

Anti-Virus: A Critical POS Safeguard

Computer viruses and other malicious software are costing business billions of dollars annually. Rogue programmers are moving beyond PCs to mobile phones, PDAs and other devices. With financial data under assault, it is time for the payments industry to proactively address future threats.

The Economic Impact of Virus Assaults

Computer viruses and other malicious software (“malware”) are believed to cost businesses in the U.S. tens of billions of dollars annually. One UK security firm projected that worldwide business costs in 2004 may have been over \$200 billion, more than double the rate of the previous year. As the world becomes increasingly computerized and connected, rogue computer code has become a serious economic issue. Businesses are literally under assault from a dizzying array of viruses, worms, Trojan Horses, spyware, bots, ransomware and other threats.

Businesses pay in a number of ways, from the cost of actually combating and cleaning out the code infecting systems, to lost productivity as systems sit idle, to actual damages from theft or corrupted systems, to liability to customers harmed by malicious intent. For many years, it was presumed malware was only a concern for PCs running Microsoft Windows. But increasing efforts to assault mobile phones and PDAs show the potential for this insidious threat to cross over to other points of opportunity, perhaps even point-of-sale devices.

Financial systems have long been a target of computer criminals. Increasingly, these perpetrators are targeting the various links in the card processing chain, whether retailers, banks or processors. The potential business liabilities resulting from theft of consumer card account data or identity theft pose serious financial risks for all companies involved in the processing of card information.

It is critical that each company, no matter what their role in the financial card processing chain, take steps to ensure its security measures are reviewed and that all appropriate measures are taken to prevent access to consumer information.

The Malware Threat

Malicious software first began to surface in the mid-1980s as personal computers were starting to proliferate and they were initially transmitted via floppy disks. In late 1988, a young Cornell University student unleashed a self-replicating program, dubbed a Worm, over the Internet, which was then still primarily used to connect university and military computers, and resulted in thousands of computer systems becoming unusable.

Melissa was the first significant virus for many computer users. The code was technically a macro virus, using the programming ability of Microsoft Word to take over a computer users email address book and use it to mail out more infected messages to other computers. Melissa literally raced around the Internet, infecting 100,000 computers during the course of a weekend and causing companies to shut down their email systems. The next year, the ill-named Love Letter worm caused even more havoc, literally flooding Internet Service Providers, many of whom had to shut down their systems, and also searching for passwords stored on individual computers.

By the end of 1990, some 200 computer viruses had been identified; by the end of 2004, some security experts estimated that number was approaching 100,000. While early viruses were often little more than pranks, later rogue programs turned malicious and aimed to wipe out the hard drives of computer users; some began inserting Trojan Horses that took control of a remote computer. More recently, programmers have developed code aimed at gathering personal and financial information and transferring it back to the author of the program.

Liabilities at the Point of Sale

There's a general misperception that Windows-based PCs are the only target of malware authors. It's true such systems are the predominant target, because they have represented the largest number of potential victims, but the threat is quickly spreading to other devices as the world becomes increasingly connected through the Internet.

Without doubt, credit card information is becoming one of the prime targets of criminals who are using rogue programs to capture consumer account information. In June 2005, MasterCard announced that information for as many as 40 million cardholder accounts – including those of Visa, American Express and Discover – may have been exposed to criminals who were able to infiltrate a computer virus into the systems at CardSystems Solutions Inc. in Tucson, AZ. Not long before that, Polo Ralph Lauren and DSW Show Warehouse suffered embarrassing breaches.

Companies handling consumer information face serious liabilities if they can be shown at fault or negligent in a breach of security. U.S. Federal Trade Commission Chairman Deborah Platt Majoras, announcing in June 2005 a settlement with BJ's Wholesale Club, declared, "Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security. This case demonstrates our intention to challenge companies that fail to protect adequately consumers' sensitive information."

No malware threat has yet been detected that has directly targeted standalone POS systems. Yet that should not deter companies from taking steps to prepare for the inevitability. In fact, the FTC asked Congress to consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety; that would in effect subject all companies to comply with existing rules that require financial institutions "to implement reasonable physical, technical, and procedural safeguards to protect customer information."

