랜섬웨어 연대기

blueangel

blueangel1275@gmail.com

http://forensic-note.blogspot.kr/

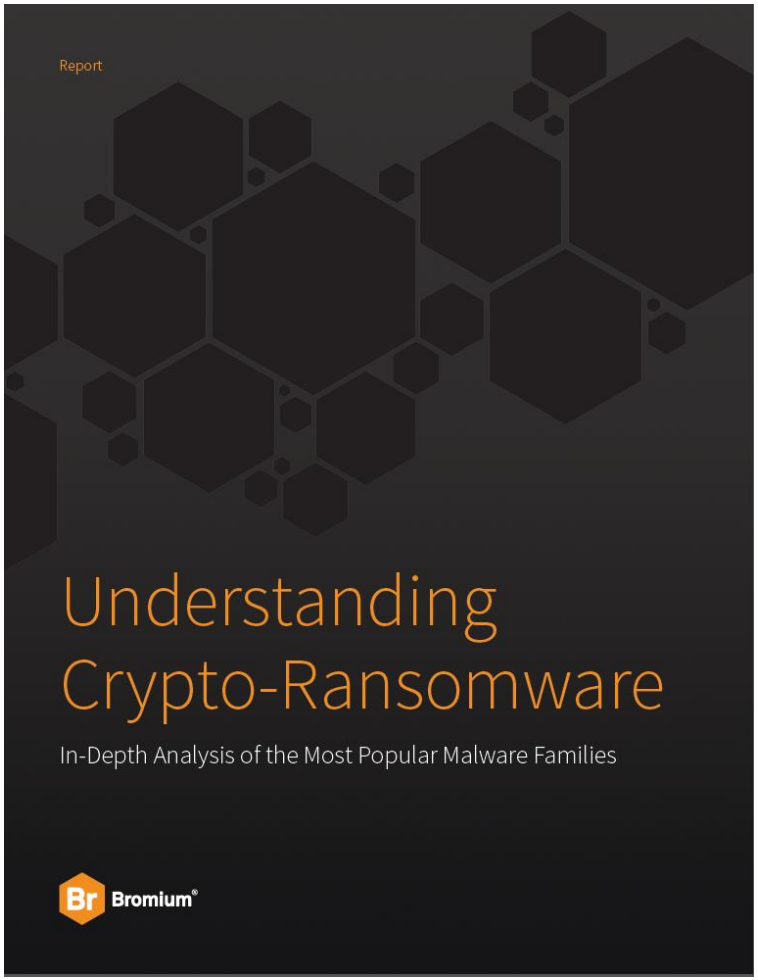
Junghoon Oh

Index

Introduction

Understanding Crypto-Ransomware

- http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf



Crypto-Ransomware ??

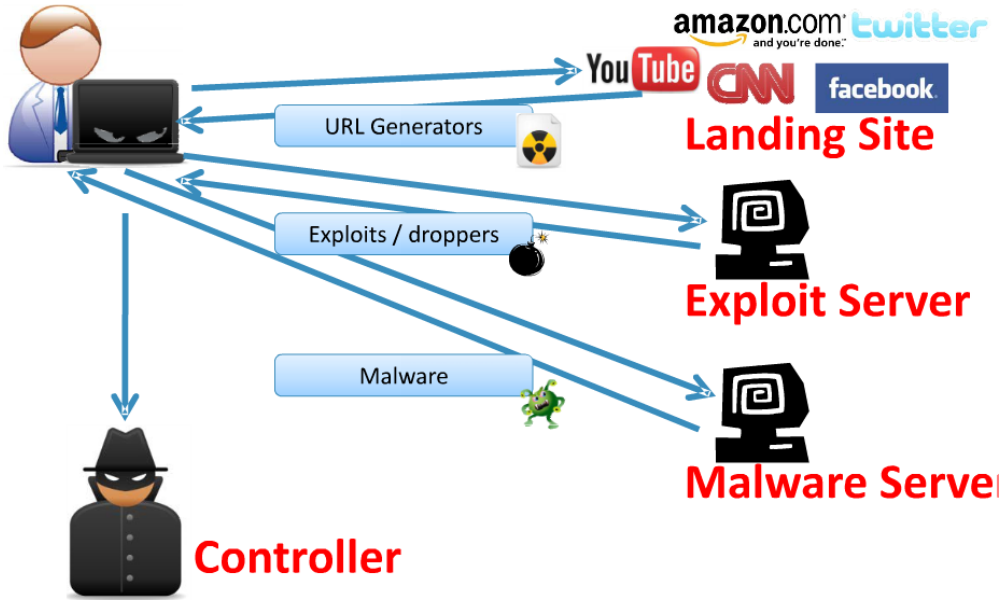
- **Crypto-Ransomware**
  - 사용자의 컴퓨터에 있는 파일들을 암호화하고 복호화를 대가로 금전적인 보상를 요구하는 악성코드
  - 복호화 키는 공격자의 서버에 저장되기 때문에 사용자는 암호화된 파일을 복호화 할 수 없음

- **랜섬웨어 분류**
  - Locker Ransomware : 사용자의 접근을 막음(ex : 화면 잠금), 해제 가능
  - Crypto Ransomware : 파일 암호화, 키를 모르면 복호화 할 수 없음

Crypto-Ransomware ??

- **기존 악성코드와의 차이점**
  - 정보를 유출하지 않음, 대신 정보를 암호화하여 접근하지 못하게 함
  - 자기 자신을 숨기려고 하지 않음, 암호화 작업 후 사용자에게 금전적인 대가 요구
  - 악성코드 생성이 상대적으로 쉬움, 강력하고 이미 공개되어 있는 암호화 알고리즘(RSA, AES)을 사용

- **유입 방식**
  - Spam, Social Engineering
  - Drive by Download
  - Malvertising
  - Botnet or Malware Installation tool

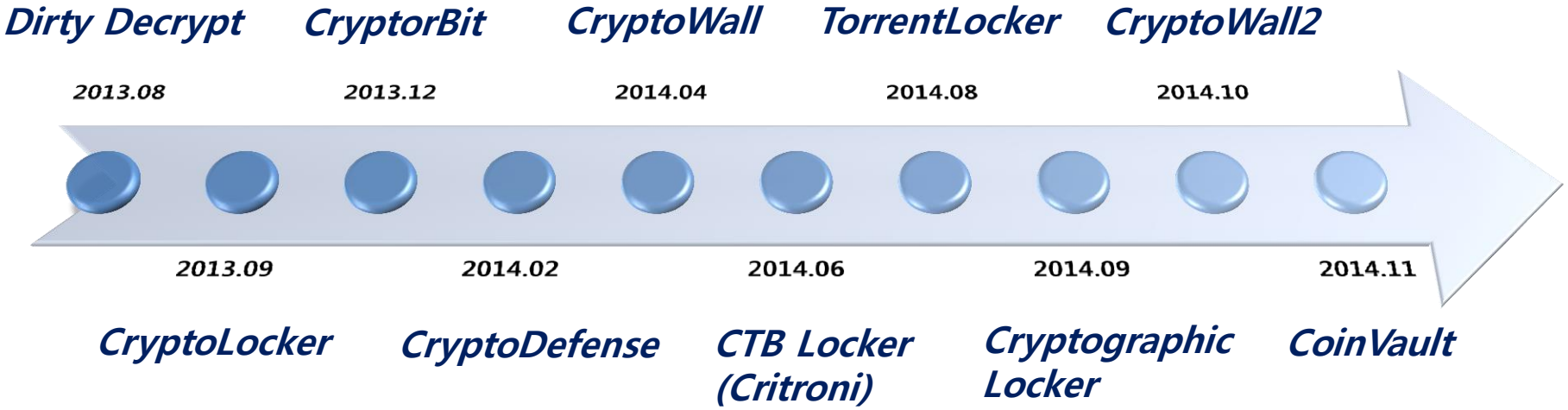


Crypto-Ransomware ??

