The Cyber Action Team

Rapidly Responding to Major Computer Intrusions

03/04/15

It can be a company's worst nightmare—the discovery that hackers have infiltrated their computer networks and made off with trade secrets, customers' personal information, and other critical data.

When such intrusions happen—and unfortunately, they occur frequently—the FBI can respond with a range of investigative assets, including the little-known Cyber Action Team (CAT). This rapid deployment group of cyber experts can be on the scene just about anywhere in the world within 48 hours, providing investigative support and helping to answer critical questions that can quickly move a case forward.

"Our goal is to provide information that can be actioned immediately," said Special Agent Chris Lamb, a CAT member since 2007. "A lot of the evidence in a cyber intrusion may only be there for a little while," he said. "The trail can get cold pretty quickly."

Established by the FBI's Cyber Division in 2006 to provide rapid incident response on major computer intrusions and cyber-related emergencies, the team has approximately 50 members located in field offices around the country. They are either special agents or computer scientists, and all possess advanced training in computer languages, forensic investigations, and malware analysis.

"I call it speaking geek," said Lamb, describing the skills CAT members must possess and maintain to be on the team. "You could compare it to an English speaker trying to learn Mandarin Chinese. You have to spend years immersing yourself in the language to become fluent. And then you have to keep practicing. But unlike Mandarin, which basically stays the same, the challenge for us is that the language of cyber is constantly changing."

Since the Cyber Action Team's inception, the FBI has investigated hundreds of cyber crimes. More than 50 of those cases were deemed of such significance that the rapid response and specialized skills of the Cyber Action Team were required. Some of those cases affected U.S. interests abroad, and the team deployed overseas, working through our legal attaché offices and with our international partners.

"Our job is to very quickly understand what the bad guy did and why," said Lamb, who works out of our Kansas City Division. "We make an initial assessment to determine what we know and what we don't know. Based on that assessment, we then call in other experts to fill whatever gaps we need to have filled."

"Using cutting-edge tools, we look for a hacker's signature," he explained. In the cyber world, such signatures are called TTPs—tools, techniques, and procedures. The TTPs usually point to a specific group or person. The hackers may represent a criminal enterprise looking for financial gain or state-sponsored entities seeking a strategic advantage over the U.S.

Either way, victim companies are often surprised by how much of their networks have been compromised—and for how long. Some intrusions are not discovered until months or even years after the fact.

Hackers have become so sophisticated that they can overcome even the best network security measures, he noted. "We tell victims that it sometimes doesn't matter how good your security is, the bad guys can still get in."

Resources:

Story Index

By Date

By Subject
- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases
- Foreign Counterintelligence
- General
- History
- Intelligence
- International
- Lab/Operational Technology
- Linguist/Translation Program
- Major Thefts/Violent Crime
- Organized Crime/Drugs
- Partnerships
- Public/Community Outreach
- Public Corruption
- Recruiting/Diversity
- Responding to Your Concerns
- Technology
- Training
- White-Collar Crime

- More on the FBI's Cyber Division

Accessibility | eRulemaking | Freedom of Information Act | Legal Notices | Legal Policies and Disclaimers | Links | Privacy Policy | USA.gov | White House
FBI.gov is an official site of the U.S. government, U.S. Department of Justice

Close