



A Check Point Company

Zone Labs Corporate Presentation

The State of Attacks and Solutions

The Most Trusted Provider
Of Endpoint Security Solutions

An Informal Discussion

- How have threats changed over the last two years?
- What is Zone Labs doing about it?
- Our best hope
- Threats: The latest realities (and some myths)
- Q&A

Stats

- 2003 is considered the year the Internet became positively criminal
- Fraudsters will take 2.8 billion out of e-commerce in 2005 (8% increase)
- From May 2004 to May 2005, 929 million was lost from phishing
- At least 80% of computers have some form of spyware
- Identity theft hit 27.3 million Americans in the last five years (out of ~296 million Americans)
- Most spam attacks are launched from _____
- A reputable online institution will *never* ask you for sensitive data from an e-mail or e-mail Web link (so don't give it)

The hacking life: From geek to rich geek

- Yesterday's hacker: "Somebody pay attention to me!"
 - Huge targets to make names for themselves
 - Easy for antivirus to find and clean (although always late)
 - In general a hack had relatively minor consequences
- Today's hacker: "Forget fame. Give me loads of cash."
 - Small, targeted attacks to take the money and run
 - Polymorphic so nearly impossible to detect in time (prevention is key)
 - Part of organized crime
 - Financial consequences are stolen identity, association with illegal activity, attacks on institutions

Criminal Tactics

- Social engineering
- Kernel level to avoid detection
- Ubiquity

Spyware Changed the Rules

- Unlike viruses, spyware is supported by well-funded companies and armies of developers
- It's ubiquitous, and found on 80% of all computers
- Once on, it can attack the OS and other programs
- It's also extremely difficult to remove safely

Adware is Also a Threat

- People aren't aware of its presence
- It's often not properly secured or patched against hackers
- This combination is ripe for adware to be exploited by hackers as means to gain root privileges, plant malware and steal identity

Kernel-Level Attacks are Growing

- Root Kits are programs designed to gain root privileges on a computer without being detected
- They exploit a known vulnerability or use a stolen/cracked password
- They create a back door for hackers to log keystrokes, launch attacks, and use the computer any way they please.

Traditional Security is Inadequate Defense

- Customers are tricked into inviting threats onto their computer and *past* network firewalls
- Signature-based anti-spyware and similar solutions are useless against *new and unknown* threats
- Root kits and other kernel-level technologies go undetected

Everyday People Face New Levels of Risk

- Unaware people easily fall prey to ID theft
- Computers quickly become slow and unusable
- Access to people's computers is bought and sold on black markets (botnets)
- Attackers steal bandwidth, distribute illegal pornography and carry out attacks – burden falls on unwitting computer owners to prove innocence

The Security Benchmark Must be Raised

- It must *prevent* spyware and malware, both known and unknown
- It must monitor not just at the perimeter, but also *on the computer itself* where threats reside
- It must prevent advanced kernel-level attacks and undetected infiltration
- It must do this without requiring more expertise from people

What is Zone Labs Doing About it?

Introducing ZoneAlarm 6.0

- Anti-spyware stops known as well as unknown threats; includes prevention, scanning and removal
- The first operating system firewall watches activity *on the computer*
- DefenseNet leverages a community of intelligence against attacks
- SmartDefense Service makes advanced technology usable to everyday people

ZoneAlarm Triple Defense Firewall



Action 1: Network FW

Protects your computer from hackers, spyware and Trojan horses

Our proven stateful stealth firewall guards the network perimeter from inbound and outbound threats.

Action 2: Program FW

Prevents bad programs from attacking good programs on your computer

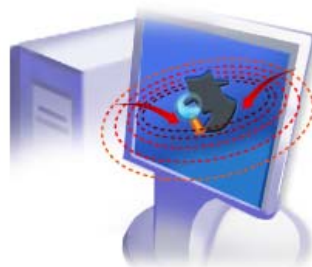
A second firewall layer surrounds each software program, protecting good programs from bad.

Action 3: OS FW

Protects the operating system down to the kernel

The third firewall layer goes down to the kernel to protect the operating system - including the registry and file systems - from attack by malicious programs.

ZoneAlarm Anti-Spyware A Sustainable, Layered Approach



Spyware gets onto the computer

Stop spies *before* they reach the computer

- Network firewall blocks PC access
- Web Privacy feature blocks drive-by downloads
- MailSafe quarantines spyware attachments from e-mail

Spyware unwraps and installs

Stop spies before they unwrap and install

- Triple Action Firewall detects and halts spyware installs

Spyware attacks other programs and the OS

Protect programs and the operating system

- Triple Action Firewall detects, blocks and even kills attacking spies
- Kernel level or simple browser attacks are stopped
- SmartDefense Advisor automates decisions

Spyware burrows in

Spyware is designed to stay on the computer.

- The spyware database in ZoneAlarm products is about quality, not quantity.
- It can even automatically treat some spyware

Our Best Hope: You

Prediction: No government policy, no legislation, no enforcement and no security company can protect the world's infrastructure like you can.

Proposal: A partnership including government policy, legislation, enforcement and security all hinged upon: YOU

So what can you do?

- Continue to educate yourselves
- Protect your own computers and networks
- Tell your friends and neighbors
- Demand security from your financial institutions, ISPs and other institutions (many institutions are doing well)
- Demand strong and usable security from Zone Labs

The Basics:

Behavior:

Never click a link from an e-mail that asks for sensitive data

Stay away from shareware, freeware unless you can validate it

Avoid shady, unknown sites such as porn sites

Update your OS, security and other software

Tools:

The basic three: firewall, antivirus, antispysware

Advanced protection: Kernel-level security

Keep your eyes out for the best technology

Threats: The Latest Realities (and Myths)

Quote



Password-stealing keyloggers skyrocket

[John Leyden](#) 18th November 2005

Hackers are on target to release more than 6,000 keystroke loggers in 2005, a 65 percent increase from last year, according to iDefense (Verisign).

Quote

ContraCostaTimes

.com

Phishing e-mail attacks steadily rise

By Mike Musgrove
WASHINGTON POST

The number of attacks was up 28 percent between May 2004 and May 2005, according to a study by research firm Gartner Inc.

Quote



Study: IM worms up again in November

By [Joris Evers](#) Staff Writer, CNET News.com

Published: November 29, 2005, 2:53 PM PST

Quote



45% of consumers would switch banks for better identity theft protection

Posted by ZDNet Research @ 2:10 pm

45% of consumers worldwide are willing to switch to financial institutions that offer more security protection, [according to survey by Unisys Corporation](#).

The Latest

- Ransomware
- Splogging

CyberTerrorism

- “Terrorists will launch attacks on the nation’s infrastructure and grind our systems to a halt. They will bring down air traffic control, prevent financial transactions, and disable military defense systems.”
- Overstatement or reality?

Nobody knows...However:

- Human involvement in most if not all systems
- Computers and automation already fail, so there are safeguards
- If we can imagine it...

- What **is** reality?
 - The likelihood of a DoS attacks on financial institutions of a large scale
 - Identity theft and other computer crime to fund terrorism
 - Terrorist organization, recruitment, and instruction



Open Forum