Trends in dForensics, Nov/2012

proneer

proneer@gmail.com

http://forensic-proof.com

Kim Jinkook

포렌식 준비도에 대한 대비 (1/2)

- **포렌식 준비도(Forensic Readiness)**

> "조사 비용은 최소화하고 디지털 증거의 활용 가능성은 최대화하기 위한 조직의 능력"
>
> 보안 사고에 따른 비용을 최소화하기 위해 사고가 발생하면 신속히 잠재적인 흔적을 법적 증거능력을 유지한 상태에서 수집하고 분석할 수 있도록 사전에 준비를 갖추는 것을 의미한다. 준비는 인적 노력을 비롯하여 정책적, 기술적, 조직적인 노력을 모두 포함한다.

  - 2009년, 영국에서 제도화
  - **이점**
    - ✓ 자산을 체계적으로 관리하고 위험을 최소화 ➔ 고객에게 신뢰
    - ✓ 업무에 지장을 주지 않고 사고 대응 가능
    - ✓ 신속한 사고 대응으로 피해 최소화
    - ✓ 기업의 법적 증거능력 확보 ➔ 승소 가능성을 높임
    - ✓ 전자증거개시, 규제 준수와 같은 다른 거버넌스 활동과 연계하여 효용을 높임

포렌식 준비도에 대한 대비 (2/2)

- **포렌식 준비도(Forensic Readiness)**
  - **단점**
    - ✓ 기존의 기업 거버넌스 활동과 충돌을 피하기 위해 충분한 정책적, 기술적 논의 필요
    - ✓ 많은 비용 부담, 비용에 따른 효율을 입증하기 어려움
  - **간단한 기술적 포렌식 준비도 대비**
    - ✓ 이벤트로그 모니터링
    - ✓ 서버 프리패치 설정
    - ✓ XP 방화벽 로그 설정
    - ✓ 크래시 덤프 설정
    - ✓ NTFS 마지막 접근 시간 설정
    - ✓ 복원지점/볼륨섀도우 복사본 설정
    - ✓ $LogFile 설정
    - ✓ 로그 설정 강화
    - ✓ 로그 백업과 무결성 유지
  - 새로운 시장의 기대감으로 과장되어 홍보 ➔ 개념적인 면에서 필요함 ➔ 현실적인 대안 고려

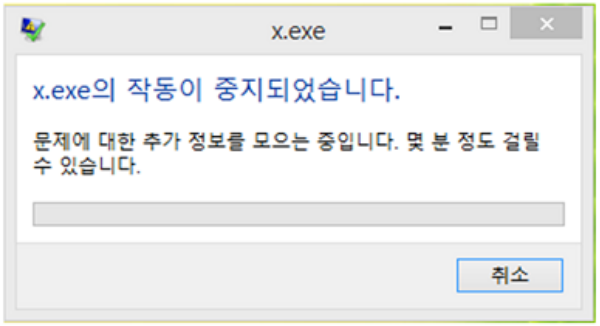
구글 크롬 프라이버시 문제

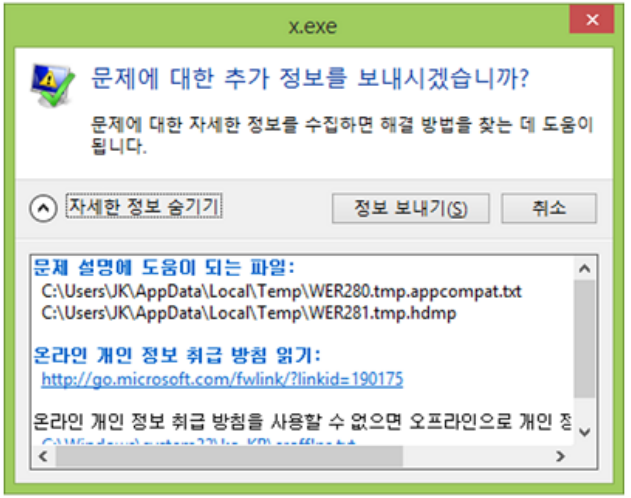
- **구글 크롬 Preferences 파일**
  - 백업, 북마크, 브라우저, 검색 엔진, 다운로드, 확장 기능, 플러그인, 세션, 싱크 설정 정보
  - 클라우드 프린트, DNS 프리패칭, 줌 레벨

