공격동향으로 잡아내는 랜섬웨어

For Clean and Safe Internet Environment HAURI

HAURI TSonNet Trusted Systems on the Net

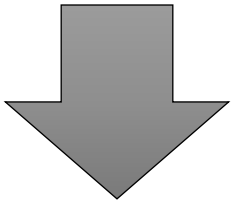
CONTENTS

HAURI

TSonNet Trusted Systems on the Net

01. 랜섬웨어의 급습

Ransom + Ware = 몸값을 요구하는 악성코드
PC에 저장된 주요 데이터 파일들을 암호화
복호화를 위한 몸값(비트코인) 을 요구

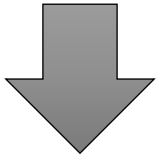


디지털 자산의 보유량 / 사용량 증가에 따른 높은 수익성 보장
공격자의 편의성
- 감염 이후 추가 프로세스 / 유지 불필요

합리적인 가격 책정
- 20만원 ~ 70만원 사이의 지불 가능한 금액

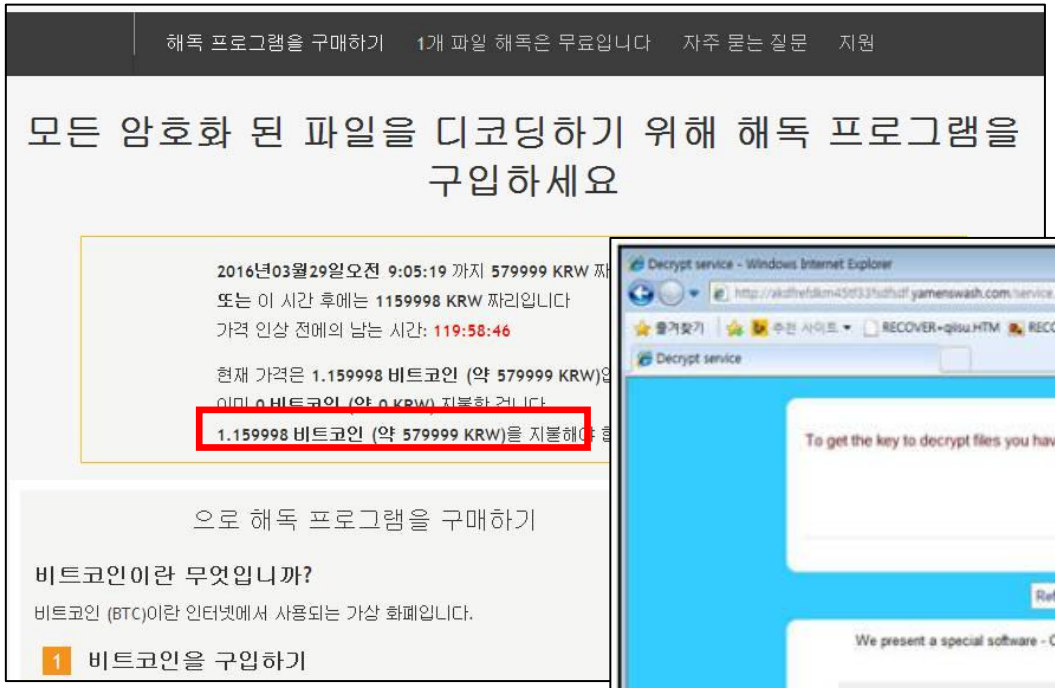
01. 랜섬웨어의 급습

1989년 최초의 랜섬웨어 AIDS 발견
2005 ~ 2006년 러시아발 랜섬웨어 발견
2013.03 ~ : 유럽을 기반으로 위협이 높아 짐
2013.09 ~ : Crypt0l0cker 유포
– 이후 Crypt0l0cker와 비슷한 teslacrypt, CTBlocker 등이 유포됨
2015.11 : 리눅스 랜섬웨어 등장
2015.12.28 : 신종 랜섬웨어 radamant 국내 상륙
2016년 ~ 현재 : Maktub, Locky 등 지속적인 변형 생산 및 유포

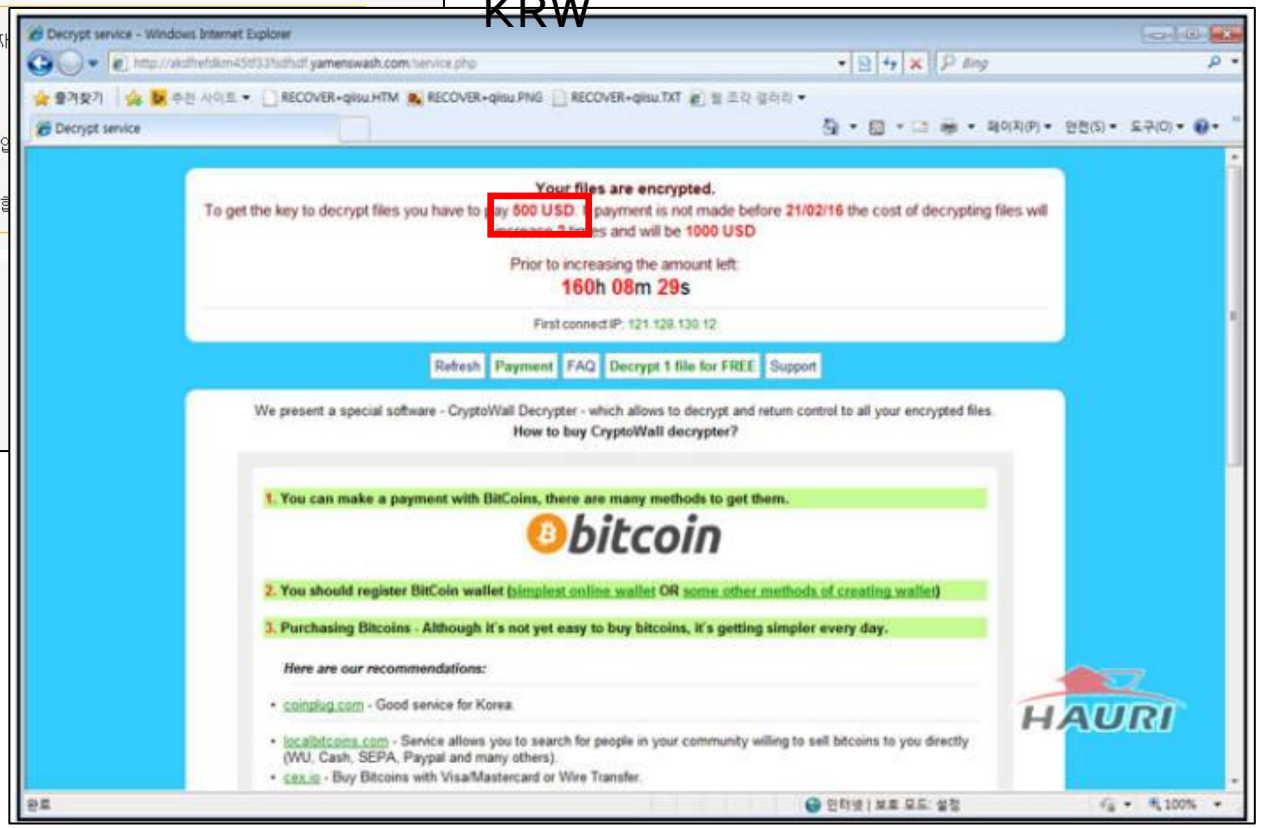


다양한 플랫폼, 지속적인 변화, 업그레이드로 위협 증대

01. 랜섬웨어의 급습



500 $. 약 585000 KRW



HAURI

TSonNet Trusted Systems on the Net

01. 랜섬웨어의 급습

- CryptoWall 수익(15년 10월 기준)

CryptoWall 3.0 Ransomware Operators Made $325 Million

Bitcoin transactions involved in ransoms left a trail that researchers were willing to follow

Because all Bitcoin transactions are logged in the service's blockchain, researchers had the opportunity to take a closer look at the Bitcoin operations that involved the wallet addresses displayed to CryptoWall infected victims.

