RSA Conference 2016

Learning Labs

Live Cyber-Exercise: Responding to National Crisis

Post-Conference Summary

A sophisticated cyberattack is in progress against the United States. Multiple industries are impacted and things are about to get much worse. How will government and industry work together with international partners to face the challenge and respond to an adaptive and innovative adversary?

Facilitators:

Dmitri Alperovitch
Co-Founder and Chief Technology Officer, Crowdstrike
Senior Fellow, Atlantic Council

Jason Healey
Senior Research Scholar, Columbia University SIPA
Senior Fellow, Atlantic Council

Overview

Defense Secretary Ashton Carter visited a cyber wargame run by Nonresident Senior Fellows from the Atlantic Council at this year's RSA Conference, the largest global cybersecurity conference.

Atlantic Council Nonresident Senior Fellows Jason Healey, Senior Research Scholar at Columbia University, and Dmitri Alperovitch, Co-Founder and Chief Technology Officer (CTO) at CrowdStrike, along with Beau Woods, Deputy Director of the Atlantic Council's Cyber Statecraft Initiate, held a cyber crisis simulation, which included senior US government officials from the Department of State, Department of Defense, White House, and Department of Justice, as well as industry cybersecurity executives and experts.

Scenario Summary

The live cyber-exercise explored the consequences of Islamic State of Iraq and al-Sham (ISIS) gaining increasingly sophisticated cyber offensive expertise, and provided important lessons for how governments can respond to non-state actors in cyberspace.

Four groups were involved in simulating responses during the wargame:

- US government team
- Private-sector team
- International team featuring former top British and Australian government officials
- Adversary team made up of former US government officials playing the role of ISIS to bring another level of interactivity to the game

During the simulation:

1. ISIS compromised driver's license databases within the US and several European countries
2. The terrorist group later used the information to launch a spear-phishing campaign against US and European banks, as well as the United States' Transportation Security Agency (TSA)
3. This spear-phishing campaign introduced malware that executed a ransomware and wiper attack, affecting data used for clearing and settling important markets, as well as TSA-maintained information about individuals on no-fly lists
4. ISIS failed to exfiltrate data, but managed to infect backup systems, causing a major loss of data

Lessons Learned

There are robust, existing processes and organizations to respond to major attacks, and these are exercised relatively frequently. In fact, some industry sectors recently exercised their defense and response against an attack by ISIS. However, as robust as these processes are, they can still be reactive and not as agile as non-state groups like ISIS. The exercise demonstrated that not enough time is devoted to thinking through what an adversary may do next as opposed to simply reacting to existing attacks.

This cyber wargame took place against the backdrop of other exercises meant to further deepen understanding and cooperation between the United States and its European allies. In November of last year, American and British government agencies and financial institutions carried out a planned drill to test how New York and London would respond to a financial cyberattack. By conducting such simulations, those involved hope to improve information sharing and collaboration, communication practices, and incident response.