



랜섬웨어와 유포 실습

201411687 김교연
201215531 김형래
201411737 양준수
201311746 이찬우

목차

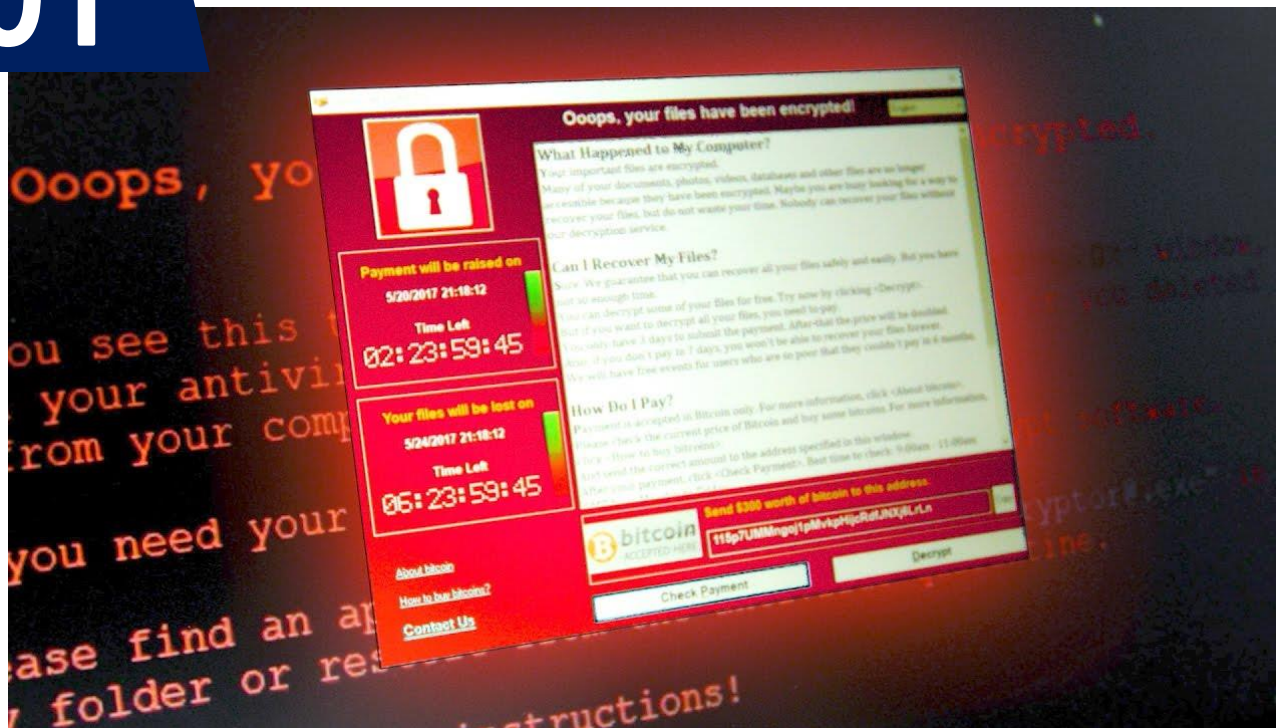


01 Ransomware?

02 랜섬웨어 구현

03 유포

04 정리



Ransomware?

a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

- Wikipedia

- 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류
- 사용자의 내부 파일을 암호화하여 금액 지불을 강요
- 최초의 랜섬웨어는 1989년 Joseph Popp이 작성한 AIDS

Dear Customer:

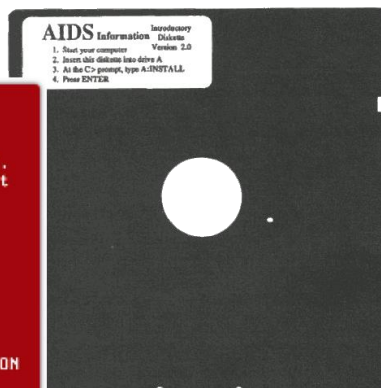
It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue



AIDS

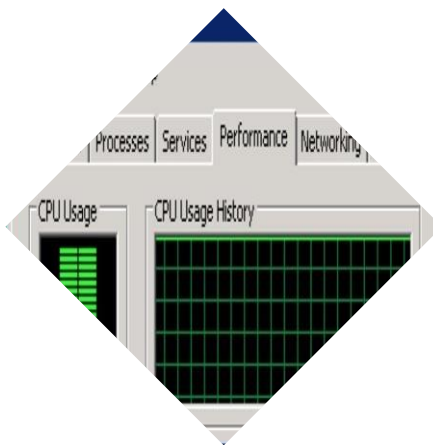
AIDS, also known as Aids Info Disk or PC Cyborg Trojan, is a trojan horse that replaces the AUTOEXEC.BAT file, which would then be used by AIDS to count the number of times the computer has booted.

- Wikipedia

- 현재 기승을 부리는 Crypto 계열의 랜섬웨어는 2005년 처음 발견됐지만 AIDS는 1989년 등장
- 플로피 디스크를 통해 시스템 감염
- AIDS.trojan은 도스의 모든 파일명을 암호화해 시스템을 사용할 수 없게 만든 후 189달러를 파나마의 우편함으로 지불하면 복호화 키가 담긴 디스크를 받을 수 있었다.



