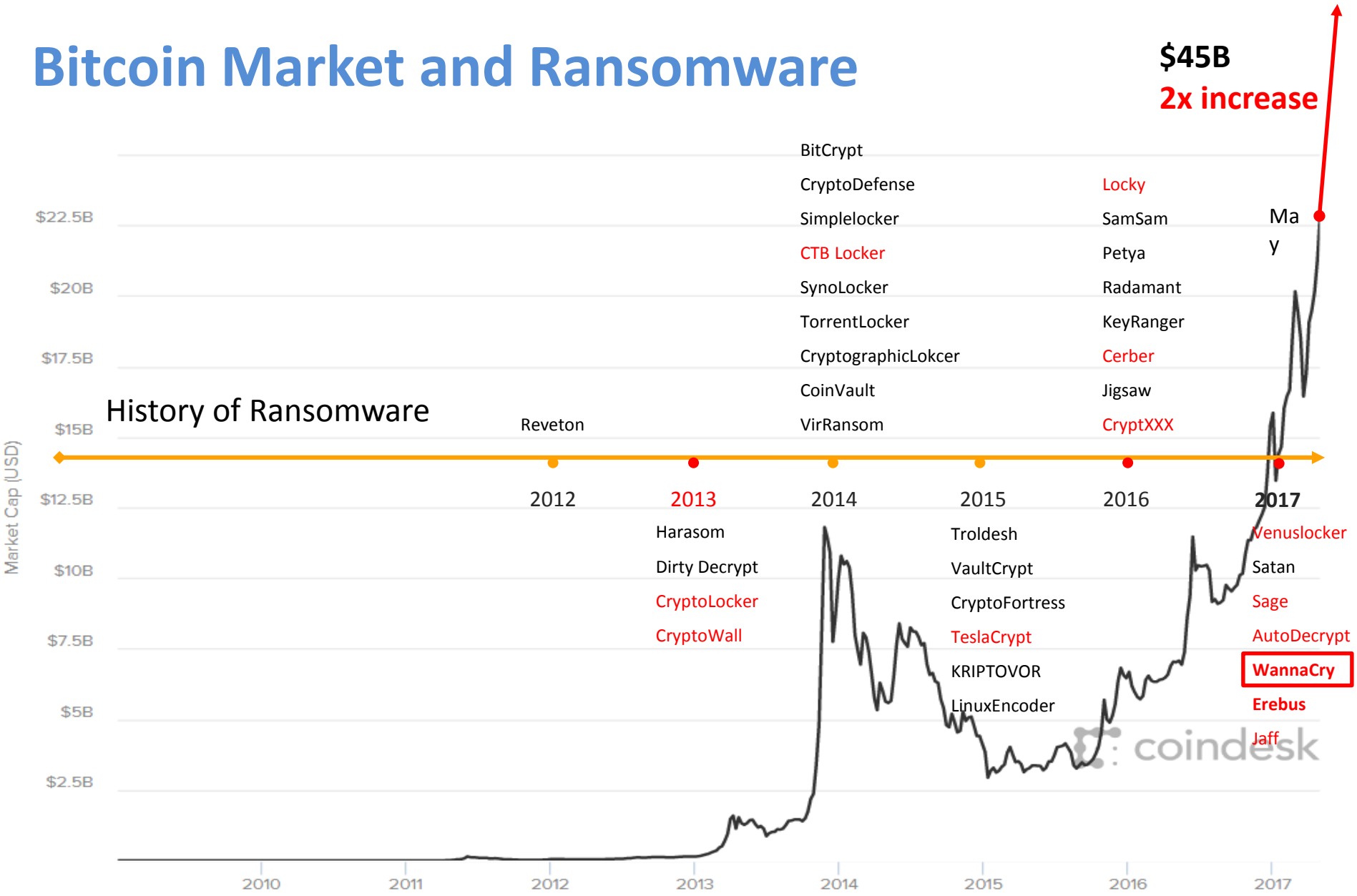

ITU

The Lessons and Challenges of WannaCry Ransomware

Keundug Park, Sangmyung Choi

WannaCry Ransomware

Bitcoin Market and Ransomware



Source: https://www.coindesk.com/

Using SMB vulnerability leaked by ShadowBrokers

Made public

Lost in Translation **Apr. 14, 2017**

theshadowbrokers in shadowbrokers — 2 months ago (2017. 4. 14. 오후 5:52:39)

KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeee

theshadowbrokers @shadowbrokerss — Jan. 8, 2017

#EquationGroup #CyberSecurity #BreakingNews @RT_com @RT_Deutsch
theShadowBrokers is having #WindowsWarez posted and now for sale.

영어 번역하기

windows_screenshots.zip (sig)
windows_warez.zip (sig)

Auction

FuzzBunch

Name	Type	Price
FuzzBunch All	FuzzBunch Everything	650.0 BTC
FuzzBunch Base	Exploit Framework only	25.0 BTC
FuzzBunch Exploits	RCEs for IIS, RDP, RPC, SMB	250.0 BTC
FuzzBunch Implants	SMB Cloaked BackDoor	50.0 BTC
FuzzBunch Payloads	Shellcode, Helpers, Tools	50.0 BTC
FuzzBunch Specials	RCE for SMB (Zero Day?)	250.0 BTC
FuzzBunch Storage	BackDoor, Shellcode, Helpers, Tools	50.0 BTC
FuzzBunch Touches	Touches	Free with Exploits

SMB protocol vulnerability

Propagation Speed of WannaCry Ransomware

NETWORK WORM

May. 13, 2017 (For about 2 hours)

from MalwareTech

Source: https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html

Global Infection Statistics of WannaCry

MalwareTech

@MalwareTechBlog

Other account is @MalwareTechLab
Tweets are not my own they are the opinions of my employer, family, and
my dog.

