1. **악성코드 감염 경로 및 유포 경로.**
2. 홈페이지, 웹하드, P2P, 이메일, 메신저, SNS, 이동형 저장장치 등을 통해 유포
3. 이메일: 정부기관 사칭 이메일을 통한 악성코드 유포: 악성코드 이메일을 발송-> 이용자가 응답 시 악성코드가 포함된 메일 재발송
4. **침해사고 주요사례(최근 3년 이내) 사고의 원인과 특징, 공격유형 등**

사례 인터파크 개인정보 유출사고(16’05),

사고의 원인과 특징:

1. 개인정보처리시스템 timeout 미설정
2. DB서버, 웹서버 등 비밀번호관리 소홀.
3. 임직원이 악성메일을 접속하게 되어 내부망에 악성코드 감염 확산 및 정보유출로 이어짐

공격유형: APT

1. **피싱, 파밍, 스피어피싱- 개념, 각각의 특징 및 차이점, 사례, 공격기법 등**

-

피싱

개념: private data를 낚는다(fishing)라는 의미의 합성어

불특정 다수에게 이메일/게시글 등을 통해 위장된 사이트에 정보를 입력하도록 유도하여 민감정보를 획득하여 재산상의 손해를 입히는 사기수법

-

피싱사례: 국민은행과 유사한 사이트를 만들어놓고 인터넷뱅킹 보안승급서비스를 해준다며 개인정보/금융정보를 입력하게 한다.

-

공격기법: 발신자 위조, 하이퍼링크 위조, 스크립트를 이용한 주소창 위조, 유사도메인 등으로 사용자가 메일의 악성링크를 클릭하게 한다. 악성링크를 클릭할 경우 변조된 사이트로 이동한다.

특징: 사용자가 주의깊게 살펴보면 알아차릴 수 있다.

파밍:

개념: 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 가짜 사이트로 유도. PC에서는 사용자가 URL로 접속하고자 할 때 host에 적혀있는 주소인 경우 DNS에 질의하지 않는다는 특징을 악용한 것이다. 따라서 공격자가host파일을 변조하면 사용자는 올바른 URL 주소로 접속했음에도 불구하고 변조된 host에 있는 해커가 유도한 사이트로 접속하게 된다.

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

스피어피싱:

개념: 피싱의 발전된 형태로 Phishing 은 불특정 다수를 대상으로 하지만 스피어피싱은 특정 타겟을 두고 공격하는 기법.

-

사례 및 공격방법

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

공격 대상 관련 행사(ex 모터쇼) 정보 수집 후 행사 관계자로 위장하거나 동일 커뮤니티 소속원을 가장하여 악성코드가 포함된 이메일을 발송.

1. **DDoS 공격 - 개념, 공격방법 및 종류, 최근사례**
2. 개념/공격방법: 악성코드에 감염된 좀비 PC들을 이용해 대량의 트래픽을 타겟에 전송하는 서비스 방해 공격
3. 3.4 DDoS공격 사례)
4. 해커가 유포/명령서버 해킹 및 숙주 사이트(웹하드업체)를 해킹하여 악성코드를 심어놓는다.
5. 약 10만대의 좀비PC에서는 감염된 웹하드 사이트를 통해 가짜 업데이트(좀비PC감염 소프트웨어)를 설치하게 된다.
6. 유포/명령서버에서는 좀비PC로 공격도구 보급, 공격대상/시점을 명령을 내린다.
7. 특정 시점이 되면 좀비 PC들은 타겟으로 DDoS공격 트래픽을 발생하게 된다
8. **좀비 PC 분석 절차**

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

1. **악성코드 유포방법**
2. 이메일: 정부기관을 사칭한 이메일을 통한 악성코드 유포시도: 악성코드 이메일을 발송-> 이용자가 응답 시 악성코드가 포함된 메일 재발송
3. 홈페이지: 공격자는 특정 서버에 서버해킹 후 홈페이지에 악성코드를 삽입해놓고 기다린다. 사용자가 홈페이지에 방문하면 악성코드가 자동전송되도록 구성되어있다.
4. 웹하드: 해커는 웹하드 사이트 운용서버를 해킹하고 악성프로그램 을 업로드해놓는다. 사용자는 홈페이지를 방문하고 컨텐츠 다운로드를 요청하는데 악성코드가 전송되고 실행된다.
5. **악성코드 분석- 정적분석, 동적분석**
6. 동적분석
   1. 파일 생성/삭제/변조 행위 분석
   2. 레지스트리 생성/삭제/변조 행위 분석
   3. 프로세스 생성/삭제/변조 행위 분석
   4. 네트워크 행위 분석
7. 정적분석
   1. 실행파일 유형 및 구조 분석
   2. 패킹 확인 및 언패킹 수행
   3. 디버깅/리버싱
8. **랜섬웨어 - 개념, 감염증상, 종류, 보안대책 등**
   1. 개념
      * 1. 금전적인 목적을 가지고 악성코드를 유포, 감연된 PC의 파일들을 암호화하고 금전을 요구하는 형태를 보인다. 복호화를 위해 결제를 하도록 유도한다.
   2. 감염증상
      * 1. 문서들이 암호화 되어 이상한 확장자로 변하고 문서가 열리지 않는다. 금전을 요구하는 형태의 파일들만 열린다.
   3. 종류
      * 1. CyptoLocker, CyptoWall, TorrenLocker 등
   4. 보안대책-
      * 1. 최근 모바일 랜섬웨어도 등장하여 스마트폰의 자료보관도 주의하여야 한다.
        2. 보안대책으로는 이메일 사용 및 인터넷 사용할 때 주의 필요

(악성링크, 첨부파일 클릭 등을 조심/ 광고배너를 함부로 클릭하지 않는 등)

* + - 1. 중요자료를 정기적으로 다른 이동장치나 웹하드 등 안전한 곳에 백업하는 것이다.

1. **IoT 보안위협**
2. Insecure web interface
3. Insecure software firmware
4. 통신암호화 미흡
5. insufficient authentication
6. Privacy concern
7. 망분리 방식과 각각의 장단점
8. 망분리란,
9. 내부 업무망과 외부 인터넷망을 분리하여 두 영역이 서로 접근할 수 없도록 통제 및 차단하는 것.
10. 망분리는 물리적 망분리와 논리적 망분리로 구분
11. 인터넷망: 인터넷을 사용할 수 있도록 연결되어있는 네트워크 구간
12. 업무망: 인터넷과 분리되고 업무용으로 사용되는 네트워크 구간
13. 망분리 장단점

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 물리적 망분리 | | |
| 구성방법 | 2대의 PC를 이용하여 업무용과 인터넷용으로 PC 및 네트워크를 물리적으로 구분 | | |
| 장점 | 높은 보안수준 타 방식에 비해  상대적으로 높은 보안수준 제공 | 단점 | 고비용 신규 망구축 및 PC 지급으로 인한 비용증가 신규 망 및 PC증가로 인한 관리 부담 증가 |

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