

2017.10

랜섬웨어는 무엇이고

기업이나 가정에서 어떻게 방어를 해야하나

코드엔진 Talk #2

www.CodeEngn.com

Code  Engn

목 차

랜섬웨어는 무엇이고 기업이나 가정에서 어떻게 방어를 해야하나

코드엔진 Talk	3
랜섬웨어의 문제점은?	4
랜섬웨어를 포함한 악성코드의 주요 감염 경로는?	10
랜섬웨어 감염사례	19
랜섬웨어 복구사례	25
랜섬웨어 감염을 막기위한 방법은?	30

코드엔진 Talk

코드엔진 Talk는 정보보안에 관련된 특정 주제에 대해 코드엔진 운영진들이 모여 채팅형식으로 대화한 내용들을 문제점, 대응책, 실무사례, 사고사례 등을 이해하기 쉽게 집필한 무료 온라인 잡지입니다.

이 잡지는 IT, 정보보안을 잘 모르시는 일반인 분들과 보안을 입문하시는 분들께 유용하도록 구성하였습니다.

주제 선정은 페이스북 또는 이메일을 통해 의견을 받거나 최신 이슈를 선정하여 비정기적으로 Talk를 진행 할 예정입니다.

- * 본 지에 언급된 내용은 운영진 개인의 의견으로 소속된 단체나 집단을 대표하지 않고, 집필한 시점에서의 의견으로 사실과 다를 수 있습니다.
- * 코드엔진 Talk는 배포 시 출처를 반드시 명시하여야 합니다.

문의사항

<http://codeengn.com/contact>

랜섬웨어의 문제점은?

랜섬웨어

위키백과, 우리 모두의 백과사전.

랜섬웨어(Ransomware)는 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다. 이때 암호화되는 랜섬웨어가 있는 반면, 어떤 것은 시스템을 단순히 잠그고 컴퓨터 사용자가 지불하게 만들기 위해 안내문구를 띄운다. 최근 전 세계적인 랜섬웨어를 통한 대량해킹은 인터넷 세계의 사이버 아마겟돈으로 불려진다.

처음 러시아에서 유행하면서 랜섬웨어를 이용한 사기는 국제적으로 증가하였는데^{[1][2]}, 보안 소프트웨어 개발사 맥아피는 2013년 1분기 동안 수집한 25만 개 이상의 고유한 랜섬웨어 표본 자료를 2013년 6월 공개했고, 이는 2012년 1분기보다 두 배 많은 수치였다.^[3] 암호화 기반 랜섬웨어를 포함한 광범위한 공격은 각각 약 300만 달러와 1800만 달러의 부당이익을 취한 크립토락커^[4]와 크립토월^[5]과 같은 트로이목마를 통해 증가하기 시작했다.

악성코드로서 사용자의 동의 없이 컴퓨터에 설치되어 내부 파일을 인질로 잡아 금전적인 요구를 한다. 일반적으로 윈도우 운영체제가 설치된 PC에서 가장 많이 발생하지만 모바일 환경에서도 발생하며, 맥 OS도 감염될 수 있다.

2017년 5월 12일에는 사상최대 규모의 랜섬웨어 공격이 발생하기도 했다. 2016년 해커들에게 탈취당한 미국국가안보국(NSA)의 해킹 툴을 활용한 "워너크라이(WannaCry)라는 랜섬웨어는 유포 하룻만에 전세계 100여개국 10여만대 이상의 컴퓨터를 감염시키며 전세계를 사이버 테러의 공포로 몰아 넣었다.



랜섬웨어에 감염된 모습이다.

출처:

<https://ko.wikipedia.org/wiki/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4>



볼트101

랜섬웨어는 무엇이고 랜섬웨어의 문제점은 무엇인지
알아봅시다.

문제점은 아무래도 내 중요한 파일들을 암호화하고 돈을
요구하는 것이 아닐까?



컴수진

랜섬웨어의 문제점은..

진짜 쉽게 생각하면 일반인 입장에선 돈을 떠나 당장 컴퓨터를

못쓴다. 파일을 못 본다. 접근되지 않는다

돈내라고 해서 복구하고 싶은데 복구 방법이 비트코인으로

지불하는거 자체가 생소할 수도 있고 제작자가 어떤 사람인지도

모르겠고

복구가 된다는 보장도 없단 말도 있고 한마디로 막막해지는

상황이라서 문제라고 생각됩니다



Henry

맞아요. 파일이 암호화됐을 때 복호화가 어렵다는 점도 있고,

사실 돈을 내라고 했을 때도 제작자가 누군지 모르니 정말

풀어줄 지 말지 알 수 없어요.

