ALSTON & BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JANUARY 11, 2013

Legal Issues with Emerging Active Defense Security Technologies

By: Kim Peretti and Todd McClelland
Contributors: Jarrett Elis and Maki DePalo

Introduction

Ten years ago, a typical cybercrime case involved a solo hacker gaining unauthorized access into one or a small number of systems for idle curiosity. The crime was detected quickly (usually by intruder bragging) and fixed with relative ease. Today's brand of cybercrime, however, has evolved, producing threat groups and actors that are a world apart from the prototypical attack of a decade ago. While some groups and actors are believed to be backed by foreign governments, others are backed by organized crime, are acting for a quasi-political purpose (e.g., "hacktivists") or are entirely independent. No common set of facts or descriptions can be garnered about these groups and individuals since their motives and means vary widely.

These advanced groups have the capability to conduct targeted, well-orchestrated, sophisticated, prolonged and repeated attacks on businesses and government entities. These incidents are often not detected until months—sometimes even years—after the initiation of the attack, and the response can take days, weeks or months to contain and remediate. On top of this, once the attack is thought to be contained or eradicated, there is no promise that the intruders won't return.

Current Technologies and Strategies

Today's most deployed defensive strategies and technologies, including passive (host-based) countermeasures, have a variety of limitations that substantially limit a company's ability to identify or take meaningful actions against their assailants, creating what is known in the information security industry as the problem of "attribution." Attribution allows individuals or groups to be held responsible for their criminal acts. It also potentially provides the victim with valuable information about the motives and acts of the intruders in their system, and how to get them out and keep them out. Without attribution, a victim is left with few practical means to prevent, with a high degree of confidence, the reoccurrence of a successful attack by a determined group or individual.

Without question, corporate victims are growing increasingly frustrated with the few defensive options at their disposal. They are also not satisfied with the new defensive mantra, advocated by the Pentagon and other industry leaders, that companies should act as if and with the assumption that the new "normal" is a state of constant and ongoing infiltration.[1] Instead, the general approach is to bolster perimeter defenses, harden application security, increase network traffic monitoring, scan for malware, respond when something is detected . . . and hope for the best.

---

[1] *See* Joseph Menn, "Hacked Companies Fight Back with Controversial Steps," Reuters, June 17, 2012, http:////www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617 (noting that many large security providers no longer advocate that keeping intruders out is paramount. "Instead, they adopt the more recent line taken by the Pentagon, which is to assume that hackers have gotten inside and will again.").

Next Generation Defense Technologies

Recognizing the limitations of today's defensive technologies, new technologies and methods are emerging that are more active, cunning and aggressive in defending against attacks and identifying the intruder. These technologies, however, are pushing the bounds of what is commonly understood as "legal." Indeed, some emerging technologies have rekindled a heated debate around what actions a nongovernmental entity can take on its own to identify the perpetrator, stop an ongoing attack and ultimately protect the entity's systems.

These new technologies deploy concepts that have been used by governments since the beginning of the spy-counterspy business—counterintelligence, and to an extent, counterespionage.[2] Preferably[3] referred to as "active defense," but also called "strike-back" or "hack back," these new technologies represent a range of activities such as:

- honey pots – decoy systems designed to lure intruders to a controlled environment from which to observe their behavior;
- disinformation campaigns and data obfuscation – distributing false information in ways in which the perpetrator is likely to obtain it;
- altering malicious code used in an attack to assist the victim; and
- offensive cyber hacks into the intruder's computer to identify stolen digital assets and the intruder.

A Legal Gray Area?

As noted above, there is considerable ongoing debate as to whether an individual or company can legally deploy many of these active defense technologies.[4] These legal issues are not new, but are resurfacing because of the recent surge in active defense security offerings and their expanding use.

The primary federal statute applicable to computer-related offenses is the Computer Fraud and Abuse Act (CFAA).[5] The CFAA lists seven categories of computer-related offenses, two of which, Sections (a)(2)(C) and (a)(5), are most pertinent to active defense technologies.[6]

---

[2] Collectively, these technologies employ mechanisms that both identify, penetrate or neutralize intruder operations and use cyber means as the primary tradecraft methodology. See Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Pracitioners*, 3945 (2001).

[3] At least by those who are trying to sell or use these technologies. The optics for the term "hack back" has obviously negative connotations.

[4] This article does not attempt to address the ethical or legal issues with regard to a government entities' ability to deploy these same technologies. The U.S. government's actions to date assume that such means are properly within its powers.

[5] 18 U.S.C. § 1030. The statute was originally enacted in 1984 as part of the Comprehensive Crime Control Act of 1984. Two years later, the statute was amended and enacted as the Computer Fraud and Abuse Act of 1986 and has since been amended eight times, with the most recent set of amendments in 2008.

[6] 18 U.S.C. § 1030(a)(2)(C), (5).
(a)(2)(C) whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . information from any protected computer;
(a)(5) whoever
(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

In general terms, the CFAA is an anti-trespass law. A person or company[7] who intentionally accesses a computer or who knowingly or intentionally causes damage[8] to protected computers,[9] without authorization, violates the statute and can be subject to both criminal and civil recourse.

