2014-04

CHDS Speaker: Hackers Critical to Defeating Cyber Threats

Monterey CA - April 2014

CHDS Speaker: Hackers Critical to Defeating Cyber Threats

Hackers are potential resources that can aid in the fight against cyber-terror far better than government bureaucrats, says internationally known security researcher Robi Sen.

Sure, sophisticated cyber-criminal hackers and organizations are utilizing leading-edge technology for their underworld enterprises, but the hacking community is more than criminals and disaffected techies. Many are so-called "white hats," curious thinkers with no malicious intent and who may even be considered patriots.

"There are a lot of people in the hacking community who expose insecurities problems and issues," Sen said during an interview prior to his classroom presentation. "They know where the threats are coming from and understand the nature of the problems and how to solve them. They don't have a good way to communicate back to government. When they are able too, they get pushed away or stonewalled. They are a massive resource that is not leveraged exploited by the government."

Sen was a guest subject matter expert for the course "Special Topics in American Government for Homeland Security: "Framing the Discourse," taught by Rodrigo-Nieto Gomez and Kathleen Kiernan. Sen is a much sought-after expert who is Chief Science Officer of Department13, a software consultancy, and is Senior Vice President with Twin Technologies. He was recruited at age 16 to write software for the Department of Defense and a major corporation.

"We wanted to examine the digital human terrain of threat," Kiernan said and we began with exploring the nature of hackers. It's a term that at one juncture was a positive one, associated with discovery and innovation, that now seems to have taken on a negative connotation."

Hackers are the people who have the needed know-how to match the increasingly technical expertise of international criminal enterprises, Sen said. And, they are the people with the skill needed to match the upper echelon players in illicit enterprises, foreign intelligence organizations, and even distributed collectives such as Anonymous. Like other illegal networks, if cyber gangs aren't dismantled at the top levels the organization re-organizes; nabbing the street-level dealer doesn't break the enterprise.

"It would behoove the law enforcement community to change from immediate disruption to strategic patience," he said. "A lot of times these criminal networks, if they are not taken down correctly, they immediately reform. It's just like disrupting a narco or terrorism organization. You can take down low-level players all day long but you have to disrupt the command and control, the major players who are the organizers."

The days of a lone actor cashing in on a virus or malware is no longer sustainable. Like any criminal operation, a support structure is needed to launder money, hide and provide logistical backing. Sen pointed to an example of a criminal cyber operation in Eastern Europe that was targeted by agencies from multiple countries. By the time the task force served the warrants, the server had been had been ripped from their cabinets and signs indicated that it had happened within hours before the raid.

Part of Sen's message was distinguishing between the term "hacker" and "criminal." The hacking community generally comprises security experts and often self-polices. The terms need to be disassociated, Sen observed.

There was a time when hackers were just quirky and technologically curious folks who at worst were occasional pranksters. As computers gained wider accessibility, moving into the average home in the 1980s, movies such as "War Games," in which a teen hacker thwarts a nuclear war after another hacker almost accidentally triggers a nuclear war via a computer controlled command system.

By the time internet connections became widely available in the mid-90s, a mafia family in America was capitalizing on the technology with gambling sites, which were illegal in the United States but not in various countries where the site was hosted.

To show there is no honor among thieves, a Russian-based crime organization was able to perform a "denial of service" attack to deny access to those gambling sites. The Russians blackmailed the mafia, but when they came back for more money, the mob

escalated the cyber war. It established a computer security company that evolved into legitimacy and is now one of the most respected cyber-protection businesses in the nation.

A major thrust of his presentation was that since the Internet, the World Wide Web, et al are relatively new as so is the hacker threat. Though policy-makers tend to believe some special new approach is needed to deal with these issues, the practices that seem to work the best have been methods from traditional policing as well as traditional espionage.

Looking to the future, the potential for cyber-crime has elevated exponentially with the advent of 3D printing. While the concern is that guns can be printed with the technology, Sen worries about terrorists possessing the ability to 3D print weapons of mass destruction, viruses, and drugs. And that kind of innovation is exactly why the hacking community should be engaged by government in battling cyber security threats and crimes.

"We need to change from stomping bugs to looking at it like we are busting a narco cartel over a long period of time," he said. "You have to build up informants. The idea of having some police go online and go undercover will work up to a point, but with the serious criminal networks you have to either flip folks in the network or build up long term undercover operations. It's standard law enforcement stuff." Kiernan added, "There is a tendency to think that the cyber domain requires an entire new set of skills and tools when in reality, many of the traditional investigative skills honed over generations can be successfully applied."