일반인 입장에서는 파일 복구가 절실한데, 그만큼 손해를 볼 수

밖에 없는 상황이 만들어지는 것도 문제 같아요.



컴수진

네 그래서 돈 내기 찝찝해서 지불하기 싫은 사람도 많고

복구해준다고 해도 우리같이 한글 기반일 때는 /파일명이

제대로 복원안되는 등.. 기껏 돈내고 샀더니 버그투성이라는

말도 있구요



Jenny

그리고 요새는 많이 알고있다고 해도 비트코인이 뭔지도 모르는 분들도 많더라구요. 안다고 해도 비트코인을 어떻게 얻고 얻은 후에는 어떻게 해야하는지 몰라서 답답한 면도 있는거같아요

음...

(양심이 있는 랜섬웨어 제작자인 경우) 개인이던 기업이던 당장 피씨에서 필요한 업무자료와 개인정보때문에 복구가 필요해서 비트코인을 해커한테 빨리주고 싶어도 비트코인 절차가 어렵고

(양심이 없는 랜섬웨어 제작자인 경우) 돈을 줘도 복원이 안될거라는 걱정이 들죠

그리고 사회적으로 비트코인을 무조건 주지말라고 하는데 그럼 어떻게 하라는건지 좀 답답할때도 있어요

메뉴얼도 랜섬웨어 방지 메뉴얼만 존재하지 감염 되었을때는 단지 비트코인을 주지말라 이것뿐 이었던거 같은데..



Thomas

비트코인과 컴퓨터를 잘 모르는 일반인을 위해 랜섬웨어 복구대행 시장이 형성되었고, 업체도 많이 생겨났어요. 업체들이 중간에서 일정 수수료를 받고 비트코인을 지불 해주는 거죠. 데이터 복구보다는 대행이 차지하는 비율이 높다고 하네요. 일부 업체에서는 랜섬웨어가 요구하는 몸값을 부풀려서 부당 이득을 취득한 사례도 있구요.



Henry

그리고 문제점 중 하나인 해커들이 비트코인 지갑을 애용하는 것도 역시 역추적하기 힘든 점을 이용한 것인데, 사람들이 랜섬웨어 피해와 예방법을 아는 것도 중요하지만 최근 랜섬웨어에 비해 보안 분야에서 비트코인이 어떻게 쓰이는지 그만큼 관심을 가지고 있지 않는 것 같아요.



Thomas

정부나 일부 전문가들이 랜섬웨어 제작자에게 비트코인을 주지 말라고 하는데... 랜섬웨어 시장을 없애는게 목적인것 같아요. 사실상 불가능한 일이죠. 정부에서 비트코인 지불을 독려하기엔 그림이 이상하니 저게 최선이 아닐까요.



볼트101

비트코인은 추적이 어려운가요? 대부분 추적이 되는걸로 알고있는데..



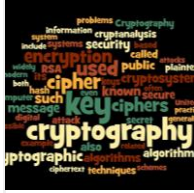
csucom

비트코인은 계속 돌리면 돈세탁이 가능한걸로 알고 있습니다.
그런걸 전문적으로 해주는 업체도 있다고 들었습니다.



Henry

비트코인 지갑 주소의 소유주가 해커인지 알지만, 그 해커가
누군지는 모르기 때문에 해당 해커를 잡는 것은 불가능하죠.
이건 코인마다 다를 수 있겠지만 개인키로 공유키를 임의로
생성하고, 그 공유키에서 지갑 주소를 생성한다고 할 때 지갑
주소로 개인키를 추적하는 건 불가능으로 알고 있습니다.
물론, 모든 것을 다 떠나서 잡힐수 있는 정보를 가진 장소가
결국은 거래소 이다보니 거래소가 정확한 정보를 가지고
있느냐가 관건인 것 같습니다.



범죄자가 수익금을 최종적으로 현금화 하는 순간 잡을 수 있지 않을까요?

