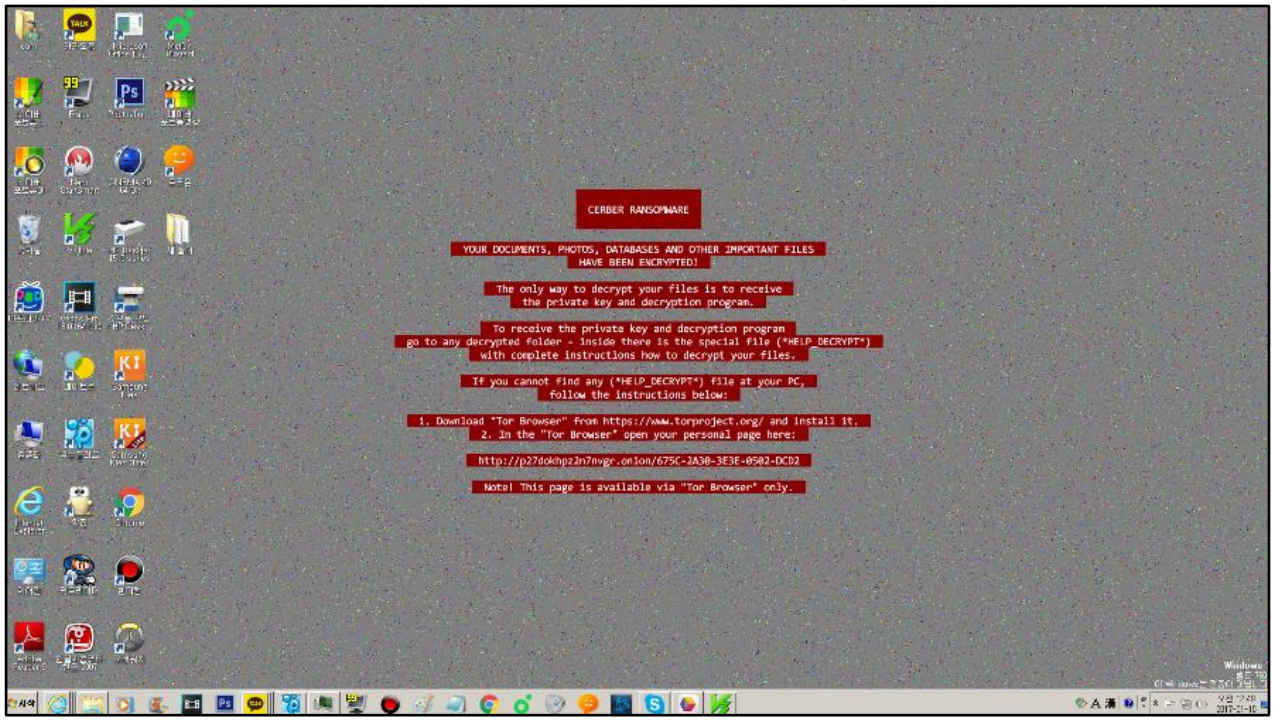
작성일자 -2019-02-28-

- **랜섬웨어란?**

몸값을 뜻하는 Ransom과 제품을 뜻하는 Ware의 합성어이며, **사용자의 동의 없이 컴퓨터에 설치하고 무단으로 사용자의 파일을 모두 암호화 시켜 인질로 잡아 금전적인 행위를 하는 악성 프로그램**을 말한다



랜섬웨어에 걸린 PC 화면 예시

감염되면 CPU 쿨러가 미친 듯이 회전하며 파일을 암호화하기 시작한다. 때문에 하드디스크와 메모리 점유율이 급격히 상승하게 된다. 종류에 따라서는 일정한 텀을 주면서 처리하여 사용자가 컴퓨터의 이상을 쉽게 눈치채기 힘들게 만든 종류도 있다.

암호화가 모두 완료되기 전에 재부팅하면 랜섬웨어에 걸렸습니다 라는 식의 협박 텍스트 파일과 복호화 파일을 전달할 html 페이지가 자동으로 팝업 된다. 그리고 대부분의 작업을 할 수 없다. 대표적인 증상은 다음과 같다.

1. 중요 시스템 프로그램이 열리지 않는다.

2. 윈도우 복원 시점이 제거되거나 업데이트를 막아버린다.

3. 별도의 다른 악성코드를 심기도 한다.

4. CPU와 램 사용량이 급격하게 증가하고 파일들이 암호화된다.

5. 안티 바이러스가 오작동한다. 혹은 강제로 꺼지거나 삭제된다.

6. 안전 모드로 진입할 수 없다.

7. 암호화된 파일을 열 수 없다.

8. 강제로 이동식 저장 장치의 연결을 해제시킨다.

