실무형 프로젝트 회의 K-Shield 주니어 보안사고 분석대용 7기

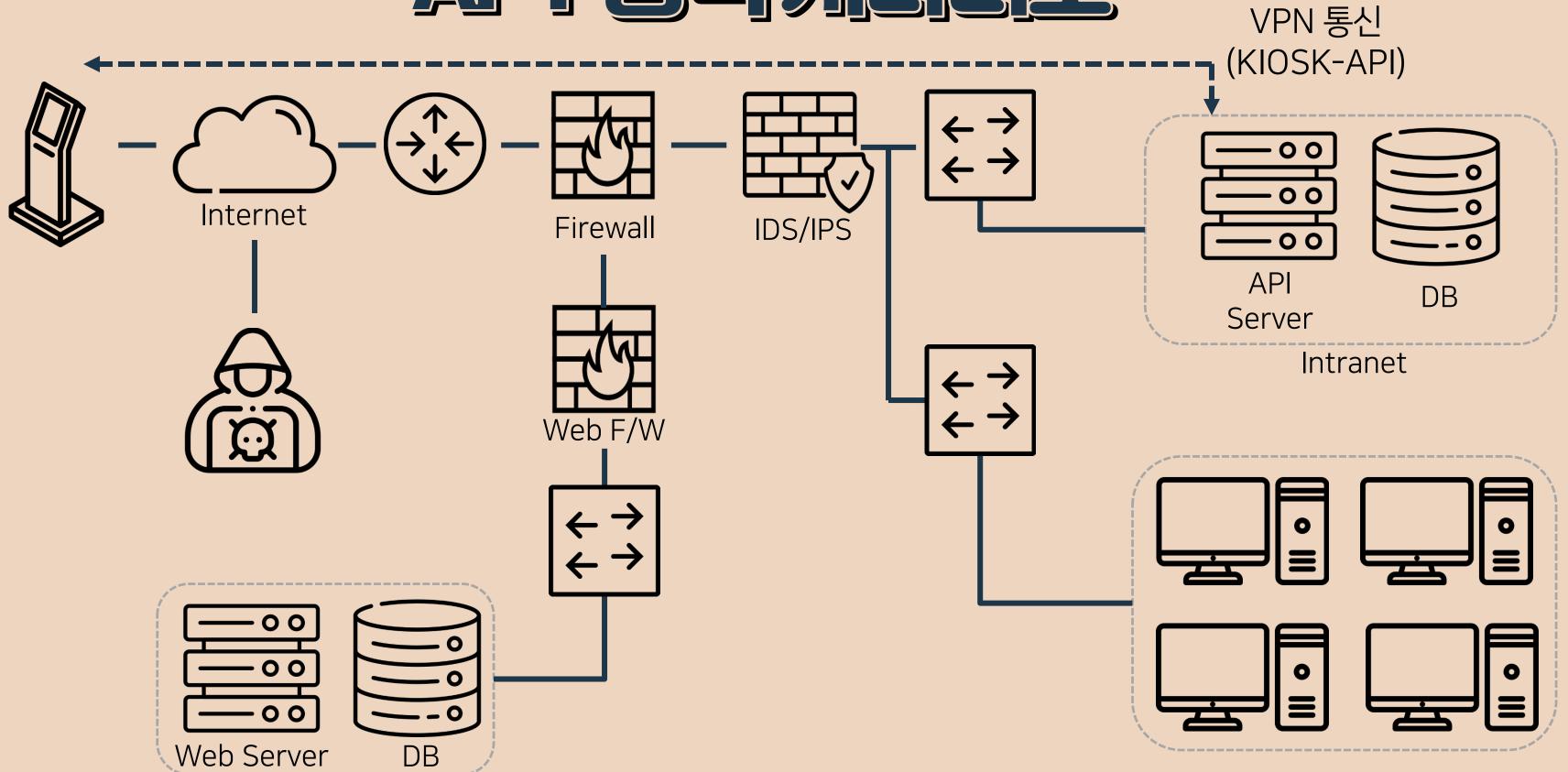
2021, 09, 27 5조 R&B

APTSA

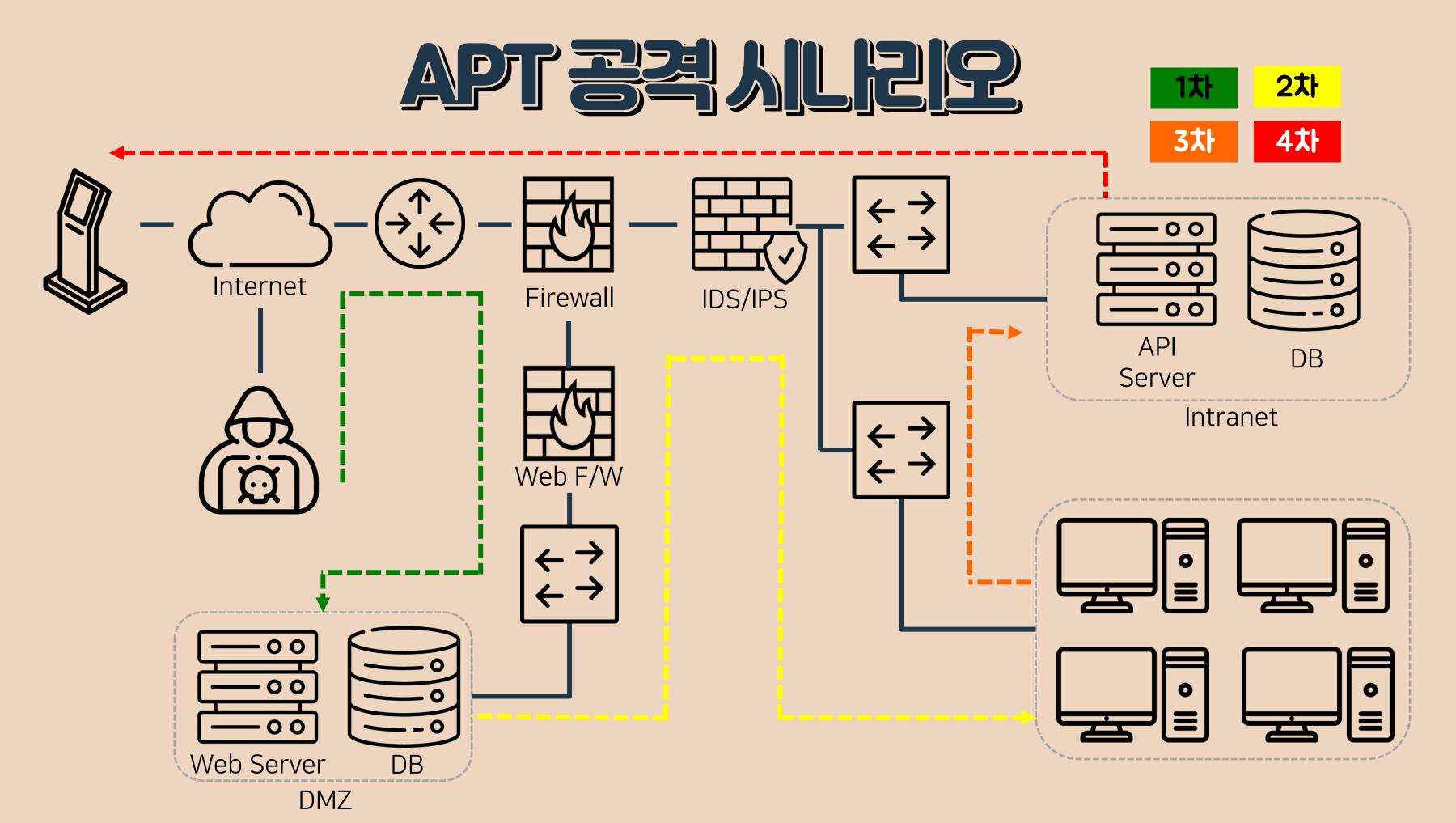
APT 목표

맥도날드 귀오스크를 사용하는 이용자(대상)의 신용카드 정보 탈취 후 흔적 삭제

