윈도우 아티팩트 수집 툴 설명

■ 데이터 수집 절차

1. 수집 데이터 목록

휘발성 데이터

항목	수집 도구	항목	수집 도구	항목	수집 도구
물리 메모리 이미지	winpmem	**네트워크 세션**	netstat, urlprotocolview	**ARP**	arp
프로세스	pslist	**TCP/IP 오픈 포트**	netstat	**라우팅**	route
서비스	tasklist	**로그온**	logonsessions	**시스템기본정보**	systeminfo
드라이버	listdrivers	**계정 및 그룹**	net	**설치 목록**	wul,psinfo
네트워크	ipconfig, promiscdetect	**공유 자원**	net	**자동 실행**	autorunsc
로컬 세션	net	**NetBIOS**	nbtstat	**파이프**	piplist

비 휘발성 데이터

항목	수집도구	항목	수집도구
레지스트리	Forecopy_handy	**Web addon**	browseraddonsview
프리패치	Forecopy_handy	**Web history**	Browsinghistoryview
$UsnJrnl	Forecopy_handy	**Web down**	browserdownloadview
이벤트로그	Forecopy_handy	**WER**	Robocopy
$LogFile	Forecopy_handy	**바로가기**	Robocopy
VBR	Forecopy_handy	**SRUM**	Robocopy
VSC	Shadowcopyview	**윈도우 타임라인**	Robocopy
MFT	Forecopy_handy	**시스템캐시**	Xcopy
작업관리자	taskschedulerview		

2. 휘발성 데이터 수집 순서

Number	휘발성 데이터	Number	휘발성 데이터
1	물리 메모리 이미지	**9**	계정 및 그룹
2	프로세스	**10**	공유자원
3	네트워크 세션	**11**	NetBios
4	로컬세션	**12**	ARP
5	드라이버	**13**	라우팅
6	서비스	**14**	설치목록
7	TCP/IP open port	**15**	자동실행
8	Logon	**16**	파이프

3. 각 도구별 아티팩트 수집 데이터 종류

□ 물리 메모리 이미지

명령	설명	출력
winpmem.exe	프로세스의 메모리 사용량을 그래픽으로 표시	프로세스 이름, 프로세스 ID, 총 메모리 사용량, 사용 중인 메모리 및 페이징된 메모리

□ 프로세스

명령	설명	출력
pslist.exe	컴퓨터에서 실행 중인 모든 프로세스를 나타냄	프로세스 ID, 프로세스 이름, 사용자 이름, CPU 사용량, 메모리 사용량 및 시작 시간
cprocess.exe	컴퓨터에서 실행 중인 모든 프로세스를 나열하고 각 프로세스의 세부 정보를 제공	프로세스 ID, 프로세스 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간 및 실행 파일 경로
procinterrogate.exe -list -md5 -ver -o	컴퓨터에서 실행 중인 모든 프로세스의 세부 정보를 나열하고 각 프로세스의 MD5 해시, 버전 및 오프라인 덤프 여부를 제공	프로세스 ID, 프로세스 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간, 실행 파일 경로, MD5 해시, 버전 및 오프라인 분석 덤프 여부
tasklist.exe -V	컴퓨터에서 실행 중인 모든 작업을 나열하고 각 작업의 세부 정보를 제공	작업 ID, 작업 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간 및 실행 파일 경로
tlist.exe -t	컴퓨터에서 실행 중인 모든 작업을 나열하고 각 작업의 CPU 사용량을 그래픽으로 표시	작업 ID, 작업 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간 및 실행 파일 경로
pslist.exe -t	컴퓨터에서 실행 중인 모든 프로세스를 나열하고 각 프로세스의 CPU 사용량을 그래픽으로 표시	프로세스 ID, 프로세스 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간 및 실행 파일 경로
handle.exe -a	컴퓨터에서 열린 모든 핸들을 나타냄	핸들 ID, 핸들 이름, 프로세스 ID, 프로세스 이름 및 해당 핸들이 열려 있는 파일 또는 장치의 경로

openedfilesview.exe	컴퓨터에서 열린 모든 파일을 나타냄	파일 이름, 파일 경로, 프로세스 ID, 프로세스 이름 및 해당 파일이 열려 있는 프로세스의 사용자 이름
listobj.exe	컴퓨터에서 열린 모든 개체를 나타냄	개체 이름, 개체 경로, 프로세스 ID, 프로세스 이름 및 해당 개체가 열려 있는 프로세스의 사용자 이름
tlist -c	컴퓨터에서 실행 중인 모든 작업의 CPU 사용량을 합산한 그래픽을 표시해 줌	작업 ID, 작업 이름, 사용자 이름, CPU 사용량, 메모리 사용량, 시작 시간 및 실행 파일 경로
listdlls.exe	컴퓨터에서 로드된 모든 DLL을 나타냄	DLL 이름, DLL 경로, 프로세스 ID 및 프로세스 이름
dllexp.exe	컴퓨터에서 로드된 특정 DLL의 함수 목록을 표시	함수 이름, 함수 주소 및 함수 설명
injecteddll.exe	컴퓨터의 프로세스에 삽입된 모든 DLL을 나타냄	DLL 이름, DLL 경로, 프로세스 ID 및 프로세스 이름

