td>
<td>58338</td>
</tr>
<tr>
<td>35408</td>
<td>2024</td>
<td>413400</td>
<td>47867</td>
</tr>
<tr>
<td>22</td>
<td>1676</td>
<td>409306</td>
<td>45061</td>
</tr>
<tr>
<td>81</td>
<td>1234</td>
<td>406559</td>
<td>45053</td>
</tr>
<tr>
<td>36357</td>
<td>1036</td>
<td>257483</td>
<td>47310</td>
</tr>
<tr>
<td>65301</td>
<td>972</td>
<td>255703</td>
<td>57820</td>
</tr>
<tr>
<td>41902</td>
<td>929</td>
<td>247191</td>
<td>44793</td>
</tr>
<tr>
<td>8080</td>
<td>909</td>
<td>246321</td>
<td>47316</td>
</tr>
<tr>
<td>34377</td>
<td>841</td>
<td>228080</td>
<td>46126</td>
</tr>
<tr>
<td>33343</td>
<td>835</td>
<td>226473</td>
<td>46449</td>
</tr>
<tr>
<td>26341</td>
<td>812</td>
<td>176254</td>
<td>59973</td>
</tr>
<tr>
<td>2552</td>
<td>785</td>
<td>173495</td>
<td>56895</td>
</tr>
<tr>
<td>31103</td>
<td>693</td>
<td>148799</td>
<td>49525</td>
</tr>
<tr>
<td>31042</td>
<td>685</td>
<td>121673</td>
<td>42682</td>
</tr>
<tr>
<td>1947</td>
<td>682</td>
<td>117104</td>
<td>1883</td>
</tr>
<tr>
<td>1024</td>
<td>648</td>
<td>114451</td>
<td>55457</td>
</tr>
<tr>
<td>37686</td>
<td>616</td>
<td>111469</td>
<td>44172</td>
</tr>
<tr>
<td>61604</td>
<td>591</td>
<td>109960</td>
<td>32767</td>
</tr>
<tr>
<td>48414</td>
<td>572</td>
<td>97022</td>
<td>50883</td>
</tr>
<tr>
<td>25755</td>
<td>536</td>
<td>83166</td>
<td>55644</td>
</tr>
<tr>
<td>29427</td>
<td>523</td>
<td>80127</td>
<td>443</td>
</tr>
<tr>
<td>48957</td>
<td>518</td>
<td>79036</td>
<td>55967</td>
</tr>
<tr>
<td>14139</td>
<td>517</td>
<td>76433</td>
<td>46410</td>
</tr>
</tbody>
</table>

Data Source: Zeek conn.log and bro-cut
4.3. Appendix C – Top Hostnames

The following table outlines the top-50 most frequently occurring hostnames from both the Apache web server logs and DNS queries obtained from the PCAP data.

