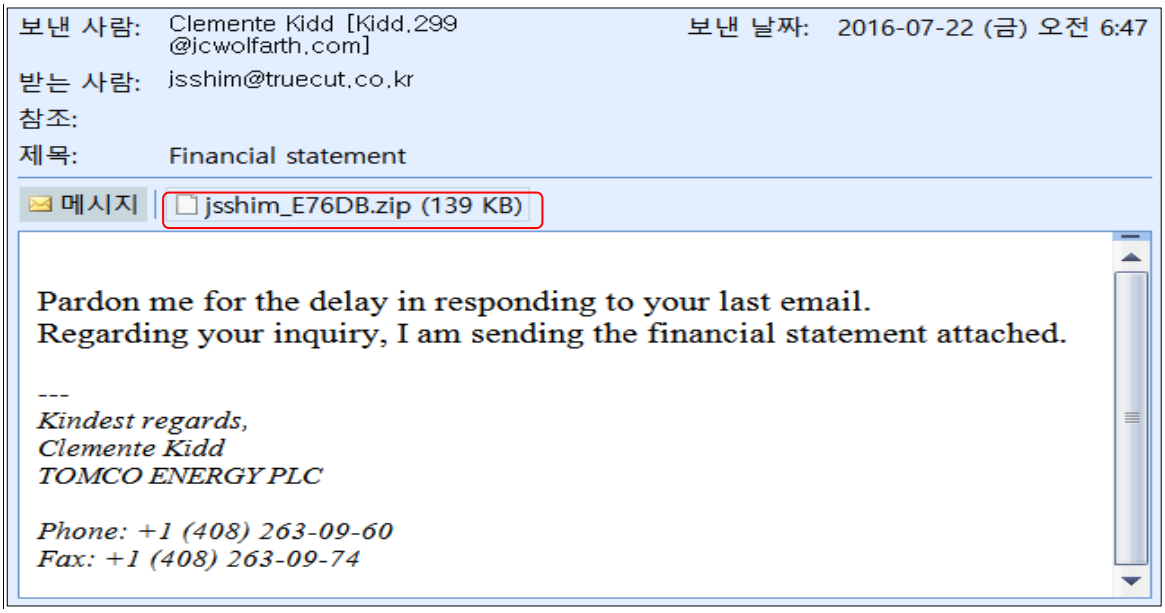
Today's Ransomware

Jul. 22, 2016

1. Today, I'm rich. I've received four ransomware.

- **jsshim_E76DB.zip => INV000 5cbd.js**
- **jsshim_2161.zip => AT00065AA.wsf**
- **jsshim_1BB2C.zip => INV000 701.js**
- **4B73B_jsshim.zip => INV000 7cb2.js**

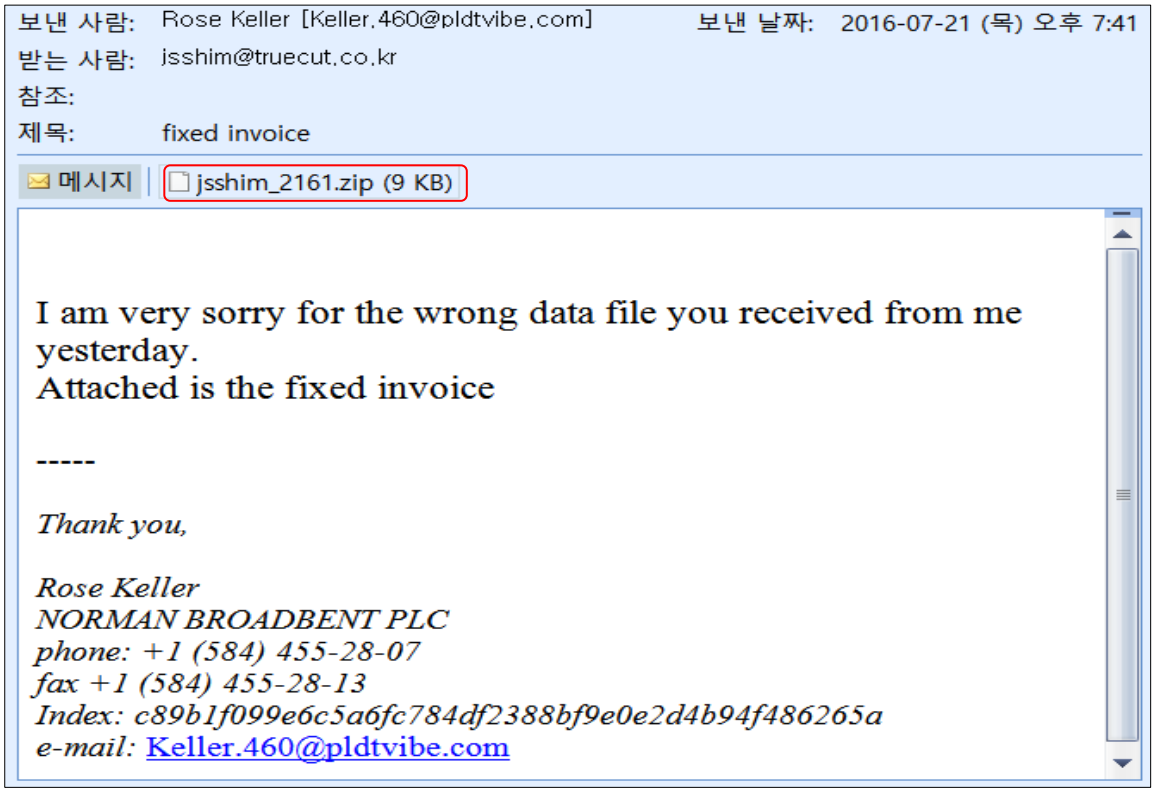


보낸 사람: Clemente Kidd [Kidd.299@jcwolfarth.com]
보낸 날짜: 2016-07-22 (금) 오전 6:47
받는 사람: jsshim@truecut.co.kr
참조:
제목: Financial statement
메시지 | jsshim_E76DB.zip (139 KB)

Pardon me for the delay in responding to your last email.
Regarding your inquiry, I am sending the financial statement attached.

