ISBN : 000-00-000-0000-0

클리앙 웹페이지 접근으로 인한 랜섬웨어 분석 보고서

2015년

한국과학기술정보연구원
과학기술사이버안전센터

랜섬웨어 / 난 너의 인질을 잡고 있다 ..!!

"…유일한 방법은 저희한테 지불하는 방법입니다. 만약 그렇지 않으면…"

다짜고짜 몸값을 요구하는 인질범…. 범인이 잡고 있는 인질은 컴퓨터 파일?

최근 국내에서 화제가 된 이 인질범은 '랜섬웨어(ransomware)'입니다. 몸값(ransom)과 악성코드(malware)의 합성어. 사용자의 파일을 '인질'로 삼고 협박하는 악성코드입니다.

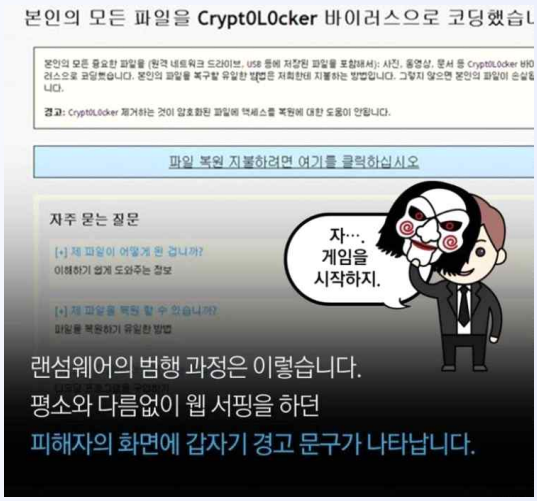
랜섬웨어의 범행 과정은 이렇습니다. 평소와 다름없이 웹 서핑을 하던 피해자 화면에 '모든 파일이 암호화됐으니, 이를 풀려면 돈을 지불하라'는 경고 문구가 나타납니다. 대부분 파일이 자신도 모르게 암호화 돼있는 것을 본 피해자는 '멘붕'에 빠지게 됩니다. 각종 문서뿐 아니라 그림, 압축 파일 등 죄다 암호가 걸려있기 때문에 손을 쓸 수가 없습니다. 결국 피해자는 울며 겨자 먹기로 돈을 지불하고 파일을 복구할 수 밖에 없습니다. 단순히 컴퓨터를 망가뜨리는게 아니라 직접 돈까지 요구하는 황당한 악성코드.

랜섬웨어는 이미 수년 전부터 외국에서 악명높았습니다. 전세계 피해액만 약 3,700억 원에 달합니다. 국내에는 '15. 4월 '클리앙'의 광고 사이트 서버가 해킹되면서 퍼지기 시작했습니다. 최근까지 피해가 급속도로 증가하고 있습니다.

하지만 아직 확실한 방법이 없습니다. 워낙 변종이 많아 백신 프로그램만으로 이 악성코드를 막는 건 불가능합니다. 인터넷 화폐인 '비트코인'으로 돈을 지불하도록 하기 때문에 유포자를 추적하는 것도 쉽지 않습니다.

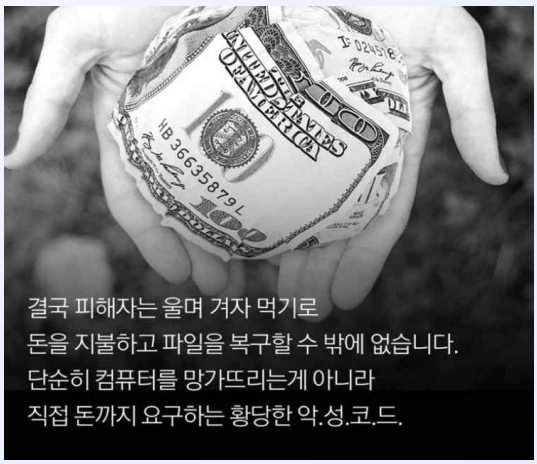
랜섬웨어는 이메일 · 메신저 · 웹사이트가 주요 경로입니다. 파일을 다운로드 할 때 주의하고, 꾸준히 컴퓨터를 업데이트하는 것이 유일한 예방법입니다. 언제 · 어디서 당신의 컴퓨터를 노리고 있을지 모르는 랜섬웨어는 중요한 자료와 소중한 추억이 '인질'로 잡히지 않도록 조심하길 바랍니다.