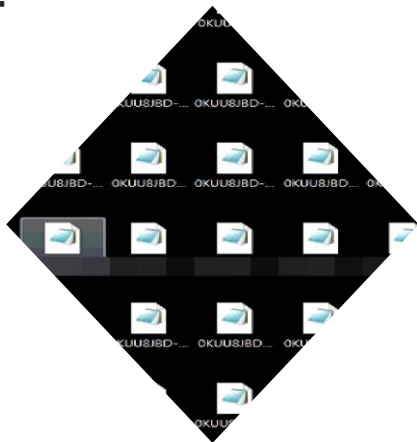
주요 시스템 파일
열기 불가



CPU와 램
사용량이 급격히
증가



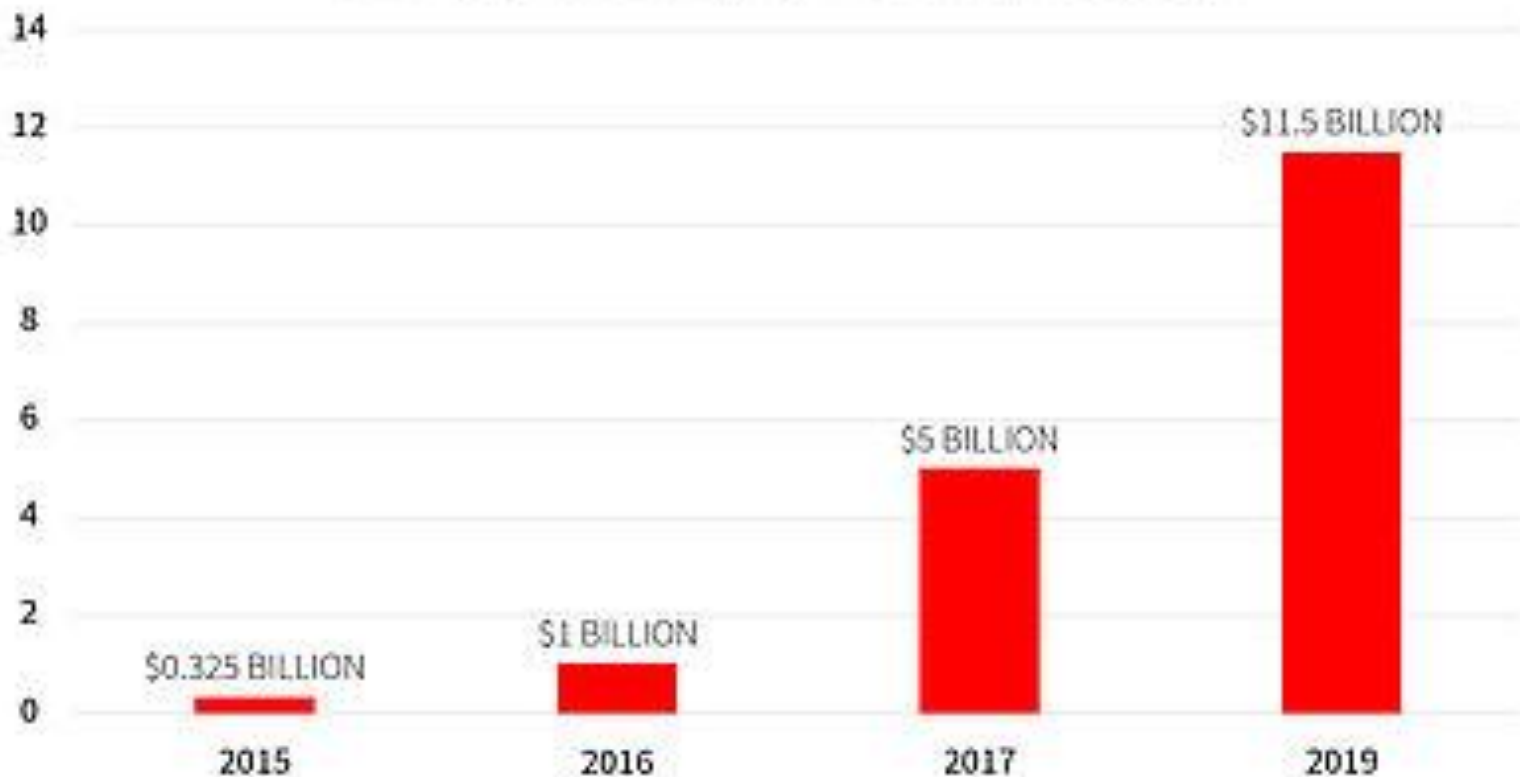
백신 프로그램 강제
종료/중지/오류
등이 지속적으로
발생



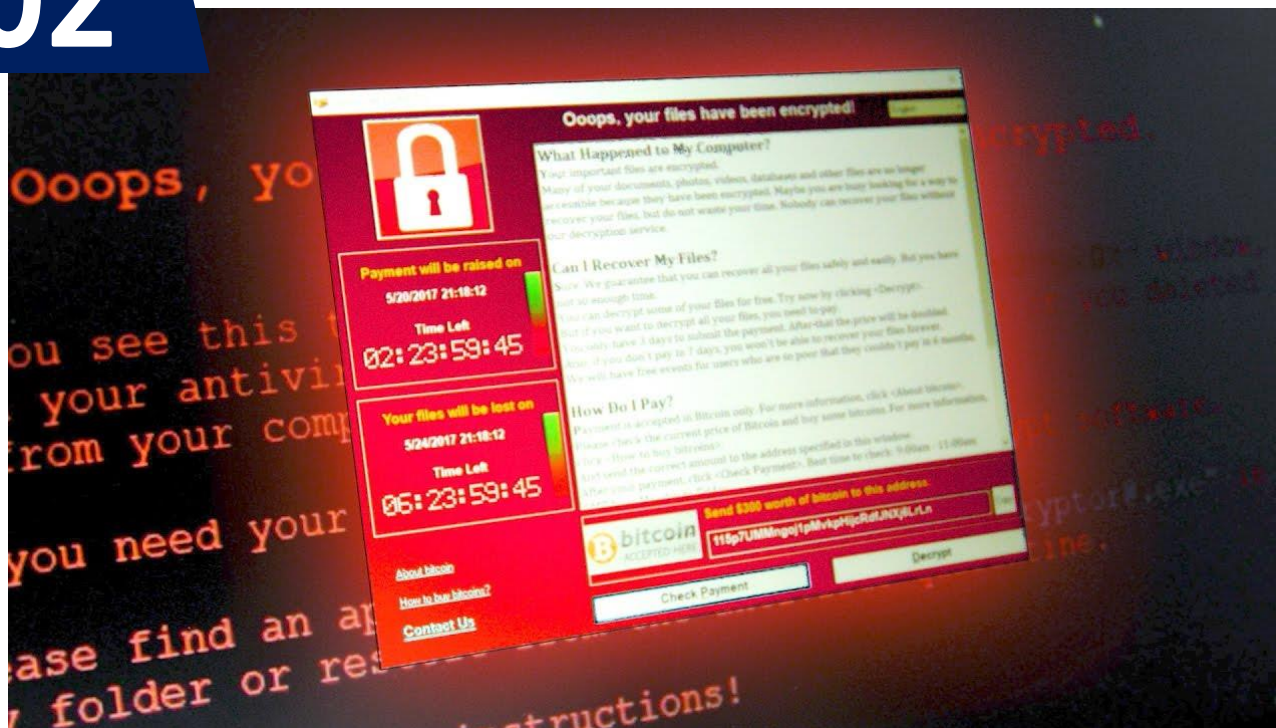
파일들의 확장자가
변경



윈도우 복원 시점
제거

RANSOMWARE: TOTAL DAMAGE COST

**2019년 현재 세계적으로 약 11.5조 달러 규모의
피해가 예상됨**

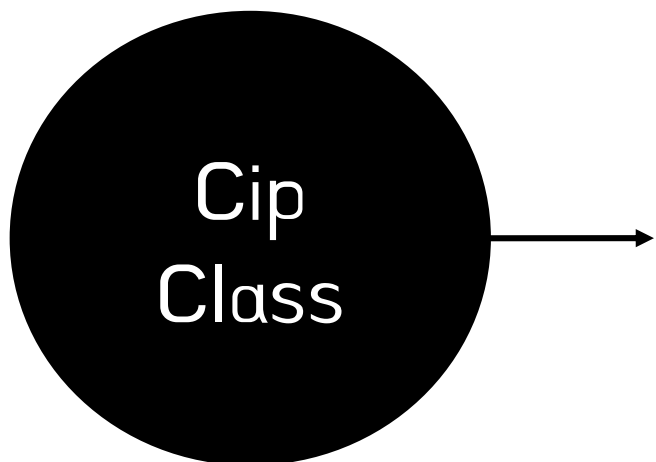


구현 (1)

랜섬웨어 감염 -> 사용자 파일
암호화 및 복호화

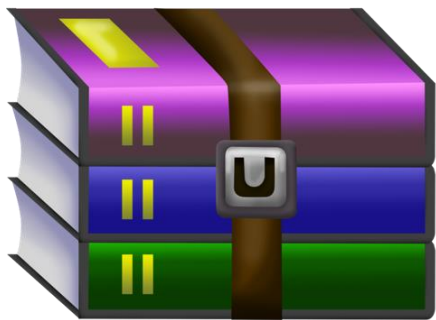
- Filesearch Class
코드 내 목록에 있는 확장자 파일 -> 암호화 및 원본 파일명 저장
(하위 디렉토리와의 그 디렉토리 파일들 찾아 리스트로 반환)
- 복호화는 아까 찾은 리스트에서 암호화된 파일 이름이 저장되어
있다면 원본으로 복호화

- 복호화 조건은 감염 컴퓨터 바탕화면에 경고 메시지가 있으면 복호화



- 키를 생성하고 리스트로 받은 파일들 암호화 시키는 클래스
- 암호화 방식은 AES/ECB
- RSA를 사용하지 않은 이유는 다량의 파일을 암호화 시키기에는 속도가 너무 느리기 때문에 상대적으로 빠른 속도의 AES 방식 차용