Mapping out a series of operations that included these publicly displayed wallet addresses and a multitude of intermediary wallets, the Cyber Threat Alliance group has observed that most of them led back to one main Bitcoin account.

It was easy for researchers to conclude that one single cyber-crime was behind all the campaigns. Past transactions and the amount of Bitcoin in the central and lower tier wallets show that the group has made around $325 million / €295 million.

약 3900억원

01. 랜섬웨어의 급습

- FBI 발표

FBI recommends that victims of ransomware pay up

Share this article:

The Federal Bureau of Investigation (FBI) advises companies that fall victim to hacks involving Cryptolocker, Cryptowall or other forms of ransomware to pay the ransom, said Joseph Bonavolonta, an assistant special agent with FBI, speaking at the Cyber Security Summit 2015 in Boston

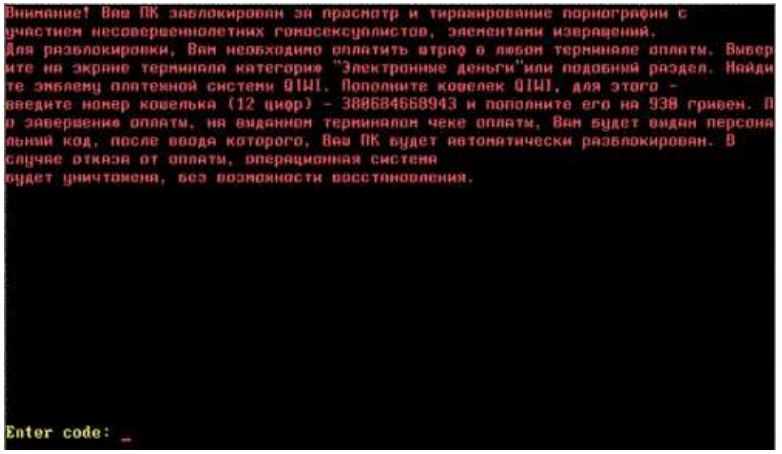
Noting that while the agency has their back, "the ransomware is that good," the Security Ledger quoted Bonavolonta as saying. "To be honest, we often advise people just to pay the ransom" because efforts by the Bureau to defeat the encryption used have proved futile.

An FBI assistant special agent told a group of security professionals that his agency recommends victims of ransomware pay up.

02. 랜섬웨어 종류

- ScreenLock

Winlock



MBR Locker

Police Ransomware

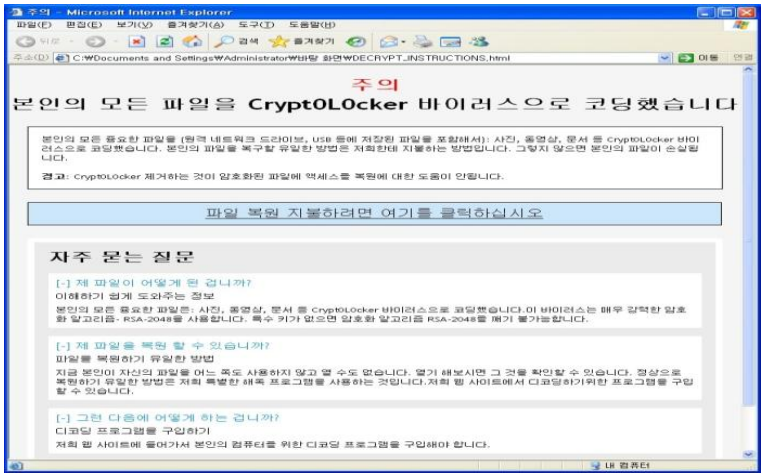
Petya

02. 랜섬웨어 종류

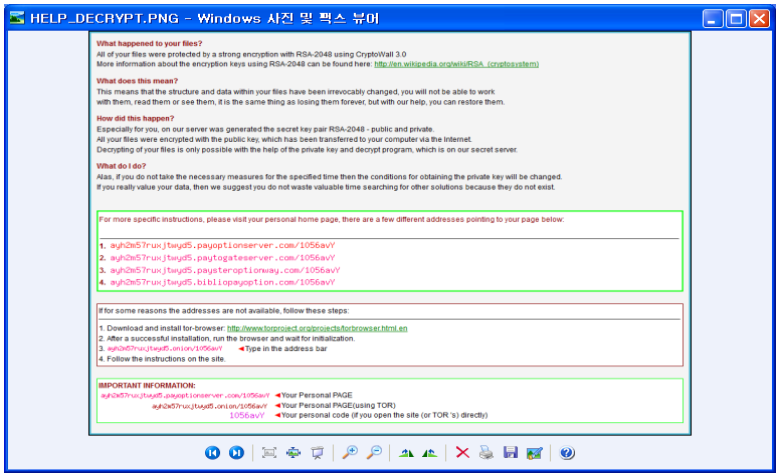
- 동영상 시연

02. 랜섬웨어 종류

- DataLock

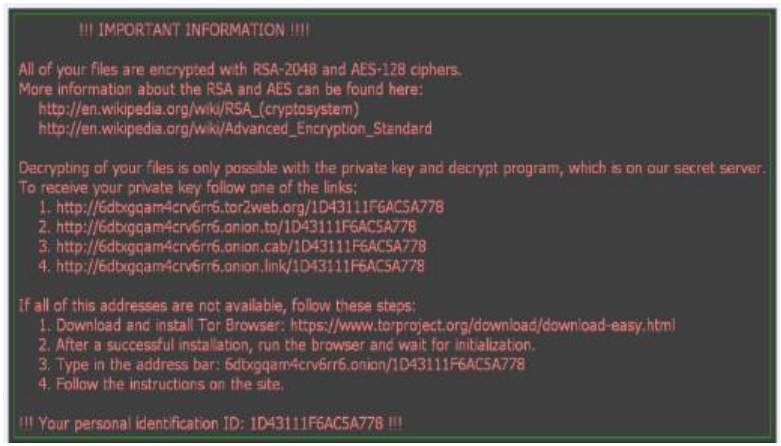


CryptoLocker



CryptoWall

CTB-Locker



Locky

02. 랜섬웨어 종류

- 동영상 시연

02. 랜섬웨어 종류

- Variety Platform Ransomware

```
encrypt_directory((int)"/home");
encrypt_directory((int)"/root");
encrypt_directory((int)"/var/lib/mysql");
while ( 1 )
{
  v8 = getpwent(v18);
  if ( !v8 )
    break;
  encrypt_directory(*(_DWORD *)(v8 + 20));
}
setpwent(v18);
```