9. 재부팅을 할 때마다 랜섬웨어 txt 파일, html 파일이 시작 프로그램 목록에 추가된다.

10. 악성코드는 대략 특정 디렉터리에 자기 자신을 복사하는 유형이 꽤 많다. 대표적인 경로는 아래를 참조하자.

- C:₩Program Files₩
- C:₩Users₩(사용자 이름)₩Appdata₩Roaming₩

물론 레지스트리에도 재부팅 시 이 경로의 프로그램을 실행하도록 되어 있으며, 이미 자기 자신으로 인해 암호화가 된 시스템인지 체크하는 루틴이 보통 별도로 있다

11. 실행되면 숙주 파일이 사라지는 경향이 있다. 따라서 한번 암호화가 끝나면 다시 암호화가 되지 않는다.

12. 특정 경우 연결된 이동식 저장매체 또한 감염된다**. 외장하드, USB 메모리, SD카드 심지어 플로피 디스크도 감염된다.** 조심할 것.

- **랜섬웨어 의심이 갈 때는?**

– 셧다운

1. **우선 데스크탑의 경우 전원 플러그를 뽑는 등 컴퓨터를 물리적으로 완전히 종료해야 한다. 노트북이라면 배터리 일체형 제품의 경우 전원 버튼을 꾹 누르거나 배터리 분리형 노트북인 경우 배터리를 분리해야 한다.**

2. **랜선을 컴퓨터와 분리, 뺀다.**

– 안전 모드로 부팅

1. 컴퓨터의 전원 버튼을 누른 후 안전 모드로 진입한다.

*** 윈도우7**

→ 시스템 부팅 시 F5키를 눌러 고급 모드에 들어간 후 다시 F8키를 눌러 안전 모드 부팅

*** 윈도우8, 윈도우xp**

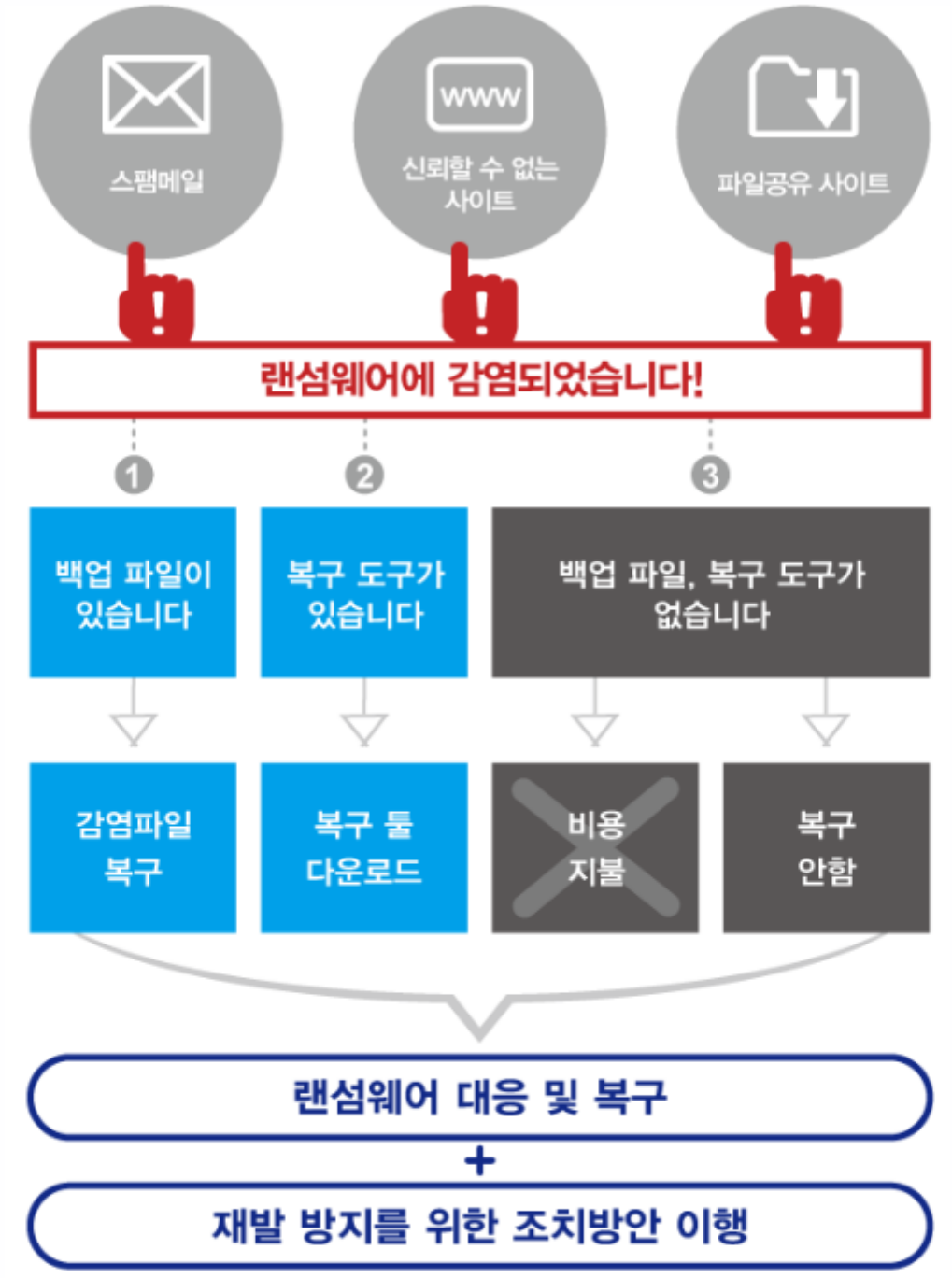
→ 시스템 부팅 전 F8 키를 연타한 뒤, 키보드의 화살표 버튼으로 '안전 모드(네트워킹 사용)'을 선택한 후, 'Enter' 키를 눌러 진입

