7차시. 4차 산업혁명을 위협하는 악성코드

01. 악성코드(Malicious Software, Malware)

- 전 세계적으로 하루에 약 100만 건의 악성코드가 유포되고 있다고 한다. 사이버 보안 침해 관련 뉴스가 연일 언론과 포털에 종종 메인을 장식하면서 전 세계를 두려움에 떨게 한 사이버공격은 이제 일상이 돼버린 듯하다. 인터넷에 연결된 모든 기기와 사람이 실시간으로 연결되는 초연결 사회의 4차 산업 혁명 시대는 어쩌면 신규 악성코드와의 전쟁의 시대일 수 있겠다는 생각이들 정도이다.

악성코드의 이해

- 미국의 상무부에서는 특별 기고를 통해서 아래와 같이 악성 소프트웨어 또는 악성코드의 정의를 하였다. '데이터를 파괴하고 파괴적이거나 침투적인 프로그램을 구동하고, 목표 컴퓨터의 데이터나 응용 프로그램 및 운영체제의 기밀성, 무결성 및 가용성을 침해하기 위하여 다른 프로그램에 은밀하게 숨어드는 프로그램', 즉, 의도적으로 피해를 주고자 만든 모든 실행 가능한 악의적인 목적을 가진 프로그램, 매크로, 스크립트를 지칭한다.
- 컴퓨터 바이러스 개념은 1972년 소설가 데이비드 제럴드의 소설 'When Harlie was One'에서 처음 등장하였다. 이후 1986년 최초의 MS-DOS 바이러스인 'Brain Virus'가 파키스탄 알비 형제에 의해서 만들어지는데 그 이유는 자신이 만든 프로그램이 불법 복제되는 것에 불만을 품었던 것이다. 1988년에는 최초의 웜(worm)인 '모리스 웜'이 등장하여 그 당시 국방 네트워크인 ARPANET에 연결된 6000대의 컴퓨터에 감염되었다. 1999년에는 멜리사(Melisa) 바이러스라는 매크로 바이러스가 출현하였으며 2000년 중반이후에는 변종의 웜들이 등장하면서 인터넷과 모바일 등을 통하여 전파되었다.
- 악성코드의 유형은 전파되는 방식이나 감염 이후의 악성행위에 따라 구분하기도 하지만 일반적으로 바이러스, 웜, 트로이목마, 스파이웨어로 구분한다. 개별적으로 학습하기로 한다.
- **바이러스**

  바이러스는 기존의 실행 프로그램에 붙어서 기생하는 소프트웨어로 다른 프로그램이나 실행 파일의 변형을 통해 감염시키며 아래와 같은 특성을 지닌다.

  - 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복제하는 프로그램

  . 여기서 변형은 원래 프로그램에 루틴을 주입하여 바이러스 코드의 복제를 의미

  - 복제와 감염이 주요 특징

  - 다른 네트워크의 컴퓨터로 스스로 전파지지는 않음

- **바이러스**

  바이러스 생존기간 동안 잠복단계, 전파단계, 트리거단계 그리고 실행단계의 4단계의 과정을 거치며 그 역할을 수행한다.

  - 잠복단계: 바이러스 모두가 잠복 단계를 거치지는 않지만, 바이러스는 휴면상태로 어떤 사건으로 활성화를 대기하는 상태이다.

  - 전파단계: 다른 프로그램이나 시스템의 디스크 영역에 자신을 복제하는 단계

  - 트리거단계: 바이러스는 원하는 조건이 활성화되어 의도한 기능을 수행하는 단계로 다양한 시스템 이벤트에 의해 유발

  - 실행단계: 바이러스의 기능이 수행되는 단계로 스크린에 메시지 표시나 파일 파괴 등 다양한 사건을 발생시킴

  바이러스는 1980년대 ~ 2000년대 초반 악성코드의 주류를 이루었는데 이 시기에 바이러스가 극성인 이유는 PC에 이용자 인증과 접근제어가 미흡하여 전파환경이 조성된 이유를 꼽는다. 그러한 바이러스는 아래와 같이 진화를 하면서 발전하였다.

