주요 민간협회 · 공공기관 · 보안전문가 초청 랜섬웨어 예방 간담회

랜섬웨어 침해사례 및 대응방안

경 찰 청
사이버안전국
CYBER BUREAU

1 랜섬웨어(Ransomware)의 정의

○ Ransom(몸값)+Ware(제품)의 합성어

○ 전자기기 화면을 잠그거나, 전자기기 내 파일을 암호화 후 복호화를 빌미로 금원을 요구하는 악성 프로그램

○ 수백종에 이르는 변종이 있으며, 현재는 사용자 PC 내 주요 파일들을 암호화하고 일정한 비트코인을 요구하는 사례가 대부분

◎ 비트코인이란? bitcoin

- 개인정보를 취급하는 중앙은행 없이 개인 간 익명거래가 가능한 가상통화의 한 종류/ 1비트코인(BTC)는 330만원 상당('17. 6. 현재)

◎ 랜섬웨어 감염화면(예시-비너스락커)

◎ 어떤 파일들이 암호화되는지?

- 공격자가 설정한 값에 따라 다르나, 대체적으로 문서, 사진, 영상 등을 포함하며 상용되는 대부분의 확장자를 암호화. 특히 최근에는 한글문서(.hwp)파일을 암호화하는 사례 등장

2 랜섬웨어 유포 경로 및 주요 사례

1 피싱 이메일 첨부파일 실행

사례) '17년 1월, 한글 이메일 첨부파일로 중·소상공인에게 랜섬웨어 집중 전파 등

'인터파크 고객정보 리스트' 사칭한 랜섬웨어 등장(전자신문)

'입사지원합니다' 이메일 열었더니 "돈 내놔" PC 먹통(연합뉴스)

- 피싱 이메일의 첨부파일에 문서·이미지 등으로 위장된 악성코드를 첨부하여 랜섬웨어를 실행하게끔 유도

- 2016년까지는 영문 이메일로 유포하는 경우가 많았으나, 올해에는 정교한 한글 이메일로 첨부파일 실행을 유도하는 사례가 본격 출현

<한글 피싱메일 예시>

제목: 예약관련 문의드립니다

안녕하세요 이창수라고 합니다

이번달 말쯤해서 여행을가려고 합니다

갑자기 일정이 잡힌거라 주위에 물어보니

추천을 해주셔서 문의를하게 되었습니다^^

정말 오랜만에 가는 휴가다보니 설레네요..ㅎㅎ

자세한 일정이랑 관련해서 간단한 질문사항들은 워드에 정리를하였습니다

여권사진이랑 같이 첨부하니

확인하신 후 예약가능여부를 알려주세요

여권이랑 같이 보내서 비밀번호를 설정해두었습니다

비밀번호는 1122로 설정했구요

압축해제하셔서 확인하시면 될거에요

답변메일 부탁드릴께요~

감사합니다

Subject: 야간 물류입출고 지원합니다

안녕하세요

세부사항은 지원서에 작성하였구요

신분증사본 같이 첨부하였습니다

그만큼 진정성있게 지원한다는거 알아주세요

이게 개인정보이다보니 압축파일에 비밀번호를 걸었습니다

비밀번호는 '1234' 이구요

egg파일은 알집압축파일입니다

꼭 일하고 싶습니다

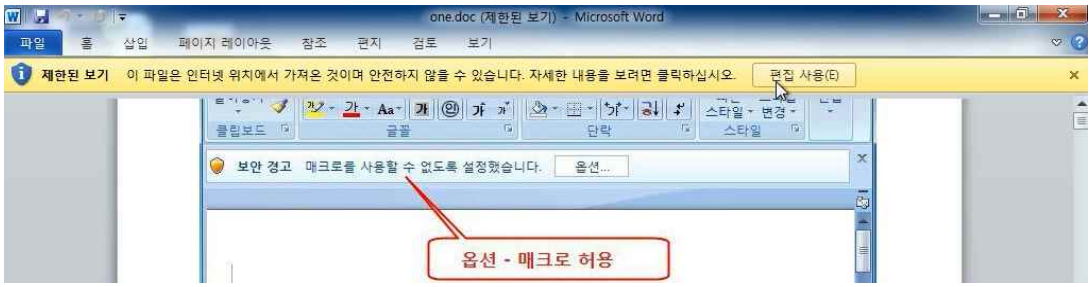
잘 부탁드리겠습니다

감사합니다

- 이메일에 실행파일(.exe) 등이 포함된 경우, 혹은 문서파일로 보이지만 상세 확장자를 확인하면 바로가기 파일(.lnk)인 경우, 문서가 정상적으로 실행되지만 매크로 실행을 유도하는 경우 악성코드일 가능성이 높음

