

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	1
Diversity of Targets	1
Diversity of Malware	2
Diversity of Infrastructure	2
Operations	2
Attribution	2
Luckycat	3
Examples of Luckycat Attacks	4
Example 1: Japan	4
Example 2: India	4
Example 3: Tibet	5
Vulnerabilities and Malware Samples	5
Campaign Codes	7
Command and Control	8
Operations	9

Attribution	11
Campaign Connections	12
ShadowNet	12
Duojeen	13
Sparksrv	15
, Comfoo	16
Conclusion	19
Defending Against APTs	19
Local and External Threat Intelligence	19
Mitigation and Cleanup Strategy	20
Educating Employees Against Social Engineering	20
Data-Centric Protection Strategy	.20
Trend Micro Threat Protection Against Luckycat	
Campaign Components	21

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
 Shipping
- Energy
 Military research
- Engineering
 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

were stored by the attackers on their C&C infrastructure.

^{1 &}lt;u>http://www.trendmicro.com/cloud-content/us/pdfs/security-</u> intelligence/white-papers/wp_trends-in-targeted-attacks.pdf

 <u>http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_luckycat_hackers.pdf</u>
 This number represents the unique MAC addresses of the victims that

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

PAGE 1 | LUCKYCAT REDUX

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 secondstage 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, "dangO102," 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_WIMMIE⁶ or VBS_WIMMIE⁷ 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
- Get external IP address
 Execute shell command
- Upload file

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.

- 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 <u>http://www.trendmicro.com/cloud-content/us/pdfs/security-</u> intelligence/white-papers/wp_understanding-wmi-malware.pdf

^{6 &}lt;u>http://about-threats.trendmicro.com/Malware.</u> aspx?language=us&name=TROJ_WIMMIE.C

EXAMPLES OF LUCKYCAT ATTACKS

Example 1: Japan

🔁 Adobe- pdf (B	(31) - Adobe Reader						1	🛛
ファイル(E) 編集(E)	表示のウルドウ酸	~117B						*
13 J B		1/10	95.1% +		3	ウール	注釈	結張
and the second se			the second se		Land			
SI.								- 11
<u>@</u> 2.								- 11
	【別紙】福島第二部	京子力党電所モニ	ニタリングによる計測す	大況				
	計測日:3月28日							
	AL most on	al minor		444.7440	1 meta	In the cost		- 11
	AT JP(D+)(A)	AT 201 VALUE	7.4%	中性子採	84.[0]	35.02 (m/s)		
	午前9時00分	MP-4付近	6, 6 # Sv/h	-	-			
	牛前8時50分	MP-4171	6.6 # Sv/h	-				
	牛前8時40分	MP-4何近	6.6 # Sv/h		-			
	牛和8時30分	MP-41Tgt	6. 6 # Sy/h	-	-	<u> </u>		
	牛約8時20分	MP-415	6, 6 # Sv/h		-			- 11
	牛和8時10分	MP-4172	6.6 # Sv/h	-	-	<u> </u>		
	牛則6時00分	MP-4172	6.7 #Sv/h	-	-			
	牛前5時50分	MP-417m	0.0 # Sv/h	-	-			
	牛前5時40分	MP-4172	6.7 µ Sv/h					
	牛前5時30分	MP-4171	6, 7 # Sv/h	-	-			
	牛前5時20分	MP-417	6.7 # Sv/h	-				
	牛前5時10分	MP-4付近	6.7 μSv/h		-			
	牛前3時00分	MP-4付近	6.8 # Sv/h	-	-			- 1
	牛前2時50分	MP-4付近	6, 7 μ Sv/h	-				
	牛約2時40分	MP-417ar	6, 8 # Sv/h	-	-			
	年前2時30分	MP-417x	6.8 # Sv/h		-	<u> </u>		- 1
	午前2時20分	MP-4172	0, 7 # Sv/h	-	-			
	牛則2時10分	MP-4172	6.8 # Sv/h		-			
	牛利(0時(0)分	MP-417x1	6,8 # Sv/h	-	-	-		
								- 1
								- 1
								×