*** 윈도우10**

→ 윈도우 검색창에서 msconfig – 부팅 탭에 안전 부팅 선택하는 방법

→ "PC설정 > 업데이트 및 복구 > 복구 > 고급 시작 옵션"에서 "다시 시작" 버튼을 클릭하여 나타나는 설정에서 "문제해결 > 고급옵션 > 시작설정 > 다시 시작"을 눌러 안전 모드로 들어가는 방법

- **복구 및 대응방법**



※ 랜섬웨어 복호화(암호화된 파일복구) 비용을 지불하기 전 고려사항

- 일부 개인이나 기업은 복호화 비용 지불 후에도 암호 해독키를 제공받지 못하는 경우 발생(비용을 지불하더라도 데이터의 복구를 100% 보장하지 않음)
- 일부 기업은 비용을 지불한 후 다시 공격의 대상이 될 수 있으며, 제시한 복호화 비용보다 더 많은 금액을 요구할 수 있음
- 복호화 비용의 지불은 추후 다른 사이버범죄에 사용되는 등, 더 많은 랜섬웨어 공격을 발생시키는 효과가 있으므로 지양해야 함

※ 복호화가 어려운 경우

- 하드디스크 원본을 보존하여 추후 복구 툴이 개발되거나 암호화키가 공개될 경우 복호화 진행
- 복호화가 필요 없는 경우, 하드디스크 초기화(포맷) 후 운영체제 및 소프트웨어 등의 최신 보안업데이트 후 사용하시기 바랍니다.

- **복구 프로그램 참고**

- **NMR(No More Ransom) 제공 랜섬웨어 복구 프로그램**

랜섬웨어 최근 동향 및 복구 프로그램 제공
- https://www.nomoreransom.org/co/index.html

- **이스트 시큐리티 제공 랜섬웨어 복구 프로그램**

랜섬웨어 최근 동향 및 복구 프로그램 제공
- http://www.estsecurity.com/ransomware#decryption

- **안랩 제공 랜섬웨어 복구 프로그램**

랜섬웨어 최근 동향 및 복구프로그램 제공
- http://www.ahnlab.com/kr/site/securityinfo/ransomware/index.do

- **랜섬웨어 침해대응 센터 복구 프로그램 안내**

랜섬웨어 복호화 프로그램 안내
- https://www.rancert.com/bbs/bbs.php?bbs_id=rest

- **카스퍼스키 제공 랜섬웨어 복구 프로그램**

랜섬웨어 사전 예방 방법 및 복구 안내 (한글설명)
- http://news.kaspersky.co.kr/news2015/10n/151029.htm

랜섬웨어 복구 프로그램 페이지
- http://support.kaspersky.com/viruses/utility
- https://noransom.kaspersky.com

- **트랜드마이크로 제공 랜섬웨어 복구 프로그램**

랜섬웨어 대응 센터
- http://trendstore.kr/ransomware.html

랜섬웨어 복구 프로그램 다운로드
- http://www.trendmicro.co.kr/kr/tools/crypto-ransomware-file-decryptor-tool/index.html