Much of the analysis and debate as to whether active defense technologies are prohibited by the CFAA centers on the meaning of the term "authorization." Unlike the activities of law enforcement personnel, there is no carve-out in the statute that expressly allows private parties to access a third party's computer for some other legally recognized purpose. There is absolutely no authorization expressly recognized in the statute for a private party to access a third-party computer for self-defense purposes or to identify, pursue or retrieve stolen property. In addition, while several cases have interpreted the statute in the context of prosecuting criminal hackers[10] and employees and others who exceed their authorized access to systems,[11] none have interpreted this statute in the context of a person who is a victim of a hack and deployed active defense technology. Under a strict reading of this statute, an individual who traces his/her stolen property to a server and accesses the server without authorization to view this information would appear to violate the statute.

Of course, the analysis does not end there. While the heavy tendency is to view the CFAA in real property terms, applying trespass and similar concepts, this statute applies to cyber assets, an entirely different paradigm that requires flexible and evolving consideration. Taking away the real property concepts and considering the policy implications of this law, a number of interpretation opportunities arise that might allow some of the more questionable active defense technologies. For example, even though there is no Castle Doctrine-type exception in the statute, does a hacker nonetheless implicitly grant authorization to a hack back when that person infiltrates a victim's systems and exfiltrates digital assets? Is authorization a binary concept, for which permission is or is not granted? If a person truly has control over the code in his/her systems, can a tripwire be written and deployed that sends a beacon back to the attacker who steals that code? Recognizing the many potential policy benefits of allowing for limited and targeted active defenses,[12] does authorization somehow otherwise arise?

Today's typical cyber incident often touches systems located in multiple jurisdictions. For example, an attacker may be located in one country, may use one or more command and control computers in other countries (often being innocent and unaware third parties), and may access the victim's systems in yet another country. Accordingly, any analysis of active defense technologies must take on a global compliance perspective that considers foreign laws and treaties, not to mention the possibility of an international incident, regardless of the legality of a given activity. For example, close to 50 countries have signed and/or ratified the Council of Europe's Cybercrime Convention, which calls for similar criminal offenses to the CFAA.[13]

As described above, the current challenges posed by sophisticated threat actors have renewed the ongoing debate on whether and to what extent certain activities by the victim may be legally permissible. The debate largely centers on the definition of "authorization" (which is not defined in the CFAA) and its application/interpretation to both data and computers,

---

7 Importantly, the statute excludes from coverage lawfully authorized activities of law enforcement and intelligence agencies. 18 U.S.C. § 1030(f).

8 "Damage" is broadly defined to include "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

9 A "protected computer" includes any computer used in or affecting interstate or foreign commerce, which is easily satisfied if a computer is connected to the Internet. *See* U.S. Department of Justice, *Prosecuting Computer Crimes*, 4, http://www.justice.gov/criminal/cybercrime /docs/ccmanual.pdf.

10 *See United States v. Morris*, 928 F.2d 504 (2d Cir. 2001); *Sony Computer Entm't Am LLC v. Hotz*, No. CV11-0167, 2011 WL 347147 (N.D.Cal. Jan. 27, 2011); and *T-Mobile USA, Inc. v. Terry*, 862 F.Supp.2d 1121 (W.D. Wash. 2012).

11 *See Int'l Airport Ctrs, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009); and *United States v. Alfred-Adekeye*, [2011] No, 25416 (Can. B.C).

12 While these questions assume a certain bit of discretion and surgical precision in the hack back activities of the victim, "scorched earth" and system-wide disabling strike-backs would seem to exceed the authority in any reasonable interpretation that might implicitly arise.

13 Council of Europe Convention on Cybercrime, Nov. 23, 2011, http://Conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

and whether there may be a common law defense of property right, like the Castle Doctrine, available in some forms of "hack back" activities. Private entities considering active defense technologies or activities, however, should be well aware that there are no cases to date that have interpreted the CFAA in a manner desirable to those who would engage in such activities. While these novel legal theories on how "authorization" could be stretched are compelling (at least from a public policy perspective) and remain mostly academic at this point, no company and no individual wants to have their liberty and criminal and civil liability hinge on these unproven theories. Clearly, this is not an area to tread lightly upon.

Conclusion

Companies caught, or that reasonably could be caught, in the unfortunate position of being targeted by sophisticated cyber threat actors should embrace the creativity that some of these technologies can afford in protecting their systems and removing the threat. However, due to the relative uncertainty of some of these technologies, both in and outside the United States, we suggest the following in your approach to these new technologies:

- Don't assume these technologies are legal. Just because a company, perhaps even a reputable and established company, offers the technology, don't assume it complies with all applicable laws. You don't want to be the company or the individual a prosecutor chooses to make an example out of for the rest.
- Remember that what may be legal in the United States is not necessarily legal outside the United States. Multiple legal regimes may apply to your analysis.
- Involve counsel early, preferably before signing up to the technology, but absolutely before deploying the technology.
- Make sure to fully understand how a technology works before it is deployed.
- Recall that the legal analysis for what the government and its agents can do is a vastly different analysis than what private sector companies can do.

While active defense technologies may be compelling complements to today's passive countermeasures, companies and individuals are well advised to pause and seek counsel before plunging into a legally questionable approach. Our attorneys have been counseling both providers and users of these technologies for a number of years. Our Security Incident Management and Response (SIMR) team has many attorneys who are thought leaders in the deployment of active defense technologies, and other practical and inventive information security practices. Please contact any of the attorneys below to learn more.

Security Incident Management & Response Team Co-Chairs

Kim Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com