

# Ransomware

## Cerber / Magniber

---

이다영

# C O N T E N T S

---



- CONTENTS 1 :: Ransomware 공격유형
- CONTENTS 2 :: Cerber
- CONTENTS 3 :: Magniber



## CONTENTS 1

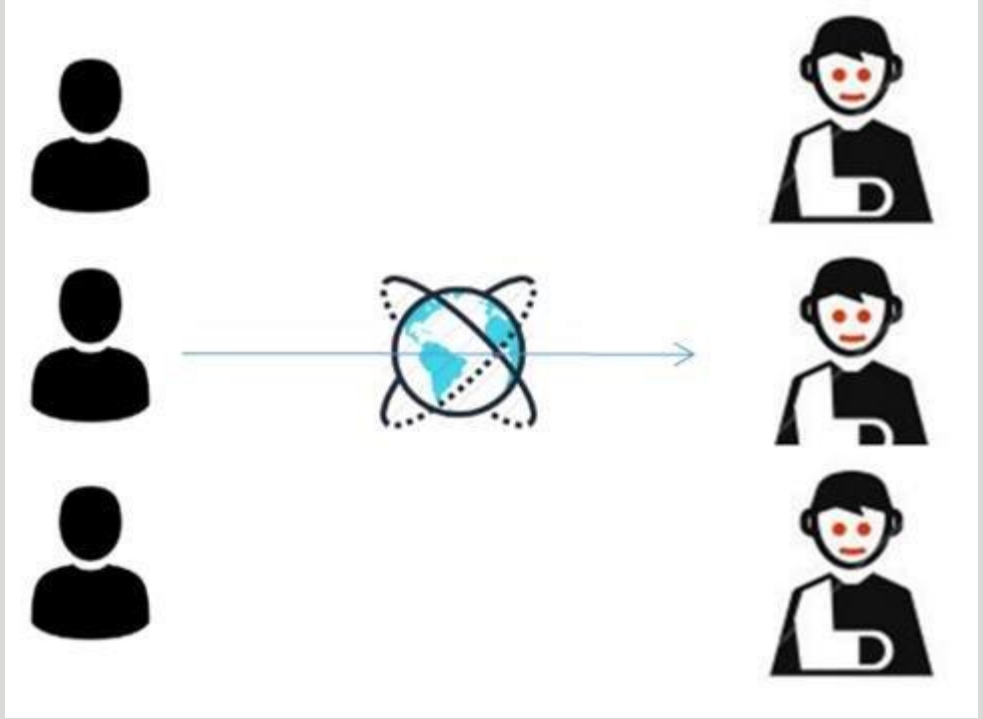
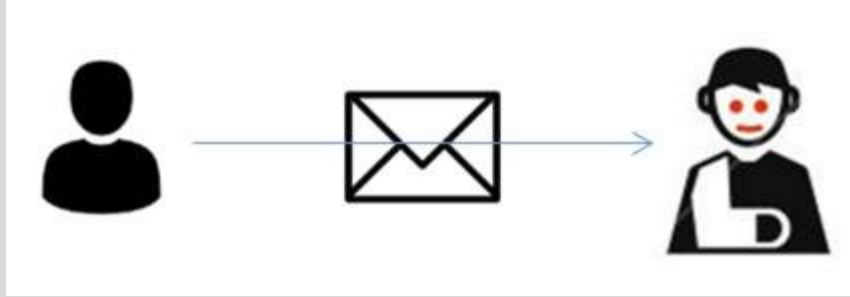
Ransomware 공격유형

## 악성코드

- 컴퓨터에 악영향을 미치는 모든 소프트웨어
- 주요 증상: 시스템 성능 저하, 개인 정보 유출

## 랜섬웨어

- 몸값(ransom) + 소프트웨어(software)
- 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성코드