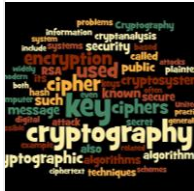
랜선웨어



거래소를 통할 경우 추적이 가능하지만, P2P 거래를 하게 되면 추적이 어려운걸로 알고 있어요! 생각보다 P2P 거래량도 많구요

posquit0

랜섬웨어를 포함한 악성코드의 주요 감염경로는?



랜선웨어

기존 이메일 첨부파일 형태로 사용자가 실행하는 방식과 클리앙 커뮤니티 사례에서 보았듯이 웹 취약점을 이용한 DBD(Drive-By-Download)형태, 최근에 SMB 취약점을 이용한 네트워크 전파방식이 있었습니다.

싱가포르 국립대학 '해적판 소프트웨어의 사이버 보안 위험성 평가' 연구에 따르면, 불법 소프트웨어 또는 무료영화 다운로드 사이트와 같은 불법 콘텐츠 열람을 위해 접속한 사이트에서 감염되는 사례가 많다고 하네요.



csucom

요새는 말씀하신대로 웹에서 구글링하다가 DBD로 감염되는 사례가 굉장히 많은 거 같아요.

그 외는 아시다시피 S/W 크랙버전이나 시리얼 키젠 등에 심어져 있는 경우도 많고.. pdf나 hwp과 같은 문서파일에 심어져 있는 경우도 많은 듯 하구요.



posquit0

이메일에 심어진 스크립트, 오피스 취약점을 노린 문서
첨부파일, 불법다운로드 사이트를 통해 유명 영상 플레이어
노린 야동, 최신 영화
또 뭐가 있을까요?
주변 피해자 분들 보면 이메일 통한 공격 피해사례가 가장
크더라구요



컴수진

단독 파일로 유포되는 것 뿐만 아니라
스크립트나 문서 파일 등.. 스팸 첨부 파일 역시 다양해지고
있어요
웹사이트 취약점으로 뿌려지는 것도 많구요
Malware traffic 이라는 사이트를 보면 취약점으로 유포되는
랜섬웨어와 패킷 정보가 데일리로 매일 올라옵니다!



Thomas

지금까지 랜섬웨어 유포 양상을 살펴보면 Targeting과 Non-
Targeting으로 구분할 수 있어요.
Targeting은 비너스락커 처럼 한글로 작성된 메일 내용과
파일명으로 실행을 유도하거나, 아니면 나야나 웹호스팅

사태처럼 내부서버 장악 후 뿌리는 형태가 있어요. 그 외에 한글 문서 취약점을 이용해서 유포할 수 있는데, 아직 랜섬웨어를 유포한건 못 봤어요.

Non-Targeting의 경우 스팸메일(오피스 매크로, 스크립트 등)과 DBD가 가장 많아요. 특이한 케이스로 워너크라이처럼 SMB 취약점을 이용하여 전 세계를 강타한 경우도 있죠.



볼트101

나야나 같은 경우 요약을 하면 APT 형태의 침투 공격이 먼저 이루어지고 랜섬웨어 감염을 시킨 형태인데 중요한건 운영서버와 백업서버 간에 망분리를 잘해놔야 하는데 미흡해서 백업서버도 감염이 된 사례이고..

한글문서는 주로 주요 정보 다루는 담당자들을 대상으로 APT 공격할때 활용되고 있으니 지금은 아니더라도 랜섬웨어를 포함시키는 경우도 있을 수는 있겠네



Thomas

네, 랜섬웨어 제작자들이 노력만 하면 충분히 가능하죠 ㅎㅎ
 주로 한글문서 취약점은 특정 조직이 많이 사용하고 있어요.
 만약 그 조직이 백도어가 아닌 랜섬웨어를 뿌릴 수도 있겠죠.



볼트101

각 감염경로 마다 감염되기까지 과정들이 어떻게 있나요?
 이메일 같은 경우 첨부파일에 실행파일 이지만 문서, 이미지,
 압축파일 형태의 아이콘이나 확장자를 속인 후에 사용자는
 파일을 다운로드 받고 문서나 이미지 파일인줄 알고 실행을
 해서 감염되는게 일반적인것 같음



Bono

웹을 이용한 감염 형태에는 DBD가 가장 대표적 이었던 것
 같네요
 사람들이 자주 사용하는 웹사이트의 내에 광고나 고정 페이지
 하나에 스크립트를 삽입하는 방식이 가장 많이 있었구요....
 특히 공격을 수행하면 광고 서비스 제공 서버에서 원론적인
 문제가 해결될때 까지 지속적으로 스크립트를 삽입하였는데,
 이때 Redirect 되는 사이트 주소도 지속적으로 변경하고,
 타겟 광고 페이지도 변경하는 경우가 많아서 동시 다발적으로
 피해사례가 증가했습니다..



