Introduction to Anti-Malware

AhnLab, Inc.
Kyu-Beom Hwang
hwangkb@ahnlab.com

CONTENTS

• MALWARE/MALCODE
  – MALWARE ?
  – MALWARE ATTACK
• DDoS ATTACK
  – DDoS ?
  – 7.7 DDOS CRISIS
• SECURITY IN A LIFE
  – SECURITY IN A LIFE
  – BANKING SECURITY
  – IT’S FREE
  – MESANGER PHISHING
  – ROUGE ANTIVIRUS
• CLOSING MENTS
MALWARE/MALCODE

MALWARE (Malicious Software)
- Computer Virus
- Trojan-Horse
- Backdoor
- Unwanted Program

MALCODE (Malicious Code)
- Internet Worm
- Rootkits

• The release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications. by Symantec

• Malicious Codes are defined as all kinds of executable programs, macros, or scripts that are produced in order to intentionally damage computer system. by AhnLab
MALWARE

MALWARE (Malicious Software)
MALCODE (Malicious Code)

Computer Virus
Internet Worm
Trojan–Horse
Backdoor
Un–wanted Program
Rootkits

ANTI–MALWARE

ANTI–VIRUS = ANTI–MALWARE

MALWARE ATTACK

• Breended Attack
  – Security exploits, commonly used by malicious hackers, are being combined with computer viruses resulting in a very complex attack, which in some cases goes beyond the general scope of antivirus software.

• Buffer Overflows
  – Buffer overflows are generally broken into multiple categories, based on both ease of exploitation and historical discovery of the technique. While there is no formal definition, buffer overflows are, by consensus, broken into three generations. First generation buffer overflows involve overwriting stack memory; second generation overflows involve heaps, function pointers, and off–by–one exploits; and finally, third generation overflows involve format string attacks and vulnerabilities in heap structure management.
MALWARE ATTACK

• Rootkits
  - Rootkits have become a huge threat. The technology is not new, its been around in the Unix world for a long time. But recently, Windows hackers have released it into the wild. Rootkits are a type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection. Wrapped in a cloak of invisibility, rootkits enable an attacker to access and run the very root of a computer. Rootkit technologies can cloak viruses to evade detection, and when malicious code is spotted, make it harder to completely eradicate it from the infected system.

• Hypervisor level (Using Virtualization Technology)
  - These rootkits work by modifying the boot sequence of the machine to load themselves as a hypervisor under the original operating system. By exploiting hardware features such as Intel VT or AMD-V, the rootkit is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system, which is now a guest. The "SubVirt" laboratory rootkit, developed jointly by Microsoft and University of Michigan researchers, is an academic example of a virtual machine based rootkit (VMBR), while Blue Pill is another.

From Wiki

MALWARE ATTACK

• http://en.wikipedia.org/wiki/Sony_BMG_CD_copy_protection_scandal

WHAT IS THE PROBLEM?
**MALWARE ATTACK**

**Behavior**
- Blended Threats
- Multi-layered Attack
- Multi Attack from Network and PC
- Using Integrated Resource – Hacking, Malware, Bot etc.

**Path**
- Gateway, Endpoint, Host
- Inbound/Outbound Threat Flow
- Variety of Threat Transmission Method

**Characteristics**
- Creating Threat Contents Endlessly
- Used for specified criminal acts
- Attacking Target for Money
- Cost-Efficient (ex. DDoS)

**Unified Threat Management**

**Intelligent Security Platform**

**Professional Service**

---

**MALWARE ATTACK**

Many users experienced malware attacks during using AV.

- **Anti-virus use**
- **Mal. code damage experience**

<table>
<thead>
<tr>
<th>5–9 Employees</th>
<th>10–49 Employees</th>
<th>50–249 Employees</th>
<th>250 Employees or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>54.4%</td>
<td>69.9%</td>
<td>83.3%</td>
<td>90.8%</td>
</tr>
<tr>
<td>11.7%</td>
<td>14.9%</td>
<td>20.9%</td>
<td>32.1%</td>
</tr>
</tbody>
</table>

**WHY?**

From 2008 IT Statistics (Enterprise sec.)
Most of the computers were infected by downloading from the internet.

From 2008 IT Analysis (Enterprise sec.)