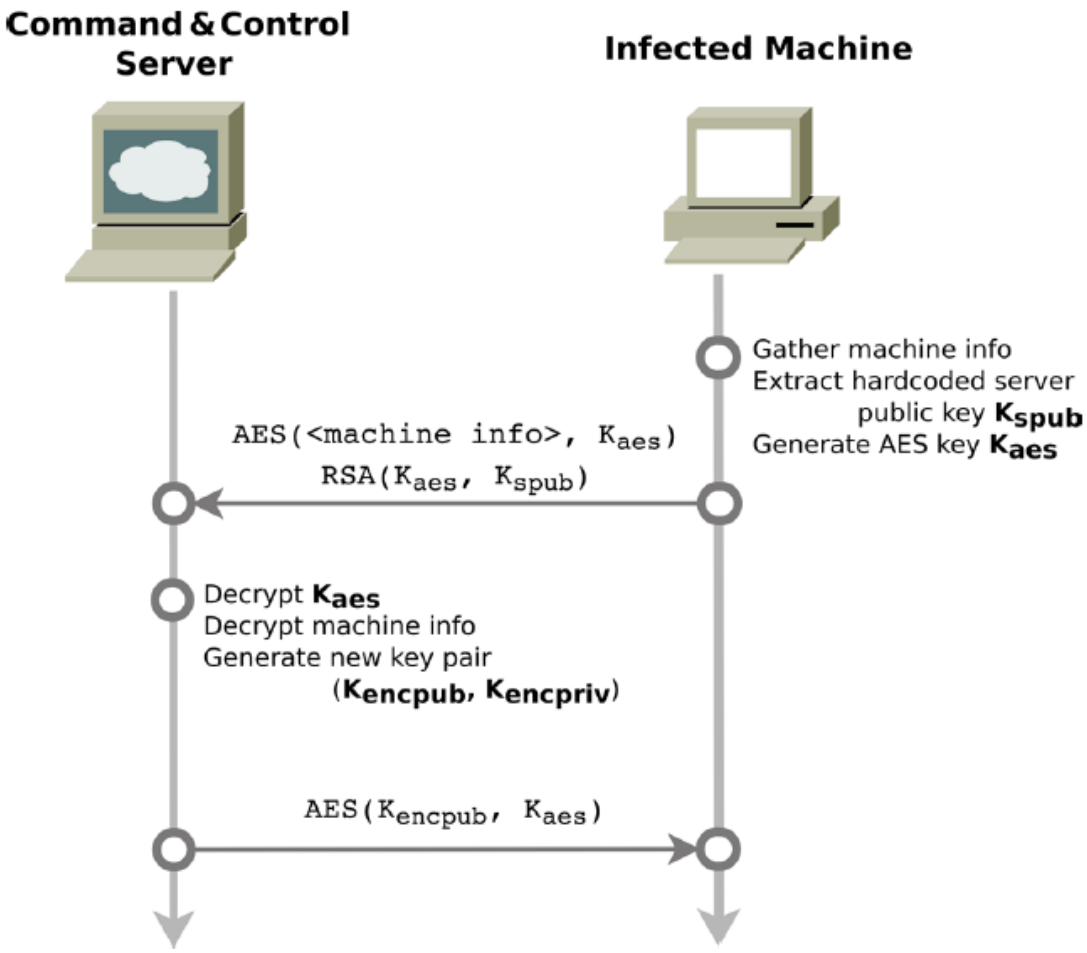
- **악성코드 군(Families) : 2013 ~ 2014**
  - Dirty Decrypt
  - CryptorBit
  - CryptoLocker
  - CryptoDefense
  - CryptoWall
  - CTB Locker(Critroni)
  - TorrentLocker
  - CryptoWall2
  - Cryptographic Locker
  - CoinVault

Crypto-Ransomware Families

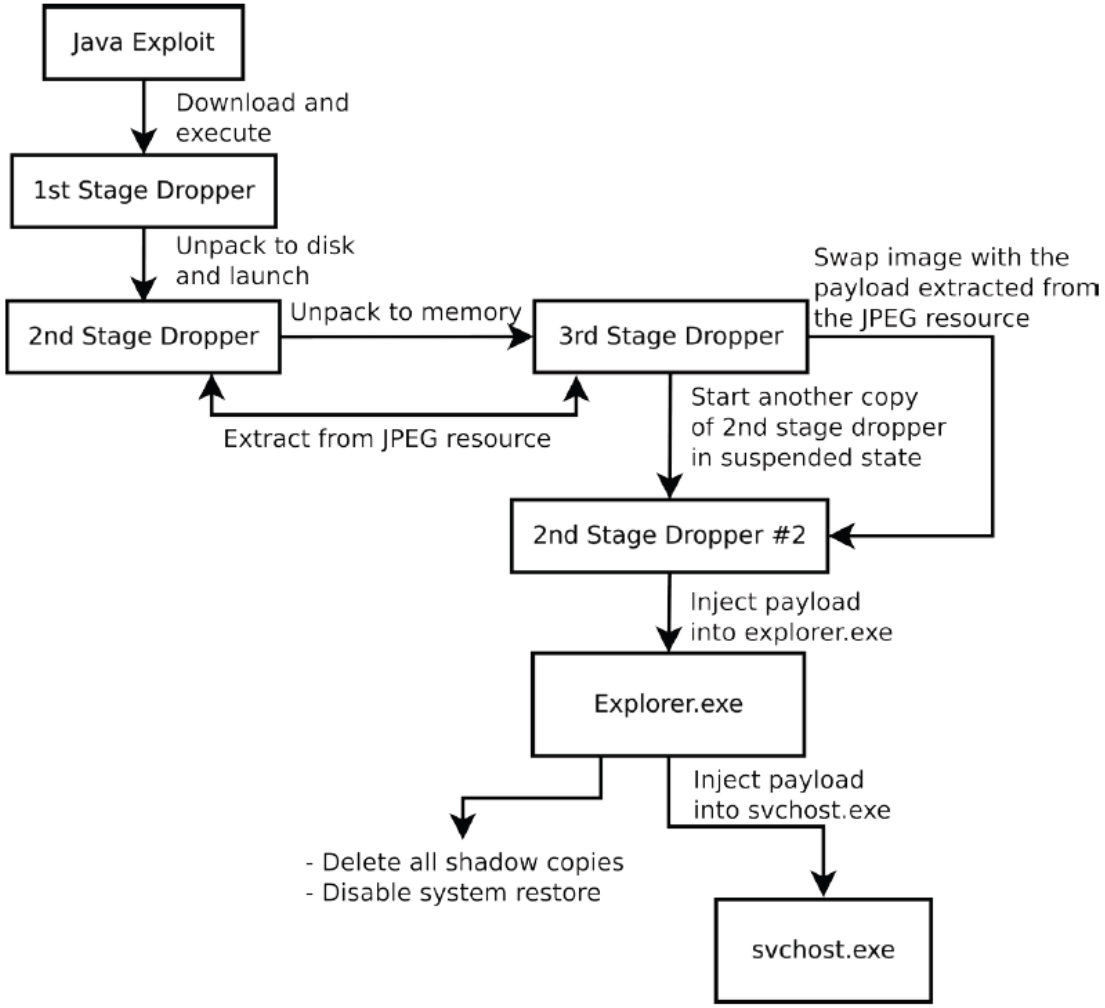
Crypto-Ransomware's History



C&C Protocol(CryptoLocker)



Infection Workflow(CryptoWall)



C&C Communication

Family	Protocol	C&C Domains
Dirty Decrypt	HTTP	DNGA
CryptoLocker	HTTP	DNGA, Hardcoded URLs
CryptoWall / CryptoDefense	HTTP ➔ TOR	Hardcoded URLs
CTB Locker(Critroni)	TOR	Hardcoded URLs
TorrentLocker	HTTPS	Hardcoded URLs
CoinVault / Cryptographic Locker	HTTP	Hardcoded URLs

- 평문 HTTP 통신에서 암호화된 HTTPS, TOR 프로토콜을 사용하는 방향으로 발전함
- DNGA 에서 점점 하드코딩된 URL 사용하는 방향으로 변화됨
  - DNGA(Domain Name Generator Algorithm)

