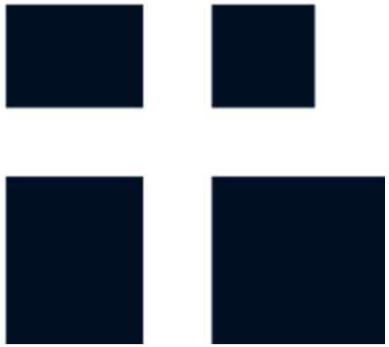
Malware Tracker?



JK Kim

(at)pr0neer

forensic-proof.com

Proneer(at)gmail.com

개요

1. 침해사고 감염 유형

2. 침해사고 포렌식 분석

침해사고 감염 유형

침해사고 감염 유형

- **침해사고 감염 유형**

1. **웹**을 통한 감염
2. **웹하드**를 통한 감염
3. **이메일**을 통한 감염
4. **외장저장장치**를 통한 감염
5. **업데이트 서버**를 통한 감염
6. **… …**

➔ **모든 감염 유형은 APT 또는 TT의 시작이 될 수 있음!!**

- **APT –** Advanced Persistent Threat
- **TT –** Targeted Threat

침해사고 감염 유형

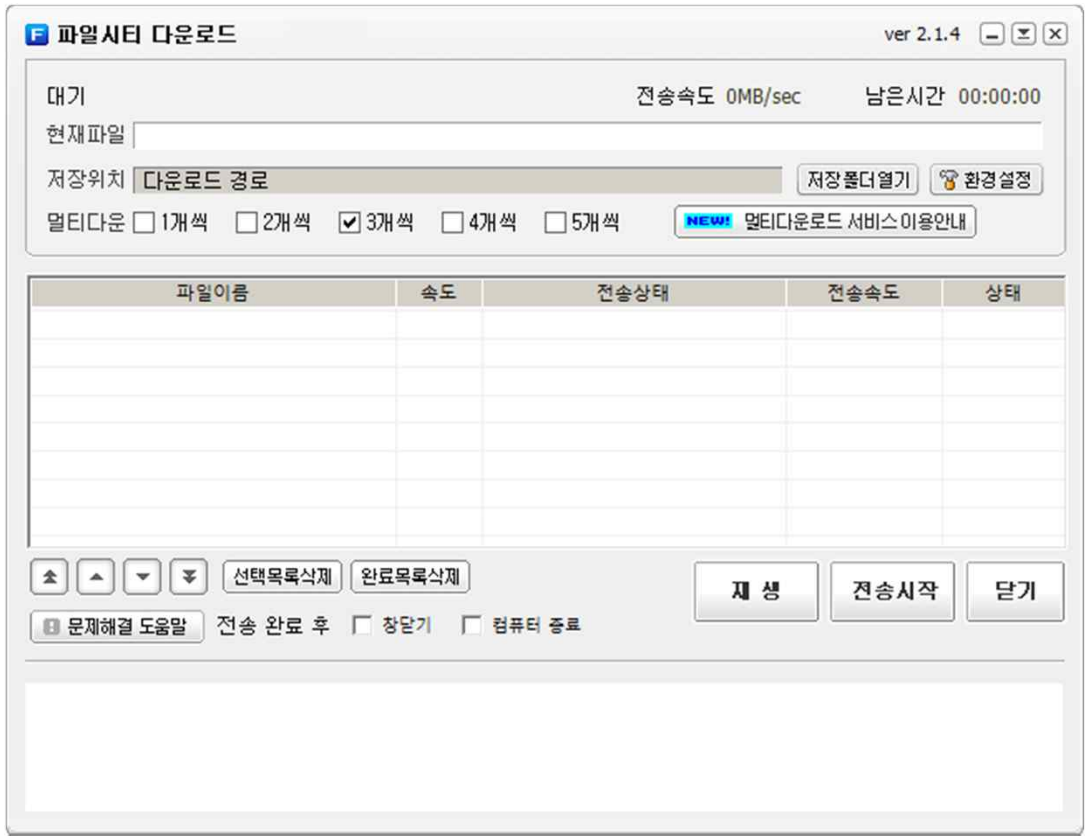
1. 웹을 통한 감염

- 웹 브라우저/웹 애플리케이션/보안 애플리케이션 취약점 악용
- 악성코드 은닉 사이트 접속 유도
- 악성 ActiveX, 자바 애플릿 설치 유도
- 확장자 변조 악성 파일 다운 유도
- 짧은 URL(goo.gl, bitly. tynyURL, mcaf.ee 등)을 이용한 클릭 유도

침해사고 감염 유형

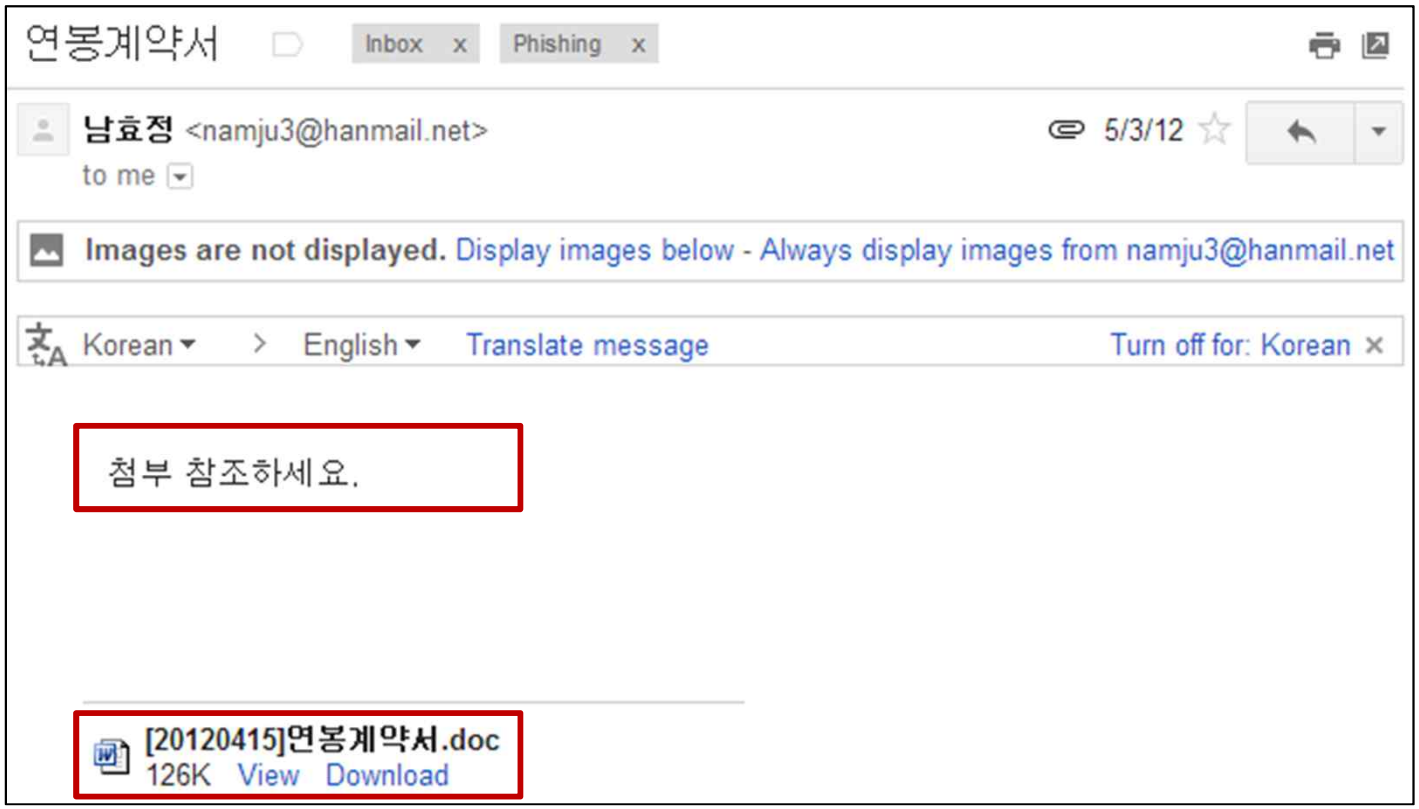
2. 웹하드를 통한 감염

- 7.7 DDoS, 3.4 DDoS, 6.25 사이버테러의 원인
- 다운로드 매니저 교체
- 악성 파일 다운 유도



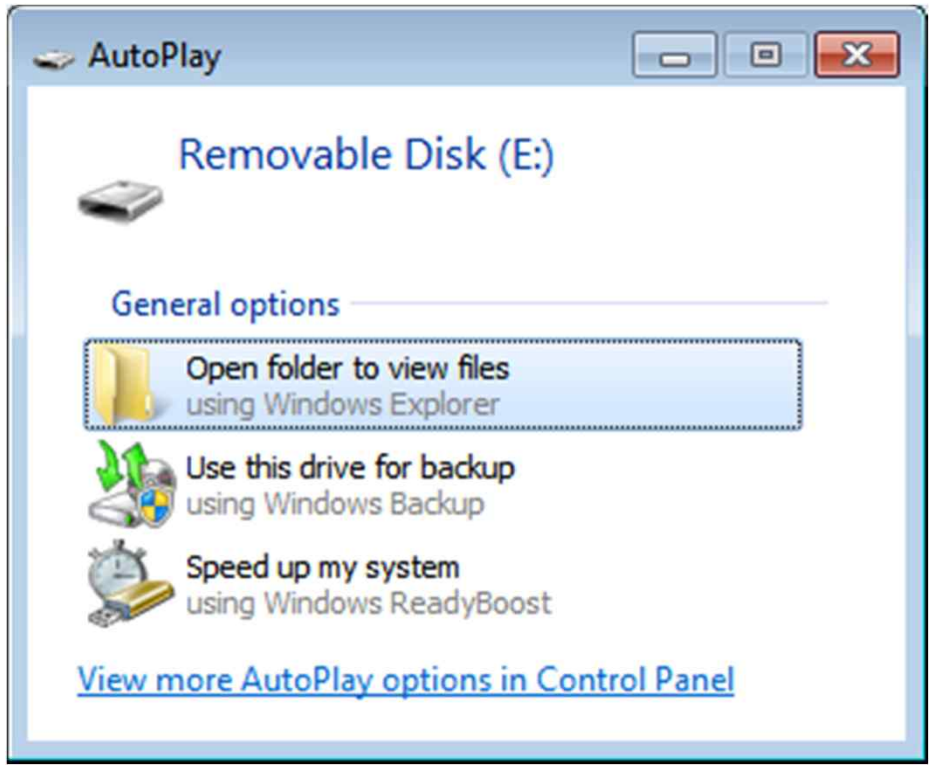
3. 이메일을 통한 감염

- 사회적 관심사, 정기 메일 등의 형식을 이용한 스피어 피싱 메일 발송
- 악성 사이트 접속 유도
- 악성 첨부파일 실행 유도



4. 외장저장장치를 통한 감염

- 국가 기간망(스턱스넷, 듀크, 플레임)과 같이 폐쇄망을 타겟
- 농협 전산망 마비와 같이 내부 시스템 감염을 위해 사용
- 우연히 습득한 저장장치?



