

Talking About 0day

Sowhat

sowhat@secway.org



X'con 2005

Who am I

- ❖ C:\>whoami
Secway.org\Sowhat
- ❖ Security Researcher @
www.AIAV.com.cn
- ❖ Application Assessment Focused
- ❖ Have found Multiple vulnerabilities in
several popular software



Overview

- ❖ **0day 6w**
- ❖ **How to Find 0day**
- ❖ **How to Get 0day**
- ❖ **Defend Against 0day**
- ❖ **0day related Laws**
- ❖ **The Future**



What's 0day

- ❖ 0day is the vulnerability that has not yet been published and therefore do not have a fix yet
- ❖ 0day exists in both Server side and Client side
 - ❖ Server side : HTTPD, FTPD, IMAPD and so forth
 - ❖ Client side : IE, Firefox, Word, Acrobat Reader, WinRAR, Realplayer, Winamp, etc



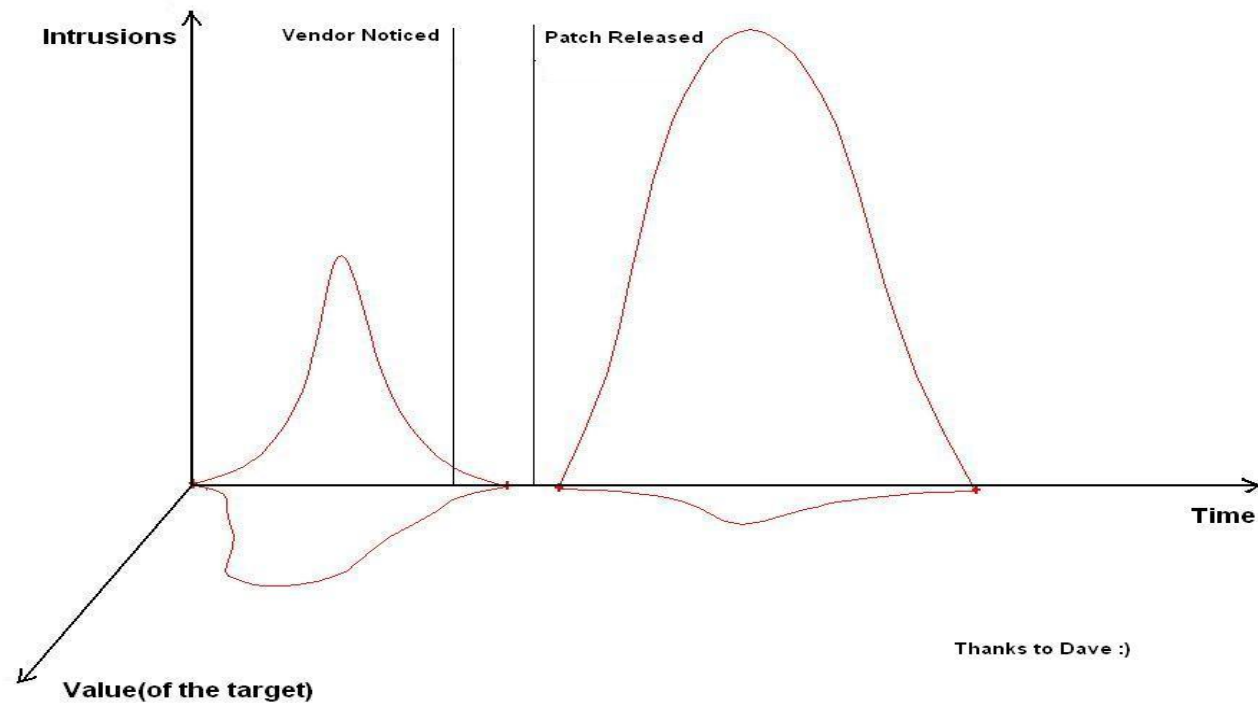
What's Oday (continued)

Oday may not be publicized and distributed privately for years

- ❖ Webdav ntdll.dll
- ❖ CVS Entry Line Heap Overflow (CAN-2004-0396)
- ❖ dtlogin remote root (Founded by Dave Aitel in 2002-06-06 AND publicized in 2004-03-23)
- ❖ Too Many.....



A 0day's Life



Who use 0day

- ❖ Intelligence department
- ❖ Hackers
- ❖ Pen-tester
- ❖ The worms exploit 0day too.

(IE iframe vulnerability exploited by W32.Bofra)



Why use 0day

- ❖ Effective

Most of the public vulnerability doesn't work any more, especially the valuable target

- ❖ Evade the detection (IDS)

- ❖ It's cool ;)



Who is the target

- ✦ Military?
- ✦ Business
- ✦ Bank (Online)Money J
- ✦ You ? Me? Everybody



Who find 0day

- ❖ Security Company. (eEye, NGS, ISS, NSFOCUS..)
- ❖ Independent Researcher
- ❖ Hackers
- ❖ VSC
- ❖ Vendor?? (Oracle said that 75% of the important vulnerability were found by themselves :)



Why find 0day

- ✦ Hack the system
- ✦ For fun
- ✦ Save the world
- ✦ Patch their own product
- ✦ Safe their own system
- ✦ Flame hunting?



Talking about 0day

◆ 0day 6w

◆ How to Find 0day

- ◆ Source code audit
- ◆ Binary Audit
- ◆ Fuzzing
- ◆ Demo1

◆ How to Get 0day

◆ Defend Against 0day

◆ 0day related Laws

◆ The Future



How to find 0day

Bug hunting is not rocket science!

- ❖ Source code audit
- ❖ Binary Audit
- ❖ Fuzzing



Source code audit

- ❖ Open Source ; some commercial vendors have shared their source code
- ❖ FlawFinder, RATS ,ITS4, SPLINT, CodeScan
- ❖ Time consuming
- ❖ Highly based on your experience
- ❖ Only when source code is available



Binary Audit

- ❖ Excellent understanding of the assembly language needed
- ❖ Binary diff (patch analysis, Microsoft Tuesday)
- ❖ IDA Pro , Bindiff, SmartRisk
- ❖ Halvar Flake, Funnywei



Fuzzing

- ❖ Effective (for my experience)
- ❖ Easy to automatic
- ❖ works for both open and close source
- ❖ Spike, iExploder, RIOT, Smudge, peach.. etc.



Fuzzing (continued)

How to design your own fuzzer

- ✦ Based on your experiences
- ✦ Learn the other fuzzer, such as Spike
- ✦ Don't rely on the other's pub fuzzer
- ✦ Need a sniffer



Fuzzing (continued)

why you need a sniffer ?

- ❖ maybe your fuzzer is wrong.use sniffer to check it first
- ❖ Even a litttttttttle error in your fuzzer maybe miss a (lot) world shocking bugz
- ❖ Ethereal

<http://www.ethereal.org>



Fuzzing (continued)

Some tips

- ❖ Fuzzer design is very time consuming
- ❖ Tune @ different target
- ❖ Need to attach a debugger
- ❖ Even though no "Access Exception", no new logs in "Event LOG", there is also maybe some surprise!



Fuzzing (continued)

Some tips

- ❖ need to run a sniffer, sometimes the server will return some surprising packet!
e.g. sometimes IIS will return lots of “undefinedundefinedundefinedundefined”
- ❖ Rather kill one thousand wrongly than miss one
- ❖ DONT ONLY focus on FTPD,HTTPD,SMTPD



Lame 0day Demo1

BNBT Remote D.O.S

client.cpp

```
// grab headers

string :: size_type iNewLine = m_strReceiveBuf.find( "\r\n" );
string :: size_type iDoubleNewLine = m_strReceiveBuf.find( "\r\n\r\n" );

strTemp = m_strReceiveBuf.substr( iNewLine + strlen( "\r\n" ), iDoubleNewLine - iNewLine - strlen( "\r\n" ) );

while( 1 )
{
    string :: size_type iSplit = strTemp.find( ":" );
    string :: size_type iEnd = strTemp.find( "\r\n" );

    if( iSplit == string :: npos )
    {
        UTIL_LogPrint( "client warning - malformed HTTP request (bad header)\n" );

        break;
    }

    string strKey = strTemp.substr( 0, iSplit );
    string strValue = strTemp.substr( iSplit + strlen( ": " ), iEnd - iSplit - strlen( "\r\n" ) );
```



Imagination

❖ 'It is not a lack of beauty of life. It is our lack of discovery'

--Auguste Rodin

❖ 'It is not a lack of bug. It is our lack of discovery'

--bug hunters ;)



Imagination (continued)

- ❖ Both of the invention and Vulnerability Research is Creative, the difference is that invention is the Creative Construction AND vulnerability Research is the Creative Destruction
- ❖ **Imagination!**



How can you get 0day

- ✦ Underground Exchange J
(IRC, Private Forum)

- ✦ DIY

- ✦ Black Market

- ✦ VSC

Vulnerability Sharing Club

e.g. Immunity, \$50,000-100,000/Year



How can you get 0day (continued)

e.g.

<i>Description</i>	<i>Single user</i>	<i>Unlimited</i>	<i>Research*</i>
WebSphere 5.0 Remote (no auth)	\$300	\$600	\$1200
Windows 2000 Local (MS05-018)	\$200	\$400	\$800
0day - Windows 2000 Local	\$350	\$700	\$1400
0day - Oracle 10g Remote DOS (no auth)	\$300	\$600	\$1200
0day - Oracle 9i Remote DOS (no auth)	\$300	\$600	\$1200

◆ From argess.com

◆ Commercial tools,
CANVAS, Core Impact(?),....and so on



How can you get public “0day” Vulnerabilities

Vulnerability Database

- ❖ Securityfocus (Symantec) , ISS X-FORCE database, OVSDB, NSFOCUS (the best public vulnerability database in CHINA)
- ❖ Secunia, SecurityTracker, Securiteam
- ❖ Unique referential between these bases: CVE (Common Vulnerabilities and Exposure)



How can you get publiced “0day” (1day) exploit

✦ Frsirt (K-otik.com)

<http://www.frsirt.com/english/>

✦ Packetstorm

<http://www.packetstormsecurity.org/>

✦ Milw0rm

<http://www.milw0rm.com/>



How many 0days in the wild

- ❖ Every complex software maybe have bugz
- ❖ We should assume that every popular software (OS, third-party applications) exist at least 1 remote 0day exploit in wild !
- ❖ Every professional may hold their own zero day!!



Know 0days in the wild

Known 0days listed by :

- ❖ VULNDISCO Pack

<http://www.gleg.net/download/VULNDISCO.pdf>

About 24 0days including 14 D.O.S

- ❖ UBC (UNRELEASED BUG CLUB)

<http://felinemenace.org/~nd/UBC.html>

6 0days listed, including 3 D.O.S

- ❖ Argeniss.com

<http://argeniss.com/products.html>

6 0days including 2 D.O.S



Defend against 0day

❖ Zero Day Protection

Does Zero Day Protection really exist?

❖ So ,what should You do to defend against 0day attack ? IDS?IPS?
Heuristic security software ?

❖ What about the 0day in IDS itself? ;)



Defend against 0day (continued)

Tips

- ❖ Third Party Assessment.

Very useful and important for Vendor and Enterprise User

- ❖ Firewall doesn't work against Client side 0day

- ❖ Assume at least 1 0day in the wild while deploying your network

- ❖ The least privilege

XP SP2, 2k3 SP1 / GRSecurity



Disclosure policy

- ❖ Full disclosure (ppl often send a copy to FD when pub it on bugtraq)
- ❖ Responsible disclosure (eEye? and?)
<http://www.eeye.com/html/research/upcoming/index.html>
- ❖ Partial Disclosure (NGS?and ?)
- ❖ VSC (immunity, idefense, and?)



0day research related laws

❖ Vulnerability Disclosure

❖ Reverse Engineering

❖ Case1: Sybase to NGSS: Stay Quiet or We'll Sue (March.2005)

<http://www.securityfocus.com/news/10821>

<http://www.securityfocus.com/news/10827>

<http://www.eweek.com/article2/0,1759,1778456,00.asp>



0day research related laws (continued)

Case2: France Makes Finding Security Bugs Illegal
(March.2005)

http://news.com.com/2100-7350_3-5606306.html

Case3: Mike Lynn VS Cisco & ISS (@blackhat July
2005)

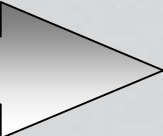
http://www.schneier.com/blog/archives/2005/08/more_lyncisco.html

<http://www.granick.com/blog/>

❖ Jennifer Stisa Granick. @ blackhat
btw: She is Lynn's attorney J



Talking about 0day

- ❖ 0day 6w
- ❖ How to Find 0day
- ❖ How to Get 0day
- ❖ Defend Against 0day
- ❖ 0day related Laws
- ❖ **The Future** 
- ❖ The Vulnerability Research trend
- ❖ The Researcher
- ❖ The Market



The vulnerability Research Trend

Client

- ❖ IE, Firefox, Realplayer...
- ❖ File Format (.rm .gif .doc .ppt .pdf.....)
- ❖ IM. (QQ, MSN, GAIM, Yahoo! MSG)
- ❖ SPIKEfile notSPIKEfile FileFuzz
- ❖ ICBM

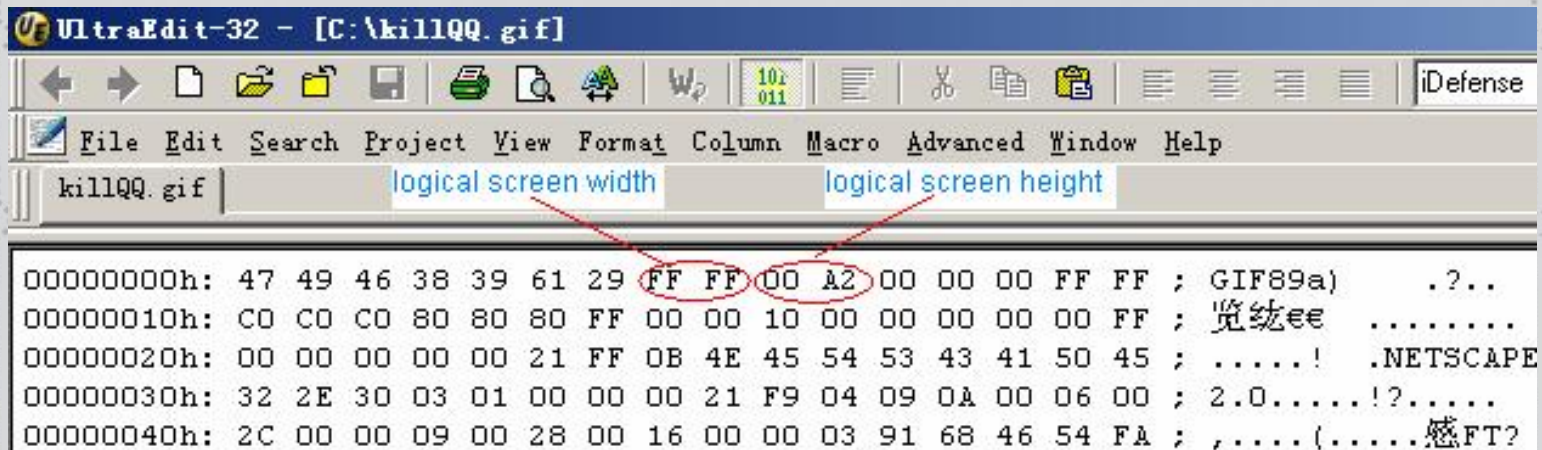
<http://blog.0x557.org/icbm/archives/ArtoffindingCV.pdf>

❖ Flashsky, Liu DieYu



Lame 0day Demo2

Microsoft Windows GIF Weakness Resulting QQ Remote GIF D.O.S



```

UltraEdit-32 - [C:\killQQ.gif]
File Edit Search Project View Format Column Macro Advanced Window Help
killQQ.gif | logical screen width | logical screen height
00000000h: 47 49 46 38 39 61 29 FF FF 00 A2 00 00 00 FF FF ; GIF89a) .?..
00000010h: C0 C0 C0 80 80 80 FF 00 00 10 00 00 00 00 FF ; 览统ee .....
00000020h: 00 00 00 00 00 21 FF 0B 4E 45 54 53 43 41 50 45 ; .....! .NETSCAPE
00000030h: 32 2E 30 03 01 00 00 00 21 F9 04 09 0A 00 06 00 ; 2.0.....!?......
00000040h: 2C 00 00 09 00 28 00 16 00 00 03 91 68 46 54 FA ; ,....(.....感FT?
  
```



Lame 0day Demo3

```
LeapFTP .1sq Buffer Overflow
//bof.1sq
|
[HOSTINFO]
HOST=AAAAA...[ long string ]...AAAAA
USER=aaaaa
PASS=aaaaaaaa

[FILES]
"1","/winis/ApiList.zip","477,839","E:\ApiList.zip"
```



The vulnerability Research Trend(continued)

Enterprise Application ,Security Application

- ❖ Dave Aitel <<Enterprise Secific Software Security Issues>>
- ❖ Example1: Multiple AntiVirus(CA Vet, Mcafee, Trend Micro,F-Secure,Symantec) Library Remote Heap/Stack by Alex Wheeler of the ISS X-Force
- ❖ Example2: Symantec Veritas Backup Exec & CA BrightStor ARCserve Backup



The vulnerability Research Trend (Continued)

COMPUTER-SECURITY SOFTWARE FLAWS			
Company	2005	2004	2003
Symantec	2	16	6
F-Secure	1	10	--
CheckPoint	3	7	1
NetScreen	--	4	1
RSA	--	3	1
BlueCoat Systems	--	3	--
McAfee	2	2	5
Internet Security Systems	--	2	1
Computer Associates	3	2	--
Zone Labs	--	2	--
Sendmail	--	--	5
SurfControl	--	--	4
WatchGuard	--	--	4
Eset Software	2	--	1

Source: Yankee Group



The vulnerability Research Trend(Continued)

TCP/IP

- ❖ Multiple vendor TCP/IP implementations ICMP Source Quench packet denial of service CAN-2004-0791
 - ❖ ICMP Protocol Unreachable CAN-2004-0790
 - ❖ TCP/IP timestamp denial of service CAN-2005-0356
 - ❖ ICMP no fragment low MTU denial of service CAN-2004-1060
 - ❖ Multiple vendor TCP/IP fragmented packet denial of service BID-11258
 - ❖ TCP spoofed reset denial of service CAN-2004-0230
- More and more and more



The Researcher

- ❖ How many vulnerability Researcher In CHINA? IN THE WORLD? how many researchers do pure vulnerability research?
- ❖ Can the researcher learn for their livings only by vulnerability research?
- ❖ iDEFENSE has 200 research contributors in over 30 countries

(according to

http://www.verisign.com/press_releases/pr/page_031054.html)



The Researcher (continued)

Do you think you could make a living at pure vuln-dev research?

❖ "I do think iDEFENSE can pay people full wages to do vulnerability research....."

<https://www.immunitysec.com/pipermail/dailydave/2003-November/000106.html>

❖ "I do think we could pay contributors enough to make it a full-time job for them. "

<https://www.immunitysec.com/pipermail/dailydave/2003-November/000105.html>

POSTED on DailyDave by Sunil James
(Sjames#iDefense.com)



The Market

◆ The Oday market

- ◆ The current Oday business model is weak

- ◆ The auction model (john Blumenthal @dailydave)

 - exploit auctions? eBay è Obay?

 - What's Obay? The benefit?

◆ The stock market

Will the stock market be hit by the publicized Oday?

Case: The Witty Worm, ISS's stock dropped about 5%, to \$15.98, after the worm was announced.



Conclusion

- ✦ There will be more and more 0days
- ✦ 0day attack will be more popular
- ✦ 0day market growing rapidly
- ✦ Defense in depth



Thank You

Questions?

sowhat@secway.org



Reference

- ❖ <https://www.immunitysec.com/pipermail/dailydave/>
- ❖ <http://www.sockpuppet.org/tqbf/log/2005/06/mayb e-im-just-mad-it-doesnt-work-on-my.html>
- ❖ http://www.nsfocus.net/index.php?act=sec_bug
- ❖ <http://www.flashsky.org/>
- ❖ <http://umbrella.name/>
- ❖ http://www.immunitysec.com/downloads/enterprise _specific_security.sxw
- ❖ <http://www.immunitysec.com/downloads/0days.pdf>

