Hack Me If You Can - DDSS Case Study #2

José Donato, donato@student.dei.uc.pt, 2016225043

I. Introduction

In this case study I will approach some aspects referred in the documentary "Hack Me If You Can" [1] (sections II, III, IV, V) and I will give my specific view about each one of them (section VI). Although the documentary had a lot of information and topics I could research about, I managed to choose this four aspects because they are somehow related to each other (all of them are related to cyber attacks and, consequently, to cybersecurity).

II. Homemade viruses with different motivations

DarkComet is a known remote access trojan (RAT) developed by a french programmer with the goal of being recognized and had no malicious intentions [1]. Although, with the spread of this tool, hackers start using it with the wrong intentions. This tool had multiple features going from webcam capture, to key log everything the victim types, check all victim's computer network info, shutdown or restart the computer and much more. All this features are provided with a GUI (graphical user interface) which makes the tool usable by less skilled attackers known as Script Kiddies. BlackShades is another known RAT to control a computer remotely and had similar features with DarkComet. It infected more than half a million computers around the world. But the goal of the creators here was not to gain recognition in the cyber security world but to profit money from the loss of the victims (by stealing their credentials).

III. APT28 - Cyber Espionage Group

APT28 is a russian hacker group most known by the name "Fancy Bear". It is thought that they are related to the russian military intelligence agency GRU. They mainly target goverment organizations. This was the group that attempted to influence the USA elections in 2016 by persuading people on social media using VPNs based in the US, US-based email accounts and stolen US identity documents to back their online identities [2]. In addition to USA, they also attack other organizations on Western Europe (like the attack to TV5Monde referred also in the documentary [1]). This are the reasons that they are thought to work besides the Russian government and their interests [3].

IV. Stuxnet - Government cyberweapons

Despite the negations from the Iran government, lot of countries think their nuclear program is far from peaceful and have malicious intentions (to build a nuclear weapon, for example). That's the reason why US and Israeli intelligence developed a cyberweapon called StuxNet. This virus had the goal of taking control and sabotaging parts of the nuclear program enrichment process by speeding up the Iranian centrifuges. One fifth of the Iranian centrifuges were affected by the virus slowing down the Iranian nuclear program. Recently, was discovered that this virus injection was carried out by a "Dutch mole" on behalf of CIA and Mossad. This was approved by the former US president George W. Bush [4].

V. Cyber Sabotage

Cyber sabotage is a type of cyber attack that has the purpose of sabotage and cause destruction or damage of the victim equipment or information [5]. There are several examples of cyber sabotage, for example: break into a self-driving car and cause it to crash, encrypt sensitive data of a hospital and demand a ransom, etc. Relating to the previous section, Stuxnet was a good example of cyber sabotage. That virus had the purpose of causing damage (sabotaging) to the victim centrifuges. Another example of cyber sabotage happened when in 2015, a cyber attack succeeded to shutdown a power station two days before Christmas. Again, it is thought that Russian government was behind this attack [6].

VI. Thoughts About The Topics

From the first comparison between the two virus (DarkComet and BlackShades), although the first one was made without bad intentions, both end up being used to carry out malicious attacks. The people that use this type of tools for malicious ends need to take consequences for their actions (the BlackShades was sentenced to 57 months of prison [7]).

In the same line of thought, the groups that do cyber attacks like APT28, need to be taken down alongside with the government that is supporting this type of activities.

About the third topic, although the Stuxnet consists on a big cyber weapon for USA, I think their motives were good and beneficial to everyone. In my opinion, the use of this tool from the USA is justified because it was done with the goal of delaying a bad event from happening (delay Iran from building a nuclear weapon capable to destroy other countries).

Finally, I think Cyber sabotage can be good or bad depending on which systems the attack damages. If the attack aims to destroy or damage some system that has the capability of harming other people, cyber sabotage can be justified (for example, the stuxnet situation). On the other hand, if the cyber sabotage has the objective of harming people, like the example of attackers shutting down the power station in the middle of winter, the cyber sabotage is far for being justified and the responsibles must take consequences for their actions and be in jail.

VII. Conclusion

To conclude, I think the documentary [1] illustrates well my opinion, i.e., condemns those who use software for bad reasons and it's greatly done because they always try to back up their ideas with people with high reputation on the area like Eugene Kaspersky (Kaspersky AV founder) or Patrick Hoffman (fbi cyber-service agent).

References

[1] Odisseia. Hack Me If You Can. https://www.youtube.com/watch?v=6JYQUh8QeLg.

[2] Wire. Did Russia affect the 2016 election - It's now undeniable. https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/.

[3] CrowdStrike. Who Is Fancy Bear. https://www.crowdstrike.com/blog/who-is-fancy-bear.

[4] Times of Israel. Dutch Mole - Stuxnet. https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/.

[5] Military. Cyber Sabotage. https://www.military.com/defensetech/2008/02/06/cyber-sabotage.

[6] Rathenau. Cyber Sabotage Attacks. https://www.rathenau.nl/en/digital-society/cyberspace-without-conflict/cyber-attacks-cyber-sabotage.

[7] Pplware. BlackShades senteced to 57 months of prison. https://pplware.sapo.pt/informacao/blackshades-rat-hacker-sentenciado-a-57-meses-de-prisao/.