

CYBER CRIMINALS GAINING SUPPORT FROM OVERSEAS OPERATIONS



GORDON SMITH
Canaudit President

I am very concerned about recent cyber incidents. There has definitely been an uptick in incidents, with new incidents reported daily. Even more interesting, the increase is in organized attacks and scams rather than single hacker-type attacks. These broad-based attacks have been around for years, increasing with the invention of bot armies (PCs that are

compromised, backdoored, and available to attack sites in concert). These attacks have reached a fever pitch as new scams have been developed and executed against poorly controlled American businesses. The most detailed report I have seen regarding one of these newer attacks appeared in the Washington Post on July 2, 2009 (see http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html).

The article details how cyber criminals engineered a scam to create wire transfers from a Bullitt County, Kentucky bank account. The cyber thieves used spyware to capture the accounts and passwords. They then changed the email address used by the bank to confirm wire transfers. After this was complete, they proceeded to steal \$415,000. The interesting part of this case is that they "hired" unsuspecting people, using online employment sites, to receive the fraudulent transfer and forward it to overseas banks. The Washington Post article does an excellent job of describing the mechanism for this fraud. It is, to say the least, quite a bold scheme. My concern as an auditor is that this fraud indicates the need for additional client-side controls, which are currently missing from many applications. In addition, we need new controls such as automated scrutiny of online transactions.

This scheme was able to work because the client machine was trojaned. Popular opinion is that the client must absorb the risk. In this case, I believe that the bank, First Federal Savings Bank, could be impacted by the bad publicity related to the incident

(see <http://www.fox41.com/Global/story.asp?s=10627534>). The reputational risk is such that we now need to reach out to our clients to ensure that their machines and the applications on their machines are safe to connect to our network.

I would like to dig a little deeper. Let us look to other areas where new fraud puts organizations at risk. My first thought is the growing number of people who work from home. They may work from home full-time, one or two days a week, or sporadically. They may use corporate or personal machines. If they are using corporate machines, one would expect the machines are protected with anti-malware software to prevent against viruses, trojans and other malicious software. I am also very concerned about staff using their home computers to login to their work email. I know that many people do not have anti-virus/malware software on their machines. Others have installed the software but stopped paying for the updates necessary to keep it current. As a result, their machines are at risk. Each time they visit a web site or open an email they may inadvertently load a keystroke logger onto their machines. When they log into the VPN or webmail application, their login credentials may be compromised.

If staff members are logging into a VPN, remember that they may have access to the internal network. If their home machine is backdoored, trojaned, or has an unauthorized keystroke logger installed, the cyber criminals may be able to login to the VPN and have access to the internal network and the devices, files and databases within it. Once they have the credentials to login to the VPN, criminals can log themselves in to capture data or take control of corporate machines for use as part of a broad-based attack on our national information infrastructure (covered later in this article).

Some of our clients require two-factor authentication. Those using tokens and other external devices, such as smart cards, to login should still be protected if the account and password is compromised. Those using digital certificates may not be so lucky. Once the cyber thief has access to a machine, they may be able to escalate their rights in order to steal the digital

certificate or cookies required to complete a successful login. In previous articles I have described how to escalate rights and easily take control of databases (see <http://www.canaudit.com/articles.html>). Extend these concepts to home PCs that have been compromised and we have an Information Technology Perfect Storm. Your security is defeated and your data and databases lie exposed to the hackers.

Home workers are not the only concern. There are also contractors who may login remotely through the VPN. This could be from their office in Canton, Ohio or Bangalore, India. If their machines are compromised and credentials stolen, then the cyber criminals will have access to program and data files the contractors have. Again, they may be able to use this access to escalate their rights up to and including the domain level. They could also compromise the Storage Area Network (SAN) to gain complete access to all of your organization's critical information. Some of the SANs have known default passwords which we have used on several client audits. Yes, they work. The warning here is that if someone is able to get into the internal network using compromised credentials, LogMeIn, or a similar product, they can easily launch a SAN attack.

Now that the risk is established, let's look to controls. The first and most important is to ensure all machines that connect to your organization's network, both internally and externally, use anti-virus and anti-spam software. The software should be updated as soon as updates are made available. It is no longer acceptable to wait several days or weeks to implement vendor updates to the malware signatures. This may be difficult for your clients. If they do not have the software, you can suggest they get it. However, there is not a lot of leverage here as customers generally do not want to buy additional software and vendors do not want to give the impression that their web sites may not be secure.

