250716

악성코드 분석 시 사용하는 툴에 대한 이해

뭘 분석해야되는지에 대한 기능적인 이해

//악성코드 종류

Virus

> 요즘에는 잘 사용되지 않는 추세

> 플로피디스크 쓰던 시대, 네트워크가 잘 발달해 있지 않던 시대에 많이 사용됨.

Worm

> "

> 같은 네트워크 내에서도 타 시스템을 감염시키기 위해서는 취약점이 필요함.

> 하지만 발생했을 때 파급효과는 매우 큰 편임.

Trojan

>

Downloader & Dropper

> 악성코드를 다운로드 받냐 생성하냐의 차이

> 다운로더는 다운로드를 끊으면 악성코드를 분석하기 어려움.

> (드로퍼가 분석하기는 더 쉬움)

Backdoor

> "

> 서버로부터 받은 명령에 따라 행위가 다름.

> RAP(Remote Access Program) 들이 잘 나와있음.

> (백도어 쓸 바에는 RAP 켜서 정보를 빼감.)

Rootkit & Bootkit

> 커널영역에서 동작하는 악성코드

Ransomware

> 니꺼 잠궈놓음 돈 내놔

> 2016년에 랜섬웨어가 급증함.

> (암호화폐 등 돈 세탁이 가능한 방법이 늘어남, 다크웹이라는 시스템의 발전)

> 이제는 개인을 공격하지 않음. 보통 기업을 공격함.

> (개인은 그냥 자신을 갈아넣어서 복구시키기 때문)

> AES/DES, RSA 등 암호화방식이 활용됨.

> 암호화풀린경우1. 개발된 랜섬웨어 자체에 취약점이 있었다(키가 프로그램에 남아있었다.)

> 암호화풀린경우2. 경찰(FBI 등)에 의해 물리적으로 모든 키가 압수되었을 때

Spyware : 정보 무단 수집

Adware & PUP : 광고 퍼먹이기 > 차단하기 애매함.

// 악성코드를 활용한 공격 방식

SpearPhishing

(참고) 개인이메일은 영장없이는 확인 불가능함.

SW 취약점

랜섬웨어 관련 최신 사례 : yes24, SGI서울보증 등

제발 좀 네트워크 연결되지 않은 백업 서버 좀 만들어 놔라

DLS(Dedicated Leak Site) : 공격자가 피해자의 데이터를 공개하는 웹 사이트.

Watering Hole

> 홈페이지에 취약점이 있으면 악성 스크립트 심어놓고 기다림.

> 준비조건이 많은 대신에 잘 안 들킴.

> Flowexploit : 다크웹에서 구하면 몇 억씩 함.

공급망 공격(Supply Chain Attack)

> 공급망 : (악성코드분석에서) SW 공급망을 의미함.

> ex) (git) 악성코드를 포함한 코드를 업로드함.

> ex) (putty) ID/PW 입력과정에서 정보 탈취됨(공급망공격보다는 SW변조에 가깝긴함).

> ex) (대구버스어플) 개발자 PC가 공격당해 개발과정에서 악성코드가 삽입됨.

> ex) (Xshell) 넷사랑컴퓨터에서 만들어진 원격접속 프로그램에 악성코드가 포함되어 있었음.

//악성코드 공격 케이스 소개

악성코드 공격 케이스1.

> 탈취된 계정이 또다른 공격에 이용됨.

악성코드 공격 케이스2.

> 기업들 대상 Phising 공격

> 메일에 Office 파일이 첨부되어있었고, Office 파일의 매크로 기능을 이용하여 악성코드를 동작되게 함.

> 강력한 기능이여서 Office에서는 Default로 막아놓음. 하지만 사용자가 컨텐츠 사용을 누르면 매크로가 동작됨.

> QH,SPIDER 등 : 해외에서 많이 사용되는 백신 프로그램들 > 있으면 실행 X

> WORKGROUP, workgroup 탐지 : 이 Default 그룹이 없으면 보안 처리 되어 있으니 실행 X

악성코드 공격 케이스3.

> 신분을 위장하여 연락하였고, 암호화된 이미지 파일을 전달하였음.

> 해당 파일을 복호화할 수 있는 프로그램(PC 및 Mobile 각각)을 제공하였고, 이에 악성 쉘이 포함되어 있었음.

악성코드 공격 케이스4.

> 레터럴 무브먼트(Lateral Movement) : 내부확산, 초기침투 이후 내부 스캐닝 및 이동하는 것을 의미함.