- 구현물은 이미지 파일로 위장되며 이미지 파일이 열릴 경우 키 생성과 동시에 감염
- exe 파일을 png 형태의 이미지 파일로 위장하는 것은 압축 프로그램 winrar의 취약점을 이용



- winrar 구버전에는 취약점이 존재하며 폴더를 압축한 후 바이너리 코드를 수정하면 exe가 정상적으로 존재하지만 png 파일 같은 이미지로 위장 가능

HxD - [C:\Users\me\Downloads\美希.zip]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(O) 창 설정(W) ?

16 ANSI 16 진수

美希.zip

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	50	4B	03	04	14	00	00	00	08	00	EF	A0	C5	4E	19	D3
00000010	0F	2A	74	40	27	00	00	36	2B	00	08	00	13	00	DA	B8
00000020	FD	F1	2E	65	78	65	75	70	0F	00	01	BF	70	F2	E9	E7
00000030	BE	8E	E5	B8	8C	2E	65	78	65	EC	3A	6D	74	14	55	96
00000040	AF	93	4E	68	20	A4	02	04	08	CA	47	83	41	50	42	E4
00000050	D3	F1	83	38	41	69	26	B0	09	76	22	8D	E1	2B	21	90
00000060	86	0E	86	04	93	0E	A2	4E	98	68	57	BB	B4	4D	39	D1
00000070	49	3C	59	65	10	34	28	E0	A0	CC	0E	20	EB	08	B6	92
00000080	11	74	64	4F	56	51	38	AE	E3	41	0D	58	21	51	23	20
00000090	46	0C	F4	DE	7B	DF	AB	EE	AA	EE	0E	F3	67	CF	FE	DA
000000A0	3A	90	AA	F7	EE	7D	F7	FB	DE	77	AB	5E	E7	2D	AE	67
000000B0	F1	8C	31	33	FC	0F	06	19	3B	C8	F8	95	CD	FE	F9	55
000000C0	07	FF	93	47	BF	99	CC	F6	F5	3D	3E	E6	A0	29	F7	F8
000000D0	98	05	AE	B2	6A	EB	BA	AA	CA	D5	55	25	6B	AD	2B	4B
000000E0	2A	2A	2A	DD	D6	15	4E	6B	55	4D	85	B5	AC	C2	3A	FB
000000F0	DE	FB	AC	6B	2B	4B	9D	99	03	06	F4	4B	17	34	EC	36
00000100	C6	72	4D	7D	D8	B7	07	ED	73	34	BA	A7	59	72	5C	7F
00000110	53	DC	6D	E9	73	12	19	FB	0C	FE	CF	03	79	06	01	20
00000120	05	FE	2F	4F	E4	D2	E1	73	1C	97	DB	24	E4	C7	6B	CB
00000130	DB	13	69	B0	E2	D6	3E	08	86	CB	CA	71	F1	4F	0A	DE
00000140	C5	AD	35	91	9D	C2	85	A7	13	59	AB	04	F7	2E	A0	BB
00000150	2D	9D	45	5D	F5	13	D9	96	5B	D8	FF	FA	95	E9	76	6E
00000160	70	C3	9D	74	44	81	72	12	49	6E	FD	B5	1C	FE	65	96
00000170	96	B8	4B	E0	D9	3D	48	E8	9E	0A	F7	DC	C4	30	12	B7
00000180	46	20	73	45	75	35	3E	77	CD	45	C7	24	B2	58	57	1D
00000190	E2	39	39	C1	53	26	6E	03	32	D2	F2	28	FC	40	66	19
000001A0	C7	23	DB	9C	16	32	AE	88	C1	B7	AA	BA	6A	25	63	DC
000001B0	76	68	C3	06	B8	57	C5	C2	73	96	57	AE	64	DC	96	60
000001C0	53	36	19	EE	89	13	A3	F8	B2	FF	BF	FE	4F	2F	87	EF
000001D0	8C	A7	73	C2	D1	D9	E9	66	F3	F2	39	4C	B1	F5	F8	66
000001E0	A7	A7	6C	3F	0D	CF	47	6D	3D	88	70	D4	9C	CE	60	04
000001F0	DC	49	8A	AD	1B	6E	16	35	A7	2D	9E	F9	3A	97	1D	51
00000200	DD	37	F2	F5	96	ED	5D	80	E2	0D	B8	EF	7F	89	95	CC
00000210	61	DB	B3	DB	70	54	B3	D8	D3	7D	DA	3D	D6	13	B0	FA
00000220	CE	E9	EA	85	AF	E3	99	7F	08	E2	C1	C8	B7	20	DD	AC
00000230	FE	F0	75	3C	47	F5	74	07	DC	23	3D	81	6C	44	FB	30