볼트101

참고로 메신저, 동영상 재생기 등의 프로그램에서 보여지는
팝업광고를 통해서도 감염될 수 있음..

사용자 입장에서 악성코드가 삽입된 뉴스 광고를 보면
스크립트는 어떻게 실행이 되고 감염이 되는건가?



Bono

우선 공격자에 의해 감염된 페이지에 사용자가 접근하게 되면
다음과 같은 과정으로 보통 진행 되었습니다

1. 공격자가 대상 사이트 페이지나 배너에 frame 태그 등을
이용하여 악성 스크립트로 연결하기 위한 코드 삽입
2. 감염 페이지에 사용자 접근 후 공격자가 의도한 페이지에
접속
3. 사용자의 소프트웨어 취약점 등을 악용하기 위해 취약점
코드 실행
4. 사용자 시스템 내 파일에 인젝션등을 시도 후 파일 암호화
수행 및 파일 자가삭제 수행
5. 감염... 당황... 지불...



Bono

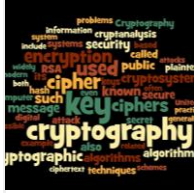
특히 2번 항목에서 나오는 악성 스크립트 주소를 지속적으로 변경한다는 이야기였습니다.

공격자는 랜섬웨어 유포 전에 redirect 되기위한 주소도 많이 준비 해 놓고 공격을 수행합니다

이때 대부분의 주소를 실제로 확인 해 보면 소규모의 쇼핑몰이나 학원 등 보안이 취약한 사이트를 먼저 공격하여 유포 준비를 수행합니다

또하나 처음 접하시는 모르는 분들을 위해 악독한걸 말해보면..

1. 공격자가 지정한 인터넷 접속 통계 사이트 개인 고유주소 삽입
 2. 지속적인 모니터링으로 공격 대상 페이지에 사용자가 가장 많이 접근하는 시간을 확인
 3. 방문자 통계가 많아지는 시간에 악성 스크립트 삽입!
(더 많은 수익을 내기 위해 시도하는 방법)
 4. 감염... 당황.. 지불..
- 과 같은 방법도 있습니다...



랜선웨어

오.. 공격의 극대화를 위해 접속자 수를 카운팅 한다는건
신선하네요.



볼트101

사용자 PC에 설치된 취약한 소프트웨어는 어떻게 있나?



Bono

주 타겟이 되는 범위는 다양하지만 사용자들의 시스템에
공통적으로 사용되는 애플리케이션을 주로 대상으로 합니다
모두가 알고있는 인터넷 익스플로러나 플래시 등등이

해당되겠죠

공격자의 입장에서 생각해보면 많은 사용자를 감염시키기 위해 공통적인 요소를 사용한다고 보시면됩니다.

이를 방어하기 위해서는.. 업데이트가 필수적이고... 업데이트를 하려면 또.. 첫번째에 했던 “코드엔진 Talk #1, 소프트웨어 업데이트 과연 신뢰해야 하나” 주제로 돌아가고...

머리가 아파오고.. 그렇네요..



Thomas

추가로 취약한 소프트웨어 중에서 자바도 있고 해외에서 많이 사용하는 실버라이트도 있어요.



Bono

넵 자바나 실버라이트 등도 사용자 PC에서 공통적으로 많이 사용되는 놀들이기에 주 공격 대상에 포함됩니다 □



Thomas

네 ㅎㅎ 주로 어떤 익스플로잇 킷을 사용하느냐에 따라 차이가 있겠네요. DBD로 유포할 때 유포 사이트에 카운트 서버를 걸어 놓는 경우가 있는데, 주로 국내 파밍 유포조직이 사용해요.
혹시 해외에서도 DBD로 악성코드 유포할 때 카운팅을 사용하는지 궁금하네요 ㅎㅎ



Thomas

SMB를 이용한 전파방식에는 보통 2가지 방식이 있는데요

1. SMB Brute-force 공격

- 1) 내부 PC 감염
- 2) 공유폴더 계정(admin, test 등)에 취약한 패스워드(1234, password 등)를 Brute-force해서 권한 획득
- 3) 해당 PC에 악성코드 복사 및 실행

