

Assignment #1

Design of Secure Computer Systems

Anton Claes

0300042110

CEG4399

University of Ottawa

September 25th, 2017

## Assignment # 1

One of the most impressive attacks performed recently is the attack against the Dyn company. Dyn's main business is Domain Name Servers management. The company hosts canonical website names in its DNS servers and provides the corresponding IP addresses to the users performing DNS lookups on these sites. The attack against the Dyn company occurred on October 21st, 2016 and targeted Dyn's DNS servers.

The attack is a Distributed Denial of Service (DDoS) Attack : "A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems", Specht (2004). Although DNS servers are usually designed to handle huge amounts of requests, they can be taken down with enough devices attacking at the same time.

What's interesting in this kind of attack is that the breach is not inside the attacked system itself, but in the compromised devices attacking it. According to Dyn's report, the attack was caused by a botnet called Mirai, which infected a 100000 endpoints, which performed 2 attacks on that day (One in the morning, the second one in the afternoon)(Hilton (2016)). The Mirai botnet is a malicious piece of software that targets Internet of Things (IoT) devices. Mirai uses the fact that a lot of these devices are poorly secured and were left with default passwords (Antonakakis et al. (2017), p. 7). Thus, to infect other devices and spread across the network, Mirai has a table storing default passwords for devices. It then scans the network and once it has found a host, it tries to log into it with one of the passwords stored in the table. It is then able to replicate itself in the device. (Antonakakis et al. (2017), p. 2).

Once the botnet is widely spread across the network, all the devices perform DNS

queries on the Dyn's servers at the same time, thus generating huge bandwidth : "Early observations of the TCP attack volume from a few of our datacenters indicate packet flow bursts 40 to 50 times higher than normal", Hilton (2016).

This attack caused major disruptions accross the internet : "The incident took offline some of the most popular sites on the web, including Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest and Fox News", Thielman, Johnston, and Ackerman (2016). Although the websites being inaccessible do not cause data loss or privacy issues, it obviously represents a huge money loss, especially for companies like Spotify which only source of revenue is through the internet. For the Dyn company, there weren't any long-term consequences neither : "we were able to substantially recover from the second attack by 17:00 UTC", Hilton (2016).

Interesting fact about this attack, it is not due to a true design error, but it's been made possible by people not changing their default passwords. Although it's arguable that compromised devices manufacturers could have designed their products to force password change on install, or delivered all devices with different random passwords, they can not really be blamed for not having done it. Users cannot be blamed neither, because changing passwords is wise, but not mandatory. By essence, these kind of attacks are hard to avoid : "During a DDoS which uses the DNS protocol it can be difficult to distinguish legitimate traffic from attack traffic", Hilton (2016). There are, though, attempts in preventing the attacks. This can for instance be achieved with specific firewalls. XFirewall is one of them, it is capable of detecting and dynamically filtering the traffic in case of an attack : "XFirewall is configured with dynamic rules based on traffic analysis. Once the DDoS storm is over, XFirewall is removed.", Aljuhani, Alharbi, and Liu (2017), p1-2. Another solution is to monitor the traffic

closer to the attacker's side.

[add other solutions]

To conclude, this attack, by directly targetting the Dyn company, also indirectly attacked all the companies which canonical names were hosted by Dyn. Considering how many big companies were impacted, and even if the attack lasted only one day, it can be considered one of the major attacks that occurred on the internet these days. By using the weakness of poorly secured devices, it was able to compromise a huge part of the web for one day. Although solutions exist against these attacks, they can be hard to implement and they may not always be efficient. The main issue to be addressed in the first place is probably the compromised IoT devices, because it was millions of them, which can not be considered a small issue.

## References

- Aljuhani, A., Alharbi, T., & Liu, H. (2017). Xfirewall: A dynamic and additional mitigation against ddos storm. In *Proceedings of the international conference on compute and data analysis* (pp. 1–5). New York, NY, USA: ACM. Retrieved from <http://doi.acm.org.proxy.bib.uottawa.ca/10.1145/3093241.3093252> doi: 10.1145/3093241.3093252
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Zhou, Y. (2017). Understanding the mirai botnet. In *Proceedings of the 26th usenix security symposium*. Retrieved from <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation>
- Hilton, S. (2016). *Dyn analysis summary of friday october 21 attack*. Retrieved from <https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>
- Specht, S. M. (2004). Distributed denial of service: taxonomies of attacks, tools and countermeasures. In *Proceedings of the international workshop on security in parallel and distributed systems, 2004* (pp. 543–550). Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.4566&rep=rep1&type=p>
- Thielman, S., Johnston, C., & Ackerman, S. (2016). *Major cyber attack disrupts internet service across europe and us*. Retrieved from <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial>