0day漫谈

公安部第三研究所

Sowhat

sowhat@secway.org

概述

- **0day 6问**
- **怎样挖掘 0day**
- 如何获取 **0day**
- 如何防御 **0day**
- **0day** 相关的法律问题
- 展望

什么是0day

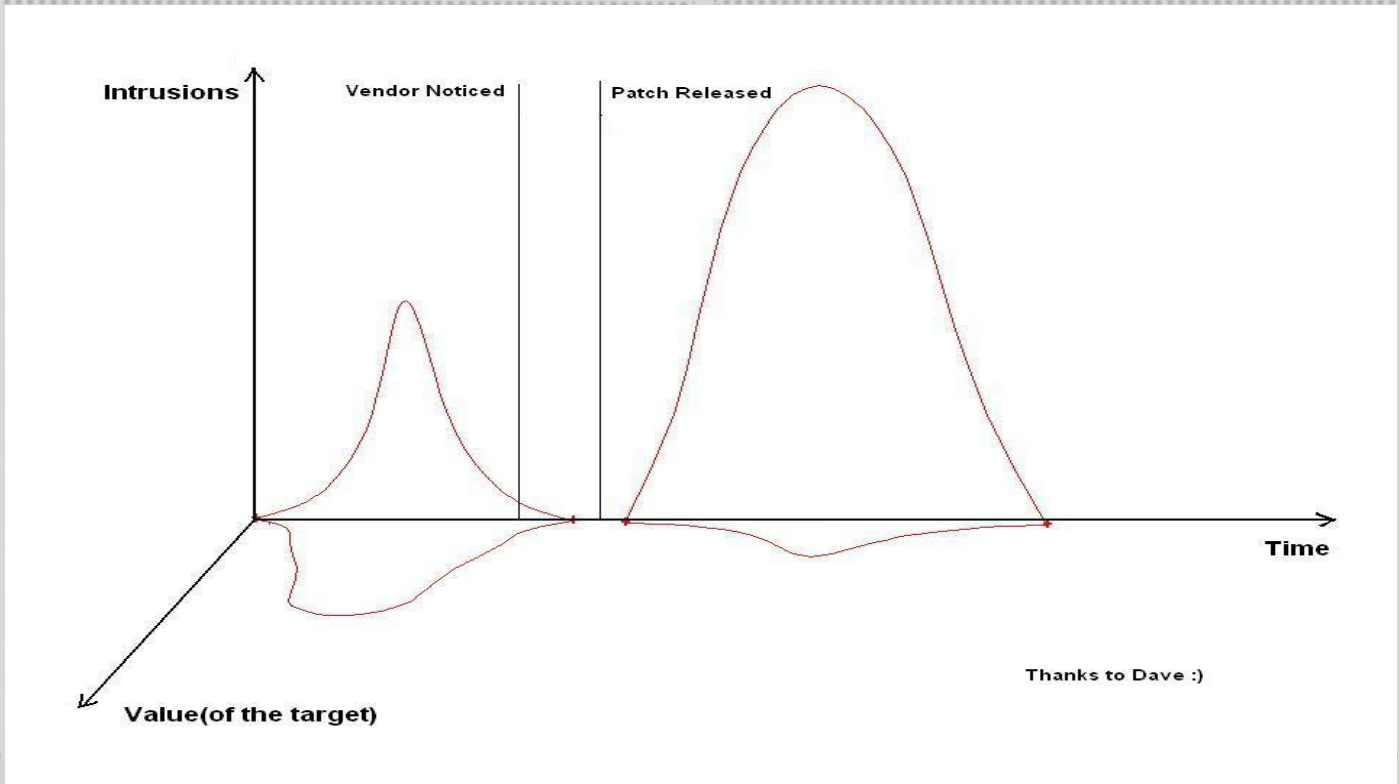
- **0day**是指那些没有公开因而也没有补丁的漏洞。也就是通常所说的"未公开漏洞"
- **0day** 同样也可以分为服务器和客户端
  - 服务器 **:HTTPD,FTPD,IMAPD** 等等
  - 客户端 **:IE, Firefox, Word, Acrobat Reader，WinRAR, Realplayer, Winamp,** 等等

什么是0day (续)

0day 可能会在地下流传很久（数月、数年）

- **Webdav ntdll.dll**
- **CVS Entry Line** 堆溢出 **(CAN-2004-0396)**
- **dtlogin remote root (Dave Aitel 2002-06-06**发现，**2004-03-23**公布 **)**
- 类似的例子数不胜数.....

0day的生命周期


Intrusions
Vendor Noticed
Patch Released
Time
Thanks to Dave :)
Value(of the target)

谁在使用 0day

- 情报机关
- 黑客
- 渗透测试人员
- 甚至蠕虫也可能利用 **0day**

  (W32.Bofra 就利用了IE iframe漏洞)

为什么使用 0day

- 有效

  大多数的公开漏洞都不再有效，尤其当你的目标价值非常高的时候
- 逃避检测 **(IDS)**
- 很酷 **;)**

谁会是目标

- 军队？
- 商业对象
- 网上银行 ....钞票 **J**
- 你 ？ 我？ 任何人！

谁在挖掘 0day

- 安全公司 **(eEye, NGS, ISS,NSFOCUS**，等等**.)**
- 独立的安全研究人员
- 黑客
- **VSC (**漏洞共享俱乐部**)**
- 厂商自己**??** （**Oracle**安全官声称**Oracle 75%**以上的严重安全漏洞都是由他们自己发现的 **:**）

为什么挖掘 0day

- 黑掉系统
- 好玩，追求乐趣
- 拯救世界 ;)
- 修补自己的产品，使其更安全
- 使自己的网络和系统更安全
- 追逐名誉?

0day漫谈

- 0day **6**问
- 怎样挖掘 **0day**
  - 源代码审核
  - 二进制审核
  - **Fuzzing**
  - **Demo1**
- 如何获取 **0day**
- 如何防御 **0day**
- **0day** 相关的法律问题
- **展望**

怎样挖掘 0day

漏洞挖掘并不是什么高科技！

- 源代码审核
- 二进制审核
- **Fuzzing**

源代码审核

- 开源；一些商业公司也开始共享他们源代码
- **FlawFinder, RATS ,ITS4, SPLINT, CodeScan**
- 非常耗时
- 经验很重要
- 只有在有源代码的时候才可行

二进制审核

- 需要很好的汇编功底
- 二进制比较 **(**补丁分析**,Microsoft**黑色星期二**)**
- 也很耗时
- **IDA Pro ,Bindiff, SmartRisk**
- **Halvar Flake, Funnywei**

Fuzzing

- 有效 (至少从我的经验来看)
- 易于自动化
- 无论测试对象是否开源都适用
- **Spike, iExploder, RIOT, Smudge, peach…**

Fuzzing (续)

怎样设计你自己的 **fuzzer**

- 基于你的经验
- 学习其它优秀的 **fuzzer,** 比如 **Spike**
- 不要过度的依赖于其它公开的**fuzzer**
- 需要一个好的 **sniffer**

Fuzzing (续)

为什么需要 **sniffer ?**

- 很可能你的**fuzzer**本身设计上存在很大的缺陷，先用**sniffer**抓包检查纠错。
- **Fuzzer**中即使是一个很小的错误都可能让你错过一个（很多个）惊天大漏洞
- 强烈推荐**Ethereal**

  http://www.ethereal.org

Fuzzing (续)

点滴经验

- **Fuzzer** 设计非常耗时
- 针对不同的目标要作一些微调
- 需要运行一个**debugger**
- 即使没有观察到“**Access Exception**”,而且日志中也没有新的记录，仍有可能有其它的惊喜

Fuzzing (续)

点滴经验

- 在**fuzz**的过程中有时仍需要运行**sniffer,** 因为服务器有时候会返回一些意想不到的信息**!**

  比如在某些情况下**IIS**会返回大量的**"undefinedundefinedundefinedundefined"**
- 宁可错杀一千，绝不放过一个
- 不要光盯着 **FTPD,HTTPD**和**SMTPD**

