Hacking Back

James Driscoll

ECPI University

CIS 425: Advanced Defense and Countermeasures

15 Mar 2022

On February 25, 2022, NVIDIA, a video card maker notified the public that they suffered a security incident. A day later an extortion group called Lapsus$ started making statements that they were responsible for the incident and made demands to NVIDIA (Gatlan, 2022). This same day, 26 February, the Lapsus$ made it known that NVIDIA had hacked their server that stored all the data that Lapsus$ had stolen and uploaded ransomware. These criminals ended up calling NVIDIA criminals (Novinson, 2022). NVIDIA hacked back the criminals that hacked them.

In a separate situation there was a US hacker known as P4X that was the victim of a cyberattack by North Korea. He was able to stop the attack and he contacted the US Government afterwards and waited for a response. After waiting a year with no response from the US Government, and his frustration mounting, he decided to handle the situation himself. So P4X, used his expertise and skills and conducted a denial-of-service attack on the limited number of internet connected networks that North Korea has (Greenberg, 2022)

**Hacking Back**

To talk about hacking back, we need to specify what it is. Hacking back is when the victim of a cyber attack hacks into the network of the threat actors that hacked them in the first place. Basically, it is what NVIDIA did in the scenario above. They got hacked and had information stolen. A few days later, they hacked the group responsible. So should companies or individuals that get hacked, hack the threat actors back? The answer to that question is a resounding no. The rationale for this answer will be in the rest of this paper.

There are two reasons this is a bad idea. The most compelling reason companies should not hack back is because they would be accessing computer systems that do not belong to the company, without permission of the owner. That is illegal under the Computer Fraud and Abuse Act (CFAA). Now it is understandable for an individual or company that gets hacked to want to conduct an active defense. The problem with that is under the CFAA an active defense is considered an offensive action (Wolf, 2017).

To skirt around the CFAA, a bill called the Active Cyber Defense Certainty Act (ACDC) was introduced in Congress in 2017. The way it skirts around the CFAA is by creating exceptions that companies can cite that would allow them to go on offense and hack back the threat actors that hacked them in the first place (Wolff, 2017). So, why is all this important? The CFAA is written just like any other law. Parts of it, if not all of it can be subject to interpretation. This explains why an active defense is thought of as offense with defense being working within a companies’ own network and offense being any work done outside of the companies’ network. This means that it is perfectly legal to monitor network traffic, set specific authentication methods for network access, or even encrypt company data because it is on the companies own network (Wolff, 2017).

Now that we have gone a little into the CFAA, lets pivot and investigate the ACDC Act. As stated earlier, this act is an attempt to skirt the CFAA by allowing exceptions so that companies who get hacked can go on offense and hack back those threat actors. This brings up the question of what these exceptions are. This is a legitimate question and one that needs to be explained.

Basically, the ACDC Act would allow the use of beacons. A beacon is nothing more that a piece of code within a file that would start communication with the owner if the file were stolen. An analogy for this would be from the movie “Speed”. There is that part of the movie where the bomber gets his suitcase full of money right after the bus blows up. Well inside the suitcase there was a GPS tracker so the police could stay hidden but still follow him. A beacon is the same thing, but in a digital form. Of course, there are requirements that must be met for this to be considered legal. 1) Locational, or attributional data must be able to be discovered. 2) The beacon must be created on the victim’s system. 3) The threat actor’s system cannot be altered nor destroyed in any way. 4) The code can install a backdoor on the threat actor’s system (Chesney, 2019).

Now, where the ACDC Act differs from the CFAA is that does facilitate offensive security operations if the activity meets one of the following three goals. 1) Determine who the attacker is so law enforcement can be notified. 2) Stop the unauthorized access. 3) Follow the attacker through the network so that new intrusion prevention and defense techniques and procedures can be created (Chesney, 2019). Going back to the scenario at the beginning of this paper, even if the ACDC act had become a law, and there is no evidence that it has, what NVIDIA did would still be considered illegal, under both the CFAA as well as the ACDC Act.

The second reason a victim hacking back their attackers is a bad idea is because unless a company is a cyber security company or employs cyber security personnel, chances are high that they do not have the experience, tools, or defensive measures to facilitate an operation such as this (Crandall, 2018). Their energy would be better spent patching any vulnerabilities, updating software, setting up procedures to detect threats a lot quicker, possibly even reworking their policies and procedures.

**Conclusion**

While companies and individuals have the right to self-defense against an attack, to include a cyberattack, taking offensive actions such as hacking back the attackers is not the way to go about it. Investing in defending the network by taking the steps above is a better answer. As is contacting law enforcement and fully cooperating with them during the investigation.

# References

Chesney, R. (2019, June 14). *Hackback is Back: Assessing the Active Cyber Defense Certainty Act*. Retrieved from LawFare: https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act

Crandall, C. (2018, September 24). *Hacking Back: Simply a Bad Idea*. Retrieved from Dark Reading: https://www.darkreading.com/threat-intelligence/hacking-back-simply-a-bad-idea

Gatlan, S. (2022, February 25). *GPU giant NVIDIA is investigating a potential cyberattack*. Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/

Greenberg, A. (2022, February 2). *North Korea Hacked Him. So He Took Down its Internet*. Retrieved from Wired.

Novinson, M. (2022, February 26). *NVIDIA Hacks Rnsomware Gang Back to Block Data Leaks, Group Claims*. Retrieved from CRN: https://www.crn.com/news/security/nvidia-hacks-ransomware-gang-back-to-block-data-leaks-group-claims

Wolf, J. (2017, July 14). *When Companies Get Hacked, Should Then be Allowed to Hack Back?* Retrieved from The Atlantic: https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/

Wolff, J. (2017, October 17). *Attack of the Hack Back: The Worst Idea in Cybersecurity is Back Again*. Retrieved from Slate: https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html