United Kingdom

malwaretech.com

206,968
ONLINE

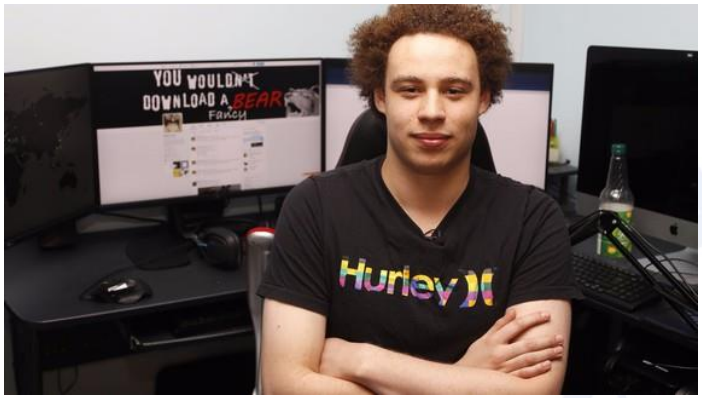
328,121
OFFLINE

535,089
TOTAL

Infection Map (age: 0h 57m 48s)

Source: https://www.malwaretech.com/

Found of Kill-Switch (British 22-year-old)

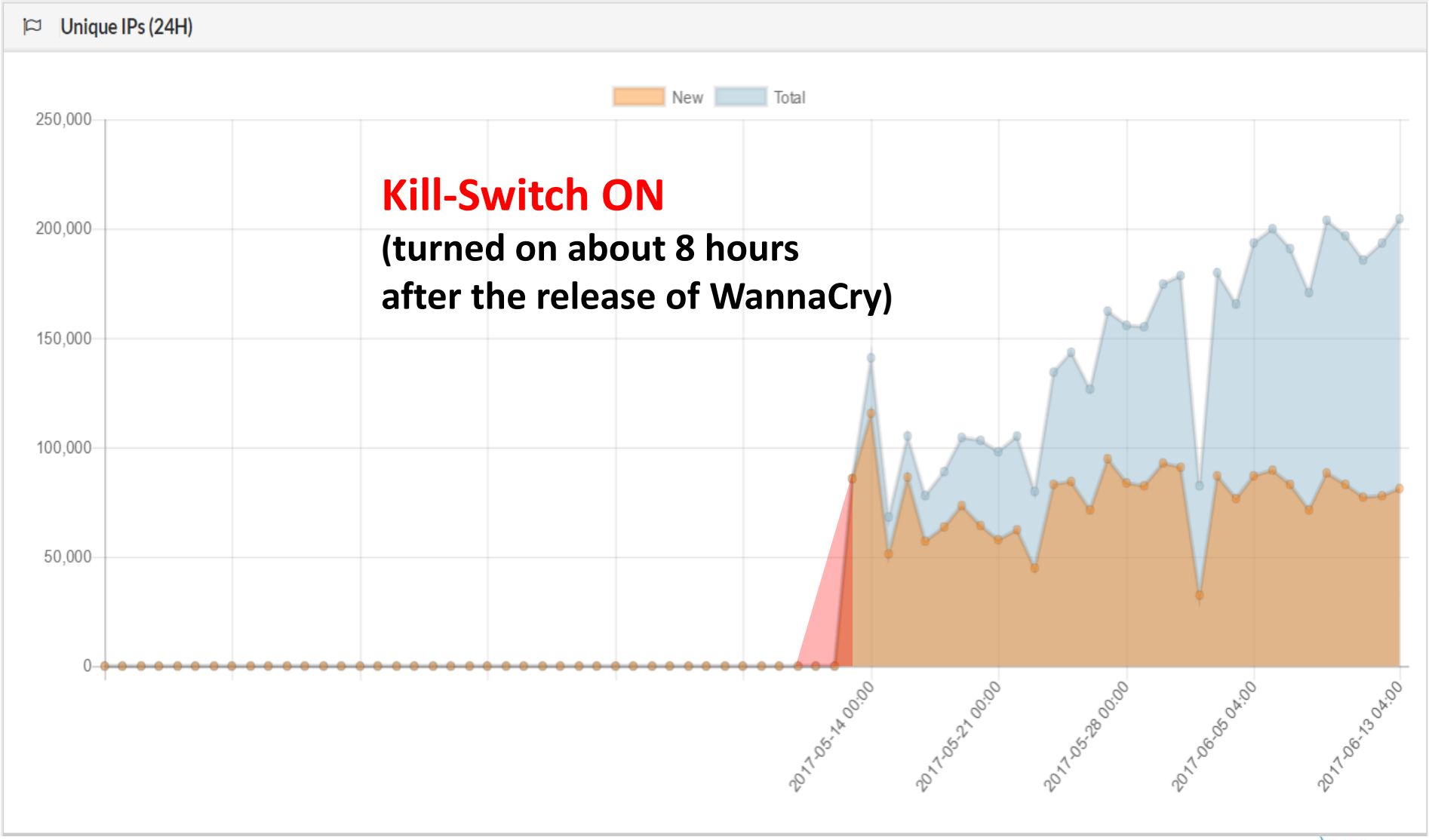


Marcus Hutchins (MalwareTech)