Demo1

- 鸡肋**0dav1 --BNBT**服务器远程拒绝服务

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" ) );
```

想象力

- "生活中并不缺少美，而是缺少发现"

  --奥古斯特·罗丹

- "并不是缺少**bug**，而是缺少发现"

  --bug hunters ;)

- 发明和漏洞研究都是创造性地，区别在于发明是"创造性地建设"，而漏洞研究则更多的是"创造性地破坏"

- **想象力！**

如何获取 0day

- 地下交换 **J (IRC,**非公开论坛**)**
- 自己动手，丰衣足食。我挖，我挖，我挖挖挖
- 黑市
- **VSC**

  漏洞共享俱乐部

  比如 **Immunity,$50,000-100,000/**年

如何获取 0day (续)

比如下图是某公司在其网站上明码标价的漏洞

Description	Single user	Unlimited	Research*
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**

- 购买商业渗透工具

  CANVAS, Core Impact(?),....等等

怎样获取已经公开的“0day”信息

漏洞库

- **Securityfocus (Symantec)，ISS X-FORCE database, OVSDB,NSFOCUS (最好的中文漏洞库之一)**
- **Secunia, SecurityTracker, Securiteam**
- **CVE (Common Vulnerabilities and Exposure，通用漏洞披露)**

如何获取已公开的 “0day” (1day) exploit

- **Frsirt (K-otik.com)**
  http://www.frsirt.com/english/
- **Packetstorm**
  http://www.packetstormsecurity.org/
- **Milw0rm**
  http://www.milw0rm.com/

有多少个0day在流传

- 每一个复杂的软件都很有可能存在**0day**
- 我们可以假设每一款流行软件**(**操作系统，第三方软件**)** 都至少有一个远程**0day**在流传
- 每一位漏洞研究者都藏有自己的**0day**!

已知的0day

已知的列出名称的**0day**：

- **VULNDISCO Pack**

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

  大约**24**个**0day** 其中包括 **14**个 **D.O.S**

- **UBC (UNRELEASED BUG CLUB)**

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

  列出了**6**个 **0days**， 其中包括 **3** 个**D.O.S**

- **Argeniss.com**

  http://argeniss.com/products.html

  列出了**6**个 **0days**， 其中包括**2**个 **D.O.S**

防御 0day

- **0Day 防护**

  0Day 防护真的存在吗？
- 那我们该如何抵御**0day**攻击呢？ **IDS**？ **IPS**？ 启发式安全软件 ？
- 如果**IDS**本身存在**0day**呢？ **;)**

防御 0day (续)

点滴

- 第三方评估

  对厂商和大型的企业用户来说尤为重要
- 防火墙对于客户端的**0day**基本上无能为力
- 在部署你的网络时应假设至少有一个**0day**在流传，或者被你的竞争对手所掌握
- 最小权限
- **XP SP2, 2k3 SP1 / GRSecurity**

披露策略

- 全面披露 **(bugtraq,FD)**
- 负责的披露 **(eEye？ And？)**

  http://www.eeye.com/html/research/upcoming/index.html
- 部分披露 **(NGS？and ？)**
- 漏洞共享俱乐部

  (immunity，idefense，3com ， and?)

0day研究的相关法律

- 漏洞披露
- 逆向工程
- **例1: Sybase to NGSS:** 闭嘴，否则我们会起诉 **(2005年3月)**
  http://www.securityfocus.com/news/10821
  http://www.securityfocus.com/news/10827
  http://www.eweek.com/article2/0,1759,1778456,00.asp

0day研究的相关法律(续)

例2:在法国，漏洞挖掘者被认为是非法的 (2005年3月)

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

例3: Mike Lynn VS Cisco && ISS (@blackhat 2005年7月)

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

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

- Jennifer Stisa Granick. @ blackhat

btw:她是 Lynn的律师

0day漫谈

- **0day 6问**
- **怎样挖掘 0day**
- 如何获取 **0day**
- 如何防御 **0day**
- **0day** 相关的法律问题
- **0day**未来展望
  - 漏洞研究趋势
  - 漏洞研究人员
  - **0day**市场

0day未来展望

- 漏洞研究趋势
- 漏洞研究人员
- **0day**市场

漏洞研究趋势

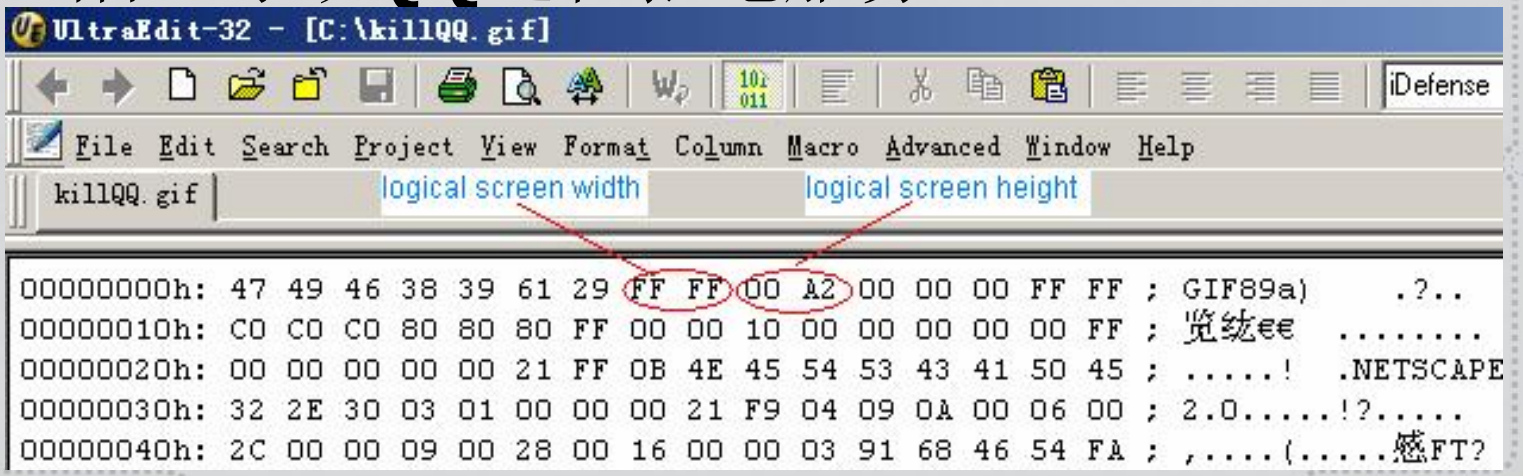
客户端

- **IE, Firefox, Realplayer…**
- 文件格式 **(.rm .gif .doc .ppt .pdf…..)**
- 即时通讯软件 **(QQ,MSN,GAIM, Yahoo!)**
- **SPIKEfile， notSPIKEfile， FileFuzz**
- **ICBM** 《寻找客户端漏洞的艺术》
- **Flashsky, Liu DieYu**

Demo2

- 鸡肋**0day2**

  Microsoft Windows处理**GIF**文件时的缺陷，导致**QQ**远程拒绝服务



Demo3

- 鸡肋 **0day3**

  LeapFTP .lsq缓冲区溢出漏洞

