calyptix™
SECURITY

Small Businesses under Attack from Organized Cyber Crooks

By Ben Yarbrough

Noted computer security journalist Brian Krebs of the *Washington Post* has recently chronicled in articles and blog entries the escalation of costly cyber security incidents encountered by small and medium businesses. The most costly involve looting bank and payroll accounts. The absence of notoriety of these incidents compared to large-scale breaches at big retailers does not minimize the impact on the victims. This article highlights these developments and suggests several practical and affordable defensive measures for small and medium businesses.

Incidents highlighted by Krebs include:

- Gainesville, Ga.-based **Slack Auto Parts**, lost nearly **$75,000** in July 2009 when fraudsters used malware to steal the company's online banking credentials and distribute the funds to six money mules around the country.
- J**M Test Systems**, an electronics calibration company in Baton Rouge, La., lost almost **$100,000,** after thieves used malicious software to send a series of payments under $10,000 each to at least five co-conspirators around the country, who then wired the money on to fraudsters in Russia.
- **Sign Designs, Inc.**, a Modesto, Calif.-based company that makes and installs electric signs, lost nearly **$100,000** on July 23, when crooks used the company's credentials to log in to its online banking account and initiate a series of transfers to 17 accomplices at seven banks around the country.
- On the morning of Aug. 17, hackers broke into computers at the **Sanford School District** in Sanford, Colorado and initiated a series of bogus fund transfers totaling **$117,000** directly out of the school's payroll account.
- In mid-July, computer crooks stole **$447,000** from **Ferma Corp.**, a Santa Maria, Calif.-based demolition company, by initiating a large batch of transfers from its online bank account.

Special risks to businesses. Businesses do not enjoy the same legal protections as consumers when banking online. Under state laws, consumers typically have up to 60 days to dispute unauthorized charges. Meanwhile business banking relationships are governed under Article 4 of Uniform Commercial Code which provides commercial banking customers as little as two business days to spot and dispute unauthorized activity. ***The burden rests on business customers to monitor activities daily if they want to have any chance of recovering unauthorized transfers from their accounts.***

How attacks occur. The victims of this type of fraud have told Krebs different stories, but the basic elements are the same. Malicious software is planted on the company's PC that allows the crooks to gain access to the victim's corporate bank account online. The attackers wire chunks of money to accomplices called "money mules" in the United States who then wire the money to the fraudsters overseas.

Common ploys include email targeting the company's controller, accounting staff or other high level executives. These email contain a virus-laiden attachment or link to a web site, that when opened, surreptitiously installs malicious software. The malicious software is designed to be undetected and steal passwords and other banking credentials. Once the credentials are obtained and communicated back to the fraudsters, the crooks start transferring small amounts (less than $10,000) out of the account to the "money mules." The transfers can take the form of wire transfers and even checks paid as online bill payments.

A recent intelligence report circulated among the financial services industry on September 14, 2009 reported one such scheme involving a new series of spam originating from the "***Cutwail botnet***" - the world's highest volume spam sending botnet (90,000 spam per hour). In this case, the spam purports to come from the U.S. Internal Revenue Service (IRS) and contains a link to the IRS web site. Instead, the link directs the recipient to a site that downloads malicious software. Users are advised to be aware that the IRS does NOT send email to conduct business, and any spoofed emails should be deleted immediately.

Today's underground online fraud economy is a sophisticated international business model equipped with expertise and multi-levels of participants. The lead research at RSA's Anti-Fraud Command Center illustrates the main goals of online fraud as "harvesting" and "cash-out." Harvesting is where criminals target user access credentials by skimming, phishing or Trojans, and cash-out fraudsters are after the profit (money) through e-commerce transactions or online banking transfers using sophisticated malware-mostly Trojans. Online fraudsters collaborate and set up business relationships through online forums to share information, tools and discuss the latest business opportunities.

The sophistication of the malicious software varies and can be extremely difficult to detect. For instance, one data-stealing Trojan program known as "Zeus" allows the attacker to change the display of a bank's login page as a victim is entering their credentials. For example, when a victim submits his one-time password along with his credentials, the malware may force the browser to return a counterfeit page (still showing the bank's domain name in the URL bar) stating that the bank's site is down for maintenance, please try back again in 15 minutes. Meanwhile, those credentials are not submitted to the bank but instead sent to the attackers. While the unwitting victim waits as instructed, the thieves use the intercepted credentials to log in as the victim and initiate unauthorized transfers from that account.

How to protect yourself. Protective measures include implementing sound financial management practices, educating staff and implementing sound IT practices and technologies.

- Reconcile your bank accounts daily. Pay special attention to all online banking and credit card activities, including checks generated from online bill pay systems. The victimized companies Krebs interviewed which were most successful in retrieving stolen funds were those who quickly spotted the fraudulent transfers through monitoring account activities.

calyptix™
SECURITY

- Ask your bank to set up a notification procedure - perhaps approval by phone -- for any transfers or bill payments that fall outside of your normal online banking activity.
- For employees who need to access accounts online, consider setting them up with a separate isolated computer. Noting most attacks have been on Microsoft Windows systems, Krebs suggests using a Mac or Linux system (perhaps even a live CD distribution of Linux).
- Be wary of unusual experiences when accessing online banking systems including login difficulties or unusual experiences with the bank's website (*e.g.* slowness, formatting, color, logos, quality, misspellings, etc.).
- Educate your staff and executives about the risks and best practices for passwords, unsolicited email, unknown website links, software updates and downloads. Make certain to highlight this issue for staff who access online bank accounts.
- Keep all systems (workstations, servers, network equipment, etc.) promptly patched with all security updates to prevent attacks against security vulnerabilities.
- Implement a coordinated layered security strategy (aka "Defense in Depth") across the network, including protection at the perimeter (*e.g.* internet gateway), servers and workstations.
- Implement a stringent perimeter defense that provides visibility into all traffic and utilizes proactive security techniques such as intrusion prevention, web filtering and other techniques to stop invisible network attacks, scans and exploits.
- Eliminate spam and other email from untrusted sources.
- Establish proper reporting and controls to prevent web surfing and software downloads from sites susceptible to malware (*e.g.* pornography, videos, pirated music and software, etc.).

* * * * *

Ben Yarbrough is the CEO of **Calyptix Security** and a practicing business attorney. Calyptix manufacturers **AccessEnforcer**,™ an all-in-one security appliance designed especially for small and medium size businesses (up to 250 users) that have limited IT budgets and limited access to network security specialists. AccessEnforcer, tailored to work with Microsoft's Small Business Server, eliminates the pains of multiple subscriptions, integrating multiple components and IT complexities. For additional information, go to www.calyptix.com where you may access a free whitepaper entitled ***Twelve Security Techniques for Small Businesses***.