Kindest regards,
Clemente Kidd
TOMCO ENERGY PLC

Phone: +1 (408) 263-09-60
Fax: +1 (408) 263-09-74

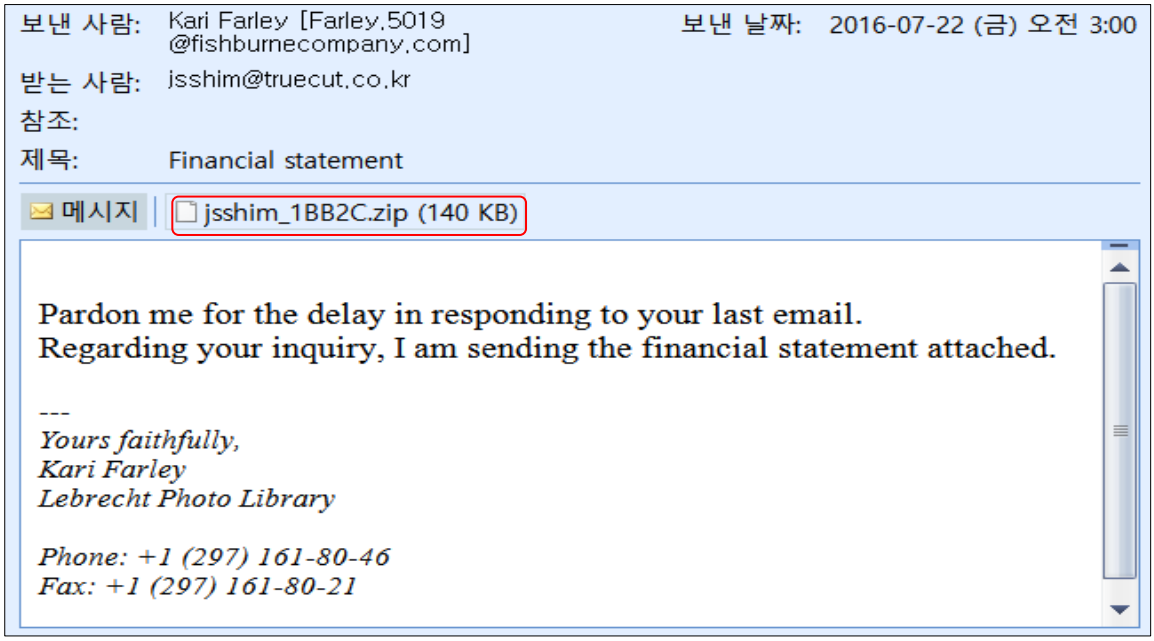


보낸 사람: Rose Keller [Keller.460@pldtvibe.com]
보낸 날짜: 2016-07-21 (목) 오후 7:41
받는 사람: jsshim@truecut.co.kr
참조:
제목: fixed invoice
메시지 | jsshim_2161.zip (9 KB)

I am very sorry for the wrong data file you received from me yesterday.
Attached is the fixed invoice

Thank you,

Rose Keller
NORMAN BROADBENT PLC
phone: +1 (584) 455-28-07
fax +1 (584) 455-28-13
Index: c89b1f099e6c5a6fc784df2388bf9e0e2d4b94f486265a
e-mail: Keller.460@pldtvibe.com

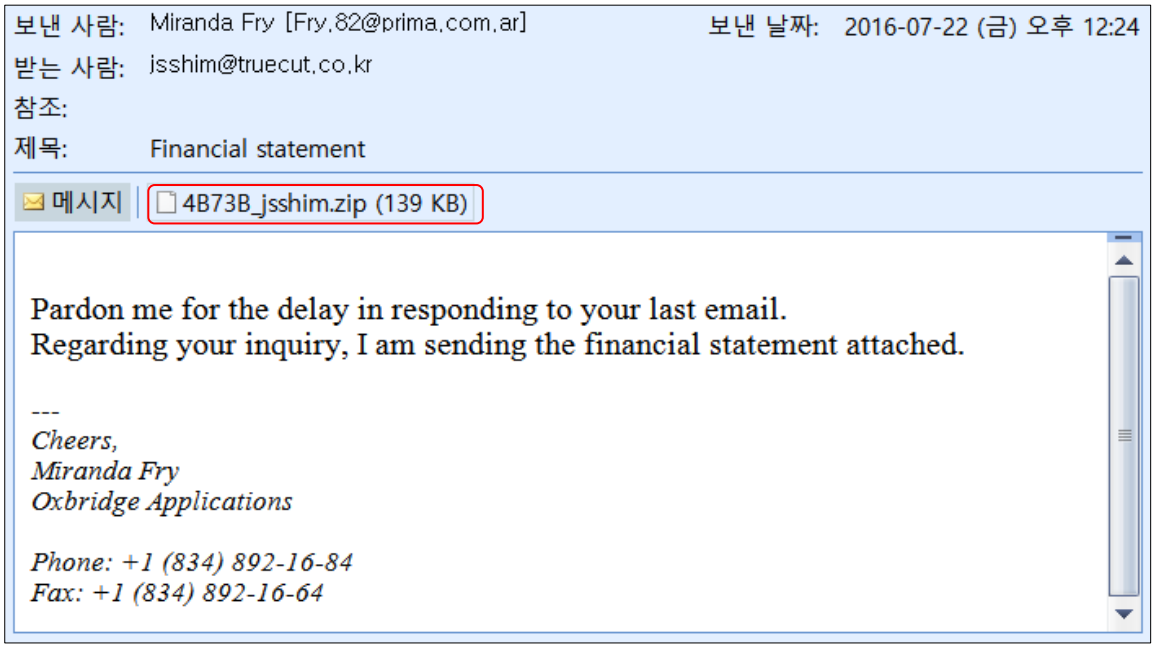


보낸 사람: Kari Farley [Farley.5019 @fishburnecompany.com]
보낸 날짜: 2016-07-22 (금) 오전 3:00
받는 사람: jsshim@truecut.co.kr
참조:
제목: Financial statement
메시지
jsshim_1BB2C.zip (140 KB)

Pardon me for the delay in responding to your last email.
Regarding your inquiry, I am sending the financial statement attached.