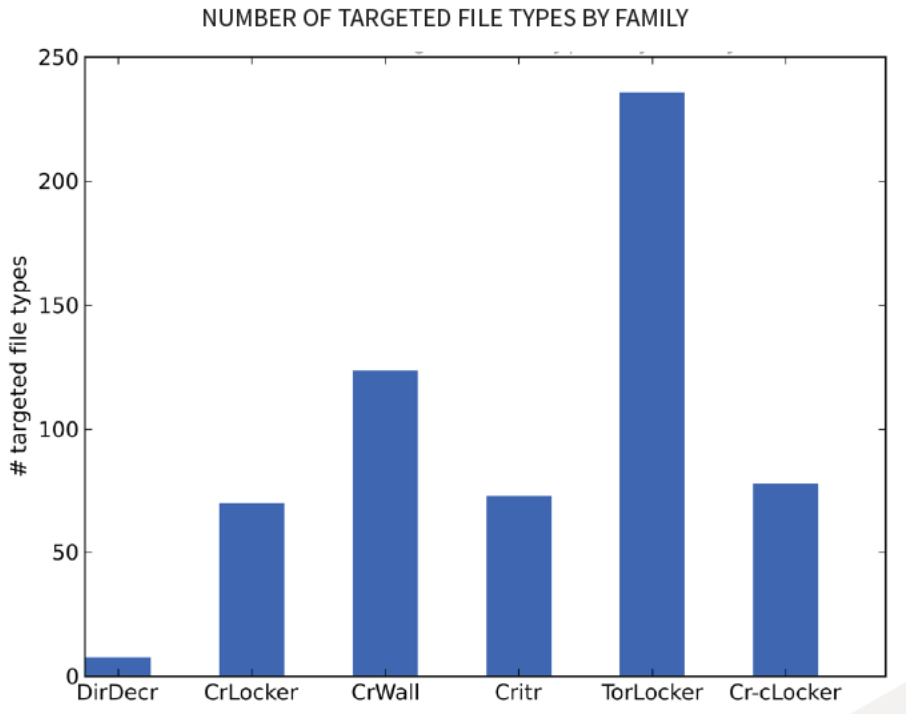
```
def generate_domain(year, month, day):
    """Generates a domain by the current date"""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain
```

Encryption

Family	Encryption Algorithms	Implementation
Dirty Decrypt	RC4 to encrypt whole files, RSA to then encrypt first 1024 bytes of each file	Inline
CryptoLocker	AES for file encryption, RSA for AES key encryption	MS Crypto API
CryptoWall / CryptoDefense	RSA for file encryption	MS Crypto API
CTB Locker(Critroni)	AES for file encryption, ECDH for AES key encryption	OpenSSL, statically linked
TorrentLocker	AES for file encryption	OpenSSL, statically linked
CoinVault / Cryptographic Locker	AES for file encryption	MS Crypto API (.NET)

- 암호 알고리즘이 RC4 에서 RSA+AES 그리고 ECDH+AES 로 발전함
- 초창기에는 MS Crypto API(WinCrypto) 를 사용하지만 점차 정적으로 링크된 OpenSSL 코드를 사용함

Targeted File Types



- 암호화 대상이 되는 파일의 종류는 계속 증가함
- 대부분의 파일 포맷은 문서와 이미지...
- 점차 개인 사용자에서 기업 사용자를 대상으로 범위가 확대됨
  - CAD, 회계 관련 프로그램 포멧...

Payment Options

Family	Payment Options	Price of Decrypting
Dirty Decrypt	PaySafeCard, MoneyPak, etc	100 USD
CryptoLocker	Bitcoin, MoneyPak, UKash, CashU ➔ Bitcoin	300 USD
CryptoWall / CryptoDefense	Bitcoin	500 USD 1000 USD (if not paid within time frame)
CTB Locker(Critroni)	Bitcoin	0.5 BTC
TorrentLocker	Bitcoin	0.8 BTC
CoinVault / Cryptographic Locker	Bitcoin	0.2-0.5 BTC

- 초기 선불카드에서 Bitcoin 을 결제 수단으로 사용되는 방향으로 변화됨
- 최근 Ransomware 의 경우, 현재 달러 단위가 아닌 BTC 단위로 금액을 정함

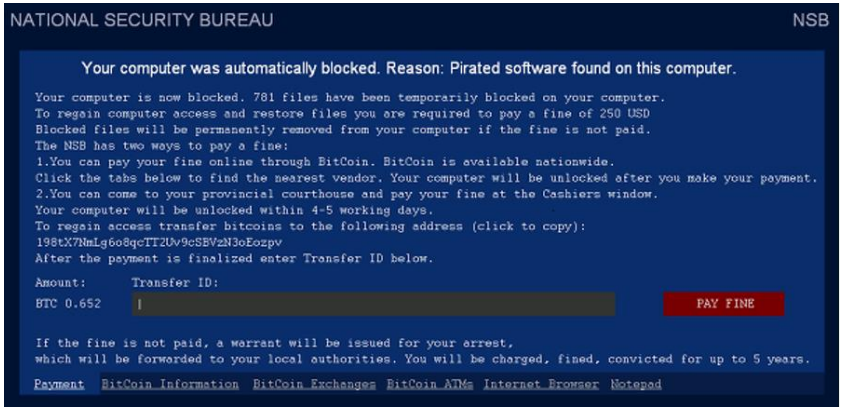
New Ransomwares in 2015

- **Crypto Locker Copycat : PClock, Crypto Locker2015**

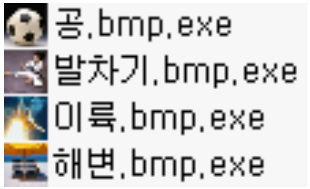
- Crypto Locker 의 유명세를 이용한 copycat
- XOR Encryption 사용;; ➔ 해당 key 는 파일 안에 존재함 ➔ 하지만 사람들은 겁을 먹고 돈을 지불함...

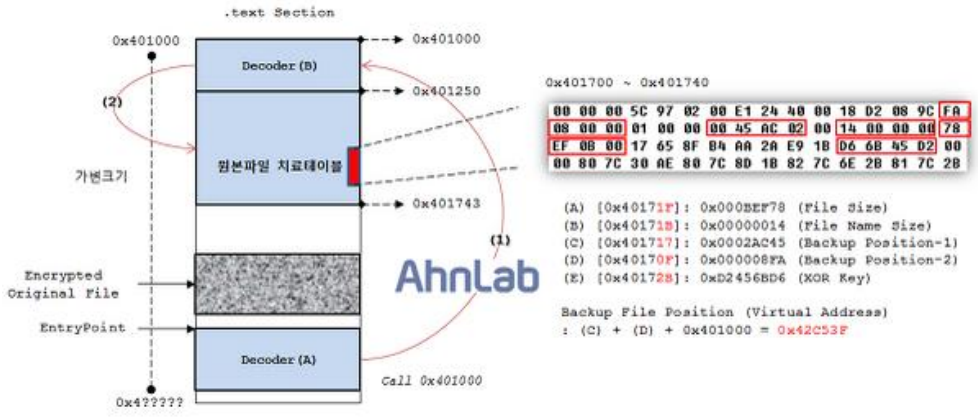
New Ransomwares in 2015

- **VIRLOCK(VIRus+Ransom Lock)(http://asec.ahnlab.com/1025)**
  - National Security Bureau(국가안보국) 을 가장하여 사용자에게 돈을 요구