Just bought the domain for only $10.69

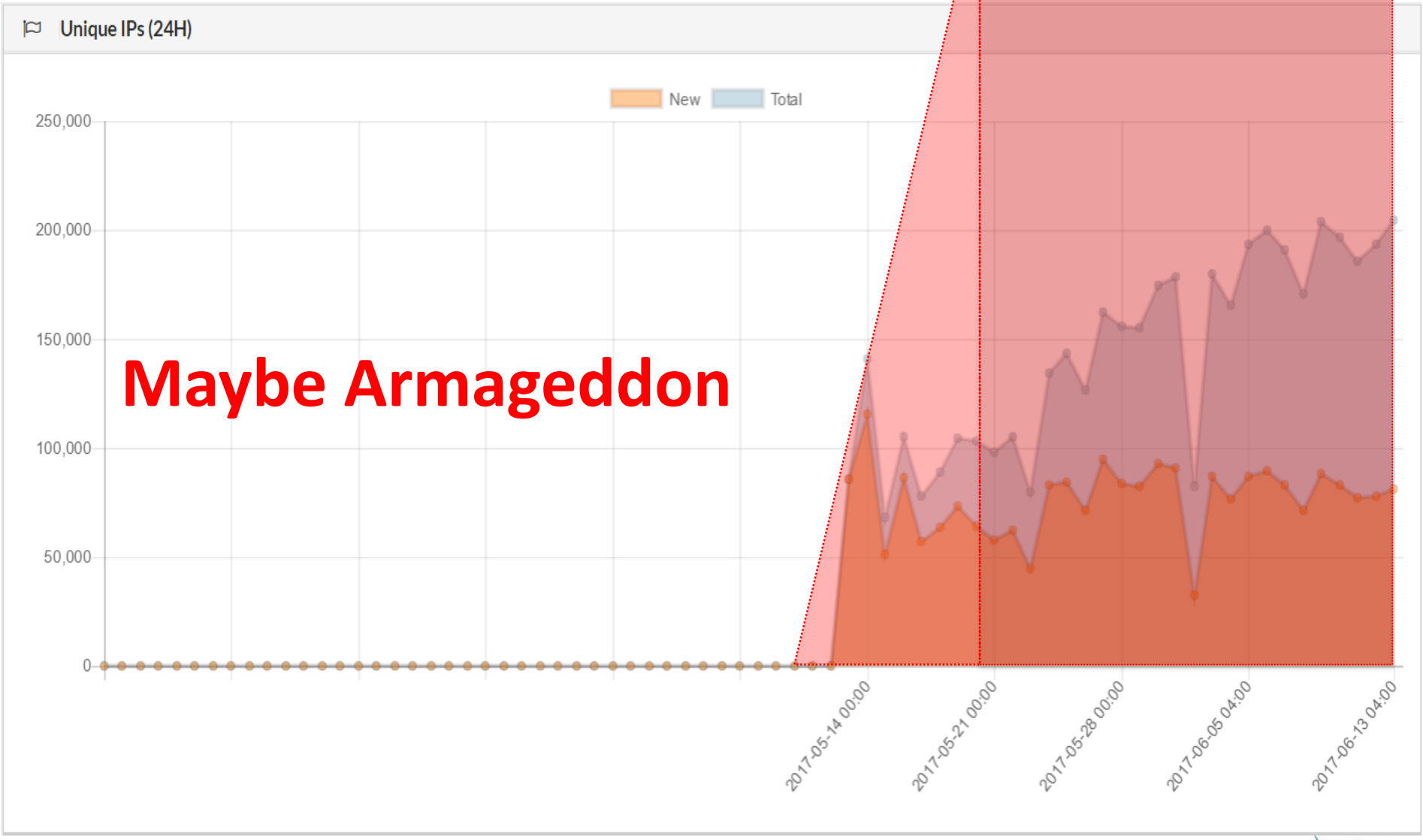
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Kill-Switch ON



Source: https://www.malwaretech.com/

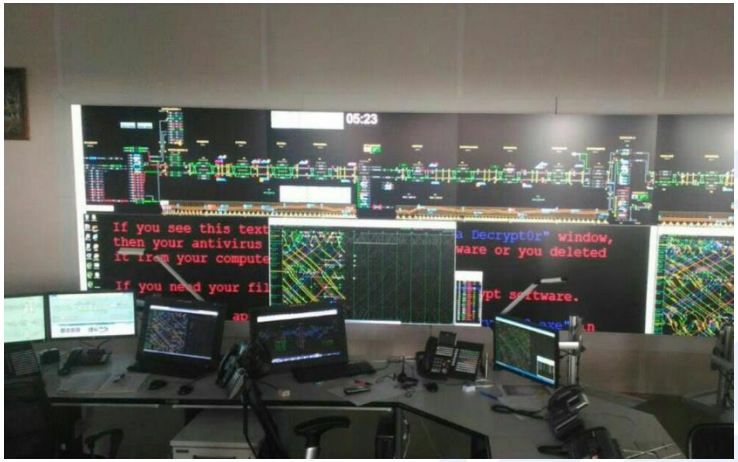
If didn't find Kill-Switch



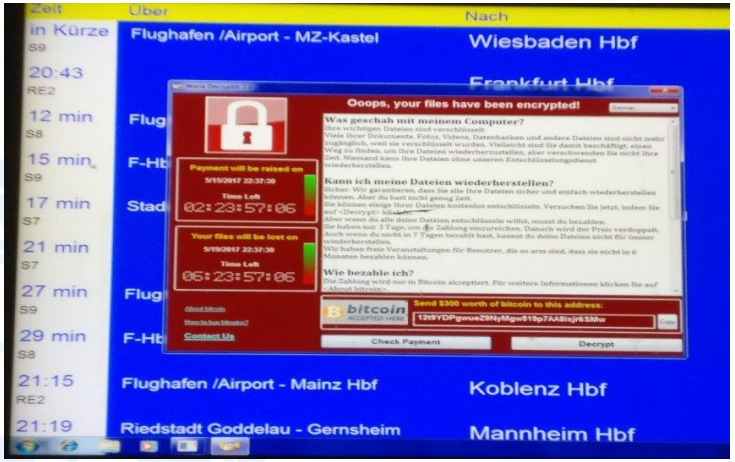
Maybe Armageddon

Source: https://www.malwaretech.com/

WannaCry damage cases (Global)

