DDoS Monitoring System using Cloud AV

2009.09.30
AhnLab, Inc.
SiHaeng Cho, Director of R & D Center
Table of Contents

I. Recent Security Threat Trend

II. Security Industry Response & Issues

III. AhnLab Smart Defense

IV. DDoS Monitoring System
I. Recent Security Threat Trend
Malicious Code Evolution

- Slow infection
  - Curiosity, self-display

- Quick infection
  - Financial motive

- Zero-Day attack
  - Financial motive

- Aggravating into crime
  - Targeted attacks
  - Quick & easy to produce variation

- Financial motives/organized

- • Trojans
  - • Social engineering technique
  - • Complicated & sophisticated
  - • Diversifying distribution methods

- WEB, P2P, USB Multimedia service
Minimum IT resource utilization

Introduction of stealth technique

Quick & easy variation production

Mass production of malware
New Threat by Spam Mailer

- Bredolab
- Palevo
- Waledoc
- Boaxxe
- Downloader
- Agent
- Virut
- FakeAv
- Autorun
- Rustock
Problem with the Removal

Spam Mailer

System Process
(svchost.exe or explorer.exe)

Malicious Activities

Malware Download

Spam Mail Sending

Spreads by Exploit

Rootkit (Stealth/API Hooking)

File Infection (ndis.sys, agp440.sys)

...
7.7 DDoS Attack Flow

- `msiexec1.exe (main)`
  - Win-Trojan/Downloader.374651
- `_S3.tmp (wmiconf.dll) Malware`
  - Win-Trojan/Agent.67072.DL
- `_S4.tmp (wpcap.dll)`
- `_S5.tmp (packet.dll)`
- `_S6.tmp (wanpacket.dll)`
- `_S7.tmp (nfp.sys)`
- `_S8.tmp (npptools.dll)`
- `_S9.tmp (wmcfg.exe) Malware`
  - Win-Trojan/Mydoom.88064
- `pxdrv.nls (Encrypted File)`
- `msiexec9.exe`
- `uregvs.nls`
  - BinImage/Host
  - Attack URL/Time/Type
- `wversion.exe (Dropper)`
  - Win-Trojan/Destroyer. 40960
- `wversion.exe (1st)`
  - Win32/Mydoom.worm.33764
- `mstimer.dll`
  - Win32/Mydoom.worm.45056.D
- `wversion.exe (2nd)`
  - Win-Trojan/Destroyer.37264

**DDoS Attack!!!**
- (30 Threads/Sites)

- **Create**
  - A certain IP address
- **Reference/Update**
  - File Download
  - (Update Target Host)
- **Destroyer**
  - Disk Data Damage
  - SPAM Mail Sending

If `msvcr90.dll` exists,
- Download

- **Memory of the Independence Day..**
  - ....................
  - .................
  - .................
  - .................

- **09.07.10 00AM**
Anti-virus Program Use vs. Malicious Code Damage

<table>
<thead>
<tr>
<th></th>
<th>Anti-virus use</th>
<th>Mal. code damage experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>5~9 persons</td>
<td>54.4%</td>
<td>11.7%</td>
</tr>
<tr>
<td>10~49 persons</td>
<td>14.9%</td>
<td>20.9%</td>
</tr>
<tr>
<td>50~249 persons</td>
<td>20.9%</td>
<td>32.1%</td>
</tr>
<tr>
<td>250 persons or more</td>
<td>90.8%</td>
<td>32.1%</td>
</tr>
</tbody>
</table>

Source: 2008 ICT Statistics

Why?
Malware vs. Anti-malware

Source: AV-test.org

Can we still survive?

2005: 333,000
2006: 972,000
2007: 5,490,000
II. Security Industry Response & Issue
Security Industry Response & Issue

- Improve detection rate
- Increase update frequency
§ Engine Size Growth

Cumulative Signature Update Size of Anti-virus Industry

Source: AV-test.org
Issues Entailing Engine Size Growth

- Higher resource utilization rate
- Slowing inspection speed
- Greater possibility of mistaken diagnoses
Security Industry Response & Issue

- Improve detection rate
- Increase update frequency
Why Update Frequency Matters?

- Propagation rate
- Anti-virus engine update
- Damage ($$$$)

Time

Copyright (C) AhnLab, Inc. 1988-2009. All rights reserved.
Update Frequency: 1 week to 1 day

Update frequency increased from daily to hourly

Update frequency increased from hourly to every 30 minutes
• 1 new malware is created every 2.5 seconds

30-minute update interval equals potential exposure to 720 new malware
A Novel Paradigm in Fighting Malicious Codes

AhnLab Smart Defense
How AhnLab Smart Defense Works

- Cloud Based Anti-Virus Engine
- Operates file DNA database containing more than several dozens of millions of records consolidated by a variety of analysis techniques
- Responds with harmfulness of a file accessed by a user in real-time
AhnLab Smart Defense Capabilities

Malicious code diagnosis
- Analyze program information
- Reputation system analysis
- Analyze file activity trends
- Conduct behavior-based activity analysis
- Analyze inter-file relation

High throughput
- Accommodate a minimum of 50 million users
- Collect over 20 million files
- 3TERA Byte DB Query

DDoS response
- Real-time N/W malfunction monitoring & detection system
- Trace file distribution path
AhnLab Smart Defense Advantages

High detection rate
- Utilize a variety of diagnostic technologies
- 20% increase from existing engines