최근 국내에서 화제가 된 이 인질범은
'랜섬웨어(ransomware)'입니다.
몸값(ransom)과 악성코드(malware)의 합성어.
사용자의 파일을 '인질'로 삼고
협박하는 악성코드입니다.



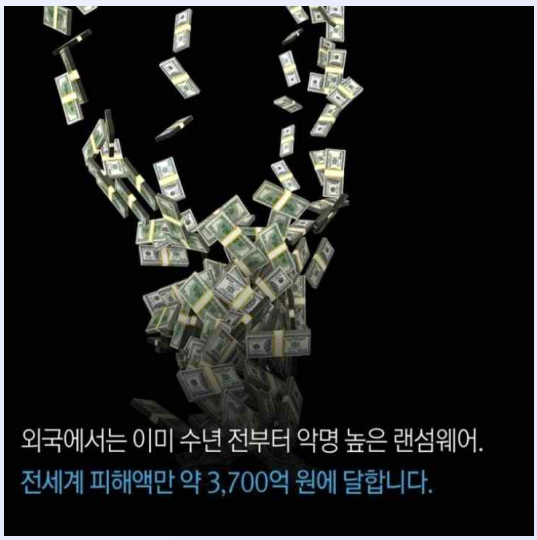
랜섬웨어의 범행 과정은 이렇습니다.
평소와 다름없이 웹 서핑을 하던
피해자의 화면에 갑자기 경고 문구가 나타납니다.

대부분 파일이 자신도 모르게 암호화 돼있는 것을
본 피해자는 '멘붕'에 빠지게 됩니다.
각종 문서뿐 아니라 그림, 압축 파일 등 죄다
암호가 걸려있기 때문에 손을 쓸 수가 없습니다.

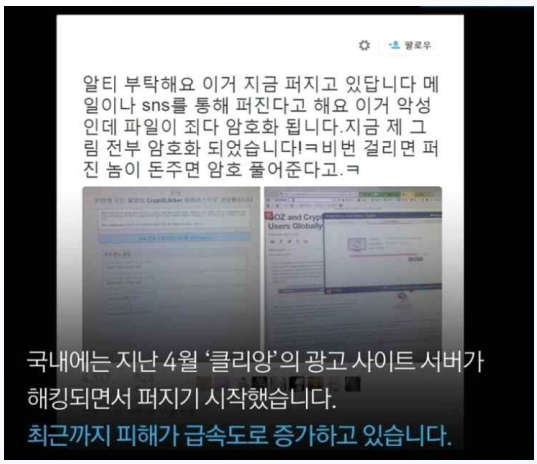


결국 피해자는 울며 겨자 먹기로
돈을 지불하고 파일을 복구할 수 밖에 없습니다.
단순히 컴퓨터를 망가뜨리는게 아니라
직접 돈까지 요구하는 황당한 악.성.코.드.

심지어 제한 시간을 제시하며 피해자를 압박하거나
스마트폰까지 감염시키는 경우도 있습니다.



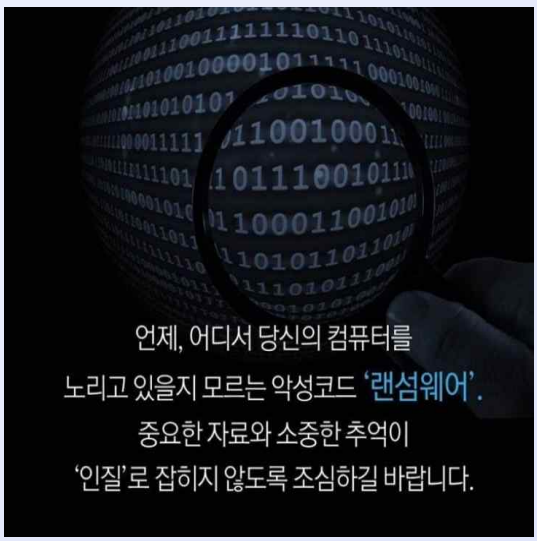
외국에서는 이미 수년 전부터 악명 높은 랜섬웨어.
전세계 피해액만 약 3,700억 원에 달합니다.