- **1세대 원시형 바이러스**

  - 단순 자기 복제 기능과 데이터 파괴 기능

  - 부트 바이러스와 파일 바이러스로 분류

  [부트 바이러스]

  ▪ 플로피나 하드 디스크의 부트 섹터에 감염

  ▪ MBR과 함께 PC 메모리에 저장되고 부팅할 때 자동으로 동작

  ▪ 부팅 후에 사용되는 모든 프로그램을 감염

  ▪ 예: 브레인, 몽키, 미켈란젤로 바이러스

  [파일 바이러스]

  ▪ 파일을 직접 감염시키는 바이러스

  ▪ 실행파일(COM, EXE), 오버레이 파일, 디바이스 드라이버 등에 감염

  ▪ 감염된 실행 파일이 실행될 때 바이러스 코드를 실행

  ▪ 예: 예루살렘 바이러스(최초 파일 바이러스), 크로우, CIH(체르노빌) 바이러스

- **2세대 암호형 바이러스**

  ▪ 1세대 바이러스가 가진 특정 패턴을 진단하는 백신을 우회하기 위해 암호형 바이러스 제작: 바이러스 코드를 쉽게 파악하고 제거할 수 없게 암호화한 바이러스

  ▪ 바이러스가 동작할 때 메모리에 올라오는 과정에서 암호화가 해제

  ▪ 백신 제작자는 실행되어 올라온 바이러스를 분석하여 백신 개발

  ▪ 예: 슬로우(Slow), 캐스케이드(Cascade), 원더러(Wanderer), 버글러(burgler)

- **3세대 은폐형 바이러스**
  - ▪ 바이러스가 확산되어 전파되도록 감염 파일들이 일정 기간의 잠복기를 가지도록 제작
  - ▪ 예: 브레인(Brain), 조시(Joshi), 4096 바이러스
- **4세대 다형성 바이러스**
  - ▪ 파일이 감염될 때마다 그 형태가 변하는 다형성(Polymorphic) 기법을 이용하여 감염여부를 확인하기 어렵도록 한 바이러스
- **5세대 매크로 바이러스**
  - ▪ 주로 MS 오피스 프로그램의 매크로 기능을 이용하여 전파
  - ▪ 엑셀, 워드 같은 문서의 매크로 기능을 이용하기 때문에 실행파일을 이용하는 기존 바이러스보다 주의를 덜해 피해가 큼
  - ▪ 예: 워드 컨셉트(Word Concept), 와쭈(Wazzu), 엑셀-라눅스 바이러스, 멜리사 바이러스
  - ▪ 증상: 문서가 오픈되지 않거나 암호가 설정되어 있거나, 문서 내용에 깨진 글자나 이상 한 문구가 포함
  - * 매크로: 일련의 명령어를 반복하여 자주 사용할 때, 개개의 명령어를 일일이 사용하 지 않아도 되도록 하나의 키 입력으로 원하는 명령군을 수행할 수 있도록 된 프로그램 기능
- **차세대 바이러스**

  악성코드를 은닉하고 빠르게 전파되는 기법을 사용
  - ▪ 웜과 바이러스 경계를 파괴하는 다기능 악성 코드
  - - 바이러스+자기복제+트로이목마+ 발신자 제거 기능 포함
  - ▪ 감염이나 데이터 파괴보다는 시스템 장악 기능으로 진화
- 한편 바이러스는 감염시키고자 하는 목표에 따라 부트섹터 감염(Boot sector infector), 파일 감염(file infector), 매크로 바이러스(macro virus) 그리고 다중 바이러스(multipartite virus)로 유형을 나누기도 한다.