침해사고 감염 유형

5. 업데이트 서버를 통한 감염

- 대형 개인정보 유출사고와 기밀 유출 사고의 원인
- 주로 애플리케이션 개발사에서 운용 ➔ 최근 자체적으로 내부 업데이트 서버를 유지
- 기업 내부로 침투할 수 있는 가장 효과적인 방법
- 업데이트 서버의 설정을 조작하여 특정 기업만 침투하기도 함
- 대상 기업의 보안성 >> 업데이트 서버의 보안성

침해사고 감염 유형

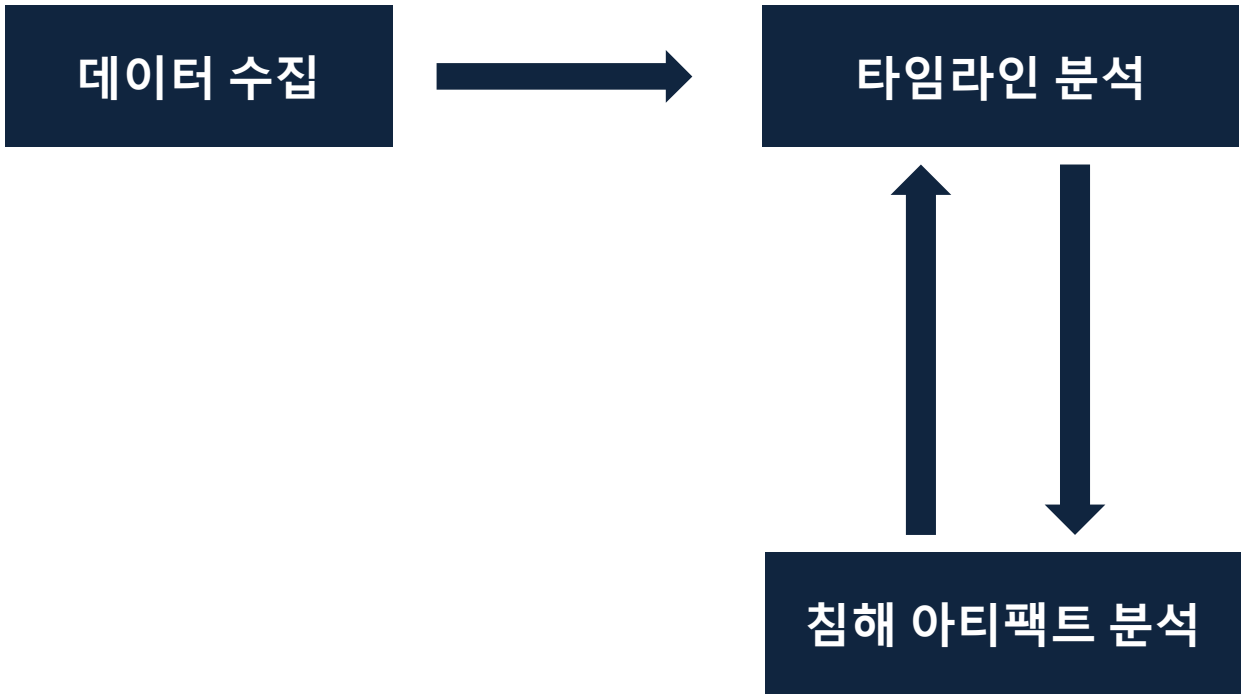
6. … …

- 그 밖의 감염 유형은?
- 감염 유형을 정형화할 수 있는가?