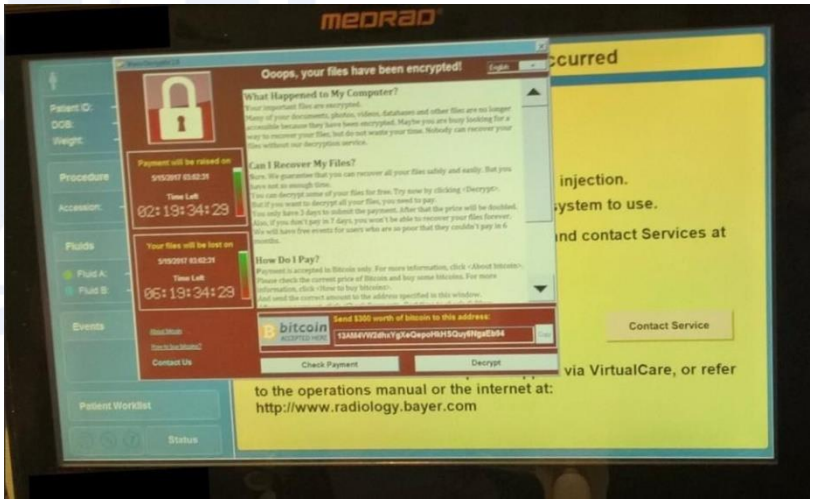


<Railroad>



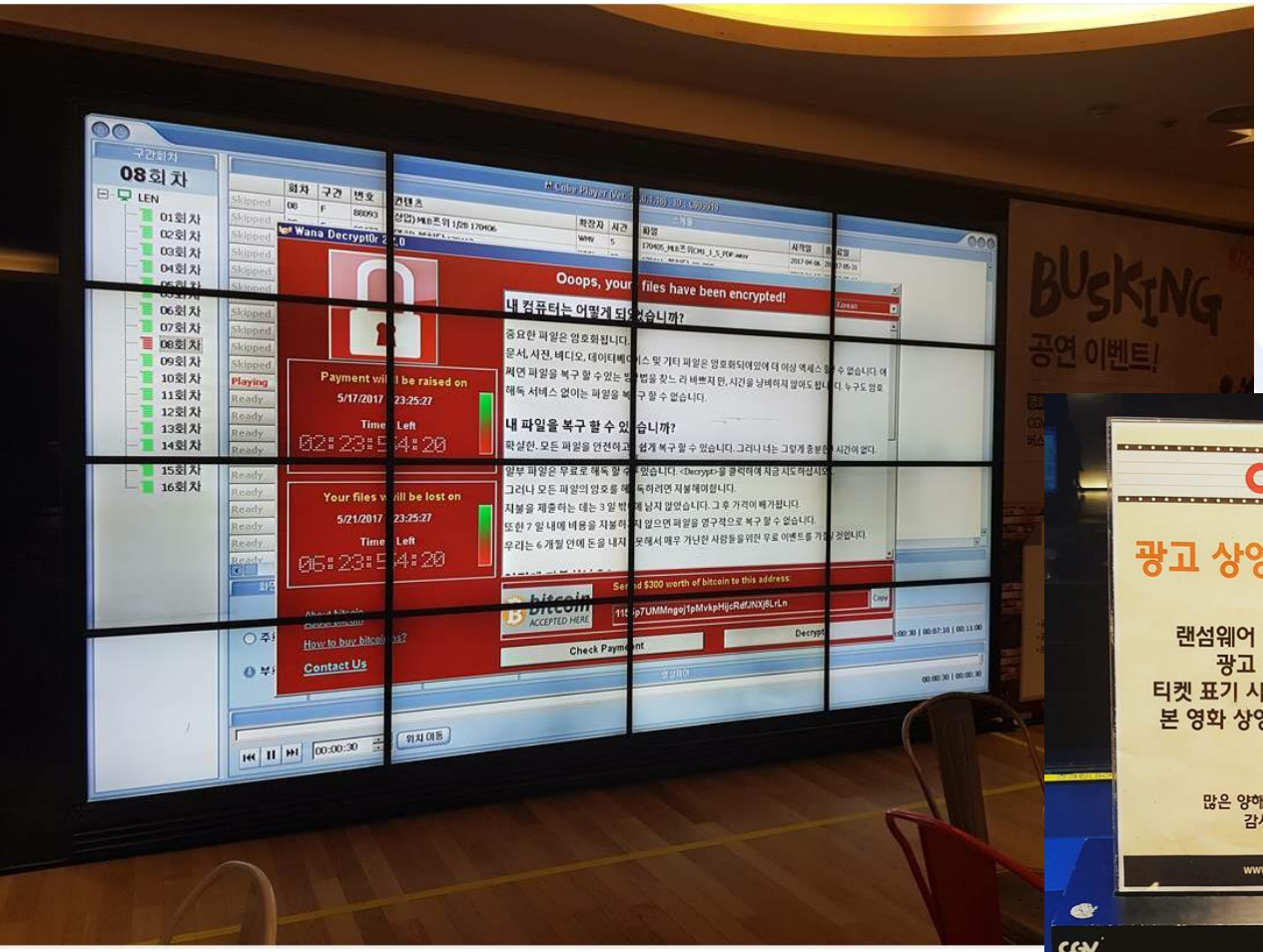
<Airport>

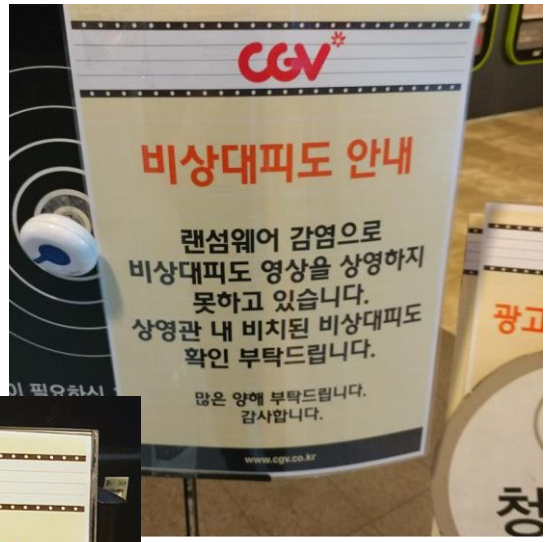
<ATM>

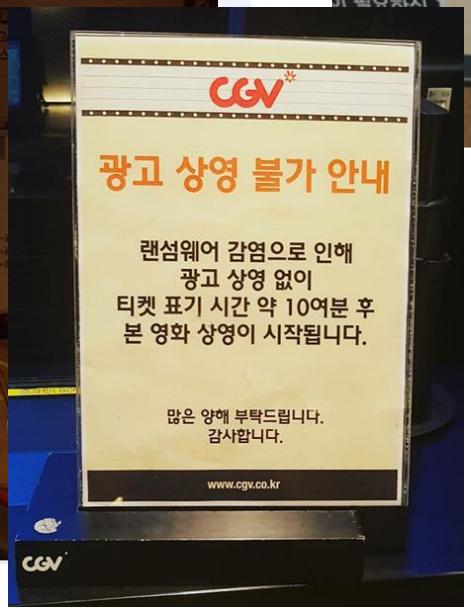


<Hospital>

WannaCry cases (Korea) - Movie theater



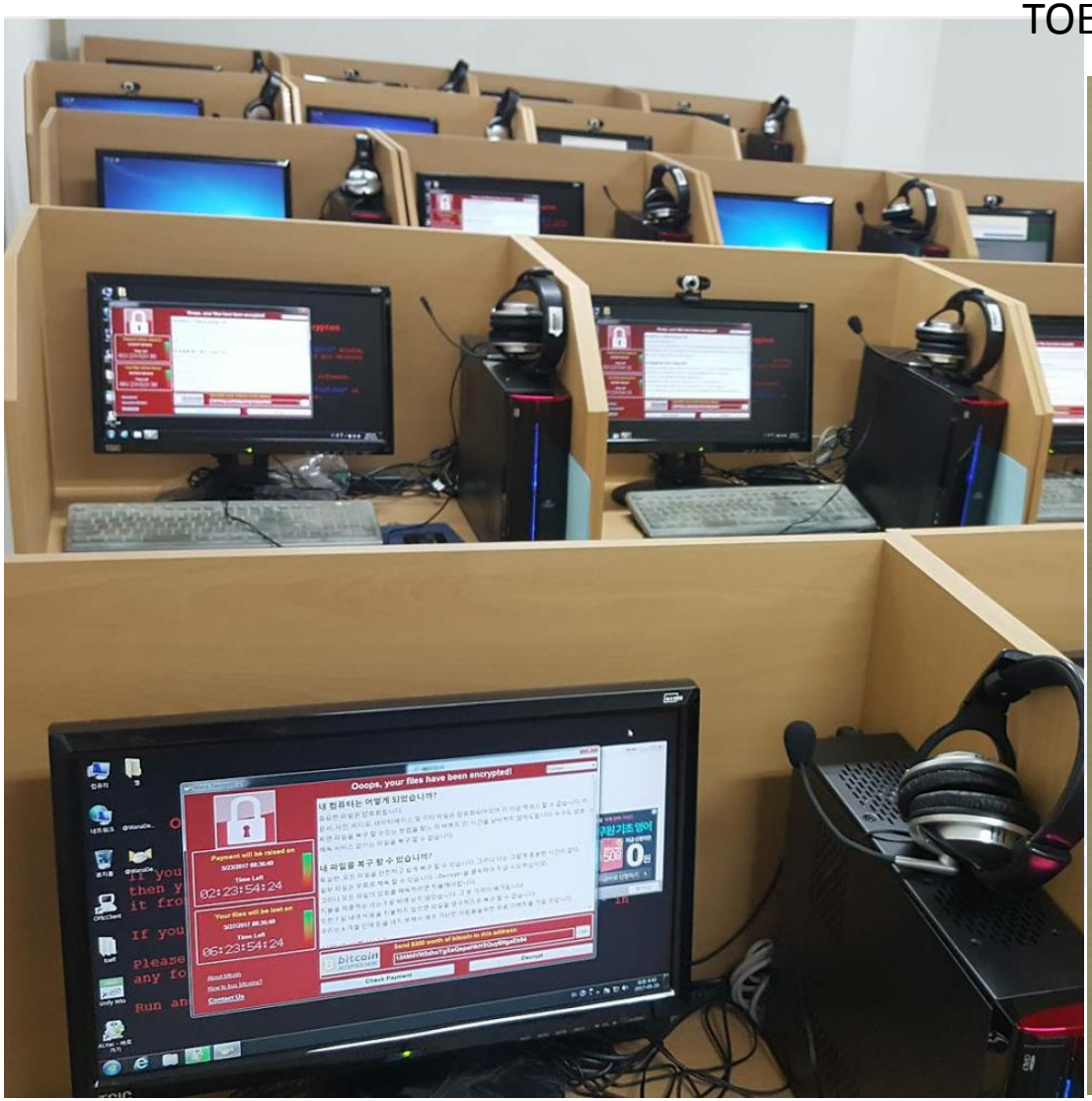


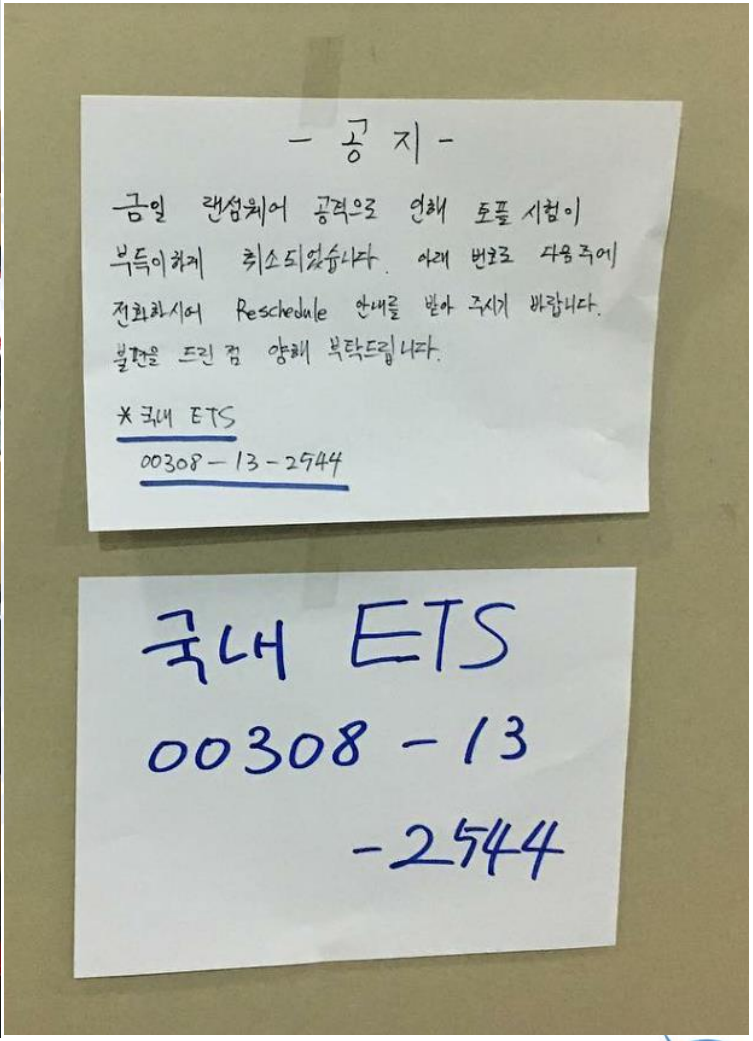


No commercials and emergency escape videos were shown for about a week.

WannaCry cases (Korea) - TOEFL Test Site

TOEFL (Test of English as a Foreign Language)





Cancellation of the TOEFL test

