



Whitepaper: PCI Meets Crimeware

Courtland Little, CISSP, QSA
January 2010

866.333.2133
www.solutionary.com

PCI Meets Crimeware

Crimeware, an emerging sub-class of the more general malware, is mainly focused on facilitating financial gain for the hacker. Crimeware typically operates through direct sniffing of financially relevant data including payment card information, passwords, and bank account numbers. This information is then used to build more complex attacks including silent, back-door account withdrawals or the creation of physical debit cards to perform ATM withdrawals.

Two of the largest and most publicized payment card breaches of late are suspected to be victims of crimeware: RBS Worldpay and Heartland Payment Systems. Heartlands' breach went undetected for nearly six months exposing ~100 million payment cards serviced for 175,000 merchants⁽¹⁾. RBS acknowledged losing 1.5 million customers' financial data from its payroll cards business. This information was in turn used to withdrawal over \$9 million dollars from ATM's across the globe. These and similar attacks, such as the Russian Coreflood Gang attacks⁽²⁾, have the hallmarks of crimeware.

These events show as much as any that crime, in fact, **does** pay. A significant amount of today's hackers are financially driven. As the code and attacks are effectively criminalized, the "community" has identified the need to also commercialize crimeware. Tools and attacks get more advanced, easier to use, come bundled with related tools, documentation, and even come with technical support. Crimeware is not a "hack" as much as it is a systematic attack against a series of weaknesses. Crimeware represents a growing problem in network security as many malicious code threats work together, seeking to pilfer financial information and funds.

So what can companies do to ensure they aren't a victim? Does PCI compliance ensure proper security coverage? No CSO wants to hear they have a malware issue, and certainly not that the malware is actually crimeware!

Solutions

The nice thing about the PCI DSS is that it's essentially the embodiment of a defense-in-depth philosophy – multiple overlapping security controls in an attempt to avoid severe weaknesses in any one area. What's key to remember is that PCI enforces compliance with the DSS, not necessarily best practice security.

First we need to understand how crimeware can infiltrate your network and systems. Many people suffer from the preconceived notion that crimeware infection happens only by opening an infected attachment. But that's only one compromise vector. An infected PC can spread it's payload as a worm in an organization; abusing local vulnerabilities or configurations. A user can visit a trusted websites that is hosting compromised/malicious online advertisements (malvertising⁽³⁾) that can be used to transmit crimeware. Phishing messages containing external links and shareware software installations can create crimeware infections. The bottom line is that you have to defend multiple paths into your network and systems. So, the question remains; what can you do to prevent such an event in the first place?

Antivirus Controls

The most important aspect to preventing malware is ensuring your organization has a comprehensive, up-to-date antivirus program. Ensuring all users have up-to-date AV controls that cover not only virus, but spyware, and malware is critical. For example Symantec sells two completely separate products to protect for virus and malware. Just having their virus protection isn't enough as it doesn't cover Internet based malware. So, yes, if you are one of those companies that have removed client-based virus scanning —only checking at the email gateway and the servers, you now have a problem. Check that your organization has proper antivirus/antispymware/antimalware coverage and that the status of updates is actively monitored and validated! Doing so, by the way, also gets you PCI DSS 5.1.1 compliant!



System Patching & Hardening

Malware will often spread like a worm once it infects a network. Some spread by taking advantage of common vulnerabilities or configuration weaknesses. Ensuring your systems are patched in a timely manner and hardened using a recognized guide (like those produced by the NSA⁽⁴⁾) can greatly minimize the spread of crimeware if a PC does get infected.

Malvertising combined with internet surfing is a great way for infection to happen. Ensuring users update their browser as appropriate, as well as their browser plugins (i.e., Adobe Flash) which are well known sources of security holes are more critical aspects to system patching companies often overlook.

And, doing this properly gets you PCI DSS 4.1 (partly), 6.1, 6.3.1, and 6.4 compliant!

Use of Security Plugins in Browser

While on the topic of browser plugins, a great addition to the security toolbox is the use of those that prevent ads and scripts from running (Flashblock, No Script, Adblock) and thus infecting a machine. While this isn't a PCI requirement, it is certainly a great security practice!

