Stop Server Incursions and Unauthorized Access:

*How to Defend Against APT Attacks*

Percy Wadia, CISSP
Sr. Manager, Product Mgmt., SCSP

Prashant Khandelwal
Sr. Product Manager, SCSP
Agenda

1. Cutting Through the Hype
2. Advanced Persistent Threats vs. Targeted Threats
3. What is Critical System Protection?
4. How Critical System Protection can stop APTs
Sophisticated Attacks Have Led To Increased Awareness

Google Hack Attack Was Ultra Sophisticated, New Details Show
By Kim Zetter

RSA SecurID Hack Shows Danger of APTs
By Tony Bradley

Massive Cyber Attack Adds to Suspensions of Concerted Chinese Hacking
Zappos.com hacked; 24 million customers affected

Stop Server Incursions and Unauthorized Access
Servers Are the Target – “Endpoints simply provide an initial foothold”

Exponential growth in Malware poses more risk than in previous years...

- Malicious attacks ↑ 81% in 2011\(^1\)

- Attacks used advanced techniques, generating unique versions of malware

- Targeted Attacks avg. 82/day
  - 58% of attacks were aimed at non-executive functions to gain foothold in organization

\(^1\)-Symantec Internet Security Threat Report April 2012
\(^2\)-Verizon Data Breach Investigations Report 2012
... But Security Execs Believe the Term APT is Overhyped...

63% of execs believe the term APT is being used excessively or in a misleading way

Source: CSO Magazine Research, October 2011
... Often leading to Confusion on how to effectively protect against them

What are the outcomes from the misuse of the term APT?

- Confusion among non-IT executives: 70%
- Confusion among IT executives: 70%
- Distraction from solving other pressing security problems: 57%
- Distraction from solving APTs: 38%
- Other (specify): 11%

Source: CSO Magazine Research, October 2011
How are Targeted Attacks and APTs Related?

APTs are Different from Targeted Attacks:

1. **Customized:**
   *Uses multiple attack vectors, that are customized to the target, not a generic burst of attack vectors*

2. **Low and Slow:**
   *Specifically designed to penetrate low-n-slow, to avoid detection, most likely stays under radar for a sustained period*

3. **Higher Aspirations:**
   *Seeking more than opportunistic gain, usually involves covert state actors*

4. **Specific Targets:**
   *Highly targeted to specific organizations (e.g., govt. agencies) and high-value targets*

An APT is **always** a targeted attack, but a targeted attack is **not necessarily** an APT.
The Advanced Persistent Threat

5 Steps …

1. Phishing Drops Malware
2. Malware Creates a Back Door
3. Malware Morphs & Moves Laterally
4. Data is Gathered
5. Remote Command & Control Exfiltrates Data
Agenda

1. Cutting Through the Hype
2. Advanced Persistent Threats vs. Targeted Threats
3. What is Critical System Protection?
4. How Critical System Protection can stop APTs
Nitro: An APT targeting organizations in the chemical industry

*Additional confirmed infections exist; however, they did not contact the command and control server during the two-week period we were monitoring it.*
Nitro APT Phases

1. Socially engineered email sent
   - Attachments installed Poison Ivy
   - Common Remote Access Tool (RAT)

2. Gathered IP addresses and computer names from network
   - Gathered password hashes to take off-machine for cracking

3. Gained admin credentials and access to critical servers

4. Captured data and moved it to internal staging servers

5. Data sent to C&C servers via port 80

Stop Server Incursions and Unauthorized Access
Stuxnet: An APT targeted at industrial control systems in energy sector

1. Highly targeted, low and slow attack
   - Specifically targeted Industrial Control Systems using Siemens Step 7 PLCs & software
   - Discovered in June’10 but further analysis revealed presence since at least a year ago
   - More than 60% of infections were specifically in Iran, targeting energy / power plants

2. Exploited Known, Unpatched Vulnerabilities
   - Exploited 4 known Microsoft vulnerabilities, 2 for self-replication and 2 for escalation of execution privilege

3. Multiple attack vectors to self-replicate and Auto-Update
   - Self-replicates through removable drives exploiting auto-execution vulnerability
   - Spreads in a LAN through a vulnerability in the Windows Print Spooler
   - Copies & executes on remote computers through network shares or WinCC dB servers
   - Contacts a command & control server to download and execute code, including updates

Customized attack, highly targeted to specific goals, low & slow exploitation, and aspirations beyond opportunistic gain
Agenda

1. Cutting Through the Hype
2. Advanced Persistent Threats vs. Targeted Threats
3. What is Critical System Protection?
4. How Critical System Protection can stop APTs
Servers Are Attacked Differently than Laptops...