Comparison with other Lazarus's malware

South Korea's media hack Malware (2013)

```
cmp     edx, 0FFFFFFFFh
jz      short loc_10002000
mov     dx, hostshort[edx*2]
push    edx             ; _DWORD
call    htons
mov     ecx, [esp+14h+arg_0]
mov     [ecx], ax
jmp     short loc_1000200C
-------------------------------------

                        ; CODE XREF
                        ; NK_sub_1
mov     eax, [esp+14h+arg_0]
dec     edi
sub     eax, 2
mov     [esp+14h+arg_0], eax

                        ; CODE XREF
mov     ecx, [esp+14h+arg_0]
inc     edi
add     ecx, 2
cmp     edi, ebx
mov     [esp+14h+arg_0], ecx
jl      short loc_10001FAE

                        ; CODE XREF
lea     edx, [ebx+ebx]
push    edx             ; _DWORD
call    htons
mov     [esi], ax
lea     eax, [esi+ebx*2+2]
pop     edi
pop     esi
mov     byte ptr [eax], 1
inc     eax
mov     byte ptr [eax], 0
mov     ecx, [ebp+0]
sub     eax, ebp
and     ecx, 0FFh
sub     eax, 3
shl     eax, 8
xor     eax, ecx
mov     [ebp+0], eax
mov     eax, ebp
pop     ebp
pop     ebx
pop     ecx
retn
```