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

11 <u>http://www.tepco.co.jp/nu/monitoring/11032805.pdf</u>

¹⁰ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2883

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:

```
{\rtfl{\shp{\sp{\sp Fragments}{\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 vulnerability¹³
- CVE-2011-0611: Adobe Flash Player AVM1 shared object type vulnerability¹⁴
- *CVE-2011-2462:* Adobe Reader U3D component vulnerability¹⁵

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
beOb2e7a53b1dcacb8c54c180dc4ca27	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	•	1090silver89

- 0609af
- 110228cl

• 110315

110321cl

• 110329

• 110504

110603p89

• 110616np

• 110705hktg

• 110706hal

• 110705hktg

110708hktaw

110711

110711hal

110711xzg

• 110713jp

• 110706■■■■

• 110606rg789

- 0613deliinfo 110311cl
- 0613f 110315cl
- 0614senior
- 0616itiT8
- 0706
- 0804**■■■**datanet1
- 0805■■■etp
- 0805**■■■**stp
- 0805ecil
- 0805
- 0818ICG
- 0823 ARDE
- 0824∎∎∎
- 0826■■■tnd
- 1017navydiwali
- 1017■■■
- 1025■■CSC
- 1025

- 110714jdap
- 110714tp
- 110715x
- 110718p
- 110816h
- 110824p
- 1108navyeast
- 1108vpsecretary
- 111031pp
- 1110mea
- 1114round
- 1122bol
- 1122gmail
- 1122other
- 11421is9
- 1145j9yb
- 1147s9
- 1148da8
-
- 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.Ofees.net	
tomygreen.0fees.net	
killmannets.Ofees.net	
maritimemaster.kilu.org	
masterchoice.shop.co	
jeepvihecle.shop.co	
lucysmith.Ofees.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.

融天 朴支 免費 関乐	20112012411222 D	進大規係,進大院員,免費損 代理局,進大費院表,費得差, 資務罰,全国最低任!親希 QQ285085378 [進大規係]	www.hc360.com www.163 www.geyl.info www.sohu.c www.123543.com www.gi www.lineig.com www.bi www.google.cn www.jipinyi	.com om jumoshu.com du.com ule.com	胜天娱乐,胜 去,变四者,变 QQ2850853 文本站公告: 板,免费技术 请联系QQ:28 所仪,夹充内油 视镜,高级纳技	又於其, 免費据代理商,推天夏於 (約23)。如此就信,1 現形, 78 设为自查 加入收藏 室外, 英費將代用商, 免費這例站度 支持,一条龙用务 了解详细内容 5085378 产品中心,单人投作分 夏快去,万倍程序填将机,免费款。)	+++++
1000 客服小器 客服小器 音版小路 音能客服 技巧建议	名服中世 Customer Service	网通用户访问美国 本店提供的部分服务器中和支持 Imrux空间(只会持 php.mysql.html) 「日本のないない」 184.82.162.133 1 1	2回站普遍不是很稳定 网站程序员型的列表如下: win空间(支持php.mysqUhtmLasp): 12.38.176.107 73.254.208.151 09.166.68.131	E,请慎重 win空间(支持 php.mysql.html.ai 67.215.230.224 109.169.67.169 199.36.76.56(只到	p) (持正规内容)	win空间(支持php.mysql.html.asp 67 215 235 220 199 .192 .156 232 109 .188 .82 218	n)c.
客服QQ:23046897125 手机:15222540882 工作时间:10:00-24:59		5	09.169.58.159 8.64.176.121(雲道空间,距私服,色 青萼内容) 8.73.86.187 84.22.87.107	109.169.82.216 58.64.179.13(要求 情報内容) 173.254.208.99 67.215.230.204	1空间,拖私服。色	109.169.88.118 111.66.14.146(書港空间,拒私服,1 情等内容) 109.169.59.104 72.11.150.157	e
		6	7.215.230.216	67.215.235.246			C

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
0S版本:	5.1.2600 Service Pack 3 Build 2600
0S 制造商:	Microsoft Corporation
OS 配置:	独立工作站
0S 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:	VMW re 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:\ccclllmm	™™\1 的目	录		
2012-01-10	15:19	<dir></dir>	S2	
2012-01-10	15:19	<dir></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:\ccclllm	mmm\HOST	的目录		
2012-01-10	15:19	<dir></dir>		
2012-01-10	15:19	<dir></dir>		
2012-01-10	15:19	<dir></dir>	distribution (see	B2EF w1229@
2012-01-10	15:19	<dir></dir>	half-comp mitted	B6F9 w1229@
2012-01-10	15:19	<dir></dir>	and the second second	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-ccclllmmmm, 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		141
[TXT]	D244_w1229@.c	20-Jan-2012 12:16	14
[]	count.php	29-Dec-2011 10:52	1.2K
[TXT]	<u>B2EF_w1229@.c</u>	20-Jan-2012 10:52	24
[]	tp.php	29-Dec-2011 10:53	88
[TXT]	<u>3C7B w1229@.c</u>	20-Jan-2012 12:12	22
[]	<u>3C7B_w1229@.t</u>	20-Jan-2012 12:11	1.4K