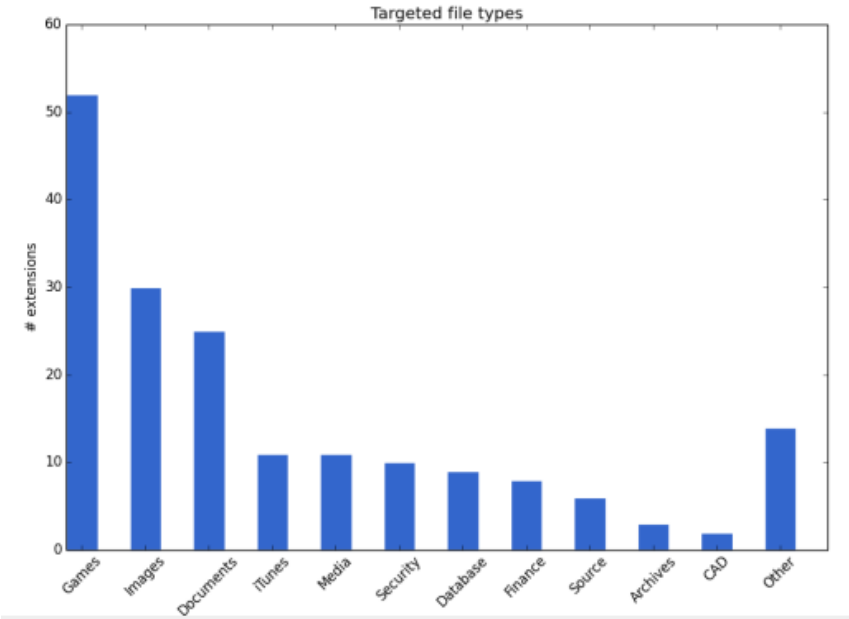
  - 문서, 그림, 실행 파일들을 인코딩 하여, 실행 압축 형태로 저장함 ➔ V3 Lite 를 통해 복구 가능





New Ransomwares in 2015

- **TeslaCrypt(http://labs.bromium.com/2015/03/12/achievement-locked-new-crypto-ransomware-pwns-video-gamers/)**
  - 게임 데이터를 목표로 하는 Ransomware
  - 사용자가 유료로 구입하여 시스템 내에 저장되어 있는 게임 데이터를 목표로 함
    - ✓ user profile data, saved games, maps, mods …
  - 185 종류의 파일을 대상
  - RSA-2048 방식으로 암호화되었다고 사기침
    - ✓ 실제로는 AES 로 암호화되어있고 관련 키파일(key.dat)은 시스템에 저장됨 ➔ 복호화 가능

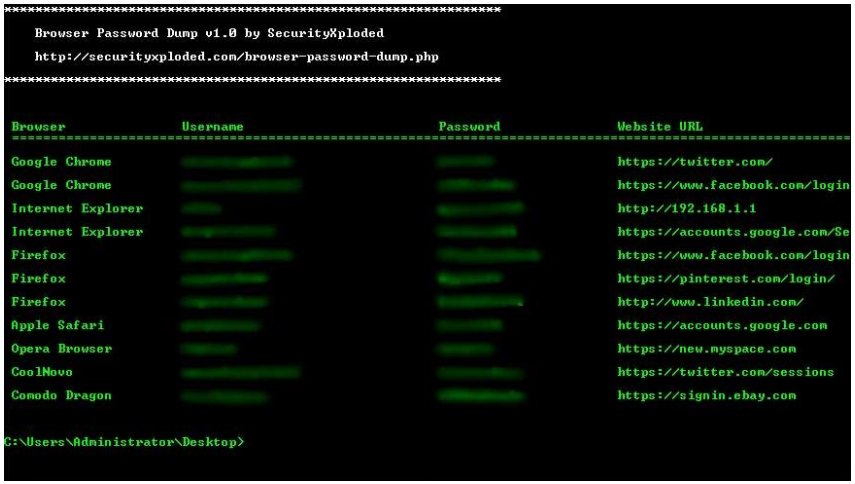


New Ransomwares in 2015

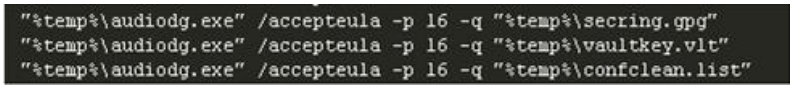
- **정보 탈취 기능이 추가된 Ransomware**

(http://blog.trendmicro.com/trendlabs-security-intelligence/crypvault-new-crypto-ransomware-encrypts-and-quarantines-files/)

- 파일 암호화 후, Browser Password Dump 를 다운로드 하여 웹 브라우저의 패스워드 정보 탈취

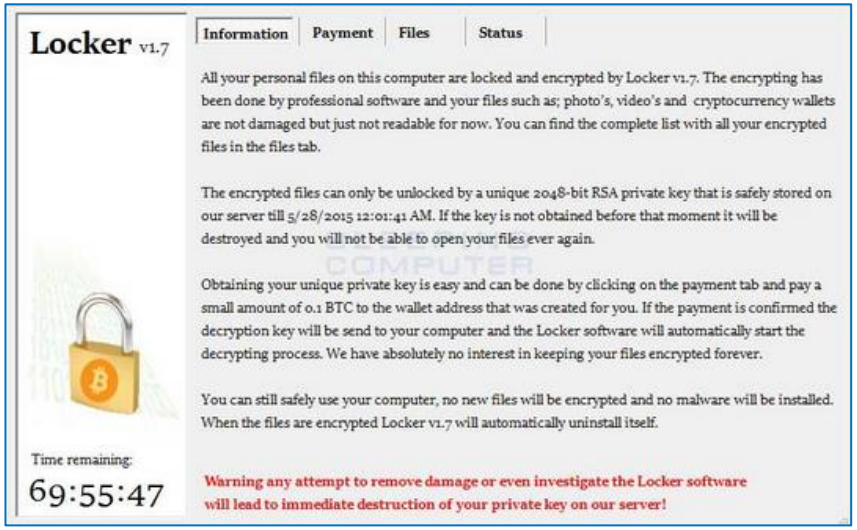


- 추가적인 특징
  - ✓ 암호화 도구(GnuPG) 및 완전 삭제 도구(sDelete) 의 이름을 변경해서 사용함



New Ransomwares in 2015

- **Locker**
  - 휴면기가 있음(5월 25일 동작)
  - 유입 경로를 알기 어려움??
    - ✓ 감염된 마인크래프트 인스톨러가 의심…



- 파일 복호화???
  - ✓ 5월 30일에 Private Key 파일과 Decrypter 공개
    - 62,703 개의 Key 와 비트코인 수입 목록
    - 22 개 감염
    - $169 …
  - ✓ 6월 2일 자동으로 복호화 ㅎㄷㄷ

New Ransomwares in 2015

- **Windows 10 무료 업데이트를 가장한 Fake Email 을 통한 감염**
  - 감염 랜섬웨어
    - ✓ CTB-Locker
    - ✓ Cryptolocker
    - ✓ …

From Microsoft <update@microsoft.com>
Subject **Windows 10 Free Update**
[redacted]

Reply Reply Followup Forward More
6:17 AM

Upgrade to Windows 10 for free

.

Windows 10 is familiar and easy to use. It includes an improved Start menu and is designed to startup and resume fast. Plus, itÂ's packed with new innovations including Microsoft Edge Â– an all–new browser. Your personal files and apps youÂ've installed will all be waiting for you. WeÂ've designed the upgrade to be easy and compatible with the hardware and software you already use.

DonÂ't miss out as this free offer wonÂ't last forever. Upgrade today. Follow the attached installer and get started.

Â"Upgrading from Windows 7 or Windows 8? You will love Windows 10!Â"

Windows device running Windows 10

You received this mandatory email service announcement to update you about important changes to your Microsoft product.
Â© 2015 Microsot Inc., One Microsoft Way Redmond, WA 98052–6399, USA

Microsoft

New Ransomwares in 2015

- **Ransomware-as-a-service**
  - Tox(Ransomware Development Kit)
  - 랜섬웨어 제작 및 기반 인프라 판매

  - 이미 봇넷을 가지고 있는 그룹에게 판매
  - 수입의 20%는 제작자에게…

국내 배포 중인 Ransomware

- **CTB Locker**

- 2015년 1월 ~ 2월, 국내 기업들을 대상으로 유포됨
- 배포 방식
  - ✓ .scr 로 된 downloader 파일이 메일에 첨부
  - ✓ 사용자가 해당 파일을 클릭하면 wordpad 를 실행하여 RTF 문서를 띄운 후, CTB Locker 를 다운로드 하여 실행

국내 배포 중인 Ransomware

- **Crypt0L0cker**

- 2015년 4월 21일, 국내 유명 커뮤니티 사이트 들에 링크된 광고를 통해 유포됨
- 기존의 스피어 피싱 기법과 다르게 Drive by Download 로 유포 방식 사용(by Angler Exploit Kit)
- 각 국가별 지역코드의 따라 안내문의 언어가 달라짐
  - ✓ 한국, 일본 등 아시아 국가들이 추가됨

