CyberCrime
2010 Symposium

Responding to the Financial
Cybercrime Epidemic

November 4-5, 2010

Conference Insights

Table of Contents

Conference Insights

The CyberCrime 2010 Symposium brought together law enforcement, financial services providers, journalists, technologists, researchers, and cybercrime victims for two days of intensive discussion on the global cybercrime epidemic. The conference, hosted by **Sage Data Security** and **noPhishing.org**, focused on corporate account takeover and ways organizations should work together to combat the cybercrime threat.

Attendees were treated to speaker presentations from professionals on the forefront of fighting cybercrime. They learned about the changing nature of cybercrime, heard victims' accounts of their losses, and received recommendations for protecting themselves against increasingly sophisticated threats. They also took part in a real-world malware infection exercise involving a banking institution and its corporate customer, where they could watch an attack unfold, and test reactions, actions, and solutions.

Conference presenters included:

Joseph Menn, journalist and author: *"The Hunt for the New Crime Lords Who are Bringing Down the Internet"*

Brian Krebs, editor, **Krebsonsecurity.com**: *"Krebs on Security: 60 Breaches and Counting"*

James Lyne, CTO, **Sophos**: *"Anatomy of an Attack: How Hackers Threaten Your Security"*

Doug Johnson, VP, risk management, **American Banking Association (ABA)**: *"Respond and Defeat – Resources for Fighting Back"*

Stephen Nix, **Secret Service Special Agent, DC Cyber Division**: *"Respond and Defeat – Resources for Fighting Back"*

Russ Brown, **FBI DC Unit Chief, Cyber Division:** *"Respond and Defeat – Resources for Fighting Back"*

Jim Woodhill, founder of **Authentify**: *"Banking in Cyberspace: Managing the New Risks"*

Gary Warner, director of research, computer forensics, **University of Alabama at Birmingham**: *"The ZeuS Botnet: Stealing Everything from Millions of Americans"*

Holly Young: Executive Vice President and CIO, **Norway Savings Bank**

Arlene Stinson: Arlene Stinson, VP Information Systems/Technology Security Officer, **Merrimack County Savings Bank**

Sari Stern Greene: president of **Sage Data Security** and managing director, **MEAPC**: *"Communicating with Customers"*

As Jim Woodhill said in his presentation, where there's money, there's theft, and criminals will take advantage of every available path to money. The internet provides a path to fraud, particularly in cases where access to money depends on trust, as it does in the relationship between banking institutions and their corporate customers. Cybercriminals have devised very sophisticated ways to use that trust to their advantage. Thwarting them will take an equally sophisticated and multifaceted strategy.

This **Cybercrime 2010 Symposium Insight** details the key takeaways from the conference, presenting primary challenges and best practice recommendations for fighting cybercrime targeting corporate accounts.

- Cybercrime is organized crime. Cybercriminals are increasingly sophisticated and share best practices.
- Malware is now in its third wave and there's been a huge change in the nature of the threat.
- Nobody knows who to blame, so there's a lot of finger-pointing between financial institutions and their corporate customers.
- Law enforcement has an enormous task fighting cybercrime. They're gaining traction but need every stakeholder onboard.
- Fighting cybercrime will require a combination of people, processes, and technologies across multiple touchpoints.

Takeaway: Cybercrime is organized crime. Cybercriminals are increasingly sophisticated and sharing best practices.

Cybercrime has come a long way from its early days when the primary targets were offshore online gambling sites. Online gambling sites made appealing targets because online gambling was illegal in the U.S. and criminals knew that cyber-attacks wouldn't be reported to the FBI. Over time, cybercriminals, part of powerful organized crime syndicates, boldly branched out to take on everyone from the biggest financial institutions and corporate brands to small businesses, non-profits, and municipalities.

Attackers have employed several methods of attack for financial gain: they launch denial-of-service attacks that crash servers and demand money to cease the activity, encrypt corporate data and hold it for "ransom" until paid and more recently, use potent malware to grab personal identifiers to gain access to financial assets. Increasingly, their targets are the corporate accounts of small-to medium-sized businesses (SMBs), which inadvertently open the door to their assets through online banking.

