



Blocking Day-Zero Threats: A Legal Imperative

An Exploit Prevention Labs (XPL) Legal White Paper

Benjamin Wright, JD

Executive Summary

“TOP OF THE NEWS: Zero-Day Exploit for WMF Flaw Circulating; Causing Widespread Infections” - SANS Institute NewsBites 31 Dec. 2005

Zero-day exploits – malicious software that seeks to take advantage of unpatched systems between the announcement of a software vulnerability and the installation of a corrective patch from the vendor - are becoming more common. They are part of a larger trend towards cybercrime by hackers who now seek financial gain from stolen passwords and trade secrets rather than the simple satisfaction of breaking system security measures.

Contemporaneous with the growth of this crime wave, the law increasingly expects organizations to protect data from theft by hackers and other criminals. Experience shows that particular security efforts are warranted for laptops and other PCs outside the security domains of large enterprises.

This paper reviews relevant legislation and case law, and advises that organizations should evaluate tools such as SocketShield to protect their operations from zero-day exploits.



Table of Contents

EXECUTIVE SUMMARY	2
THE RISE OF THE ZERO-DAY VULNERABILITY	4
ZERO-DAY EXPLOIT EXPOSES CORPORATE VPN	4
FINANCIAL MOTIVATION	5
IT SECURITY AND THE LAW	6
A DUTY OF PROFESSIONAL RESPONSIBILITY	6
GRAMM-LEACH-BLILEY	7
THE STATE OF CALIFORNIA'S DEMAND FOR REASONABLE SECURITY MEASURES	7
LIABILITY FOR IDENTITY THEFT	7
NOTICE OF DATABASE BREAK-INS	8
NEW PROBLEMS NEED NEW SOLUTIONS	9
CONCLUSION	9
ABOUT THE AUTHOR	10
ABOUT EXPLOIT PREVENTION LABS	10

© Benjamin Wright, 2006

This paper may be copied freely so long as it is copied as a whole.

Exploit Prevention Labs, the Exploit Prevention Labs logo, and SocketShield are trademarks of Exploit Prevention Labs, Inc. Other product and company names are the marks of their producing companies.



The Rise of the Zero-Day Vulnerability

Obviously, the protection of PCs calls for anti-virus software, anti-spyware software, firewalls, and the deployment of software patches as soon as vendors make them available. But new threats to PCs are now emerging so rapidly that these protections are no longer necessarily enough. Both individuals and businesses must remain on their guard; threats are now emerging before a patch or conventional security software can address the vulnerability they exploit. These threats are known as “zero-day” threats, because zero days exist between the time a vulnerability becomes known and the time a threat specifically targeting that vulnerability is distributed.

Zero-day threats are becoming more common:

“Malicious hackers are using hijacked Web servers and compromised sites to launch a wave of zero-day attacks against an unpatched flaw in Microsoft’s Internet Explorer browser . . . Microsoft confirms a wave of drive-by downloads targeting a zero-day browser vulnerability and says Internet Explorer users can expect a patch on April 11, if not sooner.” - Ryan Naraine, “IE Under Attack: Microsoft Ponders Emergency Patch,” eweek.com, Mar. 24, 2006.

The first true zero-day attack took advantage of the Windows Metafile (WMF) flaw that Microsoft patched in early 2006.¹ Hackers began propagating malware to squeeze through this particular security hole fully two weeks before Microsoft was able to issue a patch to close it.

But many users don’t install patches promptly. That’s how Graeme Frost of southwestern England unwittingly let a keystroke logger onto his machine even after the above-mentioned WMF patch was issued².

Zero-Day Exploit Exposes Corporate VPN

Hackers exploited an un-patched vulnerability in Internet Explorer to infect an Oracle Corp. telecommuter with a keystroke logger. The attack was a “drive-by download,” which surreptitiously slipped the malware onto the victim’s PC simply because he visited a booby-trapped web site. From the attack, the hackers obtained keys to the company’s VPN. According to the Washington Post, the victim was . . .

