Protecting the Public through Government, Academic, and Industrial Partnerships

Testimony of Gary Warner
Director of Research in Computer Forensics
The University of Alabama at Birmingham

Congressman Bachus and members of the committee, I would like to begin by thanking you for the opportunity to testify this afternoon, and for the vision of the committee that has lead them to hold this important hearing today. We are especially fortunate to be in this facility, the National Computer Forensics Institute, an organization that has trained hundreds of state and local law enforcement officers to be able to respond to today's complex crimes that often involve digital evidence found on the computers, phones, and servers that we rely on to protect our identities, our finances, and our intellectual property.

At UAB, the University of Alabama at Birmingham, we are also engaged in that protection effort. Our contributions are in three main areas.

> Through our teaching, we prepare the next generation of cybercrime investigators, computer forensics examiners, and computer security professionals, who will both design more secure systems and investigate those who breach them.

> Through our research, we develop tools, techniques, training, and intelligence to assist the current investigators, examiners, officers, and analysts, by combining the knowledge of computer scientists and criminologists in ways that enable a leveling of the playing field when facing ever more sophisticated criminals.

> Through our outreach, we educate and inform the public about protecting themselves from online threats through lectures and conference presentations, social media and blog posts, and traditional media outlets such as newspapers, magazines, and television.

Today's hearing is entitled "Helping Law Enforcement Protect Private Financial Information." My testimony today will outline some of the issues that currently allow financial information to be regularly stolen, and then discuss some of the ways Law Enforcement is working with Academia and Industry to move beyond these problems.

Before I start, allow me to provide a few brief definitions.

Phishing – Phishing is the crime of gathering personal information through subterfuge by imitating a website or official communication from a trusted organization, such as a financial institution. The complexity of the information gathered ranges from a simple userid and password to allow access to an online account, to full information including credit card or ATM numbers, PINs, Social Security Numbers, Drivers License information, or answers to common security questions such as Mother's Maiden Name or High School Mascot.

Malware – Malware is software which will perform an unauthorized or harmful action on a computer. Non-technical people would usually call this a computer virus, which is one of several types of malware.

Botnet – A botnet is a collection of computers which are controlled by malware to cause them to do the bidding of a criminal. Each individual computer on a botnet has been compromised by criminal malware and is referred to individually as a "bot." The criminal usually controls his botnet through a "Command & Control" or "C&C" server. The criminal controlling a botnet is often referred to as a "botherder." Criminals use botnets for many types of activities, including sending spam emails, stealing personal information or documents, launching crippling attacks on other computers, or allowing the criminal to anonymize their true location by "proxying" their network traffic through the bot computer.

Keylogger – A keylogger is a particular type of malware which steals information typed by the computer user and provides a means for the information to be retrieved by the criminal. Keyloggers are often used to steal personal financial information without the knowledge of a victim simply by observing the victim interacting with his or her online financial accounts.

Protecting Private Financial Information from Cyber Threats

Critical Infrastructure Protection, Phishing, and Law Enforcement

My very first research into phishing was a natural outgrowth of my interest in Critical Infrastructure Protection. In 1997, President Clinton convened a Commission on Critical Infrastructure Protection which resulted in goals that were stated in Presidential Decision Directive 63 (PDD-63) including that by the year 2000 we would have significantly increased the security of government computer systems, and that by 2003 we would be prepared to protect the critical infrastructures of our country from all threats, both cyber and physical. PDD-63 established the National Infrastructure Protection Center and sector specific Information Sharing and Analysis Centers. Beginning September 6, 2001, the energy company for which I then worked hosted the first InfraGard meeting in the Birmingham area, and Special Agent Mike Mauldin explained the concept of Critical Infrastructure Protection to an audience of sixty local companies including all of the largest banks in the state.

In 2002, Ron Dick, then the Director of the National Infrastructure Protection Center was speaking with me at the National InfraGard Congress. I mentioned that sometimes people asked me why I spent so much of my time on Critical Infrastructure Protection issues. His response probably changed my career path that day. He reached into his pocket and took out a White House lapel pin, pinned it on my jacket, and told me, "You tell them because the President of the United States asked you to, that's why!"