  - **클라우드 프린트** ➔ 클라우드 프린트를 설정한 대표 이메일
  - **DNS 프리패칭** ➔ 웹 페이지 내의 도메인을 미리 DNS 쿼리하여 프리패칭
  - **줌 레벨** ➔ 각 페이지별 확대/축소 정보

꺼진 불도 다시보자: 윈도우 문제 보고

- **윈도우 문제 보고 (Windows Error Reporting)**
  - 윈도우 XP 부터 추가된 서비스
  - 하드웨어나 소프트웨어 오류 발생 시 알림, 디버깅 정보 수집
  - 오류에 따라 알림 발생이 불규칙적
  - 오류 디버깅 정보를 이용해 공격 시도 탐지





date	time	MACB	sourcetype	desc
09/19/2012	22:39:44	M.C.	NTFS $MFT	/Windows/Inf/WmiApRpl/WmiApRpl.h
09/19/2012	22:39:48	M.C.	NTFS $MFT	**/Windows/Prefetch/WMIADAP.EXE-F8DFDFA2.pf**
09/19/2012	22:40:03	..C.	NTFS $MFT	**/$Recycle.Bin/x.exe**
09/19/2012	22:40:03	MAC.	NTFS $MFT	/Users/JK/Desktop
09/19/2012	22:40:03	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/CurrentVersion/Explorer
09/19/2012	22:40:03	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/CurrentVersion/Explorer/OperationStatusManager
09/19/2012	22:40:09	MACB	NTFS $MFT	**/Windows/Prefetch/DLLHOST.EXE-6A473D35.pf**
09/19/2012	22:40:12	..C.	NTFS $MFT	/Users/JK/AppData/Local/Microsoft/Sqm/WindowsLL
09/19/2012	22:40:12	M.C.	NTFS $MFT	/Users/JK/AppData/Local/Microsoft/Sqm/WindowsLL/WindowsLL.wns.14.sqm
09/19/2012	22:40:13	MACB	SOFTWARE k	Key name: HKLM/SoftwareCsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Wow6432Node/Microsoft/Windows/**Windows Error Reporting**
09/19/2012	22:40:13	MACB	SOFTWARE k	Key name: HKLM/SoftwareCsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Wow6432Node/Microsoft/Windows/Windows Error Reporting/Debug
09/19/2012	22:40:13	M.C.	NTFS $MFT	/Windows/System32/LogFiles/Scm/1db7c2f1-876c-4f24-ad17-8428211113f9
09/19/2012	22:40:14	A.B	NTFS $MFT	/Windows/System32/winevt/Logs/**Microsoft-Windows-WER-Diag%4Operational.evtx**
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6B90.tmp.dmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6BEE.tmp.cab (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6B70.tmp.appcompat.txt (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C02.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C14.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C15.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C13.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	/Users/JK/AppData/Local/Temp/WER6C27.tmp.cab.tmp (deleted)
09/19/2012	22:40:15	MACB	NTFS $MFT	**/Windows/Prefetch/X.EXE-CB615E65.pf**
09/19/2012	22:40:16	MACB	NTUSER key	Key name: HKEY_USER/CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}/Software/Microsoft/Windows/WindowsErrorReporting
09/19/2012	22:40:16	MAC.	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive
09/19/2012	22:40:16	MACB	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive/**AppCrash_x.exe_c598da7B4abfeeaa78a28a697595ebb2f4f7a43_cab_095c6e9a/Report.wer**
09/19/2012	22:40:16	MACB	NTFS $MFT	/ProgramData/Microsoft/Windows/WER/ReportArchive/AppCrash_x.exe_c598da784abfeeaa78a28a697595ebb2f4f7a43_cab_095c6e9a
09/19/2012	22:40:16	MACB	NTFS $MFT	**/Windows/Prefetch/WERFAULT.EXE-37549B7E.pf**
09/19/2012	22:40:16	MAC.	NTFS $MFT	/Windows/Prefetch
09/19/2012	22:40:16	MAC.	NTFS $MFT	/Users/JK/AppData/Local/Temp
09/19/2012	22:40:23	M.C.	NTFS $MFT	**/Windows/Prefetch/SVCHOST.EXE-80F4A784.pf**
09/19/2012	22:40:41	M.C.	NTFS $MFT	/Windows/System32/wbem/Repository/OBJECT~1.DAT
09/19/2012	22:40:41	M.C.	NTFS $MFT	/Windows/System32/wbem/Repository/INDEX.BTR