2. SMB 취약점

- 1) 내부 PC 감염 or 외부 인터넷이 연결된 PC 감염
- 2) 특정 IP에 취약한 PC에 취약점을 유발하는 SMB 패킷 전송
- 3) 취약할 경우 SMB 취약점을 이용해 해당 PC에 악성코드 생성 및 실행
- 4) 워너크라이 같은 웜의 경우 특정 로컬 IP 대역과 외부 IP 대역에 SMB 취약점 패킷 전송

랜섬웨어 감염사례



Thomas

국내

2015-04 : 클리앙 커뮤니티 Crypt0L0cker 유포

- 클리앙 랜섬웨어 악성코드 유포사건의 전말

[http://www.boannews.com/media/view.asp?idx=46010&kind=1
&search=title&find=%C5%AC%B8%AE%BE%D3](http://www.boannews.com/media/view.asp?idx=46010&kind=1&search=title&find=%C5%AC%B8%AE%BE%D3)

2016-06 : 뽀뿌 커뮤니티 CryptXXX 유포

- [긴급] 개인정보 유출로 몸살 앓은 뽀뿌, 랜섬웨어 유포로 '홍역'

[http://www.boannews.com/media/view.asp?idx=50853&page=1
&kind=1&search=title&find=%BB%CB%BB%D1](http://www.boannews.com/media/view.asp?idx=50853&page=1&kind=1&search=title&find=%BB%CB%BB%D1)

2016-06 : 부산시, 관내 기초자치단체 Cerber 감염

- 관공서·병원으로 피해 확산되는 랜섬웨어 비상...변종도 창궐

[http://www.boannews.com/media/view.asp?idx=50901&page=1
&kind=1&search=title&find=%BB%CB%BB%D1](http://www.boannews.com/media/view.asp?idx=50901&page=1&kind=1&search=title&find=%BB%CB%BB%D1)

2017-02 : 춘천시 버스정보 안내기 Philadelphia 감염

- 춘천시 버스정보 안내기 랜섬웨어 감염, 뒤늦게 드러나

[http://www.boannews.com/media/view.asp?idx=53753&page=2
&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE
+%B0%A8%BF%B0](http://www.boannews.com/media/view.asp?idx=53753&page=2&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE+%B0%A8%BF%B0)

2017-05 : CGV 극장 내부 광고판 WannaCry 감염

- CGV도 랜섬웨어 감염... “영화 시작 전 광고 못 본다?”

[http://www.visualdive.com/2017/05/cgv%EB%8F%84-
%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-
%EA%B0%90%EC%97%BC-%EC%98%81%ED%99%94-
%EC%8B%9C%EC%9E%91-%EC%A0%84-
%EA%B4%91%EA%B3%A0-%EB%AA%BB-
%EB%B3%B8%EB%8B%A4/](http://www.visualdive.com/2017/05/cgv%EB%8F%84-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-%EA%B0%90%EC%97%BC-%EC%98%81%ED%99%94-%EC%8B%9C%EC%9E%91-%EC%A0%84-%EA%B4%91%EA%B3%A0-%EB%AA%BB-%EB%B3%B8%EB%8B%A4/)

2017-06 : 나야나 인터넷 호스팅업체 Erebus 감염

- [긴급] 웹호스팅 업체 랜섬웨어 감염! 중소 웹사이트로 피해 확산되나

[http://www.boannews.com/media/view.asp?idx=55215&page=1
&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE
+%B0%A8%BF%B0](http://www.boannews.com/media/view.asp?idx=55215&page=1&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE+%B0%A8%BF%B0)

2017-06 : 미국 머크 제약사 국내지사 한국MSD New

Petya/NotPetya/ExPetr 감염

- 한국MSD 랜섬웨어 감염에 다국적제약사들 '노심초사'

<http://news1.kr/articles/?3033675>

2017-08 : LG전자 서비스센터 WannaCry 감염

- “랜섬웨어 감염된 게 맞다” LG전자, 결국 사실 인정했지만...