I took that very seriously, and that is exactly what the President asked us all to do with PDD-63, which established the need for Public-Privater Partnerships:

> "Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative." – PDD-63, May 22, 1988

Three years later when the banks in my InfraGard chapter began to have problems with phishing they turned to law enforcement for help, but they also turned to the computer security professionals who were members of the local InfraGard chapter. No one in law enforcement had seen this type of cyber attack before, and we had to figure out questions like "What is the crime?" and "Who is the victim?" There was a great deal of confusion. The then-current version of Title 18 Section 1030 stated that it was a federal crime to hack the computers of a financial institution, but wasn't clear about hacking a website belonging to an individual and using that website to pretend to be the bank! Today we have great laws making it a crime to compromise any computer attached to the Internet, but those laws are not being enforced in this area.

Just as Bill Clinton said in PDD-63, and George Bush re-iterated in Homeland Security Presidential Directive 7 (HSPD-7) and in the National Plan to Secure Cyberspace, and President Obama has said while appointing Howard Schmidt to serve as Cyber Security Advisor, we need to work together in order to stop these crimes. Birmingham, like 24 other cities, is fortunate to have both an InfraGard chapter and a US Secret Service Electronic Crimes Task Force. I have hosted both organizations in my lab, have donated students from my lab as interns to work in the computer forensics lab here in the National Computer Forensics Institute in support of law enforcement, and have stood in this building to present about phishing to a group of more than forty Alabama-based banks who had been brought together by the Electronic Crimes Task Force. We need the increased cooperation, because the problem is worse than ever.

Issue One: The increase in cybercrime far outpaces the increase in law enforcement focus on cyber

When I began investigating phishing crimes in December 2004, along with my InfraGard banking associates, we learned of the Anti-Phishing Working Group, a non-profit organization that had taken on the challenge of coordinating information about phishing. That first month, the Anti-Phishing Working Group reported there had been 1707 unique phishing sites documented that month, or a rate of about 55 new phishing websites per day.

In the first quarter of 2011, UAB saw 47,452 unique phishing sites for 300 different online brands and businesses. That is 521 cases of computer intrusion per day, with more than 50% of those computers located in the United States. Numbers for the second quarter were nearly the same with 46,134 nphishing sites attacking 303 online brands.

Almost all of those phishing sites are on hacked webservers. We're now documenting and gathering evidence from more than 15,000 phishing servers every month. More than half of those servers are located in the United States.

A report from the APWG last month[1] indicated that not only are there are dramatically more phishing websites, they are staying online longer than ever before.

What other category of crime has increased by 900% over the past seven years?

Part of the increase in online crime is a response to the increase in the online economy itself. In 2000 there were only 360 million internet users and the entire e-commerce environment was only $5 billion. Only 18% of the American public had ever used online banking! In the first quarter of 2011 by comparison, online retail sales reached $46 Billion, or 4.4% of all retail sales. 2010 online sales accounted for $164 Billion of our economy last year[2], a 3200% increase in the past decade. While the Internet only contributes 3.8% to the GDP in the United States, it accounts for 21% of the GDP growth in the past five years, making a greater contribution to GDP than Agriculture, Utilities, or Mining.[3]

The other change impacting online crime is the international demographic of the Internet itself. In 2000, the majority of those 360 million internet users were in the United States and subject to our laws. As of the first quarter of 2011 we now have 2 billion Internet users, but only 13% of them are in North America.[3] 87% of Internet users are in other countries, but the largest concentration of wealth accessible from the Internet remains in the United States.

Part of this growth has been that many more criminals are choosing to explore the area of phishing as a way to make money. Another part of the increase, however, is that criminals have embraced technology to a deeper level than law enforcement. For more advanced criminals, creating a new phishing site is literally only one mouse click. With a single click of the mouse, their programs scan the internet for a website with a well-known vulnerability, compromise the website, upload the counterfeit bank website to the compromised server, and begin to send spam messages warning consumers of a problem with their bank account and inviting them to visit the phishing site to resolve the problem.

We need a corresponding growth in our ability to use technology to investigate these cyber crimes, and that is one focus of our lab. Law enforcement officers and agents from the FBI, Secret Service, the Alabama Department of Public Safety, the IRS, four Attorney General's offices, and many state, local, and international law enforcement officers can now log in to the UAB PhishIntel system to gain evidence of phishing crimes with a click of the mouse as well.

