https://doi.org/10.48009/2_iis_2008_634-638

SECURITY OF PERSONAL IDENTIFIABLE INFORMATION

Jack D. Shorter,Texas A&M University – Kingsville, jack.shorter@tamuk.edu
Karen A. Forcht, North Carolina A & T University, forchtka@ncat.edu
Alicia Aldridge,Appalachian State University, alicia@appstate.edu
Daphyne S. Thomas, James Madison University,thomasds@jmu.edu

Abstract

In today's fast moving world, the use of technology has become a part of everyday life. Whether it is using a computer to access the Internet, sending email, or using cell phones to contact friends and family, technology is found in almost everything. Technology provides many conveniences such as online banking, renewing a driver's license, making a consumer purchase, or conducting research. However, using technology has its pros and cons. On the positive side, conducting personal business online is convenient, saves time, and is economical. However, with the pluses, there are usually minuses as well. In the case of an online consumer purchase, one may find price deals, but may discover a lack of quality or poor customer care. Also, with online advertising growing at such a high rate, the use of imbedded spyware or adware has also increased. Still, one of today's biggest threats is identity theft and the use of Personal Identifiable Information (PII). This paper discusses mishandling and appropriate handling of personal information and the difficulty of keeping up with ever-changing security threats.

Keywords: personal information, privacy, identity theft security, virus

INTRODUCTION

Privacy advocates are becoming concerned with how search engines may obtain and store user PII. One such concern is how Google maintains records of time stamps, search strings, and associated IP addresses. Google gathers a vast amount of information in the services they provide, such as Google Search, Google Talk, and Google Mail, to name a few. If the question was asked, "Does Google own us?" [10] one could easily argue no. Ownership implies having power over another, which Google does not have. However, the length that Google retains user data does deserve attention as it is a legitimate matter of concern. Due to the length that a user's data is held, how would users be impacted if Google's merger with DoubleClick is completed?

DoubleClick is one of the fastest growing digital marketers, and the amount of user data that could be provided to them from Google would be phenomenal. At issue is whether Google can be trusted with users' PII at its disposal. Armed with this information DoubleClick could target consumers with a method known as "retargeting." This type of practice was one of the topics discussed at the 17th annual Conference on Computers, Freedom & Privacy in May 2007. This method uses ads and serves them to users based on their Web surfing behaviors. [4]

A user uses a search engine such as Google to find a product such as Music CD. When the user clicks on one of the search results, a page loads a "capture" in two steps. [4] First, a 1-by-1 pixel known as a Web beacon is embedded in a graphic on the results page. A request is sent to the ad network's server where the graphic resides and a CD ad for the user is chosen. A cookie is then placed on the user's system, usually without the user knowing, which follows and reports his or her tendencies. When surfing at a later time, if the website currently viewed by the user is a member of the ad network, an ad for the CD will follow that user. Why does this create concern for privacy advocates? Because the information obtained using such methods is abused. This results in annoying pop up ads becoming a problem, or worse, the cookies used have malware or other malicious software attached. [4]

Google asserts that their intention is to collect PII and use the information to improve services and protect them against security vulnerabilities. [10] One of the biggest concerns by a leading privacy advocate, Privacy International, is in a report that criticizes Google on their privacy practices. The report states that the reason for the failure is due to the length that Google holds onto a user's information. Google is on record stating that they retain the information for 18 to 24 months. After that, Google makes all search logs anonymous. A popular European metasearch engine, Isquix, states that they delete users PII after 48 hours. Isquix maintains that there is no significant

impact on performance with the lengthy retention of users' data.[10]

Google insists it is being misrepresented, saying that the Privacy International report has inaccuracies and mistakes. [10] Google's General Counsel could not specify any mistakes, but pointed out that every product launched by Google now includes a lawyer trained on privacy issues. Those that support Google have lauded their recent efforts to choose to ignore a Department of Justice (DOJ) subpoena of their search engine logs, where their biggest competitors, AOL, Microsoft, and Yahoo, complied and surrendered their logs. The government cites the reason for the subpoena was to investigate how often children accidentally find pornography sites. The government making a move to obtain this data demonstrates that law makers are hungry to track people's Internet tendencies. Although refusing to comply with the DOJ subpoena is a noble gesture, one may ask what Google may be hiding. As stated by the Executive Director Marc Rotenberg of EPIC, a leading privacy advocate, "we supported Google when they made the decision," but he also acknowledged that EPIC felt it was a mistake to retain user information for so long. [10]

Right to Privacy or Criminal Negligence?

