The NCFTA

Combining Forces to Fight Cyber Crime

09/16/11

Long before it was acknowledged to be a significant criminal and national security threat, the FBI established a forward-looking organization to proactively address the issue of cyber crime.

Since its creation in 1997, the National Cyber-Forensics & Training Alliance (NCFTA), based in Pittsburgh, has become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.

"The exchange of strategic and threat intelligence is really the bread and butter of the NCFTA," said Special Agent Eric Strom, who heads the FBI unit—the Cyber Initiative and Resource Fusion Unit (CIRFU)—assigned to the NCFTA. "The success of this effort at every level comes down to the free flow of information among our partners."

When the nonprofit NCFTA was established, the biggest threat to industry was from spam—those annoying unsolicited e-mails that fill up inboxes. Today, the organization deals with malicious computer viruses, stock manipulation schemes, telecommunication scams, and other financial frauds perpetrated by organized crime groups who cause billions of dollars in losses to companies and consumers.

The NCFTA essentially works as an early-warning system. If investigators for a major banking institution, for example, notice a new kind of malware attacking their network, they immediately pass that information to other NCFTA members.

Alliance members—many have staff permanently located at the NCFTA—then develop strategies to mitigate the threat. FBI agents and analysts from CIRFU, also located at NCFTA headquarters, use that information to open or further existing FBI investigations, often in concert with law enforcement partners around the world.

"Cyber crime has changed so much since those early days of spamming," Strom said. "And the threat continues to evolve globally, which is why the NCFTA's work is so critical to both business and law enforcement."

The organization draws its intelligence from hundreds of private-sector members, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's Internet Crime Complaint Center (IC3). That extensive knowledge base has helped CIRFU play a key role in some of the FBI's most significant cyber cases in the past several years. (See sidebar.)

Training is another important role of the NCFTA. Last year, an international internship program was held in which cyber investigators from Germany, Great Britain, Australia, the Netherlands, Lithuania, and the Ukraine came to the alliance headquarters for 90 days to share knowledge, build relationships, and help with each others' investigations.

"Working with CIRFU and the NCFTA makes our cooperation very direct," said Mirko Manske, a cyber investigator for the German Federal Criminal Police. "We can work in real time, sharing information and moving our cases forward. That is one of the biggest gains for us."

Manske added, "If I need a contact in the U.S., I reach out to CIRFU, and they help me immediately. And we do the same for them. Basically we are opening doors for each other."

When it comes to the global reach of cyber crime, Manske said, "The FBI gets it. They realize that no one organization can succeed by itself. CIRFU started all of this," he added. "The unit is one of the

Cyber Takedowns

The FBI has conducted a number of major cyber takedowns with the help of the Cyber Initiative and Resource Fusion Unit (CIRFU)—the cyber unit attached to the NCFTA. Here is a brief look at a three of those cases:

Dark Market: Fifty-six individuals were arrested worldwide and $70 million in potential loss was prevented. A CIRFU undercover agent posing as a cyber crook infiltrated a criminal Internet forum at its highest level. More

Coreflood: Investigators disrupted an international cyber fraud operation by seizing the servers that had infected as many as two million computers with malicious software. More

Trident Breach: This major bust targeted a theft ring that used a Trojan horse virus to steal millions of dollars from victims' bank accounts. More

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

reasons the FBI is recognized as one of the worldwide leaders in the fight against cyber crime."

Resources
- NCFTA website
- Cyber crime
- Internet Crime Complaint Center (IC3)