APT1: Attack Indicators

Andrew Maddox

University of Advancing Technology

In order to develop a set of indicators for our own organization, it is important to analyze those that were found within the APT1 report. Once we understand how these indicators presented themselves in the APT1 report we can then use them to develop an idea of what that indicator would look like in our business scenario. By doing this we can compile a list of indicators that will help us identify an attack on our own business, even if it is somewhat different than the ones presented in the APT1 report.

The first, and one of the most prevalent indicators presented in the APT1: ATTACK LIFECYCLE section were the phishing emails sent by the APT1 group that conducted the attack. These emails according to the report contained “a malicious attachment or a hyperlink to a malicious file,” which would lead to a download containing an executable giving the APT1 attackers a backdoor into the system (APT1, 28). The hackers also created email accounts using the names of employees and executives at the company, however, the email extensions were not that of the company but that of a random free email service. These two facts give us a good idea of what to look for when we are trying to identify a phishing attack. Employees will receive emails from email accounts using recognizable names but that does not have the company email extension, and there will most likely be a file download or hyperlink which will contain some type of malware (usually in ZIP format).

One other attack indicator that isn’t as clear as the others presented in the report is that of outbound traffic of malicious programs. The report briefly mentions that the phishing attack is used to install a malware program that can send outbound traffic to their servers because it is much easier to send malicious traffic from inside a network to the outside than the reverse. This is because firewalls often only focus on inbound traffic. Therefore, one possible attack indicator that can be used is to look for outbound malicious traffic, and if any are found there is most likely malicious programs running from within your organization’s network, possibly indicating an attack is in progress or imminent. Meaning it is a good idea to use an outbound firewall to search for malicious traffic as a possible attack indicator.

The second major, but harder to find, attack indicator mentioned in the report, are the HTML tags hidden in the website responses from C2 servers. As the report explains “WEBC2 backdoor is designed to retrieve a webpage from a C2 server”, this means that the backdoor installed on the computer then ”expects the webpage to contain special HTML tags” (APT1, 31). By looking for these types of hidden commands in traffic we can look for computers that have been compromised. For example, if a computer is requesting these webpages and receiving responses containing hidden commands it should be an indicator that the computer is most likely compromised, this is even more so the case if the computer is making an abnormally large number of requests for webpages or the responses are from known C2 servers. This means as one of our attack indicators we can look for this kind of traffic and look to what computers are receiving the responses to find where our network may be compromised.

To add to the previous attack indicator, one way we know traffic is malicious is by checking if it contains a known attacker’s SSL certificates. The APT1 report suggested this is an effective way of finding malicious traffic, especially when it is attempting to blend in with legitimate HTTP/HTTPS traffic. Therefore, we can follow the author’s advice in the report and “incorporate [the SSL certificates] into [our] network signatures” as a possible attack indicator (APT1, 33).

One final attack indicator that the APT1 report exposes is in the method some attackers may use to try and retrieve the stolen information from a network. While your network is already compromised it is still a final last-ditch indicator that the company is under attack. The report explains that “[a]fter creating files compressed via RAR, the APT1 attackers will transfer files out of the network,” and that they might also “[split] them into chunks before transferring them” (APT1, 37). By knowing this information, by looking for an abnormal amount of FTP activity, especially that involving RAR files or when multiple files are all the same size, we can attempt to look for malicious actors stealing our information. This should be a major red flag of an attack indicator since it means the company information is already being stolen and the network is already compromised, but it is still a possible attack indicator nonetheless.

In conclusion, by analyzing prior attacks, and the reports of what others have learned from those attacks, we can gain insight into possible attack vectors or signs of an attack for our own company. For example, by analyzing the APT1 report in this paper we have gained a number of new insights, here is a quick recap. Attackers will use phishing attacks that attempt to mimic other employees or executives which contain attachments or links that will download malware containing a backdoor. We can analyze outbound network traffic for malicious traffic to see if any malicious programs exist within our network. We can look through HTTP requests and responses to look for hidden commands from backdoor programs that exist within our network, and by utilizing known attacker SSL certificates we can even identify camouflaged traffic that contains these messages. And finally, as a last-ditch effort, we can search for abnormal FTB traffic that is sending RAR or ZIP files. By knowing these attack indicators, we can better protect our company’s network from malicious entities, and hopefully, prevent future or ongoing attacks.

References

APT1: Exposing One of China’s Cyber Espionage Units. (n.d.). Retrieved from

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf