Trend Micro
Research Paper
2012

LUCKYCAT REDUX

Inside an APT Campaign with Multiple Targets in India and Japan

By: Forward-Looking Threat Research Team

CONTENTS

INTRODUCTION

The number of targeted attacks has dramatically increased. Unlike largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime, targeted attacks noticeably differ and are better characterized as "cyber espionage." Highly targeted attacks are computer intrusions threat actors stage in order to aggressively pursue and compromise specific targets, often leveraging social engineering, in order to maintain persistent presence within the victim's network so they can move laterally and extract sensitive information.[1]

In a typical targeted attack, a target receives a contextually relevant email that encourages a potential victim to click a link or open a file.[2] The links and files the attackers send contain malicious code that exploits vulnerabilities in popular software. The exploits' payload is a malware that is silently executed on the target's computer. This exploitation allows the attackers to take control of and obtain data from the compromised computer. In other cases, the attackers send disguised executable files, usually compressed in archives that, if opened, also compromise the target's computer. The malware connects back to command-and-control (C&C) servers under the attackers' control from which they can command the compromised computer to download additional malware and tools that allow them to move laterally throughout the target's network. These attacks are, however, not isolated "smash-and-grab" incidents but are part of consistent campaigns that aim to establish covert presence in a target's network so that information can be extracted as needed.

Targeted attacks are rarely isolated events. In fact, they are constant. It is more useful to think of them as campaigns—a series of failed and successful attempts to compromise a target's network over a certain period of time. The attackers, in fact, often keep track of the different attacks within a campaign in order to determine which individual attack compromised a specific victim's network. As the attackers learn more about their targets from open source research—relying on publicly available information, as well as previous attacks, the specificity of the attacks may sharply increase.

Cyber-espionage campaigns often focus on specific industries or communities of interest in addition to a geographic focus. Different positions of visibility often yield additional sets of targets pursued by the same threat actors. We have been tracking the campaign dubbed "Luckycat" and found that in addition to targeting Indian military research institutions, as previously revealed by Symantec, the same campaign targeted entities in Japan as well as the Tibetan community.[3]

The Luckycat campaign targeted the following industries and/or communities:

- Aerospace
- Energy
- Engineering
- Shipping
- Military research
- Tibetan activists

The Luckycat campaign attacked a diverse set of targets using a variety of malware, some of which have been linked to other cyber-espionage campaigns. The attackers behind this campaign maintain a diverse set of C&C infrastructure and leverages anonymity tools to obfuscate their operations. We were able to track elements of this campaign to hackers based in China.

Diversity of Targets

The Luckycat campaign, which has been active since at least June 2011, has been linked to 90 attacks against targets in Japan and India as well as Tibetan activists. Each malware attack involves a unique campaign code that can be used to track which victims were compromised by which malware attack. This illustrates that the attackers are both very aggressive and continually target their intended victims. These are not smash-and-grab attacks but constitute a "campaign" comprising a series of ongoing attacks over time. In sum, the Luckycat campaign managed to compromise 233 computers.[4]

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf

2 Targeted attacks can sometimes be conducted through instant messages instead of emails.

3 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_luckycat_hackers.pdf

4 This number represents the unique MAC addresses of the victims that were stored by the attackers on their C&C infrastructure.

Diversity of Malware

We were able to identify five malware families either utilized by or hosted on the same dedicated server the Luckycat campaign uses. Some were used as second-stage malware that the attackers pushed to victims whose networks were compromised by first-stage malware. Second-stage malware typically provide additional functionality and are especially used if the first-stage malware prove very simplistic. In addition, we found that the attackers used multiple malware families that coincide with malware that have been used in other campaigns. This indicates a level of collaboration across campaigns.

Diversity of Infrastructure

The Luckycat campaign use free web-hosting services that provide a diversity of domain names as well as IP addresses. This distributes the campaign, making it more difficult to track. However, the attackers also made use of Virtual Private Servers (VPSs) that not only housed their primary malware—TROJ_WIMMIE, but others as well.[5] These servers may also act as anchors, as servers on free hosting services are shut down for malicious activity. As a result, the campaign stabilized its infrastructure over time, transferring victims, often through the use of second-stage malware, from free hosting servers to their stable core of VPSs.

Operations

TROJ_WIMMIE, favored by the Luckycat attackers, bundles a significant amount of information on the victim and uploads it to a C&C server. One such file recovered from a C&C server is actually the result of a test run by the attackers. The information reveals that the attackers use proxy and anonymity tools to shield their identities as well as a variety of mailing programs to instigate targeted attacks. In addition, the language settings of the attackers' computers indicate that they are Chinese speakers. This is consistent with the information Symantec obtained, which shows that the attackers logged in to their C&C server from IP addresses allocated to China.

Attribution

Using open source research, we were able to connect the email address used to register one of the Luckycat C&C servers to a hacker in the Chinese underground community. He uses the nickname, "dang0102," and has published posts in the famous hacker forum, *XFocus,* as well as recruited others to join a research project on network attack and defense at the Information Security Institute of the Sichuan University. The hacker, also known as "scuhkr," has authored articles related to backdoors and shellcode in a hacking magazine.

5 VPSs are dedicated hosting services that can be purchased online.

LUCKYCAT

The malware used in the Luckycat campaign, detected by Trend Micro as TROJ_WIMMIE[6] or VBS_WIMMIE,[7] connects to a C&C server via HTTP over port 80. It is notable because it uses *Windows Management Instrumentation (WMI)*[8] to establish persistence.[9] VBS_WIMMIE registers a script that works as a backdoor to the *WMI* event handler and deletes files associated with it or TROJ_WIMMIE. As a result, the backdoor cannot be detected by antivirus software through simple file scanning.

The compromised computer posts data to a PHP script that runs on the C&C server, usually *count.php*.

```
POST/count/count.php?m=c&n=[HOSTNAME]_
[MAC_ADDRESS]_[CAMPAIGN_CODE]@HTTP/1.0
Accept: */*
UA-CPU: x86
User-Agent: Mozilla/4.0 (compatible; MSIE
7.0; Windows NT 5.1; .NET CLR 2.0.50727;
.NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)
Host: [HOSTNAME]
Content-Length: 0
Connection: Keep-Alive
Pragma: no-cache
```

The initial communication results in the creation of a file on the C&C server that contains information on the compromised computer. Although the file is empty, the file name contains the hostname of the compromised computer, followed by its MAC address, along with the campaign code the attackers use to identify which malware attack caused the compromise:

```
~[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]
```

The attacker then creates a file with a name that ends in *@.c*, which contains a command.

```
[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_
CODE]@.c
```

The compromised computer then downloads the file and executes the specified command, which may include any of the following:

- Download file
- Upload file
- Get external IP address
- Execute shell command

The compromised computer then sends the output to the C&C server and deletes the command file:

```
POST/count/count.php?m=w&n=[HOST_NAME]_
[MAC_ADDRESS]_[CAMPAIGN_CODE]@@.t HTTP/1.0
POST/count/count.php?m=d&n=[HOST_NAME]_
[MAC_ADDRESS]_[CAMPAIGN_CODE]@@.c HTTP/1.0
```

One of the common initial commands instructs the compromised computer to upload the results of information-gathering commands. This command causes the compromised computer to create a directory listing of the available drives, along with the output of the commands, "ipconfig," "tasklist," and "systeminfo." The resulting files are compressed using the CAB compression format and uploaded to the C&C server. This provides the attackers a full set of information to evaluate the nature of the compromised computer.

6 http://about-threats.trendmicro.com/Malware.aspx?language=us&name=TROJ_WIMMIE.C
7 http://about-threats.trendmicro.com/malware.aspx?language=us&name=VBS_WIMMIE.C
8 The Luckycat malware may be notable but its technique is no longer new, as the *WMI* malware featured in the paper cited below also exhibited the same capability.
9 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp__understanding-wmi-malware.pdf

Examples of Luckycat Attacks

Example 1: Japan

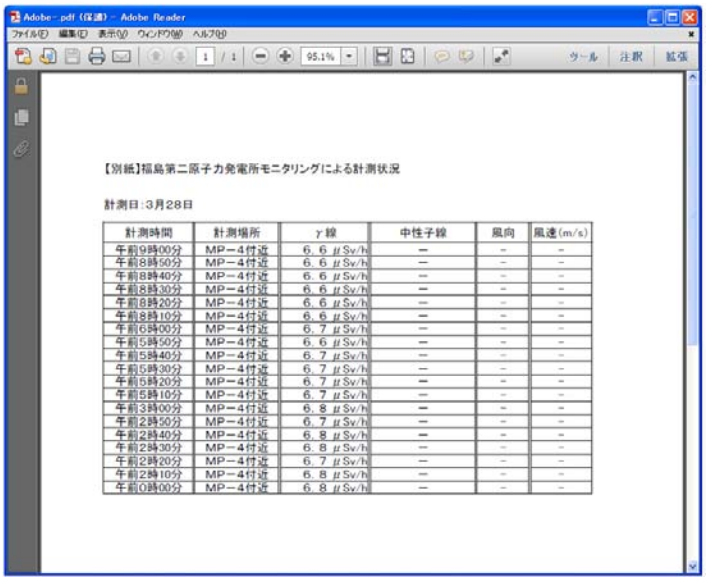


Figure 1: Decoy document opened after exploiting an Adobe Reader *vulnerability*

A targeted email was sent to some organizations in Japan. One of the attacks occurred during the confusion after the Great East Japan Earthquake and the Fukushima Nuclear Power Plant accident. The attackers used the disaster to lure potential victims into opening a malicious .PDF attachment. The .PDF file exploited a vulnerability in *Adobe Reader—CVE-2010-2883*, in order to drop TROJ_WIMMIE onto the target's system.[10] This malware communicated with a Luckycat C&C server. The decoy document contains the radiation dose measurement results, which were published on the Tokyo Power Electric Company (TEPCO) website.[11]

Example 2: India

Figure 2: Redacted decoy document opened after exploiting a Microsoft Word *vulnerability*

A malicious document containing information on India's ballistic missile defense program was used to lure potential victims into opening it. This document contains malicious code that exploits a vulnerability in *Microsoft Office—CVE-2010-3333*, to drop TROJ_WIMMIE onto a compromised system so this would connect to a C&C server the Luckycat hackers operate.[12]

10 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2883
11 http://www.tepco.co.jp/nu/monitoring/11032805.pdf
12 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333

Example 3: Tibet

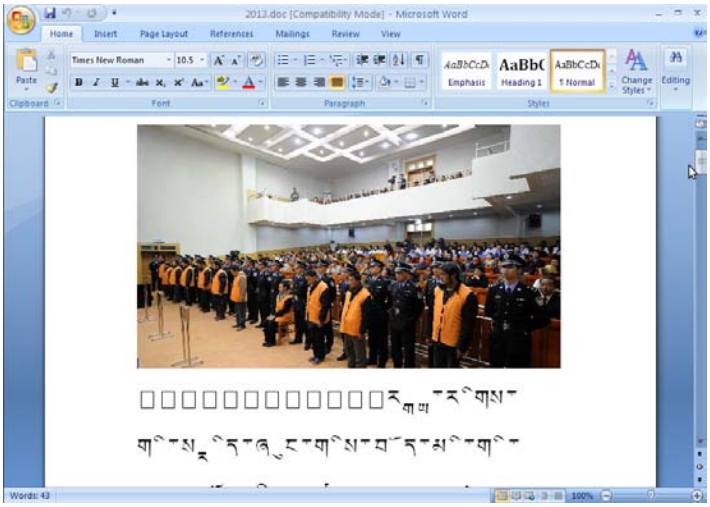


Figure 3: Decoy document opened after exploiting a Microsoft Office *vulnerability*

Malicious emails and .DOC attachments that leverage Tibetan themes in order to trick recipients into opening them have been found. This particular sample exploits the same vulnerability in *Microsoft Office—CVE-2010-3333*, to drop TROJ_WIMMIE onto the target's system so it would communicate back to a C&C server the Luckycat hackers operate.

VULNERABILITIES AND MALWARE SAMPLES

Most of the samples we have seen exploited *CVE-2010-3333*. Dubbed the "Rich Text Format (RTF) Stack Buffer Overflow Vulnerability," this causes a buffer overflow in the *Microsoft Word* RTF parser when the "pFragments" shape property is given a malformed value.

To verify the exploitation, one should look out for the following keywords:

- **pFragments:** Seen after the string, "\sn"
- **\sv:** Exploit code is seen after this

The typical structure of the malicious RTF document is:

```
{\rtf1{\shp{\sp{\sn pFragments}{\sv
"exploit code"}}}}
```

The rest of the samples we found exploited the following vulnerabilities in *Adobe Reader* and *Flash Player:*

- ***CVE-2010-2883:*** *Adobe Reader* TTF SING table parsing vulnerability
- ***CVE-2010-3654:*** *Adobe Flash Player* AVM2 multi-name button class vulnerability[13]
- ***CVE-2011-0611:*** *Adobe Flash Player* AVM1 shared object type vulnerability[14]
- ***CVE-2011-2462:*** *Adobe Reader* U3D component vulnerability[15]

13 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3654
14 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611
15 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462

MD5	CVE Identifier	Campaign Code
dab3f591b37f5147ae92570323b5c47d	*CVE-2010-3333*	w1229
c023544af85edacc66cd577a0d665dec	*CVE-2010-3333*	w1229
cff0964ed2df5659b0a563f32b7c3eca	*CVE-2010-3333*	214
3deb2a5fcb6bf1f80a074fd351e6f620	*CVE-2010-3333*	2012
1aa1e795a5ba75f2a5862c6d01205b57	*CVE-2010-2883* *CVE-2010-3654* *CVE-2011-0611*	110824p
6a62d4532c7a0656381fee8fb51874d7	*CVE-2010-2883* *CVE-2010-3654* *CVE-2011-0611*	longjiao
cb9ab22f3356a3b054a7e9282a69f71e	*CVE-2011-2462*	gop
1dafdc9e507771d0d8887348ce3f1c52	*CVE-2010-3333*	gop
039a6e012f33495a1308b815ef098459	*CVE-2010-3333*	luck
be0b2e7a53b1dcacb8c54c180dc4ca27	*CVE-2010-2883* *CVE-2010-3654* *CVE-2011-0611*	11727p
00f07b0e701dcfa49e1c907f9242d028	*CVE-2010-2883* *CVE-2010-3654* *CVE-2011-0611*	110705hktq
411ab5eb2ef3153b61a49964f9ab4e64	*CVE-2011-2462*	1229
dcac508495d9800e476aa0c8e11b748d	*CVE-2010-3333*	2012
00e686e382806c33d9ae77256f33ed93	Not applicable	LY

Table 1: Luckycat malware samples sorted by exploit and campaign code

CAMPAIGN CODES

Each malware attack involves a unique campaign code that can be used to track which systems were compromised by which attack. The campaign codes often contain dates that indicate when each malware attack was launched. This demonstrates how actively and frequently the attackers launched attacks. The campaign codes also reveal the attackers' intent, as some of these referenced the intended targets. The following lists the campaign codes we discovered:

- 0607e
- 0609af
- 0613deliinfo
- 0613f
- 0614senior
- 0616itiT8
- 0706■■■■
- 0804■■■■datanet1
- 0805■■■■etp
- 0805■■■■stp
- 0805ecil
- 0805■■■■
- 0818ICG
- 0823■■■■ARDE
- 0824■■■
- 0826■■■■tnd
- 1017navydiwali
- 1017■■■
- 1025■■■CSC
- 1025■■■SC
- 1090silver89
- 110228cl
- 110311cl
- 110315cl
- 110315
- 110321cl
- 110329
- 110504
- 110603p89
- 110606rg789
- 110616np
- 110705hktq
- 110706■■■■
- 110706hal
- 110705hktq
- 110708hktqw
- 110711■■■■
- 110711hal
- 110711xzg
- 110713jp
- 110714jdap
- 110714tp
- 110715x
- 110718p
- 110816h
- 110824p
- 1108navyeast
- 1108vpsecretary
- 111031pp
- 1110mea
- 1114round
- 1122bol
- 1122gmail
- 1122other
- 11421is9
- 1145j9yb
- 1147s9
- 1148dq8
- 11614lmpn
- 11725imp
- 11727p
- 1229
- 2012
- 214
- 28
- 64sc109pfye
- 64sc239pf9010
- 720halheli
- 729■■■■senior
- 919■■■■stp
- ■■■■stpdomainserver
- dang279wrdye
- god
- gop
- ishan99dfp
- j1141ap99
- j4611dq9
- kondulgml27pfye
- longjiao
- luck
- LY
- nec3rd79dfp
- nfounrsvan99uc
- nne
- ongs239pfye
- sai
- stmlsp211wd
- w1229
- wwwroot
- zz1227

COMMAND AND CONTROL

The Luckycat campaign extensively use free hosting services. We recorded the domains the attackers used as well as the email addresses they utilized to register the domains, if available. While the domains, including their suffixes, were considerably diverse, all were available from three different free hosting services. As such, the attackers had nothing to lose but time in order to continue creating diverse domain names for C&C servers.

Domain	Email Address
cattree.1x.biz	*lindagreen56@rediffmail.com*
charlesbrain.shop.co	*yamagami_2011@mail.goo.ne.jp*
footballworldcup.website.org	*ajayalpna@hotmail.com*
frankwhales.shop.co	*yamagami_2011@mail.goo.ne.jp*
hi21222325.x.gg	*hi2122325@hotmail.com*
kinkeechow.shop.co	*kinkee_chow@mail.goo.ne.jp*
kittyshop.kilu.org	*pbdelhioffice@gmail.com*
perfect.shop.co	*dsang72@yahoo.com*
pumasports.website.org	*ranjitrai123@hotmail.com*
tomsburs.shop.co	*yamagami_2011@mail.goo.ne.jp*
vpoasport.shopping2000.com	*beenznair@gmail.com*
goodwell.all.co.uk	*paltry.parrot@googlemail.com*
fireequipment.website.org	*shrivastava.agrim@gmail.com*
tennissport.website.org	*manindramohanshukla@yahoo.com*
waterpool.website.org	*jaganacharya@hotmail.com*
tb123.xoomsite.com	
tbda123.gwchost.com	
toms.0fees.net	
tomygreen.0fees.net	
killmannets.0fees.net	
maritimemaster.kilu.org	
masterchoice.shop.co	
jeepvihecle.shop.co	
lucysmith.0fees.net	

Table 2: Free web-hosting service domains the attackers used for C&C servers

The attackers also maintain servers that do not appear to be from free web-hosting service providers. In fact, these appear to use dedicated VPS services.

Domain	Email Address
clbest.greenglassint.net	*19013788@qq.com*
bailianlan.c.dwyu.com	*dayinok@qq.com*
duojee.info	*duojeewei@qq.com*

Table 3: C&C servers that the attackers hosted on VPSs

We also found advertisements for VPS services using two of the C&C server IP addresses in Table 3. While the VPS services were advertised in Chinese forums, the servers were actually hosted in the United States.

Figure 4: Sample ads for the VPS services the attackers use

The diversity of C&C hosting services used provided the attackers a resilient infrastructure. If one server, for instance, was shut down for malicious activity, they can easily create more servers. As victims of interest are identified, they can also be easily moved from free hosting servers to C&C servers set up on more stable VPSs. The domain and geographic diversity of the IP addresses also helped mask the attackers' locations.

OPERATIONS

The threat actors behind the Luckycat campaign tested one of their malware samples on a computer under their control. In the process, they uploaded *down.cab*, which contains a command that creates a directory listing of the available drives on a compromised system, along with the output of the commands, "ipconfig," "tasklist," and "systeminfo." We were able to download this file from the C&C server. While it does not reveal the attackers' identities, it does provide an inside view of their operations.

The result of the "systeminfo" command indicates that the attackers tested the malware in a virtual environment. The environment was set up using a Chinese-language version of *Windows XP*.

```
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.
```

Figure 5: Sample system information the attackers obtained after testing on a virtual machine (VM)

We found that the product ID of the *Windows XP* software used was posted online in the past. It was a pirated *Windows XP* version that was made available for purchase in China.

Figure 6: Sample ads for the pirated Windows XP *version used*

While the rest of the information we gathered did not reveal significant clues due to the use of a VM, we found that the attackers left a shared drive—*D:*\, which was indexed by the malware. The index was then uploaded to the C&C server.

```
D:\ccclllmmmm\1 的目录

2012-01-10  15:19    <DIR>          .
2012-01-10  15:19    <DIR>          ..
2011-12-01  08:34             1,209 count.php
2011-12-01  08:34                88 ip.php
               2 个文件          1,297 字节

 D:\ccclllmmmm\HOST 的目录

2012-01-10  15:19    <DIR>          .
2012-01-10  15:19    <DIR>          ..
2012-01-10  15:19    <DIR>          [redacted]B2EF_w1229@
2012-01-10  15:19    <DIR>          [redacted]B6F9_w1229@
2012-01-10  15:19    <DIR>          [redacted]7A2B_w1229@
               0 个文件              0 字节
```

Figure 7: Drive left available by the attackers that contains C&C scripts and victim information

In one of the directories—*cccllllmmmm*, we found that the attackers put a copy of the *count.php* C&C backend as well as a list of the victims and the contents of their computers. We were also able to find that the C&C server the attackers used was a victim's computer.

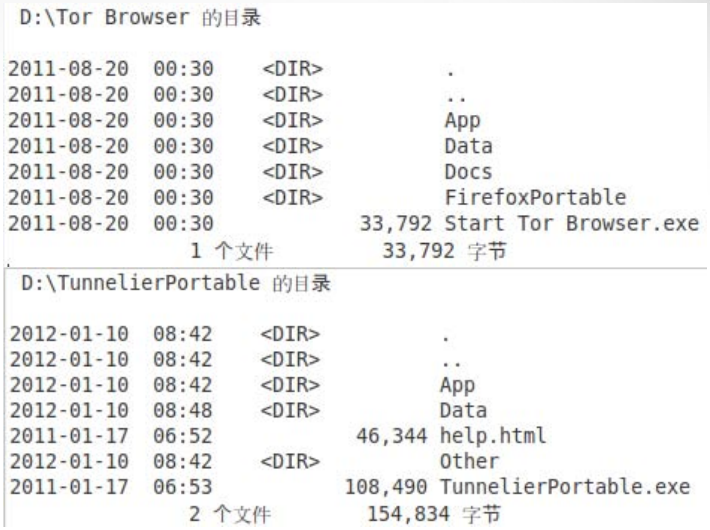
Index of /54321

[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]87A8B_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]03C7B_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]0A0834_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

Figure 8: Victim information on the attackers' C&C server that is identical to the the information on the attackers' shared D:\ *drive*

To ensure operational security, the attackers installed *Tor* and *Tunnelier*. Some of the email samples with malware attachments, in fact, sent through *Yahoo! Mail* used *Tor*. The use of this anonymity tool allowed the attackers to obscure their IP addresses, making it increasingly difficult for researchers to pinpoint their locations.



```
 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
```

Figure 9: Anonymity tools the attackers had on the shared D:\ *drive*

The attackers also had mailing software such as *FoxMail* and *Supermailer* on the shared *D:* drive. While these tools are not malicious, the attackers used these to easily send out socially engineered emails. These also allowed them to keep track of their various identities and email accounts. One of the samples we obtained used the Chinese-language version of *FoxMail*.

The attackers clearly have operational procedures in place to obscure their true locations with the aid of anonymity tools. They also have a virtualized environment set up to test and fine-tune their malware as well as the necessary tools to maintain their various identities and send out socially engineered emails with malicious attachments.

ATTRIBUTION

Additional clues concerning the attackers had to with the email address, *19013788@qq.com*, which was used to register one of the C&C servers, *clbest.greenglassint.net*. This email address can be mapped to the *QQ* number, *19013788*. *QQ* is popular instant-messaging (IM) software in China. This *QQ* number is linked to a hacker in the Chinese underground community who goes by the nickname, "dang0102," and has published posts in the famous hacker forum, *XFocus*, in 2005.

Figure 10: Sample post by dang0102 using the QQ number, 19013788

The same hacker also published a post on a student BBS of the Sichuan University using the nickname, "scuhkr," in 2005. He wanted to recruit 2–4 students to a network attack and defense research project at the Information Security Institute of the Sichuan University then. Scuhkr also authored articles related to backdoors and shellcode in a hacking magazine that same year.[16]


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]

Figure 11: Post by schuhkr using the QQ number, 19013788

The post in Figure 11 contains two email addresses–[redacted]*sccd@sina.com* and *scuhkr@21cn.com*, along with an additional *QQ* number, *2888111*. The email address, *scuhkr@21cn.com*, is also associated with an account on *rootkit.com*.[17] Investigating the second *QQ* number allowed us to determine that scuhkr also used the nickname, "lolibaso." The other individual mentioned in the post also worked and studied at the Information Security Institute of the Sichuan University and has published several articles related to "fuzzing" vulnerabilities in 2006.

16 http://www.cqvip.com/Main/Search.aspx?w=Scuhkr

17 http://dazzlepod.com/rootkit/?page=83

CAMPAIGN CONNECTIONS

We were able to identify five malware families that were either used by or hosted on the same dedicated server with the domain name, *duojee.info*. Some of these were used as second-stage malware that the attackers pushed to victims whose systems have been compromised by first-stage malware. Second-stage malware typically provided additional functionality and were especially used if the first-stage malware is very simplistic. We also found that the attackers used several malware families that have been utilized in previous campaigns. This may indicate a level of collaboration across campaigns.

SHADOWNET

The first interesting connection we noticed in conjunction with the Luckycat campaign had to do with ShadowNet, a cyber-espionage network documented by researchers at the University of Toronto and the ShadowServer Foundation.[18] We found a socially engineered email that had two malicious file attachments.

Figure 12: Sample targeted email with both Luckycat and ShadowNet malware attachments

One of the sample email's attachments was part of the Luckycat campaign while the other was part of the ShadowNet campaign. The ShadowNet campaign has a history of targeting Tibetan activists as well as the Indian government, which fits the profile of the Luckycat campaigns as well.

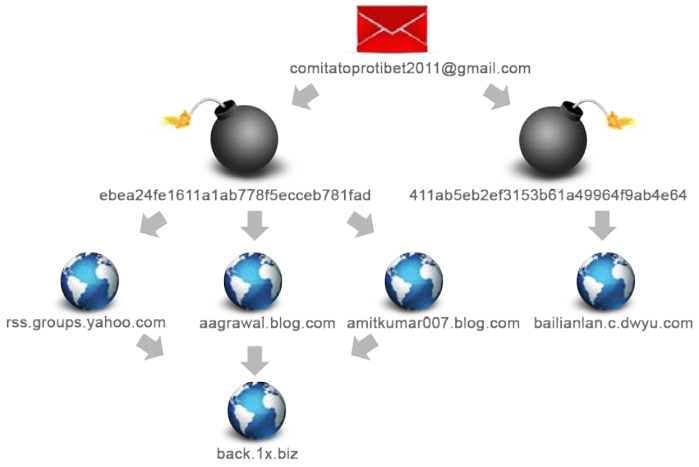


Figure 13: Relationship between the Luckycat and the ShadowNet campaigns

The ShadowNet malware, detected by Trend Micro as TROJ_GUPD.AB, first connects to a blog in order to receive the URL of the C&C server. The URL was encoded using a modulus operation. The malware on the compromised computer decodes the URL then issues a connection to the C&C server. The compromised computer posts data to a PHP script running on the server, usually named *index.php* or *all.php,* and contains information about it as well as a campaign code.

The information is stored in a .TXT file on the C&C server. The compromised computer continues to beacon to the C&C server to see if the operators have designed any commands. If they have, the compromised computer then executes the given commands and reports the results back to the C&C server.

18 http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

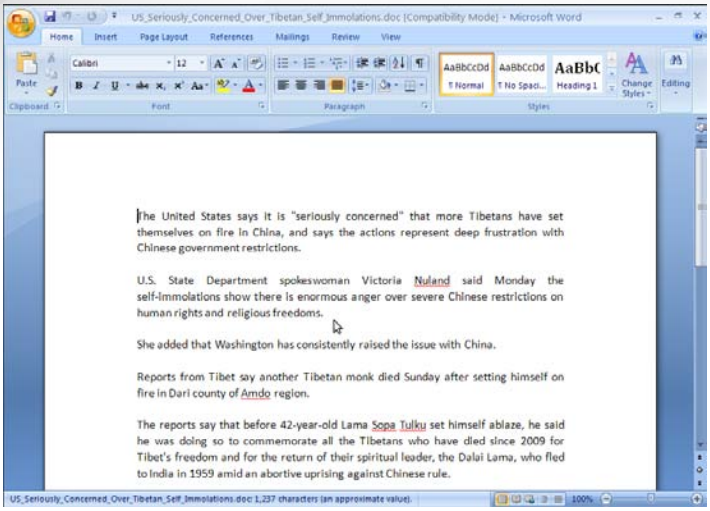


Figure 14: Sample ShadowNet malware related to a Luckycat email attack

This attack used the theme of self-immolation in Tibet for both the email and the decoy document that is opened after the vulnerability exploitation. The malicious file attachment exploits a vulnerability in *Microsoft Office*—*CVE-2010-3333*, to drop malware onto the target's system. The malware was configured to connect to two blogs and a *Yahoo! Group* in order to find the C&C server's location.

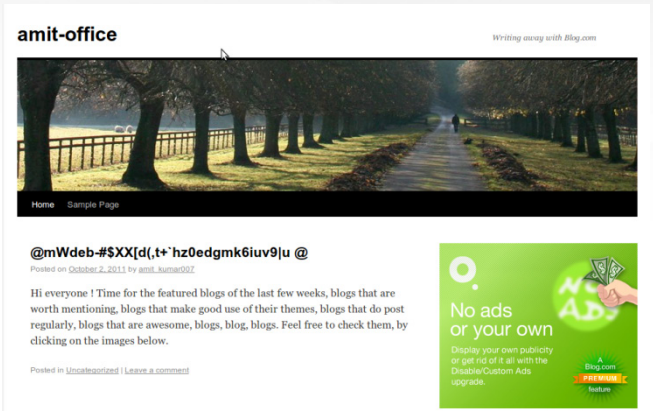


Figure 15: Example of a blog used by ShadowNet to communicate an encoded C&C server location

The blogs and groups the ShadowNet attackers use can be easily updated whenever the C&C servers are changed. The URL of the blog is embedded in the malware. The malware connects to the blog and decodes the C&C URL then connects to the C&C server. The commands the server issues are also encoded using a simple logical operator. The malware also decodes these using keycodes that are sent along with the actual commands.

MD5	CVE Identifier	Campaign Code
26891c3e4a2de034e4841db2a579734f	*CVE-2011-2462*	circle
ebea24fe1611a1ab778f5ecceb781fad	*CVE-2010-3333*	circle

Table 4: ShadowNet malware samples related to the Luckycat campaign

Duojeen

The malware attacks related to the Duojeen campaign all target the Tibetan community and use a single C&C server—*duojee.info*. We also found that a malware binary available for download from *duojee.info* is a TROJ_WIMMIE Trojan that connects back to *bailianlan.c.dwyu.com*—a C&C server the Luckycat attackers use.

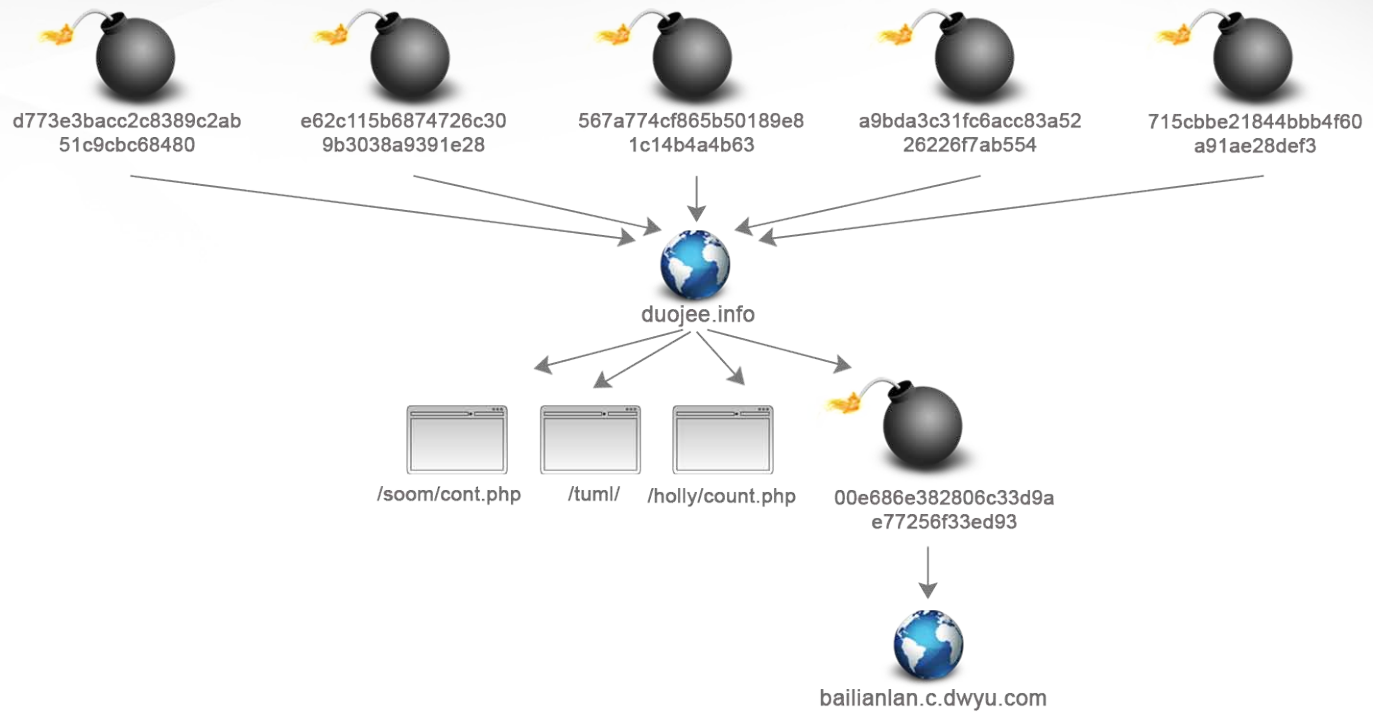


Figure 16: Relationship between the Duojeen and the Luckycat campaigns

The *duojee.info* server is the C&C component of the Duojeen campaign. The related malware, detected by Trend Micro as BKDR_DUOJEEN.A, connects to a C&C server and posts data to a PHP script typically named, *linux.php, solaris.php,* or *freebsd.php*. The following information is encoded using logical operators such as *xor, or,* or *bitwise shifting* on adjacent bytes in the malware:

- Hostname
- Computer name
- MAC address
- IP address, subnet mask, and gateway
- Network resources
- Running processes
- *Microsoft Outlook* user account information (e.g., HTTP mail user name, POP3 user name, or POP3 server)
- Recently opened files

The Duojeen malware continues to poll the C&C server then executes one of the only possible commands specified by the attackers:

- Stop the malware from communicating with the C&C server
- Download and execute a second-stage malware

Figure 17: Sample Duojeen attack email

One of the Duojeen attacks leverages a Tibetan-themed job ad to encourage potential victims to open an attached document that exploits a vulnerability in *Microsoft Office–CVE-2010-3333*, in order to drop a malware that connects to *duojee.info*.

MD5	CVE Identifier	Campaign Code
715cbbe21844bbb4f1f60a91ae28def3	*CVE-2010-3333*	aaaa
a9bda3c31fc6acc83a5226226f7ab554	*CVE-2010-3333*	aaaa
567a774cf865b50189e81c14b4ca4b63	*CVE-2010-3333*	aaaa
e62c115b6874726c309b3038a9391e28	*CVE-2010-3333*	aaaa
9860d087892fce98e6f639e3e9dba91e	Not applicable	aaa
d773e3bacc2c8389c2ab51c9cbc68480	Not applicable	aaa

Table 5: Duojeen malware samples

Duojee.info also contains the PHP scripts used for commanding and controlling the Luckycat campaign at */holly/count.php* as well as ShadowNet at */soom/cont.php*. The *duojee.info* server also has a phishing page designed to steal passwords from *mail.tibet.net* users.

