해킹 및 침해 대응

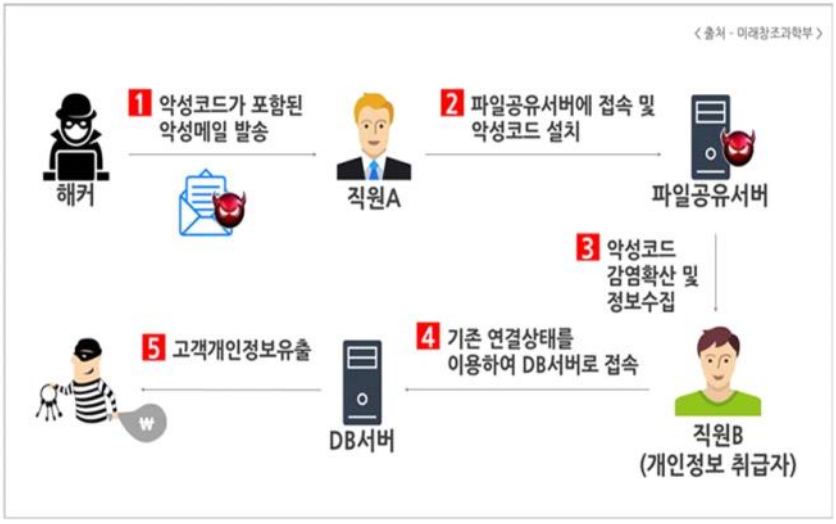
2017년 4월 2일 일요일 오전 1:11

1. 악성코드 감염 경로 및 유포 경로

- 짧은 시간 대량의 PC감염을 위해 다양한 경로가 악성코드 유포에 활용된다.
- 홈페이지, 웹하드, P2P, 이메일, 메신저, SNS, 이동형 저장장치 등을 통해 유포된다.
- 예1) 이메일: 정부기관을 사칭한 이메일을 통한 악성코드 유포시도: 악성코드 이메일을 발송 -> 이용자가 응답 시 악성코드가 포함된 메일 재발송
- 예2) 홈페이지: 공격자는 특정 서버에 서버해킹 후 홈페이지에 악성코드를 삽입해놓고 기다린다. 사용자가 홈페이지에 방문하면 악성코드가 자동전송되도록 구성되어있다.
- 예3) 웹하드: 해커는 웹하드 사이트 운용서버를 해킹하고 악성프로그램 을 업로드해놓는다. 사용자는 홈페이지를 방문하고 컨텐츠 다운로드를 요청하는데 악성코드가 전송되고 실행된다.

2. 침해사고 주요사례(최근3년이내) - 하나만 외우면 되지 않을까요?

- 사고의 원인과 특징, 공격 유형, 대응방법 등
- 사례1) 인터파크 개인정보 유출사고(16'05), 사례2) SK네트웍스 자료유출사고(14'07~16'03)
-

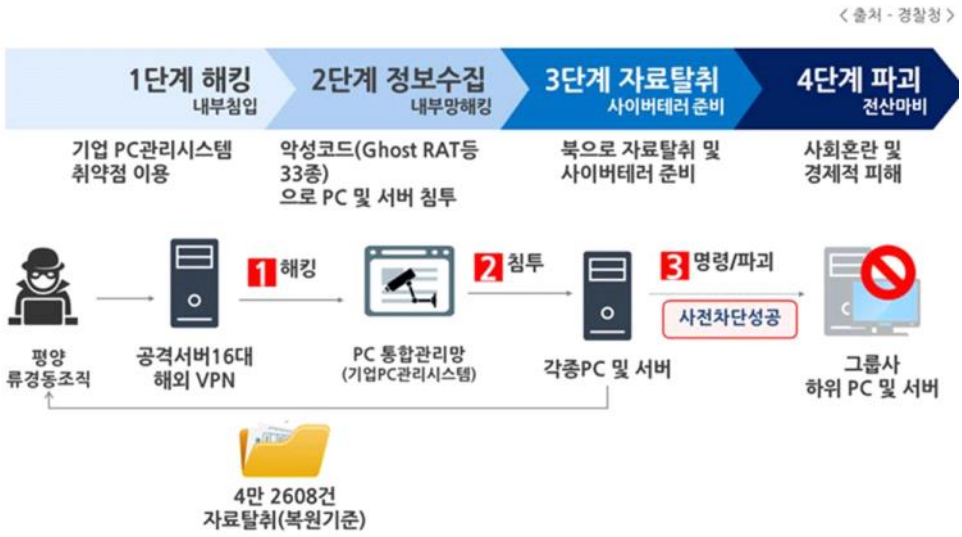


[그림 1] 인터파크 개인정보 유출사고 공격 시나리오

사례1) 인터파크 개인정보 유출사고: 2016년 5월에 발생, 고객 아이디/암호화된 비밀번호, 이름, 생년월일, 전화번호, 이메일 등 유출

- 원인과 특징: 개인정보처리시스템에 timeout 설정 하지 않음, DB서버, 웹서버 등 비밀번호 관리 소홀, 임직원이 악성메일 접속함으로 인해 내부망에 악성코드 감염 확산 및 정보유출까지 이어짐.
- 공격유형: APT
- 대응방법: 임직원 인식교육, spam 필터 정책 적용 및 보안장비 도입, DB서버 감사를 통해 이상징후 탐지 (DBMS에 최대 접속시간 제한조치)

사례2) 대기업 (SK네트웍스/한진계역/kt 관련 그룹계열사) 자료유출사고



원인과 특징: 기업 PC관리시스템 취약점을 이용하여 악성코드로 PC 및 서버에 침투하고 북으로 자료탈취하였음. 탈취된 자료에는 바위산업관련정보, 통신설비 등 관련 자료 다수.

공격유형: APT(소프트웨어 취약점 이용)

대응방법: 중앙 관리형 소프트웨어 취약점 패치 관리

3. 피싱, 파밍, 스피어피싱

- 개념, 각각의 특징 및 차이점, 사례, 공격기법 등
- 피싱: private data를 낚는다(fishing)라는 의미의 합성어이다. 불특정 다수에게 이메일/ 게시글을 통해서 위장된 사이트에 정보를 입력하도록 유도하여 개인정보/금융정보등을 획득하여 재산상의 손해를 입히는 사기수법
- 피싱사례: 국민은행의 비슷한 사이트를 만들어놓고 인터넷뱅킹 보안승급서비스를 해준다며 개인정보/금융정보를 입력하게 한다.
- 공격기법: 발신자 위조, 하이퍼링크 위조, 스크립트를 이용한 주소창 위조, 유사도메인을 사용하여 사용자가 메일의 악성링크를 클릭하게 한다. 악성링크를 클릭할 경우 변조된 사이트로 이동한다.
- 파밍: 피싱의 한 유형으로 진화한 형태. 국가기관사이트나 금융기관 사이트 등 신뢰할 수 있는 사이트로 위장해서 개인정보/금융정보를 입력하도록 유도하여 획득.
- 파밍기법: host파일변조, hosts.ics 파일악용, iframe삽입, vpn터널링이 있다.
- 사례: host파일을 변조하여 가짜사이트로 유도한다. PC에서는 사용자가 URL로 접속하고자 할 때 host에 적혀있는 주소인 경우 DNS에 질의하지 않는다는 특징을 악용한 것이다. 따라서 공격자가 host파일을 변조하면 사용자는 올바른 URL 주소로 접속했음에도 불구하고 변조된 host에 있는 해커가 유도한 사이트로 접속하게 된다.
- 스피어피싱: 피싱의 발전된 형태로 Phishing 은 불특정 다수를 대상으로 하지만 스피어피싱은 특정 타겟을 두고 공격하는 기법이다.

피싱 사례 적절치 않음

피싱사례: 대출 이자 관련 메일로 이자를 낮춰줄수 있다며 악성링크로 유도하거나 첨부파일을 열어보도록 유도한다.

피싱 특징:사용자가 주의깊게 살펴보면 알아차릴 수 있다.

파밍 특징: 사용자가 아무리 도메임 주소나 url주소를 주의 깊게 살펴본다 하더라도 쉽게 속을 수 밖에 없다.

사례 및 공격방법

1) 인사담당자에게 제목이나 파일명을 이력서 또는 채용문의 등으로 담당자가 열어볼 수 밖에 없도록 유도한다.