> 32p : 거의 템플릿처럼 활용됨.

>> 초기침투-내부스캐닝및이동-백도어설치 혹은 랜섬웨어 유포-정보 유출-금전 요구 혹은 탈취데이터 판매

악성코드 공격 케이스5.(PPT에 없음)

> 메일로 "구입에 필요한 서류 항목을 알려주시기 바랍니다." 연락함.

> 의심1. 사내 메일이 아닌 포털 메일 사용.

> 메일 응답 시 관련 파일을 첨부하여 회신함.

> 같은 제품을 판매 중이던 다른 회사에서 정보가 유출되어서 이런 공격이 진행됨.

//악성코드 분석가

악성코드 분석가 : "악성코드"를 다양한 측면에서 분석하여 "유의미한 산출물"을 생산하는 직업

Intelligence Analyst(이하 IA) : 분석 결과를 가지고 실재하는 공격자 또는 공격그룹 등의 정보를 알아내는 역할

악성코드 분석가가 IA를 포함하거나, 아예 분리되어 있는 경우도 있음.

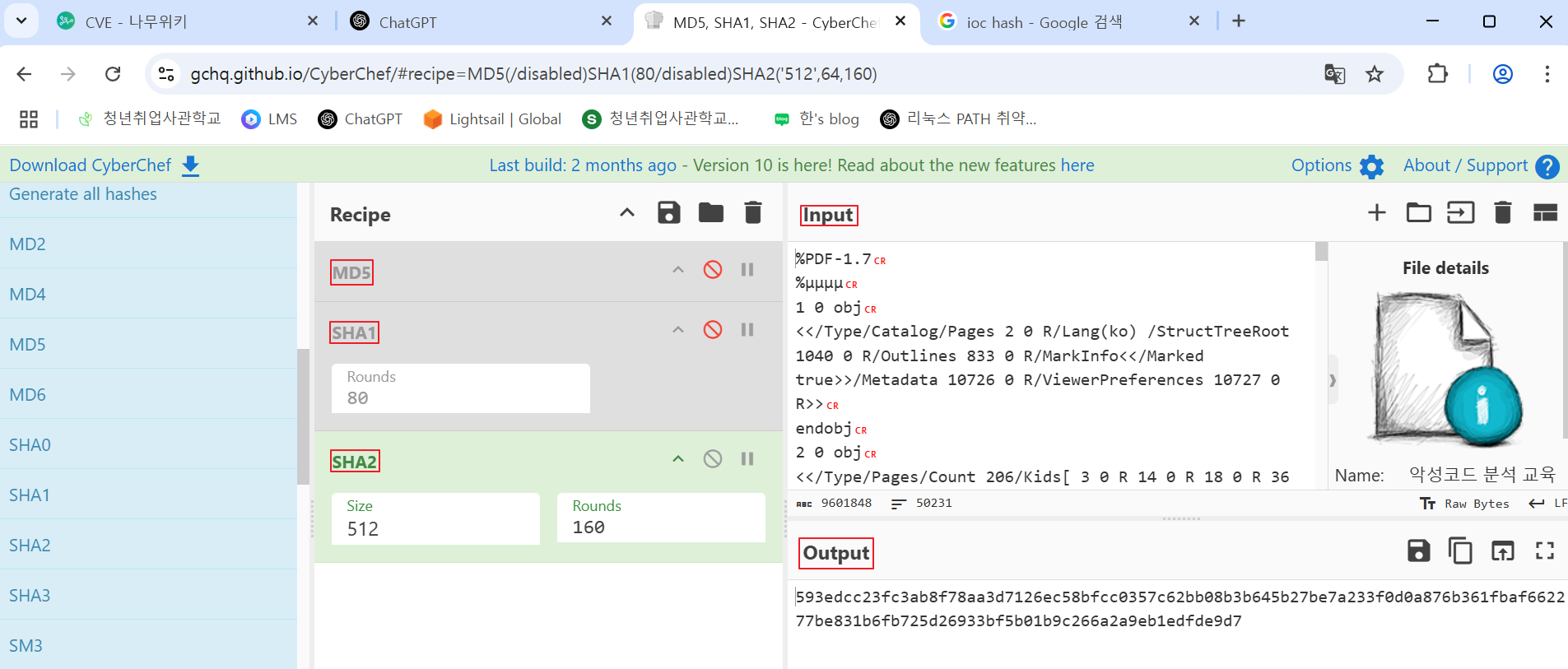
(참고) Hash : 단방향 암호화(복호화가 고려되지않음) 알고리즘.