[]	realip	20-Jan-2012 14:37	14
[TXT]	<u>3B86_w1229@.c</u>	19-Jan-2012 01:47	14
[]	BBB0_w1229@.t	20-Jan-2012 14:37	0
[]	F805_w1229@.t	20-Jan-2012 13:01	0
[]	AD244_w1229@.t	20-Jan-2012 12:11	0
[]	B7A8B_w1229@.t	20-Jan-2012 10:02	0
[]	22834 w1229@.t	14-Jan-2012 06:04	0
[]	<u>10000_w1229@.t</u>	20-Jan-2012 12:51	0
[]	35C0B2EF w1229@.t	20-Jan-2012 10:29	0
[]	4B6F9 w1229@.t	20-Jan-2012 13:56	0
[] .	503C7B w1229@.t	20-Jan-2012 12:11	0
[]	<u>'A2B_w1229@.t</u>	20-Jan-2012 12:36	0
[]	CCF00_w1229@.t	20-Jan-2012 12:28	0
[]	<u>D0A0834_w1229@.t</u>	09-Jan-2012 11:45	0
[]	B86_w1229@.t	18-Jan-2012 18:22	0
[]	0DD_w1229@.t	19-Jan-2012 18:27	0
[]	27EA9480_w1229@.t	17-Jan-2012 18:59	0
Apache	e Server at 89757.x.gg Port 80	Þ	

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> . . <DIR> 2011-08-20 00:30 App 2011-08-20 00:30 <DIR> Data 2011-08-20 00:30 <DIR> Docs FirefoxPortable 2011-08-20 00:30 <DIR> 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> <DIR> 2012-01-10 08:42 App 2012-01-10 08:48 <DIR> Data 2011-01-17 06:52 46,344 help.html 2012-01-10 08:42 <DIR> Other 108,490 TunnelierPortable.exe 2011-01-17 06:53 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 Chineselanguage 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.

主國 时轮:关于 realpla	yer.rm文件都附编栈追出通测 +上一主题 下一主题 -
dang0102	業機手: 2005-12-20 15:12
電管: 25 約分: 0 注册: 2004-11-10	 Bardwards 本型相 、製作自参加製作は進化水支が付き下、重要的なから登え top://www.cw.motre.org/cgl-bin/cgl-bin/cw.motre.org/cgl-bin/cw.motre.org/cgl-bin/cg
dang0102	業表于: 2005-12-20 15:14
发帖: 35 积分:0 注册:2004-11-10	Martania Modificata : [1201225]

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



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

The post in Figure 11 contains two email addresses– **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.*^{*T*} 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 <u>http://dazzlepod.com/rootkit/?page=83</u>

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 firststage 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. 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.



$\mathsf{S}\mathsf{hadow}\mathsf{N}\mathsf{et}$

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.

from	comitatoprotibet2011@gmail.com 🛱	
subject	Fw:Self-Immolations	12-01-11 10:09 PM
to	In page to a photo at con-	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

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

- invoire	Inset	Page Layout	Meterences	Mainings	Henew	VIEW					
ate A	Calibri B / U	- 12 - aler 18, 18' A	• A' A' 🔊		·安·律 書 語	(≭ 24 ¶ 3t · Ⅲ ·	Aa8bCcDd T Normal	AaBbCcDd T No Spaci	AaBb(A	dfS Editing
Doard G		Font			Paragraph	9		Styles		Styles * G	
											1
		1									
		The United	States says	it is "serio	ously conc	erned" that	more Tibe	tans have	set		
		themselves	on fire in Ci	hina, and s	ays the ac	tions repres	sent deep fr	ustration w	dth		
		Chinese gov	ernment rest	rictions.							
		U.S. State	Departmen	it spokesv	voman V	ictoria Nul	and said	Monday 1	the		
		self-Immola	tions show th	nere is eno	rmous ang	er over seve	ere Chinese	restrictions	on		
		human right	ts and religion	us freedom:	5.						
					13						
		She added to	hat Washingt	on has cons	sistently rai	ised the issu	e with China	L.			
		Reports from	m Tibet say	another Tit	etan moni	k died Sunda	ay after sett	ing himself	on		
		fire in Dari c	ounty of Amo	lo region.							
		fire in Dari o	say that before	lo region. pre 42-year	-old Lama	Sopa Tulku :	set himself i	ablaze, he s	ald		
		fire in Dari o The reports he was doli	say that before say that before so to con	lo region. ore 42-year imemorate	-old Lama	Sopa Tulku betans who	set himself i have died	ablaze, he s since 2009	ald		