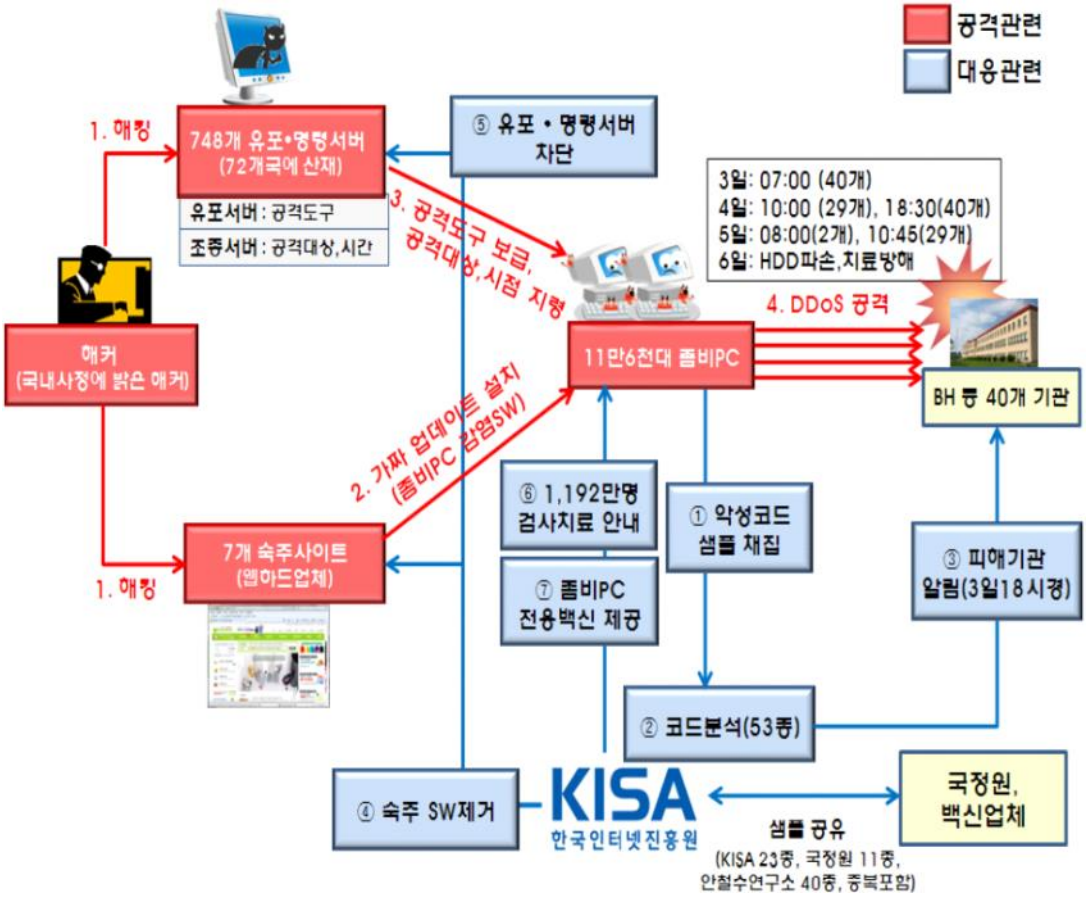
2) 공격 대상 관련 행사(ex 서울에어쇼) 정보 수집 후 행사 관계자를 위장하거나 동일 커뮤니티 소속원을 가장하여 악성코드가 포함된 이메일을 발송한다.

4. DDoS공격

- 개념, 공격방법 및 종류, 최근사례

- 개념/공격방법: 악성코드에 감염된 다수의 좀비 PC를 이용해 대량의 트래픽을 타겟에 전송해서 서비스를 방해하는 공격

- 3.4 DDoS공격 사례) 국내사정에 밝은 해커가 유포/명령서버 해킹, 7개 숙주 사이트(웹하드업체) 해킹하여 악성코드를 심어놓는다. 11만대가 넘는 좀비PC에서는 감염된 웹하드 업체 사이트를 통해 가짜 업데이트(좀비PC감염 소프트웨어)를 설치하게 된다. 그리고 유포/명령서버에서는 좀비PC로 공격도구 보급, 공격대상/시점을 명령을 내린다. 특정 시점이 되면 좀비 PC들은 타겟으로 DDoS공격 트래픽을 발생하게 된다.



