Intrusions and inside jobs:
Lessons from the banking industry

Presented by:
Michael Kalinichenko
Co-founder & CEO, SafenSoft
VB 2010

Banking Security Today

- The Zeus Banking Trojan reappeared at a UK-based online bank and has enabled the theft of more than a million dollars to date.
- Stuxnet appeared, signaling a new and deadly malware vector – the use of .LNK shortcut files to automatically launch malware from an infected USB drive.
- Barnaby Jack publicly hacked two popular brands of ATM during Black Hat 2010., showcasing the dangers of outdated security.
- Winnipeg police discovered a CAN $2M scam at a hospital ATM that involved probable insider recoding of the machine.
- A Bank of America employee pleaded guilty to planting malicious software on more than 100 of the bank's ATMs. The code instructed the ATMs to dispense cash without recording the transaction.
- Utah-based Zions Bank found that 180 pay-at-the-pump terminals had been compromised

"It's time to do a better job of protecting the PC inside the ATM." – Tracy Kitten, Editor, BankInfoSecurity, August 5, 2010

Turning the clock back – Russia 2009

- Russian banks and companies are much more closed than in North America, but in 2009 they publicly admitted to a rapid increase in security incidents with ATMs
  - Presence of illegal software (not viruses)
  - Unusual software behavior, followed by cash losses
  - Active use of ATMs to withdraw cash from suspicious accounts

Sberbank: Russia's largest retail bank

- More than 25,000 ATMs all across the country – thousands of miles, 10 time zones
- Active growth of payment terminal (PT) network
- Many cash-based operations like payments for telephone, water, Internet, gas, etc. payments are processed through PTs and ATMs.

On a mission

- After analyzing the situation, it was determined that the traditional approach to computer security was no longer effective for ATMs
  - Cannot protect against targeted attacks
  - Cannot protect from illegal activities by service personnel (internal threats)
- Why is this?
  - Threats are singular and unknown to the anti-malware research community
  - Service personnel are not concerned with threat detection

Anti-piracy Technology and Banking Security

- Looking for known crimes is ineffective
- Focus instead on preventing modification of authorized applications and system in common

- Looking for objects at the base of formal parameters (signatures) is ineffective
- Focus instead on keeping control over events in the system and their results

ATM-network interconnectivity

- ATM is the most anonymous way to get real cash from point A to point B
- ATM = PC with Windows
- ATM = old PC without the latest security updates
- Virtualization has given hackers excellent opportunities for research
- ATM networks are part of bank networks
- Bank networks are part of Internet

ATMs are the ideal vector for cybertheft

Why is this?

- Slow data transmission channels → no way for fast and regular updates
- Long distance from IT departments
- Huge territories → limited accessibility for repair in case of software problems
- Many service personnel have access to ATM → no easily-enforceable operating guidelines or security procedures
- The more services are added to ATMs, the more complex – and vulnerable – they become
- Few standard hardware or software configurations

So, we took a different approach

- To protect Sberbank's systems, we focused on developing an integrated approach:
  - A system cannot be protected with just application software; what is needed is an integrated combination of hardware, system software, application software, and people working in integrated business environment
  - The technology used must be workable in the target business environment (in this case, incorporate protection of unattended devices)
- We determined the most effective way to satisfy these requirements was to combine behavioral rules with dynamic integrity control

The best-protected system is the one that does what it is designed to do - and nothing else.

How we do things differently

Three key technologies are used to prevent unknown software from executing on an ATM (or a USB device plugged into an ATM):

- **Dynamic Integrity Control** protects all executable software on the system by detecting any unauthorized activation attempt and preventing the process from launching before damage can occur
- **Dynamic Sandbox** uses a specially-designated user account for potentially vulnerable software, providing system-level privilege controls to block dangerous software activity
- **Dynamic Resource Control** controls how different applications can access files and folders, registry keys, external devices, and network resources at the base of rules

Benefits to ATM Security

- Client remote control can be disabled to permit thin clients to work without central management
- Detects and prevents the launch of malicious software introduced via removable media
- Recognizes protected CDs/DVDs and blocks all others
- Prohibits access to system resources for all applications, except those specifically authorized to do so
- Sends heartbeat status to management console
- Constantly and invisibly monitors ATMs
- All data copy activities, including copying to removable media, monitored in shadow mode
- Forensic “camera” views and records device screen at all times to capture accidental or malicious insider activities

How corporate networks can benefit

More practical and effective than traditional anti-malware or whitelisting alone

- Independence from signature updates - controls applications' behavior, so protects against targeted attacks and "zero-day" threats with no need for updates
- Automatic system profiling and detection of unknown running applications - creates a list of trusted applications automatically; all new applications may be either blocked or run in a sandbox
- Dynamic control over software installations and updates - automatically detects installers for trusted applications, enabling routine patching and updates to occur without manual intervention
- Unified approach to protection from viruses, hackers, insiders.

About SafenSoft

- Founded in 2006, venture investments 2009
- Experienced executive team
  - History with McAfee, Kaspersky Labs, Trend Micro, Symantec.
- Global presence
  - Business HQ in US, Development HQ in Moscow
- Contacts

Technology:

Michael.kalinichenko@safensoft.com

Business:

Jim.leonard@safensoft.com

Questions?