7.7 DDoS CRISIS IN KOREA
DDoS?

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

First Stage DDoS
- Simple Attack
  - Nature: Curiosity
  - Method: Manually

Second Stage DDoS
- TCP/Application Vulnerability Attack
  - Nature: Criminalized
  - Method: Automatically
  - Objectives: Money

Third Stage DDoS
- Complicated & Intelligent Attack
  - Nature: Criminalized, Political Objective
  - Method: Automatically
  - Objectives: Money
**Case Study**

- **2009.7 : 7.7 DDoS Disaster**
  - 2008.6 : Stop service for 9 hours at the xxx site.
  - 2008.6 : Stop home pager service due to DDoS attack.
  - 2007~2008 : Attack to government site
  - 2007.5 : Attack to game related site.
  - 2007.6~8 : Attack to travel agency.

**First Response** Korea and US government agencies, Portal sites, Banks etc. (7/7 ~ 7/8)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>First received the malware from the customer</td>
</tr>
<tr>
<td></td>
<td>7/6, 1:24PM</td>
<td>Attack is reported using port 80</td>
</tr>
<tr>
<td></td>
<td>7/6, 9:52PM</td>
<td>Six signatures are added to the engine (V3: 2009.07.06) ; Gathering Samples Automatically</td>
</tr>
<tr>
<td></td>
<td>7/7, 2:48AM</td>
<td>One signature is added to the engine (V3: 2009.07.07)</td>
</tr>
<tr>
<td></td>
<td>7/6, 6:03PM</td>
<td>First DDoS Attack Response : Domestic - 13, Overseas - 13 Sites(7/7 6PM~7/8 6PM)</td>
</tr>
<tr>
<td></td>
<td>7/7, 8PM~11PM</td>
<td>Received the attacking attempt from customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attempt to attack the web site of National Assembly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requested to analyze DDoS issue from NCSC and KISA</td>
</tr>
<tr>
<td></td>
<td>7/8, 00:20AM</td>
<td>Three signatures were added to the engine (V3 : 2009.07.08.01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wmidt.dll(Win.Trojan.Agent.67072.DL) : Cause DDoS Traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>uregvs.nls(BinImage/Host) : Target URL list (Domestic 13, Overseas 13)</td>
</tr>
<tr>
<td></td>
<td>7/8, 2:05AM</td>
<td>Verified three assumed downloading IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notified to KT to cutoff the downloading IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(KT : Korea Telecom)</td>
</tr>
<tr>
<td></td>
<td>7/8, 7:00AM</td>
<td>Analyzing the source of the infection and the malware and making the removal tool</td>
</tr>
<tr>
<td></td>
<td>7/8, 11:05AM</td>
<td>Update First Removal Tool(Requested by NCSC and KISA)</td>
</tr>
</tbody>
</table>
## 7.7 DDoS CRISIS

### Second Response: Korean Web Sites + Ahnlab etc. (7/8 ~ 7/9)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Second Attack Response:** Domestic – 14 sites (7/8 6PM ~ 7/9 6PM)
- Defense Ministry, Chong Wa Doe, NIE, e-Government, USFK, Naver mail, Daum mail etc.
- Auction, Hana/Woori/Industrial Bank of KOREA, AhnLab etc.
- Moved the location of the removal tool: Ahnlab web site traffic have overloaded. Added the CDN link.

- Four signatures were added to the engine (V3 : 2009.07.09.00):
  - Samples were collected:
    - uregva.nls(BinImage/Host), Wversion.exe(Win-Trojan/Destroyer.37264),
    - flash.gif(BinImage/Destroyer), msiexec2.exe(Win-Trojan/Agent.33841)

- Acknowledged the attack schedule and updated the analysis information on the web site:
  - Recognized the algorithm of the target URL (Verified Three attacks)
  - Also found the hardware damaging function
  - Updated Removal Tool

- Update Removal Tool again: Updated for detecting nls files
- Announced the attack scheduler to the press (July 9, 9AM)

### Third Response: Korea government agencies, Portal sites, Banks etc. (7/9 ~ 7/10)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Third Attack Response:** Domestic – 7 sites (7/9 6PM ~ 7/10 6PM)
- e-Government, Naver Mail, Daum Mail, Paran Mail, Kookmin Bank, Chosun Daily, Auction

- Announcing Hardware Damaging Function (Ahnlab.com)
- On July 10, midnight the hardware will be damaged by wversion.exe(Win-Trojan/Destroyer.37264)

- ASD Removal Tool (Real Time Protecting program for DDoS Malicious code: Protecting HDD function added)

- Grasp the Damage: some companies, 130 individual users (101 free-users)