<악성 첨부파일 예시(바로가기 위장형)>

<악성 첨부파일 예시(매크로 실행 유도형)>



2 악성코드에 감염된 페이지 접속

사례) '16년 6월 초 OO 사이트 접속자 랜섬웨어 감염 등

온라인 커뮤니티 'OO' 랜섬웨어 피해 속출(SBS)

"△△에서 랜섬웨어 유포됐어요" 커뮤니티 발칵(국민일보)

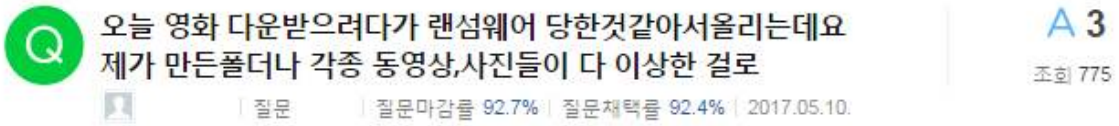
- 악성코드에 이미 감염되어 있는 홈페이지에 단순 접속만 해도 랜섬웨어에 자동으로 감염될 수 있음

- 익스플로러, 플래시(Flash), 자바(Java) 등 컴퓨터에 설치되어 있는 프로그램의 취약점을 이용한 공격기법으로,

- 이들 프로그램의 보안 업데이트가 되지 않은 경우, 공격자가 악성코드 유포지로 설정한 홈페이지에 접속하는 것만으로도 감염됨

3 토렌트, 파일공유 사이트 등을 이용한 파일 다운로드

사례) 영화·드라마 다시보기 사이트, 웹하드·토렌트 등을 통한 다운로드시 감염



- 토렌트, 웹하드 등을 통해 다운로드한 영상, 소프트웨어 혹은 영화·드라마 다시보기 사이트 등을 통해 감염되는 사례가 다수
- 공격자의 입장에서 랜섬웨어를 쉽게 대량으로 전파할 수 있는 방법으로 유사 피해가 계속될 것으로 전망

4 워너크라이 랜섬웨어 사건

사례) '17. 5. 운영체제(윈도우)의 취약점을 이용해서 인터넷 연결만으로도 랜섬웨어에 감염되는 특이 사례(워너크라이) 발생

일본 혼다, 워너크라이 공격에 자동차 생산 일시 중단(IT조선)

- '워너크라이' 랜섬웨어는 운영체제(윈도우)의 보안취약점을 랜섬웨어 공격에 이용하여 세계 100개국 이상에서 취약한 PC를 감염시킴
- 기존 랜섬웨어와 달리 인터넷 연결만으로 감염되는 특이점 존재

5 기 타

- (SNS) 페이스북 등에서 단축 URL 등을 사용한 유포사례 존재
- (스마트폰) 해외에서는 스마트폰의 랜섬웨어 감염사례가 지속적으로 보고되고 있어 국내에서도 본격적으로 유입될 것으로 전망