Despite these growing numbers of phishing sites, the banks tell us that they are even more concerned about malware than they are about phishing. Several senior banking security officials tell us that they estimate losses due to malware are three times as high as those due to phishing.

---

[1] "Global Phishing Survey: Trends and Domain Name Use in 2H2010", Aaron, G., Rasmussen, R. April 27, 2011. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf
[2] U.S. Census, "Quarterly E-Commerce Retail Sales Report", May 16, 2011, http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf
[3] "The Internet Matters", McKinsey and Company, May 2011, http://www.eg8forum.com/fr/documents/actualities/McKinsey_and_Company-internet_matters.pdf

This weekend, the UAB Spam Data Mine documented a spam email message that we received more than 60,000 times. The email message simply said "It's Bob's New Car!" and had a link to a website, claiming to show you a picture of the new car. The name was randomly generated, so that your email may have said Bob, Chris, David, or any one of thousands of names. If you clicked the link, the website you visited asked you to download and execute a Photo Archive called "archive.exe". Many tens of thousands of people visited the website, although most were too well-educated to actually run the program. Unfortunately, just by visiting the website more than twenty separate cyber attacks were launched against their computers. If they didn't have the current patches for Windows, Internet Explorer, Opera, Java, Adobe Reader, or Adobe Flash Player, the criminals would be successful in secretly causing a copy of the Zeus trojan to be downloaded and executed on their computers.

Zeus is a "keylogger" trojan. At that point, every userid and password the infected computer user types, for everything, is sent to the criminal. Email passwords, banking passwords, Facebook passwords, online shopping passwords, work systems, any password they type, along with the accompanying information about what system or website was being accessed when the password is typed, is sent to the criminal.

Because this is the Zeus trojan, the criminal can then come back to the infected computer, at any time they choose, and take remote control of the system. They can use YOUR computer with YOUR userid and YOUR password to log in to your bank account, and transfer your money anywhere they please. They can also retrieve any document on your computer and install any additional software they please. They can send emails that come from you. They can order things with your credit card. They can change your passwords! They can send instant messages (with links to viruses!) from your Instant Message or Chat program AS YOU to all of your friends.

Home users may lose hundreds of dollars each, but business banking accounts suffering losses due to a Zeus infections can approach $1 million per incident. Just this month two lawsuits on this situation have been resolved with contradictory opinions about who is responsible when a business customer loses big money to a trojan.

On June 8, 2011 the headline was "Bank dodges legal bullet over Zeus trojan lawsuit".[4] Patco Construction of Sanford, Maine was infected with the Zeus trojan. The trojan took their banking password and, logging in to their account at Ocean Bank from the construction company's computer, caused $588,000 to be transferred out of the account. The bank said it was the consumer's fault for not protecting their computer from viruses. The consumer said it was the bank's fault for not having adequate authentication measures. In this case, the bank won.

Just one week later, however, on June 15, 2011, the resolution in a second lawsuit went the other way. In that case the headline was "Court Favors EMI in Fraud Suit: Judge Says Comerica Bank Should Have Detected Wire Fraud."[5] In this case, Experi-Metal, Inc. had more than $1.9 Million in wire transfers

[4] "Bank dodges legal bullet over Zeus trojan lawsuit", Info Security News, June 8, 2011. http://www.infosecurity-us.com/view/18512/bank-dodges-legal-bullet-over-zeus-trojan-lawsuit/

[5] "Court Favors EMI in Fraud Suit", Bank Info Security, Kitten, Tracy. June 16, 2011. http://www.bankinfosecurity.asia/articles.php?art_id=3750

leave their bank account. The finding in this situation said the bank, not the customer, was responsible despite the fact that the customer's computer was the source of the compromise.

In the example about the "New Car" malware website advertised by spam, one could argue that users should know not to click on a suspicious link in email, but the risk is nearly universal at this point. In 2009, the New York Times was tricked into running a fake Vonage advertisement on their website that infected visitors with a virus. Any consumer that visited the New York Times website during the time that the malicious advertisement was in place would have a high chance of having a Zeus trojan successfully installed on their computer. The same types of malicious advertisements have been seen on many other websites, including Yahoo! and Google webpages.

