Hacking Back – Offense/Defense in Enterprise IT Security

Edgar Hurtado Jr

East Carolina University ICTN-4040: Enterprise Information Security

Abstract

One of the many thoughts that travel through the minds of the computer user are these questions, Am I being hacked? Am I safe to open this email? Am I vulnerable to a malware? Unfortunately in today's day and age we are very open to hackers invading our personal privacy and personal values without any high risks for them to be caught and persecuted. There are millions of individuals all over the world currently connected to the internet if either for personal or professional use. Many of those users are providing some scale of defense from outside attacks to the network connection they are on. But can we gather the attacker's intrusion information and attack them back. May we be considered a hacker even though it is to locate and stop that hacker from any future attacks? That will be up to you and I will try to present the views of hacking back being a way to fight the increasing flood of hackers.

Hacking Back – Offense/Defense in Enterprise IT Security

Cyberspace and Its Weakness

In the online web, it is considered by many as the cyberspace where many levels of being are present. It can be changed at any time with a simple keystroke or created with a simple idea, to be shared throughout the World Wide Web. Unfortunately it is also an open playground for the negative involvement of others within your base. Hackers are the criminals that will gain illegal access to your system and control all your personal data. May it be through a simple malware attack or converting your system into a zombie for future use in an attack? There is also the growing use of ransomware that the hacker will take control over your personal data and request ransom before giving you back the access to the system. And even there you have no idea if a virus or other malware has been installed for future use.

Now even though so many of us are connected to the cyberspace for daily use, let it be personal or professional, if we are attacked overnight the government does not have much power to control that side of law breaking. Here is where the use of active defense strategy or “hack-back” comes into play. The Department of Justice will consider it self-defense protecting your assets from an attacking thief. If the thief runs away from you yet you attack, the charge of liability will come down on to you for the crime had been committed and the situation area was considered safe.

In the act of hacking back you do have the chance to catch the hacker in the act but most likely you will notice the crime taking place after your cyber security infrastructure sounds the alarm. As Lin (2016) explained this is where it is viewed

through many groups from the Department of Justice calling it “likely Illegal” to the FBI cautioning the victims from hacking back but stops short from forbidding it. The White House Officials have come to stating hacking back as “a terrible idea”. I view this as only a grey retrospective on the act of hacking back. I see it as taking action into one’s own hands of justice. Sometimes the best defense is having a strong offense, and these are my views on that aspect with regards to business cyber security.

Discussion

As Harrington (2014) referred hack back to being a top-trending technology topic over the past year, and that it would be most likely not be brought under the Computer Fraud and Abuse Act (CFAA) for prosecution. And as Kumar (2017) mentioned there is also a new proposed bill set to amend section 1030 of the CFAA that it will allow victims of ongoing cyber-attacks to fight back against hackers by granting victims more powers to engage in active defense measures to identify the hacker and disrupt the attack. The bill is named “Active Cyber Defense Certainty” (ACDA).

There currently are ways to locate the hacker for this is the toughest area to take into consideration. There is a most cited active defense technique being used called beaconing, as mentioned by Harrington (2014). Here electronic files are enhanced to “allow for awareness of whether protected information has left an authorized network and can potentially identify the location of the files in the event that they are stolen.” This is with a gray area for the methods used by hackers the file location may be that of a botnet or a database framework being used for transport. Here is where a gray line

can be drawn, and why many corporations that use this method of hacking back work with an third party to avoid legal back lash.

The other use of active defense hack back are the honeypots that cyber security frameworks incorporate to create the trap for the hacker. Once the hacker contacts the location and starts to grab information or infect the system, it can be traced and attacked. One gray issue here is the honey pot created a deception opening the eyes of a hacker to compromise the system. As Gross (2017) states, for a hack back response to a cyber-based threat be considered lawful, it must consider how that response action will affect any innocent parties. This will trend closer to being liable for the actions or possibly, if not securely set, will open a path to information dedicated to that corporation due to improper staging.

One view to have is the anticipation for a cyber-attack is just that, anticipation. As stated in the article by InfoSec Institute (2017), “The offensive defense contemplates the possibility to hit attackers with malware that are able to neutralize or power DDoS attacks against control infrastructure.” One of the first governments to publically announce the hacking back as a method to take an active defense strategy against cyber-crime is that of the British. As stated in the article InfoSec Institute (2017), “The strategy of the UK Government has a five-year plan and aims to “work to reduce the impact of cyber-attacks and to drive up security standards across public and private sectors.” Here is a method that I truly agree with even though it does have a gray area on invading private information. Our government has passed and enacted the Rule 41 bill which gives the FBI the right to back hack into any computers within the jurisdiction and not just look into the data but also setup a trace to locate the hacker. This is in

reference mainly to botnets due to some many Distributed Denial of Service attacks as compared to the decline in ransomware attacks. It is also a view as stated by Lin (2016) that hacking back against a botnet can be as simple and nonaggressive as installing security patches into infected computers. The patches may damage innocent hijacked computers but that is a price to pay to counter attack.

Conclusion

One look at the interactive site map depicting the world's biggest data breaches (see Appendix A for detailed layout) you will notice the amazement of attacks that have hit corporations. In this light you can see how week we are and if the use of hacking back could have been implemented in a wider spread within the cyber-security infrastructure, these attacks would decrease. Now there will be innocent victims feeling the hit and also the particular concern that cyberattacks are growing from overseas locations and that is where we lose many rights. But the laws are in the process of being changed or created for this time and age in the world of hackers.