This latest threat got significantly worse in 2008, according to Jim Woodhill, who referred to the combination of the Lehman Brothers collapse, emergence of *ZeuS* malware, maturing Eastern European criminal ecosystem and vulnerabilities in the Windows operating system as the "Perfect Storm" for cybercrime rings.

What do these rings look like? At the top of the cybercrime syndicates are crime bosses just like those active in human trafficking or drug cartels, said Joseph Menn, author of the book *Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet*. Menn detailed activities in Russia, where cybercriminals, enjoying early success, found natural allies in mobsters who provide funding and protection. Couple these syndicates with complicit law enforcement professionals within many Eastern European countries and "the corruption is mind-blowing," said Menn.

"These [syndicates] do capitalism better than we do," said Menn. "They're millionaires and they invest in R&D, take money they make from phishing scams, and hire good programmers to build up their business."

The programmers they hire, said Brian Krebs, editor of *Krebsonsecurity.com*, are extremely intelligent and well-educated engineers. Primarily based in Eastern Europe, where desperate economic conditions create a powerful driver to exploit American businesses, these coders create the incredibly effective and adaptive malware that enables their groups to gain access to corporate accounts, or sell to other exploiters who want to do the same thing.

Cybercrime syndicates use another financially strapped demographic, primarily in the U.S., to serve as "money mules" — the people who withdraw the stolen funds and transfer them through wire services to their "bosses." Mules are typically lured with online ads that promise good money for work-at-home jobs. Most recently, cybercriminals have begun using "J1 mules," students who are in the U.S. on temporary visas and who physically carry cash back home.

Cybercrime rings are well-organized and well-protected, leveraging ever-growing economies of scale, and openly sharing information in cyberspace. "Bad guys are working together on forums and other places and sharing best practices. When money starts flowing you get research, innovation, and development," said James Lyne, CTO at *Sophos*. Lower-tier hackers ask for best practice tips on infecting people, and even have higher-level experts review their malware and give them tips on how to improve it.

Because it's not actually illegal in some countries to hack computers in the U.S., there have been insufficient threats to shut down cybercrime operations. Thus far, most punishment hasn't fit the crime. The recently adjudicated case involving *RBS Worldpay* earned Viktor Pleshchuk a suspended sentence, probation, and restitution in lieu of jail time, despite the fact he was a lead perpetrator.

However, *Operation Trident Breach*, which culminated in the recent arrest of five masterminds behind attacks on banks and their customers over the last couple of years, provides some hope that crackdown efforts are disrupting criminal activity. *Operation Trident Breach* was launched in May 2009, when Federal Bureau of Investigation officials based in Omaha, Nebraska, got wind of suspicious automated clearinghouse (ACH) batch payments going to 46 bank accounts across the U.S. The targets of the attacks, which used *ZeuS* malware to grab banking credentials, were the accounts of SMBs, municipalities, churches, and individuals.

The subsequent arrests and search warrants were the product of unprecedented work among the FBI, Security Service of Ukraine (SBU), the UK's Metropolitan Police Service, the Netherlands Police Agency, and other foreign law enforcement agencies. The criminals involved in the operation had used *ZeuS* to make off with $70 million out of an attempted $220 million from 390 accounts.

Takeaway: Malware is now in its third wave and there's been a huge change in the nature of the threat.

The *ZeuS* trojan, the malware used to wreak havoc with corporate bank accounts and other resources around the world, had a very busy year in 2010. It's now "the most wanted botnet in the world," said UAB's Gary Warner, who helps train law enforcement officials fighting cybercrime and whose labs at the university combine computer science and law enforcement techniques to perform forensics analysis and investigate spam, phishing, and malware.

Today, said Lyne, malware is in its "third wave," and is focusing on an "astonishing array of data." It's designed to serve the overarching purpose of letting perpetrators gain access to corporate systems, whose data they can use for financial or any other gain.

"It's about theft of information leading to theft of money, and it's a very well-funded and coordinated effort," said Lyne. Using their malware's keylogging capabilities, criminals are stealing everything from personal identifiers to intellectual property. Where it's fiscally beneficial, cybercriminals aren't just stealing data — they're manipulating and destroying it.