Reaz Chowdhury, a programmer for Oracle Corp. who works out of his home in Orlando, Fla. Chowdhury said he’s not sure which site he browsed in the past 24 hours that hijacked his browser, but he confirmed that the attackers had logged the user name and password for his company’s virtual private network (VPN). Chowdhury also uses Norton anti-virus, which did not pick up any signs of infection.³

Just as a telecommuter can be a gateway into a corporate system, so can a small supplier:

¹ Stuart J. Johnston, [“Prevent Attacks Aimed at IE and Windows”](#), PCWorld.com

² Brian Krebs, [“Hacking Made Easy: Automated Tools Gather Victims’ Keystrokes, Upload Passwords to Illicit Database,”](#) March 16, 2006, WashingtonPost.com.

³ “Security Fix - Brian Krebs on Computer and Internet Security,” [blog.washingtonpost.com](#) Mar. 27, 2006.



John Pironti, a security consultant with Unisys Corp., of Bluebell, Pa., says he helped discover a powerful Trojan that had been planted in the computer network of a major financial institution. A hacker penetrated one of the bank's custom-software suppliers and discovered the "open pipe" to the financial-services provider's network.⁴

Financial Motivation

Zero-day attacks have become more common because hackers have grown more sophisticated and more interconnected. No longer motivated simply by the ability to launch spectacular viruses that irritate and disrupt computer users, serious hackers today seek financial gain. Whether using zero-day attacks or other advanced hacking techniques, they are in search of personal, financial or trade-secret information that they can turn for a profit, as these stories attest:

Hackers are becoming more professional as the fruits of their labors are delivering greater financial rewards.

- In Graeme Frost's case above, hackers stole his online banking and Paypal passwords.
- A small computer supply company owned by Joe Lopez in Miami lost \$90,000 when criminals used his online Bank of America account to initiate a wire transfer to Riga, Latvia. An examination of Lopez's computer showed it was infected with the "coreflood" virus, which can allow a hacker to gain control of the machine.⁵
- The Securities and Exchange Commission reports a number of instances in which hackers have commandeered online stock trading accounts and stolen on the order of hundreds of thousands of dollars from each of them.⁶
- Businesses in Israel hired hackers to steal corporate intelligence by planting key logger programs on the computers of competitors.⁷

One zero-day trick fraudsters have used to make money is to install adware on victim PCs. (Adware throws revenue-generating pop-up ads onto the victim's screen.) One promoter of adware, iFrameDollars.biz, paid affiliate web sites 55 cents for each victim on which its adware was installed. The adware installed silently, by drive-by download through an unpatched vulnerability in Internet Explorer, when the unwitting victim visited an affiliated site.⁸

⁴ David Bank and Riva Richmond, "Information Security: Where the Dangers Are," *Wall Street Journal Online*, July 18, 2005.

⁵ Tom Costello, "[Crooks clean out couple's online bank account.](#)" *msnbc.com*, Dec. 14, 2004.

⁶ Eric Dash, "[E*Trade Offers to Reimburse Any Victims of Online Fraud.](#)" *New York Times Online*, Jan. 18, 2006.

⁷ Gregg Keizer, "[Israeli Couple In Spyware Ring Confess, Strike Plea Bargain.](#)" *TechWeb News*, Mar. 6, 2006.

⁸ Paul F. Roberts, "[Drive-By Download Sites Chauffeur Spyware.](#)" *eweek.com*, June 20, 2005.



IT Security and the Law

Increasingly, the battle against zero-day exploits has a legal dimension. The law demands that businesses protect information on computers. And the law is speaking with greater force today than before.

Until now, compliance with the law has focused on large enterprises and the security of the numerous machines directly tied to their corporate networks. But the law of computer security is equally applicable to individual computers outside the domain of large enterprise networks.

It is imperative for telecommuters, consultants, suppliers, doctors' offices, law firms, small businesses, schools and others who manage sensitive data to secure their laptops and desktop computers. As illustrated below, recent cases and developments show how individual machines or small networks expose their owners (including associated large enterprises) to legal liability.