Figure 18: Phishing page hosted on duojee.info

The *duojee.info* server also has other malware from two additional families available for download. One malware is known as "Comfoo," related to yet another cyber-espionage campaign, while the other is known as "Sparksrv."

Sparksrv

Sparksrv refers to a second-stage malware that provides backdoor access with significantly more functionality than first-stage droppers. Second-stage malware, often Remote Administration Trojans (RATs), are deployed because first-stage malware only provide simple "check-in" functionality such as a short list of commands that can be scheduled. Second-stage RATs, on the other hand, provide an additional access channel as well as "real-time" control over a compromised machine if the attackers and the victims are online at the same time.

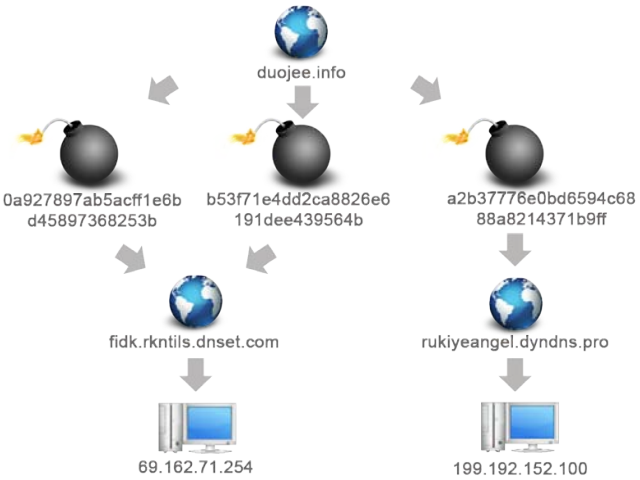


Figure 19: Relationship between the Sparksrv and the Luckycat campaigns

The Sparksrv malware, detected by Trend Micro as BKDR_RPKNUF.A, was initially found on a ShadowNet server in November 2011. We have, however, found several instances of a newer version of the same malware on *duojee.info*. The malware initially sends the following plain-text information through port 443:

- IP address
- Identifier
- MAC address

Once the malware establishes a connection, it then starts to receive commands from the C&C server, which allow the attackers to do the following:

- Start or kill a process
- Copy or search for a file
- Download or upload files
- Create or delete directories
- Load a DLL
- Invoke a command shell

MD5	Domain	IP Address
0a927897ab5acff1e6bd45897368253b	*fidk.rkntils.dnset.com*	*69.162.71.254*
b53f71e4dd2ca8826e6191dee439564b	*fidk.rkntils.dnset.com*	*69.162.71.254*
a2b37776e0bd6594c688a8214371b9ff	*rukiyeangel.dyndns.pro*	*199.192.152.100*

Table 6: Sparksrv malware samples and C&C locations

We also found an older version of the malware on a ShadowNet server, *sunshine.shop.co*.

MD5	IP Address
d0eec59f1e74c0851c8dd1c8be88f2b9	*173.208.242.25*

Table 7: Older Sparksrv malware version found on a ShadowNet server

Comfoo

Comfoo malware have been seen in conjunction with campaigns targeting sensitive entities in both Japan and India. We found a version of the Comfoo malware on the *duojee.info* server as well as an email attack that used the same version of Comfoo malware. In fact, the .DOC file used in the attack dropped an .EXE file with the same MD5 hash as the one found on the *duojee.info* server.

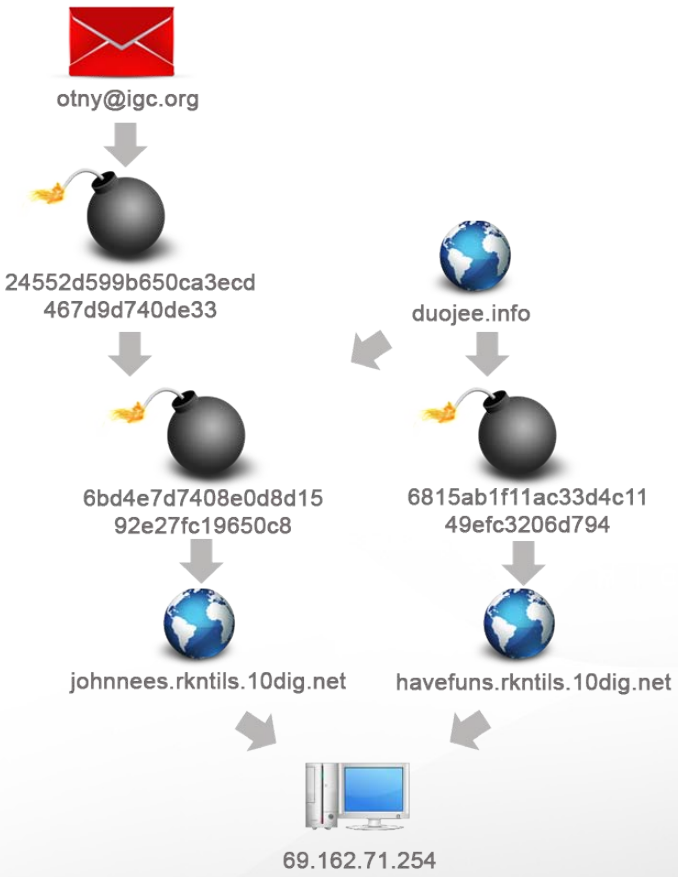


Figure 20: Relationship between the Comfoo and the Luckycat campaigns

While at least two of the Comfoo variants are essentially the same, the traffic encryption methods used in the Comfoo sample found in connection with *duojee.info* differed from other Comfoo variants we've analyzed that are not directly related to the Luckycat campaign. The more common Comfoo malware samples we analyzed used custom encryption methods while the variant found on the *duojee.info* server utilized the *Windows Cryptographic Application Programming Interface (API)*. This Comfoo variant's initial network communication sent the following information to the C&C server:

- Randomly generated characters
- MAC address
- IP address
- OS version
- String, "liberate," as campaign code

The attackers gather the following information from infected systems:

- CPU, NETBIOS, and disk information
- System, OS version, and account information
- Network adapters, protocols, and configuration information
- Installed applications as well as *Internet Explorer (IE)* and Browser Helper Object (BHO) information

The malware the attackers use is capable of receiving several commands.