Some factors and features that make the latest malware incarnations so effective and potentially harmful to corporate accounts include:

- Phishing emails look authentic and take users to bogus sites that look equally authentic. Emails come in varied forms including requests from the IRS to civil court subpoenas and other difficult-to-ignore messages. "This is not your grandfather's email; it's at a high level of sophistication," said the ABA's Doug Johnson.

- Seventy percent of malicious code sits on legitimate websites. According to Lyne, the major problem is no longer with pornographic or gambling sites infecting computers; malware is lurking at sites users need to visit, like financial and personal websites. Criminals put malicious code on a site, which redirects users to a multi-warhead exploit page in the background that "throws vulnerabilities at them until one sticks," said Lyne.

- As a potential target, a site doesn't have to stand out in any way. Automated malware tools are continually searching the internet for sites with potential weak spots so they can get bad code on the page.

- There's been a huge expansion in the number of devices accessing corporate applications and hosting sensitive data, from laptops to cell phones. Workers are more mobile than ever and they have distinct preferences in computing devices. The more devices to secure, the more opportunity for breaches.

- Many employees work from home, at least part of the time. "'Work from home' equals 'risk from home,'" said Warner. The laptop that travels home is already at risk as it's outside the firewall. If it then gets used by someone else — say, a child who doesn't know that it's a criminal and not Facebook that's asking for an

updated user name and password — then the machine can be easily compromised and act as a malware gateway to the employee's company.

- Malware adeptly uses social engineering. Malicious code understands online behavior and uses it to gain access to machines and networks. If a user gets an anti-virus pop-up ad that's sophisticated enough to list real computer files, such as medical data files, they might click on the fake ad for help, truly infecting the computer. People know viruses are bad, say Lyne, and criminals use this social engineering trait against them.

- The "man in the browser" is powerful. The capabilities ZeuS gives exploiters once it infects a machine are staggering, said Warner. For example, they get full remote control capability, so they can run the computer as if it's their own. Increasingly, exploiters are grabbing two-factor authentication IDs — used by many banking institutions to increase security levels — that allow them to do some very sophisticated swap-outs with banking transactions that conceal theft.

- Anti-virus solutions can't touch *ZeuS*. Both Lyne and Warner cited numerous malware versions that went largely undetected by the biggest AV players in testing situations.

Takeaway: Nobody knows who's to blame, so there's a lot of finger-pointing between financial institutions and their corporate customers.

While consumer accounts are protected against online theft, business accounts are not, as two small business owners testified during the conference. One, **Patco Construction**, lost $545,000 in a matter of days through fraudulent ACH transfers. The company has filed a lawsuit against its bank for unreimbursed funds. The second, **Little & King Co.**, lost $164,000 in one day through malicious ACH transfers. Since being told by her bank that she, and not its security measures, was at fault, owner Karen McCarthy took up the cause of small businesses and is working with other owners to lobby Congress for better loss regulation for corporate accounts.

While the criminals are obviously to blame, until there's better protection in place, banks and business customers will continue to argue about who should bear the brunt of financial losses. Breaches will lead to costly litigation and concerns that smaller banks can't protect their assets will drive businesses to money-center banks, said Woodhill. It's a problem that he fears could drive community banks, which he calls a critical piece of American society and local economies, out of business.

The financial services industry, Woodhill said, has to take charge of the problem and work with Congress to address it, but cautioned that onerous regulations and legislation will hamper efforts. One possible step, he said, would be to extend ***Federal Reserve Regulation E***, which regulates electronic funds transfers, to cover commercial accounts.

Given the current lack of laws governing online theft, Sari Greene urged attendees to open the lines of communications not just with their customers, but with their boards of directors, customer service representatives, commercial lenders, marketing teams, and anyone else affected by the issue. Not only are individual accounts on the line, but a bank's entire reputation.