- Operate emergency response team for the weekend: To response additional attack and for infected users
### 7.7 DDoS CRISIS

#### Connection between Malicious Codes
- More than one Malware operates with each other
- Need to know all the connection between the malwares to analyze correctly
- Operates with Downloader or Dropper

#### Attack Scheduling and Update Function
- Attacking Methods were scheduled for five days
- It can change the schedule and download from outside
- There is no C&C server

#### Multi DDoS Attack To Multi Domain
- Attacking variety of target from one zombie computer
- It could have used different method of attack and time to each target, but it didn’t
- It made harder to response by using HTTP, UDP, ICMP DDoS attack

#### Damages Hard Disk and Important Files
- Execution file that has damaging hardware function was active from July 8
- Execution file looks like image file(JPG) and it would be downloaded from variety of IPs
- Damaging important documents like DOC, PPT, etc.

---

### Multi DDoS Attack for Multi Domain

<table>
<thead>
<tr>
<th>Type</th>
<th>Attack Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP-DDoS</td>
<td>- HTTP requesting GET Sending almost 20, 12K of data per second</td>
</tr>
<tr>
<td></td>
<td>- Packet that sends from 4 to 48 byte of data through TCP/80</td>
</tr>
<tr>
<td></td>
<td>- Sending almost 21, 1.4K of data per second (using fake source IP)</td>
</tr>
<tr>
<td>UDP-DDoS</td>
<td>- Sending almost 23, 1.5K data per second (using fake source IP)</td>
</tr>
<tr>
<td></td>
<td>- Applying Smurfing method using Local LAN broadcasting</td>
</tr>
<tr>
<td>ICMP-DDoS</td>
<td>- Sending almost 23, 1.5K data per second (using fake source IP)</td>
</tr>
<tr>
<td></td>
<td>- Applying Smurfing method using Local LAN broadcasting</td>
</tr>
</tbody>
</table>

- Infected computers don’t send enormous packet. It only sends about less than 300 packets per second.
- Most of the random data are send by HTTP and 10~15% of the data are send by ICMP and UDP
- Generates traffic in order of HTTP > ICMP > UDP
- HTTP is about 70%, ICMP 12-20%, UDP 6-8% of the packet
- Generally traffic is generated approximately 260-300, 50-65K per second

---

VIRUS
### Name of the Malware

<table>
<thead>
<tr>
<th>No.</th>
<th>Major Malicious Files</th>
<th>Malware Name used in V3 products</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>msiexec1.exe</td>
<td>Win-Trojan/Downloader.374651</td>
<td>Main Program</td>
</tr>
<tr>
<td>2</td>
<td>msiexec2.exe</td>
<td>Win-Trojan/Agent.33841</td>
<td>A number of files exist in the form of msiexec2.exe and all are deleted after dropping uregvs.nls</td>
</tr>
<tr>
<td>3</td>
<td>msiexec2.exe</td>
<td>Win-Trojan/Agent.24576.AVC</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>msiexec3.exe</td>
<td>Win-Trojan/Agent.32768.AIK</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>msiexec3.exe</td>
<td>Win-Trojan/Agent.24576.AVD</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>uregvs.nls</td>
<td>BinImage/Host</td>
<td>So far 5 different uregvs.nls files have been found</td>
</tr>
<tr>
<td>7</td>
<td>wmiconf.dll</td>
<td>Win-Trojan/Agent.67072.DL</td>
<td>DDoS Attack</td>
</tr>
<tr>
<td>8</td>
<td>perfw.dll</td>
<td>Win-Trojan/Agent.65536.VE</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>mstimer.dll</td>
<td>Win32/Mydoom.worm.45056.D</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>wmctf.exe</td>
<td>Win-Trojan/Mydoom.88064</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>wversion.exe[1st]</td>
<td>Win32/Mydoom.worm.33764</td>
<td>Supports running mstimer.dll</td>
</tr>
<tr>
<td>12</td>
<td>wversion.exe[2nd]</td>
<td>Win-Trojan/Destoryer.37264</td>
<td>Damages Hardware and files</td>
</tr>
</tbody>
</table>

### Attack Flow – needs to know every connection of the files to analyze

**DDoS Attack!!!** (30 Threads/Sites)
7.7 DDoS CRISIS

• THE LESSON OF 7.7 DDoS CRISIS
  - COME UP WITH AN EFFECTIVE RESPONSE
    CAPABILITIES FOLLOWING SECURITY
    PARADIGM SHIFT
  - NETIZENS DO ACTIVELY PARTICIPATE IN
    CLEANING ZOMBIE PCs
  - MAKE AN INVESTMENT AND
    CONSIDERATION OF CYBER SECURITY IN
    THE NATIONAL LEVEL

WHAT DO YOU HAVE TO DO?

http://blog.ahnlab.com/ahnlab/660

SECURITY IN A LIFE
SECURITY IN A LIFE

• WHAT IS THE SECURITY HOLE?