Yours faithfully,
Kari Farley
Lebrecht Photo Library

Phone: +1 (297) 161-80-46
Fax: +1 (297) 161-80-21



보낸 사람: Miranda Fry [Fry.82@prima.com.ar]
보낸 날짜: 2016-07-22 (금) 오후 12:24
받는 사람: jsshim@truecut.co.kr
참조:
제목: Financial statement
메시지
4B73B_jsshim.zip (139 KB)

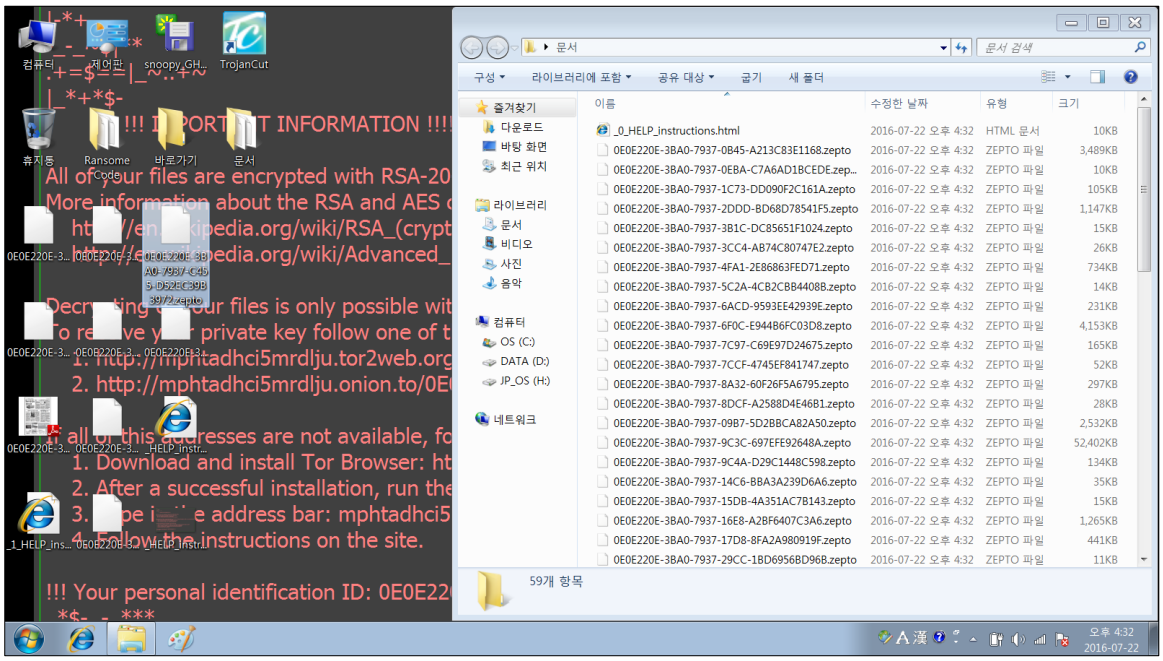
Pardon me for the delay in responding to your last email.
Regarding your inquiry, I am sending the financial statement attached.

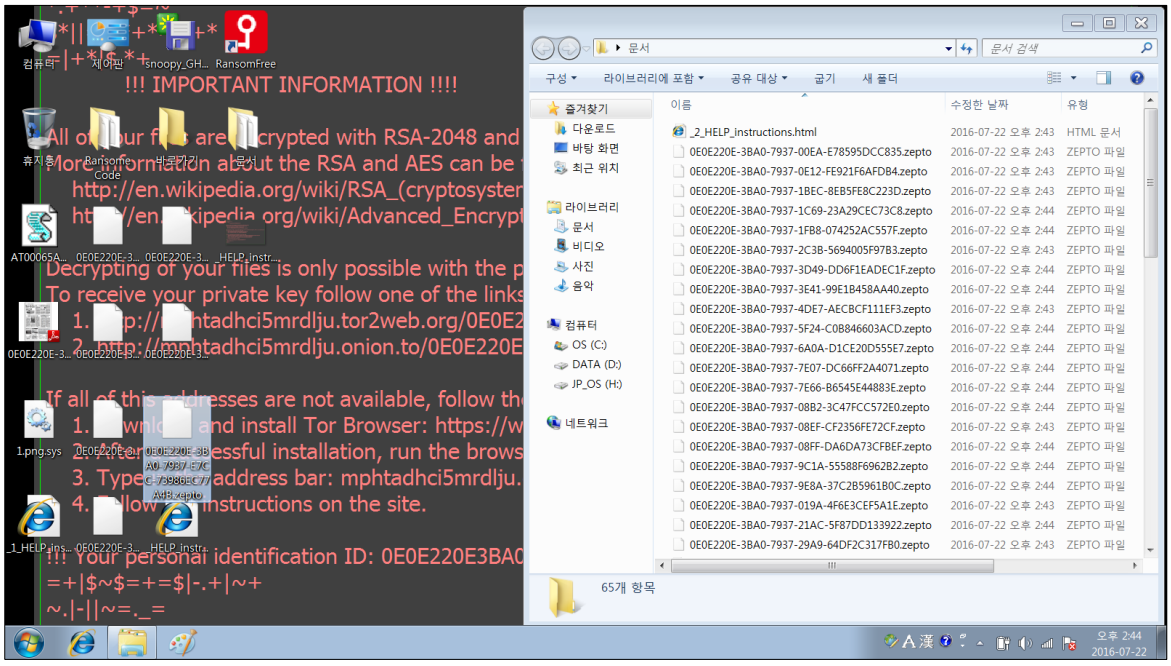
Cheers,
Miranda Fry
Oxbridge Applications

