CYBER SECURITY ADVISORY

27 October 2010

Albany, Buffalo & New York Divisions

Web 2.0 Security for Businesses and Employees

EXECUTIVE SUMMARY:

The totality of information provided by company and employee websites, blogs and profiles can lead to significant losses that would have required physical espionage to acquire the information a decade ago. In the last several years, the Internet has shifted toward an interactive environment that facilitates this information sharing, increasing the security concerns for business owners and employees. The creation of interactive web sites allows unsophisticated users to post a wide variety of information, instantly; information that will exist forever. As Web 2.0 has developed, so has Malware 2.0. This newer malware requires little, if any, user intervention. Criminals use the Internet to identify targets, develop targeted campaigns, steal information and money, and damage reputations.

This Cyber Security Advisory is provided to assist the private sector and Federal, state, and local government agencies in effectively deterring, preventing, preempting, and responding to dynamic user-based web content vulnerabilities. It is specifically intended for corporations, state and local homeland security officials and law enforcement to share with personnel and private sector entities responsible for policy and information security to discuss mitigation measures related to dynamic user-based web content. Please distribute to your employees, customers, clients, and anyone else with an interest.

DETAILS:

Web 2.0 is a term that refers to the ongoing shift toward user-based, dynamic web content and away from static web pages produced solely by professionals with programming experience. Web 1.0 allowed an Internet user to read content, Web 2.0 allows the user an interactive experience.

One of the primary effects of Web 2.0 growth is the creation of online communities and social networking sites (SNS), which cyber criminals have co-opted into malware distribution sites. An employee who visits these sites from work may inadvertently download the malware onto the company network, infecting the network with a keystroke logger, botnet or other malware. Zeus, Spyeye and similar malware, noted for their financial login compromises, are capable of stealing much more. Each attacker can modify these programs to fit their own needs, so the malware can collect information from social networking websites, company login pages and most websites that use a standard login form. The keylogger function could also be used without any additional components to gather login credentials, intellectual property or sensitive data. While many criminals rely on this type of malware to facilitate financial crimes, criminals have blackmailed companies, threatening to expose sensitive data or the actual breach to clients and investors. Other criminals steal the information to further their own business objectives or find ways to harm a company involved in negotiations.

Criminals and competitors, including those in other countries, use Web 2.0 sites to gather sensitive information. While the information posted to a single website by a single employee may not provide an abundance of details, the information posted by a single employee to multiple websites may provide a more complete picture. The information posted by multiple employees to multiple websites may provide a very complete picture. Criminals can use this information to target specific employees or companies for a multitude of purposes. Information on these sites frequently includes the answers to security questions asked by secure websites, such as "What year did you graduate high school?" and "What is the name of your favorite pet?" These sites also allow criminals to determine family members, home addresses, and routines, which makes targeting a house for burglary or family for revenge much simpler. Company specific information may be available through job title and employment location fields, and through metadata such as login IP address, and the data stored in the properties of a photograph. Criminals can use information from multiple employees to map networks, expose sensitive projects, or for social engineering, leading to specially crafted malware, blackmail or spear phishing campaigns. Automated programs that aid criminals in these tasks are widely available on the Internet.

With a growing number of smartphone users who access business data and Web 2.0 sites through their phones, which lack antivirus and other standard computer security precautions, data theft through a phone compromise is an increasing threat. Criminals have recently targeted smartphones for malware and a growing number of researchers are issuing warnings about the dangers of phone applications and how much information they transmit "home."

Even when a company or user is extremely careful online, it is impossible to control what is posted by others about the user or organization. The CEO may follow all the security recommendations and best practices, but the CEO's secretary may inadvertently defeat all of these precautions with a blog that provides information about the CEO. Client and competitor posts are even more difficult to control or monitor. Criminals may also post false profiles on SNS or within virtual worlds, to provide false information, damage reputations or gather the personal details of anyone who friends the false profile.