**Drive-By      Download**  
**지나간다    +    다운로드 하다**  
**“지나가면서 다운로드하다”**

## ① Drive By Download [드라이브 바이 다운로드]

사용자가 알지 못하는 사이에 악성 콘텐츠를 사용자의 동의 없이 컴퓨터로 다운로드 시키는 공격유형





사자가 마치 먹이를 습격하기 위해  
**물웅덩이** 근처에서 매복하고 있는  
형상을 빚댄 것으로, 표적 공격

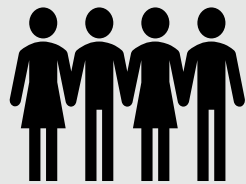
**Watering Hole**

## ② Watering Hole [워터링 홀]

표적으로 삼은 타겟이 방문할 가능성이 있는 웹 사이트를 감염시키고, 피해 대상이 그 웹사이트를 방문할 때까지 기다리는 표적형 + 잠복형 공격유형

# Footprinting [풋프린팅]

해킹 시도 대상의 관련 정보를 수집하는 사전 작업



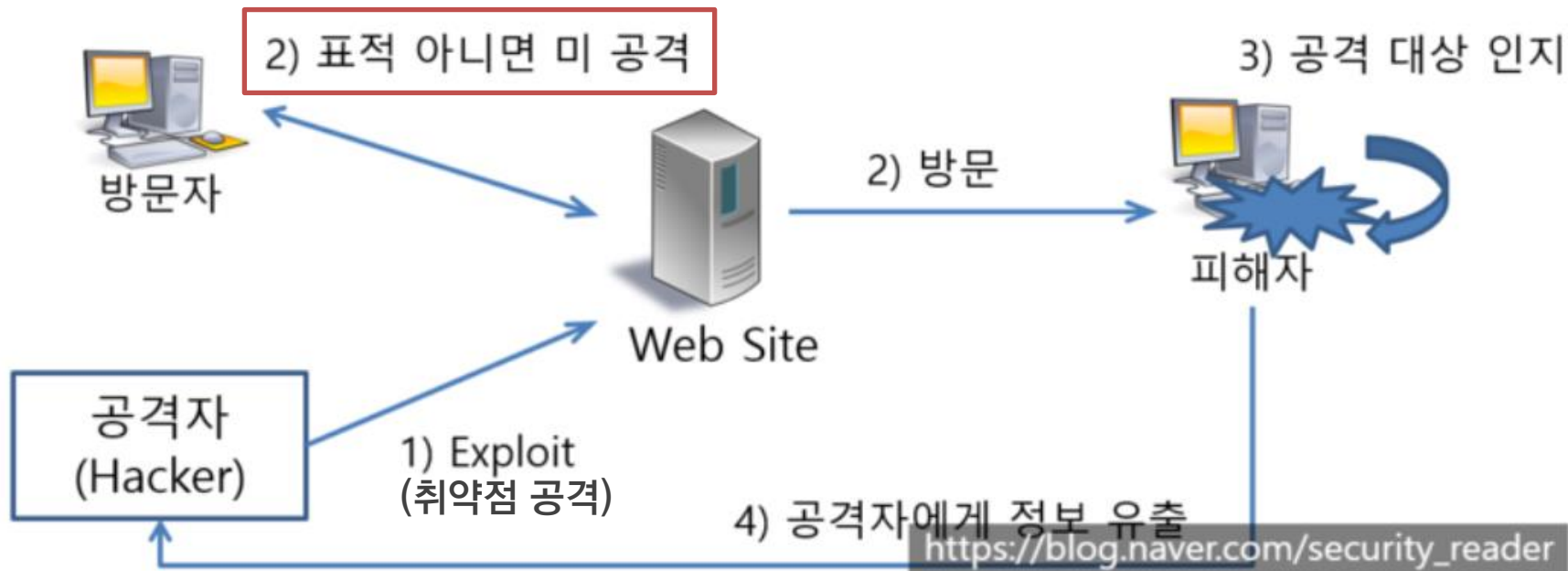
A회사

→ 가평 워크샵



가평의 숙박업소  
홈페이지에 바이러스  
심음

→ 바이러스가 숨어있는  
홈페이지 방문시 악성코드  
실행



위터링 홀의 절차



## CONTENTS 2

Cerber

▷ 2016년에 등장한 랜섬웨어

▷ CERBER1 – CERBER2 – CERBER3 – CERBER4.0.1 – CERBER5.0.1 –  
CERBER6.0.1 – CRBR

▷ Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!(×5)

주의! 주의! 주의! 당신의 문서, 사진, 데이터베이스와 다른 중요한 파일들이 암호화되었습니다!(×5) → 말하는 랜섬웨어

Your documents, photos, databases and other important files  
have been encrypted!