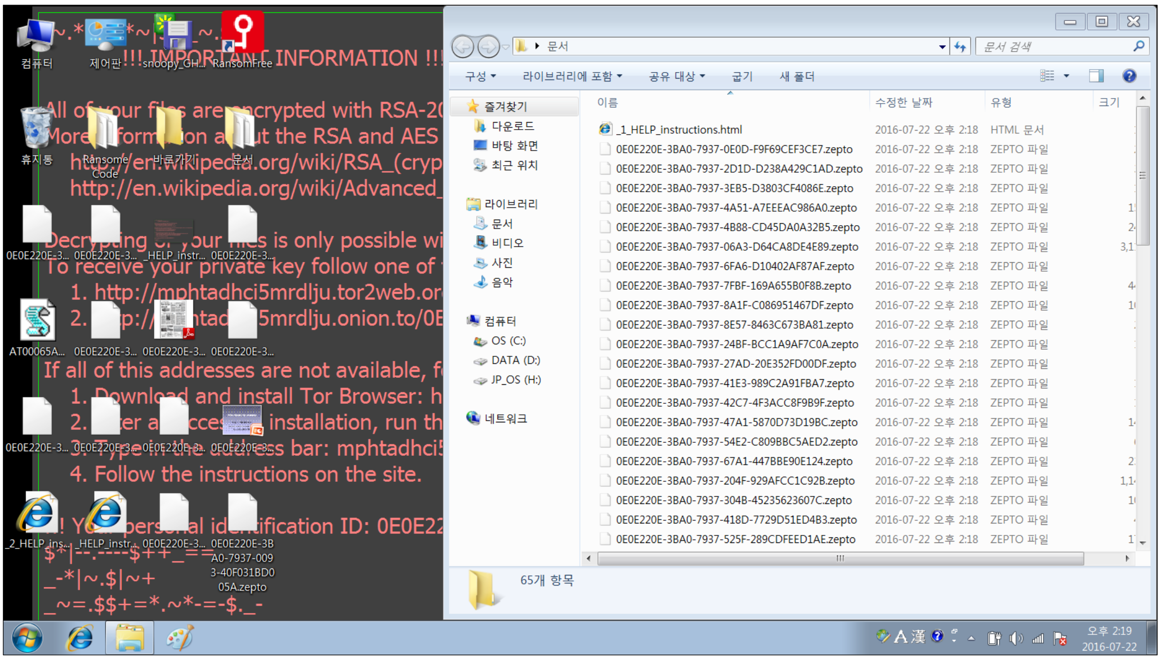
Phone: +1 (834) 892-16-84
Fax: +1 (834) 892-16-64

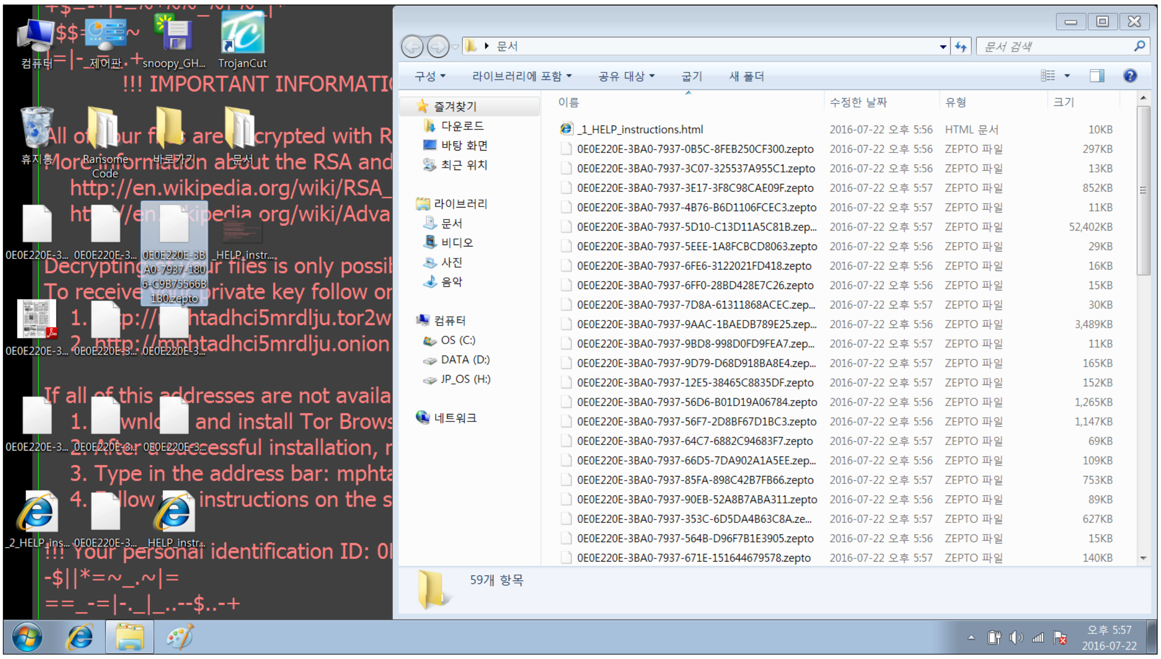
2. Victim under attack

- **Process : C:₩login account₩AppData₩Local₩Temp₩tKnJ5B7b9.exe**
- **Process : C:₩login account₩AppData₩Local₩Temp₩Nc4uhjKNhLIbzucZ.exe**
- **Process : C:₩login account₩AppData₩Local₩Temp₩syDWZqJJQI13HdH.exe**
- **Process : C:₩login account₩AppData₩Local₩Temp₩Bn5TMCxzvZbJrmYT.exe**