3 업종별 랜섬웨어 감염 가능 시나리오

중소기업 / 무역업체

시나리오 1.
인사담당자에게 채용 문의 피싱 메일 송부

시나리오 2.
이메일 무역사기와 랜섬웨어 결합
- 송장/계좌번호 변경 안내 메일 등

시나리오 3.
취약한 회사 홈페이지 대상
관리자 권한 탈취 및 중요 자료 접근
- 서버에서 직접 랜섬웨어 실행 가능

금융기관

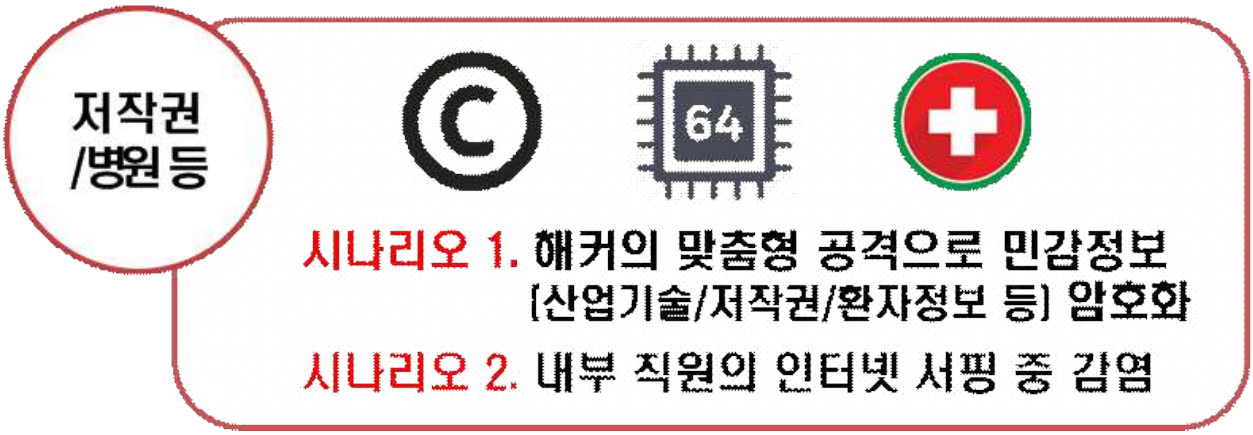
시나리오 1.
단말 PC(ATM 기기 등)의 랜섬웨어 감염

시나리오 2.
홈페이지가 악성코드 유포지로 이용