Web 2.0 allows for urban legends, inaccurate reports and chain letters to spread wildly. Through these reports, instigated by current and former employees, dissatisfied customers, protestors or random strangers, any company may become the target of blackmail, a cyber-protest or attack. Law enforcement agencies receive phone calls regarding "gang initiation" practices, hypodermic needle warnings, poisoned perfumes and other urban legends that spread through email chains and these web sites. Web 2.0 allows for the broad dissemination of information, so small companies previously known only to their local clients may find themselves at the center of a controversy originating in a foreign country. Local or date specific information may have its details removed, allowing it to be circulated perpetually, while inaccurate rumors circle the globe repeatedly without any fact checking.

Employees can pose threats to a company through their extracurricular activities. A security guard, Jesse McGraw, at the Carrell Clinic, Dallas, TX, lived online as "GhostExodus," founder and leader of the Electronik Tribulation Army. In 2009, when McGraw saw the hospital had poor cyber security, he installed malware on hospital computers that added the computers to a botnet, with the intention of conducting a distributed denial of service (DDOS) attack on July 4th. Although arrested in June 2009, McGraw had already used YouTube to post videos of himself compromising the computers and issued callouts to other hackers to conduct DDOS attacks on July 4th.[1]

[1]Wilonsky, Robert. (July 2009) Hacked! Dallas Federal Grand Jury Indicts Electronik Tribulation Army's GhostExodus. *Dallas Observer*. http://blogs.dallasobserver.com/unfairpark/2009/07/hacked_dallas_federal_grand_ju.php, 10/5/2010.

MYTHS:

Myth 1: I'm too small to be a target.

Facts: Anyone who conducts transactions or accesses the Internet can be a target or a victim. Web 2.0 allows for rapid and widely disseminated information without any verification of accuracy; more than any other form of communication. Any dissatisfied customer or employee can post negative information and damage a reputation. Intentionally, accidentally or maliciously, information about a company or employee's transactions will become available on the Internet, creating a potential breach of security. Criminals looking for victims cast a wide net through indiscriminate malware disseminations, including distributions through advertisements on legitimate sites, such as Facebook and Twitter. These infections provide login credentials or files to criminals, which facilitate several forms of fraud.

Myth 2: Too many things need to happen for me to be infected. / Antivirus software and firewalls protect me.

Facts: In theory, to construct a successful attack, a criminal must identify the business or user, craft malware or a spear phishing campaign specific to the business or user, get past any antivirus, firewalls, filters or other protective devices and then convince a user to activate the malware. But that assumes the business is fully patched, running the most up-to-date software and following the best security practices and the criminal is attacking a specific business or user. While reports vary regarding the effectiveness of antivirus software, no antivirus program catches everything and zero day exploits are continually developed. Every day cyber news organizations report multiple intrusions into companies that were following best practices.

The w32.Koobface worm spread through SNS in 2008, building a peer-to-peer botnet. The worm used SNS to convince users that a friend had posted a link to a video file. When the user clicked on the link they were asked to download the additional software necessary to view the file, and instead downloaded the malware. Koobface was able to steal information, block access to certain Internet sites, steal license keys and install other software. In August 2009, a year after the original infection, Symantec was still reporting new infections and new variations of the worm.[2]

Myth 3: No one would want to attack me. My information is not important/I don't have enough money.

Facts: Not all compromises are espionage related; financial thefts include smaller amounts totaling just a few thousand dollars. The "hitman scam" is one of the most notorious small level scams and targets users through their publicly posted information. In the classic version of the scam, the criminal identifies a potential target and researches them through the Internet. After learning enough about the victim that the criminal can convince the victim he is being watched, the criminal contacts the victim and identifies himself as a hitman who has been hired to kill the victim. The criminal then proceeds to explain that he has watched the victim for several days and the victim seems like a nice person, so the victim can pay the criminal the same amount as the original hit and the criminal will not follow through with the assassination. Variations of this scam involve the criminal identifying a victim who has a family member living or traveling overseas. The criminal pretends the family member has been injured, arrested or kidnapped, and the criminal is a friend who is trying to rescue the family member but needs money to do so. These scams are successful because they use online information to dupe the victim into thinking the criminal knows personal data, providing an instant connection between the two. Every version of this scam involves small amounts of money, totaling only a few thousand dollars.