Case Study

Ransomware 감염 케이스

- **CryptoDefense 감염 흔적**

	Name	Last Accessed	File Created	Last Written	Entry Modified	Filter	In Report	File Ext	File Type	File Category
211730	국문회신.txt	03/05/14 07:45:59오후	03/05/14 07:45:59오후	04/04/14 09:07:03오전	04/04/14 09:07:03오전			txt	Text	Document

Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Output | Lock | Codepage | 0/212908

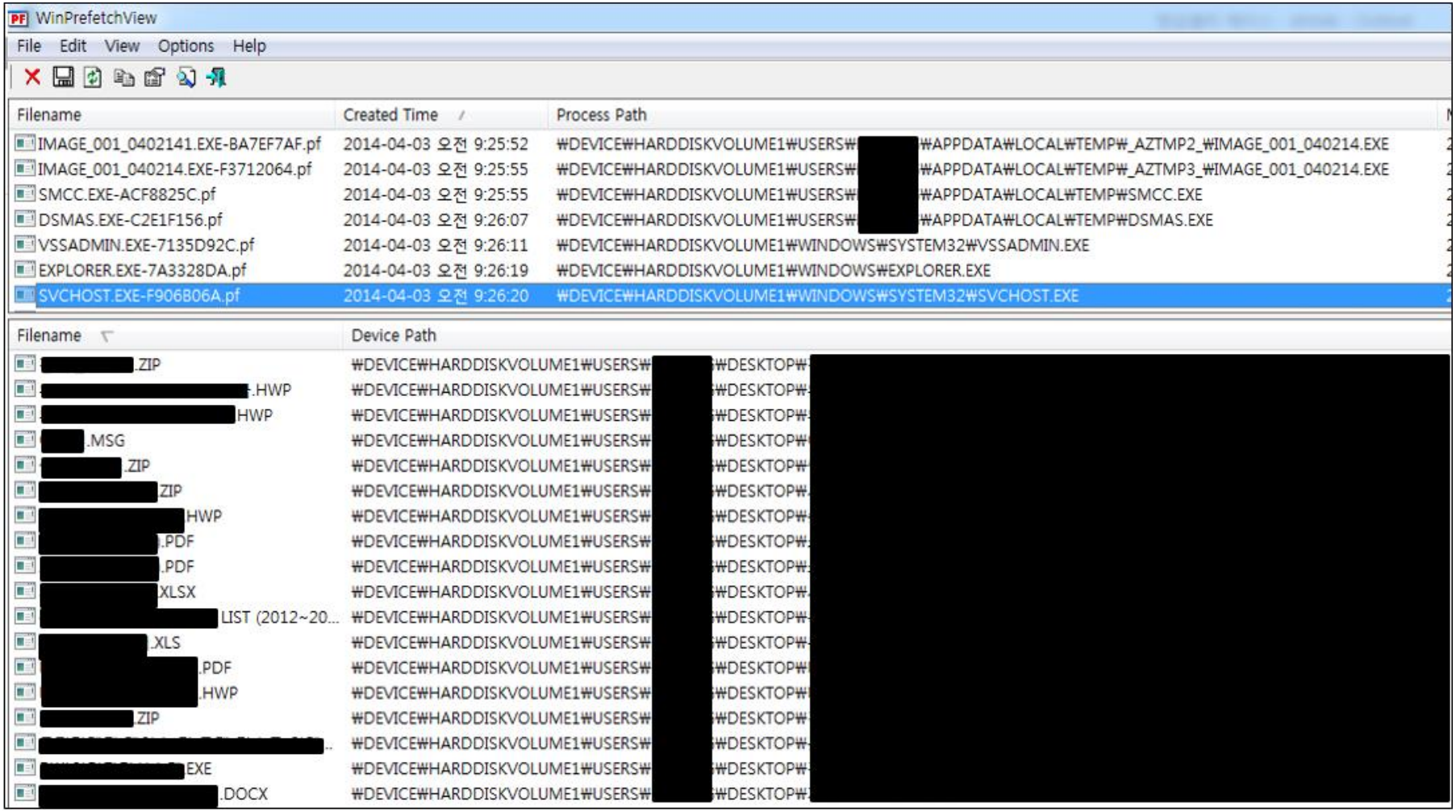
```
00021 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 21 00 00 00 45 00 36 00 42 00 42 00 31 00 36 00 34 00 46 00 46 00 34 00 46 00 32 00 32 00 44 00 41
04900 45 00 45 00 34 00 34 00 31 00 35 00 38 00 45 00 34 00 32 00 37 00 31 00 46 00 35 00 46 00 33 00 32 00 00 00 5D 35 8D D8 A2 CE 73 ED 4B 82 DD A9
09866 F3 37 75 DC 83 B3 C4 20 EB 31 BC CB DC 65 AD DC F0 DF 9F 31 D5 E3 AC 53 36 3F 38 44 CA AC 52 F4 AD F3 EC 22 32 08 8B E0 F4 2D 51 C8 5D 0A 87 64
14797 71 E9 89 BA F7 8D 33 09 B8 FE CC 7C F0 24 C7 60 47 E8 D3 9E 79 13 5D 48 A7 6A EE C4 6F C2 E3 2B 12 69 15 6A F6 BA EF 16 8E A0 45 39 FE AE 9A CB
19682 5E 83 29 FE 46 66 FC A3 2C FF 7D B8 7B 8C 73 41 69 B8 81 1C 3D B1 EB 2B F7 FB E4 DA C1 42 75 66 19 00 50 58 3E E8 6C 91 40 EE 5E AC B6 C7 E7 AB
245CE E2 85 D7 BC 6F 4C 5D B8 7B A0 E1 BE 8B 17 C3 04 E9 D8 4A 28 42 C9 B4 08 A0 20 68 B9 98 F2 95 3E D6 94 00 A3 82 A5 5F B8 3F 2E 0F EA 89 1B A6 50
294BE F4 6C 07 F3 CC 98 06 F7 34 52 EC 64 D1 4F 10 D8 95 D5 7E 28 8C A1 D9 CD 60 B8 BD EC D7 C0 D4 CF 25 59 FE B3 47 A2 2E 0D 89 E6 AF F9 18 2F 1D 3E
3430E B5 00 7E 0F EA 03 7B 46 3C 52 4E DC 4E 7E 39 9B 19 AA DB 8A 21 60 AE B1 59 BB D3 69 0C 49 0E 25 3D 31 82 E8 4F B5 6F DE 9F A3 A6 7E 0E 1E EE 04
3928F C1 71 4B 6D B5 42 F1 36 BE 8A 83 06 CF 3B 27 02 7A 6B 5F C9 CC AD 06 0F F0 2E 2A 9A 18 91 45 E2 43 06 F0 F8 DE 6B 77 2C C7 3F F1 A3 D6 27 32 FC
4411A 9D 8E D4 F9 DD C4 2B 79 1B 8F 96 50 42 28 77 FE E6 CB C5 DE 90 A6 A8 F1 B0 E5 5F A4 0B ED B4 08 91 FD 8E 60 68 BC B0 0F 06 CA 53 BA 4C B1 00 DE
490BD D1 85 2F 32 BA B5 29 4C 3B 2D BE 9F 47 D1 CB 29 DB 97 CD 23 AE 04 5D 29 20 67 30 6D 2B EC 7A EE 68 7E EB 95 C3 61 27 F1 DE C5 1C 61 DB 9A 2A E7
53912 9E 7C 2E 61 62 04 53 87 46 70 FC 49 41 00 B7 F4 E1 CA AB D8 BB 7F 74 21 B9 1B B4 31 47 45 98 5C EC 15 15 BB 27 F2 C9 73 52 C7 81 3D 12 F7 09 FF
588B3 97 C0 EC 85 21 19 2F 13 B7
```

