A Suggested Approach for Detecting, Containing and Mitigating Intruders’ Actions on an Attacked System

David Maimon University of Maryland

Cyber-dependent crimes are offenses that can only be committed by using a computer, computer networks, or other forms of Information and Communication Technology, and include hacking, distribution of malware and DDoS attacks (Furnell et al 2015). These attacks have become a common global problem. Acknowledging the potential risks these cyber-attacks pose to large organizations (both governmental and private) and to private Internet users’ privacy, substantial research and security efforts have been devoted to developing technical tools that aim to prevent the occurrence of cyber-attacks. For example, firewalls and Intrusion Detection/Prevention Systems are commonly used by large organizations to prevent the development of cyber-dependent crimes (Bace and Mell 2001). These tools are designed to detect attacks at a fairly early stages of the cyber-kill-chain (i.e. reconnaissance, weaponization, delivery and exploit (Khan et al 2018)), prevent them from developing, and provide useful information for IT managers who are responsible for recovering from cyber-dependent crimes. However, the effectiveness of these (and other) tools in achieving their goals is relatively unknown, as rigorous scientific evidence regarding the performances of these tools in the wild is relatively scarce.

Since the effectiveness of existing cyber-security tools in preventing the development of a cyber-attacks is still questionable, I posit that it is equally important to develop tools and approaches for disrupting intruders’ attempts to obtain their malicious objectives on an attacked systems/networks. Specifically, I call for the adoption of a human-focused cyber-security approach in the design and configuration of technical tools that will focus on later stages of the cyber kill chain (i.e. installation, command and control and actions on objectives). I contend that such approach could (1) increase the rate of intruders’ detection while engaging with an attacked system, and (2) mitigate the consequences of the attack to both the attacked device and the victim. This approach should draw on soft science models and rigorous empirical evidence regarding intruders’ online behaviors and responses to “embedded nudges” during the progression of malicious events.

Indeed, the relevance of adopting soft science models in guiding the security configuration of computing environments and directing the implementation of security policies has already been discussed extensively in the cyber-security literature (Pfleeger and Caputo 2012; Coles-Kemp and Theoharidou 2010). Unfortunately, developers of technical solutions (for example anti-virus software, firewall) tend to ignore insights drawn from soft science models when designing and deploying these tools. Moreover, to date, none of the existing models have been employed to explain how a cyber-attack progresses once attackers experience different situations and configurations of the attacked system. I believe that either the use of existing models (for example deterrence, situational crime prevention, etc.) or the development of a unique new model is of utmost importance for the cyber-security filed since it can support the development of environmental interventions that could mitigate consequences to crime victims.

In addition to drawing on the extensive body of literature available in the social sciences regarding the embeddedness of human behaviors in contexts, there is a need to collect as much data as possible on attackers’ behaviors during their engagement with attacked computing environments. I propose that such data collection efforts should be done in the field, and implement either experimental or quasi-experimental research designs. Experimental designs are research designs that use random assignment to the treatment and control group(s). Quasi-experimental designs are research designs that address selection bias in the experimental and control group(s) through the use of multivariate statistical methods or a matched-subject research design. Previous research which adopted such research designs has already found that a warning banner in an attacked computer substantially reduced the use of both navigation and change file permission commands on computers attacked by system trespassers who did not take administrative privileges (Testa et al 2017), and that the presence of a surveillance banner in the attacked computer systems reduced the probability of commands being typed in the system during longer first system trespassing incidents (Wilson et al 2015).

In sum, although the focus of cyber security research has been traditionally on prevention of cyber security events, the effectiveness of current cyber security tools in disrupting the early stages of the cyber kill chain is unknown. The underlying premise that guides this paper suggests that although Cyber-Dependent-Crime could not be prevented completely, its consequences to victims could be mitigated and reduced. However, in order to design computing environments, tools and policies, that are effective in mitigating victims’ harm, there is a need to integrate knowledge from soft science models and produce rigorous scientific research around intruders’ online behaviors during the last two stages of the cyber-kill chain.
References:

Bace, R., & Mell, P. (2001). *NIST special publication on intrusion detection systems*. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.