5. 좀비 PC분석 절차

좀비 PC란: 공격자에 의해 악성코드에 감염되어 공격자의 명령에 따라 PC사용자의 의도와 관계없이 각종 악의적인 행위를 수행

(windows PC 분석)

운영체제 정보 > 네트워크 연결 >프로세스 정보 > 레지스트리 > 루트킷>타임라인>악성코드 샘플수집 >감염경로 추적

1) 운영체제 정보: cmd창에서 systeminfo 호스트 이름, 운영체제 및 네트워크 정보 등을 확인

2) 네트워크 연결 정보 확인: 정보를 유출하거나 C&C서버와 통신하는 공격자 IP등을 확인 가능하다. NW연결 정보 확인할 수 있는 도구로는 TCP VIEW가 있다.

3) 프로세스 확인: process explorer 툴 이용. PC에서 실행되고 잇는 프로세스를 트리 형태로 볼 수 있으며 프로세스가 참조하고 있는 DLL과 핸들 등에 대해 상세히 확인이 가능하다.

4) 레지스트리 확인: AUTORUNS 툴을 이용하여 PC내 자동으로 실행되게끔 설정되어 있는 파일과 레지스트리를 확인할 수 있다. Publisher와 descryption등 일부 정보가 비어있거나 이상한 값으로 채워져 있는 엔트리 위주로 분석을 진행한다.

5) 루트킷 확인: 루트킷이랑 해커들이 시스템을 해킹할 때 이요자가 알아차리지 못하게 하기 위해 사용하는 도구 및 프로그램을 말한다. 루트킷이 설치될 경우 파일/프로세스/레지스트리/네트워크 등 다양한 내용을 감출 수 있다. 이런 숨겨진 레지스트리와 파일등을 찾고 삭제하기위해 ICE SWORD 또는 PC Hunter라는 툴을 이용하면 된다.

6) 타임라인: 시간 순서에 따른 악성코드 생성/수정/감염 등 행위를 파악하기 위해 타임라인 파악이 중요하다. 가장 먼저 해야할 일은 이벤트 로그 등을 통해서 PC의 시간이 변조되었는지 확인하는 것이다. 윈도우 내 검색 기능을 이용하여 악성코드가 생성된 시점 전후로 추가로 생성/수정된 파일이 존재하는지 확인한다.

7) 악성코드 샘플 수집: 악성코드 샘플을 수집하고 수집한 샘플의 경우 바이러스 토탈 사이트를 통해 행위/종류등을 확인한다.

8) 감염경로 추적: 웹브라우저의 히스토리, 쿠키/캐시정보를 확인한다. 악성코드가 생성된 날짜/시간에 접근한 내역이 있는지 확인한다. 또는 악성코드에 감염된 시점에 USB를 사용한 이력이 있는지도 확인해야한다.

6. 악성코드 유포방법 -> 1번과 연관되는 듯..

   예1) 이메일: 정부기관을 사칭한 이메일을 통한 악성코드 유포시도: 악성코드 이메일을 발송 -> 이용자가 응답 시 악성코드가 포함된 메일 재발송

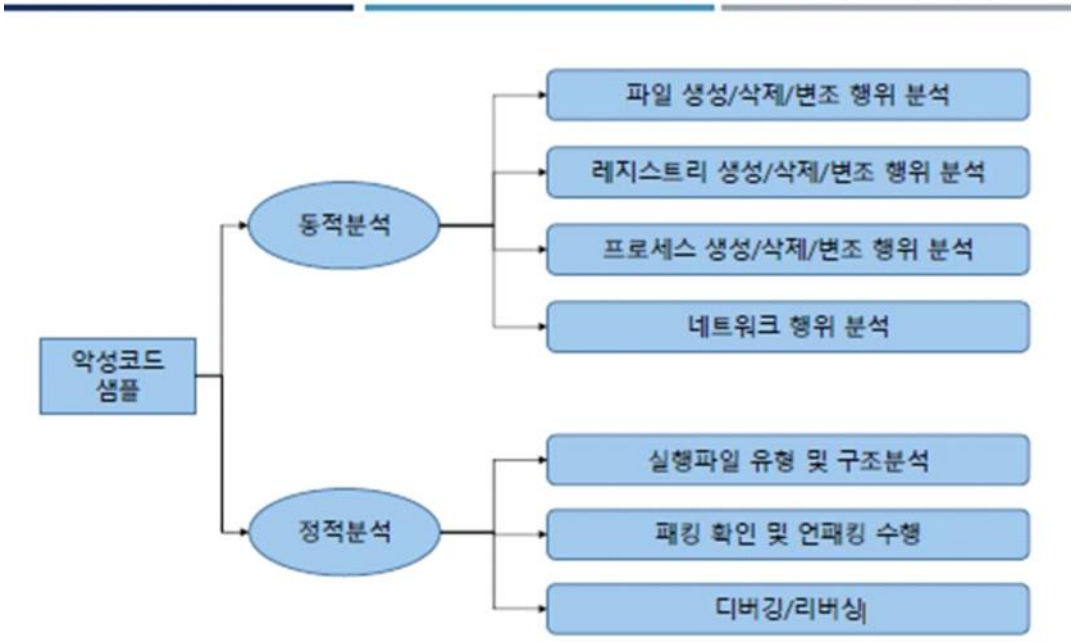
   예2) 홈페이지: 공격자는 특정 서버에 서버해킹 후 홈페이지에 악성코드를 삽입해놓고 기다린다. 사용자가 홈페이지에 방문하면 악성코드가 자동전송되도록 구성되어있다.