The legality will be changing at an increasing pace especially since the Mirai botnet attack against the DNS Dyn in 2016. Kumar (2016) points out how the discovery of a simple exploit error could have stopped the DDoS flooding by hacking back the IoT botnets and stop the Mirai-compromised devices, in this way stopping the attack. One positive move even though we will constantly be fighting attacks yet hacking back is a strong defense offense being used by both public and private sectors for a good defense is a strong offense. That is they new way to look at cybersecurity infrastructure.

References

Harrington, S. L. (2014). CYBER SECURITY ACTIVE DEFENSE: PLAYING WITH FIRE OR SOUND RISK MANAGEMENT? *Richmond Journal of Law & technology, 20*(Rich. J.L. & Tech.), 12th ser., 1-26. Retrieved from http://www.lexisnexis.com.jproxy.lib.ecu.edu/lnacui2api/api/version1/getDocCui?lni=5D83-H0N0-00B1-80N7&csi=270944,270077,11059,8411&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true

Gross, J. R. (2016). *Hack and be Hacked: A Framework for the United States to Respond to Non-state Actors in Cyberspace, 46*(Cal. W. Int'l L.J.), 109th ser., 1-26. (2016). Retrieved from http://www.lexisnexis.com.jproxy.lib.ecu.edu/lnacui2api/delivery/DownloadDoc.do?delFmt=QDS_EF_WORD60TYPE&fileSize=5000&dnldFilePath=%2Fln%2Fshared%2Fprod%2Fdiscus%2Fqds%2Frepository%2Fdocs%2F8%2F21%2F2827%3A601604218%2Fformatted_doc&zipDelivery=false&dnldFileName=46_Cal._W._Int%27l_L.J._109%2C_&jobHandle=2827%3A601604218

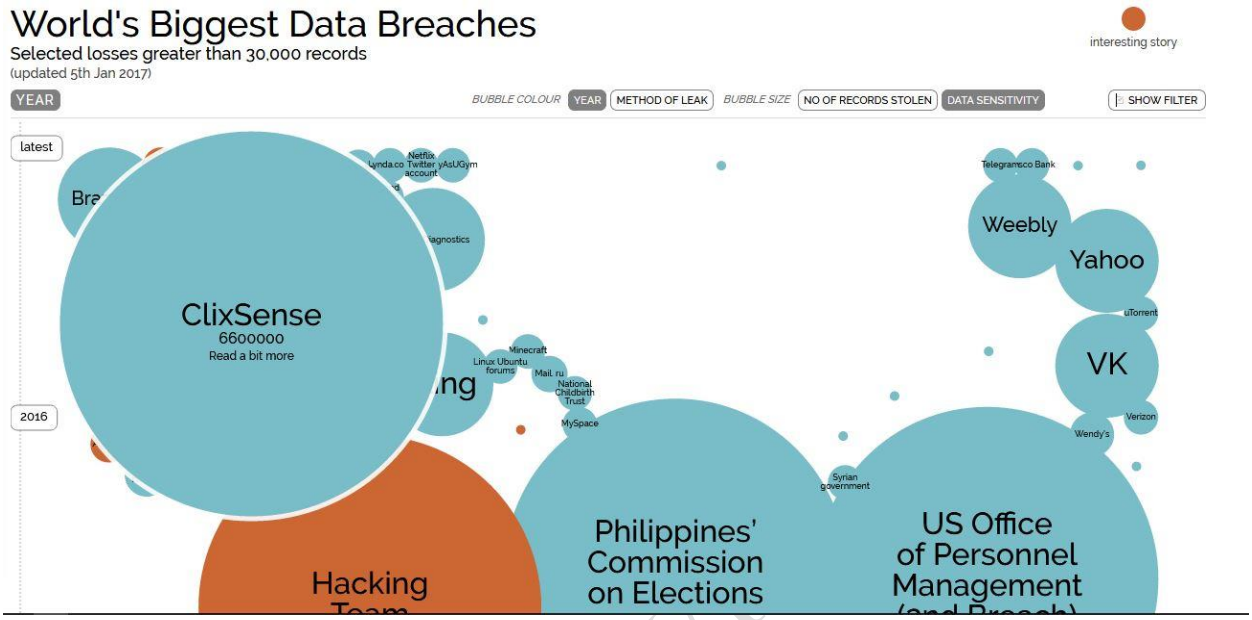
Lin, P. (2016). *Ethics of Hacking Back - Six arguments from armed conflict to zombies* (pp. 1-36) (USA, U.S. National Science Foundation). Retrieved April 4, 2017, from http://ethics.calpoly.edu/hackingback.htm

Hacking Back: Exploring a new option of cyber defense. (2016, November 07). Retrieved April 04, 2017, from http://resources.infosecinstitute.com/hacking-back-exploring-a-new-option-of-cyber-defense/#gref

Kumar, M. (2017, March 08). Proposed Bill Would Legally Allow Cyber Crime Victims to Hack Back. Retrieved April 02, 2017, from http://thehackernews.com/2017/03/hacking-back-hackers.html

Kumar, M. (2016, June 23). STOP Rule 41 - FBI should not get Legal Power to Hack Computers Worldwide. Retrieved April 03, 2017, from http://thehackernews.com/2016/06/fbi-hack-rule-41.html

Appendix A



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/