Issue Two: Lack of computer science, high performance computing, or data mining to process evidence

At UAB, some of the Computer Science specialty areas where we do research include high performance computing, knowledge discovery & data mining, natural language processing, and distributed computing. Having these resources available to draw from, the UAB Computer Forensics Research Laboratory has taken a unique approach to analyzing evidence related to cyber crimes. Our laboratory has been fortunate to receive both a COPS Technology Grant from the Office of Community Oriented Policing Services, and a Byrne Grant from the Bureau of Justice Assistance, which have been combined with contributions from the Microsoft Digital Crimes Unit and the Alabama 10th Judicial Circuit District Attorney's office to create a unique environment for gathering, analyzing, and reporting on the evidence of cyber crimes.

In our lab we have three primary focus areas: spam, phishing, and malware. In each of these areas we are building Computer Science-based solutions to deal with very large quantities of evidence.

One of the challenges faced by law enforcement in the area of personal financial information being stolen is to be able to recognize the scope of the crime. Last summer we reported on a case worked by the Federal Trade Commission that I described in my blog as "Stealing $10 Million, 20 cents at a time."[6] In this case, the FTC had identified that the criminals had made 1.3 million fraudulent charges against consumer credit accounts ranging in value from 20 cents to $10. Imagine that you were a law enforcement official in a local police department receiving the phone call that someone has stolen $6 from the victim's bank account?   90% of the victims never filed any form of a complaint.

There are parallels to this type of case in spam, phishing, and malware cases.

The UAB Spam Data Mine and the UAB PhishIntel system are two systems that allow us to assist law enforcement with understanding the scope of a particular criminal activity. Because we receive a

[6] Cybercrime & Doing Time blog, "Stealing $10 Million, 20 cents at a time", Warner, Gary, July 3, 2010, http://garwarner.blogspot.com/2010/07/stealing-10-million-20-cents-at-time.html

million new spam messages per day and have more than 500 million spam email messages archived in the UAB Spam Data Mine, we can answer questions of scale and connection with regards to digital evidence.

Last month a law enforcement agency in the state of Alabama received a complaint from a citizen who had received an email purporting to be from a senior government official. Working in the UAB Spam Data Mine, we were able to determine that this was a unique email message, and provide suggestions to the investigator on how to proceed based on the very unique nature of the message. In this case, the account which sent the email was only one day old, and it was possible to prove that only a small handful of messages had been sent from the account, and that there was only one victim, indicating that the attack may have been personally motivated.

In what sounds at first to be a nearly identical complaint, another law enforcement agency received a complaint from a citizen about an email that claimed to be from the FBI. The email message indicated that the citizen had visited more than forty illegal websites and claimed that because of this, they were required to fill out the questionnaire that had been attached to the email. The attachment was actually malware that would add the computer to a botnet if the attachment was opened, leading to a potential loss of all personal information to the cyber criminal. Unlike the Alabama complaint, where the evidence would show that a single sending computer had targeted a very particular victim, in this case the UAB Spam Data Mine had received 54,720 identical email messages on the same day as the victim. We were able to identify that these messages were sent by a botnet with at least 26,928 different computers, and that it was likely tens of millions of others had received the same email. By being able to provide detailed reporting on the other activities of the botnet over time, as well as the location of each machine which had sent spam to UAB, our lab was able to help distinguish that this was a major cyber crime ring with potentially thousands of victims, as opposed to a lone wolf actor performing a revenge attack against one individual.

Issue Three: Lack of Criminal Complaints Leads to Lack of Intelligence

A problem we are facing in the fight against financial crimes is that the criminal complaint has almost disappeared. Even when a police report is filed, it is often “so the bank will give you your money back. Case closed.”

The understandable hesitation of law enforcement to “work a case” in these areas has lead to an unfortunate form of apathy by the consumer as well as the financial institutions. Large banks lose millions of dollars each year to phishing and malware, but they reimburse the cost to customers and structure the losses into the cost of doing business. Consumers have been trained that if they experience financial losses they should contact their financial institution rather than the police. If they have had their money returned by their financial institution, there is little incentive to share that information with law enforcement.

This also makes it less likely they will ever report their victimization in a way that allows intelligence-driven policing Internet crimes to occur. Without a mechanism to gather basic complaint data into a data mine, it becomes very difficult to understand the scope and nature of the crimes we are facing.