If you understand all importance of the situation then we propose to you  
to go directly to your personal page where you will receive the complete  
instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

- 
1. <http://unocl45trpuoefft.x3nnbd.top/CB62-B9D0-08C5-0446-667B>
  2. <http://unocl45trpuoefft.3vz5yx.top/CB62-B9D0-08C5-0446-667B>
  3. <http://unocl45trpuoefft.ssd5gt.top/CB62-B9D0-08C5-0446-667B>
  4. <http://unocl45trpuoefft.y5j7e6.top/CB62-B9D0-08C5-0446-667B>
  5. <http://unocl45trpuoefft.onion.to/CB62-B9D0-08C5-0446-667B>
  6. <http://unocl45trpuoefft.onion/CB62-B9D0-08C5-0446-667B> (TOR)

CERBER1 ~ CERBER5.0.1



## CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES  
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive  
the private key and decryption program.

To receive the private key and decryption program  
go to any decrypted folder - inside there is the special file (\*README\*)  
with complete instructions how to decrypt your files.

If you cannot find any (\*README\*) file at your PC,  
follow the instructions below:

1. Download "Tor Browser" from <https://www.torproject.org/> and install it.
2. In the "Tor Browser" open your personal page here:

CERBER 6.0.1 이상

이름	수정한 날짜	유형	크기
원본 문서.doc	2016-02-29 오후...	한컴오피스 한글 ...	18KB
원본 문서.hwp	2016-02-29 오후...	한컴오피스 한글 ...	10KB
원본 문서.pdf	2016-02-29 오후...	Adobe Acrobat D...	10KB
원본 문서.ppt	2016-02-29 오후...	한컴오피스 한쇼 ...	189KB
원본 문서.rtf	2016-02-29 오후...	서식있는 텍스트(...	2KB
원본 문서.txt			
원본 사진.bi			
원본 사진.in			
원본 사진...			
원본 압축.zip			
원본 음악.mp3			

파일 암호화

이름	수정한 날짜	유형	크기
# DECRYPT MY FILES #.html	2016-03-08 오후...	HTML 문서	2KB
# DECRYPT MY FILES #.txt	2016-03-08 오후...	텍스트 문서	1KB
# DECRYPT MY FILES #.vbs	2016-03-08 오후...	VBScript 스크립...	1KB
6C qoZMjhXk.cerber		CERBER 파일	10KB
XZG5OVx.cerber		CERBER 파일	1KB
fwzzSKn.cerber		CERBER 파일	7,943KB
HR5ydQRI1R.cerber		CERBER 파일	1,056KB
IeSGsm0IQ5.cerber		CERBER 파일	2KB
KJ-BVKWfsI.cerber		CERBER 파일	19KB
LgLEG75DzZ.cerber		CERBER 파일	19KB
PBxgeNN9og.cerber		CERBER 파일	87KB
vG_SVz-1nT.cerber		CERBER 파일	190KB
YB1_3mKeKZ.cerber		CERBER 파일	8,335KB
원본 문서.hwp	2016-02-29 오후...	한컴오피스 한글 ...	10KB

HammingBird  
울지않는 별새

# 감염경로

인터넷 서핑  
(Drive By Download)