		fire in Dari o The reports he was dolo Tibet's free	say that before say that before so to con dom and for	lo region. ore 42-year imemorate the return	-old Lama all the Ti of their spi	Sopa Tulku betans who ritual leader	set himself i have died r, the Dalai L	ablaze, he s since 2009 ama, who f	ald for led		
		fire in Dari o The reports he was dolo Tibet's free to India in 1	say that before say that before so to condition of the solution of the solutio	lo region. ore 42-year imemorate the return abortive up	-old Lama all the Ti of their spi rising agai	Sopa Tulku betans who ritual leader	set himself i have died r, the Dalai L role.	ablaze, he s since 2009 ama, who f	ald for led		

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 serverduojee.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

from contracting for Director of Development	12-02-20 10:21 AM
to	other actions 🔻
Post: Director of Development	
The Tibet Fund is seeking a seasoned Development professional to des comprehensive development plan based on funding priorities establish Directors in the organizationi"s new strategic plan.	ign and implement a ed by the Board of
The Tibet Fund is seeking a seasoned Development professional to des comprehensive development plan based on funding priorities establish Directors in the organizationi's new strategic plan.	ign and implement a ed by the Board of

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	аааа
a9bda3c31fc6acc83a5226226f7ab554	CVE-2010-3333	аааа
567a774cf865b50189e81c14b4ca4b63	CVE-2010-3333	аааа
e62c115b6874726c309b3038a9391e28	CVE-2010-3333	аааа
9860d087892fce98e6f639e3e9dba91e	Not applicable	ааа
d773e3bacc2c8389c2ab51c9cbc68480	Not applicable	ааа

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.

Tibet*mail* 🚳

Please enter your passphrase:	
	Authenticate



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:

- Identifier
- IP address
- luentinei
- 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
- Create or delete
 directories
- Copy or search for a file
- Load a DLL
- Download or upload files
- 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

Сомбоо

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
Ox1B6C	Take screenshot
0x139C	Start interactive desktop
Ox1F54	Start keylogging
OxFDC	Stop service
OxFFO	Delete service
OxBCC	Enumerate running processes
OxBEO	Terminate process
Ox2EF4	Download file

🖂 reply 🔛 reply all 🔻 😺 forward from Office of Tibet <otny@igc.org>☆ 12-03-05 12:29 AM subject Open Letter To President Hu other actions **v** to

Dear Sir: The actual situation in Tibet is really verycritical and tragic. In memory of our brave brothers and sisters who are sacrificingtheir lives for our freedom and independence in Tibet, and try to stop China's massive repression and killing of Tibetans.we will sent an Open Letter to China's President Hu Jintao to awake his conscience on the eve of our national uprising anniversaries. We invite every tibetans to involve this campaign, attached is the letter sample, please forward it to your local communities or to whom may concern it. For office of Tibet 241 East 230d Strongt 241 East 32nd Street New York, NY 10016 T: (212)213-5010 F: (212) 779-9245 E: <u>otny@igc.org</u> W: <u>www.dalailama.com</u>

letter.doc a de la compañía de l

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.

Nome Page layout Reference Mating Reserve Water Image layout Image layout Reference Mating Reserve Water Image layout Image layout Reference Image layout Reference Image layout Reference		₹2/	letter.doc [[Compatibility N	Viode] + Micr	osoft Word				
0103 2012 Your Excellency The station of the water of the wate	Home Inter	rt Page Layout	References Mail	lings Review	r View					