팔로우
알티 부탁해요 이거 지금 퍼지고 있답니다 메일이나 sns를 통해 퍼진다고 해요 이거 악성인데 파일이 죄다 암호화 됩니다.지금 제 그림 전부 암호화 되었습니다ㅋㅋ비번 걸리면 퍼진 놈이 돈주면 암호 풀어준다고.ㅋ
국내에는 지난 4월 '클리앙'의 광고 사이트 서버가 해킹되면서 퍼지기 시작했습니다.
최근까지 피해가 급속도로 증가하고 있습니다.


NsbLocker
Cryptolocker
Cryptowall
Bitcrpt
Mycomego
.
.
.
하지만 아직 확실한 방법이 없습니다.
워낙 변종이 많아 백신 프로그램만으로
이 악성코드를 막는 건 불가능합니다.


bitcoin
인터넷 화폐인 '비트코인'으로 돈을 지불하도록
하기 때문에 유포자를 추적하는 것도 쉽지 않습니다.


MacBook Air
랜섬웨어는 이메일, 메신저, 웹사이트가 주요
경로입니다. 파일을 다운로드 할 때 주의하고, 꾸준히
컴퓨터를 업데이트하는 것이 유일한 예방법입니다.


언제, 어디서 당신의 컴퓨터를
노리고 있을지 모르는 악성코드 '랜섬웨어'.
중요한 자료와 소중한 추억이
'인질'로 잡히지 않도록 조심하길 바랍니다.

1. 개요

○ ’15. 4. 21. 01시38분 ~ 11시12분까지 커뮤니티 사이트*에서 **랜섬웨어 악성코드가 최초로 배포**되기 시작

* 커뮤니티 사이트 : 클리앙/www.clien.net

- 해커는 임의의 방법을 통해 광고서버의 **관리자계정을 획득**하여 악성코드를 삽입한 후 유포하는 경로를 채택

- 랜섬웨어 **크립토락커**는 사용자 PC를 감염시켜 중요 파일을 암호화 하여 암호를 해제하는 조건으로 금전을 요구

- 하지만, 랜섬웨어는 피해를 당한 사용자가 금전적 요구를 이행하더라도 복호화가 보장되지 않는 등 사용자 주의가 필요

※ 참고 사이트 : http://hummingbird.tistory.com/5880
http://www.clien.net/cs2/bbs/board.php?bo_table=park&wr_id=37308524

2. 랜섬웨어 증상 및 상세 분석

가. 램섬웨어 증상 및 대처방법

’15년부터 랜섬웨어가 대량으로 출몰하기 시작하였으며, ’13년까지 유행하던 유형은 화면을 잠그고 사용자들의 불편을 초래하거나 불안감을 조성하여 금전을 요구하는 방식이었다.

피해자들은 보통 성인사이트에 접속하거나 불법 소프트웨어를 다운로드 할 때 감염이 되는데 **루마니아에서 성인사이트에 접속했다가 경찰 랜섬웨어에 감염된 피해자가 벌금을 요구하는 화면에 자살하는 사건이 발생**하면서 국내에도 많이 알려졌다.

초기의 랜섬웨어는 유럽/북미 등에서 많은 사용자들에게 피해가 발생했으며, MS社의 보안패치 및 안전모드로 부팅하는 등의 대응법이 계속하여 발전하자 **’13년 중요 문서들을 암호화시키는 ’CryptolLocker’가 출현**하게 되었다.

과거 ‘GPCode’나 일부 랜섬웨어도 CryptoLocker 이전에 문서 암호화를 시도했으나 버전업이 느렸고 백신들이 빠르게 대처해 피해 규모도 적었으며 복호화도 가능한 수준이였다.

하지만, CryptoLocker 경우는 RSA-2048 등의 암호화를 사용하여 공격자가 아니면 암호를 해제하기 힘들게 제작되어 많은 피해가 발생하였고, 국내에서도 스팸메일 등으로 유입되어 피해가 발생하기 시작하였다.