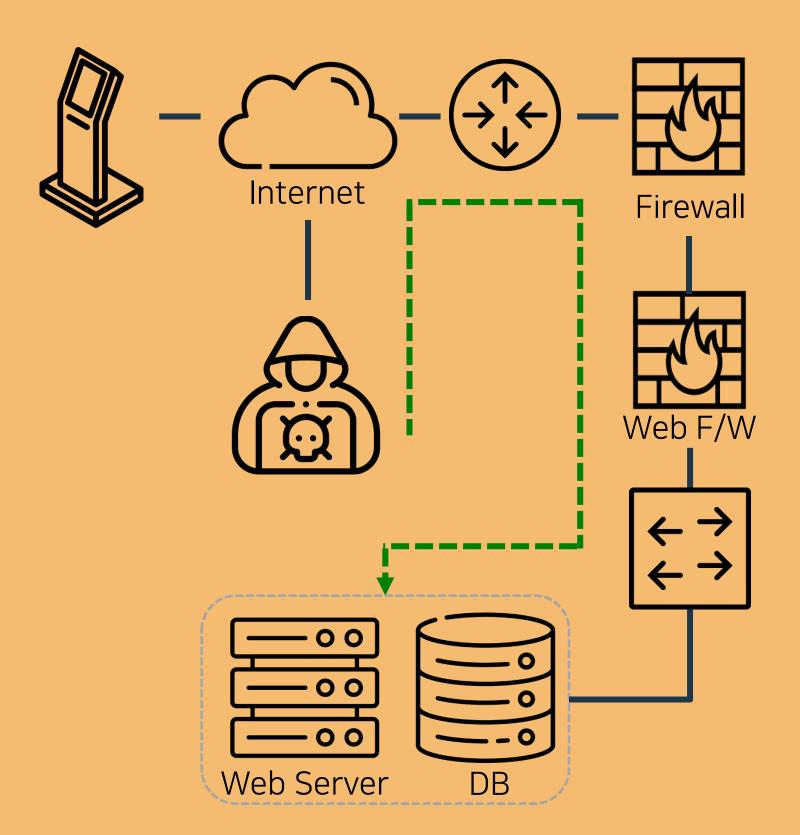
APTBALLER



DMZ



当手可ろ

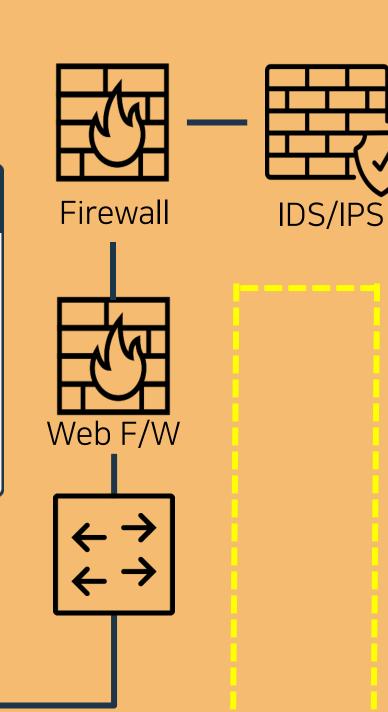


1차 침투: HACKER -> DMZ

파일 업로드 공격 맥도날드 크루 지원 홈페이지에서 지원서 작성에 악성 PDF파일 첨부하여 업로드



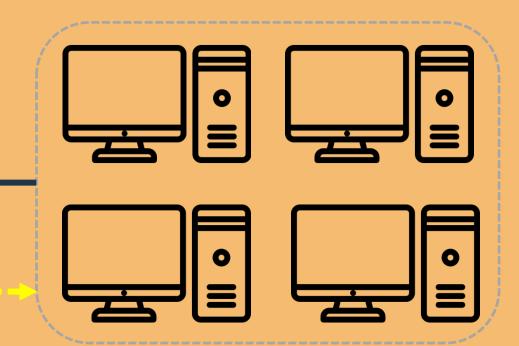
1) 웹 서버에 접근한 웹 관리자 PC 감염

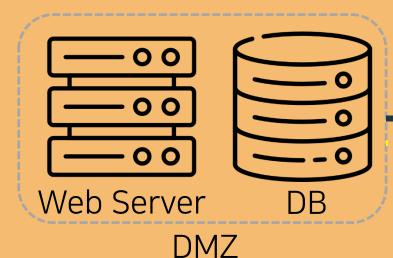


2차 침투: DMZ -> Office

2) 감염된 웹 관리자 PC를 통해 다른 직원들의 PC 감염

(Lateral Movement)





