Security Information and Event Management

Detailed Log Analysis

Objectives

Given a dataset with the network logs of traffic flows of a company's network in a normal day, we were asked to analyze what defined their behaviors as typical. After that, we were given a dataset of the same company but from a day that had anomalous and illicit behavior occurring in different ways, with the goal of identifying malicious events within the network in order to implement a cybersecurity system with alert rules of possible malicious intent fit for this company.

Normal day analysis

When analyzing the normal day, we could see working hours were between 1am and 11h30pm and data volume peak was around lunch time.

The network's machines only communicated with 4 private IP addresses, two of them we can conclude were DNS servers due to being exclusively used with UDP on port 53. The other two private addresses we can assume were assigned to another server, such as mail or web.

The machines could have up to 12000 connections, the average request size was about 9KB to 10.5KB upload and 83KB to 110KB download, depending on the machine. Upload and download ratios varied from 0.10 to 0.11, the maximum total upload a machine had at the end of the day was about 130MB and about 1.2GB download.

On this normal day, machines had up to 1500 connections with the DNS server. On average, each of these requests was about 193KB to 211KB upload and about 430 KB to 500KB download, depending on the machine. The maximum total upload and download from a given machine to the DNS servers was about 300KB and 695KB, respectively. Upload and download ratios varied from 0.41 to 0.45, to the DNS servers.

About 35 different countries were contacted on this day, with average communication volume.

No massive amounts of uploads(more than 1mB) on the same request were detected, both high amounts of traffic in a short time(frequency) and large packet size occurrences were searched for and not found. No periodic uploads of large volume were detected.

Anomalous activity analysis

Evidence to the following anomalous behaviors was detected in the provided unanalyzed network's logs:

- **Botnet activity**: machines that weren't the network's servers were found communicating directly with one another, establishing a network of 3 compromised computers. This could be due to opening malicious or phishing emails, malware present in the computer or network vulnerabilities;
- **Command & Control**: machines were found to have slightly above average number of connections to DNS servers, above average upload and a lot of connections with storage servers, but keeping up/download ratio normal. This could be upload of console logs and remote control evidence, due to network

vulnerabilities, malware, phishing or insider threats to control computers and spy on the network;

- **Never Contacted Countries/Autonomous Systems**: thirty countries/AS that weren't communicated with on the reference "normal" day, were now communicated with and the volume of data is suspicious. Some of the countries themselves are widely known to be sources of malicious activity. Once again this could be due to malware, phishing, vulnerabilities, hackers using a VPN to hide their location and the other reasons mentioned before and could cause malware infections, data exfiltration and discovery of passwords. Note: this isn't considered use of VPN or proxy because of the irregularity pattern found;
- **Exfiltration to Google Drive**: very large amounts of traffic was found using protocol UDP on port 443, with the destination some of Google Drive's servers and very large upload amounts. Data exfiltration can be caused by inside agents, malware, stolen credentials, weak encryption and the reasons mentioned before. This could compromise company secrets and it's workers privacy;
- **Exfiltration to Twitter:** large amounts of traffic was found using protocol TCP on port 443, with the destination some of Twitter's servers, spread around a large number of packets. This could be due to malware automating data exfiltration and some of the reasons previously mentioned, with also the same consequences
- **Exfiltration through DNS**: an abnormal amount of DNS connections was found on some machines, they could be encoding sensitive information into DNS requests/responses and transmitting them to an external malicious server. This could be due to malware, network vulnerabilities and lack of DNS security measures and causes the same consequences as other data exfiltration techniques;
- **After-hours Activities**: through timestamp analysis, we found unusual activities at certain hours where there should be a low amount of traffic or none at all. Most of the upload was at 7am(due to exfiltration to Google Drive), but most importantly, one machine was detected periodically uploading small amounts of data to the same server. This could be due to the machine being storing scheduled backups (weekly backups would explain absence in "normal" day log) or maintenance, but could also be a sign of malware or data exfiltration.