For customers that have high-value or high-volume accounts, you may want to provide the software and installation assistance to ensure that the anti-malware is in place and properly installed. This is only a slight modification of the old giveaway programs used by some banks: "Open a new account and get a new toaster!" Now it is: "Do business with us online and we will provide security software to protect your transactions."

Contractors should also be required to ensure that their machines have up-to-date anti-malware software and current malware signatures. To enforce this, you should execute your right-to-audit clause on some of your vendors each year. I suggest taking some of the

largest, plus one or two of the smallest, and subjecting them to an onsite audit. Whether malware comes in through a contractor providing 300 engineers for your project or through a sole proprietor contractor, the damage to your firm can be the same. Another good control is to subject the contractor to a security test prior to awarding them a contract. This could be in several forms such as a self-completed checklist or an onsite audit. While this may seem far-out by today's standards, in five years it will be the norm as malware incidents drive audit risk and future audits.

Do not forget to audit your offshore contractors and outsourcers as well. Every one or two years, the IT auditors should visit the foreign contractors to ensure that all contract terms, corporate policies and security requirements are met or exceeded. I am very concerned that authentication credentials may be shared by overseas contractors, particularly larger firms that "follow the sun". These contractors use their various offices around the world to support your IT requirements. As one office closes, your support may transfer to another office. The login credentials may move from one office to the next, creating a serious security issue.

It is also important to monitor the patterns of those who connect to your network. If Gordon Smith normally does two transactions a week, and today he has performed seven transactions, it is possible that the extra activity is fraudulent. It would be prudent to call Mr. Smith to confirm the transactions. If any of Mr. Smith's personal data changes, particularly email address or telephone number, it could be a signal that his credentials have been compromised. The email and phone numbers are used to contact a client when suspicious activity occurs. Watch for changes to the contact information. These changes should be confirmed by email to the old and new email addresses and possibly by phone to the old phone number as well. My stockbroker puts a hold on my online transactions after changes have been made to my personal information. I have to perform transactions over the phone until the confirmation window is concluded. As soon as a change is made to my information, they send out an email and a letter. The confirmation window is the mail time of the letter plus two days to ensure that I have read it. Although inconvenient, this is a good control.

Application controls must also be implemented. Daily and weekly transaction limits can be useful in preventing blatant procurement or EFT frauds. Variances in shipping addresses can be useful to detect diversion of goods frauds. Mailed and emailed confirmations can serve as detective controls provided changes to personal or billing information is properly confirmed as previously mentioned.

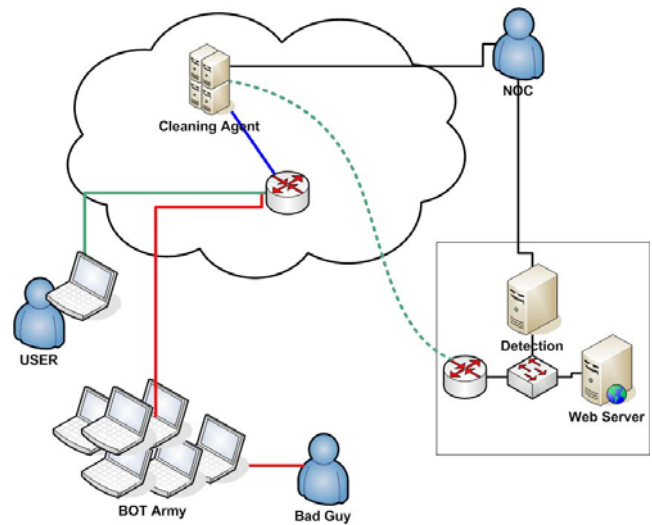
The last suggested control I will discuss relates to a security breach involving personal health information (PHI). Medical records were recently compromised by what was termed a “virus”. The “virus” mentioned in the article is called Coreflood (see <http://www.healthcareitnews.com/news/virus-blamed-ehr-breach-canada>). Several times a day, machines connected to your network should be scanned for malware. Ensure that your security folks test for all known spyware and malware. In some cases, they will balk at this suggestion. I consider this the same as car seat belts when they first came out. Many people did not wear them, as they did not see the benefit. Even I balked at wearing one until the police started to enforce it. Now we know that seat belts really do save lives. Let me tell you, actively searching for spy and malware will lead to early detection of a potential security breach and mitigate the damage that can be done.

The second item I want to cover in this article is the ability for nations, individuals, groups and conglomerates to paralyze a website. Earlier this month, the alleged North Korean attacks against government sites and the New York Stock Exchange demonstrate the distributed denial-of-service (DDoS) attack (see <http://www.foxnews.com/story/0,2933,530560,00.html> and <http://www.foxnews.com/story/0,2933,530762,00.html>).