さいころ

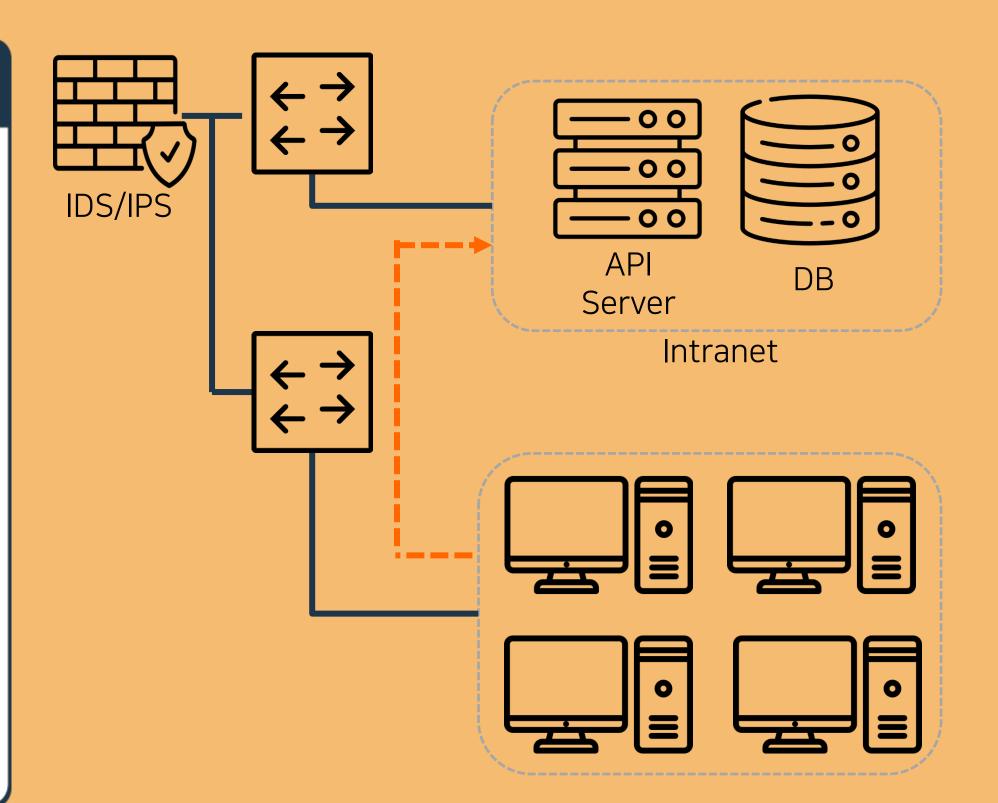
원격지에서 관리자의 크리덴셜 얻기 웹 서버에 업데이트 파일인 척 악성코드 파일을 올려놓고 관리자 PC **감염시키기** Microsoft ← foo@bar.com Enter password Keep me signed in 크롬을 이용해 원격으로 윈도우 패스워드를 훔칠 수 있 Forgot my password 는 취약점 발견 돼 https://blog.alyac.co.kr/1102 웹 서버에 접근할 때 크롬을 이용하여 크리덴셜 훔치기 로그인 하는 페이지로 위장해서 빼오기