> 하나의 값이라도 다를 경우 완전히 다른 해시값이 출력됨.

> MD5, SHA1, SHA2

> ex) 파일을 다운로드받고 해시값을 생성하여 제공되는 해시값과 비교, 다운로드받은 파일의 무결성을 확인할 수 있는 수단으로 활용.

> ex) CyberChef : 해시 실습 가능한 오픈 소스 웹 응용 프로그램(영국 정보통신본부 제공,GCHQ)



>> HMAC : 메시지인증코드(MAC)의 한 종류, 해시함수와 비밀 키를 함께 사용하여 메시지의 무결성 확인 및 인증에 사용됨.

>> "공격에 사용된 HASH 나왔나요?" > 해시값을 악성코드 분석에 활용.

>> IOC(Indicators of Compromise) : 보안 침해 사고를 탐지하고 식별하는 데 사용되는 파일의 고유한 식별자

시그니처 : 공격자 혹은 공격그룹에 따른 특징

> 악성코드의 문자열, 특징, 함수, 코드 모양등 공격자에 따라 특정하게 나타나는 파일/행위의 특징

Hash VS SIGNITURE

> 분석대상 : 1:1 vs 1:N

> 실제 백신 툴에서는 둘다 사용함.

> 스크립트 기반 파일들은 같은 동작을 하더라도 다른 파일 구성이 되어 있을 수 있어 Hash를 통한 탐지에 어려움이 있음.

? 동작이 같다면 컴파일된 어셈블리 단의 코드를 해시로 만들어 비교할 수는 없나

> 보통의 스크립트는 JAVA 혹은 Python을 기반으로 만들어지기 때문에(대부분 interpreter 방식으로 동작됨.) 질문과 같은 방식은 구현이 매우 어려움.

YARA : 악성코드의 패턴을 이용하여 특성과 행위를 기준으로 악성코드를 분류하는 도구(VirusTotal 제작)

>> meta, strings, condition 등을 가지고 비교함.

>> 최초의 악성코드 분석의 경우는 YARA룰이 아닌 자신만의 분석 툴을 사용하여 분석할 것임.

? MD5는 취약점이 발견된 것으로 아는데 실무에서 혹시 많이 사용되는지

> 아직 많이 사용됨. 중요한 정보에는 SHA2를 많이 적용하지만 퀄리젼이 있는걸 알아도 단순 정보교환등으로는 많이 사용됨(길이가 짧은 이득이 큼)

네트워크 시그니처

> 통신 방식의 도메인, IP, URL 정보/형식등도 시그니처에 해당함.

> IPS 에서 식별 가능한 도메인이나 IP등을 차단하는 시스템 구성되어 있음.

> 도메인이나 URL까지 확인하는 이유는 IP Address 가 한정되어 있기 때문임.

>> 1.해당 IP 소속 일부 도메인이 탈취당했다고하여 전체 IP를 차단하면 추가적인 문제가 발생할 수 있음. > IP를 통한 차단은 굉장히 보수적임.

>> ex) 네이버 웹툰이 털렸으면 해당 도메인만 막지 네이버 전체 도메인을 차단하지는 않음.

>> 2.도메인이 바뀌었다면 (GET방식을 예로 들어) URL에 포함되는 변수명 및 값을 확인하여 잡을 수 있도록 URL도 체크해야함.

행위 정보

> 자가 복제/삭제, 레지스트리 등록(재부팅시 자동실행을 위하여), 시스템정보 수집, 공격자의 서버로 시스템정보 전송

> ex) 프로세스 생성, 파일 생성, 네트워크 통신 등 > 이 결과 생성된 파일 혹은 행위를 모두 "Artifact"라고 표현함.

위협 행위자 도출

> 악성코드 분석, 시스템 동적분석, 네트워크 동적분석을 통해 연권상 및 특징을 도출해내고 위협행위자를 도출해냄.

(참고) C&C 서버(Command & Control)(혹은 C2) : 원격지에서 명령을 내리거나, 악성코드를 제어하는 서버

(참고) 샌드박스(Sandbox) : 외부 프로그램이나 코드가 시스템에 손상을 입히지 않도록 제한된 환경에서 실행되도록 하는 보안 기술.

(참고) EDR(Endpoint Detection and Response) : 엔드포인트 감지 및 대응

> 로그의 가시성을 확보하는 역할도 하고 있음. > 해당 Data들이 SIEM에 모이게됨.