□ 서비스

명령	설명	출력
tasklist.exe -svc	실행 중인 서비스 목록을 생성	서비스 이름, PID 및 상태 목록.
tasklist.exe -apps	실행 중인 응용 프로그램 목록을 생성	응용 프로그램 이름, PID 및 상태 목록.
psservice.exe	실행 중인 서비스 목록을 생성	서비스 이름, 상태 및 설명
tlist.exe -s	실행 중인 프로세스 목록을 생성	프로세스 이름, PID, CPU 사용량 및 메모리 사용량

□ 드라이버

명령	설명	출력
driverview.exe	컴퓨터에 설치된 모든 드라이버에 대한 정보를 나열	드라이버 이름, 드라이버 설명, 드라이버 버전 및 드라이버가 로드된 위치.
listdrivers.exe	컴퓨터에 설치된 모든 드라이버의 이름을 나열	드라이버 이름

□ 네트워크

명령	설명	출력
promiscdetect.exe	컴퓨터의 네트워크 어댑터가 도청 모드인지 확인	네트워크 이름, 네트워크 IP 주소,네트워크 PROMISCUOUS 모드로 설정 여부
ipconfig.exe /all	컴퓨터의 네트워크 어댑터에 대한 모든 설정을 표시	컴퓨터의 네트워크 어댑터에 대한 모든 설정,IP 주소, 서브넷 마스크, 게이트웨이 및 DNS 서버.
getmac.exe	컴퓨터의 네트워크 어댑터에 대한 MAC 주소를 표시	네트워크 이름, 네트워크 유형, MAC 주소, IP 주소, 서브넷 마스크, 게이트웨이 IP 주소
ipconfig.exe /displaydns	컴퓨터의 DNS 캐시를 표시	컴퓨터의 DNS 캐시에 있는 모든 DNS 항목, 도메인 이름, IP 주소 및 만료 날짜.

□ 로컬세션

명령	설명	출력
net.exe session	컴퓨터의 모든 활성 네트워크 세션을 표시	세션 ID, 세션을 시작한 사용자, 세션이 연결된 원격 컴퓨터 및 세션이 시작된 시간

□ 네트워크 세션

명령	설명	출력
netstat.exe -nao	모든 활성 네트워크 연결에 대한 정보를 표시하고 출력	포트 번호, 상태, 연결된 주소 및 연결된 프로세스
tcpvcon.exe /a /c	모든 활성 TCP 연결에 대한 정보를 표시하고 출력	포트 번호, 상태, 연결된 주소 및 연결된 프로세스
urlprotocolview.exe	모든 등록된 URL 프로토콜에 대한 정보를 표시	프로토콜 이름, 상태 및 연결된 주소

□ TCP IP OPEN PORT

명령	설명	출력
cports.exe	모든 열려 있는 포트에 대한 정보를 표시	포트 번호, 상태, 연결된 주소, 연결된 프로세스
netstat.exe -nao	열려 있는 포트와 프로세스 PID 확인	포트 번호, 상태, 연결된 주소, 연결된 프로세스

□ 계정 및 그룹

명령	설명	출력
net.exe user	모든 활성 사용자에 대한 정보를 표시	사용자 이름, 암호, 암호 만료 날짜, 암호 정책 설정, 사용자 그룹, 사용자 권한
net.exe localgroup administrators	Administrators 로컬 그룹에 속한 모든 사용자에 대한 정보를 표시	사용자 이름, 암호, 암호 만료 날짜, 암호 정책 설정, 사용자 그룹, 사용자 권한

□ LOGON

명령	설명	출력
net.exe session	모든 활성 사용자 세션에 대한 정보를 표시	사용자 이름, 컴퓨터 이름, 프로세스 ID, 연결된 시간 및 연결된 디렉토리
logonsessions.exe	모든 로그온 세션에 대한 정보를 표시	사용자 이름, 컴퓨터 이름, 프로세스 ID, 로그온 시간 및 로그온 방법
psloggedon.exe	모든 로그온 세션에 대한 정보를 표시	사용자 이름, 컴퓨터 이름, 프로세스 ID, 로그온 시간 및 로그온 방법
winlogonview.exe	모든 로그온 세션에 대한 정보를 표시	로그온 ID, 사용자 이름, 도메인, 컴퓨터, 로그온 시간, 로그오프 시간, 기간, 네트워크 주소

□ 공유 폴더

명령	설명	출력
net.exe share	네트워크 공유에 대한 정보를 표시	공유 이름, 공유 위치, 공유된 사용자 또는 그룹, 공유 권한, 파일 이름, 파일 위치, 파일 크기, 파일 소유자, 파일 권한
net.exe file	네트워크 파일에 대한 정보를 표시	공유 이름, 공유 위치, 공유된 사용자 또는 그룹, 공유 권한, 파일 이름, 파일 위치, 파일 크기, 파일 소유자, 파일 권한