Linux

```
7/25/2015  12:57 AM             5742 HKK_adminpage.aspx
7/25/2015  12:57 AM             7902 HKK_airlines.aspx
7/25/2015  12:57 AM             7502 HKK_changepassword1.aspx
7/25/2015  12:57 AM             7374 HKK_changepassword2.aspx
7/25/2015  12:57 AM            11774 HKK_deselectproduct.aspx
7/25/2015  12:57 AM            15342 HKK_Home.aspx
7/25/2015  12:57 AM             8510 HKK_hotel.aspx
7/25/2015  12:57 AM             7838 HKK_insurance.aspx
7/25/2015  12:57 AM            10510 HKK_leisure.aspx
7/25/2015  12:57 AM             7694 HKK_login.aspx
7/25/2015  12:57 AM             9710 HKK_myproduct.aspx
7/25/2015  12:58 AM              382 HKK_packages.config
7/25/2015  12:58 AM            11006 HKK_pcclistN.aspx
7/25/2015  12:58 AM            12318 HKK_productapproval.aspx
7/25/2015  12:58 AM             5870 HKK_productapproved.aspx
7/25/2015  12:58 AM            11646 HKK_productselection.aspx
7/25/2015  12:58 AM            16398 HKK_registration.aspx
7/25/2015  12:59 AM             6590 HKK_Thankyou.aspx
7/25/2015  12:59 AM             9246 HKK_unapproverequest.aspx
7/25/2015  12:59 AM              734 HKK_UnderCons.aspx
7/25/2015  12:59 AM              846 HKK_Web.config
7/25/2015   1:18 AM            <dir> images
7/25/2015   1:18 AM            <dir> Old
7/25/2015   1:18 AM            <dir> Scripts
7/25/2015   1:18 AM             4132 WHAT_IS_HKK_.txt
```

Webserver

README_FOR_DECRYPT.txt

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

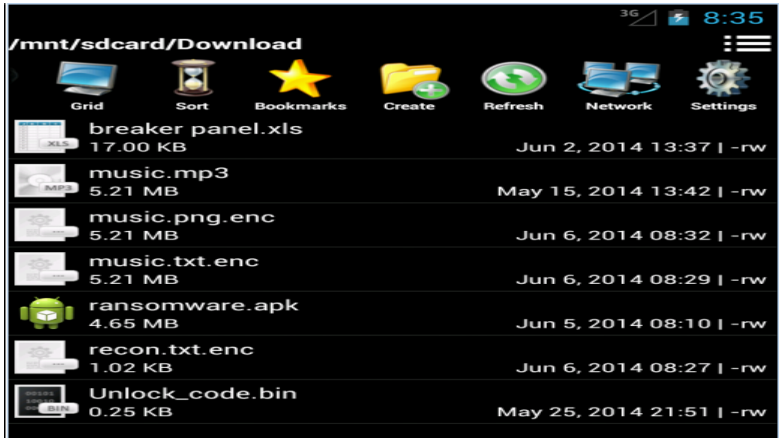
1. Go to [redacted] (IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted])
2. Use [redacted] as your ID for authentication
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoins (wallet is your ID for authentication - [redacted])
4. Download decrypt pack and run

---> Also at [redacted] you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

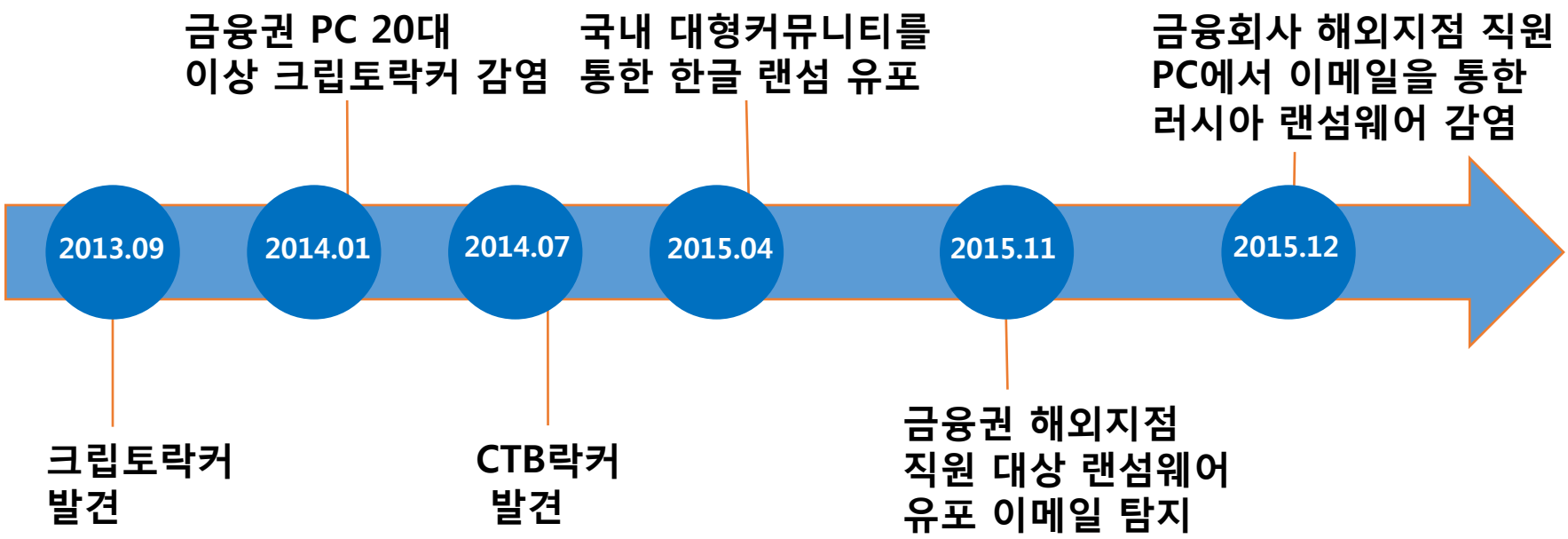
IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)

MacOs



Mobile

03. 랜섬웨어 공격동향



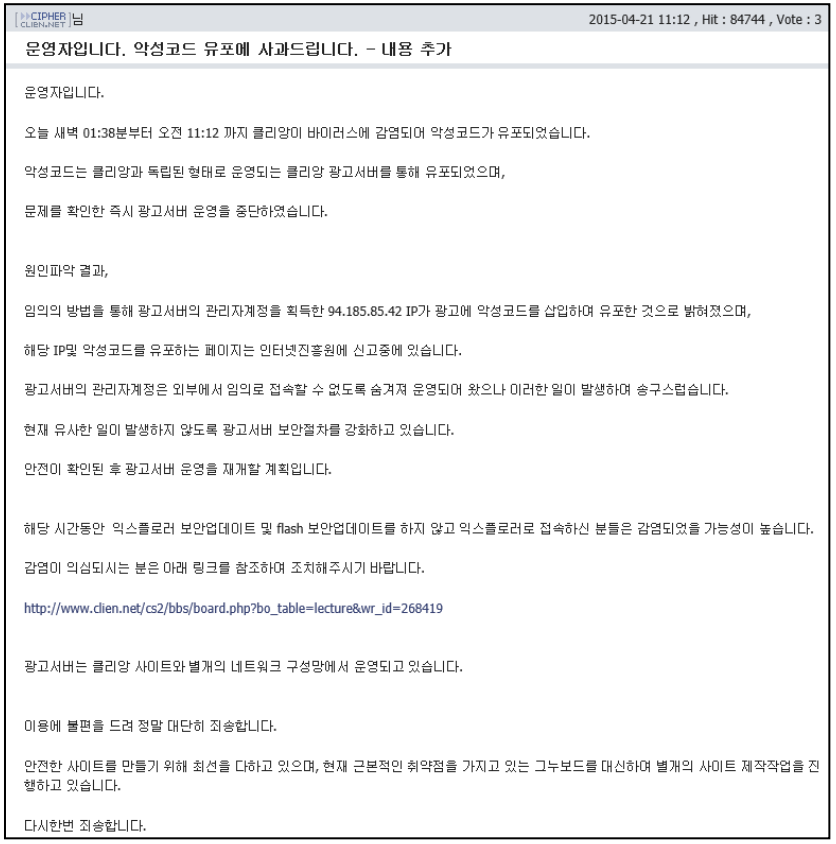
HAURI

TSonNet Trusted Systems on the Net

03. 랜섬웨어 공격동향

- 대형 커뮤니티 사이트에서 랜섬웨어 유포

대형 커뮤니티 광고 배너



2015-04-21 11:12 , Hit : 84744 , Vote : 3

운영자입니다. 악성코드 유포에 사과드립니다. – 내용 추가

운영자입니다.