3차 침투: Office -> INTRA

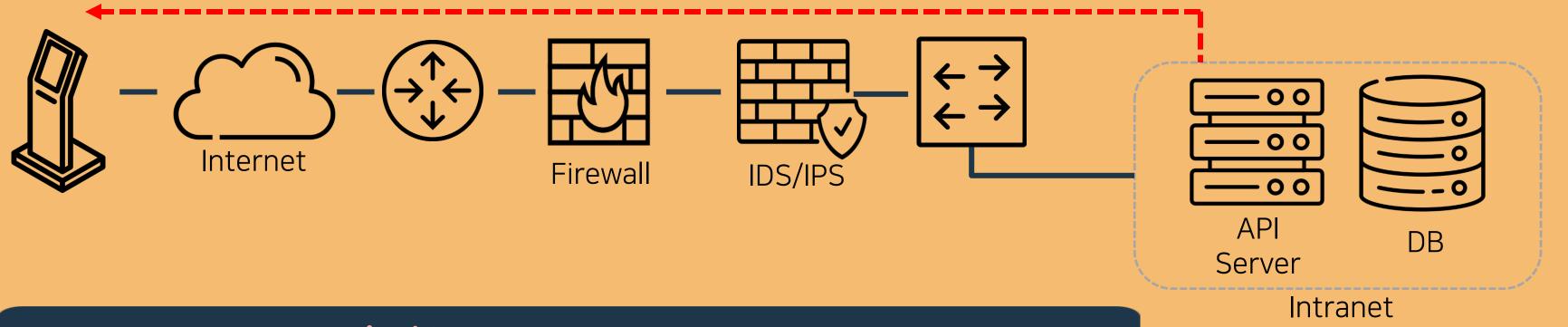
API 서버 감염

서버 구축을 REST API로 선택

→ REST API의 취약점을 이용



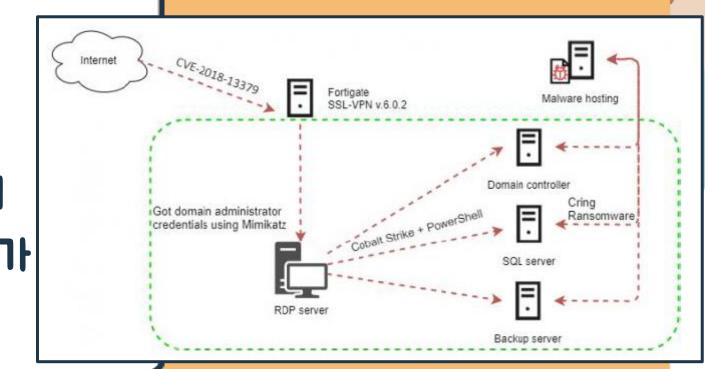
書記



4차 침투: INTRA -> KIOSK

API 서버와 VPN으로 연결된 키오스크 감염 〈 CVE-2018-13379 〉

SSL VPN 웹 포털에서 제한된 디렉토리("Path Traversal")에 대한 경로 이름의 부적절한 제한을 사용하면 인증되지 않은 공격자가 특수하게 조작된 HTTP 리소스 요청을 통해 다운로드할 수 있음



為 第 9 第



키오스크에서 결제정보 데이터를 획득하여 공격자에게 전달

* 데이터 전달 루트 *

(키오스크 -> API 서버 -> 관리자 PC -> 공격자)

APT WBS

TO TO

사전

준비

見9

Dokcer 공부 VPN 회사 별로 취약점 조사 공격에 사용될 악성코드 조사 C&C 통신 조사 방화벽 규칙 세우기

악성코드 제작 악성코드 유포 C&C 서버를 통해 연결 유지 안티 바이러스 우회 DMZ 안의 웹 서버 및 DB 구축
INTRA 안의 API 서버 및 DB 구축
방화벽 및 웹 방화벽
IDS/IPS
리오스크 프로그램 제작

1차 침투(Hacker->DMZ) 2차 침투(DMZ->Office) 3차 침투(Office->INTRA) 4차 침투(INTRA->KIOSK)

데이터 탈취

APT WES



방화벽 룰

1) 내부->외부 : 허용

내부 컴퓨터는 외부 인터넷으로 사용할 수 있게 한다.

2) 외부->내부 : 차단

외부 컴퓨터는 내부에 접속할 수 없도록 한다. 서비스 한다.