> 알려진 위협에 대해서는 Anti-Virus가 대응을 하고, 알려지지 않은 위협에 대해서는 EDR이 역할을 하고 있음.

(참고)토르로 접속한 다크웹

// 분석 정보 읽어보기

https://stic.secui.com/

https://stic.secui.com/main/main/threatInfo?id=158

(참고) IOC(Indicators of Compromise) : 보안 침해 사고 발생 시, 공격의 흔적이나 패턴을 나타내는 지표들

https://asec.ahnlab.com/

https://asec.ahnlab.com/ko/89037/

https://asec.ahnlab.com/ko/89005/

(참고) 허니팟(Honeypot) : 사이버 보안에서 공격자를 유인하여 공격 시도를 탐지하고 분석하기 위해 의도적으로 설치한 시스템 또는 가짜 자원을 의미함.

https://blog.talosintelligence.com/

https://www.virustotal.com/gui/home/upload

블로그 등 웹 페이지를 통해 제공되는 정보도 많지만 X(구 twitter)등을 통한 빠른 정보 제공도 많이 됨.(a.k.a. 폐지줍기)

//악성코드 동적 분석

정적 분석 : 코드레벨에서 악성행위를 확인하는 분석법.

동적 분석 : 악성코드를 실행하고 모니터링 툴 등을 이용해 행위를 분석하는 분석법.

VMWare가 개인용은 무료로 풀려서 사용해보는 것도 괜찮을듯.

기업에서는 VMWare나 ESXi를 사용하는듯.

악성코드 분석에서 스냅샷이 중요한 이유

(참고) 스냅샷 : 특정 시점의 데이터 상태를 저장하는 기술

악성코드 실행 전후를 비교하기 위해 많이 사용함.

실행중인 프로세스 확인 툴

> Process Explorer : procexp64

> Process Hacker :

네트워크 확인 툴

> TCP Tool : 현재 시스템의 네트워크 연결 여부를 보여줌(netstat -na 의 GUI 버전)

> WireShark : 네트워크 연결은 물론 모든 패킷을 모니터링함.

> 피들러

> Process Monitor : All in One Monitoring

> Procmon64.exe

> Filter-Filter : Category(dropdown)-options(dropdown)-text-then Include/Exclude

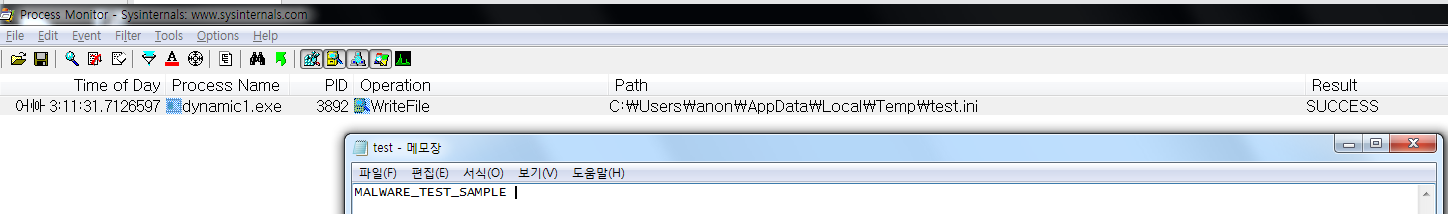
> 필터를 잘 사용하여 원하는 프로세스를 확인할 수 있는 기술이 필요함.

> 특정 레지스트리 모니터링에 대해 세팅이 잘 준비되어 있어야함.

> 필터를 거는 작업이 VirusTotal 등 리스트에서 검색하는 데에 대한 연습과정임.