<table>
<thead>
<tr>
<th>Top 50 Hostnames (Apache Logs)</th>
<th>Top 50 DNS Queries (Zeek/PCAP Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>249427 <a href="http://www.darkdata.com">www.darkdata.com</a></td>
<td>15148192 cloud.mikrotik.com</td>
</tr>
<tr>
<td>31957 rofpublic.club</td>
<td>4550014 a.root-servers.net</td>
</tr>
<tr>
<td>30782 pizzajlx.com</td>
<td>3382442 api.caipiaokong.cn</td>
</tr>
<tr>
<td>22486 goldvod.com</td>
<td>2246665 acs.oi.net.br</td>
</tr>
<tr>
<td>17753 getmyads.com</td>
<td>748984 <a href="http://www.google.com">www.google.com</a></td>
</tr>
<tr>
<td>11763 <a href="http://www.goldvod.com">www.goldvod.com</a></td>
<td>546893 support.kf6688.xyz</td>
</tr>
<tr>
<td>9846 <a href="http://www.getmyads.com">www.getmyads.com</a></td>
<td>473302 m.caipiaokong.com</td>
</tr>
<tr>
<td>5065 cyberbunker.com</td>
<td>432801 eeyoo.net</td>
</tr>
<tr>
<td>3649 traffic.getmyads.com</td>
<td>418240 access-board.gov</td>
</tr>
<tr>
<td>2416 pagarex.com</td>
<td>412577 185-35-137-85.v4.as62454.net</td>
</tr>
<tr>
<td>1645 thepiratebay.plus</td>
<td>348554 unifi.dini.com.ar</td>
</tr>
<tr>
<td>1180 lACLub.org</td>
<td>348484 185-35-139-72.v4.as62454.net</td>
</tr>
<tr>
<td>1147 utjshwqf.top</td>
<td>344122 graph.facebook.com</td>
</tr>
<tr>
<td>1023 siterp.me</td>
<td>340902 acsvelox.oi.net.br</td>
</tr>
<tr>
<td>844 wiieuqwewq.top</td>
<td>328618 nccih.nih.gov</td>
</tr>
<tr>
<td>688 tuhiffsdf.top</td>
<td>291467 v4.as62454.net</td>
</tr>
<tr>
<td>599 backdo0red.org</td>
<td>284296 connectivitycheck.gstatic.com</td>
</tr>
<tr>
<td>563 ukpressnews.com</td>
<td>260026 ns1.as62454.net</td>
</tr>
<tr>
<td>530 winner.one</td>
<td>256822 mz.gov.pl</td>
</tr>
<tr>
<td>493 <a href="http://www.goldvod.com">www.goldvod.com</a></td>
<td>252543 matrix-hax.com</td>
</tr>
<tr>
<td>328 zyztm.com</td>
<td>247678 m.youtube.com</td>
</tr>
<tr>
<td>314 ip.w.s.126.net:443</td>
<td>238241 ns2.as62454.net</td>
</tr>
<tr>
<td>300 darkdata.com</td>
<td>224981 ns2.as29090.net</td>
</tr>
<tr>
<td>299 localsbitcoin.com</td>
<td>219507 ns1.as29090.net</td>
</tr>
<tr>
<td>280 arbitao.org</td>
<td>206327 <a href="http://www.baidu.com">www.baidu.com</a></td>
</tr>
<tr>
<td>267 mainamagame.com</td>
<td>205494 i.instagram.com</td>
</tr>
<tr>
<td>266 bank66.com</td>
<td>203108 auth.api.np.ac.playstation.net</td>
</tr>
<tr>
<td>264 <a href="http://www.lACLub.org">www.lACLub.org</a></td>
<td>196777 vtk.be</td>
</tr>
<tr>
<td>259 underground.business</td>
<td>194701 <a href="http://www.instagram.com">www.instagram.com</a></td>
</tr>
<tr>
<td>259 ataconsortium.com</td>
<td>194013 <a href="http://www.netflix.com">www.netflix.com</a></td>
</tr>
<tr>
<td>252 dx4services.com</td>
<td>175583 159.138.35.185.in-addr.arpa</td>
</tr>
<tr>
<td>249 smilespontosbb.com</td>
<td>169889 doc.gov</td>
</tr>
<tr>
<td>249 anyblaze.com</td>
<td>169518 play.googleapis.com</td>
</tr>
<tr>
<td>239 xennt.com</td>
<td>168468 youtubei.googleapis.com</td>
</tr>
<tr>
<td>234 newgameplanet.com</td>
<td>159336 <a href="http://www.facebook.com">www.facebook.com</a></td>
</tr>
<tr>
<td>234 copa.media</td>
<td>158893 <a href="http://www.sscfly.com">www.sscfly.com</a></td>
</tr>
<tr>
<td>233 <a href="http://www.zyztm.com">www.zyztm.com</a></td>
<td>156760 livecm-1.bilibili.com</td>
</tr>
<tr>
<td>229 boss.chat</td>
<td>154586 android.googleapis.com</td>
</tr>
</tbody>
</table>
### Honeypot Network Forensics - CyberBunker

<table>
<thead>
<tr>
<th>Port</th>
<th>Host Name</th>
<th>Origin Port</th>
<th>Source IP/Domain</th>
<th>Destination Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>226</td>
<td>straitstoday.com</td>
<td>153239</td>
<td>googleads.g.doubleclick.net</td>
<td></td>
</tr>
<tr>
<td>216</td>
<td>verifiedemail.org</td>
<td>146397</td>
<td>185-35-138-173.v4.as62454.net</td>
<td></td>
</tr>
<tr>
<td>204</td>
<td>streamlife77.com</td>
<td>144100</td>
<td>auth.riotgames.com</td>
<td></td>
</tr>
<tr>
<td>202</td>
<td>martewz.com</td>
<td>138590</td>
<td>i.ytimg.com</td>
<td></td>
</tr>
<tr>
<td>194</td>
<td>gc4you.net</td>
<td>135198</td>
<td>android.clients.google.com</td>
<td></td>
</tr>
<tr>
<td>181</td>
<td>bitiblue.com</td>
<td>132139</td>
<td><a href="http://www.googleapis.com">www.googleapis.com</a></td>
<td></td>
</tr>
<tr>
<td>179</td>
<td>rastreiocorreios.com</td>
<td>131496</td>
<td>authserver.mojang.com</td>
<td></td>
</tr>
<tr>
<td>177</td>
<td>ref.arbitao.org</td>
<td>131466</td>
<td><a href="http://www.bb36888.com">www.bb36888.com</a></td>
<td></td>
</tr>
<tr>
<td>176</td>
<td>xxx.yt</td>
<td>130016</td>
<td>graph.instagram.com</td>
<td></td>
</tr>
<tr>
<td>175</td>
<td>timeswiss.watch</td>
<td>129137</td>
<td>accounts.spotify.com</td>
<td></td>
</tr>
<tr>
<td>174</td>
<td>sealand.center</td>
<td>124525</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Data Source: Apache HTTP logs, Zeek dns.log and bro-cut
## Upcoming Training

<table>
<thead>
<tr>
<th>Training Name</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London October 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Oct 12, 2020 - Oct 17, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS October Singapore 2020 - Live Online</td>
<td>Singapore, Singapore</td>
<td>Oct 12, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020 - Live Online</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020</td>
<td>London, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020 - Live Online</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defense Initiative 2020 - Live Online</td>
<td>Washington, DC</td>
<td>Dec 14, 2020 - Dec 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>