  - 부트 섹터 감염: 마스터 부트 레코드 또는 부트 레코드를 감염하며 바이러스를 포함한 디스크에서 시스템이 부팅될 때 전파됨

  - 파일 감염(file infector): 운영체제(OS)나 쉘이 실행 가능한 파일을 감염

  - 매크로 바이러스(macro virus): 응용 프로그램으로 표현되는 매크로 코드를 가진 파일을 감염

  - 다중 바이러스(multipartite virus): 하나 이상의 공격 유형을 조합하여 시스템 섹터와 프 로그램 파일을 감염
- **웜**

  웜은 네트워크를 통해 전파되는 악성 프로그램으로 감염시킬 더 많은 컴퓨터를 적극적으로 찾는 특성을 지닌다. 즉, 웜은 활성화되면 웜은 다시 복제와 전파를 진행하는데, 자신을 전파하는 목적으로 원격 시스템에 접근하기 위한 여러 방법을 이용한다.

- **웜**

  - 이메일이나 인스턴트 메신저 설비
  - 파일 공유
  - 원격 실행 능력
  - 원격 파일 접속 및 전달 능력
  - 원격 로그인 능력

  웜은 컴퓨터 바이러스와 같이 잠복기 단계, 전파단계, 트리거링 단계 및 실행단계를 거쳐 확산된다. 웜의 특징인 전파 단계에서는 일반적으로 다음 기능을 수행한다.

  - 감염시킬 다른 시스템에 접근할 적절한 메커니즘 탐색

  . 호스트 테이블, 주소 북(address book), 버디 목록, 신뢰할 수 있는 상대(trusted peer), 원격 시스템 저장소 등을 검사

  - 찾아낸 접근 메커니즘을 이용하여 원격 시스템에 자신의 복제를 전달하여 복사본이 구동되도록 함

  따라서 웜은 전파 형태에 따라 대량 메일 발송형(MASS Mailer형), 시스템 공격형, 네트워크 공격형으로 분류한다.

- **MASS Mailer 형 웜**

  ▪ 자기 자신을 포함하는 대량 메일 발송을 통해 확산되는 웜

  ▪ 메일 제목이 없거나 특정 제목으로 메일 전송

  - 치료 전까지 시스템에서 메일주소를 수집하여 계속 메일을 전송

  ▪ 주요 증상

  - 감염된 시스템이 많으면 SMTP 서버(TCP 25번 포트)의 네트워크 트래픽이 증가
  - 베이글 웜은 파일 실행시 가짜 오류 메시지 출력

  . Can't find a viewer associated with the file'

  - 변형된 종류에 따라 시스템에 임의의 파일을 생성

- **시스템 공격형 웜**

  ▪ OS 고유의 취약점을 이용해

  - 내부 정보를 파괴하거나 컴퓨터를 파괴하거나,
  - 외부 공격자가 시스템 내부에 접속하도록 백도어를 설치

  ▪ 패스워드 크래킹 알고리즘을 포함한 웜은 패스워드 취약 시스템 공격

  ▪ 예: 아고봇(Agobot), 블래스터(blaster worm), 웰치아(Welchia)

- **네트워크 공격형 웜**

  ▪ 특정 네트워크나 시스템에 대해 서비스거부(DoS) 공격을 수행

  ▪ 버퍼 오버플로우와 같은 시스템 취약점을 이용하여 확산되거나 공격하는 경우 많음

- **네트워크 공격형 웜**

  ▪ 분산 서비스공격을 위한 봇(Bot)과 같은 형태로 발전

  ▪ 예: 져봇(Zerbot), 클레즈(Klez)

  ▪ 주요 증상

  - 네트워크가 마비되거나 급속히 느려짐

  - 네트워크 장비가 비정상적으로 작동

- **백도어/트로이 목마**

  보안 메커니즘을 우회할 수 있는 기능을 은닉하고 잠재적 악성 기능을 가진 프로그램인 백도어와 트로이목마는 악의적인 공격자가 고의적으로 컴퓨터에 침투하여 사용자 컴퓨터를 조정한다. 어떤 경우에는 시스템 개체의 합법적 허가를 악용하여 트로이 목마 프로그램을 호출하기도 하며 백도어와 트로이목마를 구분하지 않고 백도어라고 통칭하기도 한다.