3) 외부->DMZ, 내부->DMZ : 허용

DMZ->외부, DMZ->내부 : 허용

외부 컴퓨터가 방화벽 서버의 공인 IP로 웹

서비스를 요청할 때는 내부에 있는 웹 서버가

APTWBS

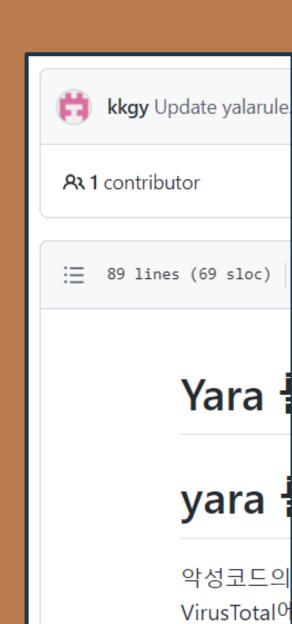
Dokcer 공부 VPN 회사 별로 취약점 조사 방화벽 규칙 세우기 공격에 사용될 악성코드 조사 C&C 통신 조사

약습사전준비

환경구축

DMZ 안의 웹 서버 및 DB 구축
INTRA 안의 API 서버 및 DB 구축
방화벽 및 웹 방화벽
IDS/IPS
키오스크 프로그램 제작

악성코드 제작 악성코드 유포 C&C 서버를 통해 연결 유지 안티 바이러스 우회 1차 침투(Hacker->DMZ) 2차 침투(DMZ->Office) 3차 침투(Office->INTRA) 4차 침투(INTRA->KIOSK) 데이터 탈취





dks1013 [21091

75 lines (66 sloc)

- Yara
- yara

악성코드의 VirusTotal^O

단순 Text St Yara는 멀티 rule 파일 =

A 1 contributor

- 1 파일 리스
- 악성코드가 /
- 웹페이지에
- 사용자 웹브리
- 감염 장소는
- 이미 설치되어
- 엑셀이나 워드
- 시그나처 매칭
- 사용자가 실행
- 방어법 : 지능
- 11 로깅 파워쉘
- 로컬 그룹정책 13
- Living off t
- LotL 공격 (X
- 16 희생자가 보유



wespito [210919] fileles

A 1 contributor

422 lines (292 sloc)

Fileless

- 1. Code Inject
 - Shellcode

합법 프로

DLL inject

프로세스



t0paz-2357 Update [210913] ELK.md

A 1 contributor

ELK

ELK (ElasticSearch, Logstash, Kibana) 란?

ElasticSearch - 분석 및 저장 기능을 담당 Logstash - 수집 기능 Kibana - 이를 시각화하는 도구

전체적으로 접근성과 용이성이 좋아 최근 가장 핫한 로그 및 데이터 분석 도구이다. 공식 사이트

ELK 사용법

ELK Introduction ELK Installation ELK 기본사용법

EDREM 子題

- 1) Sysmon + ELK 서버 구축 : EDR의 기본 틀 마련
- 2) Syslog 연계(APT 팀의 구축 환경 고려)
 - : DMZ 존 + 인트라넷망 + 워크존 모두 탐지하기 위해
- 3) Yara rule 작성

심화 - APT 공격에 자주 사용되는 Fileless 공격 탐지 구현

1) DLL injections,

2) LotL (Living of the Land)

- Reflective DLL injections,
- 3) 지속성 공격

Process hollowing

EDRWBS

Docker 공부 ELK 서버 구축 방법 API 동작 및 후킹 과정 API 공격 기술 자료 수집 악성 코드의 API 행위 분석 기존 EDR 솔루션 조사

ELK 서버 구축 Sysmon-Logstash 필터링 Syslog 연계 Kibana 시각화 구현 자료 환경 조사 구축 ELK 진단 다 가상 환경 생성 Github Repository 생성

YARA 를 탐지 진단 알고리즘 설계 프로세스 핸들 구현 메모리 추출 분석 및 진단 시스템 구현 레포트 제공 시스템 구현