Avenging Evil: Symantec Endpoint Protection 12
ISTR XVI - Threat Landscape

2010 Overarching Themes

1. **Targeted Attacks** continue to evolve
   
   Targeted attacks, while not new, gained notoriety from high-profile attacks against major organizations (Hydraq) and significant targets (Stuxnet).

2. **Social Networking** + social engineering = compromise
   
   The ability to research a target online has enabled hackers to create powerful social engineering attacks that easily fool even sophisticated users.

3. **Hide and Seek** (zero-day vulnerabilities and rootkits)
   
   Targeted attacks depend on their ability to get inside an organization and stay hidden in plain site. Zero-day vulnerabilities and rootkits have made this possible.

4. **Attack Kits** get a caffeine boost
   
   Innovations from targeted attacks will make their way into massive attacks, most likely via toolkits.

5. **Mobile Threats** increase
   
   All these types of attacks are moving to mobile devices, limited only by attackers getting a return on their investment.
January 2007: 250,000 viruses
December 2010: 286 million
Malware Authors Have Switched Tactics

From:

A mass distribution – one worm hits millions of PCs

- Storm made its way onto millions of machines across the globe

To:

A micro distribution model.

- Hacked web site builds a trojan for each visitor
- The average Harakit variant is distributed to 1.6 users!
Symantec Endpoint Protection 12
Symantec Endpoint Protection Family

Symantec Endpoint Protection Small Business Edition

- Ideal for less than 100 users
- Maintain your own infrastructure
- All data stored on premise

Symantec Endpoint Protection.cloud

- For Businesses with less than 250 users
- Cloud-based service
- No management hardware needed

Symantec Endpoint Protection

- Scales from hundreds to thousands of users
- Powerful central management
- Ideal for virtual environments
What is SEP SBE 12?

- Antivirus
- Intrusion Prevention
- Firewall
- Antispyware

Single Agent, Single Console
On-Premise Infrastructure
Windows & Mac
What is SEP.cloud?

- Antivirus
- Intrusion Prevention
- Firewall
- Antispyware

Single Agent, Single Console
Hosted Infrastructure
Windows & Mac
What is SEP 12?

Single Agent, Single Console
On-Premise Infrastructure
Windows & Mac

- Antivirus
- Antispyware
- Firewall
- Intrusion Prevention
- Device Control
- Application Control
- Network Access Control
What’s New in SEP 12

Unrivaled Security
- Powered by Insight
- Real Time Behavior Monitoring with SONAR

Blazing Performance
- Up to 70% reduction in scan overhead
- Smarter Updates
- Faster Management

Built for Virtual Environments
- Tested and optimized for virtual environments
- Higher VM densities
Powered by Insight

Proactive protection against new, mutating threats

- Puts files in context, using their age, frequency, location and more to expose threats otherwise missed
- Using community-based security ratings
- Derived from Symantec's more than 175 million endpoints

Insight caught Stuxnet
Why Insight?

- No existing protection addresses the “Long Tail”

Unfortunately neither technique works well for the tens of millions of files with low prevalence.

(But this is precisely where the majority of today’s malware falls)

Bad Files

Blacklisting works well here.

For this long tail a new technique is needed.

Good Files

Whitelisting works well here.
How Insight Works

1. 175 million PCs
2. 2.5 billion files
3. Look for associations
4. Check the DB during scans
5. Provide actionable data

Is it new? Bad reputation?

Prevalence
- Age
- Source
- Behavior
- Associations
Symantec Protection Model

Defense in Depth

1. Network-based Protection
   - Stops malware as it travels over the network and tries to take up residence on a system
     - Protocol aware IPS
     - Browser Protection

2. File-based Protection
   - Looks for and eradicates malware that has already taken up residence on a system
     - Antivirus Engine
     - Auto Protect
     - Malheur

3. Reputation-based Protection
   - Establishes information about entities e.g. websites, files, IP addresses to be used in effective security
     - Insight
     - Domain Reputation
     - File Reputation

4. Behavioral-based Protection
   - Looks at processes as they execute and uses malicious behaviors to indicate the presence of malware
     - SONAR
     - Behavioral Signatures
Most Effective in Real World Test

- Symantec: 98.1% blocked, 1.9% partial, 0% infected
- Sophos: 82.7% blocked, 3.8% partial, 13.5% infected
- Kaspersky: 63.5% blocked, 3.8% partial, 26.9% infected
- Trend Micro: 57.7% blocked, 5.8% partial, 32.7% infected
- Microsoft: 53.8% blocked, 5.8% partial, 40.4% infected
- McAfee: 51.9% blocked, 3.8% partial, 44.2% infected

4% false positives for Kaspersky.
Most Effective in Remediation

- **Symantec**: 114
- **Kaspersky**: 108
- **Microsoft**: 98
- **Sophos**: 95
- **MalwareBytes**: 79
- **McAfee**: 73
- **Trend**: 26

*Only product with a false positive*
Blazing Performance
Faster Scans

Traditional Scanning
Has to scan every file

Insight - Optimized Scanning
Skips any file we are sure is good, leading to much faster scan times

On a typical system, 70% of active applications can be skipped!
Scan Speed

Symantec Endpoint Protection 12 Scans:
• 3.5X faster than McAfee
• 2X faster than Microsoft

Ranked 1st in overall Performance!
Symantec Endpoint Protection 12 uses:

- 66% less memory than McAfee
- 76% less memory than Microsoft
Built for Virtual Environments
Most Important IT Priorities for 2011 and 2012

Top 3 Priorities

1. Increase use of server virtualization
2. Manage data growth
3. Information security initiatives

Built for Virtual Environments

- Optimized for VMware, Citrix and Microsoft virtual environments
- Easy to manage physical and virtual clients
- Maximizes performance and density without sacrificing security
- Best in class performance and security
Virtualization Features

Virtual Client Tagging  Virtual Image Exception  Shared Insight Cache

Offline Image Scanning  Resource Leveling

Together – up to 90% reduction in disk IO
Virtual Desktop Malware Defense

Symantec Endpoint Protection (SEP) 12.1
100%

Trend OfficeScan 8.5
84%

McAfee MOVE + HIPS + SiteAdvisor
60%

12%
4%
40%

Compromised
Neutralized
Defended

Performance in Virtual Environments

- Symantec – completed on-demand scans in almost ½ the time - with 49% less Disk I/O
- Agentless doesn’t mean faster

Note: McAfee’s performance suffered when the VMs were left powered on for more than a day, as denoted by the additional graph. For the on-demand scans on each VM, SEP completed the scan in 12 - 13 minutes; Trend Micro products required 23 - 24 minutes to complete the scan. McAfee MOVE for VDI does not offer on-demand scanning.

Source: Tolly, June 2011
Symantec Endpoint Protection 12

Unrivaled Security
Blazing Performance
Built for Virtual Environments

Download Now!
http://go.symantec.com/sep12
Thank you!

<insert speaker name>
<insert speaker email address>
<insert speaker phone number>