Command	Description
0x233C	Invoke command shell
0x1B6C	Take screenshot
0x139C	Start interactive desktop
0x1F54	Start keylogging
0xFDC	Stop service
0xFF0	Delete service
0xBCC	Enumerate running processes
0xBE0	Terminate process
0x2EF4	Download file

Table 8: Commands the Comfoo malware receive

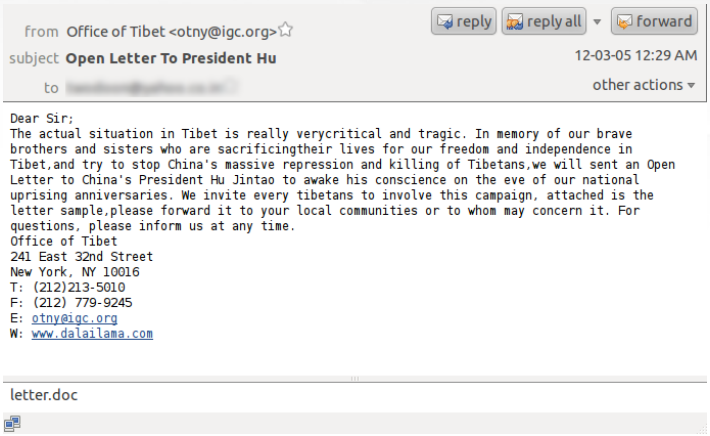


Figure 21: Sample Comfoo campaign email

This Comfoo email attack leverages the current situation in Tibet to encourage recipients to open a malicious attachment that exploits a vulnerability in *Microsoft Office–CVE-2010-3333*, in order to drop a malware onto the target's system.

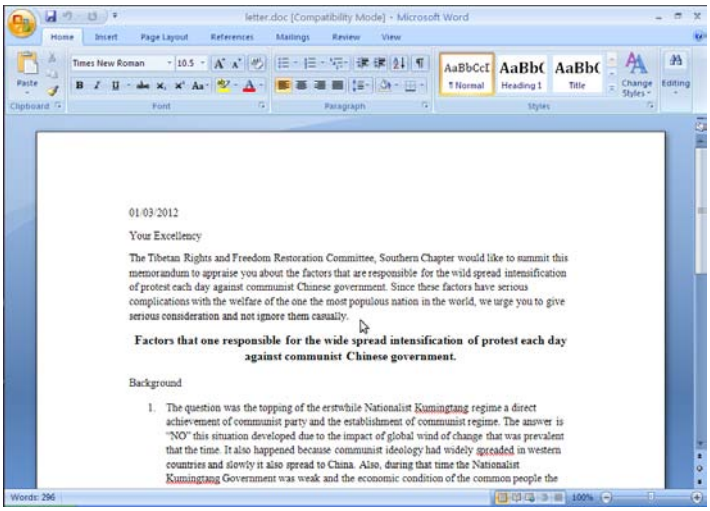


Figure 22: Comfoo decoy document that exploits a Microsoft Office *vulnerability*

After the decoy document opens, the Comfoo malware begins to communicate with *johnnees.rkntils.10dig.net*, which resolves to the IP address, *69.162.71.254*–the same host that some Sparksrv malware samples we analyzed use.

MD5	CVE Identifier	Campaign Code
24552d599b650ca3ecd467d9d740de33	*CVE-2010-3333*	liberate
6815ab1f11ac33d4c1149efc3206d794	Not applicable	liberate
6bd4e7d7408e0d8d1592e27fc19650c8	Not applicable	liberate

Table 9: Comfoo malware samples

The samples in Table 9 connect to *havefuns.rkntils.10dig.net* or *johnnees.rkntils.10dig.net*, which both resolve to the same IP address–*69.162.71.254*.

CONCLUSION

Targeted attacks have been extremely successful, making the scope of the problem truly global. These have been affecting governments, militaries, defense industries, high-technology companies, intergovernmental organizations, nongovernmental organizations (NGOs), media organizations, academic institutions, and activists worldwide.

Targeted attacks are not isolated smash-and-grab incidents. They are part of consistent campaigns that aim to establish persistent, covert presence in a target's network so that information can be extracted as needed.

Targeted attacks may not be easy to understand but careful monitoring allows researchers to leverage the mistakes attackers make to get a glimpse inside their operations. Moreover, we can track cyber-espionage campaigns over time using a combination of technical and contextual indicators.

This paper specifically discussed the Luckycat campaign. In the course of our research, we discovered that it had a much more diverse target set than previously thought. Not only did the attackers target military research institutions in India, as earlier disclosed by Symantec, they also targeted sensitive entities in Japan and India as well as Tibetan activists. They used a diversity of infrastructure as well, ranging from throw-away free-hosting sites to dedicated VPSs.

We also found that the Luckycat campaign can be linked to other campaigns as well. The people behind it used or provided infrastructure for other campaigns that have also been linked to past targeted attacks such as the previously documented ShadowNet campaign.[19]

Understanding the attack tools, techniques, and infrastructure used in the Luckycat campaign as well as how an individual incident is related to a broader campaign provides the context necessary for us to assess its impact and come up with defensive strategies in order to protect our customers.

DEFENDING AGAINST APTS

Sufficiently motivated threat actors can penetrate even networks that use moderately advanced security measures. As such, apart from standard and relevant attack prevention measures and mechanisms such as solid patch management; endpoint and network security; firewall use; and the like, enterprises should also focus on detecting and mitigating attacks. Moreover, data loss prevention (DLP) strategies such as identifying exactly what an organization is protecting and taking into account the context of data use should be employed.

Local and External Threat Intelligence

Threat intelligence refers to indicators that can be used to identify the tools, tactics, and procedures threat actors engaging in targeted attacks utilize. Both external and local threat intelligence is crucial for developing the ability to detect attacks early. The following are the core components of this defense strategy:

- **Enhanced visibility:** Logs from endpoint, server, and network monitoring are an important and often underused resource that can be aggregated to provide a view of the activities within an organization that can be processed for anomalous behaviors that can indicate a targeted attack.

- **Integrity checks:** In order to maintain persistence, malware will make modifications to the file system and registry. Monitoring such changes can indicate the presence of malware.

- **Empowering the human analyst:** Humans are best positioned to identify anomalous behaviors when presented with a view of aggregated logs from across a network. This information is used in conjunction with custom alerts based on the local and external threat intelligence available.

19 http://www.nytimes.com/2010/04/06/science/06cyber.html?_r=2

Technologies available today such as *Deep Discovery* provide visibility, insight, and control over networks to defend against targeted threats.[20] *Deep Discovery* uniquely detects and identifies evasive threats in real time and provides in-depth analysis and actionable intelligence to prevent, discover, and reduce risks.

Mitigation and Cleanup Strategy

Once an attack is identified, the cleanup strategy should focus on the following objectives:

- Determine the attack vector and cut off communications with the C&C server.
- Determine the scope of the compromise.
- Assess the damage by analyzing the data and forensic artifacts available on compromised machines.

Remediation should be applied soon afterward, which includes steps to fortify affected servers, machines, or devices into secure states, informed in part by how the compromised machines were infiltrated.

Educating Employees Against Social Engineering

Security-related policies and procedures combined with education and training programs are essential components of defense. Traditional training methods can be fortified by simulations and exercises using real spear-phishing attempts sent to test employees. Employees trained to expect targeted attacks are better positioned to report potential threats and constitute an important source of threat intelligence.

Data-Centric Protection Strategy

The ultimate objective of targeted attacks is to acquire sensitive data. As such, DLP strategies that focus on identifying and protecting confidential information are critical. Enhanced data protection and visibility across an enterprise provides the ability to control access to sensitive data as well as monitor and log successful and unsuccessful attempts to access it. Enhanced access control and logging capabilities allow security analysts to locate and investigate anomalies, respond to incidents, and initiate remediation strategies and damage assessment.

20 http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/index.html

TREND MICRO THREAT PROTECTION AGAINST LUCKYCAT CAMPAIGN COMPONENTS

The following table summarizes the Trend Micro solutions for the components of the Luckycat campaign. Trend Micro recommends a comprehensive security risk management strategy that goes further than advanced protection to meet the real-time threat management requirements of dealing with targeted attacks.

