3Qs: Analyzing the cybersecurity threat posed by hackers

June 5 2012, By Casey Bayer

Two weeks ago, Anonymous, a global group of hackers, successfully infiltrated the Department of Justice's system and released stolen data. At the same time, al-Qaida, the international terrorist organization, released a video calling for an "electronic jihad" on the United States. Northeastern University news office asked Themis Papageorge, an associate clinical professor in the College of Computer and Information Science, and the director of the college's information assurance program, to analyze the threat posed by rogue hacker groups and what the U.S. government can do to protect itself against future attacks.

This isn't the first time the Department of Justice was hacked. What do groups such as Anonymous accomplish by hacking into these networks and releasing data? What is the motivation behind their attacks?

Groups like Anonymous are becoming a critical threat to society and national security: They attack government, public and private companies, and individuals' networks and computer systems multiple times every day. When they breach a computer system they steal data and many times install malicious software programs that, unbeknownst to the systems' owners, allow for future access by the hackers and continuous leaking of confidential data.

Stolen data can vary from proprietary product information and other intellectual property to national-security data. Anonymous and similar groups can embarrass a government or a company by breaching its networks and computer systems and can also gain financially by selling the stolen data.

The motivation of hacker groups such as Anonymous is a key component of the threat analysis that we teach in information assurance courses at Northeastern. Threat agents, such as Anonymous group members, are motivated by many factors, ranging from personal gain to revenge, peer recognition, curiosity, and crime; to political, religious and secular influence; and potentially to terrorism and national military objectives. We train our students to assess the cybersecurity risk posed by each group by ranking these motivation factors.

What can government do to thwart future breaches? What challenges do federal entities face in protecting themselves from hackers?

We need to defend more effectively against such groups, both from a technical capabilities perspective as well from a contextual perspective. Government and public organizations need to consistently implement risk-based technical countermeasures and controls for networks and computer systems, along with policies and user awareness.

Many times a cybersecurity control, such as a software patch, may be available for months before it is impliemented. People can be our most capable firewall by training employees to defend against social engineering. It is important to know not to click on a malicious attachment in an email and not to provide confidential information to an unidentified telephone caller. User training and awareness are some of the valuable components in security risk management.

The greatest challenges facing federal entities come from a limited knowledge of the threat agents' modus operandi.

Since the attackers have the advantage of choosing the method and time of attack, federal agencies could make risk-based decisions by defending against the most damaging attacks only by having access to a comprehensive and current data set of attacks and methods. This can be accomplished by sharing attack and method data and scenarios across federal agencies and public companies. This strategy would help build effective network and computer system security controls, countermeasures, policies and incident response strategies.

Al-Qaida has called for an "electronic jihad," promoting attacks on a range of online targets. Is there evidence that a network of al-Qaida operatives could plan coordinated attacks?

Al-Qaida has a well-documented record as a terrorist group with multiple physical attacks. In terms of organizational structure, hacker groups have been a collection of individual threat agents with networking abilities (initially using the Internet and also later technologies such as Peer-to-Peer and BitTorrent) to talk about their exploits and share malicious tools. Al-Qaida is reported to have a hierarchy but seems to operate as a network of semiautonomous cells of threat agents whose actions are thus even more difficult to predict and stop.

Therefore, if al-Qaida were to acquire the technical capabilities of a hacker group such as Anonymous, they would be a very credible and high-risk cybersecurity threat. Planning and executing coordinated attacks in the cybersecurity domain is very different from executing attacks in the physical security domain, because the space and time constraints of physical attacks are considerably reduced in the cyber

domain. It may take weeks or months to plan a cybersecurity attack, but it could only take a few minutes to launch a denial-of-service attack, using a botnet of computers belonging to unsuspecting companies and individuals, and potentially bring down a component of critical infrastructure.

Provided by Northeastern University