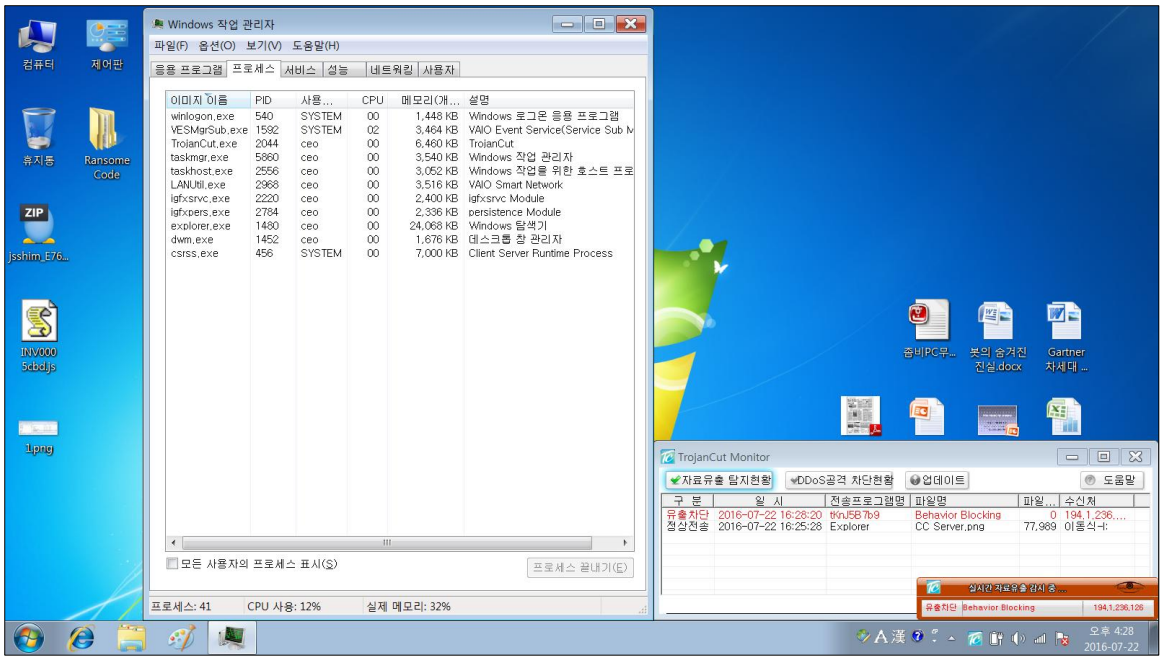


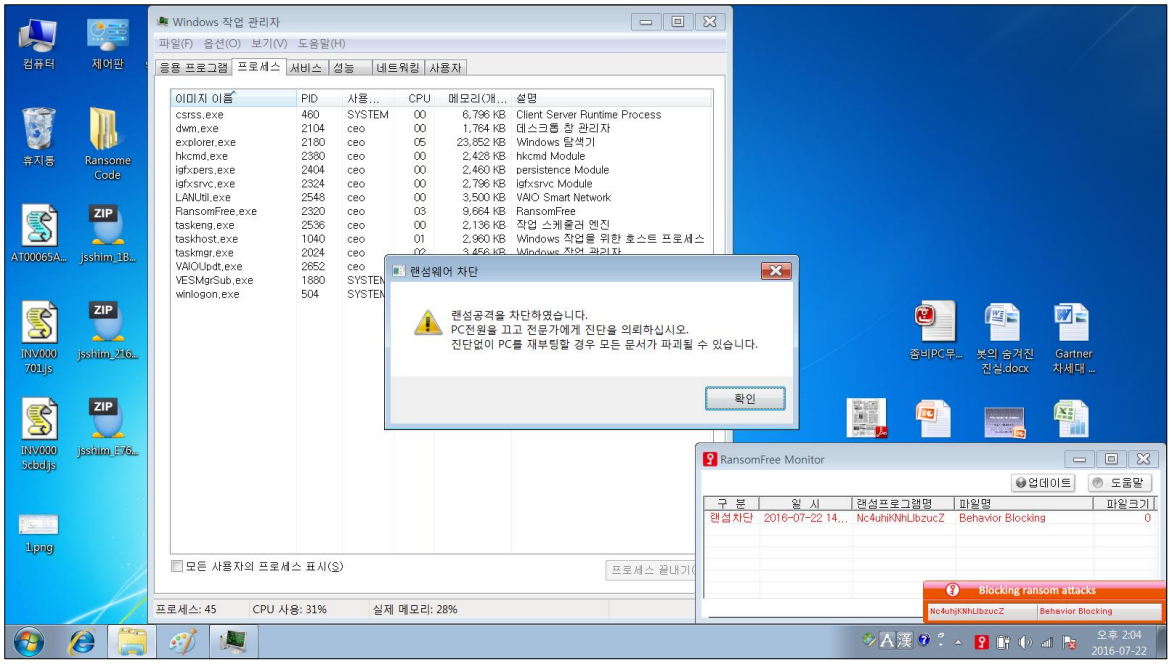


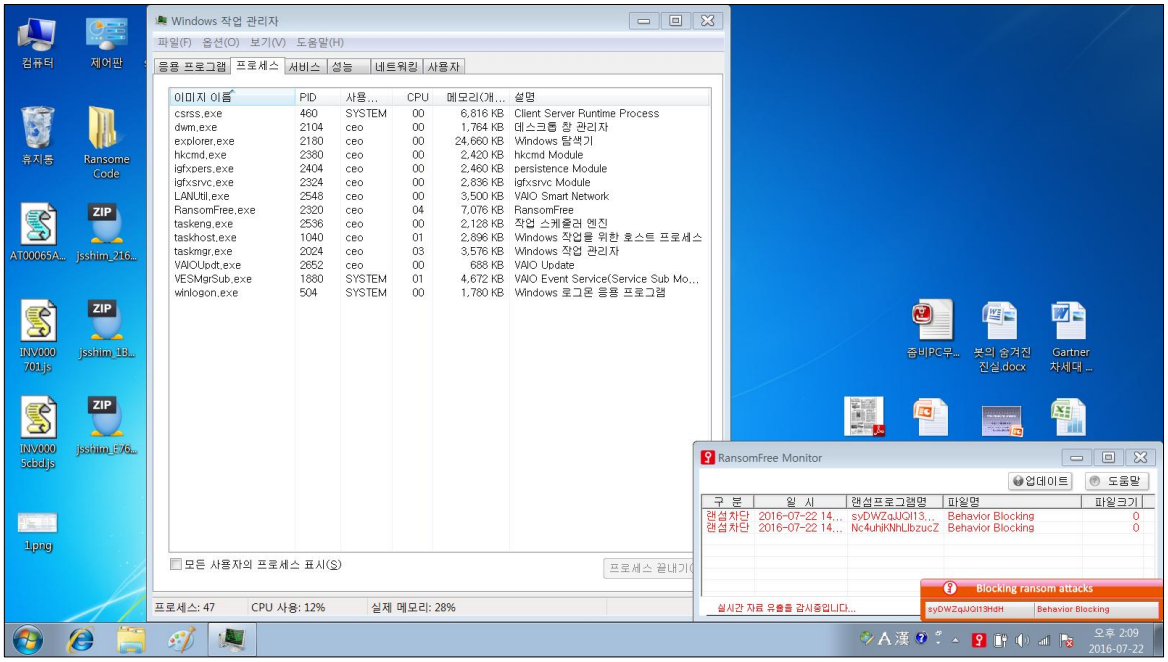

!!! IMPORTANT INFORMATION !!!
All of your files are encrypted with RSA-2
More information about the RSA and AES
http://en.wikipedia.org/wiki/RSA_(cryp
http://en.wikipedia.org/wiki/Advanced_
Decrypting of your files is only possible wi
To receive your private key follow one of
1. http://mphtadhci5mrdlju.tor2web.or
2. http://mphtadhci5mrdlju.onion.to/0E
If all of this addresses are not available, f
1. Download and install Tor Browser: h
2. After a successful installation, run th
3. Type in the address bar: mphtadhci5
4. Follow the instructions on the site.
!!! Your personal identification ID: 0E0E22
문서
구성
라이브러리에 포함
공유 대상
굽기
새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
OS (C:)
DATA (D:)
JP_OS (H:)
네트워크
이름
수정한 날짜
유형
크기
_1_HELP_instructions.html
0E0E220E-3BA0-7937-0E0D-F9F69CEF3CE7.zepto