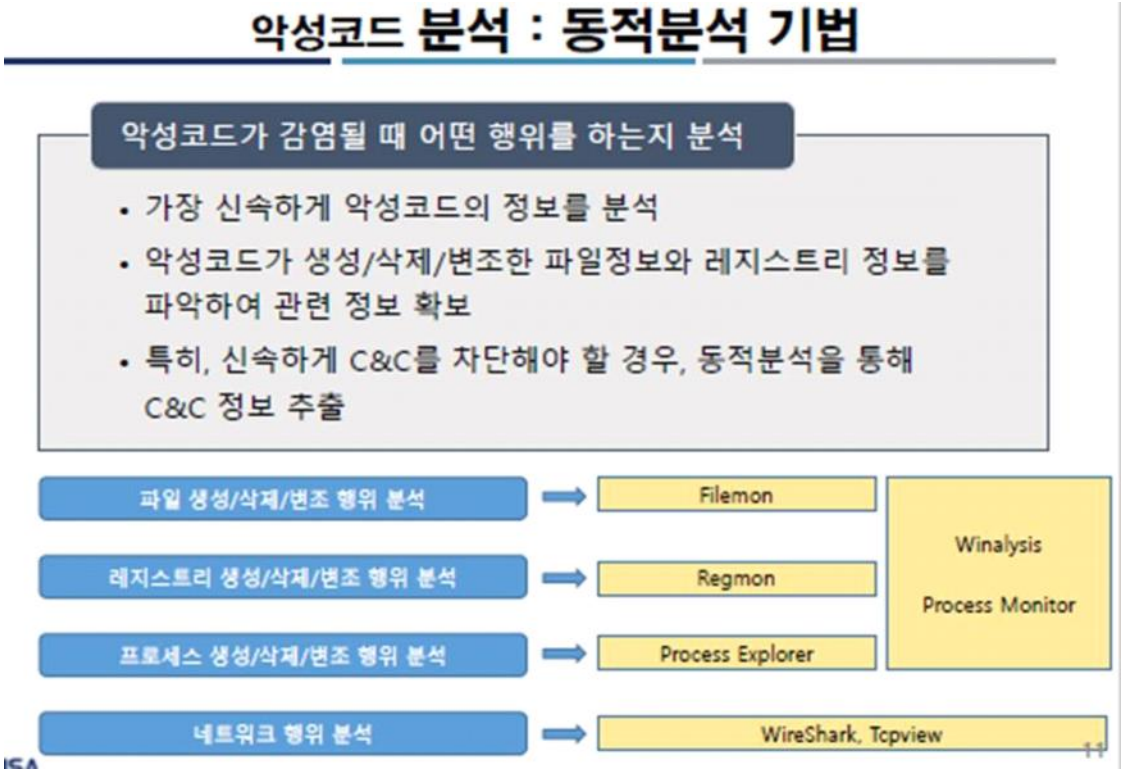
   예3) 웹하드: 해커는 웹하드 사이트 운용서버를 해킹하고 악성프로그램 을 업로드해놓는다. 사용자는 홈페이지를 방문하고 컨텐츠 다운로드를 요청하는데 악성코드가 전송되고 실행된다.