Month of the strangthy of	Times New	Roman - 10.5 - 11 - al- x, x' Aa-	Λ΄ Λ΄ (⁴) ⊞ ⁴ 2 · Δ · ■	· (= · \\[-] +	F (F (21))	AaBbCcI	AaBb(Heading 1	AaBb(Change	AA Editing
01.03.2012 Your Excellency Thereas Rights and Freedom Restoration Committee, Southern Chapter would like to mumit this memorandum to appraise you about the factors that are responsible for the wild greed intensification of protost each day against communit. Chanse government. Since these factors have serious complications with the wolfare of the one the most populous attoin in the world, we upp you to give serious consideration and not ingore them canally. W Factors that one responsible for the wide spread intensification of protest each day gainst communist Chinese government. Background 1 chic question was the topping of the eritwhile Nationalist Kamingtang regime a direct activement of community party and the establishment of communist regime. The answer is "NO" this situation developed due to the impact of global wind of change that was prevalen that the time. If also happened because communit ideology had widely graded in wettern commisse and dowly it also great to China. Also, during that mus the Nationalist Kamingtang Government was was wide the economic condition of the commo projet the	aboard G	Font	a .	Patagrap	in .	6	Styles			1
Background 1. The question was the topping of the erstwhile Nationalis Kamingtang regime a direct achievement of communist party and the erstwhile Nationalis Kamingtang tregime. The answer is "NO" this simulo developed due to the impact of global wind of change that was prevalent that the time. I raiso happened because communit ideology had woldy oggedded in wettern commiss and dowly in side spread to Chaina. Also, during that time the Nationalist Kumingang Government was weak and the economic conditions of the common people the		01/03/2012								
		The Tibetan Right memorandum to a of protest each day complications with serious considerati Factors that on	s and Freedom Rest ppraise you about th against communist the welfare of the ion and not ignore th ne responsible fo	oration Commit the factors that as the Chinese govern one the most po- hem casually. or the wide sp	ttee, Southern re responsible nment. Since ipulous nation pread inten	Chapter would li for the wild spre- these factors have in the world, we sification of pr	ike to summit ad intensificat e serious urge you to g rotest each o	this tion tive day		

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.

Table 8: Commands the Comfoo malware receive

Figure 21: Sample Comfoo campaign email

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

DEFENDING AGAINST APTS

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. 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.

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.

$M_{\text{ITIGATION}} \text{ and } C_{\text{LEANUP}} \text{ Strategy}$

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-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 #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 tennissport.website.org tb123.xoomsite.com tbda123.gwchost.com toms.Ofees.net killmannets.Ofees.net killmannets.Ofees.net maritimemaster.kilu.org masterchoice.shop.co jeepvihecle.shop.co lucysmith.Ofees.net	Web, Domain, and IP Reputation	Endpoint (<i>Titanium</i> , <i>Worry-Free Business</i> 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 cloudbased 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



Securing Your Journey to the Cloud

©2012 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks or tredemarks or tr

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 EN

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.