[2] Symantec. (September 2009) Busy Days for the Koobface Gang. *Symantec*. http://www.symantec.com/connect/blogs/busy-days-koobface-gang, 10/6/10.

Criminals may have a personal vendetta against a business or employee and use cyber attacks. In one of the more infamous insider-created cyber attacks, the Maroochy Wastewater Treatment Plant, Queensland, Australia, experienced a series of malfunctions with its new system over several months in 2000. When the culprit was identified, he was a former contractor who knew the system and used a commercially available radio transmitter and stolen software to control sewage flow to disrupt company operations and gain revenge. Forty-six separate incidents disrupted the plant, the most severe of which released more than one million liters of raw sewage into local waterways.[3]

Myth 4: I am careful online, I use security settings and no one could use what I post against me.
Facts: Metadata and the totality of posts can be just as valuable. If a criminal can watch posts from multiple employees of one company for login names and other information, then they can begin to map the company network. Multiple posts from the organization may also allow a criminal to develop a "big picture," learning about special projects, clients, employee travel and company vulnerabilities.

The "get to know me" posts ask for information that is commonly used to vet a user's identity by a financial institution or security service. Security settings are notorious for loopholes and controversial measures, as evidenced by the ongoing debate surrounding the Facebook privacy settings which default to a completely open status. Additionally, security settings are only as strong as the company that holds them. Websites based outside of the U.S. adhere to different laws and may not protect user privacy or may share private information with government authorities. All sites are at risk of cyber breaches and personal information may be compromised through such a breach.

Several examples exist of fake profiles used to damage reputations or lure in unsuspecting users. In July 2010, news stories exposed "Robin Sage," the fake profile on LinkedIn, Twitter and Facebook that deceived experienced members of the US intelligence community. "Robin" invited members of the intelligence community to be friends with her and many accepted. A US Army Ranger befriended her, which allowed "Robin" to see the GeoIP data hidden within pictures on the Ranger's profile. This information and online discussions between Rangers was enough for "Robin" to locate the Rangers in Afghanistan and learn where they were going. "Robin" became friends with members in the Joint Chiefs of Staff, the CIO of NSA, an intelligence director for the U.S. Marines, a chief of staff for the U.S. House of Representatives and several Pentagon and Department of Defense employees. "Robin" also received job offers from several major firms.[4]

[3] IEEE. (August 2009) Control System Security in the Shift to Open Systems. *IEEE.* http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05333007, 10/6/10.
[4] Higgins, Kelly Jackson. (July 2010) 'Robin Sage' Profile Duped Military Intelligence, IT Security Pros. *Dark Reading.* http://www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=225702468&cid=RSSfeed_DR_News, 10/6/10.

RECOMMENDATIONS:

The following recommendations are cyber security best practices that help reduce the risks associated with Web 2.0 use. Nothing can eliminate *all* of the risks, however, an informed and vigilant user is a key defense.

To take a proactive approach against this type of vulnerability, distribute this entire paper to your Information Technology and Security staff and the first four pages of this paper to your employees and clients. Provide the Employee Recommendations to your users as part of an ongoing cyber security awareness program. Distributing a few recommendations at a time will help your employees become more aware of cyber security matters without overwhelming them.

Enterprise Recommendations for Web 2.0 Protection:

- Standardize what information is released, by whom, to where, and in what format.
- Create company policies that inform employees about vulnerabilities created by mixing professional information with their personal lives, such as posting pictures in uniform or professional titles on social networking sites.
- Beware that what happens on the Internet stays on the Internet, forever. Just because it has been taken down, it is not gone.
- Know what information is on the Internet. Run periodic Internet searches on the company, phone numbers, email addresses, physical addresses, etc.
- If the company has the legal authority, vet employees and potential employees online.
- Require business issued mobile phones to have a password to unlock the phone. Install software that will allow a phone to be remotely erased and that erases all data on the phone after a set number of failed login attempts.