오프셋: 2740E3

랜섬웨어를 헥스
에디터로 오픈한 모습

eclipse-workspace - Ransomware/src/newRansom/Main.java - Eclipse IDE

File Edit Source Refactor Navigate Search Project Run Window Help

Package Explorer

- Ransomware
 - src
 - newRansom
 - Cip.java
 - CipInterface.java
 - FileSearch.java
 - Main.java
 - img
 - Referenced Libraries

FileSearch.java

```

103     }
104     // System.out
105     return true
106 }
107 catch (Exception e) {
108     {
109         return
110     }
111 }
112 }
113
114 public static
115 try {
116     Array

```

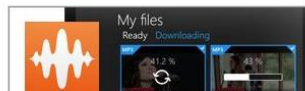
개발한 랜섬웨어
클래스 구조



신뢰할 수 없는
사이트

Möchtest du YouTube zu mp3 kopieren?

Benötigst du Lieder für dein Gerät? Der beste YouTube-zu-MP3-Konverter im ganzen Netz steht dir hier zu Diensten! Mit "free" meinen wir wirklich kostenlos: Ohne einen einzigen Cent dafür zu



스팸 메일





SNS

광고 배너



torrent Client

	Name	% Done	Size	Downloaded	Dc
<input type="checkbox"/>	ubuntu-18.10-desktop-amd64.iso	<div></div>	1.86 GB	1.88 GB	0 b
	Koinonein-BitTorrent-Client-4.5....	<div></div>	9.11 MB	0 bytes	0 b
	Koinonein-BitTorrent-Client-4.4....	<div></div>	9.10 MB	0 bytes	0 b
	Koinonein-BitTorrent-Client-4.3....	<div></div>	9.06 MB	0 bytes	0 b
	Koinonein-BitTorrent-Client-4.2....	<div></div>	9.05 MB	9.05 MB	0 b
	Koinonein-BitTorrent-Client-4.1....	<div></div>	9.05 MB	0 bytes	0 b
	Koinonein-BitTorrent-Client-4.0....	<div></div>	9.03 MB	0 bytes	0 b
	gimp-2.10.8-setup-2.exe	<div></div>	194 MB	197 MB	0 b

