ON TARGET NEWSLETTER

A newsletter covering industrial security issues.

Volume 2, Issue 1 January, 2008

In this issue:

Remarks of FBI Director Robert Mueller at the Penn State Forum Speaker Series.

ON TARGET NEWSLETTER
A security newsletter for MSU
Not approved for public release
Submit comments and questions to:
Neil E. Lewis, 5-8682

Remarks of FBI Director Robert Mueller at the Penn State Forum Speaker Series on 7 November 2007

Good afternoon. I am indeed honored to be here today.

Two weeks ago, in the middle of the World Series, the Colorado Rockies suffered a denial of service attack—just minutes after tickets went on sale for the Rockies' home games against the Red Sox. Thousands of fans were unable to buy tickets—fans who were ultimately spared the spectacle of witnessing a clean sweep.

I reference this case because it highlights our dependence on computer technology and the seriousness of the cyber threat. But it also gives me one more excuse to remind everyone that the Red Sox won the World Series…again.

Today, I want to talk about cyber threats to our national security and what we in the FBI are doing to meet these diverse dangers. A cyber attack could impact our national security as much as other terrorist acts have in the past. Indeed, the intersection between cyber crime and terrorism is becoming increasingly evident.

Cyber criminals and terrorists seek to harm our economy, our infrastructure, and our way of life. We cannot give them free reign to do so. Our success rests upon our partnerships with other law enforcement and intelligence agencies and with our partners in academia and in the private sector—indeed, many of you here today.

It has been said that the Internet, much like Carl Sandburg's fog, in the poem of the same name, came into our lives on little cat feet…unannounced, too subtle to be noticed at first, and then, seemingly overnight, impossible to ignore.

But unlike Sandburg's fog, which sat silently over the city before moving on, the fog of cyber space has nearly enveloped us. And it is by no means sitting silently.

I recently watched a video on YouTube about the impact of the Internet. And before we go any further, I will answer the question of everyone under the age of 25. Yes, those of us over a certain age are allowed to access YouTube. As I understand it, many older people actually contribute to sites such as YouTube and MySpace. It only proves that senior citizens, such as myself, though slow and potentially dangerous behind the wheel, can still serve a purpose.

According to this video, entitled “Did You Know,” the average 21-year-old has sent and received more than 250,000 e-mails and instant messages. More than 70 percent of 4-year-olds in the United States have used a computer at least once. And Internet users query Google nearly 3 billion times each month.

The Internet has changed the way we communicate, learn, and work. It has also become the primary means by which we conduct business, store data, and connect operating systems, from air traffic control to power grids. But that widespread use has also left us vulnerable to attack from hostile foreign powers, hackers, and even terrorists.

I want to start with cyber terrorism, because protecting America from terrorist attack is the FBI’s highest priority. To date, terrorists have not used the Internet to launch cyber attacks. But there are thousands of extremist websites, comprising everything from propaganda to blogs.

In the past six years, al Qaeda’s online presence has become pervasive. For terrorists, the Internet has become a marketing tool, a moneymaker, a training ground, and a virtual town square, all in one.

In July of this year, three men in Britain were the first to be sentenced to prison for using the Internet to incite terrorism. One of these men, Younis Tsouli, went by the moniker “Irhabi 007”—which translates in Arabic to “Terrorist 007.” He was a loner in a London basement apartment, with no previous connection to al Qaeda, yet he became a key part of its propaganda campaign.

Tsouli posted thousands of files online, from videos of beheadings to detailed instructions for building car bombs. He hacked into servers around the world to gain additional bandwidth.

But he did more than merely act as an al Qaeda webmaster. He was a hub of communication between terrorist plotters in Canada, Denmark, Bosnia, and the United States. He and his colleagues stole thousands of credit card accounts through phishing schemes. They ran up charges of more than $3 million for items they thought fellow extremists might need, from night vision goggles to GPS devices. And they laundered money through more than a dozen Internet gambling sites.

According to British authorities, just before his arrest, Tsouli set up a website that he hoped would become the YouTube for terrorists. He called the site “You bomb it.”