Lightweight / High performance
- Engine file size: 1MB
- Engine memory utilization: 2MB
- Network traffic: Less than 0.1% (100Mbps)
- Faster inspection: 15 sec. (initial) or 2 sec. (retry) when inspecting Windows folders (13,115)

Real-time update
- No need for update, as engine access the AhnLab Smart Defense Center to inquire abnormality of a file in real-time
HAS (Hybrid Analysis System) increases detection rate

- Determine if a file is normal or malicious by analyzing file profile data, program digital signature, reputation system, file activity trends, behavior-based activity, and inter-file relation, etc.
- Improve detection rate with the ability to collect/analyze new malicious codes in real-time
DDoS Monitoring System
Recent DDoS Attack Trends

**Primary Attack Targets**
- Expands to include large game publishers, Web portals and financial service sites

**Social Awareness**
- Expands across the IT industry in general

**Driver & Type of Attack**
- Financial ransom & trial attack
- Diversifying attack patterns (TCP/UDP/ICMP/IGMP)

---

**Primary Attack Targets**
- Expands to include large contents providers

**Social Awareness**
- Only some experts pay attention

**Driver & Type of Attack**
- Financial ransom
- Small/mid-size TCP/UDP Traffic attack

---

**Primary Attack Targets**
- Expands to include small/mid-size contents providers as well

**Social Awareness**
- Some IT media show interest

**Driver & Type of Attack**
- Financial ransom & trial attack
- Diversifying attack patterns (TCP/UDP/ICMP/IGMP)

---

**Primary Attack Targets**
- Ransom amount on the rise (to dozens of million Korean won)

**Social Awareness**
- Social awareness increases greatly

**Driver & Type of Attack**
- Stronger TCP Connection attack & massive UDP attack
- Financial transaction of Chinese attacking tools & emergence of attack on contract
DDoS Attack Evolution

TCP Protocol
- TCP Syn Flooding

Non-TCP Protocol
- UDP Flooding
- ICMP Flooding

TCP Protocol
- Spoofed / Non-Spoofed
- TCP Syn Flooding
- TCP Syn-Ack Flooding
- TCP Ack Flooding
- TCP Fin Flooding
- TCP Rst Flooding
- TCP Connection Flooding
- TCP Other Flags Flooding

Non-TCP Protocol
- Small-Size UDP Flooding
- Big-Size UDP Flooding
- Small-Size ICMP Flooding
- Big-Size UDP Flooding
- UDP/ICMP + Fragments
DDoS Attack Evolution

**Attack Type**
- One Type Attack
  - TCP/IP Attack

**Control Attack PCs**
- Combined Type Attack
  - TCP + UDP
- Generate Random Protocol
- Application Protocol Attack
  - HTTP Get Refresh
  - HTTP CC Attack
  - HTTP no-cache Attack
  - HTTP Get Nothing Attack
  - DNS Query Flooding
  - SIP Signaling Flooding
  - BGP Attack

**Control Attack PCs**
- 1:1 DoS Attack
  - CLI Based Control
  - Tunneling Control
  - Advanced Technology

- N:1 or N:N DDoS Attack
  - DrDoS Attack
  - GUI Based Control with Auto-Making Zombie PCs
  - Easy Technology
“Anti-DDoS protection alone cannot defeat DDoS attack attempts.”

A new form of compound attack

- Compound attack, unlike conventional type of attack, frustrates simple anti-DDoS protection arrangement
  - DDoS attack is no longer distinguishable from normal traffic

Intelligent attack

- Scheduler built in malicious codes renders defense ineffective, unless malicious codes are fully analyzed
  - DDoS codes wait in complete ambush even after infection before launching attack at once

Damage HW in addition to turning PC into Zombie

- Defense is not possible unless malicious code designed to damage HW is fixed or prevented from being downloaded in advance
  - Early action intended to keep PC from being turned into Zombie in advance is essential
DDoS Monitoring System

1. Detect abnormal network traffic from a specific file
2. Monitor identical events
3. Analyze in real time
   - Analyze program information
   - Analyze reputation system
   - Analyze file activity trend
   - Analyze behavior-based activity
   - Analyze inter-file relation
   - Analyze malicious code distribution path
4. Apply analysis results in real time

Risk information collector

DDoS Monitoring Center

Early DDoS propagation warning
Preemptive DDoS defense

Authorities/ ISPs
Businesses

Prevent propagation of Zombie PCs
- Analyze program information
- Analyze reputation system
- Analyze file activity trend
- Analyze behavior-based activity
- Analyze inter-file relation

- If network traffic exceeds predefined DDoS threshold, but, whether a file contains malicious codes or not cannot be determined, statistics-base processing is utilized (Ex.: network traffic generated in multiple clients for the same destination exceeds Predefined threshold)

- Analyze traffic statistics including entity causing network traffic, destination and traffic volume
- Trace file distribution path
DDoS Monitoring System Advantages

<table>
<thead>
<tr>
<th>Respond to unknown malicious codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Employ a variety of diagnostic technologies</td>
</tr>
<tr>
<td>- Enable real time response prior to vaccine engine update</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduce diagnostic error rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Reduce diagnostic error rate by determining existence of malicious code in reference to AhnLab Smart Defense Database</td>
</tr>
<tr>
<td>- Reduce error rate by analyzing on the basis of behavior &amp; statistics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real time update benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Update information on new malicious code real time to keep Zombie PCs from multiplying</td>
</tr>
</tbody>
</table>
AhnLab
The Joy of Care-Free Your Internet World

Thank You.