Proposed SIEM Rules

These are our proposed rules to implement, in this company's network, in order to alert when the anomalous detected in our analysis occurs, with the intent to prevent malicious actions such as data exfiltration and propagation:

- **Botnet Activity Prevention Rule**: generate an alert whenever traffic is detected with a private destination IP that isn't a local server(such as DNS/web/mail servers);
- **C&C Prevention Rule**: generate an alert whenever a machine has more than 270 KB upload to DNS servers, more than 1400 connections to DNS server and more than 1000 connections with IPs from known storage networks, such as 157.240.212.0/24 (Facebook) or Google Drive's various networks;
- **Unknown Country/Autonomous System Communication Prevention**: generate an alert whenever a machine communicates with more than 5 suspicious, blacklisted or never seen before countries(or autonomous systems) and has above 500MB of upload(average upload of machines in reference day);

- **Google Drive Exfiltration Prevention Rule**: generate an alert whenever a machine, on UDP connections on port 443, has more than 150KB of upload;
- **Social Networks Exfiltration Prevention Rule**: generate an alert whenever a machine, on TCP connections, has more than 900 connections to a known Social Network server(such as Twitter, Facebook or Skype) and has more than 150KB of upload;
- **DNS Exfiltration Prevention Rule**: generate an alert whenever a machine generates more than 2500 requests to the DNS servers or more than 300KB of upload to the DNS servers;
- **After-Hours Exfiltration Prevention Rule**: generate an alert whenever traffic is found between 11:40 pm and 1:00 am with an amount of uploaded bytes more than 11KB(more than average upload size per request in reference day).

Anomalous Machine Detection

The following machines were detected with the anomalous behavior previously described and the test results that made them get flagged as anomalous:

- **Botnet Evidence**: **192.168.103.177**, **192.168.103.54** and **192.168.103.58** were the only machines with requests to private addresses that weren't the network's servers, the destination of these connections being each other, with about 146 to 276 requests made. We found them by searching the number of private addresses that each machine made a request to;
- **Command & Control Evidence**: **192.168.103.78** and **192.168.103.107** were found to have slightly above average number of connections to DNS servers, at around 1600, above average total upload, at 300KB to 350KB to the DNS servers, and frequent connections with Google Drive and Facebook servers were detected. We found these machines by searching for the number of requests evolving DNS servers, the total upload size of requests to the DNS servers and after identifying a few suspects, we analyzed the rest of their requests(frequency, size and destination);
- **Never Contacted Countries/AS Evidence**: **192.168.103.34**, **192.168.103.67** and **192.168.103.160** were found communicating with 11, 18 and 16 new countries, respectively. Their requests added to 6MB or 12MB of uploaded data, depending on the machine. We found this by filtering requests that we made to unknown countries or autonomous systems, we had 5 results but 2 of those machines couldn't confidently be considered as anomalous due to the traffic frequency, total size and country destination;
- **Google Drive Exfiltration Evidence**: **192.168.103.43** and **192.168.103.47** were found having 4.2GB and 6.7GB, respectively, of uploaded data in 26 and 39 requests, respectively, to destination IPs belonging to Google Drive. The upload/download ratio for each machine was 58 and 51. We found evidence of this by searching for the most total upload, high upload/download ratios and by filtering by UDP requests on port 443, commonly used by Google Drive. We confirmed the large amount of data exfiltration since the number of requests is very low;
- **Twitter Exfiltration Evidence**: **192.168.103.110** and **192.168.103.207** were found having 0.37 and 0.39 upload/down ratios, respectively, which is way above average. Their requests to the Twitter IP amounted to a total of 72MB and 143MB uploaded data, using 159 and 319 connections, respectively, on TCP protocol. We found them by sorting by high upload/download ratios, high amount and frequency of requests. This behavior is particularly strange for a social network which usually has way more download than upload, especially with this high number of requests;

- **DNS Exfiltration Evidence**: **192.168.103.137** and **192.168.103.175** were flagged with DNS exfiltration for having 50000 and 30000 requests to the DNS servers, respectively. With these connections they uploaded 1MB and 580KB of data, respectively, which is way above the average established by the “normal” day. These machines were found by filtering for connections with de DNS servers, sorting by total upload amount and total number of requests. The suspicions were confirmed by the normal upload/download ratio and the normal average request size;
- **Anomalous After-hours Activity Evidence**: **192.168.103.47** was found having suspicious activities outside service hours. From 10:20pm to 00:20am, this machine was found to periodically(every 20 minutes) send requests with 125MB to 285MB to a Google Drive server. We found this anomaly by analyzing entries with timestamps without activity in the reference day, sorting by amount of upload per second and per minute and finally by sorting the timestamps by upload amount, thus detecting the exfiltration pattern.

Conclusion

After the thorough analysis of both a normal and an anomalous day of this company’s network, we were able to detect 14 machines with possible malicious intent, using one of 7 ways to possibly cause harm to this corporate network. With the proposed SIEM rules to be implemented to trigger real-time alerts we hope to allow security analysts teams to promptly investigate and respond to potential security incidents, minimizing the time between detection and response, enhancing the organization's ability to mitigate security threats effectively.