Even though strides are being made in the protection of PII, there is a move afoot to help criminals obscure their illegal online activities. The Internet Corporation for Assigned Names and Numbers (ICANN) is considering making it possible for anyone to avoid putting Web site ownership and contact information into the Internet's WHOIS database. Today's Internet already has very loose requirements for website registration. The argument being made is that the "less that is known about a Web site owner, the better a person's rights are protected." [2] The irony in such a move is in fact that those who are intended to be protected, are indeed the ones that are affected the most. The negligence in such a move would allow crooks to defraud Internet users by targeting them in phishing scams. These scams often redirect victims to counterfeit web sites, and then dupe the intended victim into providing some form of PII, such as bank account information. The WHOIS data base is one small tool available to identify and shut down spurious Web sites such as this. Consumer Reports says that "more than a million people lost a total of $2.1 billion during the past two years from phishing". [3] Without a resource such as WHOIS, matters may become much worse. A policy being pursued by ICANN and creating great concern for security chiefs and privacy advocates is Operational Point of Contact. This policy would eliminate the requirement that site owners identify themselves in WHOIS. Opponents of the Operational Point of Contact policy have proposed a policy known as Special Circumstances. This policy would let individuals and organizations such as shelters for abused women hide their WHOIS data from prying eyes. Many feel that this is a better option if they find that a change is necessary. Is a change really necessary though? There will be no appreciable privacy gains by adopting a new policy, "except in the abstract thinking of privacy-rights zealots." [2] The reality of such a move is that it is more likely that increasing numbers of people will get their private information stolen if ICANN embraces Operational Point of Contact for WHOIS. At least with WHOIS, a search of the website's owner can be done. Another growing problem is a variation of phishing known as Typosquatters.

Typosquatters and Botnets

Typosquatters prey on online consumers' poor typing skills. Dozens, if not hundreds, of possible misspelled domain names are used to build vast networks of Web sites to siphon traffic away from legitimate companies. A botnet is a large number of typical Web users' computers that are compromised via a Trojan horse program to create and send spam or viruses. Siphoning traffic away from legitimate sites provides the online underworld with the opportunity to employ users' machines to send out malware used to hijack another user's machine for use in a botnet. This underworld has been nicknamed the "botnet mafia.' [9] and is buying and selling control of computers. Security firm Symantec Corp. estimates that six million home and office computers worldwide have been involved in botnets since January. These families amass bots through weak security systems and rent out 10,000 strong armies at $4 per bot. Malware is spewing across the Internet so pervasively that some hackers must defend the compromised machines that they control. IDC estimates that malware writers release 450 new strains of viruses, Trojan horses and other apps of their ilk each month. [9] Web application vulnerabilities have contributed to the success of attacks because the lack of security within the application is like leaving an open door to attackers. Cenzic Inc. concluded that the percentage of security holes in applications jumped to 72% in Q2 2007 from 67% in Q1 2007. [9] Mandepp Khera of Cenzic emphasized that Web application developers continue to short cut security in part because they are not taught how to write secure programs in school. "This

shortfall in security is due to development timelines, and programmers barely have the time to get all the functionality in their applications." [3] With the lack of security built into many of today's Web-based applications, the keepers of PII have a responsibility to handle that information appropriately.