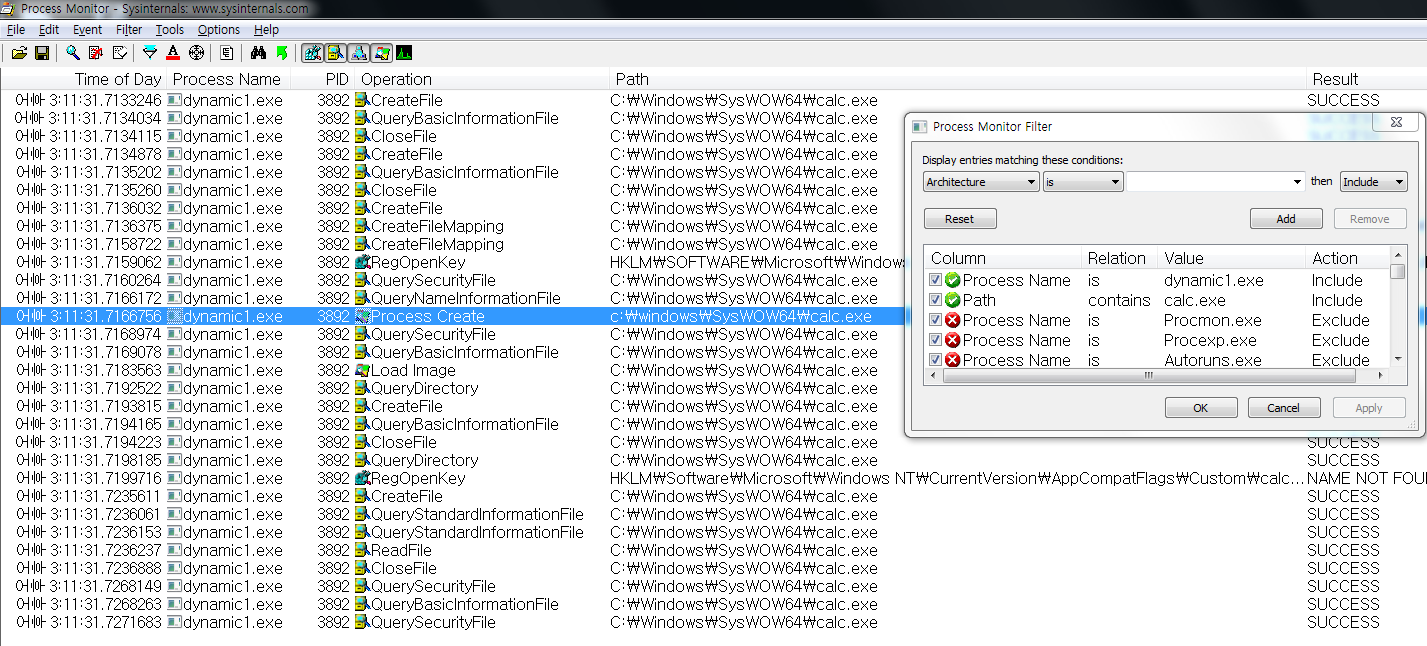
>> 또는 관제에서 잔뜩 쌓이는 로그 중 유의미한 로그를 찾아내는 작업 > 디깅

> 커널 드라이버에서 로그를 저장하는 필터 드라이브가 생성되고 지나가면 삭제됨(휘발됨)



Filter1 : Process Name is dynamic1.exe then Include

Filter2 : Operation is WriteFile then Include



Filter1 : Process Name is dynamic1.exe then Include

Filter2 : Path contains calc.exe then Include

악성코드 분석에서 어려운 점

> 1. 탐지

> 2. 샘플 구하기

VirusTotal 쿼리 기능은 유료임.

// 리버싱 : 리버스 엔지니어링 :

x32DBG + dbg0\_assembly\_practice(Desktop\malware\_education)

ReverseMe / CrackMe : 리버스 엔지니어링 실습 툴

Crack과의 싸움은 현재진행형임.

>불법 Crack을 방지하기 위한 프로그램 : Denuvo, Themida, VMProtector등

> ex ) 카카오톡에 Themida가 포함되어 있어 Denuvo가 있으면 실행이 안된다.

프로그램의 이해 : 변수, 함수, 반복문, 비교문, API

PE File Format(Portable Executable File Format)

: exe, dll, sys, ocx 파일 등 윈도우에서 사용되는 모든 실행 가능 파일은 PE 구조를 가짐.

필요하다면 다른 용도로도 사용되지만, 기본적으로 주어진 역할은 위와 같다.

> 절대로 임의로 값을 바꾸면 안되는 것 : EBP, ESP, EIP

>> EBP : 스택의 베이스 주소

>> ESP : 스택의 현재 위치 주소

>> EIP : 실행중인 명령 주소

Operand 중 DWORD PTR(Operand) : 포인터

어셈블리어 Opcode : 103p~109p

조건부 점프는 확인하고 가야하므로 test나 cmp 뒤에 있음

F7 : Step in(함수 따라들어감), 한 줄 실행

F8 : Step out(함수 지나감), 한 줄 실행

F2 : breakpoint 설정

F9 : breakpoint까지 실행

궁금하면 "드림핵" 참고하여서 알아서 복습해라

더 설명해야 하는거

> 스택의 동작방식, 스택의 활용법, 임의로 어셈블리 명령 넣어서 확인하기(디버거), 디버거 사용법(메모리 맵 보는법)