0E0E220E-3BA0-7937-2D1D-D238A429C1AD.zepto
0E0E220E-3BA0-7937-3EB5-D3803CF4086E.zepto
0E0E220E-3BA0-7937-4A51-A7EEEAC986A0.zepto
0E0E220E-3BA0-7937-4B88-CD45DA0A32B5.zepto
0E0E220E-3BA0-7937-06A3-D64CA8DE4E89.zepto
0E0E220E-3BA0-7937-6FA6-D10402AF87AF.zepto
0E0E220E-3BA0-7937-7FBF-169A655B0F8B.zepto
0E0E220E-3BA0-7937-8A1F-C086951467DF.zepto
0E0E220E-3BA0-7937-8E57-8463C673BA81.zepto
0E0E220E-3BA0-7937-24BF-BCC1A9AF7C0A.zepto
0E0E220E-3BA0-7937-27AD-20E352FD00DF.zepto
0E0E220E-3BA0-7937-41E3-989C2A91FBA7.zepto
0E0E220E-3BA0-7937-42C7-4F3ACC8F9B9F.zepto
0E0E220E-3BA0-7937-47A1-5870D73D19BC.zepto
0E0E220E-3BA0-7937-54E2-C809BBC5AED2.zepto
0E0E220E-3BA0-7937-67A1-447BBE90E124.zepto
0E0E220E-3BA0-7937-204F-929AFCC1C92B.zepto
0E0E220E-3BA0-7937-304B-45235623607C.zepto
0E0E220E-3BA0-7937-418D-7729D51ED4B3.zepto
0E0E220E-3BA0-7937-525F-289CDFEED1AE.zepto
2016-07-22 오후 2:18
HTML 문서
ZEPTO 파일
65개 항목
오후 2:19
2016-07-22