랜섬웨어가 국내에 널리 알려지게 된 계기는 ’15. 4·21 국내 대형 커뮤니티 사이트(클리앙)에서 한글로 제작된 랜섬웨어가 유포되면서 부터이며, 기존 방식과(※ 스팸메일를 통한 유포)달리 드라이브 바이 다운로드 기법을 이용하였다. 보안패치가 되지 않은 사용자가 PC에서 감염된 웹 사이트에 접속하면 즉시 감염되기 때문에 매우 위험하다. 최근에는 Critroni, CoinVault 등의 랜섬웨어가 연이어 등장하고 있어 항상 사용자 주의가 요구되고 있다.

화면 잠금형 랜섬웨어

화면 잠금형 랜섬웨어에 감염될 경우 바탕화면 전체를 사용 불가능 상태로 만들고 금전을 요구하는데, 이러한 랜섬웨어의 경우 안전모드로 부팅하여 백신 등으로 치료하거나 윈도우 시스템 복원을 통해 이전으로 되돌릴 수 있다.

암호화형 랜섬웨어

파일 암호화형 랜섬웨어에 감염될 경우 사용자 파일이 암호화 된 사실을 그림 파일이나 TXT · HTML 파일 등으로 알려준다. 화면 잠금형 랜섬웨어와 다르게 시스템을 사용할 수 있으나 각종 문서 파일이나 개발 소스, 데이터베이스 등 중요한 사용자 파일을 암호화 시키므로 정상적으로 실행되지 않는다.

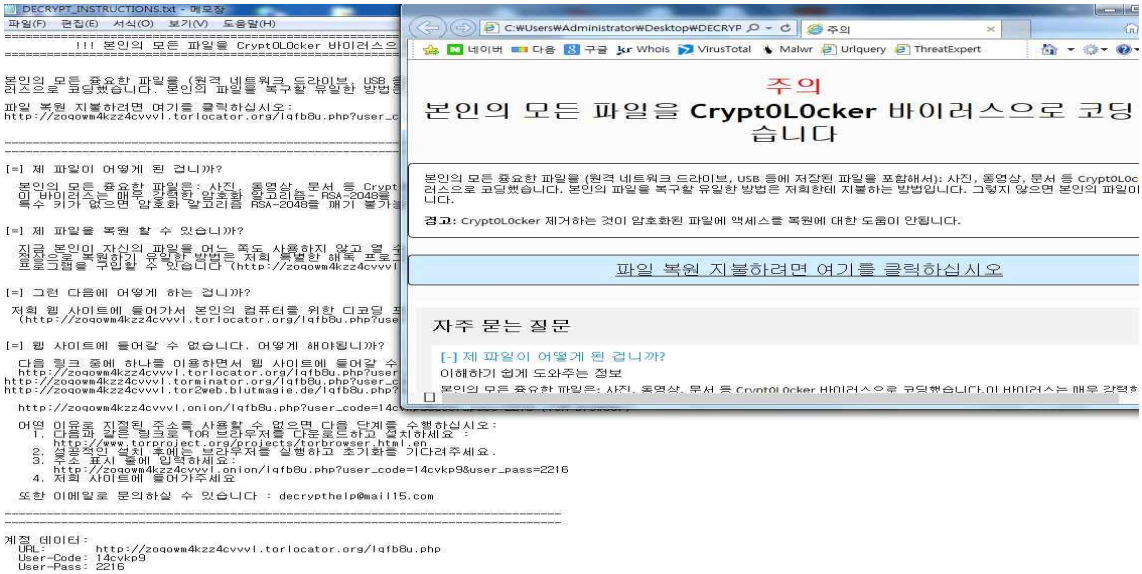
랜섬웨어 감염 시 대처 방법

최근 랜섬에어는 네트워크 공유폴더를 통해 전파되므로 감염 증상(파일 암호화형 랜섬웨어의 경우 감염 동작과정에 드라이브 전체를 탐색하여 파일을 암호화 시키므로 시스템이 느려지거나 하드디스크 램프가 빠른 속도로 깜빡임)이 나타나면 신속히 랜선을 분리하고 다른 시스템에 감염되는 것을 방지해야 한다.