Government mishandling of information

Texas has been identified as mishandling personal information on the Secretary of State's SOSDirect website. Sensitive personal data about thousands of Texans, to include former Dallas Cowboy Troy Aikman, is available on the website. The Secretary of State's office commented that Texas "is working to remove sensitive information from the Web so the data can't be misused by criminals." [6] The state has been automatically removing personal data from all documents filed since June 2005. However, Scott Haywood, a spokesman from the Secretary of State's office, added that residents whose Social Security numbers are posted in documents on the SOSDirect need to contact the Secretary of State in order to have them removed right away. Mr. Haywood commented that "the office is committed to protecting personal information, but the office of the Secretary of State has a responsibility to post public information that has been submitted to the office." [6] The office maintains that it is trying to balance those responsibilities.

Recent notable exploits

Attackers using a Trojan horse stole more that 1.6 million records belonging to users of Monster Worldwide Inc.'s online job search service. [5] The malicious program utilized the pilfered data to send Monster.com users phishing emails that planted malware on their machines. The phishing scams and malware were targeted at stealing names, email addresses, home addresses, phone numbers and resume identification numbers of 1.3 million users. [5] It was discovered by Monster that a remote server used by the attackers was used to store the stolen information. The scammers accessed job seeker contact information through unauthorized use of compromised legitimate employer client log-in credentials. Monster identified and shut down the rogue server that was accessing the job seekers' contact information.

There is a plethora of evidence indicating that the spyware threat has expanded beyond Web snooping and pop-up ads. A recent blended attack aptly named "The Italian job" was a cyber attack that targeted Italian Web sites, combining hacked Web servers, drive-by browser exploits, password stealing spyware programs, and stealthy rootkits. [7] Trend Micro discovered this attack in July when thousands of Italian language websites were hacked and booby trapped. By the time this attack was discovered, the attack's keystroke-logging software had uploaded a multitude of user names and passwords to hacker-controlled servers. Paul Ferguson of Trend Micro stated that "they were just casting the net as wide as possible." [7] These thieves were mostly looking for user names and passwords for online games and banking sites. Traditional signature based antivirus and antispyware protections did not provide much help until after the malicious Web sites were discovered. These successful attacks are attributed to a rootkit component called MPack. MPack hides deep inside an attacked operating system, away from inquisitive eyes of security scanners. Roger Thompson of Exploit Prevention Labs expresses concern that today's sophisticated malware threats demand a stronger response from antispyware applications that merely looks at client/server communications for signs of usage-tracking activity. He stated that "when you depend on signatures, you're always playing catch-up." [7] He also continues to comment on how it is becoming more difficult to catch the bad guys because they are carefully timing their attacks. They also stay ahead of antivirus and antispyware software by tweaking their code ever so slightly. It is no secret that as these types of threats evolve, security companies struggle to keep pace. [7]

Combating the Threat

Many businesses work very hard in trying to protect their customers. These businesses have hired brand-protection services that are designed to hunt down and close phishing sites. These third party groups are necessary due to the fact that law enforcement agencies are not able to obtain the necessary bandwidth to combat such threats. MarkMonitor, a brand-protection service, claims that phishing incidents increased 104% in 2007's first quarter. [2] Also, federal and state governments have taken steps to introduce new legislation to combat threats. Two recent bills, the Internet Spyware Prevention Act and the Cyber Security Enhancement Act, would give $30 million to law enforcement, stiffen penalties, and slap racketeering onto charges against botnet herders. Symantec Corp.'s senior manager of security response, Eric Chien, says that the battle between botnet perpetrators and law enforcement is like an arms race. "We always need to add to our defenses." [9] Chien says, "there's no shortage of people

looking for vulnerabilities to exploit. It's a cat and mouse game." [9]

Although these attacks are prevalent in today's Internet, networks can be secured by taking proactive steps to protect themselves by doing the following: (1) protect the perimeter. Quite simply, a firewall is necessary. Many firewalls offer unified threaten management features such as scanning all traffic for malware [1]; (2) protect the network by compartmentalizing network traffic using physical segmenting. This technique can help contain the spread of infection should a network be compromised [1]; (3) make sure users have appropriate account privileges; there is no need for most users to have administrator privileges; and (4) educate network users on the risks and common techniques used in attacks. Something as simple as opening an email attachment containing a virus could bring down a network for an extended period of time. [1] A suspicious attachment from a friend's email address may have been sent by a virus or an attacker spoofing that address. Also, never click on suspicious ads, run ActiveX, or java code from unfamiliar Web sites. To combat threats such as these, investment in a software security suite should be made.