- **백도어**

  ▪ 원래 의미는 OS나 프로그램 생성시 인증과정 없이 OS나 프로그램에 접근할 수 있도 록 만든 일종의 통로

  - OS 개발 시 만약의 상황(설정 패스워드 모름)에 대비한 통로

  - 개발 완료 후에는 백도어를 완전 삭제하지 않는 경우 발생

  - 해커에 의해서 백도어 발견 시에는 치명적 취약점이 됨

- **트로이 목마**

  ▪ 백도어와 마찬가지로 OS의 원래 인증을 우회하여 원격에서 시스템 내부에 접근 허용

  - 설치과정이 관리자가 아닌 바이러스나 웜에 의한 것

  - 접근자가 관리자가 아닌 해커의 경우

- **스파이웨어**

  스파이웨어는 트로이목마와 비슷한 종류의 악성코드로 아래와 같은 특성을 지닌다.

  - 자신이 설치된 시스템의 정보를 원격지의 특정 서버에 주기적으로 전송

  - 사용자가 주로 방문하는 사이트, 검색어 등의 취향을 파악하는 목적 외에 패스워드와 같은 특정 정보를 원격에 전송하기도 함

  - 리얼 플레이어와 같은 상용 프로그램에 스파이웨어가 설치되어 문제시 됨

  . 사용자 정보 수집 시에는 반드시 사용자의 동의가 요구됨.

- **스팸**

  스팸은 원치 않는 대량의 이메일을 발송시키는 악성코드의 일종으로 이용자와 네트워크에 부담을 초래한다. 즉 네트워크는 스팸 이메일의 대량 발송으로 인한 트래픽 부담이 발생하며, 이용자는 정당한 이메일 만을 선택해야 하는 수고를 해야 한다. 최근의 스팸은 손상된 이용자 시스템을 이용하는 봇넷을 통해 발송되거나 일부 스팸은 합법적 메일 서버에서 발송된다.

- **스팸**

  또한 스팸은 말웨어를 전달하는 캐리어 역할을 수행한다. 이메일 첨부를 확인할 때 소프트웨어 취약점을 악용하여 말웨어가 설치되고 이어서 피싱 공격에 악용되기도 한다. 즉, 위장 웹사이트로 유도하여 로그인 및 패스워드 정보를 갈취하고 이어서 이용자로 하여금 금융 등의 중요정보를 입력하도록 유도하여 금전 피해까지 발생시킨다.

- **악성코드 탐지 및 대응**

  말웨어가 목표 시스템에서 활성화된 후 특정 조건이 부합되면 다양한 악성행위가 발생한다.

  - 감염 시스템 내의 데이터 파괴

  - 원하지 않는 이미지나 컨텐츠 노출

  - 사용자 데이터 암호화한 후 복호화 대가로 금전요구: 랜섬웨어

  - 시스템에 실제적인 손상 발생

  . 컴퓨터를 초기화 하도록 BIOS 코드의 재작성을 시도

  . 특정의 산업용 제어시스템 소프트웨어(SCADA)를 목표로 공격: 예, 스턱스넷

  - 논리 폭탄(Logic bomb)은 말웨어에 내장된 코드로 특정 파일이나 장비가 없어지는 순간, 특정요일이나 특정 날짜, 일부 소프트웨어의 특정 버전, 응용 프로그램을 특정 사용자가 이용하는 경우 등의 특정 조건이 부합한 경우 폭발(explode)하듯 악성행위가 실행

  심지어 악성코드에 감염된 피해자의 시스템을 장악하여 공격자가 원격에서 조정하면서 이용할 수 있는데, 이런 경우를 봇(Bot) 또는 좀비 컴퓨터라 부른다. 이렇게 함으로써 실제 공격자는 추적을 차단하면서 다수의 좀비 컴퓨터를 이용하여 다른 공격을 개시하게 된다. 여기서 다수의 좀비 컴퓨터 집단으로 봇넷(botnet)이라 부르며 분산 서비스 공격 등의 조직적인 공격에 이용된다.

  이러한 악성코드의 행위에 대한 대응으로 선제적 예방 대책을 고려하게 된다. 주요 예방 요소로는 정책, 인식제고(awareness), 취약점 완화, 위협 완화를 포함한다.

