Internet Crime Attribution – Past, Present, Future

Even as some of us, a dwindling and sometimes extinct few, strive toward a perfect world, as long as humans reside on Earth, the world cannot be perfect. Ideally, in this world continually consumed by cyberspace, information security would not only react to cyberspace criminals, but create a wall of deterrence, neutering the attack as soon as the criminal creates the malcontent thought. With the age old tale of prediction versus reaction, either entity can seize an upper-hand in a battle with the information that prediction can potentially provide; that is, if they can predict correctly. Sun Tzu said in *The Art of War* “For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill” (JFQ 75). With the additional accreditation of prediction and deterrence as the epitome of battle tactics, Clorinda Trujillo representing Joint Force Quarterly (JFQ) defines deterrence as the prevention of action simply caused by the existence of a worthy threat of unacceptable counteraction or that the cost of action outweighs the perceived benefits (JFQ 75). Before deterrence can become a fully grown defense structure, being able to quickly identify the attacker is vital. This step is called attribution, if security experts are to one day predict an attack, opposed to always reacting to one, they must understand their enemy better than their enemy does. As we all move towards Internet-based industries, it’s worth uplifting the vision that one day we’ll be able to instantaneously react, defer and attribute lowly or sophisticated attacks even if we have not seen those attacks previously. With that idea in mind as a reference to the potential of this field, the previous accounts of cyber attacks are just as critical to understanding the techniques of the Internet criminal.

Any real internet crime relations are referred to after the 1970s because the first tangible evidence that the Internet had been created was in 1969, where four host computers were connected to form the initial ARPANET (Leiner). In 1971, John Draper creates a “blue box” from a whistle in a Cap’n Crunch cereal box that made wire fraud and free calls possible (Wavefront). The instructions to operate and create these free calls were published by Esquire magazine (Price). Not only did Draper make a dramatic impact on the raise of wire fraud rates, he was recognized for this feat and given the nickname Captain Crunch. When it comes to Internet crime accreditation and attribution, there are criminals that want to be identified and those who want to remain unidentified. Criminals or thieves such as Draper are not entirely interested in personal profit, as the profit gained from creating free calls for himself would have been negligible. Within the year, Esquire magazine wrote about Draper, further glorifying his creation and probably entitling his ego with a “watch what I can do with a toy found in a cereal box” mentality. As we enter the 1980s, attribution is still prominent and Ian Murphy, aka. “Captain Zap”, is the first felon of a computer crime. Murphy broke into AT&T’s computers to change the time schedule, so that many people would receive discounted rates at normal business hours; this as opposed to discounted rates at off-business hours (Wavefront). A stunt like this shows weaknesses in a company’s system, the appeared to be unfairness of business strategy, and that even an accredited criminal can be convicted. In 1986 “BRAIN”, originating from Pakistan, is considered the first and oldest known virus on the PC, affecting IBM computers (F-Secure). This virus was likely created to look at something on a computer or simply prove that it can be done, as it was relatively harmless. Regardless of the intent, this shows that malicious creators can spread viruses while not actively engaged. When viruses are created by eager-minded people, even if for them it is simply a matter of pride, it shows the rest of the world what’s possible. Others, who are less likely to create earth-shattering viruses and rootkits, can merely copy or replicate that excellence. As conviction rates rise and at least some laws or acts are created, nicknames and Internet aliases such as Captain Zap are becoming a thing of the past. Although sometimes a criminal will overstep their bounds and attempt, and succeed, to steal millions of credit card information records from major companies (and still not get caught), slipping under and the radar and recreating others’ work for a personal profit is what we are likely to see more of as we move toward today’s cybercrime.

Cite

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. “Brief History of the Internet.” *Internet Society*. Internet Society, 15 Oct. 2012. Web. 30 Nov. 2014. <www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Timeline>

Trujillo, Clorinda. “JFQ 75 | The Limits of Cyberspace Deterrence.” *National Defense University Press*. NDU Press, 30 Sept. 2014. Web. 30 Nov. 2014.

“A Brief History of Crybecrime.” *Wavefront*. Wavefront Consulting Group, (Winter, 2014). Web. 30 Nov. 2014. <www.wavefrontcg.com/A\_Brief\_History\_of\_Cybercrime.html>

Price, David. “Blind Whistling Phreaks and the FBI’s Historical Reliance on Phone Tap Criminality.” *Counterpunch*. CounterPunch, 30 June 2008. Web. 30 Nov. 2014. <www.counterpunch.org/2008/06/30/blind-whistling-phreaks-and-the-fbi-s-historical-reliance-on-phone-tap-criminality/>

“BRAIN: Searching for the first PC virus in Pakistan.” *F-Secure: Protectring the irreplaceable.* F-Secure, (2011). Web. 30 Nov. 2014. <campaigns.f-secure.com/brain/virus.html>