[http://www.boannews.com/media/view.asp?idx=56380&page=1
&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE
+%B0%A8%BF%B0](http://www.boannews.com/media/view.asp?idx=56380&page=1&kind=1&search=title&find=%B7%A3%BC%B6%BF%FE%BE%EE+%B0%A8%BF%B0)

2017-09 : 불필요한 프로그램(PUP) Qbridge을 통해 AllCry

유포

- [긴급] 올크라이(AllCry) 신종 랜섬웨어 국내 유포중...주의

[http://www.dailysecu.com/?mod=news&act=articleView&idxno
=24519](http://www.dailysecu.com/?mod=news&act=articleView&idxno=24519)

해외

2016-02 : 미국 할리우드장로병원

- 차병원 투자 美 할리우드장로병원, 랜섬웨어로 1주일째 마비

<http://www.boannews.com/media/view.asp?idx=49620>

**2016-03 : 미국 감리병원, 치노밸리의료센터, 데저트밸리병원
랜섬웨어 감염**

- 한 주 만에 병원 세 곳이 랜섬웨어에! 의료계 위기

<http://www.boannews.com/media/view.asp?idx=50052>

2016-11 : 미국 인디애나 카운티정부 랜섬웨어 감염

- 美 인디애나 카운티정부, 랜섬웨어 감염 후 몸 값 지불해

http://www.dailysecu.com/?mod=news&act=articleView&idxno=17034&sc_code=&page=4&total=100

2016-11 : 샌프란시스코 경전철 HDDCryptor 감염

- 샌프란시스코 경전철 '랜섬웨어' 공격으로 결제시스템 마비

<http://www.yonhapnews.co.kr/bulletin/2016/11/29/0200000000AKR20161129029400091.HTML>

2017-06 : 우크라이나 유럽 미국 등 New

Petya/NotPetya/ExPetr 감염

- 우크라이나 강타한 '랜섬웨어' 공격, 유럽·미국 등 확산

<https://www.voakorea.com/a/3919389.html>

2017-07 : 일본 혼다 공장 WannaCry 감염

- 일본 혼다 공장 워너크라이에 당했다... 대 랜섬웨어 시대의 시작?

<http://osen.mt.co.kr/article/G1110673524>

2017-07 : 페덱스 New Petya/NotPetya/ExPetr 감염

페덱스, 페트야 랜섬웨어에 감염돼...복구에 어려움

http://www.dailysecu.com/?mod=news&act=articleView&idxno=22010&sc_code=&page=&total=

2017-08 : 스코틀랜드 남부 래닉서 Bitpaymer 감염

- 새로운 랜섬웨어 등장, 스코틀랜드 병원 시스템에 침투

<http://www.dailysecu.com/?mod=news&act=articleView&idxno=23345>

2017-10 : 러시아, 우크라이나 등 유럽 일부 지역 Badrabbitt

감염

- 유럽 일부지역 또 '멀웨어' 습격... 러·우크라 등 피해보고
(종합)

<http://www.yonhapnews.co.kr/bulletin/2017/10/25/0200000000>

[AKR20171025000951080.HTML?input=1195m](http://www.yonhapnews.co.kr/bulletin/2017/10/25/0200000000)

랜섬웨어 복구사례

작동 원리 [편집]

흐름 [편집]

1. 공격 대상 파일검색
2. 파일 암호화
 1. 고정키 암호화
 2. 다이나믹키 암호화
 1. 암호화키 생성
 2. 암호화키 서버 전달
3. 파일 이동
4. 감염 안내 및 복구 방법 메시지 출력

원리 [편집]

암호화 알고리즘의 이용이다. 파일 데이터에 암호화 알고리즘을 이용하여 암호화하여 사용할 수 없도록 하는 것이다. 암호화 방식에는 크게 단방향, 양방향 방식이 있다. 단방향 암호화란 한 번 암호화하면 다시 복호화할 수 없도록 하는 것이다. 양방향 암호화는 암호화한 후 복호화가 가능한 것이다.

최근에는 단순히 홈페이지를 방문만 해도 랜섬웨어에 감염되기도 한다. 일명 '드라이브 바이 다운로드(Drive by Download)' 기법을 이용해서다. 드라이브 바이 다운로드란 공격자가 해당 웹사이트에서 보안이 취약한 점을 노려 악성코드를 숨기고, 이 악성코드를 사용자가 자신도 모르게 내려받아 실행해 감염되는 방식이다.

출처 :

<https://ko.wikipedia.org/wiki/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4>



Thomas

랜섬웨어 복구 사례는 어떻게 있을까요?



컴수진

복구사례는 꽤 많았던것 같아요.