Malware

69% of Breaches
95% of Records

Hacking

81% of Breaches
99% of Records
... And Servers Have Unique Security Requirements

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Laptops/Desktops</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blanket, consistent protections</td>
<td>Blanket, consistent protections more important</td>
<td>Targeted Protections based on housed data, function more important</td>
</tr>
<tr>
<td>more important</td>
<td>Change visibility less important. Just block malware.</td>
<td>Change visibility highly important. Who/what/where/when</td>
</tr>
<tr>
<td>Integrity</td>
<td>Continuous availability less important. Reboots expected/OK</td>
<td>Continuous availability highly important</td>
</tr>
<tr>
<td>Availability</td>
<td>Blanket, consistent protections more important</td>
<td>Targeted Protections based on housed data, function more important</td>
</tr>
<tr>
<td>Change visibility less important.</td>
<td>Continuous availability less important. Reboots expected/OK</td>
<td>Change visibility highly important. Who/what/where/when</td>
</tr>
<tr>
<td>who/what/where/when</td>
<td>Continuous availability highly important</td>
<td>Continuous availability highly important</td>
</tr>
</tbody>
</table>

*Desktop-oriented Protections are largely a *Subset* of Server-oriented Protections*
Symantec Critical System Protection
Multi-layer protection for critical systems

- Close back doors (block ports)
- Limit network connectivity by application
- Restrict traffic flow inbound and outbound

Network Protection (Host IPS)
Exploit Prevention (Host IPS)

- Restrict apps & O/S behaviors
- Protect systems from buffer overflow
- Intrusion prevention for zero-day attacks
- Application control

System Controls (Host IPS)
Auditing & Alerting (Host IDS)

- Monitor logs and security events
- Consolidate & forward logs for archives and reporting
- Smart event response for quick action

- Lock down configuration & settings
- Enforce security policy
- De-escalate user privileges
- Prevent removable media use

Stop Server Incursions and Unauthorized Access
SYMANTEC VISION 2012
SCSP Architecture

Symantec Critical System Protection Architecture

Scalability = 5K-8K agents/server

Policy Management
Agent Management
Real-time Monitoring
Users and Roles

Management Console
Reporting

Management Server
Agent Registration
Policy Configuration
Event Logging

HTTPS
JDBC

Asset Data
Policies
Operational State
Event Data

SQL Data Store

Servers
Desktops & Laptops

SCSP Agents

Event Logging

HTTPS
## Critical System Protection Key Capabilities

**Monitoring (HIDS)**
- Event Monitoring
- File Integrity Monitoring
- Intrusion Detection

**Prevention (HIPS)**
- Host Firewall
- File and Configuration Lock Down
- Admin Access Control
- Malware and Exploit Prevention
- Device Control
- Application Control

**Ease of Management**
- Centralized Management
- Out of Box Policy Templates
- Multiple OS Support

---

**SINGLE SOLUTION**
IDS Capabilities Provide Alerting and Real-Time File Integrity Monitoring

**How it Works**

1. SCSP collectors gather events & compare them to IDS rule sets (custom or library), will monitor and log what, where, when and by whom did changes occur, all w/o requiring OS advanced logging.
2. Upon a match, take action.
3. Record event in local SCSP log.

**Stop Server Incursions and Unauthorized Access**

SYMANTEC VISION 2012
IPS Capabilities Provide Least Privilege Application Control (Sandboxing) to lockdown Servers

Most programs require a limited set of resources and access rights to perform normal functions. But most programs have privileges and resource rights far beyond what is required – attacks readily exploit this gap.

creates a “sandbox” or “containment jail” for one or more programs (processes) using a policy that defines least privilege controls or “acceptable” resource access behaviors.

Stop Server Incursions and Unauthorized Access
SCSP Exploit Prevention Function

- SCSP intercepts system calls to/from the application
- The agent runs a limited number of checks for each OS call

Is this resource access allowed for this process?

Host Programs
- Core OS Daemons
  - cron
  - RPC
  - LPD Printer
- Application Daemons
  - Mail
  - Web
- Interactive Programs
  - Email Client
  - Office
  - Browser

Normal Resource Access
- Files
  - Read/Write Data Files
- Registry
  - Read Only Configuration Information
- Network
  - Usage of Selected Ports and Devices
- Devices
Agenda

1. Cutting Through the Hype
2. Advanced Persistent Threats vs. Targeted Threats
3. What is Critical System Protection?
4. How Critical System Protection can stop APTs
Defending Against APTs: Myths and Truths

**MYTHS**
- What worked in the past can stop an APT
- A single technology can stop an APT
- Defending against unknown malware stops an APT
- Employee education is sufficient

**TRUTHS**
- Defense-in-depth is key – no silver bullet
- Malware is just one component of an APT
- People will always be the weakest link
What do APT’s Target on a Server?