I have two concerns. The first is that most organizations do not perform regular web application audits. We believe that this is an essential part of a security or IT audit regimen. Our Web Application Security Assessments generally reveal that there are significant security flaws in web-based applications. These flaws must be detected and remediated before your organization becomes a victim of organized criminals seeking to earn a living off of companies with shoddy controls. I need not mention the everyday hacker and the risks they pose. These are already well known.

I am also concerned that news articles represent that there is little that can be done to respond to a denial-of-service attack. That is not only incorrect, but it leads to an acceptance of a serious risk without proper evaluation. Cisco wrote a fantastic white paper on this issue (see http://www.cisco.com/en/US/tech/tk59/technologies_white_paper09186a0080174a5b.shtml#prevention).

I use three slides in my IT Audit and Security Boot Camp to show the before, during and after examples of a DDoS. One of these slides is below. It shows how to successfully deal with a DDoS:



In the example shown, the ISP for the client is using a cleansing agent to identify the DDoS messages and filter them out. This cleansing agent is a massive software application that is invoked when a DDoS is detected for supported clients. We suggest that you check with your ISP to determine if they have this type of software and what the cost of invoking the product is. If they do not have a product, then it is time to look for a new ISP. Do not wait until the bot army of compromised machines is pointed at your site and commences firing.

The bad guys are constantly scouring the Internet and phishing in their quest for poorly secured machines. Once found, they take control of the machines, place their software on them, and organize them into a battle group for hire. They then rent out their bot armies to those who can pay. In some cases, even governments have been known to use bot armies. The Russians apparently did prior to and during their attack on Georgia on August 7, 2007. It crippled the ability of Georgia to respond to the attack. On July 4, North Korea may have done the same thing to our government.

The lesson here is do not let complacency or a feeling of hopelessness prevent your firm from building the cyber defenses needed in today’s environment. You need to be able to ensure controls are in place in your network and the networks that connect to yours. You also need to be able to respond to a cyber attack and deflect a DDoS by a massive bot army. All of these things can be achieved. Given the risks of the last few weeks, now is the time to start a detailed risk analysis of the client-side and application risks.

The opinions expressed in this article are mine and mine alone. I look forward to receiving your comments on this article and answering any questions you may have. You can email me at Gordon@canaudit.com If you would like to receive articles like this in the future directly, please opt-in to our distribution list on the Canaudit website.

As always, I like to provide an incentive for my clients to conduct the required audit work. I believe that the web application and external risk is very high. Therefore, I am willing to price an Internet Review and Web Application Security Assessment for our clients at \$12,500. To qualify, the audit must be confirmed by August 31, 2009 and performed in August or September of 2009. If purchased separately, the cost is \$23,000. For those clients who want to review both the internal and external security risks, we will provide a 10% discount on our IT Security Baseline or Network Penetration Audit. To qualify, the audit must be confirmed by August 31, 2009 and performed in September or October of 2009.

If you would like additional information on how Canaudit can assist you with risk identification and remediation methodologies, please contact Tamra Savage Jones at (805) 583-3723 or by emailing her at Tamra@canaudit.com.

AUDIT & SECURITY SERVICES

Canaudit specializes in a variety of information system and technology audits, ranging from periodic network penetration testing to full network and operating system security review. Our tailored audits provide an objective, disciplined, and in-depth analysis to evaluate and improve the effectiveness of risk management, control and security within your organization's technological environment.

For interest in Canaudit to perform an IT audit for your organization, please email Gordon@canaudit.com or Tamra@canaudit.com, or call (805) 583-3723.

PROFESSIONAL DEVELOPMENT

Canaudit provides quality seminars to various organizations including audit and security chapters and major corporations. These seminars range from technical information system audit classes to internal audit classes aimed at everyone from an introductory level up to management. With nearly 20 courses to choose from, we are sure to have one that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. For more information and to register for upcoming public courses, visit our website at www.canaudit.com.

Upcoming Public Courses:

St. Louis, MO

August 12-13, 2009

Control and Security of Web Applications (*Hands-On*)

Phoenix, AZ

November 16-19, 2009

November 16-17, 2009

November 18-19, 2009

Hands-On: Performing an IT Audit and Security Baseline (*Hands-On*)

Control and Security of UNIX

Understanding and Preventing Electronic Fraud

For additional information or to schedule a Canaudit seminar, please email Brenna@canaudit.com or call (805) 583-3723.