랜섬웨어가 파일을 암호화 하였을 때 사용하였던 암호화 키가

파일 내에 있을 경우에는 랜섬웨어 제작자에게 지불하지

않고서도 복구가 가능하기도 하였고

드물게 암호화 방식의 오류가 있을 때는 RSA 와 같은

비대칭키를 이용한 암호화 방식 역시 복구가 되기도 하였죠

<https://support.kaspersky.com/viruses/utility>

해외의 KAV 를 포함해 국내외 벤더에서도 복구툴을 배포하기도 하였어요.



Thomas

그렇군요 ㅎㅎ 작년 12월부터 국내에 유포됐던 비너스락커의

경우 C2가 막혔을때 하드코딩된 AES키를 사용해서 암호화하기

때문에 이 경우에 복구가 가능했어요. 안랩에서 제작한 툴을


써봤는데 비너스락커를 아주 깔끔하게 복구 하더라구요.


랜섬웨어 복구는 노모어랜섬도 유명해요. 여러 벤더사와


기관에서 참여하고 있어요.

<https://www.nomoreransom.org>

	<p>노모어랜섬에서 일부 랜섬웨어의 경우 C2 서버를 털어서 얻은 KEY로 복구해준다고 들었어요. 하지만 걱정하고 만든 랜섬웨어는 공격자 밖에 복구할 수 없죠.</p> <p>올해 국내 인터넷 호스팅 업체 나야나 사건이 대표적인 지불 복구 사례라고 생각해요.</p>
--	---

 <p>Thomas</p>	<p>몸값 금액을 가지고 랜섬웨어 제작자와 협상도 하고, 결국 13억을 지불하고 복구하긴 했죠 π</p> <p>물론 완벽하게 복구가 안되어서... 문제가 있었지만요.</p>
---	--

 <p>컴수진</p>	<p>맞아요 진짜 너무 안타까운 사례예요... 해커와 거래를 하게 되고 제대로 복구도 안되고...</p>
--	--

 <p>Thomas</p>	<p>나야나 사건 때문에 한국이 랜섬웨어 몸값을 잘 준다고 해외에 소문났대요ㅋㅋ 그래서 많이들 공격한다는 소리가 있습니다..</p>
---	---



컴수진

근데 국내에서도 랜섬웨어 제작자들이 많을까요?

문득 궁금해지네요



Thomas

아예 없진 않을거 같은데...

요즘 비트코인으로 RAT나 서비스형 랜섬웨어(RaaS)를 많이 팔고 있어서 저런거 사서 쓰지 않을까요.

서비스형 랜섬웨어(RaaS)는 몸값 일부를 수수료로 떼간다고 하는거 같아요





Henry

국내 랜섬웨어 제작자들이 만든 랜섬웨어 자체는 실제 유포를 통해 아직까지 큰 피해는 없었던 것 같아요. 하지만, 국내에서 제작되었다는 확실한 증거가 조금씩 확인되고 있어요.

작년에 한국인이 만들었다는 카카오톡 위장 랜섬웨어가 등장했고, 올해는 한국어를 모국어로 사용하고 있는 것으로 추정되는 사람이 Jigsaw 랜섬웨어 변종을 제작했다고 하죠.

	<p>실제로 감염됐을 때, 한국어로 작성된 메시지가 나오는 경우가 점점 많아져서 한국도 더 이상 타겟에서 빠질 수 없게 됐어요.</p> <p>올해 나야나 사건 때문에 지불한 금액이 해외의 저명한 뉴스인 BBC, Gizmodo 등에 이미 보도된 바가 있어서 앞으로 추가적인 공격들이 불가피할 것 같아요...</p>
--	--

 <p>Thomas</p>	<p>아무래도 랜섬웨어가 수익이 괜찮고, 비트코인도 계속 오르고 있어서... 국내 제작자들도 점점 늘어날거 같네요 ππ</p>
---	--

 <p>Henry</p>	<p>맞아요. 이미 오픈소스로 공개된 EDA2, Hidden-Tear 랜섬웨어를 기반으로 한 변종 랜섬웨어들이 계속 생겨나는 추세인데,</p> <p>이렇게 발전하는 랜섬웨어의 끝이 어디가 될지.. 무섭네요.</p>
--	---

랜섬웨어 감염을 막기위한 방법은?