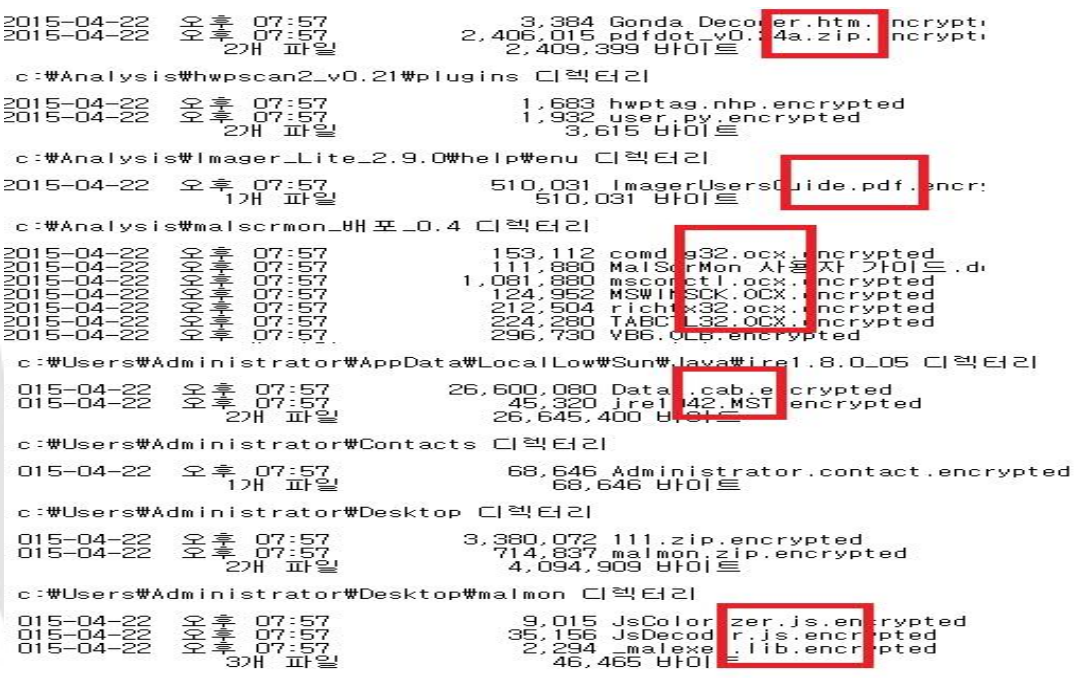
그러나, 이러한 증상이 랜섬웨어 감염이라고 단정지을 수 없으므로 일부 파일을 복구하고자 강제로 전원을 내린다면 오히려 시스템이 파괴될 수 있으니 주의해야 한다. 랜섬웨어에 감염되었다면 디스크를 포맷한 후 백업된 데이터를 복구하여 사용하는데, 만약 백업된 데이터가 존재하지 않더라도 가급적 비용을 지불하면서 복구는 하지 않는 것이 추가적인 피해를 막을 수 있다.

나. 상세분석

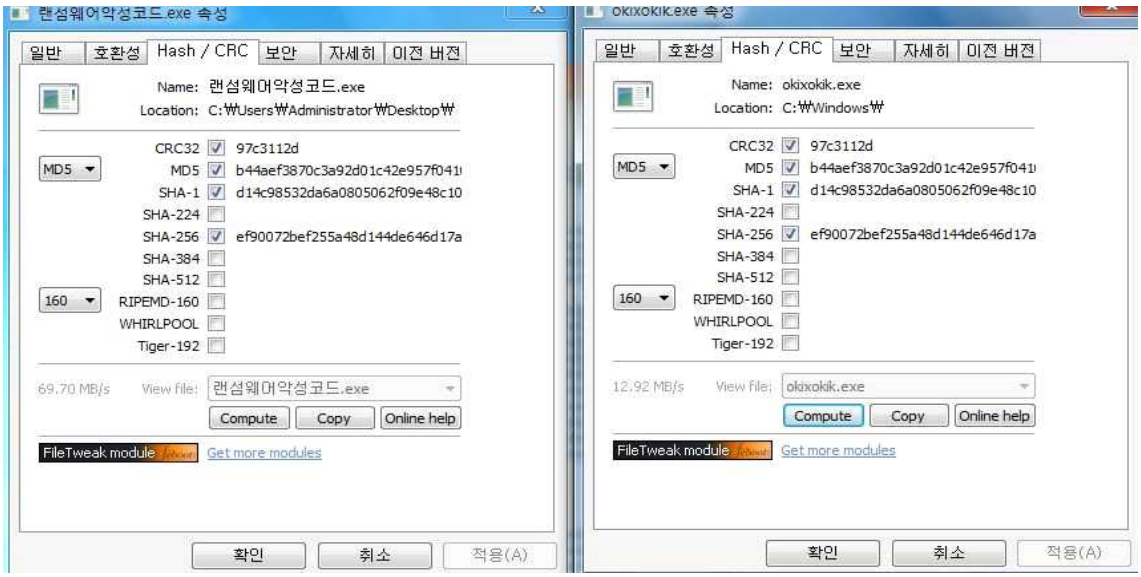
○ 랜선웨어 악성코드에 감염되면 <아래>와 같은 팝업창이 생성되며 경고 피해자에게 경고 메시지를 전송



