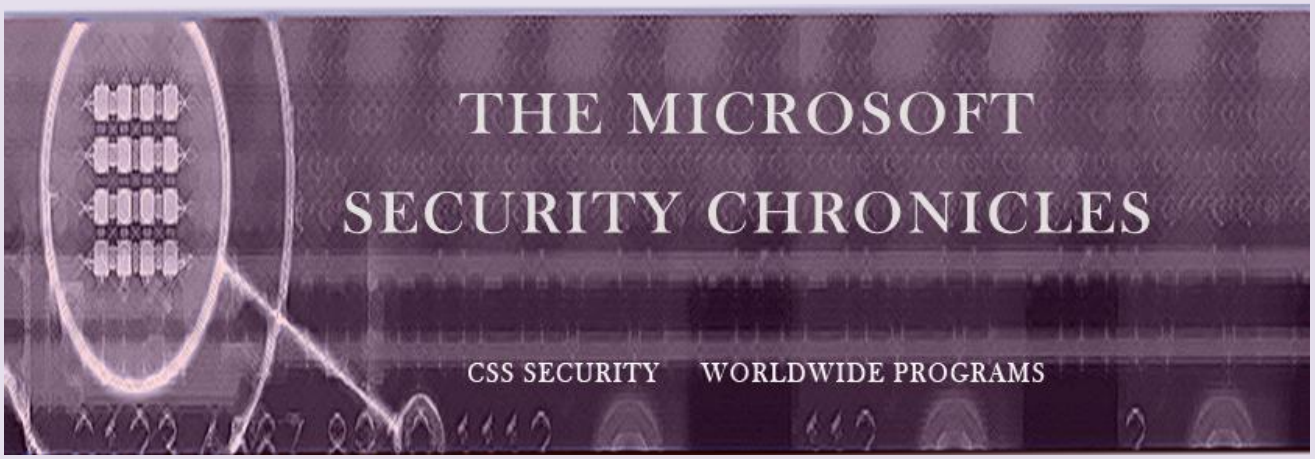

December 15, 2011

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

Hackers Hit Supermarket Self-Checkout Lanes, Steal Money from Shoppers

Ars Technica

Criminals have tampered with the credit and debit card readers at self-checkout lanes in more than 20 supermarkets operated by a [U.S.] California chain, allowing them to steal money from shoppers who used the compromised machines. The chain, Lucky Supermarkets, which is owned by Save Mart, is now inspecting the rest of its 234 stores in northern California and northern Nevada and urging customers who used self-checkout lanes to close their bank and credit card accounts.

Related reading: Magnetic Strip Technology in Our Credit Cards Facilitates Fraud.

Analysis:

It is the holiday season so it seemed appropriate to report on security stories affecting shoppers. Stories about electronic skimmers and identity theft are definitely not something new in our world today — as a matter of fact they are a daily occurrence. The availability of credit card skimmers for a really cheap price and the profit made when an identity is sold make this a very lucrative business. In the current economy people seem to be using this business model to earn extra money as indicated by these stories on the FBI [U.S. Federal Bureau of Investigation] website.

While it is important to be extra careful about packages being stolen from your doorstep during the holidays, it pays to be extra vigilant about your credit card information and identity as well. Some examples of caution near ATM machines include:

- Use secure ATM machines (preferably those inside a lobby).
- Cover the ATM keypad as you enter your PIN (to avoid hidden cameras).

SECURITY CALENDAR

December 2011

28 ISAI - Dubai

28 ICCNS - Dubai

January 2012

02 NCS - India

05 Microsoft Bulletin Advance Notification

10 Microsoft Security Bulletin Release

17 SANS Security East – New Orleans

20 SANS DoD Cyber Crime – Atlanta

21 SANS North American SCADA – Orlando

30 SANS - Monterey

- Don't accept "help" from anyone hanging around the ATM.
- Don't let a merchant walk off with your card — even for a few seconds.
- If an area looks suspicious, don't use an ATM machine there.

Skimming devices can be of many types. As noted in this article, skimming devices and hidden cameras can be spotted if you pay close attention. The University of Texas has provided these pictures of a skimmer attached to an ATM machine.

ATMs are not the only place where you can become a victim of skimming. They can also be installed on gas station pumps and other places where cards with magnetic stripes are used. The skimming devices are also getting smaller and more sophisticated. Security guru Bruce Schneier points out, "The moral is that they are getting better and better at this." The crooks can use Bluetooth technology to download information from the skimmer without ever leaving their car! Brian Krebs describes on his *Krebs on Security* blog how these skimmers can be installed in a way that they are nearly undetectable.

The take-away for this holiday season is to be a vigilant consumer and credit card user. If you notice something that does not seem normal while using an ATM or a credit card device, take precautions to keep yourself and your money safe.

Microsoft's New Windows Defender Tool Runs Outside Windows

CNET

Making its debut as a publicly available beta, the new Windows Defender is designed to run directly off a CD, DVD, or USB flash drive to scan your PC outside of Windows. As such, its aim is to detect rootkit viruses and other malware that can infect your computer during the boot process.

Analysis:

In the Internet security world, the year 2011 can be cause for both consternation and optimism. We have witnessed a rise in the frequency of attempted and successful corporate hacking incidents such as the data breaches of Sony and RSA, the phone hacking scandal at the News of the World, Anonymous/Lulzsec incidents, as well as attacks on banking, technology, defense, and consumers. While publicized hacking events have been on the rise, improved tools and greater cooperation between governments and industry have resulted in the exposure and takedown of nefarious enterprises such as the Rustock botnet.

Microsoft offers several options for protecting and cleaning enterprise and consumer computer systems from malware, including the following:

- Microsoft Security Compliance Manager 2 (SCM 2) is a free tool to help achieve a secure, reliable, and centralized IT environment and access the latest security setting and configuration recommendations from Microsoft.
- Microsoft Baseline Security Analyzer 2.2 (MBSA 2.2) is an easy-to-use tool that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA 2.2 to detect common security misconfigurations and missing security updates on your computer systems.
- The Microsoft Security Assessment Tool 4.0 (MSAT 4.0) is a risk-assessment application designed to help organizations assess weaknesses in their current IT security environment, create a prioritized list of issues, and help provide specific guidance to minimize those risks. MSAT is an easy, cost-effective way to begin strengthening the security of your computing environment and your business.
- Microsoft Safety Scanner is a free, downloadable security tool that provides on-demand scanning and helps remove viruses, spyware, and other malicious software. It works with your existing antivirus software.
- The Microsoft Malicious Software Removal Tool (MSRT) checks computers for infections by specific, prevalent malicious software and helps remove any infections found. When the detection and removal process is complete, the MSRT displays a report describing the outcome, including which, if any, malware was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month.
- Microsoft Security Essentials (MSE) can provide free, real-time protection against viruses and spyware for your home or small business with up to 10 PCs. MSE is free to consumers running genuine Windows and is designed to be simple to install and to run quietly in the background.
- Windows Defender is free software that protects computers against pop-ups, slow performance, and security threats caused by spyware and other potentially unwanted software. The new Windows Defender Offline Beta can also help to remove hard to find malicious programs using definitions that recognize threats.
- Microsoft Forefront is available for protecting enterprise systems and businesses with more than 10 PCs. There are several versions of Microsoft Forefront offering comprehensive solutions for protection on premises and in the cloud.