세상에서 가장 안전한 파일보관 방법

랜섬웨어 방지를 위한

Stealth WORM Backup

UPSYST@M

1. 랜섬웨어란?

1-1. 랜섬웨어란?

랜섬웨어(Ransomware)는 '몸값'을 뜻하는 영어단어 'ransom'과 하드웨어 또는 소프트웨어 등을 의미하는 'ware'의 합성어로, 파일을 인질로 잡아 몸값을 요구하는 악의적인 소프트웨어 ' 를 의미합니다.

사용자의 PC 뿐만 아니라 공유된 폴더에 **문서, 사진, 동영상 등을 암호화하여** 사용하지 못하게 만들고 이를 인질로 삼아 **몸값(Ransom)**을 요구하는 악성 코드입니다.

그렇게 암호화된 파일은 복호화 키 없이 복구가 불가능해 매우 치명적입니다.

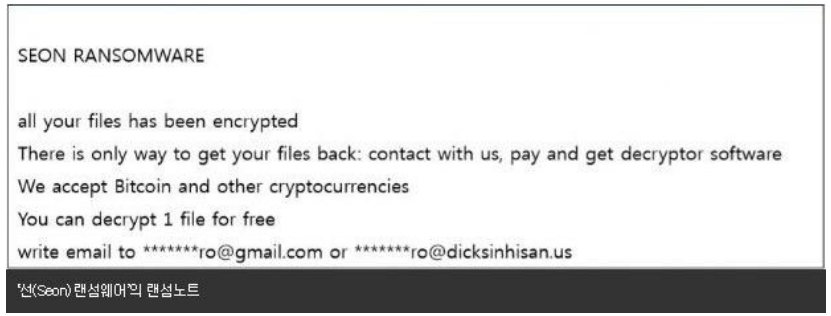
1-2. 랜섬웨어 감염경로와 증상

랜섬웨어는 주로 악의적으로 제작된 이메일의 첨부 파일을 실행하거나 이메일에 본문 또는 메신저, SNS등에 포함된 악성 단축URL을 클릭했을 때 감염될 수 있습니다.

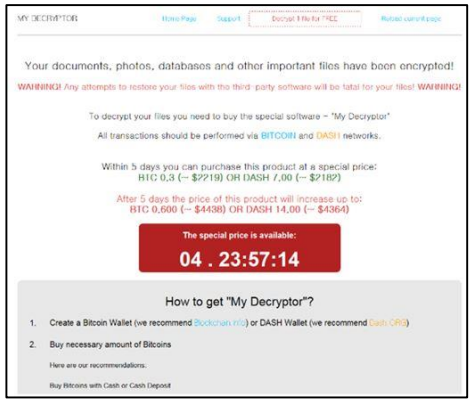
또한 최근 광고 서버에 악성 스크립트를 삽입하여 웹사이트에 접속하면 광고에 삽입된 악성스크립트가 자동으로 동작하게 하여 플래시 버전이 낮은 사용자 PC의 '선 랜섬웨어' 를 감염시킵니다.

랜섬웨어의 감염된 파일 및 폴더는 다양한 확장자(ECC,VVV,,ZZZ,AAA등)로 암호화 되어 변환 됩니다. 암호화를 하면서 동시에 피해자에게 감염사실 알리기 위해 윈도우 바탕화면을 변경하거나 해당폴더에 랜섬노트 파일을 생성하여 암호화된 파일을 복구 하기 위한 비용과 방법을 남깁니다.

2. 랜섬웨어 종류



'선(Seon) 랜섬웨어'의 랜섬노트



1. 선 랜섬웨어

사용자가 해당 웹사이트에 접속하면 광고에 삽입된 악성 스크립트가 자동으로 동작해 악성코드 유포 도구인 ' 그린플래시 선다운 익스플로잇 킷 ' 이 실행된다.
사용자 PC의 '어도비 플래시 플레이어 ' 의 버전을 확인해 구버전의 취약점이 확인되면 이를 악용해 랜섬웨어를 감염시킨다.

2. 매그니베르

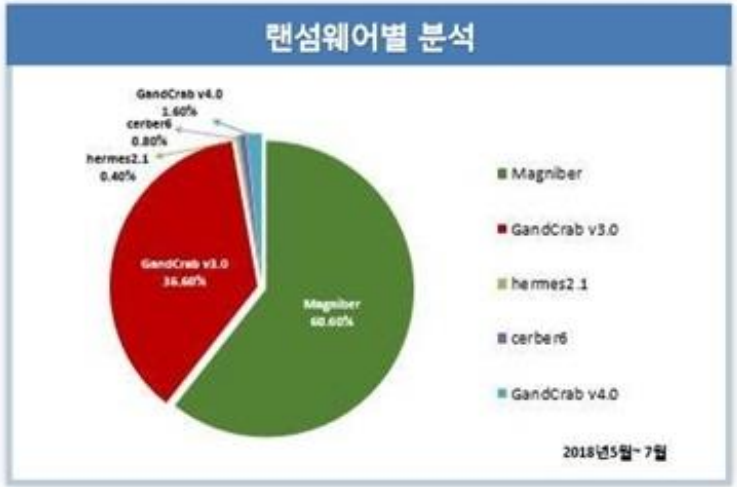
한국 OS만을 타킷으로 감염시키며 주 감염경로는 이메일 및 P2P 다운로드 뿐만 아니라 인터넷 홈페이지 접속만 해도 감염될 수 있다.
매그니베르는 감염되면 스케쥴을 변경시켜 오프라인에서도 작동되기 때문에 컴퓨터를 재부팅 해도 암호화가 진행 된다.