SECURITY IN A LIFE

• USB FLASH DRIVE
  - FOR PERSONAL DATA TRANSPORT
  - FOR CONNECT THE INCREDIBLE PCs
  - CAN EASILY CONNECT TO PCs
  - MAY USE TO COPY THE CRITICAL CONTENTS (CONFIDENTIAL OR PRIVATE)
  - SOMETIMES, AUTO EXECUTES A MALWARE FROM VIRUS INFECTED ONE.

WHAT DO YOU DO IF YOU LOSE IT?
SECURITY IN A LIFE

• UN-CONTROLLED (FREEDOM) WIRELESS LAN
  - EASY OF USE OF CONNECTING INTERNET
  - NO WIRE, NO LIMITATION OF SPACE
  - NO ANY PERMISSION (ID AND PW)
  - EASY OF SHARING FOLDER
  - USE INTERNET FOR FREE!

WE CAN USE INTERNET FOR FREE, ANYWHERE, ANYTIME. REALLY?

DO YOU LOVE THE "DEFAULT" SETTING?

SECURITY IN A LIFE

• FREE APs
SECURITY IN A LIFE

• MALWARE DOWNLOADER

WEB SERVERS

ATTACKER

INTERNET

GET ATTACK URL LIST

AUTOMATICALLY DOWN LOADING MALWARES BY DOWNLOADER
SECURITY IN A LIFE

Outflows private information using free WLAN service in the coffee shop.

BANKING SECURITY

• DO YOU SAVE THE SECURITY CARD IMAGE IN YOUR PC?

Police Investigating Hana Bank Hacking

By Bjo. Sork
Staff Reporter

Police are investigating the alleged hacking of Hana Bank's online banking system that led to the theft of tens of millions of won last month.

The Seoul Gangnam Police Station said it received a report that a total of 21 million won ($15,000) was withdrawn from an account of a woman identified as Shin, Jan. 5.

She received a phone call from KiwonBank, a bank at which she holds accounts, warning her of possible private information leakage. She changed the passwords but soon found out that money had been withdrawn from her account at Hana Bank. She changed her security card number, but again, large amounts of money were withdrawn.

Her account at KiwonBank was also reported to have been accessed by an IP addressed in China, but she had no balance there, incurring no damage.

Both Hana and KiwonBank said their own online banking systems were not hacked. They said Shin seemed to have hacked private information hacked elsewhere and criminals withdrew the money with the stolen information.

Police are tracing the IP address and investigating where the money was withdrawn.

tjs@koreatimes.co.kr


ABLE TO HIJACK BY MALWARE

LOGIN ID/PW
CERTIFICATE AND PW
TRANSFER PW
ACCOUNT PW
SECURITY CARD


Outflows private information using free WLAN service in the coffee shop.

IT’S FREE!

• IT’S A FREE SOFTWARE FOR YOU AND ME.

COULD INSTALL SPONSER PROGRAM...

DOWNLOAD A FREE SOFTWARE FROM TRUST SITES!

MESSANGER PHISHING

WHO ARE YOU?

http://blog.naver.com/sthe2002/140099254945
http://blog.naver.com/choaa10/60088243316
http://blog.naver.com/khjung0625/140059583692

http://blog.naver.com/chooa10/60088243316
http://blog.naver.com/chooa10/60088243316
MESSANGER PHISHING

POLICE ARREST THE MESSANGER PHISHING GANG

ROGUE ANTIVIRUS

WHAT IS THE BEST CHOICE?
CLOSING MENTS

• THE SECURITY ACCIDENT IS THE RESULT OF A MOMENT’S INATTENTION.

• THE SECURITY ACCIDENT IS THE RESULT OF WICKED HABITS.

• RAISE YOUR PC SECURITY AND ENJOY THE SECURE COMPUTING!

• YOU DO PATCH VULNERABLE OS AND DO USE AV(FREE OR COMMERCIAL).