- **최초 암호화 시작 시간**

	Name	Last Accessed	File Created	Last Written	Entry Modified
206294	IMAGE_001_040214.EXE-BA7EF7AF.pf	04/03/14 09:25:52오전	04/03/14 09:25:52오전	04/03/14 09:25:52오전	04/04/14 10:07:02오전
206295	smcc.exe	04/03/14 09:25:52오전	04/03/14 09:25:52오전	04/03/14 09:25:52오전	04/03/14 09:25:52오전
206296	SMCC.EXE-ACF8825C.pf	04/03/14 09:25:55오전	04/03/14 09:25:55오전	04/03/14 09:26:07오전	04/04/14 10:07:02오전
206297	IMAGE_001_040214.EXE-F3712064.pf	04/03/14 09:25:55오전	04/03/14 09:25:55오전	04/03/14 09:25:55오전	04/04/14 10:07:02오전
206298	DSMAS.EXE-C2E1F156.pf	04/03/14 09:26:07오전	04/03/14 09:26:07오전	04/03/14 09:26:09오전	04/04/14 10:07:02오전
206299	VSSADMIN.EXE-7135D92C.pf	04/03/14 09:26:11오전	04/03/14 09:26:11오전	04/03/14 09:26:11오전	04/04/14 10:07:02오전
206300	EXPLORER.EXE-7A3328DA.pf	04/03/14 09:26:19오전	04/03/14 09:26:19오전	04/04/14 09:02:40오전	04/04/14 10:07:02오전
206301	SVCHOST.EXE-F906B06A.pf	04/03/14 09:26:20오전	04/03/14 09:26:20오전	04/04/14 09:02:40오전	04/04/14 10:07:02오전
206302	HOW_DECRYPT.TXT	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전
206303	HOW_DECRYPT.HTML	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전
206304	HOW_DECRYPT.URL	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전	04/03/14 09:28:35오전
206305	HOW_DECRYPT.TXT	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전
206306	HOW_DECRYPT.HTML	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전
206307	HOW_DECRYPT.URL	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전	04/03/14 09:28:36오전
206308	HOW_DECRYPT.HTML	04/03/14 09:28:37오전	04/03/14 09:28:37오전	04/03/14 09:28:37오전	04/03/14 09:28:37오전
206309	HOW_DECRYPT.URL	04/03/14 09:28:37오전	04/03/14 09:28:37오전	04/03/14 09:28:37오전	04/03/14 09:28:37오전

Ransomware 감염 케이스

- 프리패치



Case Study

Ransomware 감염 케이스

- **UsnJrnl 분석**

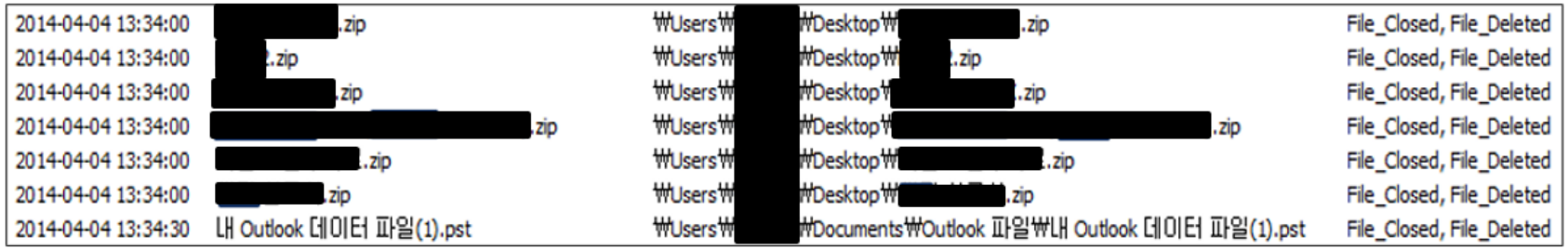
TimeStamp	FileName	Full Path(from $MFT)	Event
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	File_Created
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	File_Created, File_Closed
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	File_Truncated
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	File_Added, File_Truncated
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Attr_Changed, File_Added,
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Attr_Changed, File_Added,
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Named_Stream_Changed
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Named_Data_Stream_Adde
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Named_Data_Stream_Adde
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Created
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Created, File_Closed
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Truncated
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Added, File_Truncated
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Added, Data_Overwritt
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Added, Data_Overwritt
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Added, Data_Overwritt
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	File_Added, Data_Overwritt
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	Attr_Changed, File_Added,
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	Attr_Changed, File_Added,
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	Attr_Changed
2014-04-03 09:25:48	Image_001_040214 (2).zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214 (2).zip	Attr_Changed, File_Closed
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Attr_Changed
2014-04-03 09:25:48	Image_001_040214.zip	₩Users₩nesong₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.Outlook₩3QPS0IXF₩Image_001_040214.zip	Attr_Changed, File_Closed

TimeStamp	FileName	Full Path(from $MFT)	Event
2014-04-03 09:25:51	_AZTMP2_	₩Users₩nesong₩AppData₩Local₩Temp₩_AZTMP2_	File_Created
2014-04-03 09:25:51	_AZTMP2_	₩Users₩nesong₩AppData₩Local₩Temp₩_AZTMP2_	File_Created, File_Closed
2014-04-03 09:25:51	Image_001_040214.exe		File_Created
2014-04-03 09:25:51	Image_001_040214.exe		File_Created, File_Added
2014-04-03 09:25:51	Image_001_040214.exe		File_Created, Attr_Changed, File_Added
2014-04-03 09:25:51	Image_001_040214.exe		File_Created, Attr_Changed, File_Added, File_Closed
2014-04-03 09:25:51	Image_001_040214.exe		Attr_Changed, Content_Indexed_Attr_Changed
2014-04-03 09:25:51	Image_001_040214.exe		Attr_Changed, Content_Indexed_Attr_Changed, File_Closed

Ransomware 감염 케이스

분석 요약

- 사용자는 오피스 프로그램을 통해 메일의 첨부된 ZIP 파일(Image_001_040214.zip)을 알집을 통해 압축은 푼 후, 압축 파일 안에 있는 EXE 파일(Image_001_040214.exe)을 실행함
- 관련 메일 파일(.PST)은 사용자가 케이스 시작 전에 삭제하였기 때문에 공격에 사용된 메일을 찾을 수 없었음

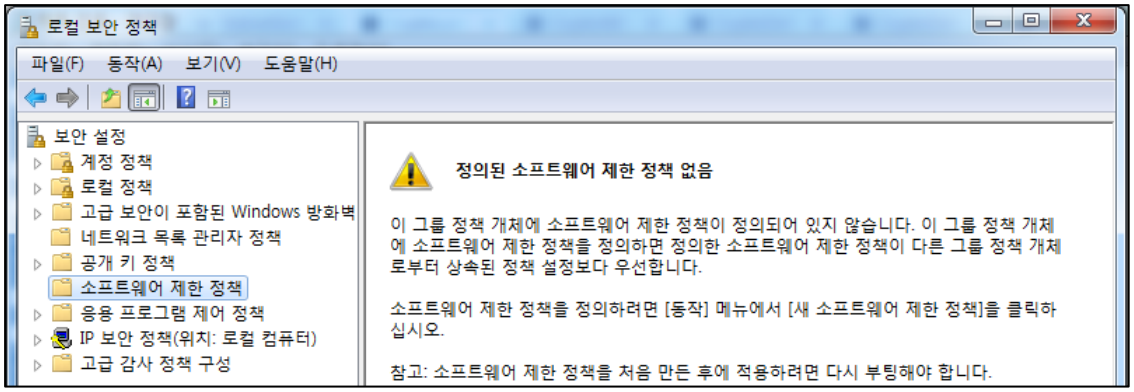


2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:00	[redacted].zip	₩Users₩[redacted]₩Desktop₩[redacted].zip	File_Closed, File_Deleted
2014-04-04 13:34:30	내 Outlook 데이터 파일(1).pst	₩Users₩[redacted]₩Documents₩Outlook 파일₩내 Outlook 데이터 파일(1).pst	File_Closed, File_Deleted