  - 정책: 기업이나 조직의 악성코드에 대한 예방적 대응으로서 예방정책 수립

  - 인식 제고: 사회공학적 공격 대응을 위한 사용자 인식제고 및 교육

  - 취약점 완화: 악용 가능한 취약점 수를 줄이기 위한 최신 버전의 패치 업데이트

  - 위협완화: 응용 및 데이터에 대한 접근제어 강화

악성코드 전파방식

- 악성코드는 다양한 경로를 통해서 전파된다. 악성코드는 이메일, 웹사이트 방문, 메신저 프로그램, P2P프로그램, 파일 다운로드, 상용 프로그램 취약점 및 USB 등은 물론 보안 의식이 부족한 사람을 통해서 전파된다. 이 가운데 대표적인 전파경로는 이메일이다.

[악성코드 전파 경로]

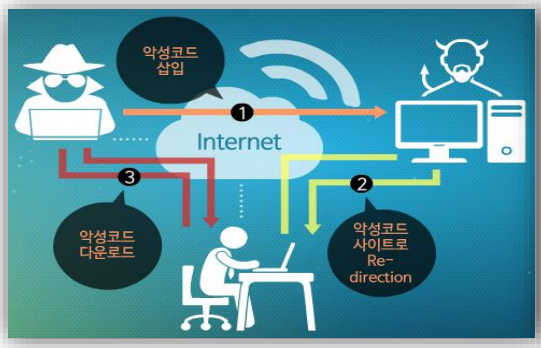
- 아래의 그림은 웹사이트를 통한 악성코드의 유포과정을 도시한 것이다.

  ① 이용자들이 많이 방문하는 웹사이트가 해킹을 당하여 악성코드가 삽입

  ② 보안패치가 적용되어 있지 않은 사용자 PC는 웹 서핑 과정에서 악성코드 사이트로 re-direct

  ③ 악성코드 다운로드하면서 감염

- 감염 후에는 개인정보 유출을 통한 다른 2차 피해 발생하게 된다



[웹사이트를 통한 악성코드 전파]

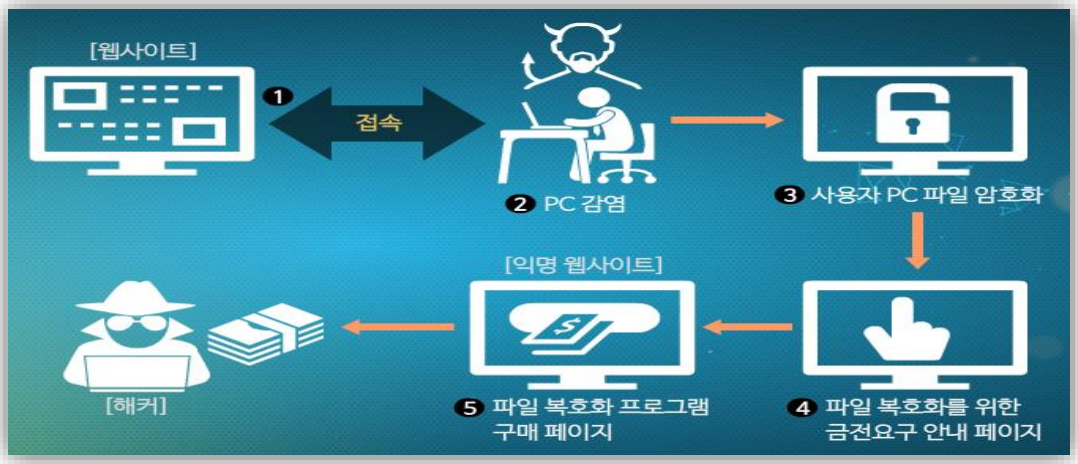
[악성코드에 의한 2차 피해]

02. 랜섬웨어의 이해

- 세계 최대 소프트웨어 회사 마이크로소프트(MS)의 브래드 스미스 사장(사진)이 올해 5월 전 세계를 혼란시켰던 '워너크라이 공격'의 배후로 북한을 지목했다. 워너크라이는 MS 윈도 운영체제를 교란시킨 랜섬웨어로 단기간 내 150여 개국에서 23만 대 이상의 컴퓨터를 감염시켜 큰 혼란을 불러일으켰다. 2015년과 2016년에는 랜섬웨어가 국내에서 극성을 부리면서 많은 사람들을 경약시켰지만 지금은 어느덧 일상으로 받아들이는 분위기다. 그러한 랜섬웨어에 대해서 학습한다.