오늘 새벽 01:38분부터 오전 11:12 까지 클리앙이 바이러스에 감염되어 악성코드가 유포되었습니다.

악성코드는 클리앙과 독립된 형태로 운영되는 클리앙 광고서버를 통해 유포되었으며,

문제를 확인한 즉시 광고서버 운영을 중단하였습니다.

원인파악 결과,

임의의 방법을 통해 광고서버의 관리자계정을 획득한 94.185.85.42 IP가 광고에 악성코드를 삽입하여 유포한 것으로 밝혀졌으며,

해당 IP및 악성코드를 유포하는 페이지는 인터넷진흥원에 신고중에 있습니다.

광고서버의 관리자계정은 외부에서 임의로 접속할 수 없도록 숨겨져 운영되어 왔으나 이러한 일이 발생하여 송구스럽습니다.

현재 유사한 일이 발생하지 않도록 광고서버 보안절차를 강화하고 있습니다.

안전이 확인된 후 광고서버 운영을 재개할 계획입니다.

해당 시간동안 익스플로러 보안업데이트 및 flash 보안업데이트를 하지 않고 익스플로러로 접속하신 분들은 감염되었을 가능성이 높습니다.

감염이 의심되시는 분은 아래 링크를 참조하여 조치해주시기 바랍니다.

http://www.clien.net/cs2/bbs/board.php?bo_table=lecture&wr_id=268419

광고서버는 클리앙 사이트와 별개의 네트워크 구성망에서 운영되고 있습니다.

이용에 불편을 드려 정말 대단히 죄송합니다.

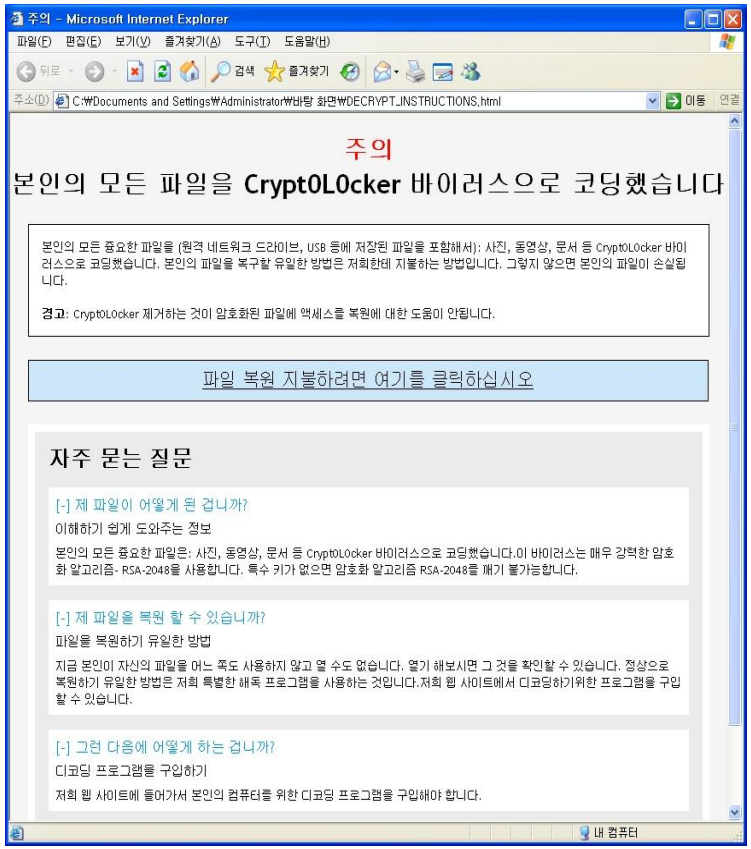
안전한 사이트를 만들기 위해 최선을 다하고 있으며, 현재 근본적인 취약점을 가지고 있는 그누보드를 대신하여 별개의 사이트 제작작업을 진행하고 있습니다.

다시한번 죄송합니다.