Countermeasure

감염 전 대응 방안

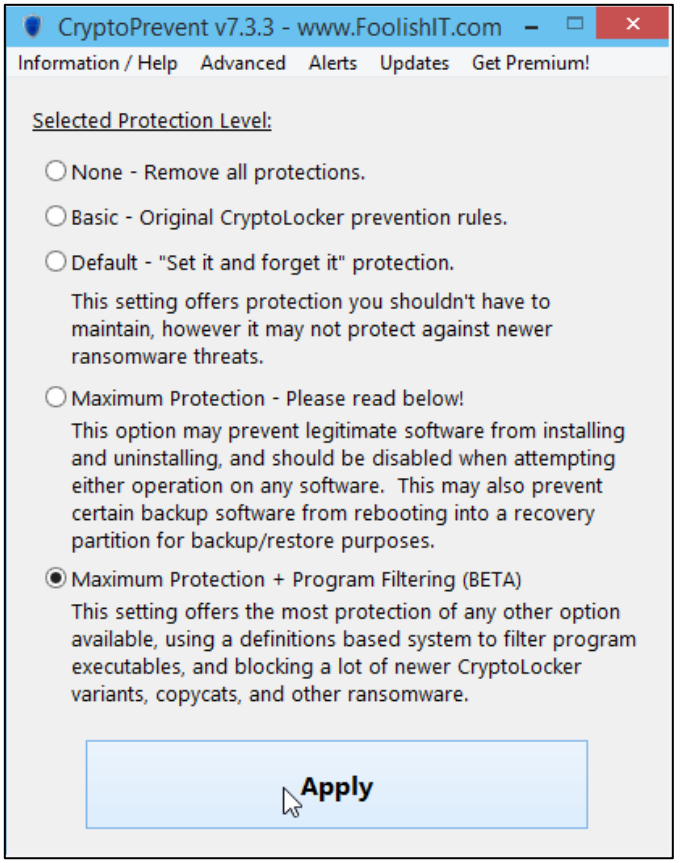
- **Software Restriction Policies**



- 특정 경로에서 파일이 실행되는 것을 막음
- 설정 예
  - ✓ Block CryptoLocker executable in %AppData%
    - Path: %AppData%₩*.exe
    - Security Level: Disallowed
    - Description: Don't allow executables to run from %AppData%.
  - ✓ Block CryptoLocker executable in %LocalAppData%
    - Path if using Windows XP: %UserProfile%₩Local Settings₩*.exe
    - Path if using Windows Vista/7/8: %LocalAppData%₩*.exe
    - Security Level: Disallowed
    - Description: Don't allow executables to run from %AppData%.

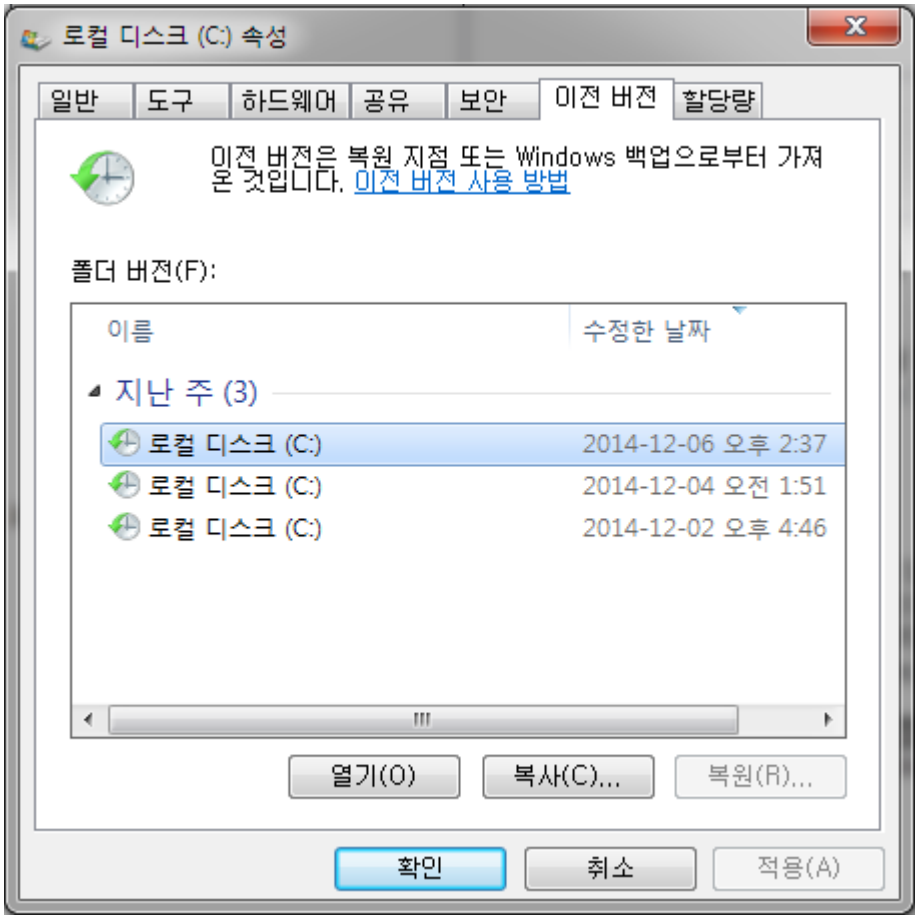
감염 전 대응 방안

- **Software Restriction Policies(계속)**
  - CryptoPrevent(https://www.foolishit.com/vb6-projects/cryptoprevent/)
    - ✓ 소프트웨어 제한 정책 자동 설정
    - ✓ 화이트리스트 필터링



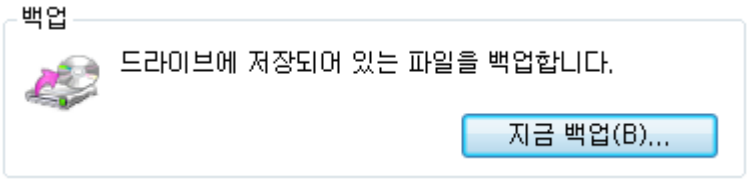
감염 후 대응 방안 : 시스템 & 파일 시스템

- **Volume Shadow Copy 를 통한 복구**
  - 특정 날짜의 상태로 시스템 상태 복원
  - 시스템 볼륨을 기본 설정 되어 있음



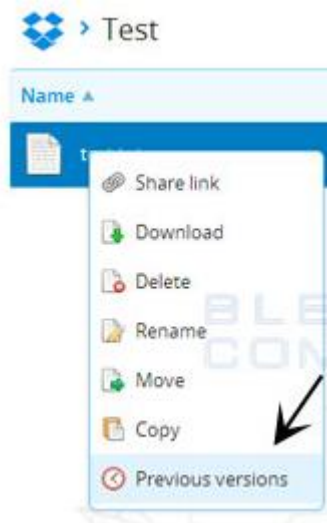
감염 후 대응 방안 : 시스템 & 파일 시스템

- **Windows Backup 기능 사용**
  - 사용자가 미리 생성해 놓은 디스크 백업으로 복구



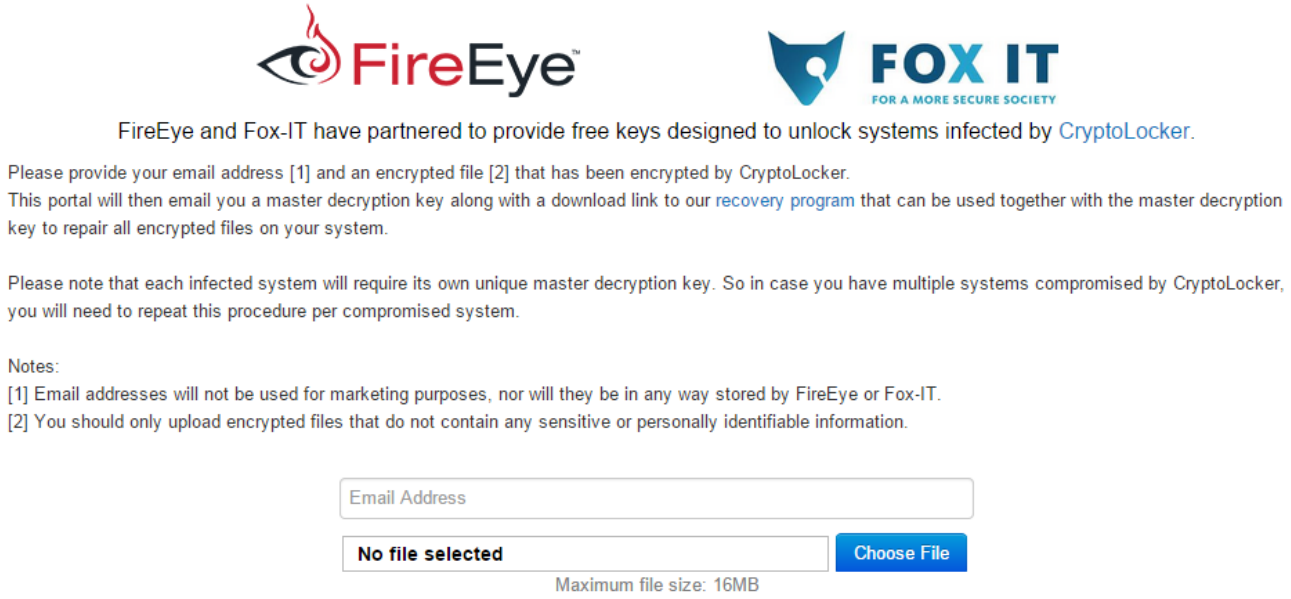
- **파일 복구 도구 사용**
  - CryptoWall, CTB Locker, CoinVault 의 경우, 원본 파일을 복사하고 복사한 파일을 암호화(원본 파일을 삭제함)
  - 삭제된 원본 파일을 파일 복구 프로그램을 통해 복구함(CrptoWall2 에서는 원본 파일을 완전 삭제)