The FTC collects consumer complaints from a large number of sources, including the Internet Crime and Complaint Center (ic3.gov), the Better Business Bureau, the US Postal Inspection Service, and many state Attorney General's Offices. But there is still an enormous amount of unreported crime. The most recent FTC Consumer Sentinel Report[7] indicates 1.3 million complaints were received from consumers, however the best estimates indicate that there are now more than 11 million identity theft victims per year in the United States. One of the challenges is how to make sure these additional victims can have the crimes against them documented. If even the minor cases are documented properly, data mining of the complaint data can lead to significant cases being brought by linking the smaller cases together.

This is the basis for a new partnership called "Operation: Swordphish" which brings together UAB, the Alabama District Attorney's Association, and the Alabama Department of Public Safety. One of the key components of the project is to work with our law enforcement partners on Public Service Announcements and an awareness campaign on how to report financial cyber crimes effectively. UAB will provide support to our law enforcement partners by hosting a web server for people to report cybercrime victimization. These reports will be enhanced by comparing key pieces of information from the received complaints with information available in the UAB Spam Data Mine, UAB PhishIntel system and malware data mine to determine whether the case has links to prominent cybercrime outbreaks or to other Alabama-based crimes. In many cases, UAB will be aware of a cluster of related phishing websites, but may be lacking a victim.

Our Operation Swordphish partners agreed that when a case had an Alabama nexus, UAB would perform searches in our various databases to qualify or "triage" the case, and make an investigative lead to law enforcement.

[7] Consumer Sentinel Network Data Book for January – December 2010. Federal Trade Commission, March 2011. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

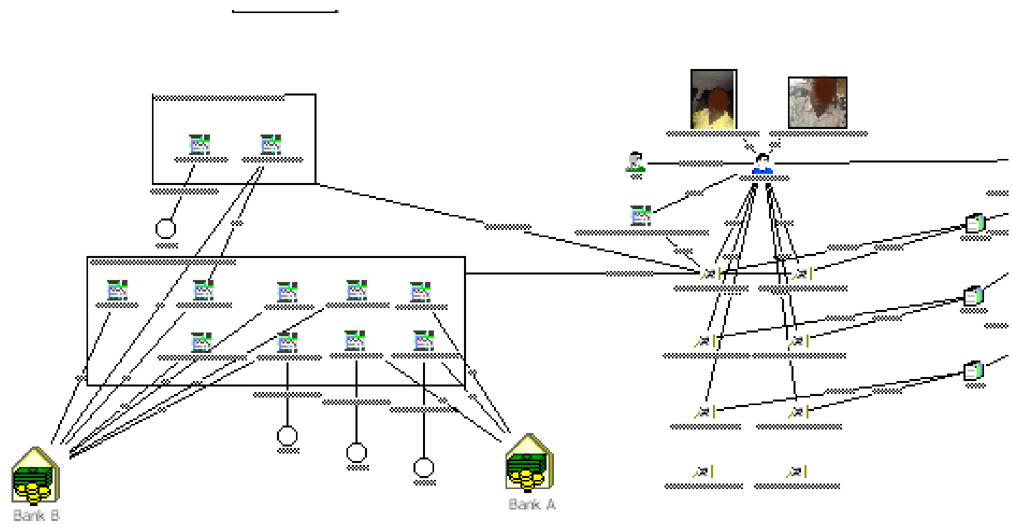

Figure 1 - An Example Operation Swordphish Case

In our first experiment in Operation Swordphish, we had identified three phishing sites for an Alabama-based bank, (Bank A) that PhishIntel showed were related by two common email addresses belonging to the criminal.

The searches revealed a small number of victims for the Alabama bank, but revealed six previously unknown phishing sites and a large number of victims for a bank in another state that we were unaware was related until the searches were performed. Several additional criminal email addresses were also revealed in the emails, including accounts that confirmed a Facebook page for the criminal.

In a second case, evidence from the UAB PhishIntel system was able to link together phishing crimes against seven financial institutions to a single criminal, based on a common email address. The criminal had hacked into three servers in order to create fake websites targeting an Alabama-based brand. UAB PhishIntel was able to provide conclusive evidence that all thirty-two phishing sites were related to one criminal. It is likely that with thirty-two known phishing sites this criminal has stolen personal financial information, and possibly funds, from hundreds of victims.