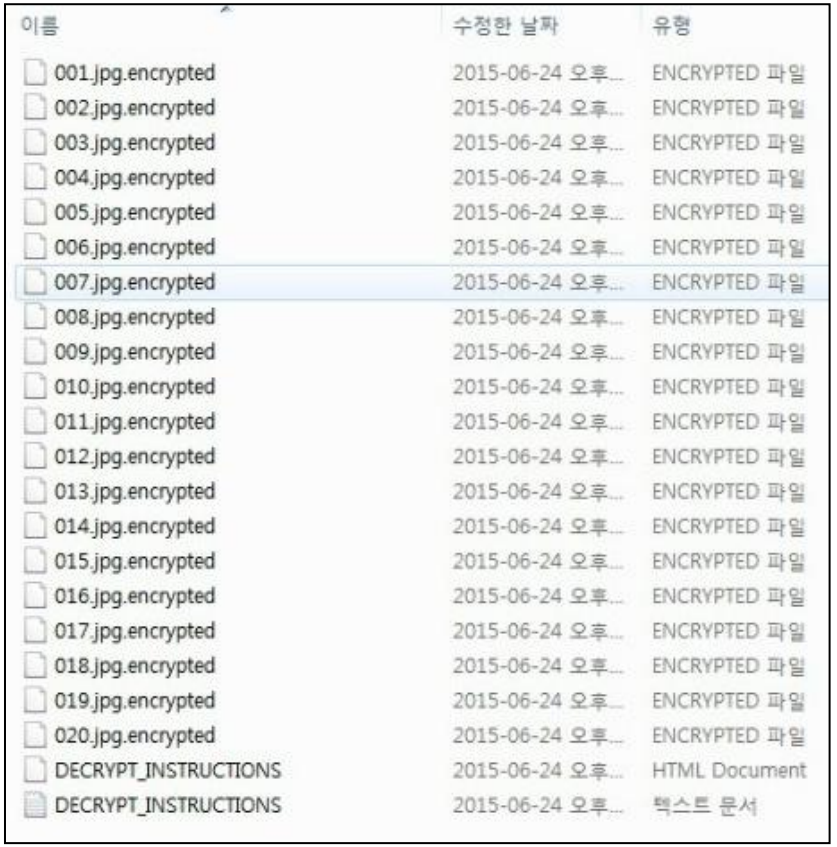
랜섬웨어 유포 사과공지

03. 랜섬웨어 공격동향

- 랜섬웨어 증상 / 신고 급증



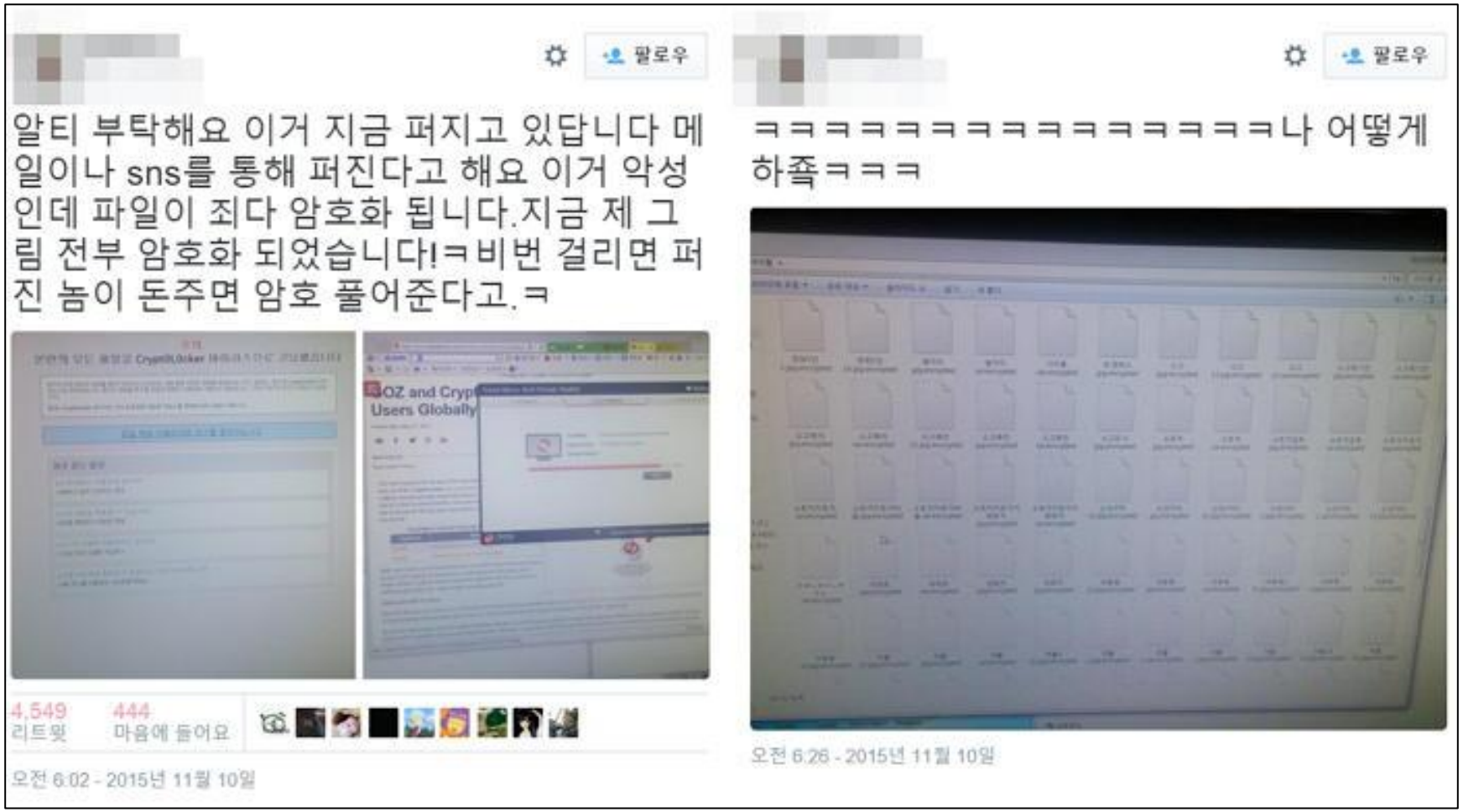
CryptoLocker 감염화면



암호화된 파일

03. 랜섬웨어 공격동향

- 랜섬웨어 증상 / 신고 급증



03. 랜섬웨어 공격동향

- 할리우드 장로교 의료 센터 랜섬웨어 감염

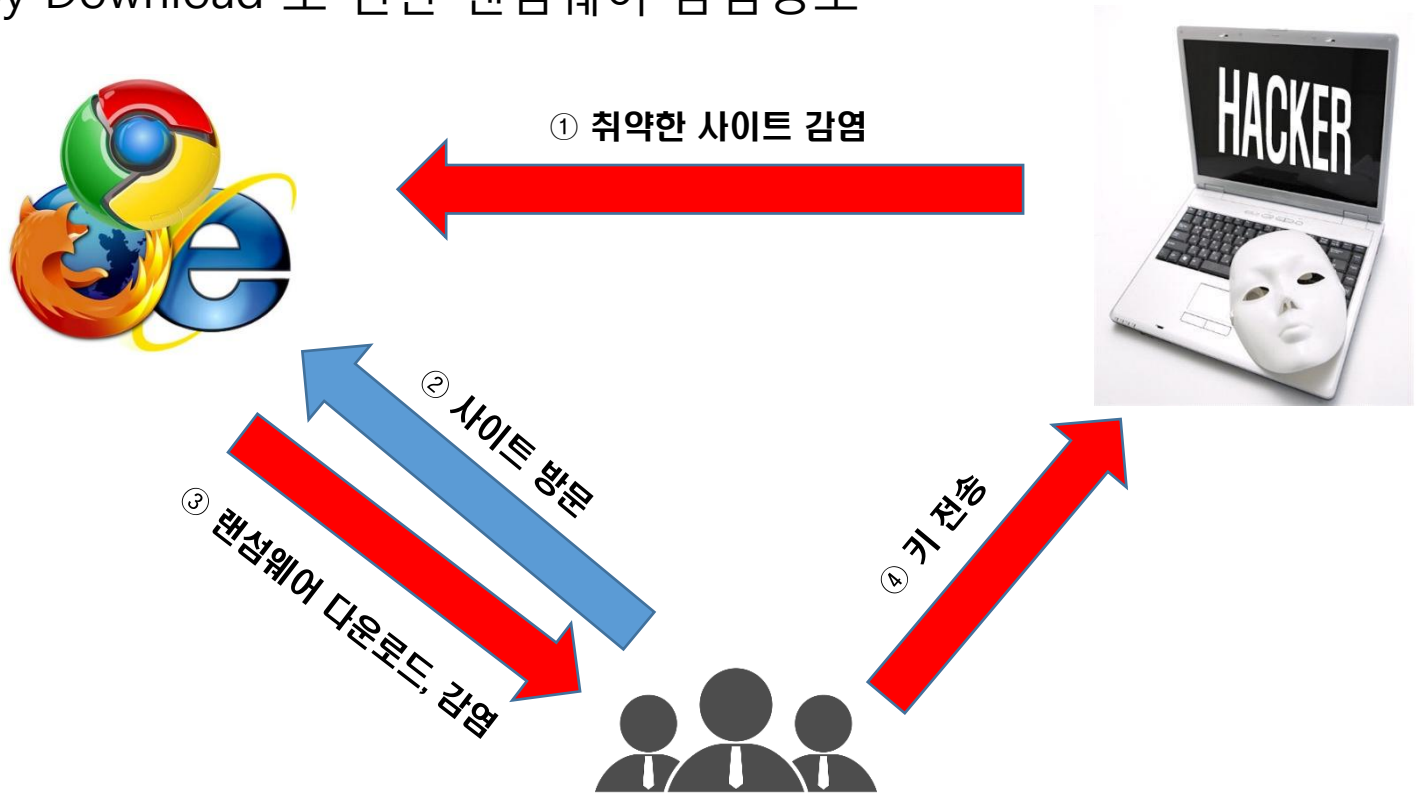
'The quickest and most efficient way to restore our systems ... was to pay the ransom,' said Allen Stefanek, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni/Reuters

A Los Angeles hospital hit by ransomware swallowed the bitter pill: it paid off the hackers.

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their computer files. The only out was if the hospital paid the hackers $17,000 worth of bitcoins, the digital currency.