When the need for security from malware began taking shape, antivirus software fought viruses and worms, and antispyware software fought spyware and adware. That trait has largely become a thing of the past. With the macro virus and the email worm becoming the old way of infecting computers, antivirus companies were forced to combat the next formidable attack. Spyware has presented itself as the next formidable opponent, and it has become necessary to find products that effectively fight Trojan horses and other backdoor programs. [7] Many consumers question if specialized antispyware tools are particularly effective in fighting today's threats. In an independent test, a German research company, AV-Test.org, conducted a malware test using five well known programs. The test bombarded the applications with samples of current adware and spyware. The test measured the products' ability to recognize 110,000 inactive adware, spyware, and rootkit samples. [7] An inactive sample is like a downloaded application that has not been installed. The antispyware product should recognize those samples based on a match to a signature database of known threats, before the sample unpacks itself and activates in various areas of the PC or network. Since individual threats can break down into more than 100 components, disinfection can be a difficult job. [7] It is important that anti-spyware look for the programs in order to clean up major file and registry changes. It is also important that the software be able to detect and block changes to key areas of an infected system without having to recognize anything about a specific invader. Spyware writers are continually releasing new threats, and security companies typically take some time to release signatures to catch those threats. Although Microsoft Windows Defender included with the Windows Vista operating system is free, it does not do much protecting of computers. Windows Defender is not designed to guard against certain types of spyware. In order to adequately protect computers from malware, purchasing a third party tool such as Spyware Doctor, SpySweeper or AdAware Plus is strongly encouraged. However, using a third party tool increases the chances of having a machine hijacked, or worse, identifiable information stolen.

CONCLUSION

Society is very dependant on technology. It is embedded in almost everything. Technology advancement is moving at such velocity, things once thought impossible are now occurring. This dependency makes society vulnerable to privacy attacks and related crimes, such as identity theft. Most Internet users are proponents of improving technology, but more needs to be done to protect users from such abuses as keeping vulnerable user information for twenty-four to forty-eight months. The general public will continue to use, develop, and to improve technology. Users will not halt their forward thinking processes for privacy laws to catch up. Technology is a convenient and useful tool for all users. Many would argue that the risk of compromise is offset by the gains that improve one's standard of living. But, when will it become time to seize control from those that corrupt, leaving the public vulnerable to attacks and abuses of personal information?

REFERENCES

1. Barrel, M. (2007). Security Success Story. *PC Magazine*, *26*(15), 82-82. Retrieved September 23, 2007, from Computer Source database.
2. Hall, M. (2007). Criminal Negligence. *Computerworld*, *41*(33), 4-4. Retrieved September 24, 2007, from Computer Source database.
3. Hall, M. (2007). Bot Wolves Defend flocks. *Computerworld*, *41*(34), 22-22. Retrieved September 23, 2007, from Computer Source database.

4. How Web Ads Follow You. (2007, July). *PC Magazine*. Retrieved September 24, 2007, from Computer Source database.
5. Keizer, G. (2007). Monster Hit With Theft of Client Data. *Computerworld*, *41*(35), 10-10. Retrieved September 24, 2007, from Computer Source database.
6. McMillan, R. (2007). Texas Not Hiding Data Under Its Hat. *Computerworld*, *41*(30), 10-10. Retrieved September 24, 2007, from Computer Source database.
7. Naraine, R (2007). Die, Spyware, Die! *PC World*. Retrieved September 23, 2007, from Computer Source database.
8. Naraine, R. (2007). The Italian Job. *PC World*. Retrieved September 23, 2007, from Computer Source database.
9. Travers, E. (2007). The Botnet Mafia. *PC Magazine*, *26*(16), 15-15. Retrieved September 23, 2007, from Computer Source database.
10. Vaas, L. (2007). Is it OK for Google to own us? *eWeek*, *24*(24), 16-17. Retrieved August 25, 2007, from Computer Source database.