## 현재 Cerber 상황

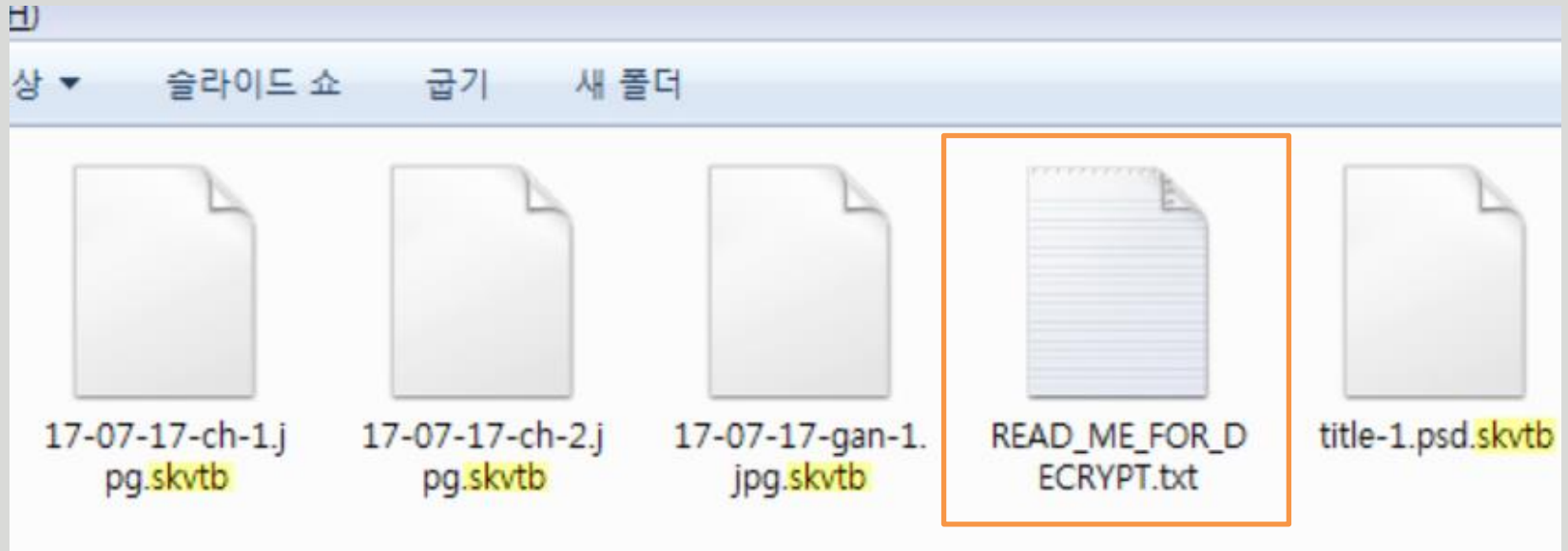




## CONTENTS 3

Magniber

- ▷ 2017년에 등장한, Cerber의 후속 랜섬웨어
- ▷ 한국을 타겟으로 유포되었으나 이후 아시아권으로 세력을 넓힘



skvtb 외에도 ymdmf, hlgjkir, yjnowl, zjgvnwh, madrcby, nbxegz, keaopk 등이 있음

ALL YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

=====

Your files are NOT damaged! Your files are modified only. This modification is reversible.  
The only 1 way to decrypt your files is to receive the private key and decryption program.  
Any attempts to restore your files with the third-party software will be fatal for your files!  
=====

To receive the private key and decryption program follow the instructions below:

1. Download "Tor Browser" from <https://www.torproject.org/> and install it.
2. In the "Tor Browser" open your personal page here:

[http://2o89vqhmy1277tke64g.e263g2eb53wgzvqk.onion/U261\[REDACTED\]](http://2o89vqhmy1277tke64g.e263g2eb53wgzvqk.onion/U261[REDACTED])

Note! This page is available via "Tor Browser" only.

=====

Also you can use temporary addresses on your personal page without using "Tor Browser":

[http://2o89vqhmy1277tke64g.icehas.today/U261\[REDACTED\]](http://2o89vqhmy1277tke64g.icehas.today/U261[REDACTED])

[http://2o89vqhmy1277tke64g.ofguide.xyz/U261X\[REDACTED\]](http://2o89vqhmy1277tke64g.ofguide.xyz/U261X[REDACTED])

[http://2o89vqhmy1277tke64g.withguy.space/U26\[REDACTED\]](http://2o89vqhmy1277tke64g.withguy.space/U26[REDACTED])

[http://2o89vqhmy1277tke64g.lowson.agency/U26\[REDACTED\]](http://2o89vqhmy1277tke64g.lowson.agency/U26[REDACTED])

Note! These are temporary addresses! They will be available for a limited amount of time!



# 감염경로

인터넷 서핑  
(Drive By Download)

## 랜섬웨어 대비

- 윈도우 운영체제, 보안프로그램 업데이트
- 중요한 파일은 그때그때 백업
- 백업한 usb는 사용 완료 후 바로 컴퓨터와 연결을 끊어줄 것

T H A N K  
Y O U

---