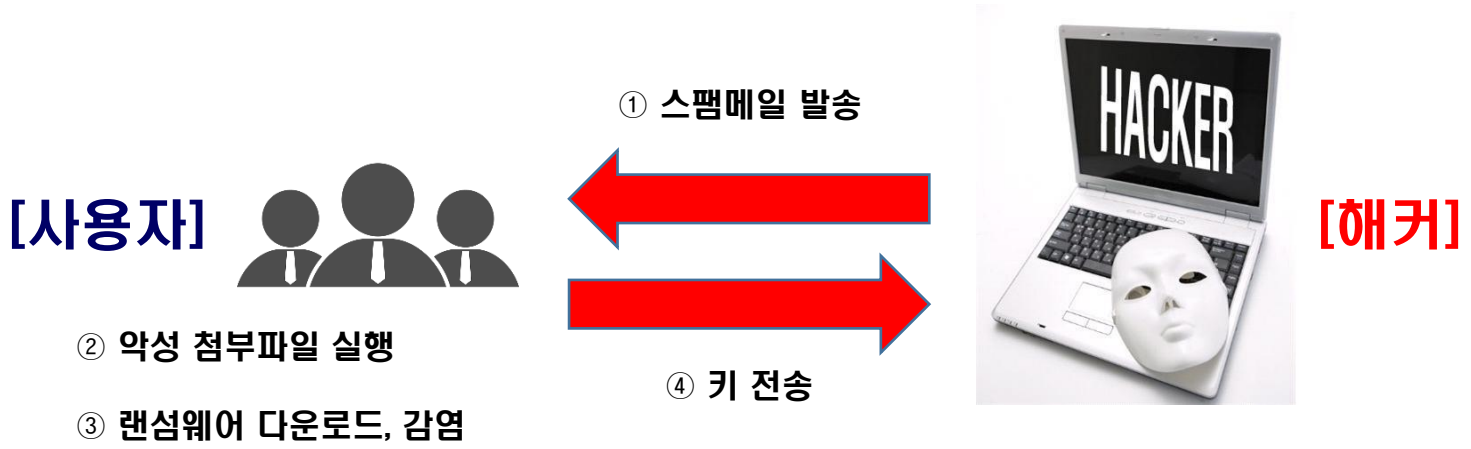
03. 랜섬웨어 공격동향

- Drive By Download 로 인한 랜섬웨어 감염경로



03. 랜섬웨어 공격동향

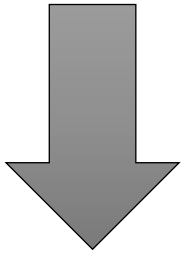
- 스팸메일 감염경로



04. 대응현황

안전한 플랫폼은 존재하지 않음.
- Linux, MacOs, Mobile 다양한 플랫폼에 랜섬웨어 유포

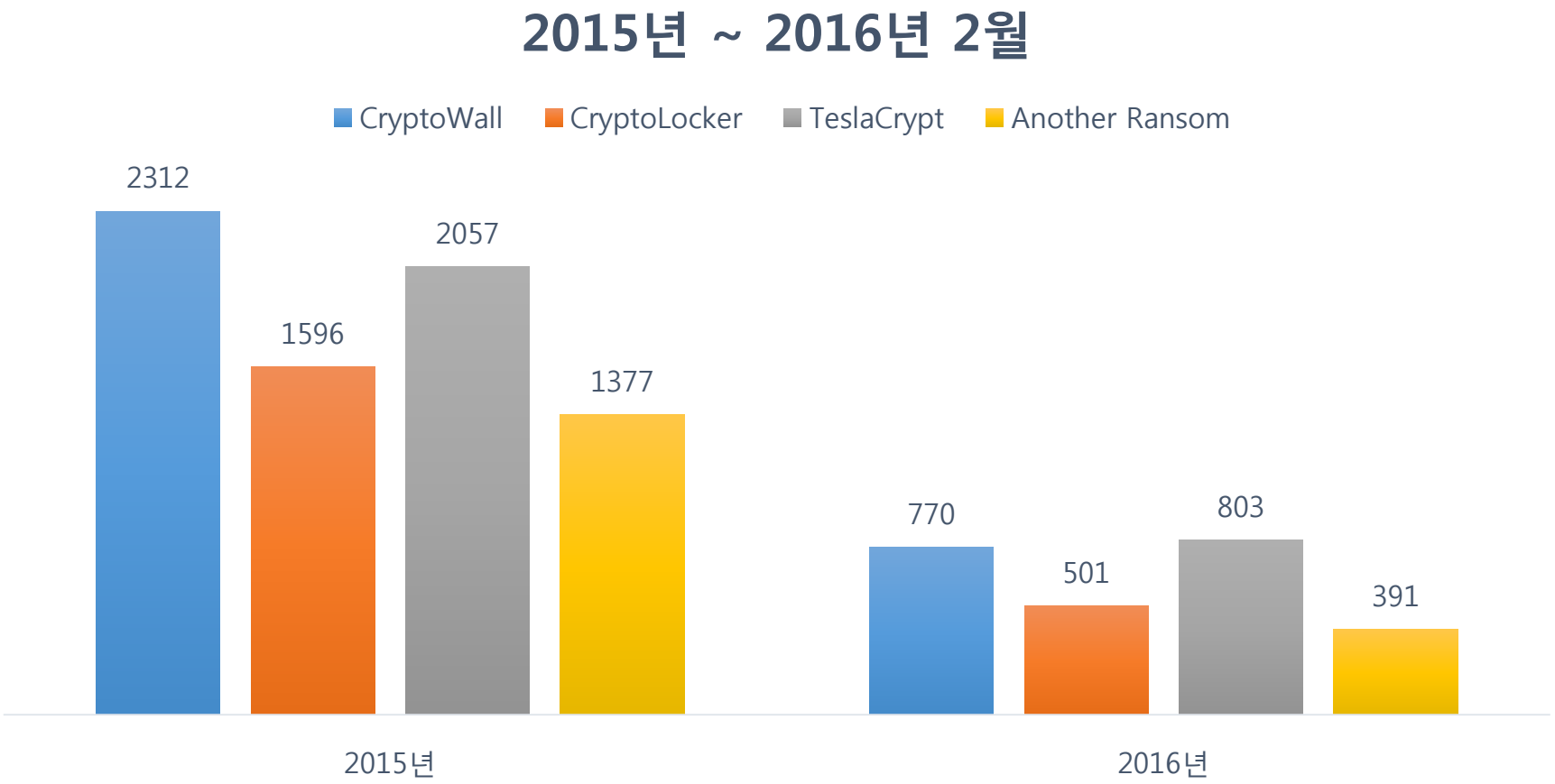
위협에 대한 근본적인 방어대책 미흡
- 스팸메일 차단, C&C 차단 등 기존 방어대책의 문제점 발견.



