INTELLIGENCE & NATIONAL SECURITY SUMMIT

Active Cyber Defense: Whether or Not to Hack Back
Breakout Session

Overview

Active cyber defense (ACD) is a proactive and preventative approach to cyberattacks that seeks to provide cyber defenders with capabilities to discover, analyze and mitigate threats quickly. While ACD enables defenders to disrupt attacks as they happen, its capabilities are exclusively defensive and only affect networks where they have been installed. ACD allows enterprises to detect and prevent zero-day attacks and leverage the capabilities already built into their networks. However, ACD capabilities are, for now, largely restricted to DoD-controlled cyberspace, leaving many firms alone to secure their networks against sophisticated adversaries.

Summary

Speakers examined options private companies have for securing their networks against cyber criminals backed by nation-states. While statutes generally preclude government agencies and private companies from ‘hacking back’ to recover lost data, it is not entirely clear how some active cyber defense activities – such as “beaconing” data so it “calls home” in case of theft – might be treated under the law. Panelists went on to provide guidance on how companies should react to cyber breaches.

Panelists

- **Rich Boscovich**, Assistant General Counsel, Digital Crime Unit, Microsoft
- **Glenn Gerstell**, General Counsel, NSA
- **Adam Hickey**, Deputy Assistant Attorney General, Department of Justice
- **Wyatt Hoffman**, Sr. Research Analyst, Cyber Policy Initiative, Carnegie Endowment for International Peace
- **John Carlin**, Partner, Morrison & Foerster, (moderator)

Key Takeaways:

- The "global cyber pandemic" will get worse before it gets better: losses attributable to cyber mischief will approach $8 trillion over the next five years.
- The Internet of Things (IoT) and 5G will increase attack surface area greatly, as 5 million more devices are connected to the Internet every day.
- The FBI can assist firms that had data stolen and are considering 'hacking back' to recover it.
- It is USCYBERCOM's, not private companies', responsibility to disrupt adversaries.
- Microsoft disrupted cyber adversaries by using botnets, which allowed the company to map out malicious actors' command and control structure, understand their malware, and identify legal frameworks (such as seizing domains used by hackers) that would disable their ability to attack.
- The Computer Fraud and Abuse Act explicitly states there is no free pass for hacking back. Panelists agreed, unanimously condemning full-blown hack-backs intended to cause damage to, or steal data back from, hackers' infrastructure.
- Buying back stolen data on the Dark Web presents issues: You could unwittingly (and illegally) pay a sanctioned nation-state like Iran or North Korea, for example, or you could (illegally) buy stolen data that actually belongs to a third party.
- Market forces can put pressure on shady domain hosters. Spreading the word, rather than hacking back, is often more effective.
- Even passive responses like placing beacons on data may run afoul of the law, as beacons cause another entity's infrastructure to take an action.
- ACD should not even be considered by organizations until they have taken the full range of steps to ensure good cyber hygiene, in which case "self-help" may be the next logical step. Firms that have not instituted basic cybersecurity should not undertake – and may have less legal basis for undertaking – ACD measures of questionable effectiveness and legality.

Recommendations

- Do not hack back. It rarely works, and it can easily lead to unanticipated actions that can place a firm at legal risk.
- The private sector needs to recognize that the NSA does not have responsibility for their networks. It needs to make further investment in security, especially as the IoT and 5G will expand attack surface area exponentially.
- When firms believe data may have been stolen, they should reach out to the FBI rather than take actions to locate or recover their data.
- Government must share tools for permitted ACD activities with industry rather than just provide indicators of compromise.
- Sharing malware code is a good technique for reverse engineering attacks and identifying ways to boost cyber defenses.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. A 501(c)(6) membership organization, INSA strives to identify, develop, and promote collaborative approaches to national security challenges. INSA has more than 160 organizations in its membership and enjoys extensive participation from leaders and senior executives in the public, private, and academic sectors. Learn more at www.INSAonline.org.