A Duty of Professional Responsibility

Professionals owe a duty of confidentiality to their clients. A doctor, lawyer, accountant, banker, or broker exposes herself to a potential lawsuit for malpractice when she fails to safeguard client information on her PC. The Washington Post reports how a hacker installed a keystroke logger on a physician's PC and accessed patient medical data.⁹

Direct confirmation of such liability comes from *Guin v. Brazos Higher Education Service*.¹⁰ In that case, a borrower sued his lender, a financial institution, for failing to safeguard his personally identifiable data from criminals. The lender had entrusted the data to a telecommuter who worked from home. The telecommuter stored the data on a laptop, which a burglar snatched. There was no evidence the burglar found or used the borrower's data.

The court suggested this financial institution, like any banker, had a general duty to take reasonable steps to protect the borrower's social security number and other sensitive data. Then the court assessed whether the lender had fulfilled its duty. Under the facts of the case, the court concluded that the lender had indeed fulfilled its duty. It had taken a number of security measures that had contributed to protecting the borrower from identity theft or financial loss in this particular case.

While the *Guin* case is not specifically related to zero-day exploits, it reconfirms the obligation of financial institutions and professionals to take reasonable steps to protect private information. Fall short on that obligation, and a banker or other professional can be forced to compensate their customers under negligence law.

A similar case took place in the medical field. A West Virginia jury awarded three mental health patients a total of \$2.3 million because a hospital failed to prevent a clerk from disclosing records to the public.¹¹

⁹ Brian Krebs, "Bringing Botnets Out of the Shadows," *washingtonpost.com*, Mar. 21, 2006.

¹⁰ US Dist. Ct, Minn. 2006 Civ. No. 05-668 (RHK/JSM) [Memorandum Opinion and Order](#).

¹¹ HIPAA Weekly Advisor Archive, "Jury awards \$2.3 million to victims of privacy breach," February 24, 2003.



Gramm-Leach-Bliley

Consistent with general negligence law, the Gramm-Leach Bliley Act requires financial institutions to secure customer data. Under GLB, the Federal Trade Commission has sanctioned small financial institutions such as Nationwide Mortgage Group, Inc. In a settlement with the FTC, Nationwide is required every two years for the next decade to hire an outside professional to conduct a security assessment. In addition, for 10 years the company must file security reports with the government, and the company's CEO must notify the FTC every time he changes jobs.¹²

The State of California's Demand for Reasonable Security Measures

The duty to secure data is expanding beyond traditional professions such as banking and medicine. The California legislature maintains that any enterprise can be legally liable for inadequate data security. Under A.B. 1950, almost any business possessing private data about a California resident (such as name plus social security number or credit card information) has an affirmative duty to use "reasonable security" measures to protect that data.

The requirement to use reasonable measures is the same requirement set by general negligence law.

One of the challenges with A.B. 1950 is that a business in Florida might hold the social security number of a person and not know that he is a California resident. A California resident can have a postal address in Florida, or any other place outside California. Thus, California's A.B. 1950 is having an impact far beyond the state's borders. The legislation is motivating firms nationwide to protect data.

The law is not far away that says all enterprises have a general legal duty to employ reasonable measures to safeguard sensitive data.

Liability for Identity Theft

The public is angry about identity theft. Consequently, legal authority is beginning to hold enterprises liable for identity theft resulting from faulty information security. The bellwether case is *Bell v. Michigan Council 25 AFSCME*, Feb. 15, 2005, MI Ct. of App., No. 246684.

The *Bell* court awarded several members of a small labor union a total of \$275,000 in compensatory damages for identity theft. The theft occurred because the labor union's treasurer had failed to secure social security numbers in her possession, thus allowing her daughter to steal and abuse them. We can expect more cases like *Bell* punishing professionals or small businesses for neglecting to lock down employee or customer data.

¹² Federal Trade Commission [Press Release](#), "Mortgage Company Settles FTC Charges: Consumers' Financial Information at Risk by Lack of Required Security Practices," Mar. 4, 2005.