행위를 기반으로 한 근본적 방어 방법 필요

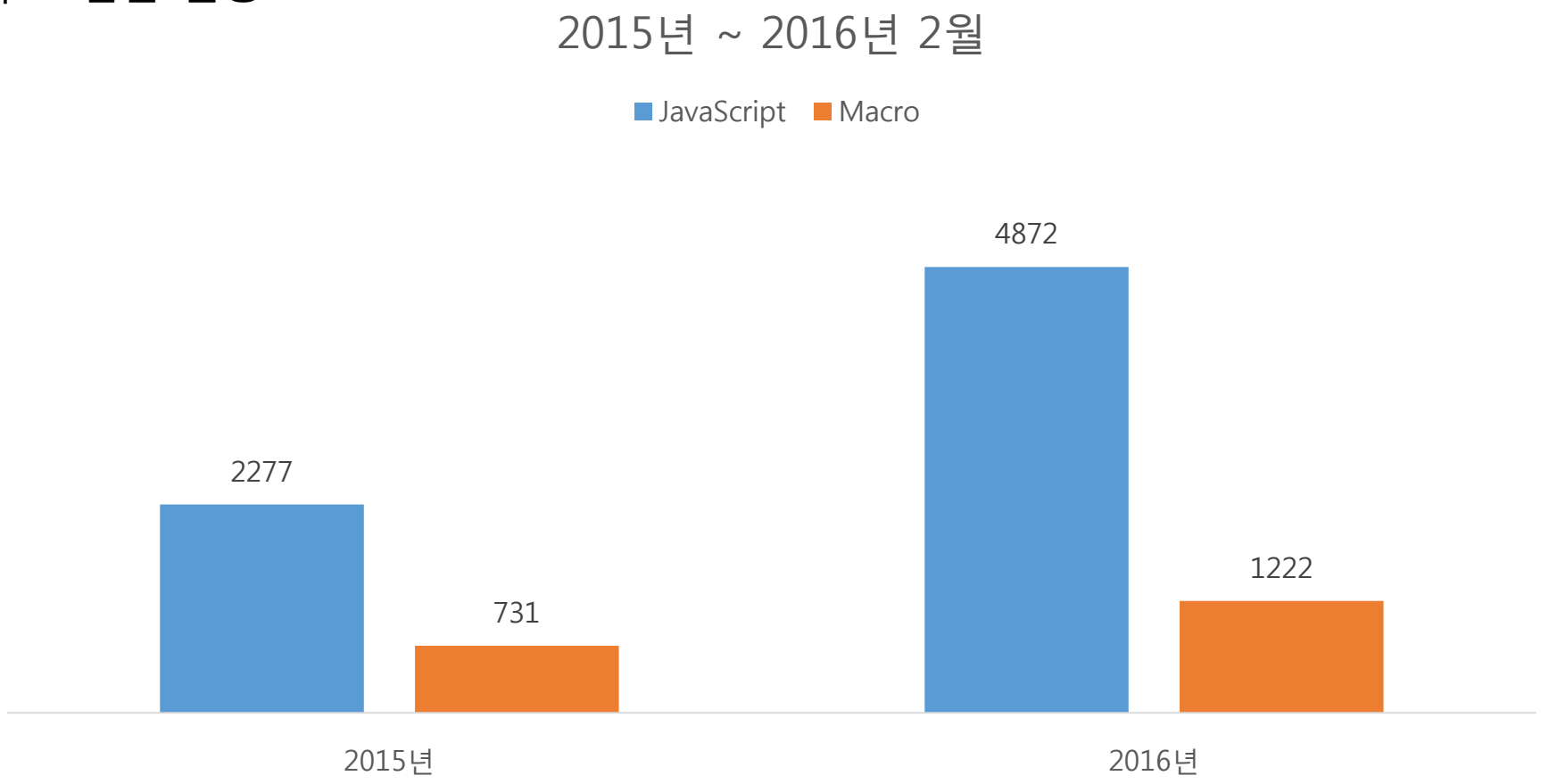
04. 대응현황

- 랜섬웨어 샘플 현황



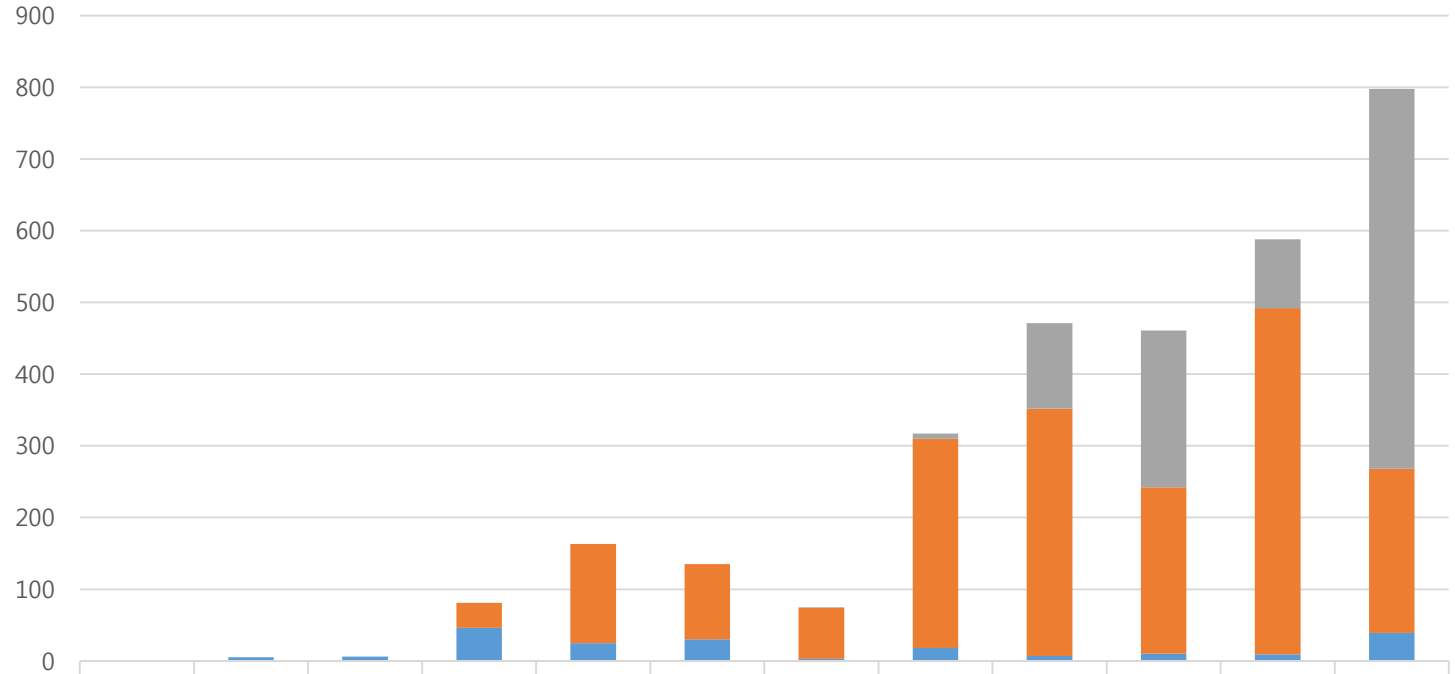
04. 대응현황

- 유포 샘플 현황



04. 대응현황

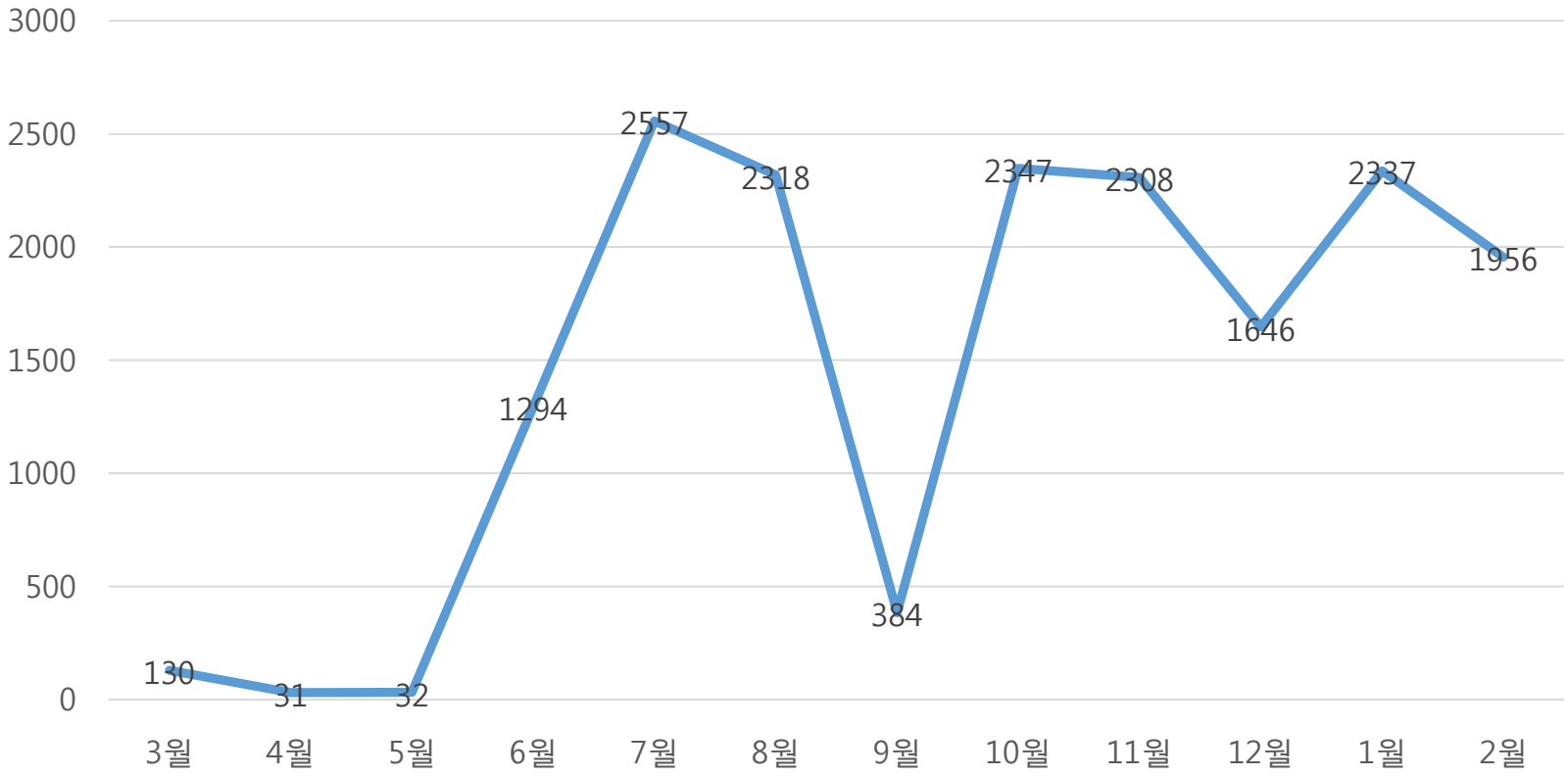
- 대표 3종의 랜섬웨어가 드라이브 바이 다운로드 방식으로 국내 사이트를 통해 유포된 현황 (2015년 3월~2016년 2월)



	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	1월	2월
TeslaCrypt	0	0	0	0	0	0	1	7	119	219	96	530