근클립토락커의 예방 [편집]

- 선 뽑기 / 와이파이 끄기
- 방화벽 설정 변경
- 모든 소프트웨어는 최신 상태를 유지
- 백신소프트웨어 설치 및 최신버전 유지
- 출처가 불분명한 첨부파일이나, URL은 열람하지 않는다.
- 불법 파일공유사이트 이용 시 유의
- 주기적인 백업
- SMB 포트 차단
- SMB 1.0/CIFS 파일 공유 지원 해제

출처 :

<https://ko.wikipedia.org/wiki/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4>



볼트101

일반 회사나 가정에서 NAS를 사용하고 있다면 NAS에서 제공하는 기능들을 살펴보는것도 좋은데 시놀로지 NAS의 경우 파일 스냅샷 기능이 있어서 파일이 변경될때마다 스냅샷을 기록할 수 있어서 언제든지 특정 버전으로 복원이 가능한 장점이 있습니다



Thomas

일반적으로 아래 5가지 정도면 막을 수 있다고 생각해요.

1. 윈도우, 자바, 플래쉬, 인터넷 익스플로러를 최신 버전 유지
2. 출처가 불분명 하고 의심스러운 이메일 열람 자제
3. 백신이나 랜섬웨어 탐지 솔루션 사용
4. 중요 파일의 주기적인 백업 (개인 백업, 백업 솔루션 등)
5. 환경이 된다면 가상환경에서 이메일 열람, 웹서핑

예외적인 사항도 있어요.

1. 제로데이 취약점 이용한 랜섬웨어 유포
2. 백신, 랜섬웨어 탐지 솔루션 우회 기능
3. 원격 접속 후 랜섬웨어 감염 (RDP, 팀뷰어 등)

가장 안전한건 주기적인 백업!!!





Henry

확장 프로그램을 설치할 수 있는 브라우저에서 Adblock, Adguard 등의 광고차단 프로그램을 이용해도 도움이 될 것 같아요.

웹 사이트의 광고를 차단하면 광고를 통해 감염되는 랜섬웨어 대부분을 예방이 가능할 겁니다. 다만, 의심스러운 이메일을 열어보면 감염될 수 있기 때문에 습관을 조금씩 고쳐야 하죠..

	<p>저는 macOS를 쓰면서 RansomWhere? 라는 앱을 사용 중인데, 이 앱은 시스템에서 벌어지는 모든 암호화 과정을 모니터링 해서 암호화 전에 사용자가 직접 끊어버릴 수 있습니다. 맥 사용자 분들에게는 편리한 랜섬웨어 예방 프로그램인 것 같아요.</p> <p>https://objective-see.com/products/ransomwhere.html</p>
--	--

 <p>컴수진</p>	<p>랜섬웨어는 우선 패치나 백업 등 예방이 최우선이라는데 동의하구요, 광고 차단 역시 사용자에게 피해사례 등을 좀 더 적극적으로 홍보하면 보다 효과적인 대응책이 될것 같습니다!</p>
---	---

 <p>Thomas</p>	<p>랜섬웨어 대응은 사용자뿐만 아니라 관련 기업과 기관에서도 적극적인 홍보와 신속하게 조치 한다면 랜섬웨어로부터 더욱 안전하지 않을까 싶네요.</p>
---	--



나의 소중한 자료를 지키는

랜섬웨어 피해 예방 5대 수칙

랜섬웨어란?
Ransomware

몸값 + 소프트웨어
Ransom + Software

시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램

1 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.

 운영체제 OS
  응용 프로그램 SW

> 최신 보안 업데이트



2 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.

 신뢰할 수 있는 백신
  안티 익스플로잇 도구

> 백신 설치, 최신 업데이트



3 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.

 스팸메일 첨부파일
  URL 링크

> 이메일 및 URL 실행 주의



4 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.

 P2P 토렌트 블로그
  파일공유 사이트

> 파일 다운로드 및 실행 주의



5 중요 자료는 정기적으로 백업합니다.

 문서
  사진

> 별도 매체 백업



정보보호 안내 | KISA 보호나라® KrCERT www.krcert.or.kr | KISA 118 센터

출처 : <https://www.boho.or.kr/ransomware/prevention.do>

2017.10

랜섬웨어는 무엇이고 기업이나 가정에서 어떻게 방어를 해야하나

코드엔진 Talk #2

www.CodeEngn.com

문의사항

www.codeengn.com/contact

Code  Engn