Attack Component	Protection Technology	Trend Micro Solution
HTTP C&C communication fingerprint *count.php?m=c&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@*	Web Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*
TROJ_WIMMIE VBS_WIMMIE	File Reputation (Antivirus/Anti-malware)	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*

Attack Component	Protection Technology	Trend Micro Solution
CVE-2010-3333 *CVE-2010-2883* *CVE-2010-3654* *CVE-2011-0611* *CVE-2011-2462*	Vulnerability Shielding/Virtual Patching	Server *(Deep Security)* Endpoint *(OfficeScan* with *Intrusion Defense Firewall Plug-In)* For *CVE-2010-3333:* Rule #1004498 *(Microsoft Word* .RTF File Parsing Stack Buffer Overflow Vulnerability) For *CVE-2010-2883:* Rule #1004393 *(Adobe Reader* SING Table Parsing Vulnerability) Rule #1004113 (identified malicious .PDF file) Rule #1004315 (identified malicious .PDF file - 3) For *CVE-2010-3654:* Rule #1004497 *(Adobe Flash Player* Unspecified Code Execution Vulnerability) For *CVE-2011-0611:* Rule #1004801 *(Adobe Flash Player* .SWF File Remote Memory Corruption Vulnerability) Rule #1004114 (identified malicious .SWF file) Rule #1004647 (restrict *Microsoft Office* file with embedded .SWF file) For *CVE-2011-2462:* Rule #1004871 *(Adobe Acrobat/ Reader* U3D Component Memory Corruption Vulnerability) Rule #1004873 *(Adobe Acrobat/ Reader* U3D Component Memory Corruption)

Attack Component	Protection Technology	Trend Micro Solution
cattree.1x.biz *charlesbrain.shop.co* *footballworldcup.website.org* *frankwhales.shop.co* *hi21222325.x.gg* *kinkeechow.shop.co* *kittyshop.kilu.org* *perfect.shop.co* *pumasports.website.org* *tomsburs.shop.co* *vpoasport.shopping2000.com* *goodwell.all.co.uk* *fireequipment.website.org* *tennissport.website.org* *waterpool.website.org* *tb123.xoomsite.com* *tbda123.gwchost.com* *toms.0fees.net* *tomygreen.0fees.net* *killmannets.0fees.net* *maritimemaster.kilu.org* *masterchoice.shop.co* *jeepvihecle.shop.co* *lucysmith.0fees.net*	Web, Domain, and IP Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

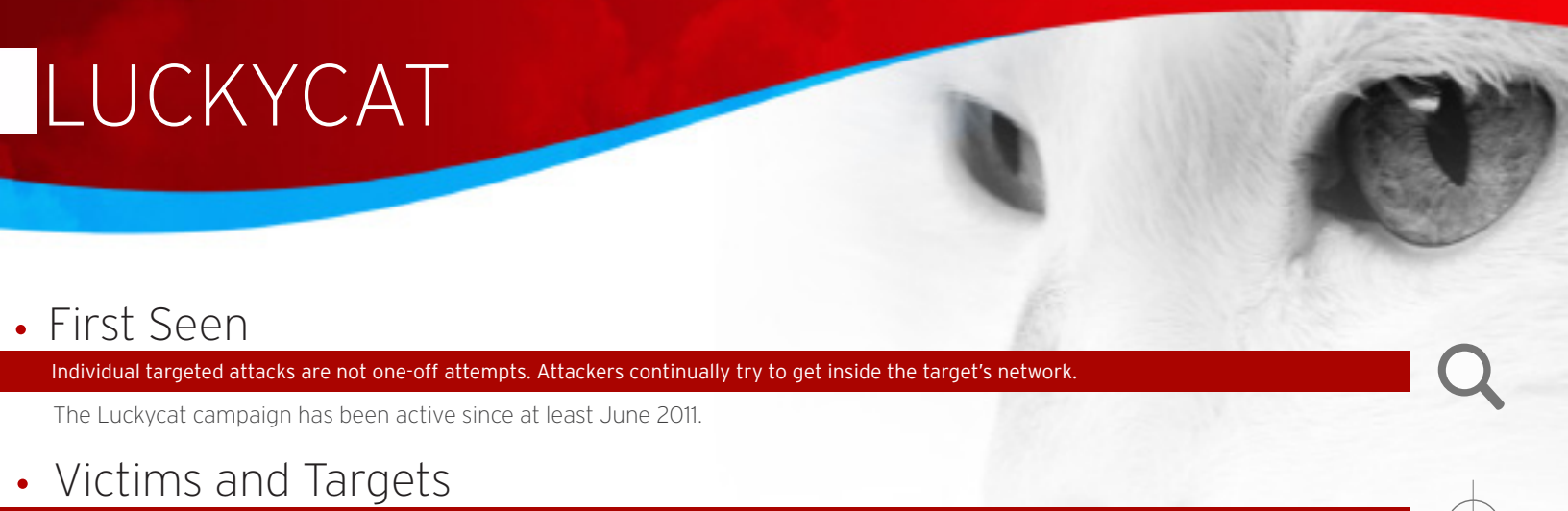
TREND MICRO™

Securing Your Journey to the Cloud

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.

LUCKYCAT



First Seen

Individual targeted attacks are not one-off attempts. Attackers continually try to get inside the target's network.

The Luckycat campaign has been active since at least June 2011.

Victims and Targets

APT campaigns target specific industries or communities of interest in specific regions.

The Luckycat campaign has been linked to 90 attacks against the following industries and/or communities in Japan and India:

AEROSPACE | ENERGY | ENGINEERING | SHIPPING | MILITARY RESEARCH | TIBETAN ACTIVISTS

The threat actors behind the Luckycat campaign used a unique campaign code to track victims of specific attacks.

Operations

The 1st-stage computer intrusions often use social engineering. Attackers custom-fit attacks to their targets.

- Targeted emails that are contextually relevant (i.e., emails containing a decoy document of radiation dose measurement results sent some time after the Great East Japan Earthquake)
- Exploited *CVE-2010-3333* (aka, Rich Text Format [RTF] Stack Buffer Overflow Vulnerability) in several instances, although *Adobe Reader* and *Flash Player* vulnerabilities were also exploited
- Used TROJ_WIMMIE or VBS_WIMMIE–malware that take advantage of the *Windows Management Instrumentation (WMI),* making the backdoor component undetectable through file scanning
- The WIMMIE malware, once inside the network, connects to a command-and-control (C&C) server via HTTP over port 80
- Attackers heavily used free web-hosting services to host their C&C servers under a diverse set of domain names but also used virtual private servers (VPSs) for more stable operations

Possible Indicators of Compromise

Attackers want to remain undetected as long as possible. A key characteristic of these attacks is stealth.

WIMMIE malware do not leave much network fingerprint. However, the following is an identifiable HTTP C&C communication fingerprint–**count.php?m=c&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@**. This format can also be seen in the URL inside the script when **/namespace:\\root\subscription path __eventconsumer** is typed in the command line for *WMI*.

Relationship with Other APT Campaigns

Malware identified with the ShadowNet, Duojeen, Sparksrv, and Comfoo campaigns were used or found hosted on the same dedicated server used by the Luckycat campaign.