CryptoWall	0	0	0	35	138	105	71	292	345	232	483	229
CryptoLocker	0	5	6	46	25	30	3	18	7	10	9	39

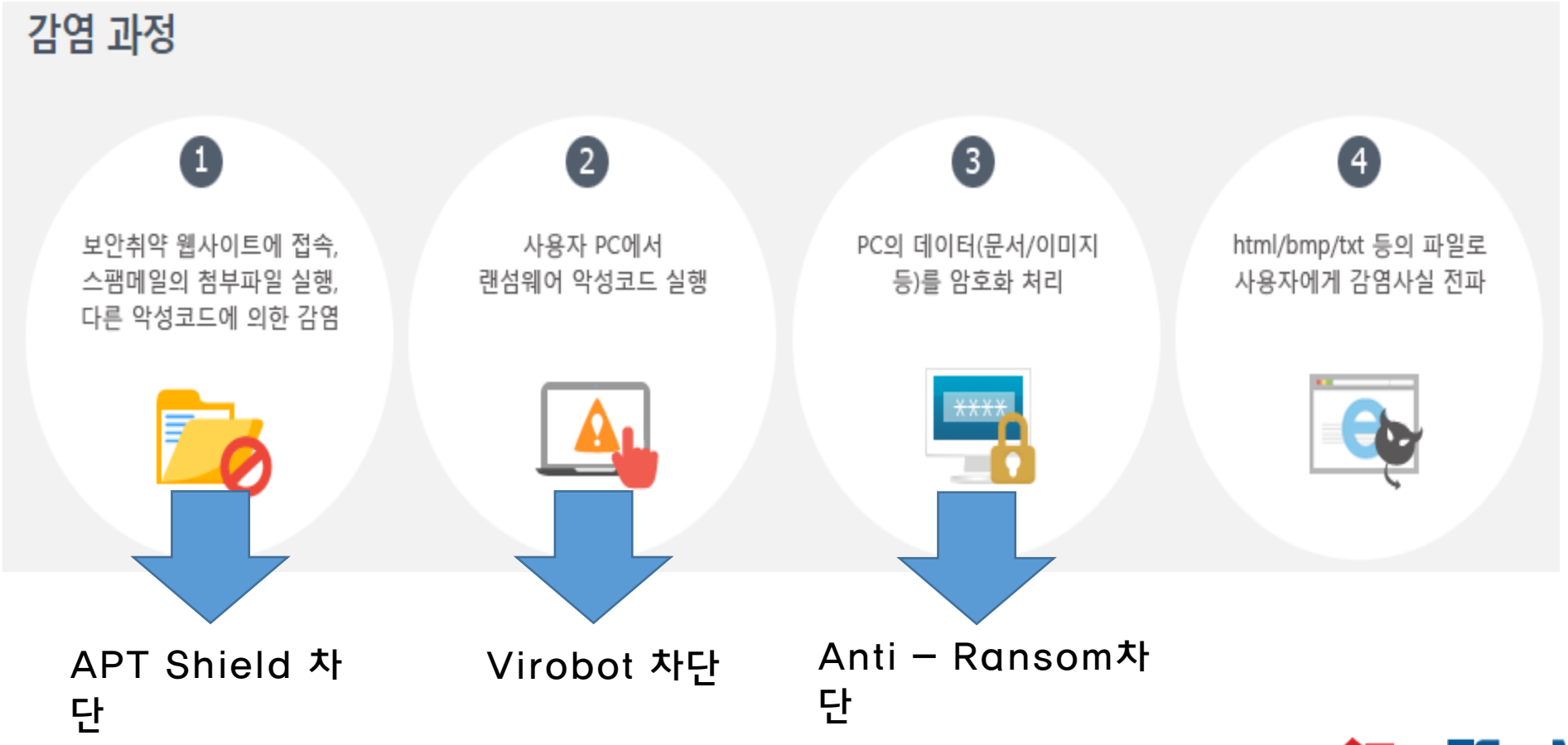
04. 대응현황

- APT Shield에서 드라이브 바이 다운로드를 통해 유포되는 랜섬웨어 차단 현황 (2015년 3월~2016년 2월)



04. 대응현황

- Ransomware 차단 과정



04. 대응현황

- APT Shield 차단 시연 동영상

05. Q & A

Thank you!

For Clean and Safe Internet Environment HAURI



HAURI TSonNet Trusted Systems on the Net