DTrace를 이용한 악성코드 분석

Malware analysis using Dynamic Trace Framework

forensic.nofate.com

순서

- DTrace 소개
- DTrace 구성
- 관련 스크립트 정리
- 악성코드 동적 분석 예제

DTrace

- 포괄적인 동적 추적 프레임워크
- 솔라리스 운영체제를 위해 최초 개발함
- 커널 코드에 통합되어 있음
- 지원 운영체제
  - Solaris 10, Mac OS X 10.5, FreeBSD 7.1, NetBSD, Linux Kernel(?)

DTrace

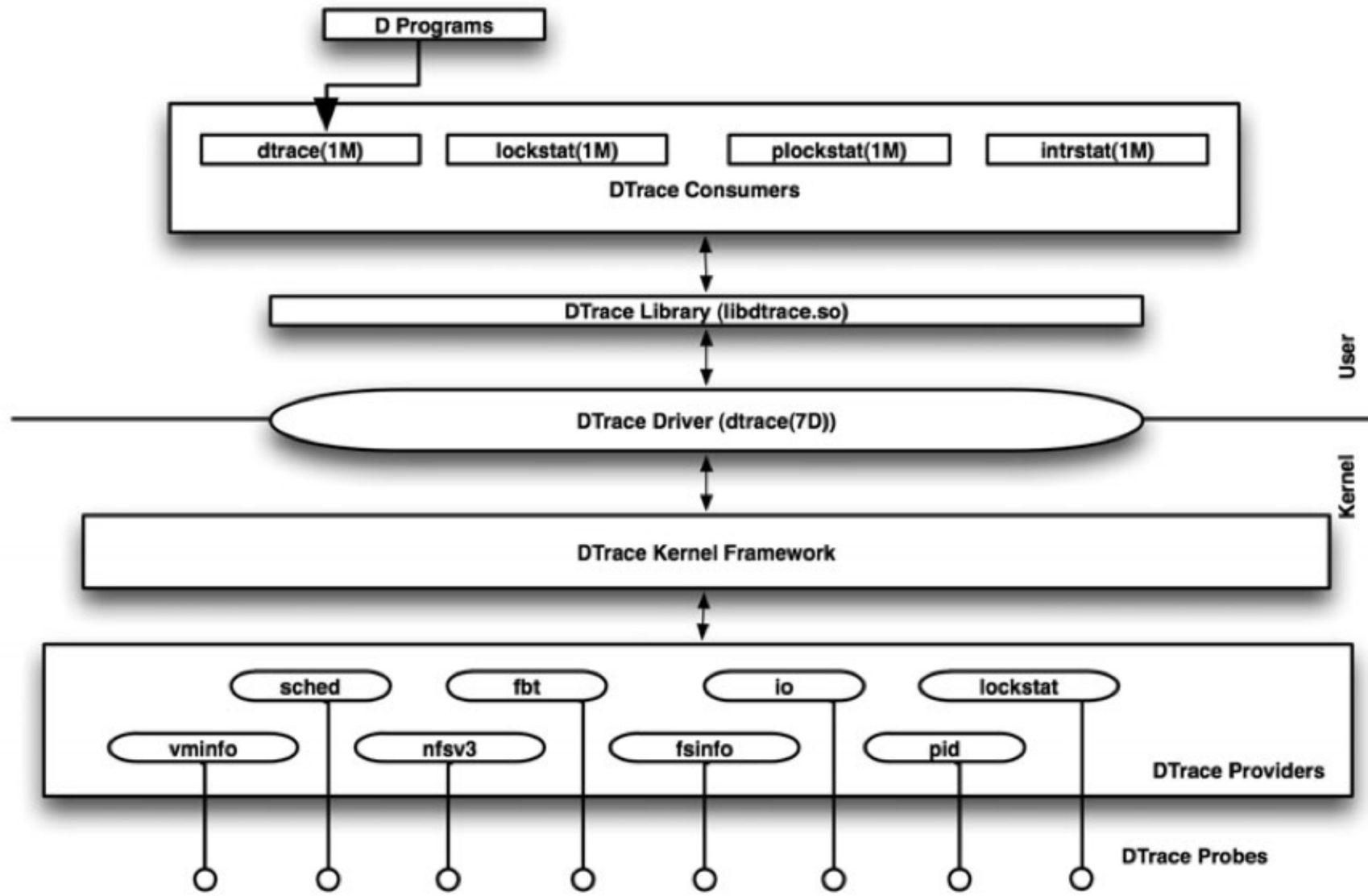
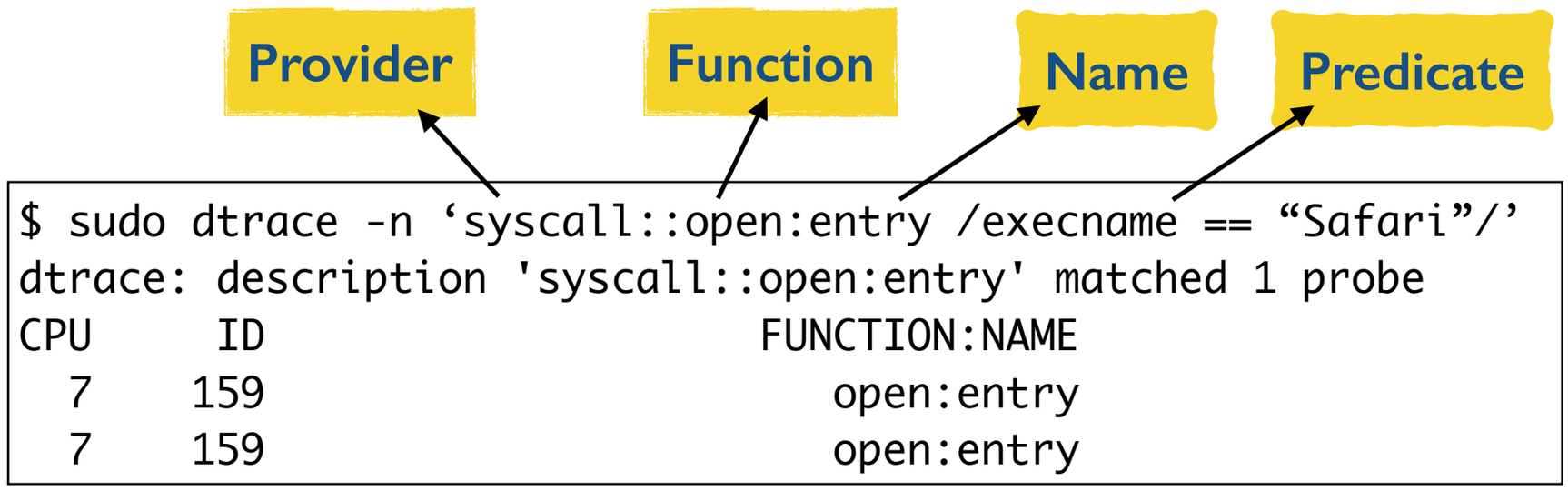


Figure 1-2 DTrace architecture

Reference : Brendan gregg, DTrace

DTrace

```
$ dtrace
Usage: dtrace [-aACeFHlqSvVwZ] [-arch i386|x86_64] [-b bufsz] [-c cmd] [-D name[=def]]
    [-I path] [-L path] [-o output] [-p pid] [-s script] [-U name]
    [-x opt[=val]]
```



용어정리

- Provider : 함수 클래스와 유사, syscall의 경우 유닉스 시스템 콜을 의미, 특정 프로세스 ID도 될 수 있으며, Objective-C의 클래스도 가능
- Module : Provider를 기준으로 정해짐. 모듈이 없다면 생략할 수 있음. 동적 라이브러리(.dylib)도 사용 가능
- Function : 모듈 또는 Provider 내의 함수
  - 예를 들면 syscall의 open
- Name : Provider에 의해 정해지며, 보통 특정 함수의 실행 시점인 entry와 종료 시점인 return을 가짐
  - DTrace 자체의 생성자/소멸자인 BEGIN/END 가능

용어정리

- Predicate// : 일치 여부를 판단(if)하는 정보
- actions{} : probe에 해당하는 데이터가 predicate를 통과하면 실행
- probe : 동작 중인 소프트웨어에 동적으로 instrumentation 포인트 추가하는 지점
- fire : probe를 활성화하고 코드 흐름에서 instrumented probe point 지점에 도달하면 발생

D Script

- DTrace 코드를 스크립트화 시킬 수 있음
  - 커맨드라인은 비효율적
- D Language로 작성
- -s 옵션으로 사용 가능

D Script

```
$ cat open.d
#!/usr/sbin/dtrace -s

syscall::open:entry
/execname == "Safari"/
{
    printf("open %s file\n", copyinstr(arg0));
}
```

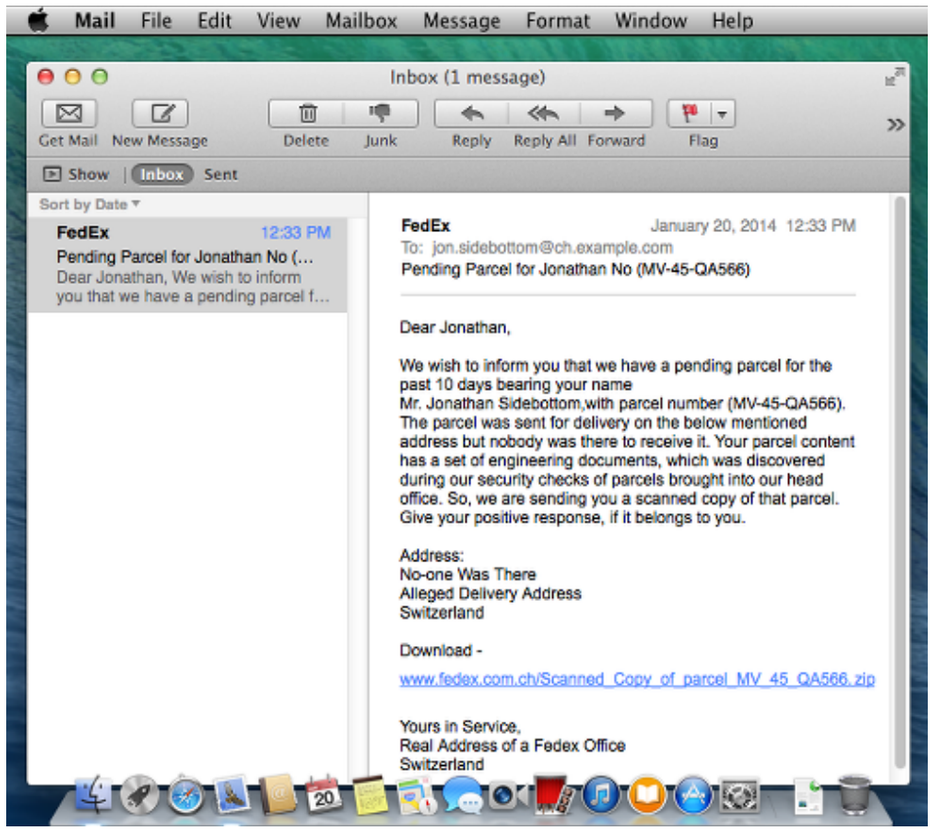

```
$ chmod 755 open.d
$ sudo ./open.d
dtrace: script './open.d' matched 1 probe
CPU     ID                    FUNCTION:NAME
  0    159                       open:entry open /Library/Internet Plug-Ins/QuickTime
Plugin.plugin/Contents/Resources/English.lproj/InfoPlist.strings file

  0    159                       open:entry open /Users/chainbreaker/Library/Preferences/
com.apple.quicktime.plugin.preferences.plist file

  0    159                       open:entry open /Library/Internet Plug-Ins/
SharePointBrowserPlugin.plugin/Contents/PkgInfo file
```

추천 스크립트

이름	내용	기본 탑재
execsnoop	exec로 실행되는 프로세스 추적	O
iosnoop	I/O 추적	O
opensnoop	오픈되는 파일 추적	O
rwsnoop	읽기/쓰기 추적	O
newproc.d	새로 생성되는 프로세스(인자 포함) 추적	O
soconnect_mac.d	네트워크 연결 추적	X
maclife.d	파일 생성/삭제 추적	X

분석 예제

(Reference : Digitally signed data-stealing malware targets Mac users in "undelivered courier item" attack)



- OSX/Laoshu-A
- 이메일을 이용한 Spear-phising attack

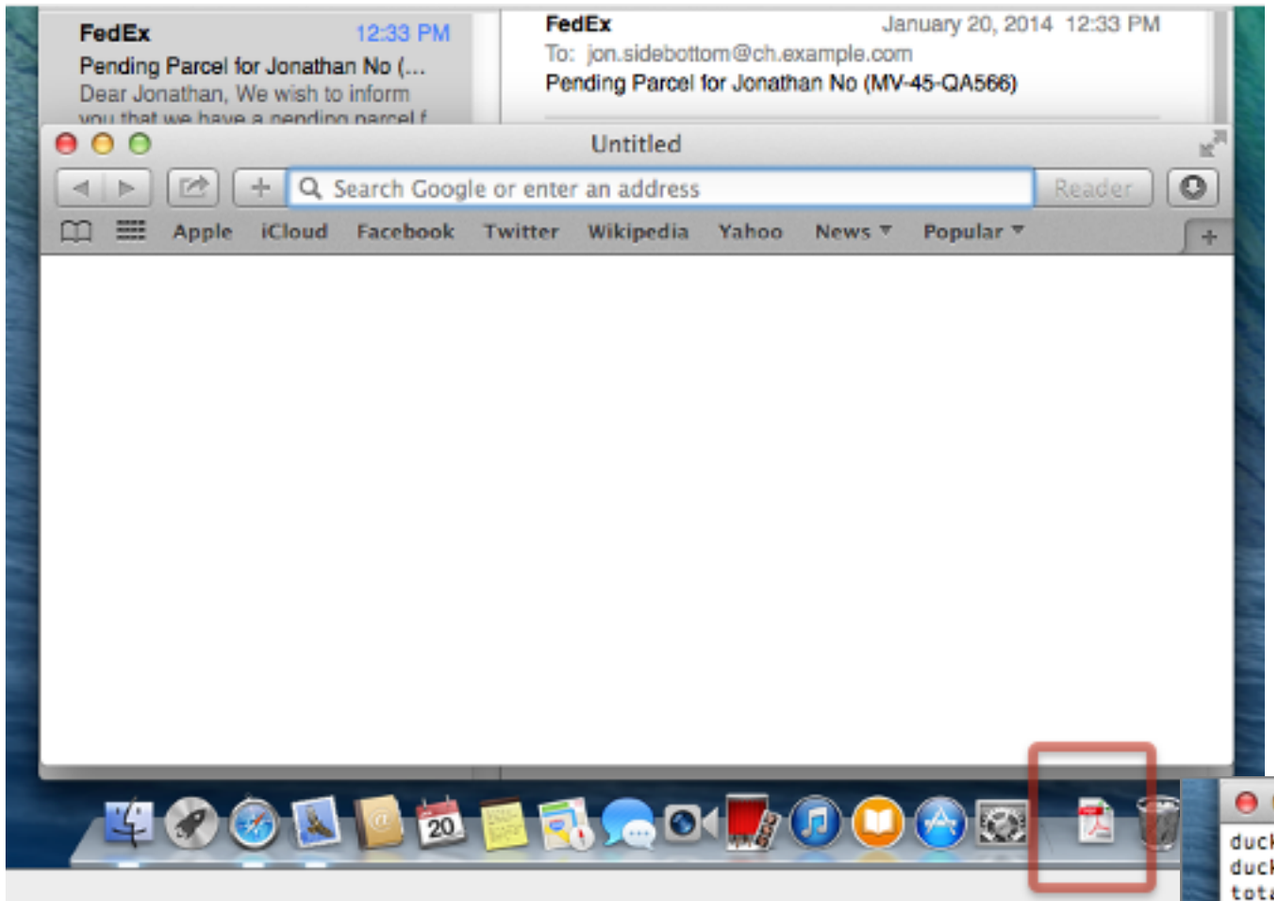
분석 예제

(Reference : Digitally signed data-stealing malware targets Mac users in "undelivered courier item" attack)

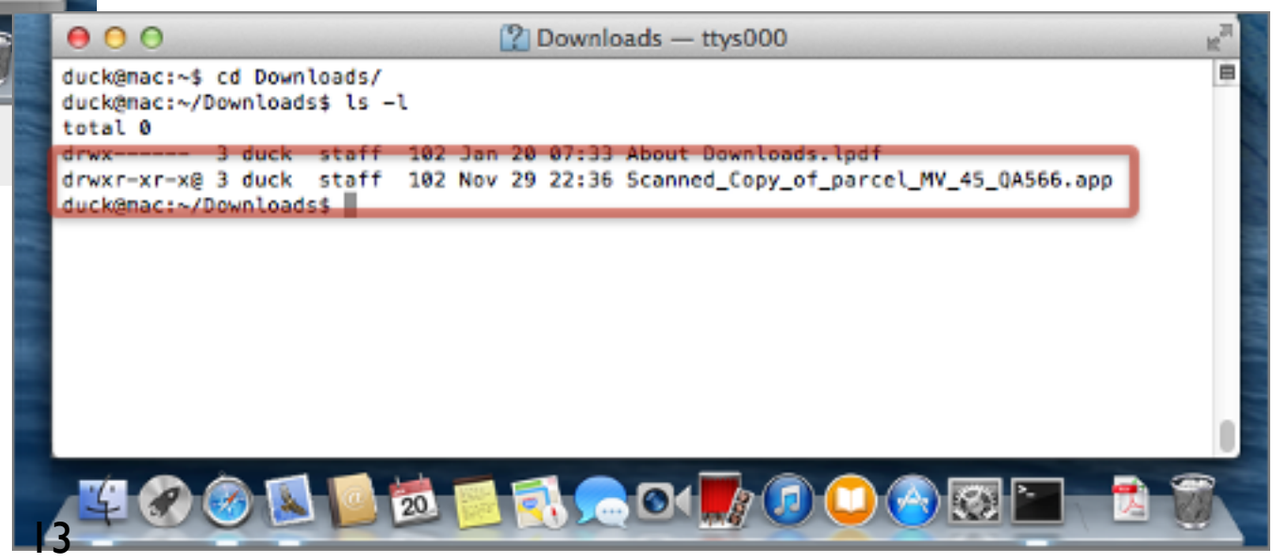
- 링크를 통해 zip 파일 다운로드
  - Safari의 경우, 알려진 압축 파일 자동 해제
- 겉으로 보기에는 PDF 파일
  - 알려진 확장자 자동 숨김을 이용
  - 아이콘을 PDF로 설정
- 디지털 서명되어 있음

분석 예제

(Reference : Digitally signed data-stealing malware targets Mac users in "undelivered courier item" attack)

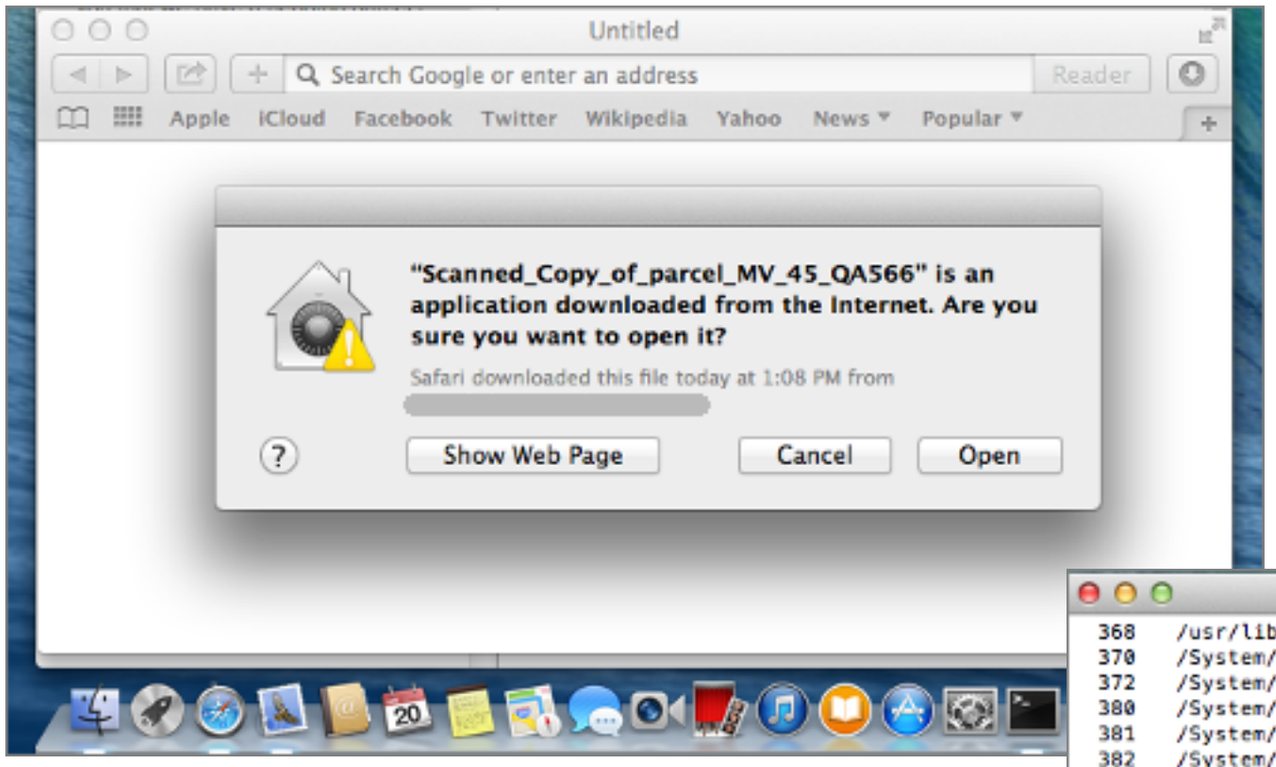


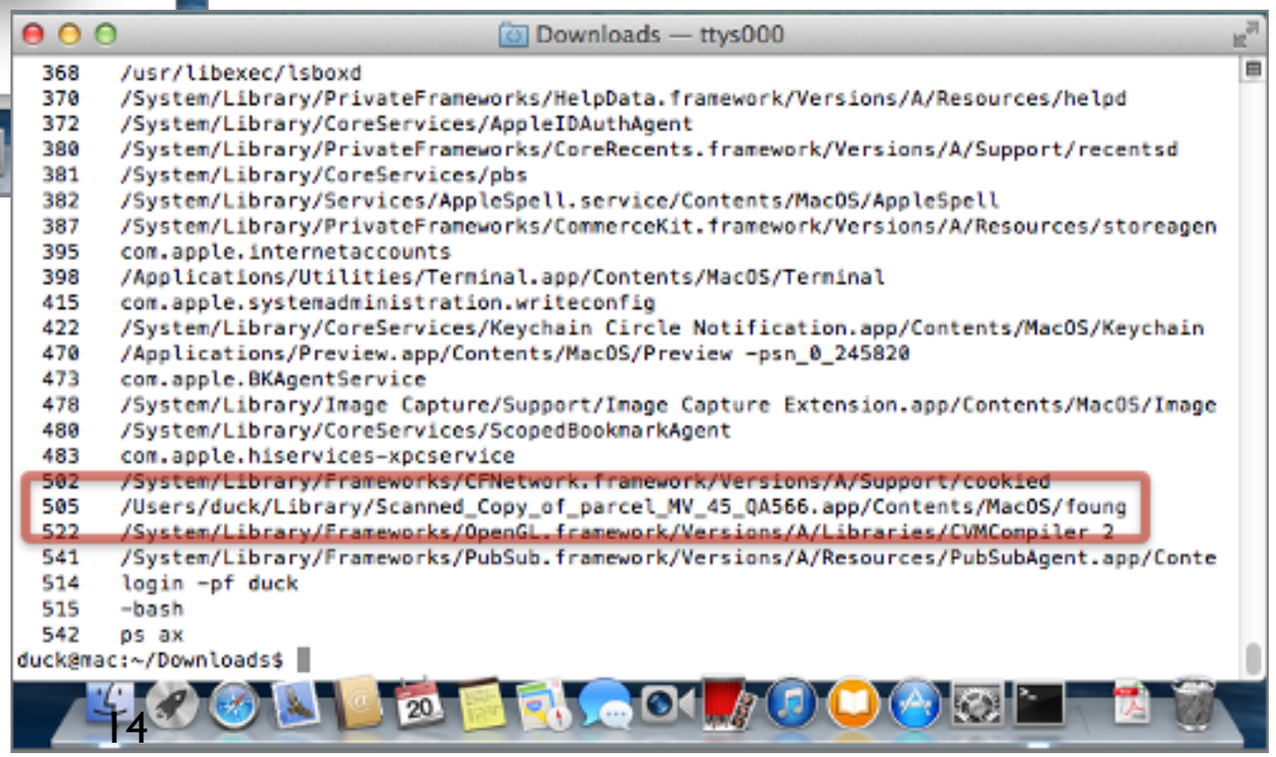
Clicking the email link automatically brings down a file that appears to be a PDF



분석 예제

(Reference : Digitally signed data-stealing malware targets Mac users in "undelivered courier item" attack)





분석 예제

(Reference : Digitally signed data-stealing malware targets Mac users in "undelivered courier item" attack)

- 주요 기능
  - 문서 파일 검색 및 압축
    - (DOC,XLS,PPT,DOCX,XLSX,PPTX)
  - 특정 서버에 업로드
  - 새로운 파일 다운로드
  - 커맨드 명령어 실행
- 새로운 파일 다운로드 : DTrace 분석 예제

분석 예제

- OSX/Laoshu-A에서 다운로드하는 악성코드
- MD5(OSX_Update.app/Contents/MacOS/worty) = ea2045d1344719d95f85ee8a2fcbe0a7
- 주요 기능 : 화면을 캡쳐하여 특정 URL에 업로드
- 상세 분석 자료 : http://forensic.n0fate.com/?p=706

분석 예제

```
lea     rdx, cccdatetimeformat ; "kLBf7h7di4kSVBDQsZgCuzfbz16dIBnW"
mov     rsi, cs:selRef_cxx_
mov     rdi, r15          ; yy-MM-dd-HH:mm:ss
call    r13 ; _objc_msgSend
mov     rsi, cs:selRef_setDateFormat_
mov     rdi, rbx
mov     rdx, rax
call    r13 ; _objc_msgSend
mov     rsi, cs:selRef_stringFromDate_
mov     rdi, rbx
mov     rdx, r12
call    r13 ; _objc_msgSend
mov     rbx, rax
lea     rdx, cfstr_Lmhrvudjsky ; "LMHrvuDJskY="
mov     rsi, cs:selRef_cxx_
mov     rdi, r15          ; .png
call    r13 ; _objc_msgSend
lea     rdx, cfstr_□□□□ ; "%□%□%□%□"
```

- 모든 문자열을 암호화한 후 Base64로 인코딩
  - 실행 시점에 특정 클래스의 함수로 복호화

분석 예제

- cry class : 암복호화
  - fi : Base64 decoding
  - chi : Base64 encoding
  - end : DES encryption
  - ded : DES decryption
- CCCryptor : Common Cryptographic Algorithm Interfaces

```
mov     [rbp+var_20], rax
mov     rsi, cs:selRef_fi_
mov     rdi, cs:classRef_cry
mov     r15, cs:_objc_msgSend_ptr
call    r15 ; _objc_msgSend ; [cry fi:]
mov     rbx, rax
mov     [rbp+var_420], 0
mov     rax, 8070605040302 01h
mov     [rbp+var_428], 0
mov     [rbp+IV], rax
mov     rsi, cs:selRef_UTF8String
mov     rdi, r14
call    r15 ; _objc_msgSend
mov     r14, rax
mov     rsi, cs:selRef_bytes
mov     rdi, rbx
call    r15 ; _objc_msgSend
mov     r15, rax
lea     rsi, msgRef_length__objc_msgSend_fixup
mov     rdi, rbx
call    cs:msgRef_length__objc_msgSend_fixup
lea     r9, [rbp+IV]
lea     rcx, [rbp+var_420]
lea     rdx, [rbp+var_428]
mov     [rsp+460h+var_440], rdx ; 0
mov     [rsp+460h+var_450], rcx ; 0
mov     [rsp+460h+var_458], rax
mov     [rsp+460h+var_460], r15
mov     [rsp+460h+var_448], 1024
mov     edi, 1
mov     esi, 1
mov     edx, 1
mov     rcx, r14
mov     r8d, 8          ; keylength
call    _CCCrypt
```

분석 예제

- 추적에 필요한 것
  - Provider : Process ID
  - Module : libcommonCrypto.dylib
  - Function : CCCrypt
  - Name : entry or return
  - 함수 인자

```
CCCryptorStatus
CCCrypt(CCOperation op, CCAlgorithm alg, CCOptions options,
    const void *key, size_t keyLength, const void *iv,
    const void *dataIn, size_t dataInLength, void *dataOut,
    size_t dataOutAvailable, size_t *dataOutMoved);
```

분석 예제

```
/* written by n0fate
 * dtrace -q -s cccrypt.d PID
 */
pid$1:libcommonCrypto.dylib:CCCrypt:entry
/execname == "worty"/
{
    printf("%d %d %d key:%016llx size:%d iv:%016llx datainput:%x, dataoutput:%x", arg0,
arg1, arg2, *(unsigned long long *)copyin(arg3, arg4), arg4, *(unsigned long long
*)copyin(arg5, 8), arg6, arg8);
    self->dataoutput = arg8;
}

pid$1:libcommonCrypto.dylib:CCCrypt:return
/execname == "worty"/
{
    printf("(%s)\n", copyinstr(self->dataoutput, *(unsigned int*)copyin(arg9, 4)));
    ustack(5,0);
}
```

시연

참고 문서

- Brendan Gregg, dtrace.org
- SourceFire Vulnerability Research Team, http://vrt-blog.snort.org/2014/03/osxtrojanleverage-breakdown-using-dtrace.html.
- Sophos, http://nakedsecurity.sophos.com/2014/01/21/data-stealing-malware-targets-mac-users-in-undelivered-courier-item-attack/.

Q & A

nofate@nofate.com