```
LeapFTP .lsq Buffer Overflow
//bof.lsq

[HOSTINFO]
HOST=AAAAA...[ long string ]...AAAAA
USER=aaaaa
PASS=aaaaaaa

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

漏洞研究趋势(续)

企业软件，安全软件

- **Dave Aitel <<Enterprise Secific Software Security Issues>>**
- 例**1:** 多个杀毒软件**(CA Vet, Mcafee, Trend Micro, F-Secure, Symantec, Sophos)** 库远程堆栈溢出

  by Alex Wheeler ISS X-Force
- 例**2: Symantec Veritas Backup Exec & CA BrightStor ARCserve Backup**

漏洞研究趋势(续)

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

漏洞研究趋势(续)

TCP / IP

- 多家厂商**TCP/IP**协议栈实现**ICMP**拒绝服务漏洞 **CAN-2004-0791**
- **ICMP** 协议不可达拒绝服务漏洞 **CAN-2004-0790**
- 多家厂商的**TCP/IP**协议栈实现时间戳**PAWS**远程拒绝服务漏洞 **CAN-2005-0356**
- **ICMP PMTUD**拒绝服务漏洞 **CAN-2004-1060**
- 多家厂商分片包拒绝服务漏洞 **BID-11258**
- **TCP** 欺骗连接重置拒绝服务漏洞 **CAN-2004-0230**

More and more and more .....

漏洞研究人员

- 中国大概有多少漏洞研究人员？全世界呢？
- 多少人在做纯漏洞研究？
- 漏洞研究者能靠纯漏洞挖掘来养活自己吗？
- **iDEFENSE** 在全球**30**多个国家有超过**200**个 **contributor**

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

漏洞研究人员(续)

你认为你能够靠纯漏洞研究来养活自己吗?

- **"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

Sunil James发表于 DailyDave (sjames#iDefense.com)

0day市场

- **0day**市场
  - 目前的**0day**市场商业模式非常脆弱，不健全
  - 拍卖模式 **(john Blumenthal @ dailydave)**

    exploit 拍卖**? eBay è 0bay?**

    什么是**0bay?** 有什么好处**?**
- 股市

  股市会受到**0day**的影响吗？

例**:** 在**Witty**蠕虫被放出以后，**ISS**公司的股票下跌了**5%**

结论

- 会有越来越多的**0day**
- **0day**攻击会越来越流行
- **0day**市场会迅速成长
- 深度防御

谢谢

Questions?

sowhat@secway.org

Reference

- https://www.immunitysec.com/pipermail/dailydave/
- http://www.sockpuppet.org/tqbf/log/2005/06/maybe-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