랜섬웨어의 개념 및 감염경로

- 랜섬웨어(ransomware)는 '인질에 대한 몸값(Ransom)'에서 유래한 용어이다. 정보를 인질처럼 잡아 일방적으로 암호화한 뒤 이를 해제하기 위한 키(Key)에 대한 금전적 대가를 요구하는 사이버 범죄행위인 것이다. 비트 코인 등 추적이 어려운 전자화폐를 주로 요구하며 기존의 금전 목적의 해킹에 대한 수익 모델 진화과정에서 등장한 신종 사이버 범죄 행위이다.
- 주요 감염경로는 메일, 웹사이트, 스마트폰의 순이다. 즉, 중요문서로 위장한 메일을 수신하도록 하고 첨부파일의 클릭을 유도하여 감염된다. 따라서 샌드박스와 같은 가상화 환경에서 메일 수신을 권장하며 메일 보안 솔루션을 적용하여 피해를 예방할 수 있다. 그림 4는 웹사이트를 통해 랜섬웨어에 감염되는 과정을 도시한 것이다. 웹사이트를 통해 랜섬웨어에 감염된 PC의 파일은 암호화되며 파일 복호화를 위한 금전요구 안내 페이지/파일 복호화 프로그램 구매 페이지를 접하면서 랜섬웨어의 피해를 겪게 된다.



랜섬웨어 유형 및 특성

- **랜섬웨어 유형**

  일반적으로 랜섬웨어는 난이도에 따라 스케어웨어(scareware), 락스크린(lock-screen) 바이러스 그리고 네스티 스터프 바이러스(really nasty stuff)로 분류한다.

- **스케어웨어(scareware)**
  - ▪ 팝업창으로 감염사실을 지속적으로 알려 겁을 주면서 문제 해결 대가를 요구하는 초기 랜섬웨어 형태
  - ▪ 2000년대 불량 안티바이러스 판매기법에서 비롯
- **락스크린 바이러스(Lock-screen Virus)**
  - ▪ 지능적인 공포심 유발 전략을 활용
  - ▪ FBI/사법부 로고가 들어간 창을 띄워 놓고 불법 다운로드 위반 벌금 협박
  - ▪ 성인 사이트 방문 대상자로 경찰빙자 금전 요구
- **네스티 스터프 바이러스(Really Nasty Stuff)**
  - ▪ 금전 요구 불응 시 컴퓨터 개인파일/자료를 열지 못함
  - ▪ 경제성, 전파력, 효용성 기능 등을 겸비한 형태로 발전
- **AIDS 트로이목마**
  - 1989.12.8.~12.12: PC 사이보그사의 에이즈 정보 디스켓을 통해 유포된 스케어웨어
  - ▪ 하드 디스크의 루트 디렉토리 정보를 암호화 하는 트로이목마
  - 인증료 189달러를 요구: 파나마의 한 주소로 송금토록 함
- **지피코더(GPCoder)**
  - 2005년 크로튼(krotten), 아키비우스(Archiveus)와 함께 멀웨어 트로이카 명성 획득
  - 당시로는 1024 비트의 강력한 RSA 암호화 방식 사용
- **분도(Vundo)**
  - 2009년 등장한 scareware 에서 랜섬웨어로 전환한 첫 사례
  - ▪ PDF, DOC, JPG 파일을 대상으로 암호화
- **레베톤(Reveton)**
  - 2012년 경찰기관을 사칭한 대표적
  - 성인물 사이트 운용자, 불법 콘텐츠 유통자 등을 대상
  - ▪ 복호화에 대한 보상보다는 벌금을 요구하는 수법을 사용