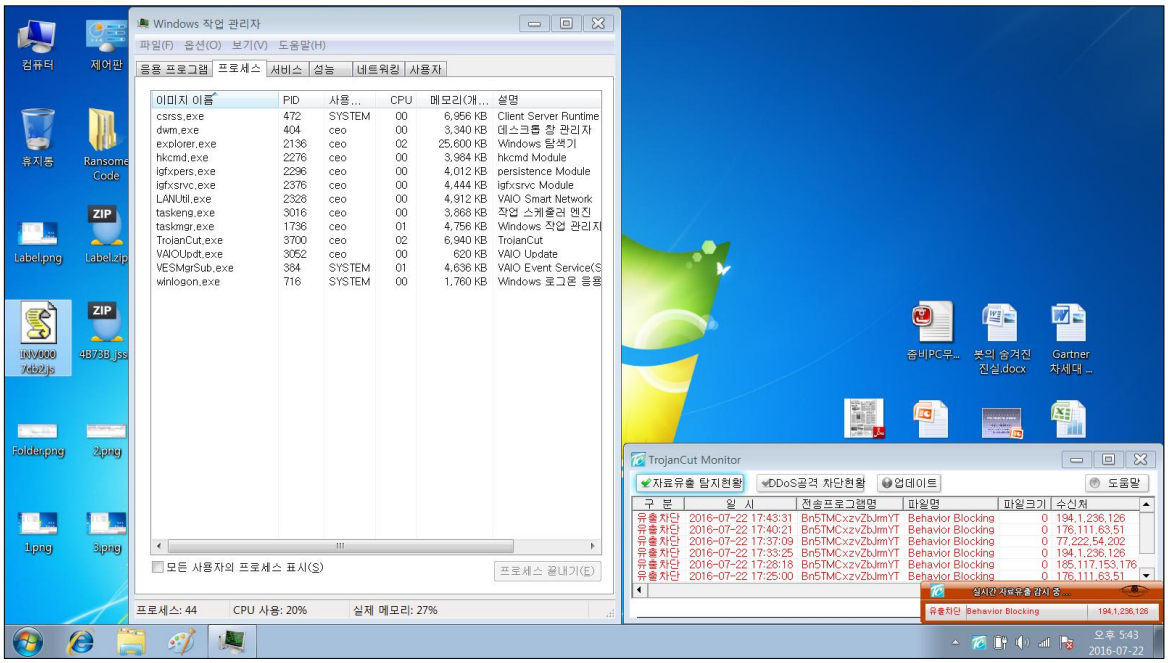

!!! IMPORTANT INFORMATI
All of your files are encrypted with R
More information about the RSA and
http://en.wikipedia.org/wiki/RSA_
http://en.wikipedia.org/wiki/Adva
Decrypting of your files is only possil
To receive your private key follow or
1. http://mphtadhci5mrdlju.tor2w
2. http://mphtadhci5mrdlju.onion
If all of this addresses are not availa
1. Download and install Tor Brows
2. After a successful installation, r
3. Type in the address bar: mphta
4. Follow the instructions on the s
!!! Your personal identification ID: 0I
문서
이름
수정한 날짜
유형
크기
_1_HELP_instructions.html 2016-07-22 오후 5:56 HTML 문서 10KB
0E0E220E-3BA0-7937-0B5C-8FEB250CF300.zepto 2016-07-22 오후 5:56 ZEPTO 파일 297KB
0E0E220E-3BA0-7937-3C07-325537A955C1.zepto 2016-07-22 오후 5:56 ZEPTO 파일 13KB
0E0E220E-3BA0-7937-3E17-3F8C98CAE09F.zepto 2016-07-22 오후 5:57 ZEPTO 파일 852KB
0E0E220E-3BA0-7937-4B76-B6D1106FCEC3.zepto 2016-07-22 오후 5:56 ZEPTO 파일 11KB
0E0E220E-3BA0-7937-5D10-C13D11A5C81B.zep... 2016-07-22 오후 5:57 ZEPTO 파일 52,402KB
0E0E220E-3BA0-7937-5EEE-1A8FCBCD8063.zepto 2016-07-22 오후 5:56 ZEPTO 파일 29KB
0E0E220E-3BA0-7937-6FE6-3122021FD418.zepto 2016-07-22 오후 5:56 ZEPTO 파일 16KB
0E0E220E-3BA0-7937-6FF0-28BD428E7C26.zepto 2016-07-22 오후 5:56 ZEPTO 파일 15KB
0E0E220E-3BA0-7937-7D8A-61311868ACEC.zep... 2016-07-22 오후 5:57 ZEPTO 파일 30KB
0E0E220E-3BA0-7937-9AAC-1BAEDB789E25.zep... 2016-07-22 오후 5:56 ZEPTO 파일 3,489KB
0E0E220E-3BA0-7937-9BD8-998D0FD9FEA7.zep... 2016-07-22 오후 5:57 ZEPTO 파일 11KB
0E0E220E-3BA0-7937-9D79-D68D918BA8E4.zep... 2016-07-22 오후 5:57 ZEPTO 파일 165KB
0E0E220E-3BA0-7937-12E5-38465C8835DF.zepto 2016-07-22 오후 5:57 ZEPTO 파일 152KB
0E0E220E-3BA0-7937-56D6-B01D19A06784.zepto 2016-07-22 오후 5:56 ZEPTO 파일 1,265KB
0E0E220E-3BA0-7937-56F7-2D8BF67D1BC3.zepto 2016-07-22 오후 5:56 ZEPTO 파일 1,147KB
0E0E220E-3BA0-7937-64C7-6882C94683F7.zepto 2016-07-22 오후 5:57 ZEPTO 파일 69KB
0E0E220E-3BA0-7937-66D5-7DA902A1A5EE.zep... 2016-07-22 오후 5:56 ZEPTO 파일 109KB
0E0E220E-3BA0-7937-85FA-898C42B7FB66.zepto 2016-07-22 오후 5:57 ZEPTO 파일 753KB
0E0E220E-3BA0-7937-90EB-52A8B7ABA311.zepto 2016-07-22 오후 5:56 ZEPTO 파일 89KB
0E0E220E-3BA0-7937-353C-6D5DA4B63C8A.ze... 2016-07-22 오후 5:57 ZEPTO 파일 627KB
0E0E220E-3BA0-7937-564B-D96F7B1E3905.zepto 2016-07-22 오후 5:56 ZEPTO 파일 15KB
0E0E220E-3BA0-7937-671E-151644679578.zepto 2016-07-22 오후 5:57 ZEPTO 파일 140KB
59개 항목
오후 5:57
2016-07-22