SWIFT Bank hack Malware (2015)

```
cmp     edx, 0FFFFFFFFh
jz      short loc_10004C60
mov     dx, hostshort[edx*2]
push    edx             ; _DWORD
call    htons
mov     ecx, [esp+14h+arg_0]
mov     [ecx], ax
jmp     short loc_10004C6C
-------------------------------------

                        ; CODE XR
                        ; NK_sub_
mov     eax, [esp+14h+arg_0]
dec     edi
sub     eax, 2
mov     [esp+14h+arg_0], eax

                        ; CODE XR
mov     ecx, [esp+14h+arg_0]
inc     edi
add     ecx, 2
cmp     edi, ebx
mov     [esp+14h+arg_0], ecx
jl      short loc_10004C0E

                        ; CODE XR
lea     edx, [ebx+ebx]
push    edx             ; _DWORD
call    htons
mov     [esi], ax
lea     eax, [esi+ebx*2+2]
pop     edi
pop     esi
mov     byte ptr [eax], 1
inc     eax
mov     byte ptr [eax], 0
mov     ecx, [ebp+0]
sub     eax, ebp
and     ecx, 0FFh
sub     eax, 3
shl     eax, 8
xor     eax, ecx
mov     [ebp+0], eax
mov     eax, ebp
pop     ebp
pop     ebx
pop     ecx
retn
```

WannaCry Malware (2017)

```
cmp     edx, 0FFFFFFFFh
jz      short loc_402617
mov     dx, ds:hostshort[edx*2]
push    edx             ; hostshort
call    ds:htons
mov     ecx, [esp+14h+arg_0]
mov     [ecx], ax
jmp     short loc_402623
-------------------------------------

                        ; CODE XREF:
                        ; NK_sub_402
mov     eax, [esp+14h+arg_0]
dec     edi
sub     eax, 2
mov     [esp+14h+arg_0], eax

                        ; CODE XREF:
mov     ecx, [esp+14h+arg_0]
inc     edi
add     ecx, 2
cmp     edi, ebx
mov     [esp+14h+arg_0], ecx
jl      short loc_4025C5

                        ; CODE XREF:
lea     edx, [ebx+ebx]
push    edx             ; hostshort
call    ds:htons
mov     [esi], ax
lea     eax, [esi+ebx*2+2]
pop     edi
pop     esi
mov     byte ptr [eax], 1
inc     eax
mov     byte ptr [eax], 0
mov     ecx, [ebp+0]
sub     eax, ebp
and     ecx, 0FFh
sub     eax, 3
shl     eax, 8
xor     eax, ecx
mov     [ebp+0], eax
mov     eax, ebp
pop     ebp
pop     ebx
pop     ecx
retn
```

Same as camouflage communication protocol

Comparison with other Lazarus's malware

Sony Pictures Malware (2014)

```
.text:0040555C sub_40555C      proc near               ; CODE XREF: sub_40536C+B1p
.text:0040555C                                         ; sub_40536C+20Fp ...
.text:0040555C
.text:0040555C arg_0           = dword ptr  4
.text:0040555C arg_4           = dword ptr  8
.text:0040555C
.text:0040555C                 push    ebx
.text:0040555D                 push    esi
.text:0040555E                 mov     esi, [esp+8+arg_0]
.text:00405562                 push    edi
.text:00405563                 mov     ebx, ecx
.text:00405565                 push    esi
.text:00405566                 call    sub_40550A
.text:0040556B                 mov     edi, [esp+0Ch+arg_4]
.text:0040556F
.text:0040556F loc_40556F:                             ; CODE XREF: sub_40555C+4D↓j
.text:0040556F                 cmp     byte ptr [edi], 0
.text:00405572                 jz      short loc_4055AB
.text:00405574                 push    esi
.text:00405575                 mov     ecx, ebx
.text:00405577                 call    sub_405539
.text:0040557C                 push    esi
.text:0040557D                 mov     ecx, ebx
.text:0040557F                 call    sub_405539
.text:00405584                 push    esi
.text:00405585                 mov     ecx, ebx
.text:00405587                 call    sub_405539
.text:0040558C                 push    esi
.text:0040558D                 mov     ecx, ebx
.text:0040558F                 call    sub_405539
.text:00405594                 mov     al, [edi]
.text:00405596                 cmp     al, 61h
.text:00405598                 movsx   eax, al
.text:0040559B                 jge     short loc_4055A2
.text:0040559D                 sub     eax, 30h
.text:004055A0                 jmp     short loc_4055A5
.text:004055A2 ; ---------------------------------------------------------------------------
.text:004055A2
.text:004055A2 loc_4055A2:                             ; CODE XREF: sub_40555C+3F↑j
.text:004055A2                 sub     eax, 57h
.text:004055A5
.text:004055A5 loc_4055A5:                             ; CODE XREF: sub_40555C+44↑j
.text:004055A5                 add     [esi], ax
.text:004055A8                 inc     edi
.text:004055A9                 jmp     short loc_40556F
.text:004055AB ; ---------------------------------------------------------------------------
.text:004055AB
.text:004055AB loc_4055AB:                             ; CODE XREF: sub_40555C+16↑j
.text:004055AB                 pop     edi
.text:004055AC                 pop     esi
.text:004055AD                 pop     ebx
.text:004055AE                 retn    8
.text:004055AE sub_40555C      endp
```