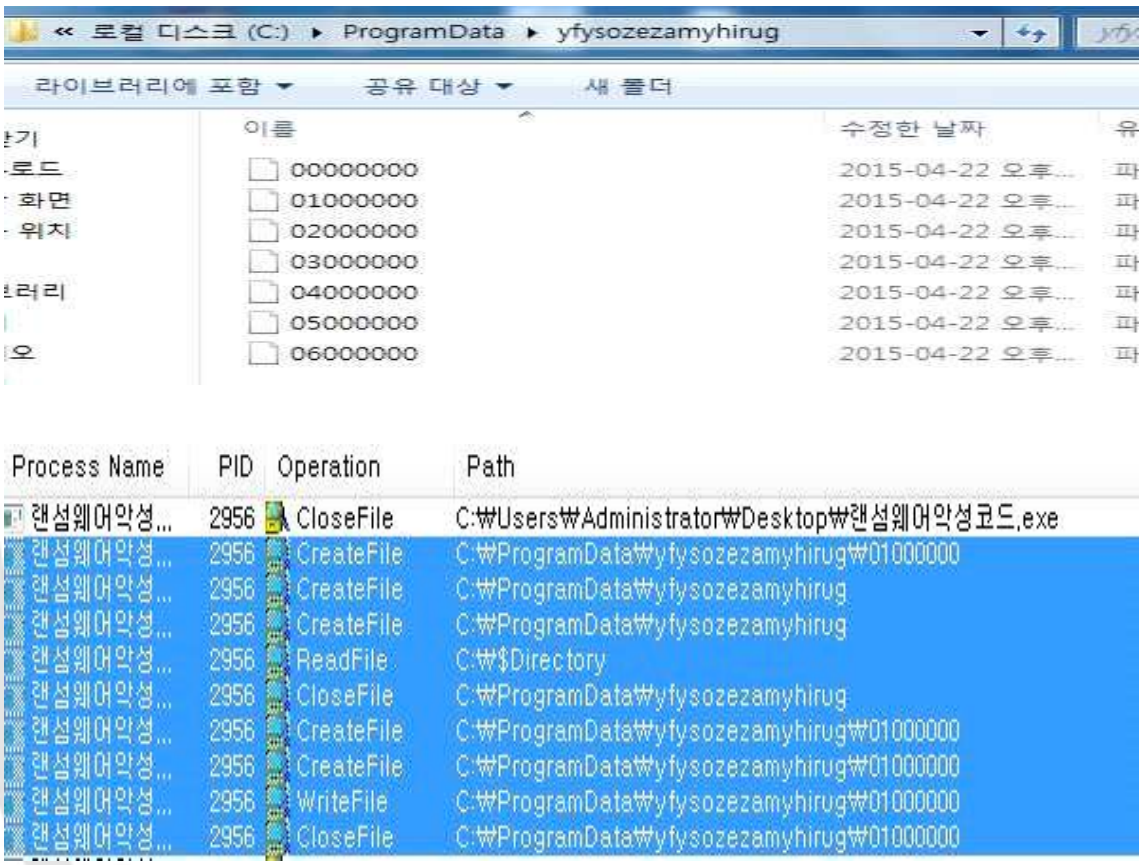
○ 악성코드 감염 시 htm, zop, pdf, ocx, jx, hwp, xlsx 등 파일이 암화되는 현상이 발생