"If banks told their customers that their commercial accounts don't have the same protection as consumer accounts and that banks aren't required to provide reimbursements for certain losses, most customers would be astounded," said Greene. "The first time they hear this news should not be on the day they're finding out about their losses. They need to understand so they can make risk-based decisions about online banking."

Representatives from two New England banks were on hand to discuss their online security and customer communications efforts. **Merrimack County Savings Bank's** Arlene Stinson described how they intercepted two fraudulent wire transfers from a customer's account and managed to stop the attack. Because they were already in the process of distributing Go ID Tokens to customers for two-factor authentication — and had gotten some resistance — they used the opportunity to train all their business customers on the threat. They held three cash management training sessions, alerting customers to cybercrime threats, risks, and security measures.

"It was a real eye-opener for customers," said Stinson. "They were extremely grateful for the information and the token rollout went off without a hitch."

Norway Savings, said Holly Young, was about to go through a similar token rollout for multi-factor authentication and decided to hold training sessions to not only introduce the tokens, but to educate customers on the larger issues.

The entire banking community is harmed every time security breaches happen, said Greene. Banking institutions need to closely examine their controls. If they're confident strong controls are in place, then the bank can offer online banking services, but only after talking with customers about the ultimate risks, legalities, and kinds of security measures in place. This ensures customers have the information they need to make informed decisions about their banking practices. Controls that merely require customers to enter a user name, password, answer some challenge questions and don't incorporate fraud monitoring are asking to be compromised, said Greene.

As for banks' concerns that customers won't accept increased security measures and that frank conversations about online banking will drive them to competitors, Greene said customers ultimately want to protect themselves and will appreciate communications about their risks.

Takeaway: Law enforcement has an enormous task fighting cybercrime. They're gaining traction but need every stakeholder onboard.

The open communications lines that must exist between financial institutions and their customers concerning online banking should extend to every entity touched by cybercrime. If the U.S. is going to win its cybercrime battle, it's going to take a concerted effort involving law enforcement agencies worldwide, public and private sector organizations and the public in general. Having people on the ground actively working on threats is the only way to stem the cybercrime tide, said the **ABA's** Doug Johnson, adding that the financial services industry works closely with commercial security providers, government agencies, the Secret Service, FBI, and other law enforcement entities on cybercrime issues.

An integral part of this effort is the **Financial Services – Information Sharing and Analysis Center (FS-ISAC)**, a membership organization that monitors and analyzes threats and provides alerts throughout the financial service community.

"We have broad membership within the task force, including government partners, core processors, and institutional banking service providers. We're building protection, prevention, and response tools," said Johnson. "This problem's not going away, and over the course of the next year we'll continue to deploy additional resources to help." For instance, the **FS-ISAC** has worked with one of its membership organizations, **NACHA**, to develop a broad advisory for business and consumers about corporate account takeover and mule recruitment that financial institutions can disseminate.

Another initiative working to hinder criminal activity is the **FBI's National Cyber-Forensics & Training Alliance**, a partnership between the private sector and public agency. The alliance is working to address ACH fraud and other cybercrime activity by encouraging banks to share information on mule activity, said Russ Brown, FBI.

Further, the kinds of overseas partnerships the FBI has developed over many years through the legal attaché program have started to pay dividends on the cybercrime front. Cyberagents are embedded with law enforcement in Estonia, The Netherlands, Colombia, Romania, Latvia, and Ukraine. The work has resulted in arrests over the last five years in Romania, Estonia, England, and other countries, said Brown.

Nix says the Secret Service has a relatively small number of cyberagents, but their efforts are aided by the fact that their counterparts in other countries, such as the SBU in Ukraine, are equally motivated to stop cybercrime. He and his team are continually undercover on cybercrime forums, traveling around the world to meet with local law enforcement officials and criminals, and imaging servers for analysis, acting on tips from stakeholders.

Both Brown and Nix said that their efforts at this early stage must focus more on building relationships with foreign law enforcement and cybercriminals than on punitive measures.

"We're always working on the next lead. The arrest is not what's most important; it's a tool to get to the real end, which is disrupting and dismantling these rings," said Nix. His agency has a very small window of time to act after getting information because data is stored for such a short period. Nix said his company has international agents who can take off on a moment's notice to grab servers and take relevant action.