gimp-2.10.8-setup-2.exe

y mktorrent 1.0

n 2018-11-16 14:34:22

GIMP 2.10.8 Installer for Microsoft Windows - 32 and 64 Bit

P2P



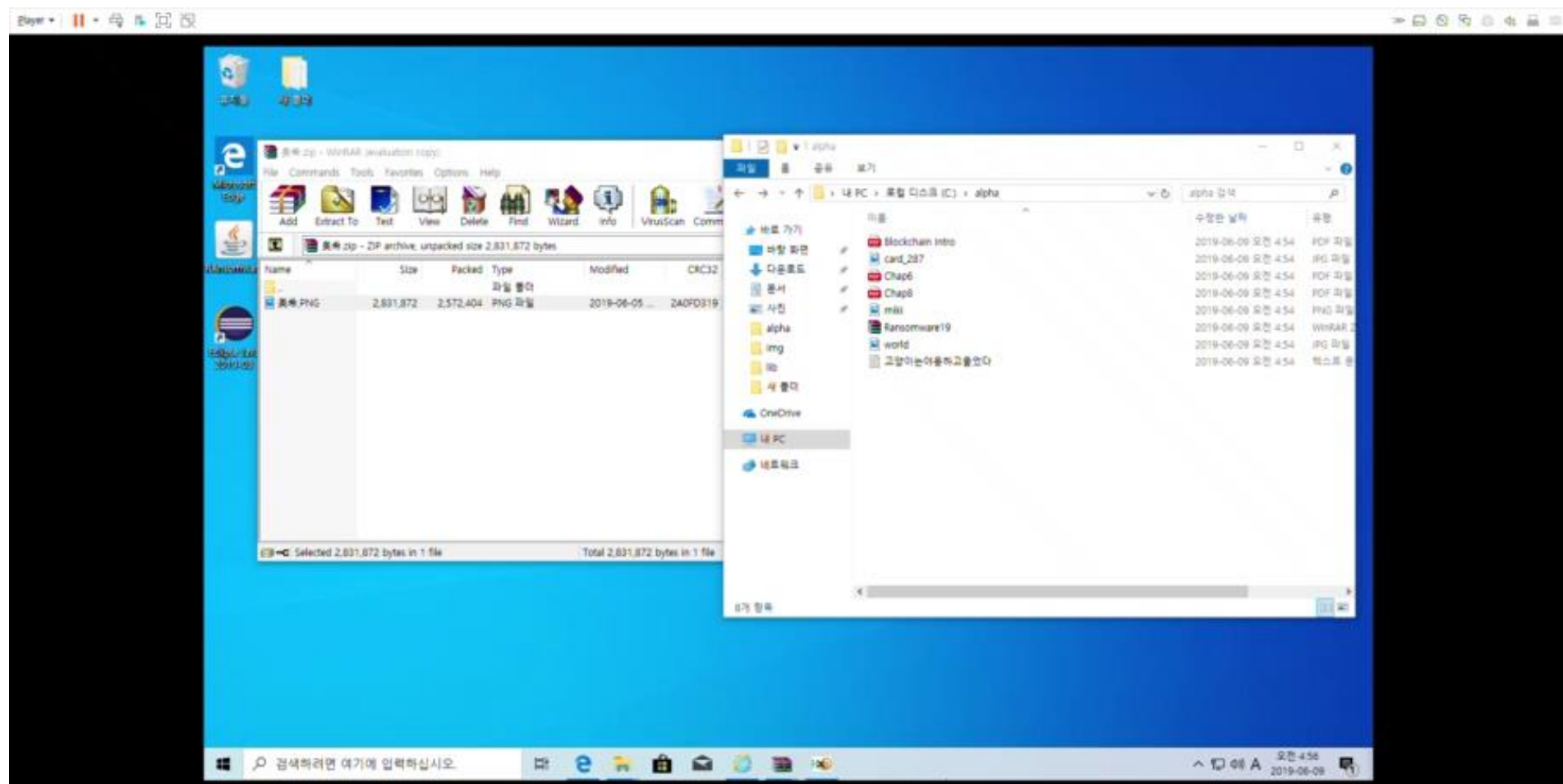
exe를 PNG 이미지
파일로 위장

사용자에게 보여질
위장된 파일의 이미지



03

실제 구현물의 동작



Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Install Tools

Remind Me Later

Never Remind Me



- 악의적으로 유포되는 악성코드들은 프로그램 업데이트만 주기적으로 해도 대개 감염되는 것을 예방할 수 있다.
- 용도에 따라 암호화 방식별로 다른 속도 차이를 고려해야 한다.
- 악성코드 자체의 개발은 의외로 어렵지 않으며 유포가 관건이다.



감사합니다