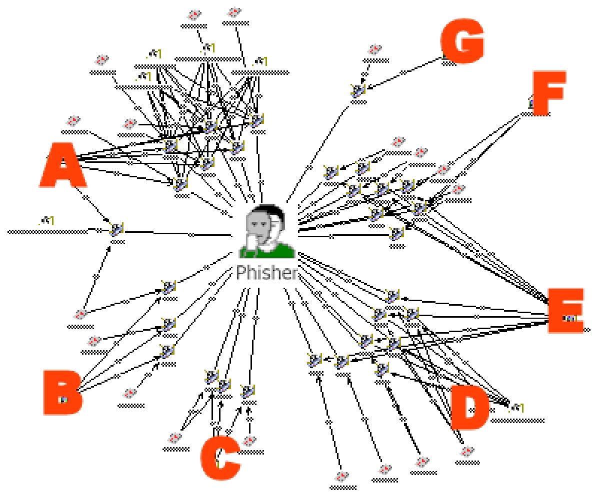

Figure 2 – In this example UAB PhishIntel links financial crimes by criminal's email

Issue Four: The international and trans-jurisdictional nature of the Internet

There are several jurisdictional issues that are faced when dealing with cyber crimes against one's personal information. One of these is that "small crimes" are normally the jurisdiction of local law enforcement while "major crimes" are more appropriate for Federal law enforcements. It is also usual that local crimes are the purview of local law enforcement while international crimes are the purview of federal law enforcement.

But what is a "local" crime on the Internet? A spammer in Nigeria sends an email to Alabama, inviting someone to visit a hacked Polish website that imitates a bank in New York. If they are successful in tricking the victim, a criminal in Romania may buy the credentials from the Nigerian and transfer the money to an account in California, where a local person removes the money and sends 50% of it via Western Union to Romania. How much money was stolen? Perhaps $500 from that victim.

It is increasingly difficult to gain law enforcement cooperation for the investigation of an international cyber crime. Some members of the committee have personal experience in this area, as servers at the House of Representatives have been compromised by website defacers from overseas. These defacements occurred in exactly the same manner in which websites are transformed into phishing sites. International gangs of hackers operate with complete impunity, boasting about their crimes and providing links to their email address, blog pages, and chat rooms in the messages they leave behind.

Website owners hosting their small business and personal websites in the United States, have had their servers hacked for use by phishing criminals more than 40,000 times so far in 2011. At the present time, I am unaware of a single situation where the hacker was arrested. Because of the experience of the crime "going overseas" many law enforcement officers are hesitant to take these cases, and local law enforcement officers question whether it is even appropriate for them to be involved in a case that is potentially international.

It is often the case that while portions of the crime may go overseas, parties to the conspiracy are located in the United States. Many financial cyber criminals have found it is easier to work with US-based accomplices to remove money from bank accounts. The most common method of doing so is to recruit a "money mule" to receive the stolen funds into an established local bank account.

Money mules often begin as disposable employees who believe they have been selected for a "work at home" job. These jobs are often advertised by spam email messages promising amazing earning potential for hard workers with little or no educational requirements or experience. A popular version at the present time is a "Mystery Shopper" position. In this position the new employee is told that they will test the customer service and friendliness of various businesses, such as check cashing businesses, bank tellers, and international money transfer services. The mystery shopper may be asked to open a new bank account and evaluate the friendliness of the bank personnel, or receive a deposit into their personal account and then evaluate the customer service of the employee at Western Union as they send the money to Eastern Europe. Some criminal organizations use several thousand money mules per year in various schemes of this sort. The advertisements promise earnings up to $300 for each assignment.

While Money Mules of the type above are likely not chargeable, many large rings of money mules continue to operate domestically with the full knowledge of their participants. Without investigating the phishing crime, the opportunity to identify this critical US-based part of the criminal enterprise is lost.

Issue Five: A Need for more trained cyber crime professionals

Others presenting testimony today will share with the committee some of the outstanding work of the US Secret Service and the National Computer Forensics Institute. We are also making a contribution at UAB by training students who will graduate from UAB with two to four years experience working in the UAB Computer Forensics Research Lab in addition to course work specifically designed to meet the needs of law enforcement cyber crime investigators.

This year UAB launched a new Masters Degree in "Computer Forensics and Security Management" which is a partnership between the Computer & Information Sciences Department, the Justice Science Department, and the School of Business.