Nix told attendees that everyone has a potential part to play in slowing cybercrime and recommended they start immediately building relationships with state and federal law enforcement agencies. Financial institutions have IP logs, user credentials, and other evidence the Secret Service and other agencies can use to build cases, so it's critical that banks and victims come forward immediately after suffering a cyberattack.

Takeaway: Fighting financial cybercrime will require a combination of people, processes, and technologies across multiple touchpoints.

The **Cybercrime 2010 Symposium** presenters agreed no one technology, service, organization, or regulation can stop cybercrime. To address the complexities of the ever-changing problem will require organizations to address a wide range of people, process, and technology issues. Presenters provided both immediate and long-term security recommendations for the financial services providers and the corporate customers in attendance.

People Recommendations

- Stay abreast of the latest trends and track cybercrime threats by becoming members of such organizations as **FS-IASC** and the **InfraGard IG Malware** mailing list, published by what the group calls its "volunteer forensics community" dedicated to analyzing malware and appropriate defenses.
- Help raise public awareness overall. Cybercrime doesn't affect just banks and their corporate customers; the general public needs to be made aware of the threat as well, particularly about the role of mules and how they're lured. As part of **"Operation Swordfish,"** UAB's Warner, in conjunction with Alabama officials, is rolling out a PSA campaign in March about mules and money laundering. Similar campaigns in other states will help.
- Educate corporate customers about cybercrime, even if you think they'll initially shy away. They must be made aware of the nature of the problem and the potential damage so they can make educated decisions about online banking and general computer use. Also educate them about the steps you're taking to protect them.
- Preemptively connect with state and federal law enforcement officials to develop a relationship.
- Educate youth about cybercrime threats and career opportunities that will be increasingly available in computer forensics and related activities.

Process Recommendations

- Move beyond mere anti-virus adoption toward "malware intelligence."
- Encourage customers to use a dedicated system for banking, particularly a non-Windows-based system.
- Adopt multi-factor and multi-channel authentication, dual controls for payment initiation, and other enhanced security measures.
- Adopt "out-of-band" processes where appropriate.

- Employ fraud monitoring and predictive analytics tools and services.
- Have procedures in place to respond to breaches and brief customers on whom they should contact and what steps they should take if a breach occurs.

Advisories & Guidance

Given the current inequities in cybercrime — which Woodhill called "asymmetric warfare" considering the brilliance of attackers and the tens of millions of possible victims who aren't well-protected — banks and their corporate customers are going to need every possible weapon at their disposal. The cost of failed attempts is low, while the payoff from successful attacks is high, so criminals will continue to make malware and other exploits increasingly sophisticated. To stay informed on the latest cybercrime threats, as well as activities on the part of law enforcement, financial services, and other organizations, visit:

- **Fraud Advisory for Businesses –Corporate Account Takeover:** http://ww.ic3.gov/media2010/corporateaccounttakeover.pdf
- **Fraud Advisory for Consumers – Involvement in Criminal Activity through Work from Home Scams:** http://www.ic3.gov/media2010/WorkAtHome.pdf
- **The Financial Services – Information Sharing and Analysis Center (FS-ISAC)**, which includes the Online Fraud Working Group: http://www.fsisac.com
- **Local FBI offices:** http://www.fbi.gov/contact-us/field/field-offices
- **The Internet Crime Complaint Center (IC3)**, a partnership between the FBI, National White Collar Crime Center (NW3C), and Bureau of Justice Assistance (BJA): http://www.ic3.gov/default.aspx
- **National Cyber-Forensics & Training Alliance:** http://www.ncfta.net
- **US-CERT (United States Computer Emergency Readiness Team)**: http://www.us-cert.gov
- **InfraGard:** http://www.infragard.net
- **Anti-Phishing Working Group (APWG)**: http://www.antiphishing.org
- **Maine Anti-Phishing Coalition (MEAPC)**: http://nophishing.org

For more information on the CyberCrime 2010 Symposium, visit cybercrime2010.com or sagedatasecurity.com.

www.cybercrime2010.com