At the time of his arrest, he was just a 22-year-old student. Today, he is a guest of Belmarsh Prison in the U.K. But he is hardly the end of the line; many more cyber-savvy extremists hope to carry on where he left off.

The Internet is not only the means by which attacks may be planned and executed, it is a target in and of itself. Last April, Estonia suffered what has been called a “cyber blockade.” Wave after wave of data requests from computers around the world shut down banks and emergency phone lines, gas stations and grocery stores, newspapers and television stations, even the prime minister’s office.

Although the source of this attack has not been confirmed, the effect was real, and left all of us aware of the potential risk we face. How long before others around the world begin to employ similar tactics?

Of course, terrorists are not the only ones using the Internet for criminal purposes. Far from it. Computer intrusion cases are becoming more commonplace. And studies show that computers in the United States are attacked at a rate 10 times that of other countries.

Today, botnets—so-called “robot networks” of computers that are controlled by hackers—are the weapon of choice. Botnets are considered the Swiss Army knives of cyber crime. You name it, they can do it, from attacking networks, sending spam, and collecting data, to infecting computers and injecting spyware.

Botnets do not require highly technical skills, yet the national security implications are broad. A botnet could shut down a power grid, flood an emergency call center with millions of spam messages, or disable a military command post.

Odds are there are more than a few of you here today whose computers may be part of a botnet, unbeknownst to you. The possibilities are endless, and that is what is so daunting.

I want to turn for a moment to counterintelligence intrusions and economic espionage. There is no shortage of countries that seek our information technology, our innovation, and our intelligence—information we have spent years and billions of dollars developing.

The simple truth is we do not protect cyber space to the same degree we protect our physical space. We have in large part left the doors open to our business practices, our sensitive data, and our intellectual property.

The espionage game once pitted spy versus spy, country against country. Today, our adversaries sit on fiber optic cables and wi-fi networks, invisible and undetected. Hackers are using sophisticated techniques to steal sensitive intelligence, scientific research, and communications data. They are difficult to identify and track because they move in and out of international systems at will, and they do not leave broken glass behind.

A member of our cyber team describes it as having an invisible man in the room, standing over your shoulder, seeing and hearing everything you do, watching every word you type. And you may never know he is there…who he represents…or how much damage he has done.

We are concerned not only with loss of data, but with corruption of data, from false information to altered code. Such manipulation can cause electronic devices to fail and networks to freeze. It can alter physical environments in laboratories and shut down safety systems in nuclear power stations.

There are also those who seek to block access to our own information, for political, financial, or ideological gain. If we lose the Internet, we do not simply lose the ability to e-mail or to surf the web. We lose access to our data. We lose our connectivity. We lose our intellectual property. We lose our security. What happens when the so-called “Invisible Man” locks us out of our own homes, our offices, and our information?

On the economic front, hackers are stealing vast amounts of information from American companies. Cyber thieves are targeting data at the research and development stage before it becomes classified, when it is easier to access.

And the threat is not limited to hackers on the outside. Insiders present a significant problem. Contractors may take the appropriate security measures, but what about those with whom they subcontract and their subs? And what of those who may take advantage of open access to research and development facilities on campuses such as this?

One recent case underscores this threat. In November 2001, a man named Li Sun told FBI agents in Palo Alto that he believed his business partner had stolen trade secrets from his employers.

One week later, Fei Ye and Ming Zhong were arrested at the San Francisco airport, just moments before boarding a flight bound for Shanghai. FBI agents and Customs officials seized thousands of proprietary documents and electronic media from two major semiconductor companies.

In the following months, investigators examined several hard drives. They reviewed nearly 9,000 pages of documents from several companies, including Sun Microsystems, Transmeta, NEC, and Trident. They searched more than 25,000 pages of e-mails on five separate Yahoo accounts.

These two men had planned to start a semiconductor company in China, using this proprietary information. They had requested funding from a Chinese government program dedicated to acquiring and developing science and technology. They had received more than $2 million in start-up funding from city and provincial Chinese government agencies.

In December 2006, these two pled guilty to economic espionage—the first such convictions in this country. Each faces up to 30 years in prison.

Collectively, these threats paint a troubling picture, but one we in the FBI must confront.