APTs attempt to change critical system resources

Critical System Protection

- Ensure Registry Integrity
- Ensure File Integrity
- Prevent Data Leakage
- Prevent Targeted/Advanced Malware
- Ensure Memory Protection
- Prevent Rootkits
How SCSP Protects Against APT’s

1. **Phishing**
   SEP protects endpoint from compromise

2. **Backdoor**
   CSP prevents malware communication on endpoint

3. **Malware Spreads**
   CSP protects servers from compromise
   CSP can segment key assets from potential high risk workstations

4. **Exfiltration**
   CSP prevents outbound communication to untrusted systems
   CSP protects critical data on server from unauthorized users

Stop Server Incursions and Unauthorized Access

SYMANTEC VISION 2012
SCSP Provides out-of-the-box Policy Templates for greater flexibility & control

- **Targeted**: Customizable Policy for Specific, Targeted Prevention
  - Enables easy / fast build out of custom IPS policies in targeted stages, sequentially enabling prevention capabilities

- **Core**: Core OS Protection with Maximum Application Compatibility
  - OS Hardening + Buffer Overflow protection

- **Strict**: Strict OS and Application control
  - Buffer Overflow + Network Lockdown + System file lockdown

- **Limited Execution**: Limits Execution of non-server applications
  - Strict + execution denial for interactive processes, unless in white-list

Stop Server Incursions and Unauthorized Access
Targeted Prevention Policy

What it does: Focuses on a few customer use cases

- Black listing
- White listing
- Resource restriction
- Network control
- Memory protection
- CSP Self Protection
- Wide open, no restrictions by default

What it does not do

- Lock down the core OS
- Restrict inbound and outbound connections
- De-escalate administrator rights
- Govern good behavior of applications
- Provide out of the box protection for several common applications
- Prevent applications from starting

Stop Server Incursions and Unauthorized Access

SYMANTEC VISION 2012
Summary: Targeted Attacks and APTs are constantly reinventing themselves...

Malware variants exploit new zero-day vulnerabilities and leverage new attack vectors each day, making it challenging for security solutions to “keep up”

<table>
<thead>
<tr>
<th>Vulnerability or Attack Vector</th>
<th>Targeted Attack/Malware/APT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability</td>
<td>Stuxnet Worm</td>
</tr>
<tr>
<td>Poison Ivy Trojan (sent as email attachment)</td>
<td>Nitro</td>
</tr>
<tr>
<td>IE Remote Code Execution Vulnerability</td>
<td>Hydraq (Operation Aurora)</td>
</tr>
<tr>
<td>Vulnerability in Windows Kernel-Mode Drivers</td>
<td>Duqu</td>
</tr>
</tbody>
</table>
… and SCSP can protect against these attacks by focusing on enforcing “good” behavior

Buffer Overflow Incursion via LNK vulnerability
Spreads to USB drives and network using Print Spooler vulnerability, file shares, etc.

SCSP detects the Stuxnet buffer overflow
Uses LPAC to confine process (no access to system resources)

Poison Ivy Trojan
Spreads through email, injects itself into other processes to control machine

SCSP detects the execution of Poison Ivy
Uses LPAC to prevent thread injection, stops registry modification and execution

IE Remote Code Execution Vulnerability
Exploits IE vulnerability to open back door that allow remote attacker access to machine

SCSP blocks inbound/outbound network access
Uses LPAC to block installation, stateless firewall prevents connection to C&C servers

Vulnerability in Windows Kernel-Mode Drivers
Allows remote code execution if user opens a special document or visits a malicious Web page

SCSP blocks shell code from launching
Uses LPAC to prevent launch of a shell to install programs, create accounts, manipulate files

Regardless of the attack vectors or vulnerabilities exploited by known or unknown threats, SCSP protects by leveraging least privilege application control features
# Critical System Protection Helps Organizations Achieve Key Business Initiatives

## Block Advanced Attacks
- Strong zero day protection
- “Least Privilege” sandbox prevents malicious behavior
- High performance: policy-based & signature-less

## Patch Mitigation
- Secure against unpatched vulnerabilities
- Broad platform coverage (Over 33 platforms, physical and virtual)
- Reduce cost of custom platform support

## Visibility into Compliance Posture
- Track and monitor user access real-time
- Monitor key files and report on changes with differentials
- Manage configuration drift: restrict access to only specified admin

---

**Case Studies: Meeting Compliance & Applying Proactive Prevention**  
**SYMANTEC VISION 2012**
Thank you!