Not so long ago, it was believed there was little threat to mobile phones because there is no predominant operating system for those systems equivalent to Windows on PCs. Yet, today malicious programmers are

actively targeting mobile phones and PDAs. According to *The Times* of London, in the first half of 2005 more than 50 viruses targeted at mobile phones had been detected. One of those, known as Commwarrior, infects a handset through a Bluetooth wireless connection and sends out text and picture messages to all the numbers in the infected device's address book and also seeks out other Bluetooth phones to infect. Many other devices are being developed with Bluetooth, including some POS systems. Computer security solutions developer McAfee began working with Japanese telecom provider NTT DoCoMo in January 2002, long before any mobile threat surfaced, on developing virus protection for mobile phones, based on the understanding that increasing sophistication and globalization of such devices would make them a target.

Some companies may believe they don't need to implement measures until an actual assault occurs. Waiting until an incursion happens may be cheaper in the short-term, but the cost in terms of damage repair, lost productivity and damage to brand image may be incalculable; once the consumer's trust has been breached with a particular company it may take years to recover, if ever. Pressure is also building for government to mandate businesses take action.

Others may think that they can avoid the threat by simply not using Internet-connected devices. That is certainly an option, but it comes at a tremendous cost in lost opportunity. Without access to broadband transmission, companies will pass up access to new revenue-generating applications. They also risk the potential loss of customers who prefer to make purchases at locations where fast card payments make their experience speedier and more enjoyable. It would also mean that companies must pass on the opportunity to use wireless transmission, which can be a tremendous time and money saver.

VeriFone and McAfee Solve the POS Issue

VeriFone, the leading provider of electronic payment solutions, has teamed up with McAfee, the leader in Intrusion Prevention and Security Risk Management solutions, to jointly develop the point-of-sale payment industry's first virus protection solution.

VeriFone recognized that the growth in Internet Protocol-enabled payment devices required tools to protect transaction data from sophisticated

malicious software. Even though VeriFone payment solutions already provide the highest-levels of security and no intrusions have been experienced, the company is determined to preempt the threat of malicious software.

McAfee® VirusScan® Mobile for Verix® will ultimately be extended to all VeriFone IP-enabled payment devices, including those already installed in the field, to provide real-time monitoring and attack pattern update services for VeriFone payment solutions utilizing Ethernet, Wi-Fi, 2.5G and 3G wireless IP networks.

McAfee VirusScan Mobile for Verix includes software, download, support, virus detection and routine updates of virus profiles, utilizing the well-established yearly subscription model of the anti-virus software industry. VeriFone payment solutions deployed with VirusScan Mobile automatically check for updates at configurable intervals to ensure that protection is always up-to-date with the latest industry threats. The software operates automatically in the background and is transparent to the merchant.

This Malware protection product leverages VeriFone's leadership in payment protection and McAfee's leadership in intrusion protection to provide merchants with the 'peace of mind' that their investment and transaction data is safe from increasingly sophisticated malicious software. The solution is a preemptive measure that provides a quick and efficient response mechanism to protect against future attacks, reducing the likelihood of transaction downtime, theft of credit card numbers and transaction data, or other malicious activity.

The anti-virus offering from VeriFone and McAfee provides ISOs and Acquirers with an integrated solution they can make available to their merchant customers either pre-installed or through updates in the field. The automatic updates provide merchants with a demonstration of the benefits of utilizing IP-enabled systems. McAfee VirusScan Mobile for Verix enables ISOs and acquirers to provide merchants with VeriFone payment solutions that provide an additional layer of protection beyond current industry standards for IP-enabled payment devices.

As an extension of VeriFone's Enhanced Communications solutions, McAfee VirusScan Mobile for Verix provides ISOs, acquirers and merchants with the opportunity to take full advantage of IP with the knowledge that their

businesses will be secure. It provides protection against future potential threats of Internet connected POS systems with an immediate and consistent response to threats with no disruption to business. Online offenders will always be on the lookout for new opportunities to spread malicious threats and VeriFone and McAfee have teamed up to stay ahead of them.