7. 악성코드 분석

- 악성코드 분석 (일반적인) 기본 절차: 사전조사 > 행위기반분석> 패킹여부 > 언패킹 > 코드기반 분석

- 정적분석,동적분석(큰 틀만 외우면 될거같애요)





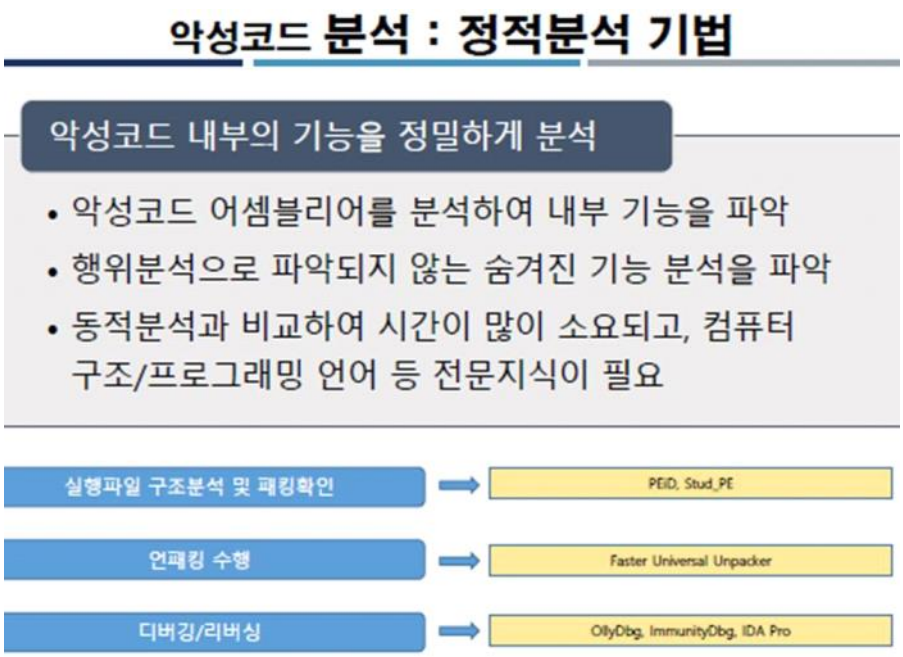
파일 변경 모니터링: 악성코드의 행위, 실행 특징 분석

레지스트리 변경 모니터링: 프로그램에 접근하는 모든 레지스트리 확인 가능

프로세스와 쓰레드 모니터링: Process Explorer 도구 이용하여 현재 실행중인 프로세스/쓰레드 활동을 실시간 모니터링가능. DLL, handle의 삽입 및 실행 확인 가능

네트워크 포트 모니터링: TCPView 도구 이용하여 각각의 프로세스와 연결된 포트를 보여줌

.



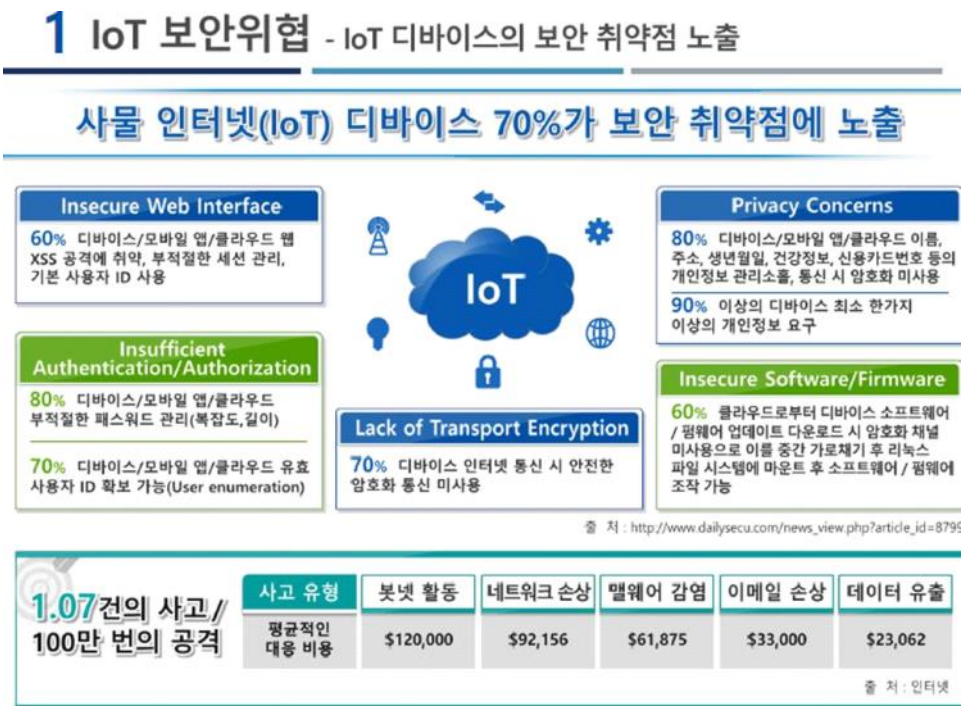
패킹 확인 및 언패킹 수행: 먼저 패킹여부를 확인하고 각 패커의 언패커를 이용하여 언패킹한다.