○ 악성코드 실행 시 **윈도우 폴더에 랜덤파일명.exe 악성코드를 복사**

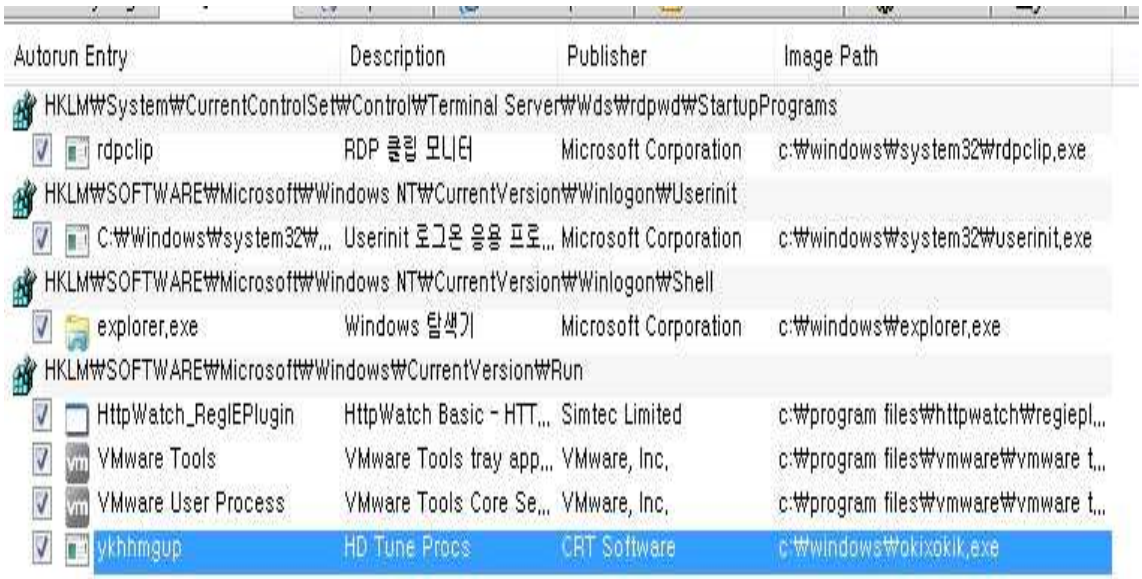


○ **ProgramData \ 랜덤 폴더명 \ 랜덤파일 생성 : 파일은 암호화되어 분석 불가**



○ 악성코드 실행

- 윈도우 시작 시 악성코드 동작



Autorun Entry	Description	Publisher	Image Path
HKLM₩System₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd₩StartupPrograms			
rdpclip	RDP 클립 모니터	Microsoft Corporation	c:₩windows₩system32₩rdpclip.exe
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit			
C:₩Windows₩system32₩...	Userinit 로그온 응용 프로...	Microsoft Corporation	c:₩windows₩system32₩userinit.exe
HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Shell			
explorer.exe	Windows 탐색기	Microsoft Corporation	c:₩windows₩explorer.exe
HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run			
HttpWatch_RegIEPlugin	HttpWatch Basic - HTT...	Simtec Limited	c:₩program files₩httpwatch₩regiepl...
VMware Tools	VMware Tools tray app...	VMware, Inc.	c:₩program files₩vmware₩vmware t...
VMware User Process	VMware Tools Core Se...	VMware, Inc.	c:₩program files₩vmware₩vmware t...
ykhhmgup	HD Tune Procs	CRT Software	c:₩windows₩okixokik.exe