Data Loss Prevention (DLP) Systems

DLP is an enterprise level security tool that monitors Internet traffic, looking for sensitive data leaving or entering your network. It isn't a silver bullet but can be a powerful control to help monitor (or block) the spread of financial, personal or corporate data if an infection does happen. Once again, while DLP is not a PCI requirement, it's a powerful security tool.

File & Kernel Integrity Monitoring (FIM)

FIM builds a snapshot of the files contained on your system when it is in a known good state. For crimeware to work, it has to infect your machine, typically by installing an executable or shared library. If your FIM detects a change in a file (like the size and/or date of an executable), that is an indication that the file has been changed by malware. You have to monitor the right folders/files but it's an effective layer of security. Proper FIM integration is a requirement within PCI DSS 10.5.5.

Database & Transport Encryption

Simply put, if the data is encrypted properly it's of no use to criminals even if they do access it. If it's transmitted properly over encrypted channels it makes access to sensitive data much more difficult. This is the backbone to PCI and is covered by PCI DSS 3.1, 3.2.X, 3.3, 3.4, 3.5, 4.1.X and so forth.

Increased User Awareness

The importance of solid user awareness cannot be overlooked. Having users trained on secure email and Internet usage, including education about new risks, is key. In addition, users that understand the sensitivity of the data they work with and the compliance obligations of the organization can take precautions consistent with the organizations security and compliance program. This is a mandate from PCI within PCI DSS 12.6.X.

Proper Log Monitoring

Proper log monitoring is the cornerstone of any good security program. Several of the solutions above are merely detection mechanisms. If your security group isn't monitoring the logs at least daily then all the controls in the world won't do much good if the threats go unchecked. Not every attack can be prevented, but early detection is guaranteed to minimize the damage done. This is especially true in the case of crimeware where early detection can prevent hackers from having the necessary time to gather information needed to build a more complex attack. This is a major component to PCI and is addressed in the PCI DSS 10.X, 11.4, and 12.5.2.



Mandatory Access Control (MAC)

MAC is popular in the government and is an emerging technology/process in the commercial space. Think of it as the Windows GPO on steroids. The basic tenets of MAC security are found in system hardening guides today. If you have done everything in this article, and want to do more, MAC is for you. This isn't a PCI requirement but is yet another solid best practice.

In the event your organization is compromised; understanding the distinction between a malware infection and crimeware infection is critical. Forty-five states currently have breach disclosure laws. If your organization is infected with crimeware, depending on the depth and level of compromise, you will have both compliance and regulatory reporting guidelines to follow. Ensuring that your organization has a security and compliance program which includes security controls, log monitoring, and an incident response plan (PCI DSS 12.5.3, 12.9.X) can help minimize the financial and reputational damage done, and get you back on the road to recovery that much sooner.

- (1) http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-br each_N.htm.
- (2) http://www.usatoday.com/tech/news/computersecurity/2008-07-15-coreflood_N.htm
- (3) <http://isc.sans.org/diary.html?storyid=3727>
- (4) http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

About the Author

Courtlend Little is a senior product manager for Solutionary, Inc. focusing on product development of Solutionary's managed service offerings.

Courtlend has over ten years of experience in networking technology and security. He has a background performing external and internal penetration engagements, as well as application and security architecture reviews and assessments for Fortune 500 companies.

Courtlend's previous experiences were as a senior consultant in Solutionary's consulting division; and prior to that he was with PWC's TRS security group.

Courtlend received is B.A. in geochemistry from the University of Texas at Austin and an M.S. in geochemistry from Virginia Polytechnic Institute and State University. He is certified in CISSP-ISSMp, QSA and is fluent in Spanish.

About Solutionary

Solutionary is an information security company that delivers a wide range of managed security solutions and professional services to reduce risk, increase security and ensure compliance for medium-to-large businesses.

The company's services are based on next generation security intelligence and offer true security and compliance management. Solutionary provides customers with advanced service delivery, patented technology, thought leadership, years of innovative groundwork and proprietary certifications that exceed industry standards, enabling the company to have one of the highest client retention rates in the industry.

Solutionary is positioned by Gartner as a "visionary" in the MSSP Magic Quadrant, and Forrester as a "strong performer" in the MSSP Wave. The company maintains 24/7, fully redundant security operations centers (SOCs) in Pittsburgh and Omaha where it is headquartered.

