Assignment block 2 - Group 9

What security issue does the data speak to?

The dataset collects packets originating from the Mirai botnet. A botnet such as Mirai consists of infected computers that are used to infect new computers and perform arbitrary attacks as ordered by the controller of the botnet. One of the most prevalent forms of attack is a DDoS attack[1] in which all of these computers will start connecting to a targeted service with the goal of taking down the servers by overloading them. This is not the only threat however, as your computer could also be part of the botnet, in which the risk is that the controller can access private information stored on your computer.

Given these risks we identify two security issues caused by a botnet infection, and analyse the three components (whose security, what to secure, and security from who).

1. Your service being the target of DDoS attacks, during which the service is very likely to incur downtime. This issue threatens the security of the owners of the servers being targetted, since their availability will be threatened by the botnet owners.

2. Hosts in your network being infected thereby possibly revealing or corrupting private data. This issue threatens the security of the owner of the infected computer, because each aspect of CIA-security is threatened by the

What would be the ideal metrics for security decision makers?

The role of a security decision maker is to weigh the cost of a security measure against the increase in safety, and thus the decrease in incidents. The ideal metrics for this role would make it easy to perform such a cost/benefit analysis. We therefore chose a set of metrics that describe the risk and cost of incidents occurring. Because the security issue we discuss is about the Mirai botnet, we specifically chose metrics related to botnets.

1. Number of infected machines in own network
2. Rate of infection in own network
3. Damage/cost per infection
4. Cost to prevent infection
5. Cost to fix infection

To get an idea of the risk to security issues, the decision maker wants to know the likelihood of the security issue occurring and the impact of this issue. With these metrics the security decision maker can make an appropriate analysis of the current level of security, assess how new security measures with their individual costs would impact the security level and therefore determine the potential security benefits of any new measures. In the following table we summarize expand upon the metrics above and place them in a context that enables risk analysis for both security issues:

	Likelihood	Impact
(1) DDos Attacks	How many hosts from a botnet are connecting to my service? At what size DDoS attack will we experience downtime/outages?	What are the damages associated with downtime of my service? How long until we can recover from an attack?
(2) Personal Data	How often are computers in my network infected by a botnet? How capable are we of detecting infections and mitigating them?	What personal data am I storing on the computers / servers that run my service? To what data that is not stored locally do the computers / servers that run my service have access? What is the possible damage from losing this data? What does it cost to deal with an infection?

Metrics used in practice

In this section we discuss some research done into detecting botnet infection, botnet behaviour, and botnet analysis.

Akiyama et al.[2] discuss metrics for detecting that a botnet infection is present. They focus on three metrics: relationship, response and synchronization, which we will briefly detail. The relationship metric uses the fact that the bots have a bot-master somewhere, which each bot communicates with. The response metric relies on identifying a consistent response time between a bot receiving a signal from its master and its response to that signal. The synchronization metric uses the simultaneous acting nature of the entire botnet. All (or at least a large portion of) the bots will take the same actions, such as a DDoS attack or reporting their status to the master, at almost the same time. These three metrics can be used to identify compromised systems in a network traffic analysis.

Antonakakis et al.[3] use a combination of techniques for measuring botnet size and tracking the evolution of the botnet's capabilities. The botnet size was measured by making use of a network telescope. Using this network telescope, infected hosts scanning for new victims could be found. The metric used to estimate the size of the botnet is the number of hosts which actively scan for potential infectants at the start of every hour. In order to track the capabilities of the botnet a telnet honeypot was used to obtain infected binaries in combination with a set of binaries from VirusTotal. The total number of unique binaries gives an estimation on the size of the set of capabilities of the mirai like botnet. These could be analyzed further to determine architecture and vendor targets.