3. 워너크라이

2017년 5월 12일 부터 대규모 사이버 공격으로 널리 배포되었으며 전세계 99개국 12만대 이상을 감염시켰다.
일반적인 랜섬웨어와 달리 인터넷 네트워크에 접속만 해도 감염된다. 이 공격으로 마이크로소프트는 윈도우 XP등 오래된 미지원 운영체제에 대한 업데이트를 제공하기도 했다.

3. 랜섬웨어 피해 분석

2018년 1분기 랜섬웨어 피해 분석



출처 = rancert

4. 랜섬웨어 예방방법

1. 모든 소프트웨어 최신 버전 업데이트

운영체제(OS) 및 응용 프로그램(SW)은 상시 최신 보안 업데이트하여 인터넷 사용을 합니다. (예: 플래시 플레이어, 자바등)

2. 백신 소프트웨어 설치 및 최신버전으로 업데이트

랜섬웨어를 대비하기 위해선 백신 설치는 기본이며, 주기적인 백신 업데이트와 실시간 검사 기능은 필수로 활성화 시킨다. 백신은 정기적/주기적 검사를 한다.

3. 출처 불명확한 이메일 및 URL 링크 실행 금지!

메일 제목을 청구서 같은 비슷한 제목으로 이메일 이나 URL 링크 제공으로 사용자 PC를 감염시키기 때문에 상시 주의해야 한다.

4. 토렌트 및 p2p등 공유사이트 파일 다운로드 주의

랜섬웨어를 배포하기 가장 쉬운 방법으로 사이트 관리자가 검열을 하지 않기 때문에 이용자는 쉽게 다운로드하여 감염된다. 항상 실행파일은 주의를 해야 한다.

5. 중요 자료 오프라인 백업

중요문서는 별도 외장매체에 주기적으로 백업하여 분리 관리한다. 공유폴더 및 네트워크 드라이브 그리고 외장 하드등 연결되어 있는 모든 감염되기 때문이다.

5. 랜섬웨어 복구 및 재발 방지

1. 랜섬웨어 복호화

각종 백신 개발 업체에서 제공하는 복호화 프로그램을 이용해서 복구시도를 한다. 단 복구프로그램은 특정 랜섬웨어만 적용된다.

2. 1번 방법 외에 복구 불가능!

랜섬노트에 요구사항으로 비용을 지불 할 경우 암호 해독키를 제공받지 못할 경우가 대부분이며 비용 환불은 불가능하다.
또한 복구 업체를 통한 복구는 신뢰할 수 없어 비용만 증가 할 뿐이다.

재발 방지

협업 : 개인 폴더 및 공유폴더 상시 사용

백업 : 개인 폴더 및 공유폴더 상시 자동 백업

복구 : 랜섬웨어 발생시 바로 복구

Stealth WORM Backups

6. Stealth WORM Backup 기능

사용자1

사용자2

사용자3

네트워크 업무공유

업무를 공유 하기 위해서 공유폴더를 연결하여 업무

협업을 하기 위해서는 파일의 쓰기/삭제/수정이 가능해야함.

랜섬웨어 감염시 파일 손상됨.

Stealth Storage

Stealth Backup

"Stealth Backup " 은 스케줄링 되어 있는 시간에 Stealth WORM 영역에 파일을 자동 백업 한다.

일반유저의 파일 접근이 불가능하며 관리자만 파일의 접근이 가능함.

Stealth Worm 영역

관리자만 Stealth Worm 영역에 접근 가능

사용자는 보이지 않는 Stealth Worm 영역 접근 불가

7. Stealth WORM Backup 복구

공유폴더 사용

랜섬웨어 감염된
사용자가 관리자에게 공지

랜섬웨어 복구

관리자는 스냅샷으로 1차 복구 시도
복구 실패 시
2차 Stealth WORM 영역에 접근하여 복구함
-> 읽기전용 영역으로 데이터 위변조 불가함

소기업/중소기업

합사/단위 사업장 용도

HW에 따라 저장 용량 선택

중견기업 이상

데이터가 많은 경우

HW에 따라 저장 용량 선택

Stealth WORM Backup Server

■ 랜섬웨어 감염 시 즉시 복구

랜섬웨어에 감염된 폴더 및 파일을 파악한 후에 손상되기 전으로 시점 복구 (Snapshot 무제한)

■ Stealth WORM Backup 영역 복구

랜섬웨어 및 HDD 장애로 인하여 바로 복구가 안 될 경우 Stealth Worm 영역으로 바로 복구

Thank You

THINKS for READING

서울특별시 구로구 디지털로 33길 28
우림이비지센터 1차 601-8호 유피시스템

구매문의 : 02-785-6055~6
http://www.upips.com

UPSYST@M