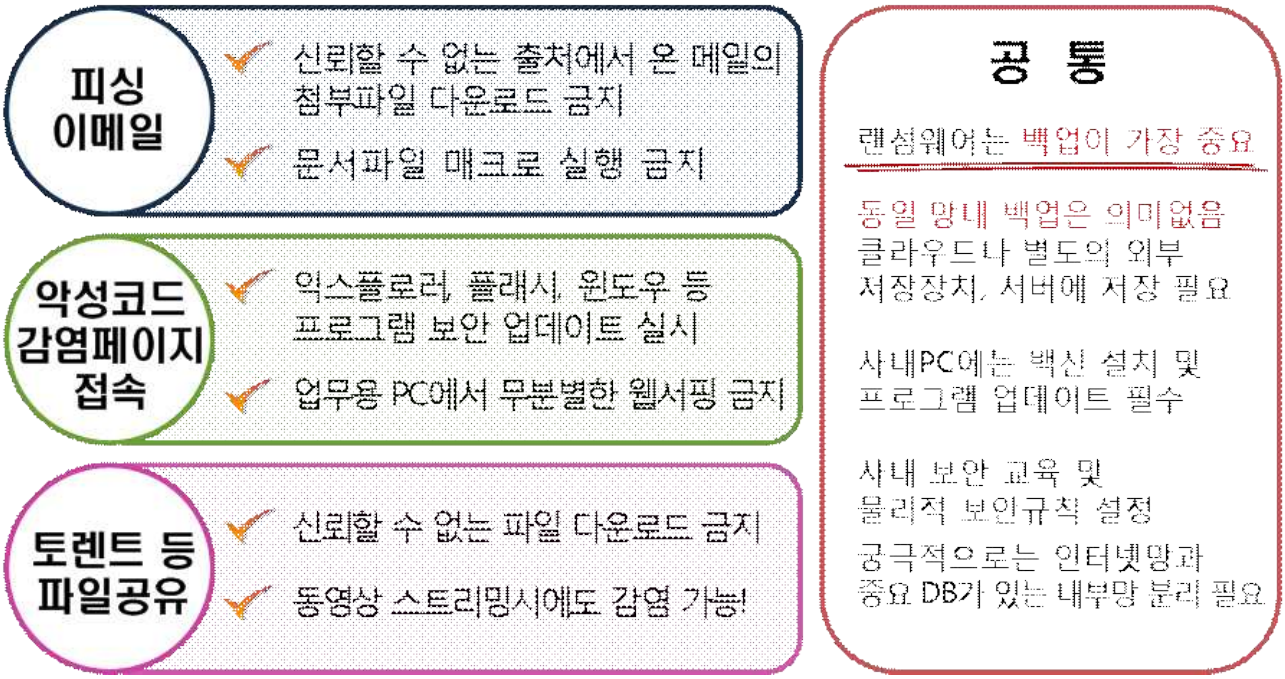
온라인 업체 등

시나리오 1.
온라인 배너 광고를 통한 랜섬웨어 유포

시나리오 2.
온라인 게시판을 통한 랜섬웨어 유포

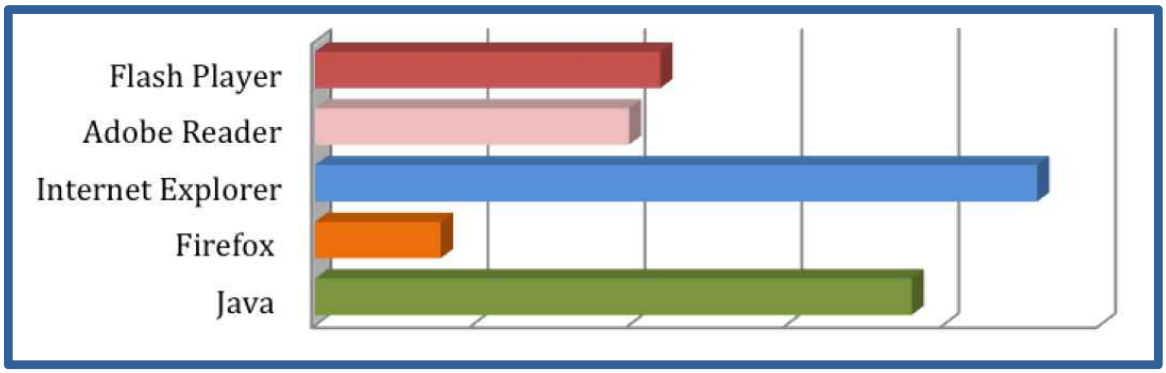


4 랜섬웨어 예방 방안



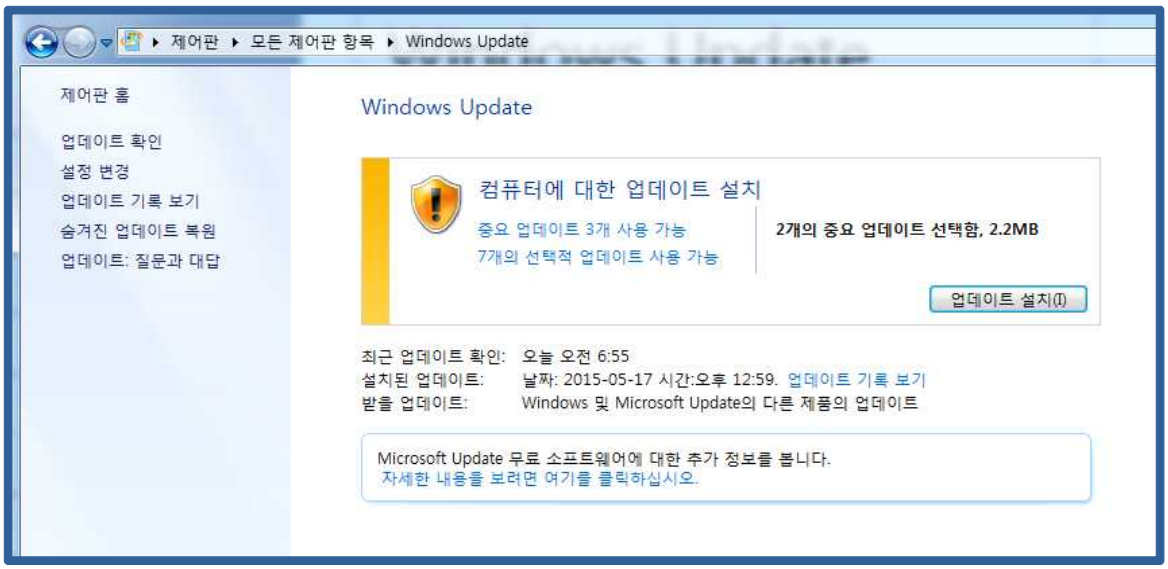
- **(공통)** ① 중요자료는 별도의 저장장치에 백업하고, ② 주요 프로그램을 주기적으로 업데이트하며, ③ 신뢰할 수 없는 파일을 다운로드 및 실행하지 않아야 함