디버깅/리버싱: 대표적인 도구나 디버거를 이용해서 디버거를 수행하고 리버싱을 수행해본다.

8. 랜섬웨어

- 개념, 감염증상, 종류, 보안대책 등
- 개념: 금전적인 목적을 가지고 악성코드를 유포, 감연된 PC의 파일들을 암호화하고 금전을 요구하는 형태를 보인다. 복호화를 위해 결제를 하도록 유도한다.
- 감염증상: 문서들이 암호화 되어 이상한 확장자로 변하고 문서가 열리지 않는다. 금전을 요구하는 형태의 파일들만 열린다.
- 종류: CyptoLocker, CyptoWall, TorrenLocker 등이 있다.
- 최근 모바일 랜섬웨어도 등장하여 스마트폰의 자료보관도 주의하여야 한다.
- 보안대책으로는 이메일 사용 및 인터넷 사용할 때 주의가 필요하다.(악성링크, 첨부파일 클릭 등을 조심/ 광고배너를 함부로 클릭하지 않는 등)
- 그리고 가장 best보안대책은 중요자료를 정기적으로 다른 이동장치나 웹하드 등 안전한 곳에 백업하는 것이다.

9. IoT 보안위협



Iot보안위협은
Insecure web interface
Insecure software firmware 통신암호화 미흡
insufficient authentication
Privacy concern
5가지가 있고 사례로는 이런게 있다

10. 망분리 방식과 각각의 장단점

망분리란, 내부 업무망과 외부 인터넷망을 분리하여 두 영역이 서로 접근할 수 없도록 통제하고 차단하는 것. 망분리는 물리적 망분리와 논리적 망분리로 나뉘어 진다.

인터넷망: 인터넷을 사용할 수 있도록 연결되어있는 네트워크 구간

업무망: 인터넷과 분리되고 업무용으로 사용되는 네트워크 구간

장단점은 뒤에 표 보세요

구분	물리적 망분리	
구성방법	2대의 PC를 이용해 업무용과 인터넷용으로 PC 및 네트워크를 물리적으로 구분	
장점	높은 보안 수준 타 방식에 비해 상대적으로 높은 보안 수준 제공	
단점	고비용 신규 망구축 및 PC 지급으로 인한 고비용 신규 망 및 PC증가로 인한 관리 부담 증가	

논리적 망분리	논리적 망분리
서버기반 (SBC)	PC기반 (CBC)
서버기반의 가상 데스크톱을 구성하는 방식이 사용자 클라이언트에서 가상 데스크톱으로 원격 접속하여 이용한다. 중앙 가상 데스크톱에서 업무망 혹은 인터넷망을 분리하여 사용한다.	기존 사용자 Client에 가상화 SW를 설치하여 사용 가상화 SW를 통해서 PC에 기존 PC에 가상화된 인터넷/업무 영역을 생성한다.
물리적 망분리에 비해 비용 효율적 접속 장치를 통한 바이러스 및 악성코드 유입 업무망을 가상화할 경우 업무데이터에 대한 중앙관리 용이 및 내부정보 유출방지 효과	보조기억매체를 통한 정보 유출 및 악성코드 감염 타 방식에 비해 가장 비용 효율적
망분리 가상화 서버팜 구축 비용 발생 VDI 서버 장애 시 모든 사용자가 사용 불가능	다양한 PC환경에서의 가상화 SW호환성 문제로 인한 안정성/관리 효율성 이슈