- 악성코드 최초 통신 IP(62.173.145.212)는 TLS 통신으로 상세 패킷분석 어려움

	Destination	Protocol	Length	Info
.238.130	62.173.145.212	TCP	66	49162 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1
.145.212	192.168.238.130	TCP	60	https > 49162 [SYN, ACK] Seq=0 Ack=1 Win=64240
.238.130	62.173.145.212	TCP	54	49162 > https [ACK] Seq=1 Ack=1 Win=64240 Len=
.238.130	62.173.145.212	TLSv1	178	Client Hello
.145.212	192.168.238.130	TCP	60	https > 49162 [ACK] Seq=1 Ack=125 Win=64240 Le
.145.212	192.168.238.130	TLSv1	1023	Server Hello, Certificate, Server Hello Done
.238.130	62.173.145.212	TLSv1	380	Client Key Exchange, Change Cipher Spec, Encry
.145.212	192.168.238.130	TCP	60	https > 49162 [ACK] Seq=970 Ack=451 Win=64240
.145.212	192.168.238.130	TLSv1	113	Change Cipher Spec, Encrypted Handshake Messag
.145.212	192.168.238.130	TLSv1	113	[TCP Retransmission] Change Cipher Spec, Encry
.238.130	62.173.145.212	TCP	54	49162 > https [ACK] Seq=451 Ack=1029 Win=6321
.238.130	62.173.145.212	TLSv1	331	Application Data
.145.212	192.168.238.130	TCP	60	https > 49162 [ACK] Seq=1029 Ack=728 Win=64240
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]
.145.212	192.168.238.130	TCP	886	[TCP segment of a reassembled PDU]
.238.130	62.173.145.212	TCP	54	49162 > https [ACK] Seq=728 Ack=4781 Win=64240
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]
.145.212	192.168.238.130	TCP	682	[TCP segment of a reassembled PDU]
.238.130	62.173.145.212	TCP	54	49162 > https [ACK] Seq=728 Ack=8329 Win=64240
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]
.145.212	192.168.238.130	TCP	1514	[TCP segment of a reassembled PDU]

○ 참고 사이트 : http://hummingbird.tistory.com/5880

3. 분석 결과

○ 랜섬웨어 악성코드 감염 경로

- '15. 4. 21. 01시 38분 ~ 11시12분 까지 커뮤니티 사이트(클리앙 : www.clien.net)에 접속한 경우 (※ 윈도우, 자바, IE, Flash Old 버전 사용 시)

  ⇒ 주로 국내 사용자를 대상으로 제작

○ **피해 증상**

- 랜섬웨어 감염 시 문서 파일(xlsx, hwp, ppt), 그림파일(jpg) 파일 등을 암호화 하여 실행 불가능하게 함
- 암호화된 파일은 개인키가 있어야 복구 가능한 구조로 되어있어 현실적으로 파일 복구가 불가능

4. 조치 방안

○ 기관에서 운영하는 **침입방지시스템(IPS)에 <아래>와 같은 탐지·차단 정책**을 추가 적용하여 운영

```
drop tcp any any <> any any (content:"|30 82 01 0a 02 82 01 01 00 9b
19 8a 6f 43 2c a1 d6 99 02 e9 b4 75 c1 90 e4 02 bf 4b 5e e4 ae b6
15 fa 8c a7 6a e7 b0 c5 b7 a3 c1 a8 61 65 dd 50 ec ab 3b e9 be 2f
a4 d3 98 20 46 48 14 34 32 97 b0 9f 53 50 76 d5 f8 1b 8e 7e 40 b2
39 4f 83 b0 0f f3 6d 9c a2 a8 f6 1f 71 8a bd 61 77 6d 34 a2 d7 b2 3
6 a6 2e c9 c9 28 5f a0 36 be aa 4b 3c e8 e9 72 3f 88 65 83 bf 13 b3
25 c5 d2 27 f3 1c 08 f6 f0 70 4d 2d a8 c4 e1 a6 c8 5d 56 a0 28 1b 0
a 3c 63 ed ce b9 2a 12 fe d5 05 89 c9 80 27 a7 b6 09 96 63 90 c6 6
0 74 f5 be dc 98 99 8e e1 fb 10 d1 29 27 56 18 90 bc bc f8 48 64 65
9f 4d 51 48 dc 22 37 a2 48 2d 5b 76 b7 de cd b4 08 38 92 79 93 26
75 e5 c5 01 c5 a4 ed 72 ea 0c 80 5e b9 07 61 08 6a 05 fe fd 23 a0
a2 32 2a 8d e5 51 06 30 9c c9 32 08 84 3f ce 7e 42 84 80 35 31 24
47 0f 8e 34 c5 86 1c 2b 52 02 e3 02 03 01 00 01|"; nocase;)
```

○ 백신 최신 버전 업데이트 및 주기적인 정밀검사 권고

○ 윈도우, IE, 자바, Adobe 제품 등 최신 버전으로 업데이트 권고

○ 감염 PC 포맷 및 업무상 관계없는 사이트 접근 자제 권고