WannaCry Malware (2017)

```
.text:0040261F sub_40261F      proc near               ; CODE XREF: sub_40259F+12↑p
.text:0040261F                                         ; sub_40259F+25↑p
.text:0040261F
.text:0040261F arg_0           = dword ptr  4
.text:0040261F arg_4           = dword ptr  8
.text:0040261F
.text:0040261F                 push    ebx
.text:00402620                 push    esi
.text:00402621                 mov     esi, [esp+8+arg_0]
.text:00402625                 push    edi
.text:00402626                 mov     ebx, ecx
.text:00402628                 push    esi
.text:00402629                 call    sub_4025CD
.text:0040262E                 mov     edi, [esp+0Ch+arg_4]
.text:00402632
.text:00402632 loc_402632:                             ; CODE XREF: sub_40261F+4D↓j
.text:00402632                 cmp     byte ptr [edi], 0
.text:00402635                 jz      short loc_40266E
.text:00402637                 push    esi
.text:00402638                 mov     ecx, ebx
.text:0040263A                 call    sub_4025FC
.text:0040263F                 push    esi
.text:00402640                 mov     ecx, ebx
.text:00402642                 call    sub_4025FC
.text:00402647                 push    esi
.text:00402648                 mov     ecx, ebx
.text:0040264A                 call    sub_4025FC
.text:0040264F                 push    esi
.text:00402650                 mov     ecx, ebx
.text:00402652                 call    sub_4025FC
.text:00402657                 mov     al, [edi]
.text:00402659                 cmp     al, 61h
.text:0040265B                 movsx   eax, al
.text:0040265E                 jge     short loc_402665
.text:00402660                 sub     eax, 30h
.text:00402663                 jmp     short loc_402668
.text:00402665 ; ---------------------------------------------------------------------------
.text:00402665
.text:00402665 loc_402665:                             ; CODE XREF: sub_40261F+3F↑j
.text:00402665                 sub     eax, 57h
.text:00402668
.text:00402668 loc_402668:                             ; CODE XREF: sub_40261F+44↑j
.text:00402668                 add     [esi], ax
.text:0040266B                 inc     edi
.text:0040266C                 jmp     short loc_402632
.text:0040266E ; ---------------------------------------------------------------------------
.text:0040266E
.text:0040266E loc_40266E:                             ; CODE XREF: sub_40261F+16↑j
.text:0040266E                 pop     edi
.text:0040266F                 pop     esi
.text:00402670                 pop     ebx
.text:00402671                 retn    8
.text:00402671 sub_40261F      endp
```

Same encryption computation logic

Let's do PATCH(Security Update)!

MS17-010: Security update for Windows SMB Server: March 14, 2017

Applies to: Windows Server 2016 Datacenter, Windows Server 2016 Essentials, Windows Server 2016 Standard, More

Microsoft

Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.
To learn more about the vulnerability, see Microsoft Security Bulletin MS17-010.

Microsoft Windows 공격도구 공개에 따른 주의 권고 2017.04.15

KISA KOREA INTERNET & SECURITY AGENCY

보안공지 수정 : 2017-04-17

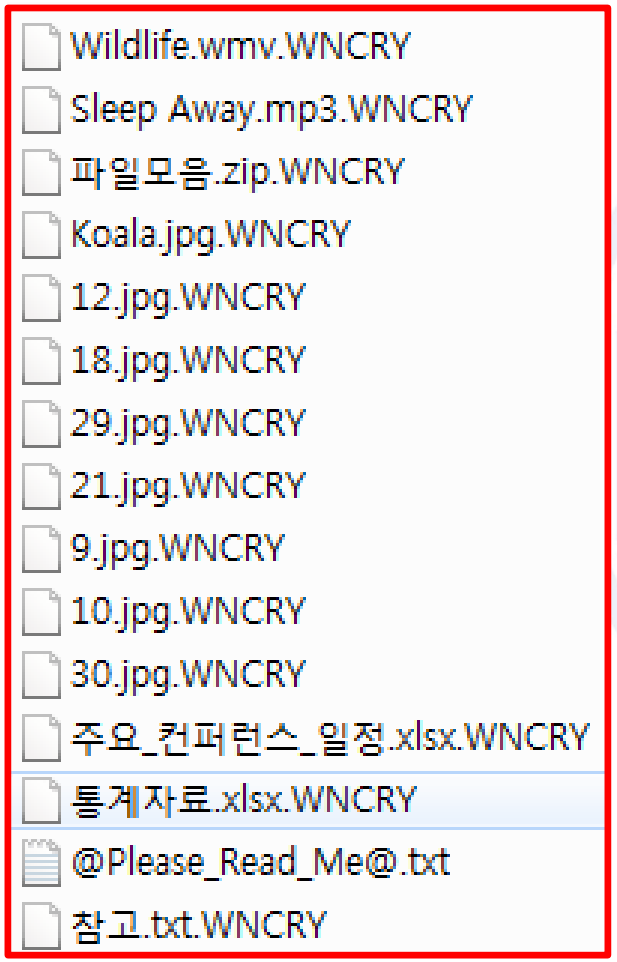
□ 개요

o Shadow Brokers(해킹그룹)이 Microsoft Windows OS Exploit 도구를 공개함에 따라 공격 가능성에 대비 주의 필요

o 공개 된 공격 도구에 사용된 취약점은 Windows 최신 버전에는 발생하지 않으므로 운영체제에 대한 최신 보안 업데이트 및 버전 업그레이드 권고

Let's do BACKUP!

All data from a South Korea's web hosting company was **encrypted** due to ransomware.



웹호스팅 '인터넷나야나' 랜섬웨어 감염…원본·백업파일 모두 암호화

이데일리

[뉴스pick] 랜섬웨어 감염된 웹호스팅 업체 "해커, 27억 원 비트코인 요구"

SBS NEWS

랜섬웨어 피해 웹호스팅 업체 '13억 내고 데이터 복구하기로'

KBS NEWS

$1.14M paid to hacker for recovery costs

Build and operate backup systems

- Establish policies for data backup management, build and operate backup system (network configuration, backup procedure, backup media, etc.)

Enhance security of backup system

- Recommendations to backup data using **external storage devices separate from the network**

Cooperate response at the national level -> Global

Building an Intelligence Network for Prevention Ransomware in South Korea

National Security Campaign for Prevention Ransomware