The FBI has the authority to handle these threats from start to finish. We have cyber squads in each of our 56 field offices across the country. These agents, intelligence analysts, and computer experts mesh technological expertise with investigative experience.

They run complex undercover operations to catch computer hackers and child predators the world over. They investigate threats to both companies and consumers. And they teach their law enforcement counterparts—at home and abroad—how to work cyber investigations.

Our capabilities are strong, but they rely on key partnerships with other federal agencies, law enforcement, private industry, academia, and citizens alike.

Officers, agents, and IT specialists in our Regional Computer Forensic Labs find and examine digital evidence from e-mail and cell phone data to documents on hard drives. Together, we continue to break new ground in the investigation and prosecution of cyber criminals.

But we cannot limit our operations to the United States. Increasingly, cyber threats originate outside of our borders. And as more people around the world gain access to computer technology, new dangers will surface. For this reason, global cooperation is vital.

We have 60 Legal Attaché offices around the world. We are working with our partners in Romania, Russia, Poland, Hungary, Italy, and Estonia, among others, to investigate international cyber threats.

In 2005, for example, FBI agents and analysts worked closely with Microsoft to find those responsible for creating the Mytob and Zotob worms. Together with our law enforcement partners overseas, FBI agents arrested the originators in Turkey and Morocco just two weeks after the attack.

We understand that we must continue to work closely with all of you—members of the private sector and the academic community.

In June of this year, we initiated Operation Bot Roast. Together with the Department of Justice, the CERT Coordination Center at Carnegie Mellon, private sector companies, and internet service providers, we identified more than 1 million infected computers and shut down several bot-herders. This operation is ongoing, and we will continue to pursue these criminals for as long, and as far away, as necessary.

Much of our collaboration begins in Pittsburgh—at the FBI's Cyber Fusion Center. Think of the fusion center as a hub, with spokes that range from federal agencies, software companies, and ISPs, to merchants and members of the financial sector.

Industry experts from companies such as Cisco, Bank of America, and Target sit side-by-side with the FBI, postal inspectors, the Federal Trade Commission, and many others, sharing information and ideas. Together, we have created a neutral space where cyber experts and competitors, who might not otherwise collaborate, can talk about cyber threats and security breaches.

The FBI's InfraGard program is a more localized example of our private sector partnerships. Members from a host of industries, from computer security to the chemical sector, share information about threats to their own companies, in their own communities, through a secure computer server.

To date, there are nearly 21,000 members of InfraGard, from Fortune 500 companies to small businesses. That amounts to 21,000 partners in our mission to protect America.

We are also reaching out to academia. In 2005, we created the National Security Higher Education Advisory Board. We asked your president, Graham Spanier, to lead the group. We knew it wouldn't be an easy sell, because of the perceived tension between law enforcement and academia.

But once we briefed President Spanier on the national security threats that impact all of you here at Penn State—and other academic institutions—it became clear to all of us why this partnership is so important.

The Advisory Board provides a forum to discuss issues that affect not just the academic culture, but the country, from campus security and counterterrorism to cyber crime and espionage. Presidents and chancellors from Carnegie Mellon, NYU, the University of Washington, and Iowa State, among others, share their concerns and their collective expertise.

We fully understand that universities are the creators of knowledge, not merely the disseminators. And it is not our intent to interfere with the academic environment in any way. But we must remain alert to the threats we all face, and we must learn to balance openness with awareness.

There is an old saying that all roads lead to Rome. In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles.

The Romans built these roads to access the vast areas they had conquered. But, in the end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.

The Internet has opened up thousands of new roads for each of us—new ideas and information, new sights and sounds, new people and places. But the invaders—those whose intent is not enlightenment, but exploitation and extremism—are marching right down those same roads to attack us in multiple ways.

We stand a much greater chance of staying safe if we stand together. We must continue to safeguard our systems and our data. We must continue to share intelligence. Most importantly, we must continue to stay connected.

The enemies, as they say, are at the gates, and we must rely on our agility, our resourcefulness, and our resolve to stop them, together.

Thank you and God bless.

****

Security is a team effort!