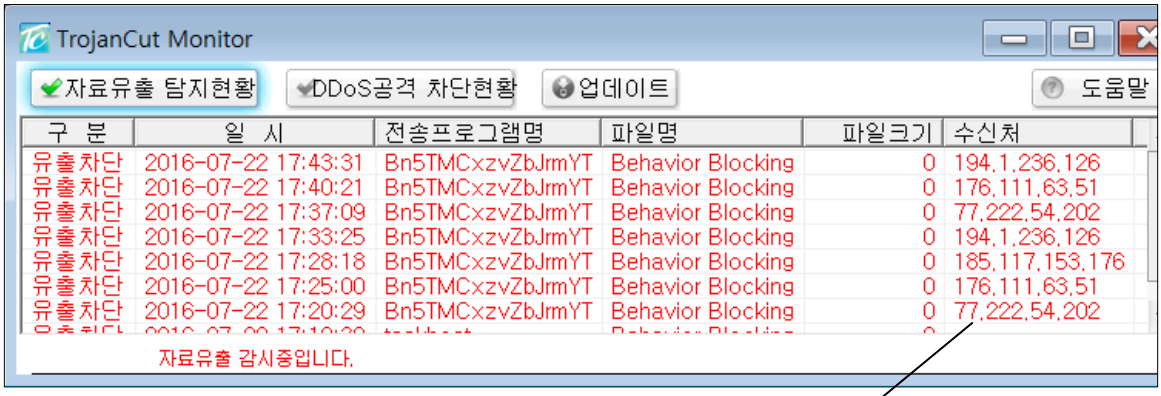
3. Blocking by RansomFree®






Windows 작업 관리자
파일(F) 옵션(O) 보기(V) 도움말(H)
응용 프로그램 프로세스 서비스 성능 네트워킹 사용자
이미지 이름 PID 사용... CPU 메모리(개... 설명
csrss.exe 460 SYSTEM 00 6,816 KB Client Server Runtime Process
dwm.exe 2104 ceo 00 1,764 KB 데스크톱 창 관리자
explorer.exe 2180 ceo 00 24,660 KB Windows 탐색기
hkcmd.exe 2380 ceo 00 2,420 KB hkcmd Module
igfxpers.exe 2404 ceo 00 2,460 KB persistence Module
igfxsrvc.exe 2324 ceo 00 2,836 KB igfxsrvc Module
LANUtil.exe 2548 ceo 00 3,500 KB VAIO Smart Network
RansomFree.exe 2320 ceo 04 7,076 KB RansomFree
taskeng.exe 2536 ceo 00 2,128 KB 작업 스케줄러 엔진
taskhost.exe 1040 ceo 01 2,896 KB Windows 작업을 위한 호스트 프로세스
taskmgr.exe 2024 ceo 03 3,576 KB Windows 작업 관리자
VAIOUpdt.exe 2652 ceo 00 688 KB VAIO Update
VESMgrSub.exe 1880 SYSTEM 01 4,672 KB VAIO Event Service(Service Sub Mo...
winlogon.exe 504 SYSTEM 00 1,780 KB Windows 로그온 응용 프로그램
모든 사용자의 프로세스 표시(S)
프로세스 끝내기(E)
프로세스: 47 CPU 사용: 12% 실제 메모리: 28%
RansomFree Monitor
업데이트 도움말
구 분 일 시 랜섬프로그램명 파일명 파일크기
랜섬차단 2016-07-22 14... syDWZqJJQI13... Behavior Blocking 0
랜섬차단 2016-07-22 14... Nc4uhlKNhLlbzucZ Behavior Blocking 0
실시간 자료 유출을 감시중입니다...
Blocking ransom attacks
syDWZqJJQI13HdH Behavior Blocking
오후 2:09
2016-07-22


Windows 작업 관리자
파일(F) 옵션(O) 보기(V) 도움말(H)
응용 프로그램 프로세스 서비스 성능 네트워킹 사용자
이미지 이름 PID 사용... CPU 메모리(개... 설명
csrss.exe 472 SYSTEM 00 6,956 KB Client Server Runtime
dwm.exe 404 ceo 00 3,340 KB 데스크톱 창 관리자
explorer.exe 2136 ceo 02 25,600 KB Windows 탐색기
hkcmd.exe 2276 ceo 00 3,984 KB hkcmd Module
igfxpers.exe 2296 ceo 00 4,012 KB persistence Module
igfxsrvc.exe 2376 ceo 00 4,444 KB igfxsrvc Module
LANUtil.exe 2328 ceo 00 4,912 KB VAIO Smart Network
taskeng.exe 3016 ceo 00 3,868 KB 작업 스케줄러 엔진
taskmgr.exe 1736 ceo 01 4,756 KB Windows 작업 관리자
TrojanCut.exe 3700 ceo 02 6,940 KB TrojanCut
VAIOUpdt.exe 3052 ceo 00 620 KB VAIO Update
VESMgrSub.exe 384 SYSTEM 01 4,636 KB VAIO Event Service(S
winlogon.exe 716 SYSTEM 00 1,760 KB Windows 로그온 응용
모든 사용자의 프로세스 표시(S)
프로세스 끝내기(E)
프로세스: 44 CPU 사용: 20% 실제 메모리: 27%
TrojanCut Monitor
자료유출 탐지현황 DDoS공격 차단현황 업데이트 도움말
구 분 일 시 전송프로그램명 파일명 파일크기 수신처
유출차단 2016-07-22 17:43:31 Bn5TMCxzvZbJrmYT Behavior Blocking 0 194.1.236.126
유출차단 2016-07-22 17:40:21 Bn5TMCxzvZbJrmYT Behavior Blocking 0 176.111.63.51
유출차단 2016-07-22 17:37:09 Bn5TMCxzvZbJrmYT Behavior Blocking 0 77.222.54.202
유출차단 2016-07-22 17:33:25 Bn5TMCxzvZbJrmYT Behavior Blocking 0 194.1.236.126
유출차단 2016-07-22 17:28:18 Bn5TMCxzvZbJrmYT Behavior Blocking 0 185.117.153.176
유출차단 2016-07-22 17:25:00 Bn5TMCxzvZbJrmYT Behavior Blocking 0 176.111.63.51
실시간 자료유출 감시 중...
유출차단 Behavior Blocking 194.1.236.126
오후 5:43
2016-07-22



As you see the above,
C&C server is changing all the time.

77.222.54.202 RUSSIA

176.111.63.51 UKRAINE

185.117.153.176 RUSSIA

194.1.236.126 RUSSIA

☞ TrojanCut® is blocking in real-time until the unknown ransomware.