[경찰기관 사칭 랜섬웨어 화면]

- **크립토락커(Crypt0L0cker)**
  - 2013년 말 등장
    - 게임오버 제우스(Gameover Zeus)라는 봇넷을 통해 전파
    - 단기간 내 300만 달러의 수익을 냄
    - 2014년 5월 국제 공조로 게임오버 봇넷 폐쇄
  - 이후 크립토월(CrytoWall)이 새로 등장
- **Locky Ransomware**
  - 2015년 2월 등장, 다양한 종류의 파일을 암호화
    - 하루 10만대 속도로 사용자 PC를 감염
    - 발견 당시에는 매크로가 포함된 문서 파일을 이메일에 첨부
    - 매크로 실행하면 랜섬웨어를 다운로드하는 방식으로 유포
  - 단순 협박이 아닌 다단계 사업으로 진화
    - 파트너 모집, 기술전수, 수수료 수익 회수
    - Locky 랜섬웨어 감염 시 암호화한 파일 확장자는 .locky 로 변경
    - 비트코인 지불 요구
    - 한글문서 파일(hwp)도 암호화: 공격대상이 국내 기관및 개인 포함
    - 현재 테슬라크립트에 이어 Locky 랜섬웨어가 광범위하게 유포 되고 있음
- **Cerber Ransomware**
  - 음성을 통해 파일 암호화 사실을 통보
    - 암호화된 파일들은 모두 .cerber 확장자로 변경
    - html, bxt, vbs 파일을 생성하여 감염사실을 사용자에게 보냄
    - 파일복구 대가로 비트코인 요구
    - 감염 시 생성된 v b s 파일을 통해서 PC에서 음성 출력

    “attention! attention! attention! Your documents, photos, databases and other important files have been encrypted!”
- **키레인저(KeRanger)**
  - 2016년 2월 등장하여 맥 환경을 공격
    - OS X의 BITTORRENT 관련 어플인 Transmission의 공식 웹사이트의 정상 파일을 악성파일로 변조해 유포

    * BitTorrent: P2P 형 파일 공유 프로그램

    * Transmission: Bit Torrent client
    - 감염 후 3일간 잠복 후 Tor 익명 네트워크를 통해 C&C와 연결
    - 파일 암호화와 함께 파일 복구 시스템도 무력화

- **랜섬웨어의 특징**

초창기에는 공격자의 암호키 없이도 파일 복구가 가능한 경우가 많았으나 최근 들어 대칭키 알고리즘인 AES와 비대칭키 알고리즘 RSA를 동시에 사용하여 공격자의 암호키 없이 파일 복구가 거의 불가능한 상황이다.

아울러 랜섬웨어의 진화 방향도

- 대규모 공격에서 표적형 공격으로 대가 상승
- 복호화 대가 요구에서 정보노출 협박으로 수익극대화
- 개인대상에서 업체나 정부로 확대
- 대규모 다단계 사업화
- 클라우드(BYOD), 사물인터넷 등으로 대상 확장
- 스마트폰: 화면잠금에서 SD카드의 문서, 이미지 암호화

- **랜섬웨어 감염 증상 및 복구여부**

초창기에는 공격자의 암호키 없이도 파일 복구가 가능한 경우가 많았으나 최근 들어 대칭키 알고리즘인 AES와 비대칭키 알고리즘 RSA를 동시에 사용하여 공격자의 암호키 없이 파일 복구가 거의 불가능한 상황이다.