침해사고 포렌식 분석

침해사고 포렌식 분석

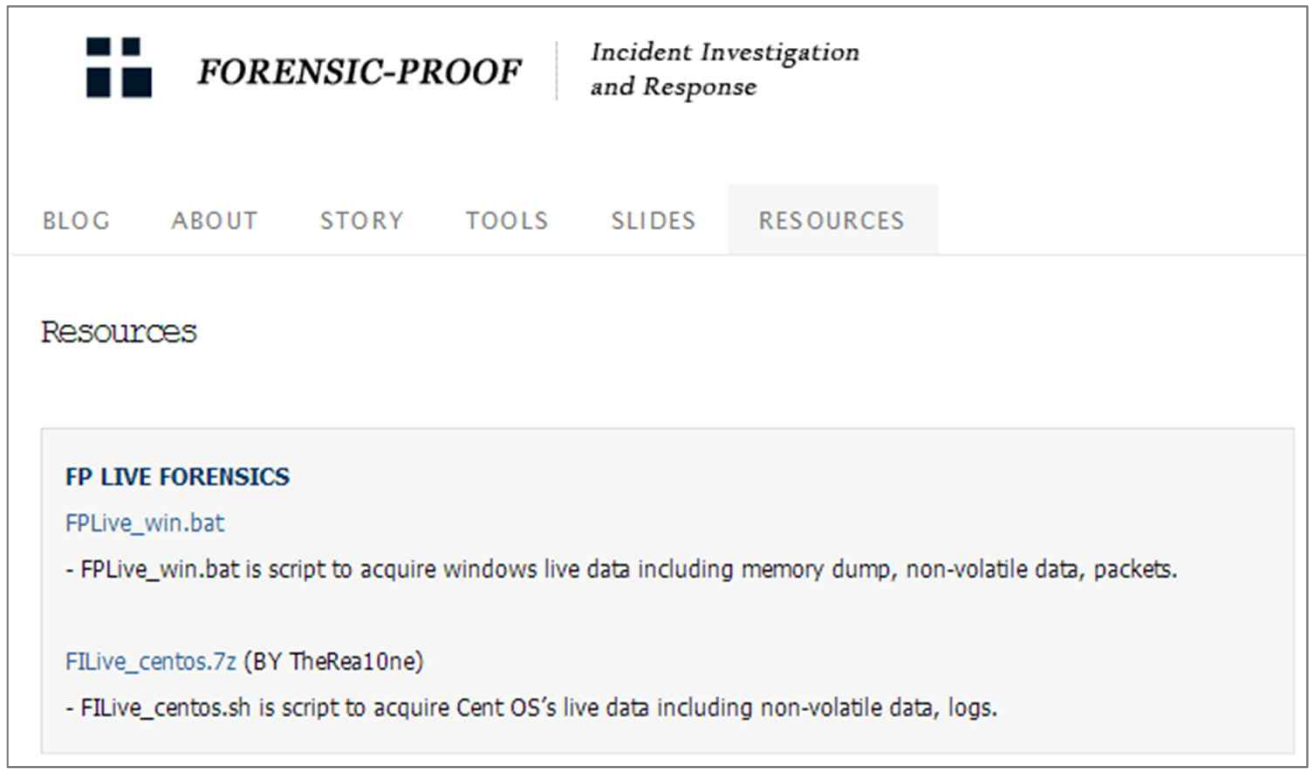
- 일반적인 분석 절차



- **데이터 수집**

1) 수집 스크립트를 이용한 라이브 데이터 수집

- ✓ 활성 데이터
- ✓ 물리 메모리
- ✓ 비활성 데이터
- ✓ 네트워크 패킷



▪ 데이터 수집

2) 선별 데이터 복사

- ✓ 이미징이 불가능한 경우 상황에 따라 주요 포렌식 분석 데이터만 선별 추출
- ✓ 단순 복사나 전문 복사 도구(forecopy, robocopy 등) 이용

3) 저장장치 복제/이미징

- ✓ 일반적으로 복제가 이미징보다 빠름
- ✓ 증거 분배나 분석 효율을 위해 최종 분석 작업은 이미징 후 수행
- ✓ 온라인 이미징일 경우, 공개된 무료 도구(FTK Imager, dd + netcat 등) 사용
- ✓ 오프라인 이미징일 경우, 속도나 안전성의 이유로 전문 장비 이용

- **타임라인 분석**

1) 시간 정보를 포함한 다양한 포렌식 아티팩트 추출
2) 추출된 아티팩트를 시간 정보를 기준으로 정형화
3) 시간 순으로 정렬 후 특정 시간 대에 일어난 흔적 분석