Notice of Database Break-ins

Approximately half of all American states have adopted legislation requiring that businesses suffering database break-ins give notices to individuals whose data might have been compromised. The model legislation is California S.B. 1386, which went into effect July 2003. Under 1386, if a business holding private electronic information about a California resident (such as name plus social security number or credit card information) has reason to believe the security of the information has been compromised, then the business must promptly notify the California resident. Notice must be given regardless of whether there exists evidence of identity theft.

S.B. 1386 and its sister laws in other states have spawned a torrent of mail to consumers throughout the country. Hundreds of enterprises, large and small, have sent notices about possible computer hacks.

Many of the reported incidents have involved laptop computers. A common story has been that a professional in a larger enterprise stored financial or social security data on a laptop. Then, while outside the enterprise's normal security domain, the laptop was stolen, lost or broken-into. The enterprise had to send embarrassing notices to customers or employees.

A case in point is accounting firm Ernst & Young. A laptop stolen from a locked automobile contained social security numbers for employees at some of the firm's corporate clients. One of those employees was Scott McNealy, then-CEO of Sun Microsystems. After a news organization published a story about the incident, E&Y sent notices to the affected employees. The publicity reflects poorly on the accounting firm's public image.¹³

Georgetown University sent notices to 41,000 senior citizens after hackers broke into a computer the university was maintaining for the DC Office of Aging. See Mar. 5, 2006 [press release](#). Hinsdale Central High School in Illinois notified 2400 students and staff after two students hacked into a school computer containing social security numbers.¹⁴

¹³ Ashlee Vance, ["Ernst & Young fails to disclose high-profile data loss."](#) *The Register*, Feb. 25, 2006.

¹⁴ Karen Jordan, ["Two students investigated for identity theft at high school,"](#) May 12, 2005. [ABC7Chicago.com](#).



New Problems Need New Solutions

In response to this spike in zero-day exploits and cybercrime in general, a veteran IT security team is unveiling a new protection method. Exploit Prevention Labs has developed SocketShield, a patent-pending product and back-end service dedicated to stopping zero-day exploits.

The product part of SocketShield is software that monitors all the IP data transmitted to a computer through port 80, the standard Internet data access channel; it stops any data that contains known or suspected zero-day exploits or is linked to a known or suspected malware distribution site.

SocketShield stops zero-day attack code before it can enter a victim's PC.

The service part of SocketShield is a system for finding new zero-day exploits as they emerge within the hacker community. This system has grown from research the company has been undertaking for the past several years. The research shows that, while the crafting of code to exploit a software vulnerability (such as a weakness in Windows or Internet Explorer) is hard work, the copying and re-use of that code is easy because it is freely available through underground cybernetworks. Therefore, for any given vulnerability, the hacker community may cut and paste the code onto many different packages (image, web site, etc.) and many different payloads (zombie, keystroke logger, etc.), even though examples of code developed for exploiting it are few in number.

The SocketShield service is at work constantly, identifying the latest examples of exploit code that are likely to cause trouble. As soon as the service discovers new code, it updates the SocketShield software to monitor for it and block it. See www.explabs.com.

Conclusion

Zero-day vulnerabilities are fertile ground for criminals in the hunt for financial and commercial secrets. Closing these vulnerabilities with a tool such as SocketShield is becoming a general legal duty for all enterprises, whether large or small.



About the Author

Benjamin Wright is a Dallas-based attorney and author of several books on technology law, the most recent being *Business Law and Computer Security*, published by the SANS Institute.

wright.safeshopper.com

This paper is not legal advice for any particular situation. If you need legal advice, you should consult a lawyer.

About Exploit Prevention Labs

Founded by information security veterans Bob Bales and Roger Thompson in 2005, Exploit Prevention Labs develops security software to protect against vulnerability exploits. SocketShield, the company's flagship product, provides patent-pending protection against zero-day exploits during the critical risk window between the announcement of a vulnerability and the provision of a patch by the vendor. More information about Exploit Prevention Labs and SocketShield may be found on the company's website at www.explabs.com.