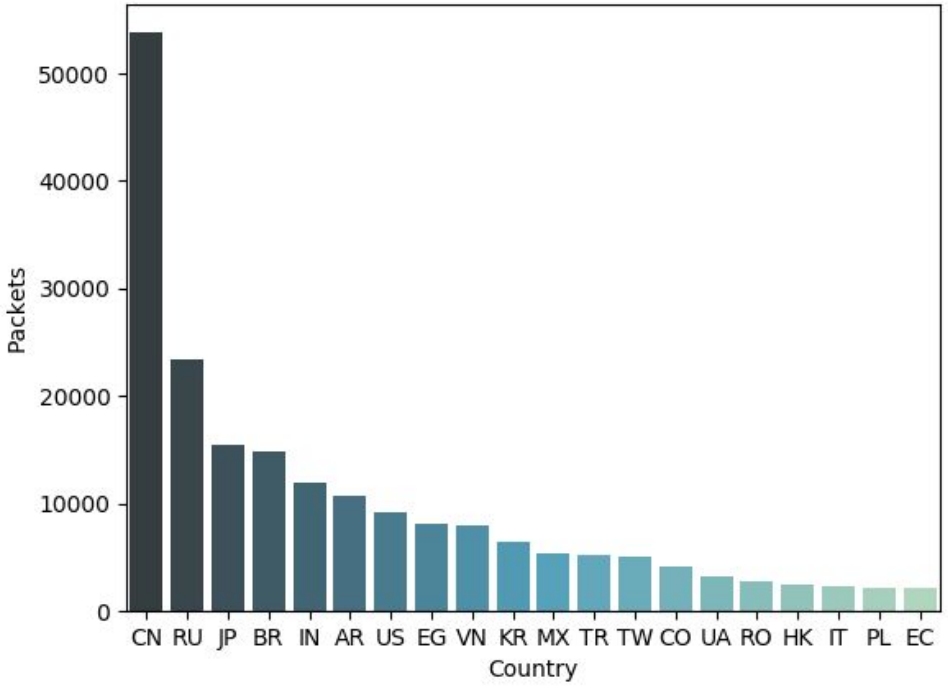
Imperva Security[4], an IT security provider, has broken down the behaviour of the Mirai botnet. The results show various elements of the botnet behaviour, some of which can be measured as metrics. First, bots will perform scans on the entire IP-address range, except for a limited set of IPs such as the network of the Department of Defense. The metric can be measured by recording the destinations of outgoing packets. Second, the method used by Mirai bots to infect new hosts is by attempting a known list of username/password combinations. By recording attempted logins, an attack by a Mirai bot can be detected, and the risk of infection increases. The metric would describe the number of attempted logins using credentials from this list.

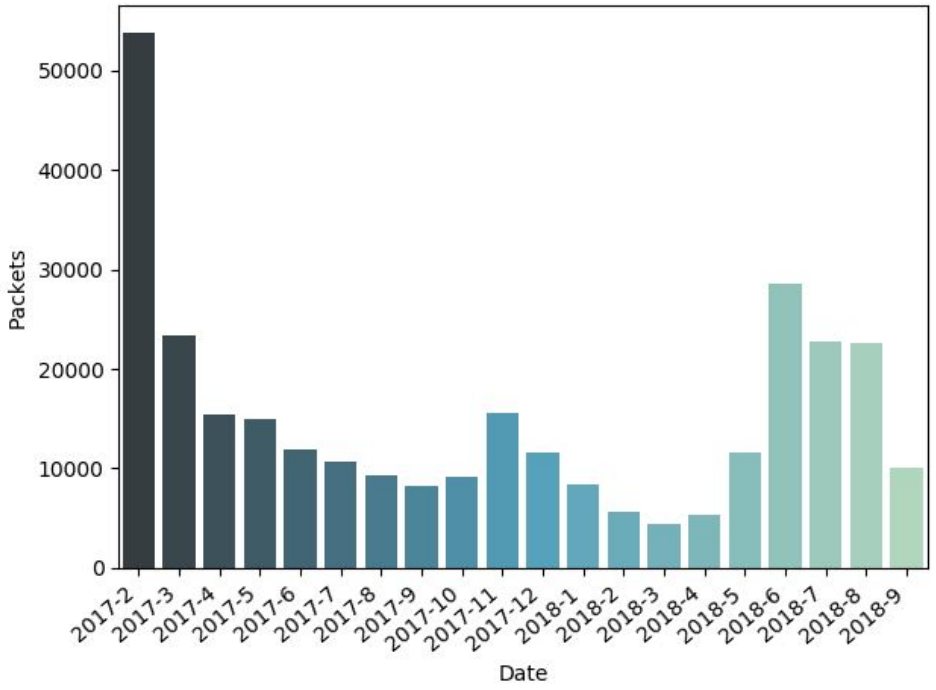
Metrics designed from the dataset

The type of these metrics is *incidents*, because the dataset contains incidents of mirai packets being sent. The data is thus related to the threat environment.

1. Number of infected IP sightings per country (normalized for machines in country?)
   Roughly shows the hosts which are targeted to become part of a mirai botnet.
2. Rank of normalized infected IP's per country
   Estimates how well one country's security policies hold up against other countries, although other factors such as attacker intention also could influence this metric.
3. Number of new infected IP sightings over time
   Gives an idea on how fast mirai-like botnets are spreading to new hosts, it also can help determine if new vulnerabilities are used when spikes of newly infected IP's are seen.
4. Number of infections per ASN normalized to ASN size over time
   Measures which ASN's are actively maintained by the botnet manager.
5. Amount of infections over country and time
   Can show if there are specific timed attack against specific countries.
6. Spread of infection through world over time
   Gives a nice total overview of the activity involving mirai-like botnets over time.

Evaluating the Metrics





References

[1] A Survey of Botnet Technology and Defenses - M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir
[2] Akiyama, Mitsuaki et al. “A Proposal of Metrics for Botnet Detection Based on Its Cooperative Behavior.” 2007 International Symposium on Applications and the Internet Workshops
[3] Manos Antonakakis et al. “Understanding the Mirai Botnet”. 2017 USENIX Security Symposium
[4] Imperva Security, Online Technical Analysis, https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/