Employee Recommendations for Web 2.0 Protection:

- Understand company policies that address mixing professional and personal lives, such as posting pictures in uniform or professional titles on social networking sites.
- Beware that what happens on the Internet stays on the Internet, forever. Just because it has been taken down, it is not gone.
- Log out from the site when you are done and close your Internet browser window.
- Be careful when clicking on a URL from a friend, email, SNS or instant message, especially shortened URLs (eg: bit.ly, TinyURL).
- Do not use the same login name and password for every website. Before entering personal information into a website, check its authenticity. Who owns the website? Are there positive or negative reviews about it on the Internet? What does the Better Business Bureau say about the company?
- Do not mix your business contacts with your personal contacts.
- Limit the amount of personal information posted online. Do not post information about your schedule, location or ways to physically contact you. Do not complete "get to know me" forms that ask a large number of personal questions. Remember that information from multiple sites can be combined to form a more complete picture.
- Do not to allow any website to remember your password.
- Set profile privacy levels properly and stay current with privacy changes.
- Do not assume that profiles contain accurate information. Age-verification mechanisms have a low success rate. Fake profiles and malicious profiles are extremely common.
- Immediately report stolen or lost mobile phones or compromised accounts to your security officer.

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Best Enterprise Security Practice Recommendations:

- Install a security software suite from a reputable vendor that includes antivirus, anti-spyware, malware and adware detection. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans on a routine basis. This will help to protect a computer against known viruses, malware, and adware, but remember many viruses, malware, and adware programs are undetectable by antivirus software.
- Use spam filtering techniques.
- Routinely install all new software and hardware patches or use the automatic update feature when available. Ensure that all your application software such as Microsoft Office, Adobe Flash, Apple QuickTime, Adobe Acrobat, etc., are updated as well and not just the computer's operating system.
- Use a dedicated computer with a static IP address for all online financial transactions and implement white listing methods to prevent the system from going to any site/address that does not have a documented business need. If possible, register the static IP address with the financial institution. Actively monitor the computer for viruses and other malware.
- Consider blocking Internet plug-ins on the computers that access online accounts. Disabling Flash, scripts, pop-up windows, etc. can be frustrating for general users but prevent multiple exploits.
- Educate users on good cyber security practices to include how to avoid having malware installed on a computer and new malware trends such as the development of fake antivirus, and malvertising, where malware is hidden in the advertisements posted on a legitimate website.
- When dealing with a computer professional research their background and the reputation of their brand. Beware of cash deals and cheap software.
- Control the sites your employees have access to. Implement block/black lists and enforce them on the network perimeter.
- Employ advanced authentication techniques for user logins (two-factor authentication).
- Utilize a security expert to test your network ("penetration testing") or run security software that will aid in closing known vulnerabilities.
- Monitor log files, especially proxy server logs, for unauthorized/suspicious Internet connections. Check for incoming and outgoing connections.
- Develop a working relationship with a member of law enforcement so there is an established venue for reporting incidents.
- Whenever possible, do not use a wireless network for financial transactions. If a wireless network must be used, enforce security measures such as enabling encryption and MAC address filtering, changing the service set identifier (SSID) and turning off SSID broadcasting.
- Change the default login names and passwords on routers, firewalls, other network equipment and software.
- Use the on-screen keyboard when possible to circumvent keystroke loggers. Newer keystroke loggers capture a screen image every time a key is pressed or mouse button clicked so the on-screen keyboard may not be a completely effective preventative measure.
- Add a caveat to the computer user agreement (CUA) that warns employees about posting to the Internet from company computers or posting about the company.
- Clean erase and reformat all harddrives and media before releasing them for overseas travel or destruction. Include smartphones, personal electronic devices (PEDs), copier and fax machines harddrives in this practice.

Best Employee Security Practice Recommendations:

- Change your passwords frequently.
- Immediately report any suspicious activity in your accounts. There is a limited recovery window and a rapid response may prevent additional losses.
- Do not install any software without first checking with your Information Technology staff. Many new malware packages are made to look like legitimate software, even requiring a credit card for purchase and providing a 24 hour English-language telephone support line.
- Use a "non-privileged user" account on the computer to prevent unauthorized changes. Use this non-privileged account for web browsing whenever possible.
- Make sure any financial or transaction site you are using starts with "https://" instead of "http://". The "s" indicates a secure transaction, using a different method of communication than standard Internet traffic.
- Know what the financial institution's website looks like and what questions are asked to verify your identity. Some attacks, known as man-in-the-middle attacks, will change the login page. These changes allow the attacker to see your answers and to add additional security questions. When you login, the information is transmitted to the attacker and to your financial institution, logging you into your bank's website while also giving your attacker all your account information. A vigilant user can sometimes spot these attacks by noticing slight modifications to the standard page: extra security questions, poor grammar, misspellings, a fuzzy or older logo or a change in the location of webpage features.
- Do not open emails from un-trusted sources or suspicious emails from trusted sources.
- Be suspicious of emails and text messages purporting to be from friends, co-workers, other companies, or a government agency. No company should contact you via email to request you to verify information. If you do not think the person sending the email would send you an email with that subject line or type of information, delete the email or call to verify its authenticity. If you believe the contact may be legitimate, do not use the link provided in the email, instead type the link in the Internet browser's address bar. Be aware "Reading Pane" features, like those within Microsoft Outlook, automatically open the emails they display. Phishing attacks may appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as disasters (e.g., Deepwater Horizon oil spill, Haiti earthquake), epidemics and health scares (e.g., toxic sludge near Danube, H1N1), economic concerns (e.g., IRS scams), major political elections, and holidays.
- Restrict online purchases to "one-time credit cards" or "Virtual Account Numbers" to reduce the risk of account numbers being compromised. If you do shop with a regular credit card, use only a single credit card, with a low limit. Choose a credit card with an online purchase protection plan, if possible, and monitor the activity on that card as often as possible; at least every two or three days.
- Avoid using check or debit cards for online transactions.
- Always lock your computer when you leave it unattended. Set the computer to automatically lock after a set period of inactivity, e.g. 15 minutes.
- Do not allow your computer or web browser to save your login names or passwords.
- Use a strong password; at least 10 characters combining upper case and lower case letters, numbers and symbols.
- Clear the Internet browser's cache before visiting a website requiring financial transactions.
- Never access your financial institution or a privileged/sensitive system from a public computer at a hotel, library or public wireless access point.

- Properly log out of all web sites and close the browser window. Simply closing the active window may not be enough.
- When you are finished with your computer, turn it off or disconnect it from the Internet by unplugging the modem or Ethernet/DSL cable.
- Do not use the same computer for online transactions that children or "non-savvy" Internet users use for regular Internet access.
- Do not use the login or password for your financial institution on any other website or software. Do not write it down. Do not post your personal information on the web. Your high school, date of graduation, maiden name, date of birth, first car, first school, sibling's names, mother's full name, father's full name, best friend's name, etc. are the answers to many security questions on financial websites. When you post this information, you are making it easier for criminals to gain access to your financial information.

My account was compromised, what now?

- Immediately stop using any computers that may be involved.
- If the compromise involves financial transactions, contact your financial institution to request their help in preventing further loss and to aid in the possible recovery of any money.
- If the compromise involves an online account, contact the company holding that account and ask for their help in remediation.
- Begin a log of your activities, including who you have talked with, what information you have and what mitigation steps you have taken.
- Ask the company to report the incident to local law enforcement (for personal accounts), New York State Police, the Federal Bureau of Investigation or the United States Secret Service.
- Confirm that the company reported the incident and call the appropriate agency yourself to provide additional details.

Points of Contact	
FBI Albany 200 McCarty Ave. Albany, NY 12209 518-465-7551	MS-ISAC 31 Tech Valley Drive East Greenbush, NY 12061 (518) 266-3485 7x24 SOC 1-866-787-4722
NY State Police Cyber Crime Unit 1220 Washington Ave. Albany, NY 12226 518-457-8812	United States Secret Service, Albany 39 N Pearl St # 2 Albany, NY 12207-2785 (518) 436-9600
NY State Division of Homeland Security and Emergency Services Office of Cyber Security 30 S. Pearl Street P2 Albany, New York 12207-3425 518-474-0865	NY State Division of Homeland Security and Emergency Services Office of Homeland Security 1220 Washington Avenue State Office Campus Building 7A Suite 710 Albany, NY 12242 518-402-2227