Our outreach also involves training for current law enforcement. Specifically in the area of Phishing, we developed curriculum called "The Seven Steps of a Phishing Investigation" and presented it last October at the Digital Crimes Consortium in Montreal to over one hundred law enforcement professionals.

We continue to seek opportunities to provide more US-based law enforcement with access to our UAB PhishIntel tool, and to provide training for them in our phishing investigation methodology. PhishIntel is currently used by more than 200 users, including 70 law enforcement officers from 35 agencies.

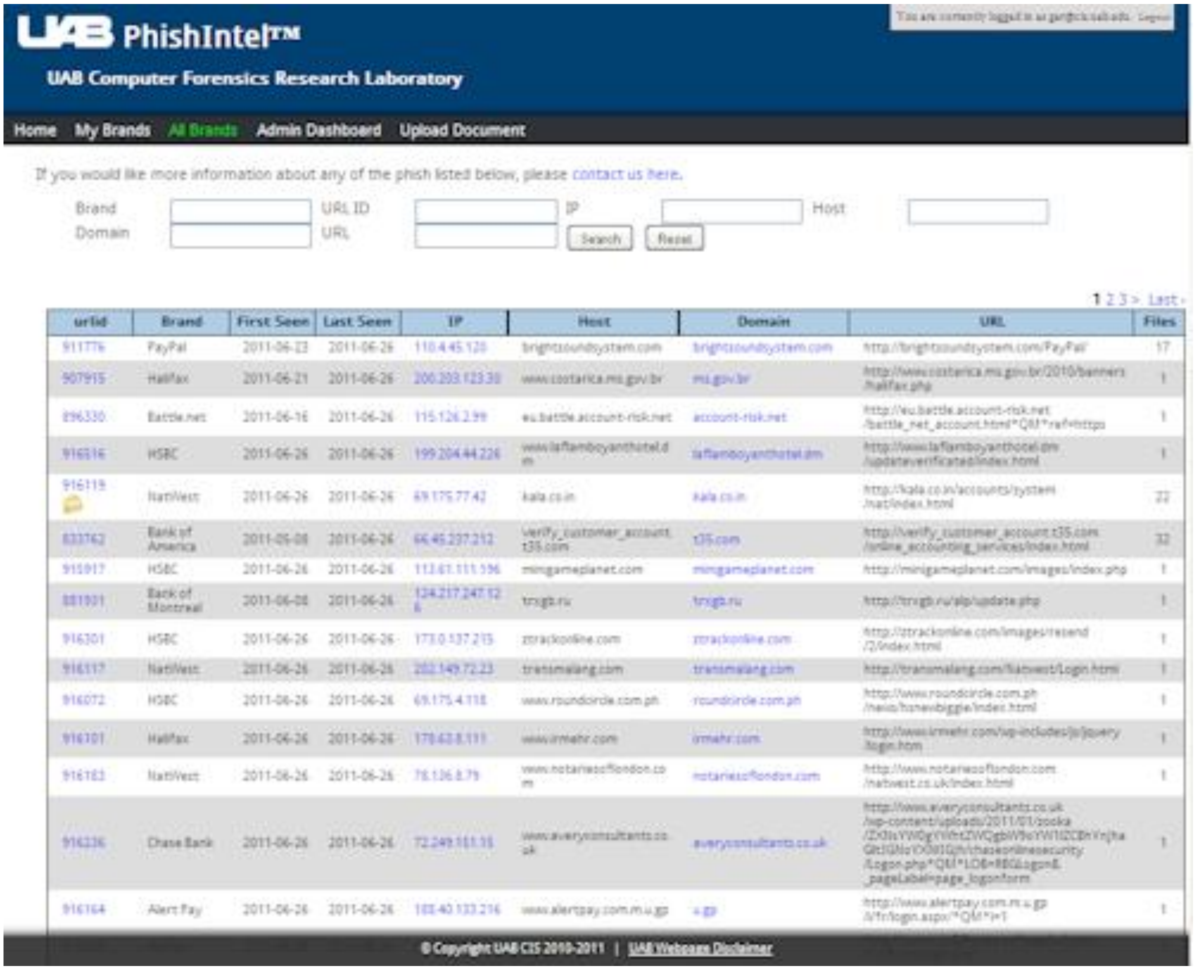

Figure 3 - An example screenshot from the UAB PhishIntel portal