아울러 랜섬웨어의 진화 방향도

- 대규모 공격에서 표적형 공격으로 대가 상승
- 복호화 대가 요구에서 정보노출 협박으로 수익극대화
- 개인대상에서 업체나 정부로 확대
- 대규모 다단계 사업화
- 클라우드(BYOD), 사물인터넷 등으로 대상 확장
- 스마트폰: 화면잠금에서 SD카드의 문서, 이미지 암호화

랜섬웨어에 감염되었을 경우 암호화 복구 관련

- 요구하는 돈을 지불할 경우 복구해주는 경우도 있으며 돈만 받고 먹튀하는 경우도 있음

. 복구대행업체에 의뢰하는 경우에도 비트코인 환전을 대신해주는 수준인 경우가 많음

- 랜섬웨어 유포자 검거나 랜섬웨어 해제키를 찾을 때까지 기다림

. 테슬라 크립토 개발자가 마스터 키를 공개

▪ 현재 TeslaDecode로 teslaCrypt 0.3.4a ~ 2.2.0까지 복구 가능: ecc, ezz, exx, xyz, zzz, aaa, abc, ccc, vvv, … 복구

. CoinVault 개발자/유포자 검거(2015.11.13)

▪ 복호화 키 받아 카스퍼스키에서 복구툴을 만들어 배포한 사례도 있음

- 복구지원 툴 사용(복호화 키가 확보된 경우)

. 안랩/카스퍼스키랩: 크립토xxx 2.0등 일부 랜섬웨어에 대해 완전 혹은 일부 복구 지원

- **랜섬웨어 감염 증상 및 복구여부**

  - 시스템 복원 기능 활성화

  . 윈도우 비스타/7/8 버전의 볼륨 쉐도우 복사본 검색 프로그램 활용

  . 기존의 백업복원 지점 삭제를 시도 후 감염하는 랜섬웨어도 있음

- **랜섬웨어 예방 및 대응**

  랜섬웨어의 최선의 대응책으로는 백업과 격리 그리고 예방이다.

- **백업**

  ◦ 물리적으로 격리된 드라이브(Ex. DVD) 사용

  ◦ 동기화 클라우드 서비스 이용: 원드라이브, 구글드라이브, 드롭박스

  ◦ 폴더위치 활용: System 32, OS 폴더

- **하지만 무엇보다도 평상 시 예방 조치가 더욱 중요하다.**

- **OS 및 백신 프로그램의 지속적 업데이트**

  . 윈도우 업데이트

  . 바이러스 토탈 활용: 접속 사이트 및 다운로드 파일 점검

  . Exploit(취약점) 차단 솔루션이나 안티 랜섬웨어 활용을 권고

  ▪ 취약점 차단 솔루션: 하우리 바이로봇 APT 쉴드, 알약 잇스플로잇 쉴드, 멀웨어바이트 안티 익스플로잇(베타)

  ▪ 안티 랜섬웨어: 앱체크, 비트 디펜더, 멀웨어바이트

- **읽기 전용 디스크 설정**

  ◦ 백업 디스크는 Diskpart 명령을 사용하여 읽기전용으로 설정: 파일 위변조차단 효과

- **보안취약 S/W 삭제**

  ◦ 플래시 보안 취약점을 이용한 랜섬웨어 극성

  . 플래시 플레이어를 사용하는 서비스 사용 불가를 고려

- **평시 습관 주의**

  ◦ PC 등: 스팸성 이메일 실행 자제

  ◦ 스마트폰: 공식 마켓에서 확인 후 앱 다운로드

  ▪ 문자/SNS 내 URL 실행

- **보안 패치**

  ◦ SW/윈도우 OS 최신 업데이트

  ◦ 취약점 공격 차단 프로그램 설치(Anti-Exploit Solution)

- **파일 백업 관리**

  ◦ 중요 파일 권한 변경(읽기전용)

- **파일 백업 관리**
  - ◒ 네트워크 폴더 사용자 접근 권한 변경
  - ▪ 감영 PC를 통해 연결될 경우 감염 우려
  - ◒ 윈도우 시점 복구 기능 사용
  - ◒ 사용자 파일 백업 및 복원 기능 사용(별도 백업 프로그램 사용)
- **랜섬웨어에 감염된 경우의 수동 대처 방법**
  - – 감염 확인 시 무조건 컴퓨터 종료하여 암호화 진행을 차단
  - – 윈도우 자체복구 모드나 부팅 USB를 통해 복구 모드 진행
  - ▪ 랜섬웨어 활동을 차단하고 랜섬웨어 감염여부 확인
  - ▪ 암호화되지 않은 파일을 백업하여 피해 최소화