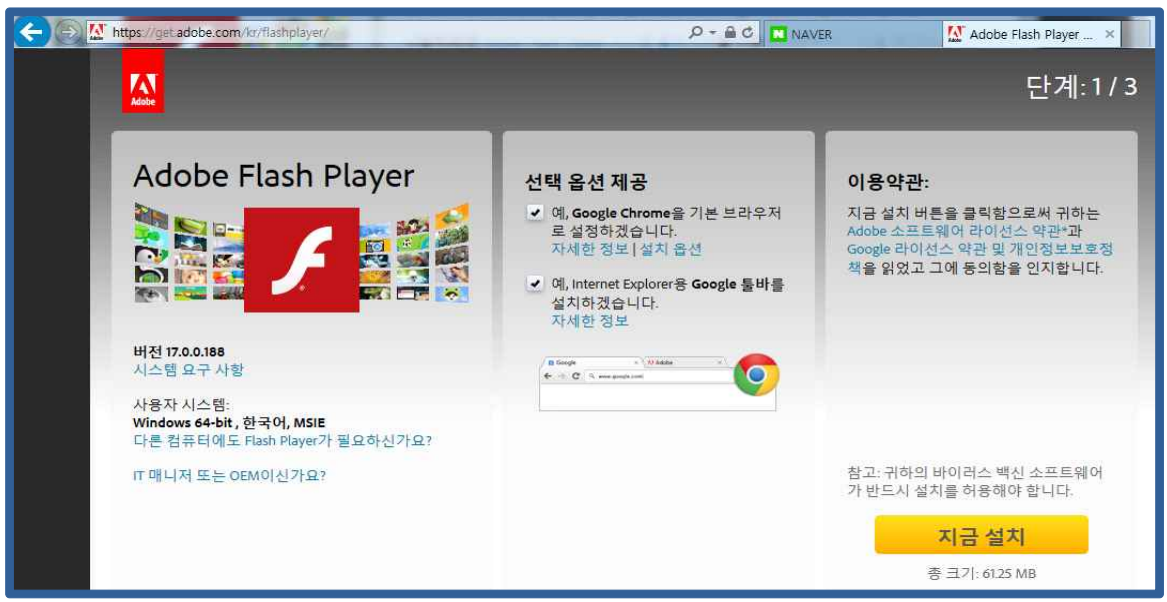
- 일반적으로, 보안 취약점이 많이 보고되어 공격자가 쉽게 이용할 수 있는 프로그램은 아래 그림과 같이 **인터넷 익스플로러, 자바, 어도비 리더, 플래시 플레이어** 등이 있음



<주요 프로그램별 취약점 수 비교>

- 위 프로그램에 대해서는 제조사에서 제공하는 최신 업데이트를 주기적으로 해야만 랜섬웨어 감염을 막을 수 있음





5 감염시 행동요령

○ 랜섬웨어에 감염되었다면 다음과 같은 조치가 필요합니다.

- 포맷하지 않은 상태로 가까운 경찰서 사이버팀이나 한국인터넷진흥원(KISA, 118)에 신고
- 복구 가능한 랜섬웨어인지 여부 확인(아래 별첨)
- 복구가 현재 불가능한 랜섬웨어라도 추후 복구 프로그램이 개발될 수 있으므로 감염된 중요파일을 별도로 보관하는 방안을 권장
- 감염된 PC는 신고 이후 포맷 및 백신 설치 후 사용

○ 랜섬웨어는 일반적으로 복구가 어려우나, 아래 사이트에서 일부 랜섬웨어의 복구 프로그램을 제공하고 있습니다.

기관·업체	제공 서비스	사이트
경찰청	노모어랜섬 한국어페이지 제공 (랜섬웨어 60여종의 복구프로그램 제공)	www.nomoreransom.org /co/index.html
하우리	백신 및 일부 랜섬웨어 복구 프로그램 제공	www.hauri.co.kr/Ransomware/
안랩		www.ahnlab.com/kr/site /securityinfo/ransomware/index.do
이스트 시큐리티		www.estsecurity.com /ransomware#decryption
카스퍼스키		noransom.kaspersky.com

Q) 노모어랜섬(No More Ransom)이란?

A) 유로폴과 카스퍼스키랩, 인텔시큐리티 등에서 '16. 7. 시작한 전세계 랜섬웨어 대응 프로젝트로, 노모어랜섬 사이트(www.nomoreransom.org)에서 랜섬웨어 복구 도구 제공(단일사이트 중 최다, 경찰청 가입 및 한국어 사이트 제공 중)

<랜섬웨어 예방 홍보 웹툰>


우리 오늘따라 사진빨 좀 받는데? 컴퓨터에 옮겨 놓자!
좋아! 근데 자기야~ 너무 뒤에서 찍지마~^^
찰칵
컴퓨터에 다 옮겼고~ 어... 뭐지?
(경고) 모든 파일을 암호화했으니 찾고 싶다면 돈을 내놔라!
이게뭐야..? 내 사진! 날아가면 어떡해?! 돈을 보내야하나?!
네?! 그럼 제 파일들은 어떡해요?!
잠깐! 현혹되면 안돼요! 복원이 확실치 않고 오히려 랜섬웨어 범죄를 조장합니다!
※랜섬웨어 몸값(ransom)과 제품(ware)의 합성어로 컴퓨터 사용을 제한하고 해제 비용을 요구하는 악성코드
당황하지말고 피해 상태 그대로 신속하게 경찰에 신고하고
한국인터넷진흥원 및 전문IT보안업체에 피해복구와 악성코드 치료를 요청하세요!
"랜섬웨어" 예방 수칙 기억하기! 참 쉽죠~?
1 중요한 자료는 정기적인 백업
2 백신·윈도우·익스플로러·플래시 등 항상 최신 업데이트
3 이메일의 첨부 파일 클릭 주의!