Kevin's Attic for Security Research

- Why Information Security Fails Often in Korea? (1)
- Why Information Security Fails Often in Korea? (2)
- Global IP Finder using GeoIP for fun

Android Pin/Password Cracking

- 안드로이드 PIN/Password 공격 복잡도

An In-Depth Look Into Data Stacking (1/3)

- **Data Stacking?**

비이상적인 데이터를 분리/확인하기 위해 유사한 데이터의 대용량 볼륨에서 수행하는 빈도 분석 기법으로 모래밭에서 바늘을 찾는 조사 기법이다. 큰 볼륨 데이터에서 불필요하거나 관리적인 데이터를 제거해나가는 반복적인 작업이다.

- 맨디언트 ➔ 수백~수천의 호스트로 이루어진 큰 조직을 조사
  - ✓ 처리되지 않은 데이터를 줄이는 작업인 데이터 스태킹이 필요
  - ✓ 알려지지 않은 악성코드를 발견하기 위해 데이터 스태킹 사용
  - ✓ IOC (Indicator of Compromise) 사용
- 데이터 스태킹 4단계

단계	행위	검토가 필요한 열
1	호스트에서 데이터 획득	수백만
2	독특한 열을 생성하기 위해 데이터를 그룹화	수만 ~ 수십만
3	세부 특성과 계산에 기반해 열을 그룹화	수백 ~ 수천
4	비정상적인 흔적 탐지	백 이하

An In-Depth Look Into Data Stacking (2/3)

- **Data Stacking?**
  - 1단계
    - ✓ 가능한 환경 내에서 많은 호스트를 대상으로 데이터 획득 (MIR, Mandiant Intelligent Response)
  - 2단계
    - ✓ 데이터를 특성 별로 쌓음
  - 3단계
    - ✓ 속성별로 다양한 그룹화
    - ✓ 세부 항목이나 빈도를 기준으로 분류
    - ✓ 추가 조사가 필요한 속성 집합을 만듦

ServiceItem Attributes:

```
name
descriptiveName
description
mode
startedAs
path
arguments
serviceDLL
status
pid
type
pathmd5sum
pathsha1sum
pathsha256sum
pathSignatureExists
pathSignatureVerified
pathSignatureDescription
pathCertificateSubject
pathCertificateIssuer
serviceDLLmd5sum
serviceDLLsha1sum
serviceDLLsha256sum
serviceDLLCertificateSubject
serviceDLLCertificateIssuer
serviceDLLSignatureExists
serviceDLLSignatureVerified
serviceDLLSignatureDescription
```

SerivceItem Attributes:

```
name
descriptiveName
path
serviceDLL
pathmd5sum
serviceDLLmd5sum
```

An In-Depth Look Into Data Stacking (3/3)

- **Data Stacking?**
  - 4단계

✓ 비정상적인 흔적을 살펴봄 ➔ 지루한 작업

Count	Service Name	Path	Service DLL
5598	Seclogon	system32\svchost.exe	system32\sedogon.dll
2	Seclogon	system32\svchost.exe	system32\selogon.dll
5235	iprip	system32\svchost.exe	system32\iprip.dll
2	iprip	system32\svchost.exe	system32\iprinp.dll
3	iprip	system32\svchost.exe	temp\iprip.dll

Count	Service Name	Path	Path MD5
1	psexec	windows\psexesvc.exe	16c19f597b338f81729b88032b3a7255
1	psexec	windows\psexesvc.exe	f558d98b5679be09b36c503c7663df26
1	psexec	system32\psexesvc.exe	077c0ce3571e4a8c7e849642df1a4b7e

Count	Service Name	Service DLL	Service DLL Signature Verified	MD5
2	Bits	qmgr.dll	true	6bed1...
13	Bits	qmgr.dll	true	0a83d...
1	Bits	qmgr.dll	false	d3147...
65	Bits	qmgr.dll	true	151dc...

Finding An Infection Vector After IT Cleaned the System

- **시스템 관리자의 대응 후에도 남아있는 시스템 흔적**
  - **보통 관리자의 문제 해결 방법**
    - ✓ McAfee 백신 스캔
    - ✓ 모든 임시 폴더/프리패치/시스템 복원 지점 삭제
    - ✓ 모든 휴지통 비우기
    - ✓ Avast! 설치 후 스캔
  - **이후에도 남는 잠재적인 흔적**
    - ✓ Host Based Logs – AV Logs
    - ✓ NTFS Artifact
    - ✓ Registry Artifacts
    - ✓ System Timeline

Finding An Infection Vector After IT Cleaned the System

- **시스템 관리자의 대응 후에도 남아있는 시스템 흔적**
  - **보통 관리자의 문제 해결 방법**
    - ✓ McAfee 백신 스캔
    - ✓ 모든 임시 폴더/프리패치/시스템 복원 지점 삭제
    - ✓ 모든 휴지통 비우기
    - ✓ Avast! 설치 후 스캔
  - **이후에도 남는 잠재적인 흔적**
    - ✓ Host Based Logs – AV Logs
    - ✓ NTFS Artifact
    - ✓ Registry Artifacts
    - ✓ System Timeline

Windows Memory Forensics Training for Analysts by Volatility Developers

- **볼라틸리티 교육 프로그램**
  - 볼라틸리티 개발자가 교육
  - 5일 코스 (자료, 점심, 커피 제공)
  - 사전 구성된 개인 노트북 지참
    - ✓ 하드웨어 : CPU 2.0 GHz, 4GB RAM, 20 GB Disk, DVD-ROM, USB 2.0, Wireless NIC
    - ✓ 소프트웨어 : Python 2.6/2.7, MS Windows Debugger, VMWare, 7-zip, Wireshark
  - 비용 : $3500 (한화 370 만원)

Raising Your Public Profile as an Information Security Professional

- **정보보호 전문가로서 명성을 높이는 방법**

1. **SNS를 활용** ➔ 단순히 새로운 아티클 링크 X, 실명 사용, 다음 단계의 내용을 적용
2. **공개/사적인 메일링 리스트에 가입** ➔ 정보보호 관련 다양한 메일링 리스트
3. **정기적인 블로그 포스팅** ➔ 트위터의 시대에서 꾸준한 블로깅은 어려움
4. **백서 작성** ➔ 자신의 이름을 사용해 특정 주제에 대한 백서 작성 또는 매거진 기고
5. **CFP에 반응** ➔ 자신이 없다면 작은 이벤트 부터 시작
6. **좋은 책 쓰기** ➔ 나쁜 책은 오히려 안 쓰니만 못할 수도…
7. **오픈소스 소프트웨어 개발/참여**

Unacceptable Acceptable Use Policy

- **AUP의 문제점**
  - 사용자에게 정보를 알리기 위한 목적이기 보다는 의무적으로 공개 ➔ 내용과 구성이 지루함
  - 자신의 경험을 미루어 AUP를 개선한 결과, 상당한 양의 불필요한 내용 제거

> Hi. Welcome to Organisation.
>
> We take Information Security and the use of our systems very seriously - to this end, there are a few things that we'd really like you to agree to do when using any of the company computer systems.
>
> Please choose a good password, a mix of letters and numbers, both lower and upper case are good. Remembering a good password can be difficult, but as a help, you might like to try using a consonant vowel consonant sequence to make it pronounceable - bogdotfan - and then add a number - bogdotfan25 and then mix it up with some upper case - bOgDotfAn25. Please do change the password when requested by the system, and do use a completely new one each and every time. Do protect the password - it is part of what identifies you on the system, and, when it is entered any and all action taken when using it will be assumed to be yours.
>
> Do turn your laptop off when you are in transit - the encryption doesn't work if the device has been left on or in standby.
>
> Please help us to reduce the risk of malware or data loss by using only officially issued, encrypted USB devices in your company laptop or desktop.
>
> … …

Use of a Hammer and of Wiping Software to Destroy Evidence Results in Dismissal of Plaintiff's Claims (1/2)

- **증거를 완전삭제하고 망치로 훼손한 행위에 대한 판례**
  - 2009년 원고는 "피고인에 대한 자신의 예상 청구"와 관련하여 변호사 고용
  - 변호사는 원고가 한 문서 변조 행위에 대해 경고 ➔ 원고는 다른 변호사 고용
  - 원고는 업무상 데스크톱 컴퓨터 사용
  - 2010~2011경 데스크톱이 맛이 가서 ➔ 백업 시도 ➔ 제한적인 성공 (아내 의료 정보 복구)
  - 새로운 노트북으로 내용 전송 ➔ 데스크톱과 하드 교체
  - 이 당시, 데스크톱 컴퓨터를 망치로 부수고 쓰레기 매립지에 묻음 ➔ 부인 안함
  - 2011년 원고는 CCleaner가 설치된 노트북 지급 받음
  - CCleaner 백업 복원 과정에서 설치됐다고 주장
  - 법원은 조사를 명령

Use of a Hammer and of Wiping Software to Destroy Evidence Results in Dismissal of Plaintiff's Claims (2/2)

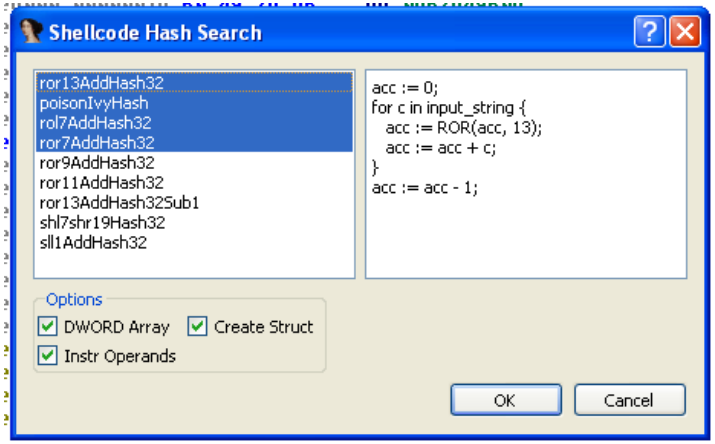
- **증거를 완전삭제하고 망치로 훼손한 행위에 대한 판례**
  - 원고가 변호사에게 보낸 메일에서 원고의 불만과 그의 행위에 대한 흔적을 찾음
  - 또 다른 흔적
    - ✓ 법원 조사 명령을 받은 후 곧바로 Evidence Eliminator 다운
    - ✓ 프로그램은 적어도 1번, 아마도 3번 실행
    - ✓ CCleaner에 의해 최소 16,000 파일이 삭제됨
  - 법원은 변호사와 주고 받은 메일과 시스템 흔적을 기반으로 원고의 주장을 기각
    - ✓ 피고의 합리적인 변호사 수임료와 비용을 보상
    - ✓ 징벌적 금전적 제제는 하지 않음

Court Adopt New E-Discovery Guidelines Effective November 27, 2012

- **캘리포이나 북부 지방 법원에서 전자증거개시와 관련한 새로운 가이드라인 공개**
  - 새로운 ESI 관련 문서
    - ✓ Guidelines for the Discovery of Electronically Stored Information;
    - ✓ ESI checklist for use during the Rule 26(f) meet and confer process;
    - ✓ Model Stipulated Order Re: the Discovery of Electronically Stored Information.
    - ✓ Standing Order for All Judges of the Northern District of California

Using Precalculated String Hashes when Reverse Engineering Shellcode

- **쉘코드 리버싱**
  - 쉘코드 제작자는 API 함수 길이의 제한과 같은 크기 제한에 직면
  - 보통 특정 해시를 이용하여 함수 이름을 줄임
  - 알려진 해시를 이용해 API 함수 이름을 미리 계산
  - 이를 이용해 임포트/익스포트 함수 판단
  - IDA 스크립트 공개




```
seg000:00000002 sub     esp, 17Ch
seg000:00000008 call    sub_17B
seg000:00000008 ; ---------------------------------------------------------
seg000:0000000D dd 0EC0E4E8Eh   ; kernel32.dll!LoadLibraryA
seg000:00000011 dd 16B3FE72h    ; kernel32.dll!CreateProcessA
seg000:00000015 dd 78B5B983h    ; kernel32.dll!TerminateProcess
seg000:00000019 dd 7B8F17E6h    ; kernel32.dll!GetCurrentProcess
seg000:0000001D dd 5B8ACA33h    ; kernel32.dll!GetTempPathA
seg000:00000021 dd 0BFC7034Fh   ; kernel32.dll!SetCurrentDirectoryA
seg000:00000025 dd 7C0017A5h    ; kernel32.dll!CreateFileA
seg000:00000029 dd 0DF7D9BADh   ; kernel32.dll!GetFileSize
seg000:0000002D dd 76DA08ACh    ; kernel32.dll!SetFilePointer
seg000:00000031 dd 10FA6516h    ; kernel32.dll!ReadFile
seg000:00000035 dd 0E80A791Fh   ; kernel32.dll!WriteFile
seg000:00000039 dd 0FFD97FBh    ; kernel32.dll!CloseHandle
seg000:0000003D dd 0C0397ECh    ; kernel32.dll!GlobalAlloc
seg000:00000041 dd 7CB922F6h    ; kernel32.dll!GlobalFree
seg000:00000045 dd 1BE1BB5Eh    ; shell32.dll!ShellExecuteA
```

```
seg000:000002BF sub_2BF proc near ; CODE XREF: sub_2BF:loc_364↓p
seg000:000002BF pop     ebx
seg000:000002C0 call    sub_29E
seg000:000002C5 mov     edx, eax
seg000:000002C7 push    0EC0E4E8Eh ; kernel32.dll!LoadLibraryA
seg000:000002CC push    edx
seg000:000002CD call    sub_252
seg000:000002D2 mov     [ebp-4], eax
seg000:000002D5 push    0B8E579C1h ; kernel32.dll!GetSystemDirectoryA
seg000:000002DA push    edx
seg000:000002DB call    sub_252
seg000:000002E0 mov     [ebp-8], eax
seg000:000002E3 push    78B5B983h ; kernel32.dll!TerminateProcess
seg000:000002E8 push    edx
seg000:000002E9 call    sub_252
seg000:000002EE mov     [ebp-0Ch], eax
seg000:000002F1 push    7B8F17E6h ; kernel32.dll!GetCurrentProcess
seg000:000002F6 push    edx
seg000:000002F7 call    sub_252
```

Others

- **Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds**
  - 분산처리에 기반한 Blacksheep 으로 감염과 0-day를 탐지할 수 있다는 내용의 논문
- **Tracing UDP Backdoor Activity on MacOS X**
  - Dtrace를 이용해 MacOS X에서 동작 중인 UDP 백도어를 탐지/추적하는 내용
- **A technical analysis on new Java vulnerability (CVE-2012-5076)**
  - 새로운 자바 취약점인 CVE-2012-5076의 기술적인 분석 내용
- **Deobfuscating Blackhole V2 HTML pages with Python**
  - Blackhole v2 HTML 페이지의 난독화를 푼 내용을 간단히 소개
- **64-bit Linux rootkit injecting iframes into web page**
  - 웹 페이지에 iframe을 삽입하는 64비트 기반 루트킷 분석 내용

Others

- **AxCrypt Artifacts**
  - 윈도우의 오픈소스 파일 암호화 소프트웨어인 AxCrypt의 아티팩트 ➔ 아티팩트 뱅크 (?)
- **S.C. tax breach began when employee fell for spear phishing**
  - 사우스 캐롤라이나 국세청이 스피어 피싱으로 인해 수백만건의 사회보장번호와 개인정보가 유출됨 ➔ 이에 대한 맨디언트의 보고서를 확인할 수 있음
- **ICLOUD (IN)SECURITY – EXAMINING IOS DATA BACKED UP IN THE CLOUD**
  - iOS 에 대한 기본적인 포렌식 방법과 iCloud 와의 통신 방식을 소개
- **Proactive detection of security incidents II - honypots**
  - ENISA(European Network and Information Security Agency)에서 작년이 이어 공개한 [네트워크 보안 사고 사전 탐지]와 관련한 보고서

Forensics Tools

- **Memoryze** for the Mac: Support Added for OS X Mountain Lion (10.8)
- **VMInjector** – DLL Injection tool to unlock guest VMs
- **Nmap** 6.25 holiday season relased!
- **OllyDbg** 2.01 Updated – sample plugins, preliminary plugin API, test application
- **Tableau Imager** Enhancements and Bug Fixes
- **BAREF** – Browser Artifact Recovery Forensic Framework
- **python-oldtools**, phtyon tools to analyze OLE files
- **Google Analytics Cookie Parser**
- **AnalyzePESig** Updated!
- **Bulk_extractor** 1.3.1 updated!

Question and Answer