□ NetBIOS

명령	설명	출력
nbtstat.exe -c	컴퓨터의 NetBIOS 이름 해상도 캐시를 표시	컴퓨터 이름, 컴퓨터의 IP 주소, 컴퓨터의 NetBIOS 이름, 컴퓨터의 서비스
nbtstat.exe -n	컴퓨터의 NetBIOS 이름을 표시	컴퓨터 이름, 컴퓨터의 IP 주소, 컴퓨터의 NetBIOS 이름, 컴퓨터의 서비스
nbtstat.exe -s	컴퓨터의 NetBIOS 서비스 목록을 표시	컴퓨터 이름, 컴퓨터의 IP 주소, 컴퓨터의 NetBIOS 이름, 컴퓨터의 서비스

□ ARP

명령	설명	출력
arp.exe -a -v	현재 ARP 캐시의 모든 항목을 나열하고 각 항목에 대한 자세한 정보	IP 주소, 하드웨어 주소, 시간 및 날짜

□ 라이팅

명령	설명	출력
route.exe PRINT -4	컴퓨터의 IPv4 라우팅 테이블을 표시	목적지, 게이트웨이, 인터페이스 및 metric

□ 시스템 기본 정보

명령	설명	출력
systeminfo.exe	컴퓨터의 시스템 정보를 표시	컴퓨터 이름, 운영 체제 버전, 프로세서 유형, 메모리 크기, 하드 드라이브 크기 및 드라이버 버전
psinfo.exe -d	컴퓨터에서 실행 중인 모든 프로세스의 자세한 정보	프로세스 ID, 프로세스 이름, 사용자 이름, CPU 사용량, 메모리 사용량 및 시작 시간

□ 설치 목록

명령	설명	출력
wul.exe	wul.exe(Windows Update Log Collector) Windows 업데이트 기록을 텍스트 파일에 수집	Windows 업데이트 기록
systeminfo	systeminfo 명령은 컴퓨터의 시스템 정보에 대한 자세한 보고서를 생성	컴퓨터의 하드웨어 구성, 소프트웨어 구성 및 네트워크 구성이 포함
psinfo.exe -h	현재 실행 중인 프로세스에 대한 자세한 정보를 생성	프로세스의 이름, PID, CPU 사용량 및 메모리 사용량
psinfo.exe -s	현재 실행 중인 서비스에 대한 자세한 정보를 생성	서비스의 이름, PID, CPU 사용량 및 메모리 사용량

□ 자동 실행

명령	설명	출력
autorunsc.exe -a * -c -h -s -u * -o	Windows에서 자동으로 실행되는 항목 목록을 생성	시작 프로그램, 서비스 및 드라이버

□ 파이프

명령	설명	출력
pipelist.exe	Windows에서 실행 중인 파이프 목록을 생성	파이프의 이름, PID, 상태 및 소유자 ID

□ 비 휘발성

명령	설명	출력 데이터 유형
dd.exe	지정된 디스크 또는 파티션의 내용을 다른 위치로 복사하는 도구	복사된 데이터의 크기, 시간, 날짜, 원본 및 대상 위치
forecopy_handy.exe	지정된 디렉토리의 내용을 백업하는 도구	백업된 파일 또는 폴더의 목록, 시간, 날짜, 원본 및 대상 위치
taskschedulerview.exe	Windows 작업 스케줄러에서 실행 중인 모든 작업에 대한 정보를 표시하는 도구	작업 이름, 설명, 시작 시간, 종료 시간, 주기, 실행 권한, 실행 파일 및 대상 위치
shadowcopyview.exe	Windows 컴퓨터에서 생성된 모든 섀도 복사본에 대한 정보를 표시하는 도구	섀도 복사본 이름, 설명, 시작 시간, 종료 시간, 크기, 사용 가능한 공간, 볼륨 및 대상 위치
robocopy.exe	한 디렉토리에서 다른 디렉토리로 파일과 폴더를 복사하는 도구	복사된 파일 또는 폴더의 목록, 시간, 날짜, 원본 및 대상 위치
xcopy.exe	한 디렉토리에서 다른 디렉토리로 파일과 폴더를 복사하는 도구	복사된 파일 또는 폴더의 목록, 시간, 날짜, 원본 및 대상 위치
browsinghistoryview.exe	Windows 컴퓨터에서 저장된 모든 브라우징 기록에 대한 정보를 표시	방문한 웹 사이트 목록, 방문 시간, 방문 날짜, 방문한 페이지 수 및 대

	하는 도구	상 위치
browserdownloadsview.exe	Windows 컴퓨터에서 저장된 모든 다운로드에 대한 정보를 표시하는 도구	다운로드된 파일 목록, 다운로드 시간, 다운로드 날짜, 다운로드 크기 및 대상 위치
browseraddonsview.exe	Windows 컴퓨터에서 설치된 모든 브라우저 추가 기능에 대한 정보를 표시하는 도구	추가 기능 이름, 설명, 버전, 작성자, 대상 위치 및 설치 날짜

■ 별도 첨부

GIT HUB LINK: https://github.com/goodmentos/IR_Script.git