FILE OPENING
WEB HISTORY
DELETED DATA
EXECUTION
DEVICE or USB USAGE
FOLDER OPENING
LOG FILE

date_time	MACB	sourcetype	type	user	desc
2013-05-16 13:00:57	M.C.	NTFS $MFT	$SI [M.C.] time	-	/Users/lee/AppData/LocalLow/naver/SafeGuard/Data/nSafeGuard_20130516_130041_4540.dat
2013-05-16 13:00:57	MACB	System	Event Logged	-	System/Service Control Manager ID [7036] :EventData/Data -> param1 = Windows Media Player Network Sharing Service param2 = 실행 - EventData/Binary -> 57004D0050004E006500740077006F0072006B00530076006300 2F0034000000
2013-05-16 13:00:57	MACB	System	Event Logged	-	System/WMPNetworkSvc ID [14204] :EventData/Data -> ServiceName = WMPNetworkSvc
2013-05-16 13:00:58	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [3] :EventData/Data -> string = {AC76BA86-1042-0000-7760-000000000004} string2 = lee-PC/lee string3 =
2013-05-16 13:01:03	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [59] :EventData/Data -> transferId = {1788EA0F-F6F4-490B-8B67-B5458C61031C} name = {AC76BA86-1042-0000-7760-000000000004} Id = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} url = https://armmf.adobe.com/arm-updates/win/ARM/1.7.4/ARM_1740.msi peer = fileTime = 1368275311 fileLength = 373760 bytesTotal = 373760 bytesTransferred = 0 bytesTransferredFromPeer = 0
2013-05-16 13:01:05	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-HomeGroup Provider Service/Operational/Microsoft-Windows-HomeGroup-ProviderService ID [5013] :EventData/Data -> OldStatus = 4 NewStatus = 132
2013-05-16 13:01:07	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [60] :EventData/Data -> transferId = {1788EA0F-F6F4-490B-8B67-B5458C61031C} name = {AC76BA86-1042-0000-7760-000000000004} Id = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} url = https://armmf.adobe.com/arm-updates/win/ARM/1.7.4/ARM_1740.msi peer = hr = 0 fileTime = 1368275311 fileLength = 373760 bytesTotal = 373760 bytesTransferred = 373760 proxy = peerProtocolFlags = 0 bytesTransferredFromPeer = 0 AdditionalInfoHr = 0 PeerContextInfo = 0 bandwidthLimit = 18446744073709551615 ignoreBandwidthLimitsOnLan = false
2013-05-16 13:01:07	MACB	System	Event Logged	-	System/Service Control Manager ID [7036] :EventData/Data -> param1 = Multimedia Class Scheduler param2 = 실행 - EventData/Binary -> 4D004D0043005300530053002F0034000000
2013-05-16 13:01:09	..C.	NTFS $MFT	$FN [..C.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/ARM.msi
2013-05-16 13:01:09	..C.	NTFS $MFT	$SI [..C.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/ARM.msi
2013-05-16 13:01:09	MACB	Microsoft-Wi	Event Logged	-	Microsoft-Windows-Bits-Client/Operational/Microsoft-Windows-Bits-Client ID [4] :EventData/Data -> User = lee-PC/lee jobTitle = {AC76BA86-1042-0000-7760-000000000004} jobId = {2A0ED9C0-9F6E-4C08-8B58-4AA4BCFB7EE2} jobOwner = lee-PC/lee fileCount = 1 bytesTransferred = 373760 bytesTransferredFromPeer = 0
2013-05-16 13:01:13	.A.B	NTFS $MFT	$FN [MACB] time	-	/Windows/Prefetch/NVTRAY.EXE-39D19720.pf
2013-05-16 13:01:13	.A.B	NTFS $MFT	$SI [.A.B] time	-	/Windows/Prefetch/NVTRAY.EXE-39D19720.pf
2013-05-16 13:01:17	..C.	NTFS $MFT	$SI [..C.] time	-	/Program Files (x86)/Common Files/Adobe/ARM/1.0/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AcrobatUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARM.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$FN [MACB] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/ReaderUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AcrobatUpdater.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARM.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/AdobeARMHelper.exe
2013-05-16 13:01:17	.AC.	NTFS $MFT	$SI [.AC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/380/ReaderUpdater.exe
2013-05-16 13:01:17	MAC.	NTFS $MFT	$FN [MAC.] time	-	/ProgramData/Adobe/Acrobat/9.2/ARM/AdobeARM.bin

▪ 타임라인 분석

• 타임라인 분석을 왜 하는가?

✓ 특정 이벤트 발생 시점 전, 후로 시스템 상에서 어떤 일이 발생했는지 쉽게 파악 가능

✓ 정밀 분석 대상을 빠르게 선별 가능

• 시점을 알고 있는 경우

✓ 타임라인 추출 후 해당 시점을 기준으로 분석

• 시점을 모르는 경우

✓ 다양한 침해 아티팩트를 분석하여 관련 시점 획득

▪ 타임라인 분석

• 시간 정보를 포함하는 윈도우 아티팩트

- ✓ 파일시스템 메타데이터 (FAT=3, NTFS=8)
- ✓ 프리패치 파일 생성 시간, 내부 최종 실행 시간
- ✓ 레지스트리 키의 마지막 기록 시간
- ✓ 이벤트 로그의 이벤트 생성/작성 시간
- ✓ 바로가기 파일의 생성/수정/접근 시간과 바로가기 대상의 생성/수정/접근 시간
- ✓ IIS, FTP, MS-SQL Error, AV 로그 등의 시간 정보
- ✓ 웹 브라우저 사용 흔적의 방문/수정/접근/만료/다운로드 시간
- ✓ 시스템 복원 지점과 볼륨 섀도 복사본의 파일시스템 시간 정보
- ✓ PE 파일의 컴파일 시간
- ✓ 휴지통의 삭제된 시간
- ✓ JPEG EXIF의 사진 촬영 시간
- ✓ … …

- **침해 아티팩트 분석 (윈도우 환경의 클라이언트 분석 관점)**

1. 침해 유입 아티팩트
2. 침해 실행 아티팩트
3. 침해 지속 아티팩트

1. 침해 유입 아티팩트

- 웹 브라우저 아티팩트
- 자바 IDX
- 이메일 아티팩트
- 외부저장장치 아티팩트
- AV 로그
- 방화벽 로그
- 이벤트 로그

2. 침해 실행 아티팩트

- 프리패치
- 파일시스템 로그
- 바로가기
- 점프 목록
- 레지스트리
- 볼륨 섀도 복사본
- 응용프로그램 호환성 캐시
- WoW64
- 윈도우 문제 보고
- 이벤트 로그

3. 침해 지속 아티팩트

- 루트킷
- 악성코드 선호 경로
- 비정상 파일
- 슬랙 공간
- 시간 조작
- 자동 실행 목록
- 작업 스케줄러
- 이벤트 로그

- **어려운 점**
  - 고급 안티포렌식 기법의 일반화
  - 다양한 취약점 및 악성코드 기법
  - 미흡한 침해사고 준비도
  - 미흡한 초기 대응
  - 평시 일어나는 침해 이벤트에 대해 무감각
  - 대용량 데이터 분석
  - 결과를 통한 시너지 부족

요구 사항

- 디지털포렌식 기술의 꽃!!
- 운영체제에 대한 폭넓은 이해
- 다양한 환경 및 기술에 대해 깊은 이해보다 폭넓은 이해 필요
- 급변하는 취약점 혹은 악성코드 기법에 대한 정보를 주기적으로 모니터링
- 다양한 침해사고나 가상 케이스에 대한 많은 경험이 반드시 필요
- 두 명 이상의 종합적이고 객관적인 판단
- 상시 분석이 가능한 침해사고 분석 인력 필요
- 침해사고 준비도를 갖추자!!

질문 및 답변