- **국내 랜섬웨어 대응 센터**

안랩 : http://www.ahnlab.com/kr/site/securityinfo/ransomware/index.do

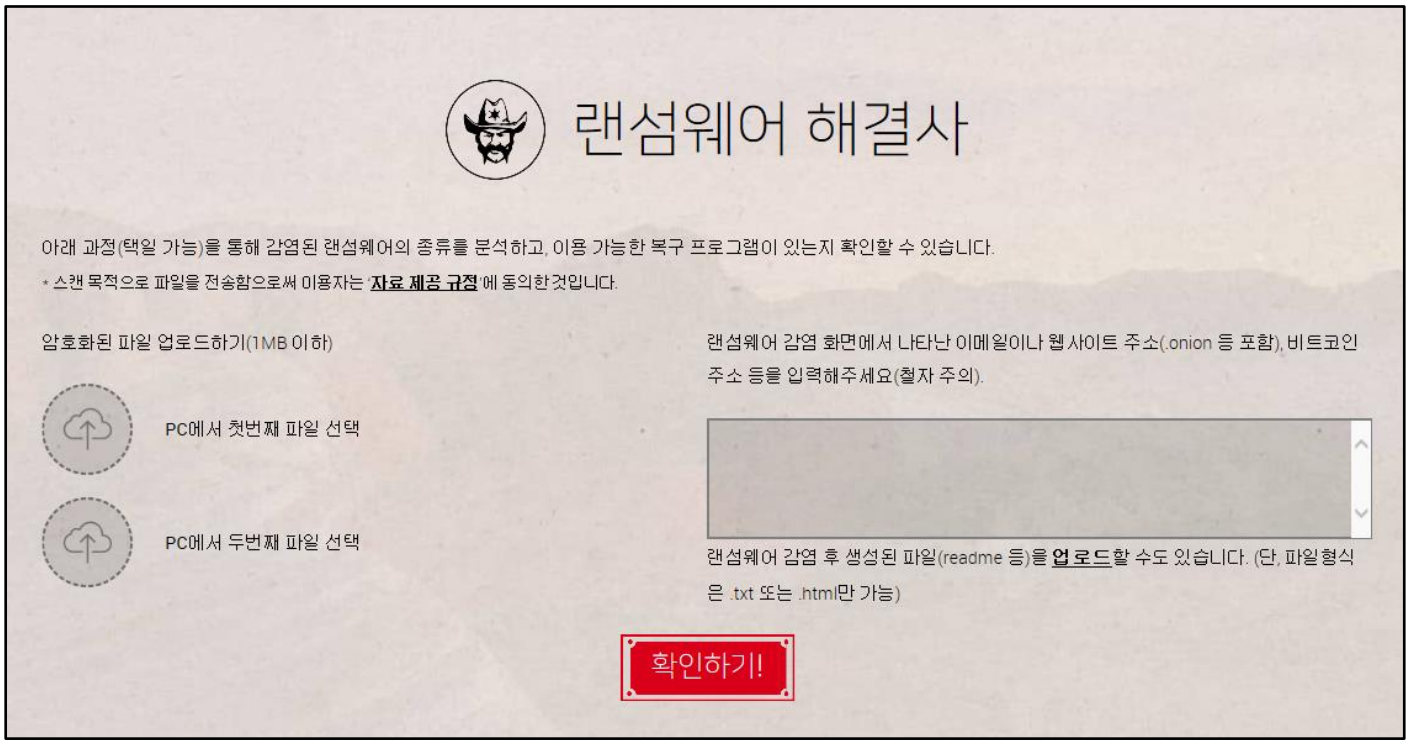
이스트 시큐리티 : http://www.estsecurity.com/ransomware#decryption

하우리 : http://www.hauri.co.kr/Ransomware/index.html

랜섬웨어 침해대응 센터 : https://www.rancert.com

- **랜섬웨어 해결사**

랜섬웨어 해결사 – 감염 시 종류 분석과 복구 프로그램이 있는지 확인 가능한 웹 사이트
- https://www.nomoreransom.org/crypto-sheriff.php?lang=ko



- **예방 - 백업과 보안 조치**

- 랜섬웨어 전문 백신 설치 (백신의 주기적 업데이트와 의심스러운 사이트 접속을 피하는 것만으로도 상당 부분 예방이 가능하니 참고)

- 백업

- **랜섬웨어 감염 Case**

- 광고 사이트에 접속만 하더라도 감염
- 광고 이벤트 링크를 통해서 감염
- 메일 계정으로 랜섬웨어가 심어진 스팸 메일이 무차별적으로 살포(특히 메일 중에는 사용자 자신이 자신에게 보낸 메일인 것처럼 위장하는 메일도 있으므로 자신에게 메일쓰기 기능을 쓴 적이 없다면 호기심에라도 열어보는 일이 없도록)

- **한국 사이트에서의 사례**

- 컬쳐랜드 사이트에서
- 뽐뿌에서 이벤트 링크를 통해서
- 오늘의 유머 광고에서
- 나무 라이브 사이트에서
- 동방 프로젝트 갤러리에서
- 국내 유명 호스팅 업체 '인터넷나야나'에서