KASPERSKY lab

WatchGuard™

SIZE DOESN'T MATTER

Why Cybercriminals Attack Small and Medium Size Businesses

According to the FBI, a handful of Trojans (a type of malicious software) engineered to steal on-line banking credentials were responsible for over $100 million in losses to small businesses in the United States between mid-2009 and mid-2010. Worldwide, cybercriminals earn over $100 billion per year through their increasingly sophisticated attacks.

SMBs are frequently more exposed to risk from cybercriminals than larger companies are. This is because:

- Larger enterprises have become better defended so cybercriminals are moving down the business food chain
- Crooks target only those employees responsible for online banking activities by sending them socially engineered emails containing malware designed to hijack banking login details
- Many organizations fail to uncover the theft for many days due to:
  - poor anti-virus detection
  - limited staff
  - they see no need to monitor accounts which are only used to transfer money for direct deposits
  - thefts are timed to allay suspicion - cybercriminals begin stealing during the window of time SMBs are not using the account
- Only slightly more than half of small business owners check their computers on a weekly basis to confirm the currency of security updates (per an NCSA study)
- Only 35 percent provide cybersecurity training to employees, only 28 percent have an internet security policy in place and only 6 percent fear the loss of customer information
- End-users lacking education on cybercrime risks can undo all the security protection in place with a single click

Summary of security challenges specific to small business:

- Limited IT infrastructure budget
- Absence of IT security procedures and policies
- Insufficient awareness among employees
- No dedicated IT specialist on the company's payroll
- Outsourcing of security to unqualified contractors or system administrators

- Phishers often use U.S. government agencies as the faux sender to heighten the apparent legitimacy of their attempts
- $100 billion, a "low estimate" of what cybercriminals earn worldwide per year, is able to finance the most brilliant hackers and social engineers
- Larger organizations have implemented multiple layers of security whereas SMBs haven't yet begun – making them significantly more exposed than bigger companies
- Being small does not make a business less of a target – in the game of spreading botnet infections, size doesn't matter – the criminals just want in
- There is also targeted malware which is very effective in certain key verticals
- Many new cybercrime tactics are entirely automated so return-on-investment is irrelevant
- Less protected companies with any level of assets are vulnerable

KASPERSKY lab

Some Victims of Cybercriminals

Business sector:

- **Slack Auto Parts**, a small business in Georgia, lost nearly $75,000 when fraudsters used malware to steal the company's online banking credentials and distribute the funds to six money mules around the country.
- **JM Test Systems**, an electronics calibration company in Baton Rouge, lost almost $100,000, after Clampi sent a series of sub-$10,000 payments to at least five mules, who then wired the money on to fraudsters in Eastern Europe.
- **Genlabs Corp.**, a California chemical manufacturing firm, lost nearly $437,000 after Clampi thieves broke into its bank account and sent transfers to roughly 50 different money mules. The attackers succeeded despite the fact that the company's bank requires the user to enter their password in addition to the output from a key fob that generates a new six-digit number every 60 seconds.

Educational institutions:

- **Sand Springs**, a school district in Oklahoma, was attacked by a cyber gang in August 2010. Thieves stole roughly $150,000, after breaking into the company's online bank account and setting up two batches of fraudulent transfers.
- **Marian University**, a Catholic university in Wisconsin, lost more than $189,000 by bank transfers to 20 money mules. The school was able to recover just $54,000.
- **Sanford School district** in Sanford, Colorado lost $177,000 which was transferred to 17 different money mules in amounts mostly just under $10,000. They were able to reverse two of the transfers before the money left the country, but only $18,000 worth. Sanford only serves 340 children.
- **University of Florida** admitted to a data breach in 2009 where 100,000 student and faculty social security numbers were stolen.

Healthcare:

- **Evergreen Children's Association** in Seattle, who provide on-site childcare for schools, lost $30,000 to cybercriminals (September 2009) via an on-line banking trojan.
- $200,000 was stolen by hackers from **Steuben Arc**, a nonprofit which provides care for developmentally disabled adults. The scam was discovered in time to recover some of the money. The entry point was a fake invoice opened by an accountant.
- **Medilink Georgia**, who provide health care to the under and non-insured, lost $44,000 when their banking credentials were stolen.

Quick and Easy fixes

- Raise employee awareness and knowledge
  - Distribute a basic security policy to all employees
  - Provide employees the "Cybercrime Quiz"
  - Once a month distribute a security article on cybercrime to employees as a reminder
  - For content, try: www.krebsonsecurity.com or www.threatpost.com or www.theregister.co.uk/security
  - Share this responsibility with other interested employees
- Check workstations to ensure anti-malware updates are current
- Make sure systems are updated with the latest application patches – try www.secunia.com to perform a free system check
- Restrict on-line banking activities to a computer dedicated to that purpose (not used for any other internet activity). If this is not possible, ensure anti-virus is up to date before using the internet
- Contact your bank and set up an alert notification by phone for any money requests or transfers

Longer Term Solution

- Purchase as much security as you can afford. The calculation should be balanced against:
  - the cost of losing valuable company data such as customer lists
  - compromising customer privacy
  - losing credibility in your community
  - money that could be lost from on-line banking accounts