- **DropBox 폴더 복구**
  - 드라이브 맵핑 기능을 Dropbox에서 사용하고 있었다면 "이전 버전" 기능을 통해 복구



감염 후 대응 방안 : 복구 서비스

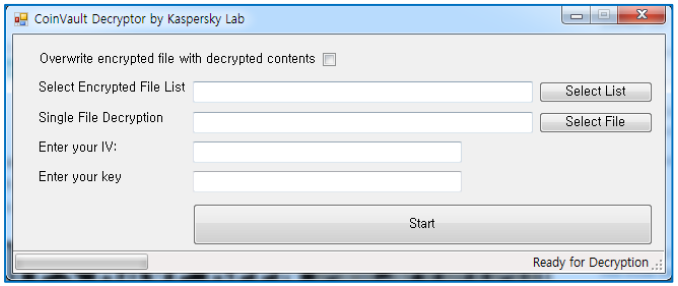
- **CryptoLocker 감염 파일 복구**
  - Operation Torva 수행 중에 CrptoLocker Decryption key 들이 발견됨
  - FireEye, FoxIT 가 합작하여 복구 서비스 제공
  - 복구 사이트 (https://www.decryptcryptolocker.com/)



감염 후 대응 방안 : 복구 서비스

- **CoinVault 감염 파일 복구 방안(4월 13일)**
  - 최근 NHTCU(National High Tech Crime Unit of Netherlands'police) 와 Netherlands' National Prosecutors Office 그리고 Kaspersky 가 공동으로 수사하여 CoinVault C&C 서버를 확보, IV, Private Key 획득
  - 복화키 검색 사이트를 통해 암호화된 파일의 IV, Private Key 검색 가능
    (https://noransom.kaspersky.com/?utm_source=securelist&utm_medium=text&utm_campaign=com-securelist)

  - 복호화 도구 (https://noransom.kaspersky.com/static/kaspersky-coinvault-decryptor.exe)



감염 후 대응 방안 : 제작자의 실수 or 버그

- **CryptorBit 감염 파일 복구**
  - 파일의 헤더 첫 512 byte 만 암호화함
  - 해당 파일 포멧의 원래 헤더를 복구해주면 파일 복원 가능
  - 복구 프로그램 : DecrypterFixer(http://download.bleepingcomputer.com/cryptorbit/Anti-CryptorBitV2.zip)

감염 후 대응 방안 : 제작자의 실수 or 버그

- **CryptoDefense 감염 파일 복구**
  - 2014년 4월 1일 이전 버전에서는 개발자의 실수로, 암호화 시 사용되는 Private Key 가 시스템에 남아 있음
    - ✓ %appdata%₩Microsoft₩Crypto₩RSA
  - 시스템에 남아 있는 Private Key 를 통해 파일 복호화 가능
  - 복구 도구 : Emsisoft Decrypter(http://tmp.emsisoft.com/fw/decrypt_cryptodefense.zip)

감염 후 대응 방안 : 제작자의 실수 or 버그

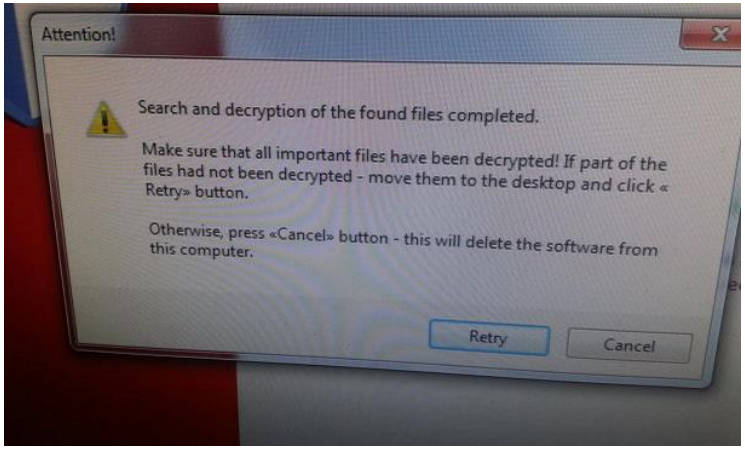
- **TeslaCrypt 감염 파일 복구 방안**
  - AES 방식(CBC Mode)으로 파일 암호화(RSA-2048 로 암호화 했다고 사기침;;)
  - %APPDATA% 경로에 키 파일(key.dat) 파일 생성
  - 복호화 알고리즘
    - ✓ key.dat 파일 내 0x177~0x197 데이터(0x20)를 SHA256 연산한 값이 AES 키 값임
    - ✓ IV 값은 감염된 파일의 첫 16바이트

```
# read_key: 'key.dat' 에서 읽은 값
read_key = KeyBuff[0x177:0x197]
# SHA256 변환
h = SHA256.new()
h.update(read_key)
# aes_key: 실제 복원시 사용되는 AES Key
aes_key = h.digest()

# iv_key: '*.ecc'에서 읽은 값
iv_key = EncBuff[:16]
# aes_key, iv_key 를 이용한 복호화
obj = AES.new(aes_key , AES.MODE_CBC, iv_key)
# enc_data: '*.ecc'에서 읽은 값
enc_data  = encbuff[20:]
dec_data = obj.decrypt(enc_data)
```

  - 자세한 내용은 : http://asec.ahnlab.com/1032

감염 후 대응 방안 : 최후의 수단

- **돈 지불하고 복구!!!**
  - Crypto Locker 복구 경험담(http://kinlife.tistory.com/entry/%EC%A7%80%EC%98%A5%EC%9D%98-%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C-%ED%81%AC%EB%A6%BD%ED%86%A0%EB%9D%BD%EC%BB%A4Cryptolocker-%EA%B2%B0%EC%A0%9C%ED%95%98%EB%A9%B4-%EC%96%B4%EB%96%BB%EA%B2%8C-%EB%90%A0%EA%B9%8C)
  - $300 결제 후, 복구 성공...ㄷㄷ



Conclusion

Conclusion

- **Crypto-Ransomware**
  - 사용자 시스템의 파일을 암호화하고 금전적 대가를 요구
  - 자기 자신을 숨기는데 관심 없음

- **Crypto-Ransomware's Evolution**
  - C&C 통신 : HTTP ➔ HTTPS or TOR
  - 암호화 방식 : Win Crypt API ➔ OpenSSL Library
  - 대상 파일 : 8 formats ➔ more 200 formats and Targeting Enterprise User
  - 지불 방식 : Prepaid Card ➔ Bitcoin

- **Countermeasure**
  - Software Restriction Policies 설정
  - Volume Shadow Copy, Windows Backup 기능, 파일 복구 프로그램, Dropbox ….
  - 보안 업체에서 제공하는 복구 서비스/프로그램 이용
  - UAC 활성화
  - 정기적인 백업 및 외장 디스크의 연결 해제

Question and Answer