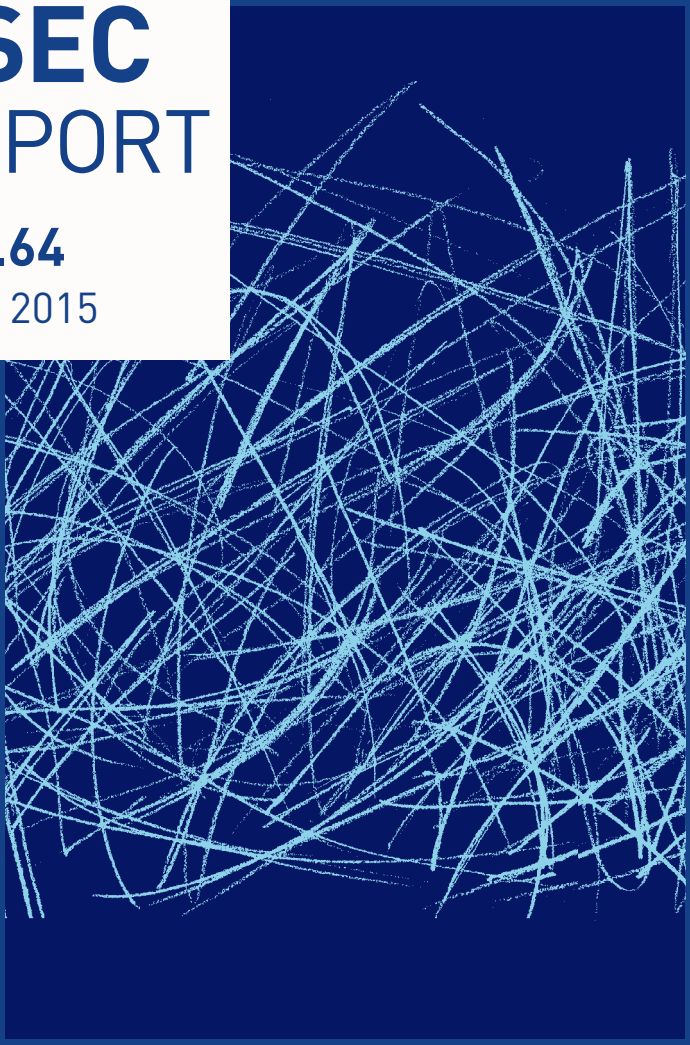
Security Trend

# ASEC REPORT

## VOL.64

April, 2015



AhnLab

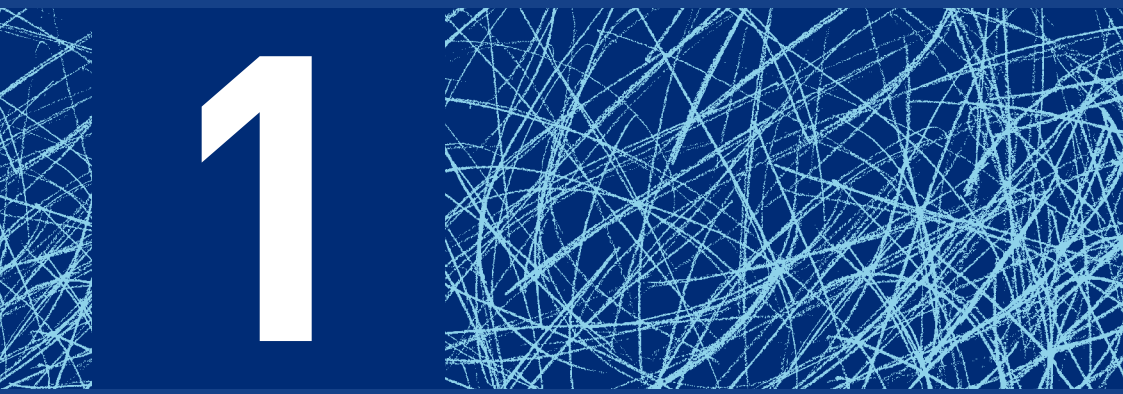
# ASEC REPORT

**VOL.64** April, 2015

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다

## 2015년 4월 보안 동향

Table of Contents



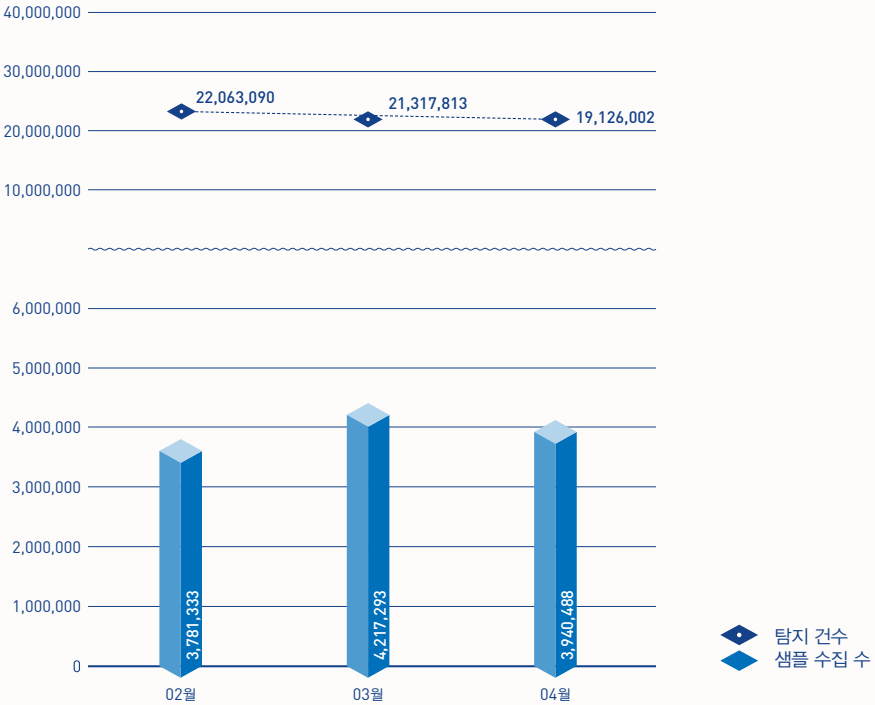
# 1

# 보안 통계
# STATISTICS

# 01
# 악성코드 통계

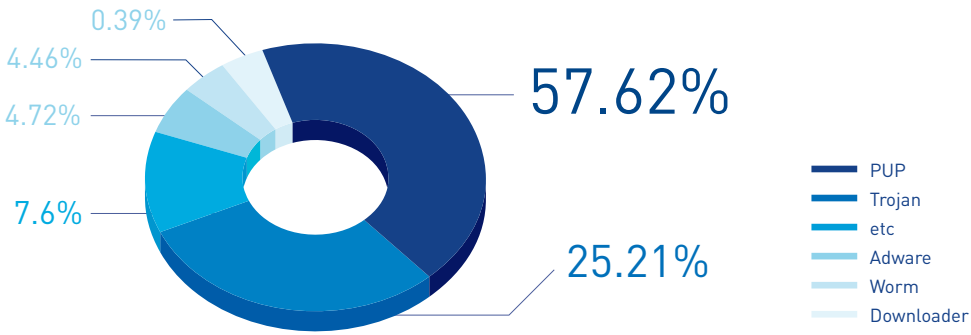
ASEC이 집계한 바에 따르면 2015년 4월 한 달간 탐지된 악성코드 수는 1,912만 6,002건이다. 이는 전월 2,131만 7,813건에 비해 219만 1,811건 감소한 수치다. 한편 4월에 수집된 악성코드 샘플 수는 394만 488건이다.

[그림 1-1]에서 '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.




[그림 1-1] 악성코드 추이(2015년 2월 ~ 2015년 4월)

[그림 1-2]는 2015년 4월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 57.62%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 25.21%, 애드웨어(Adware)가 4.72%로 그 뒤를 이었다.




[그림 1-2] 2015년 4월 주요 악성코드 유형

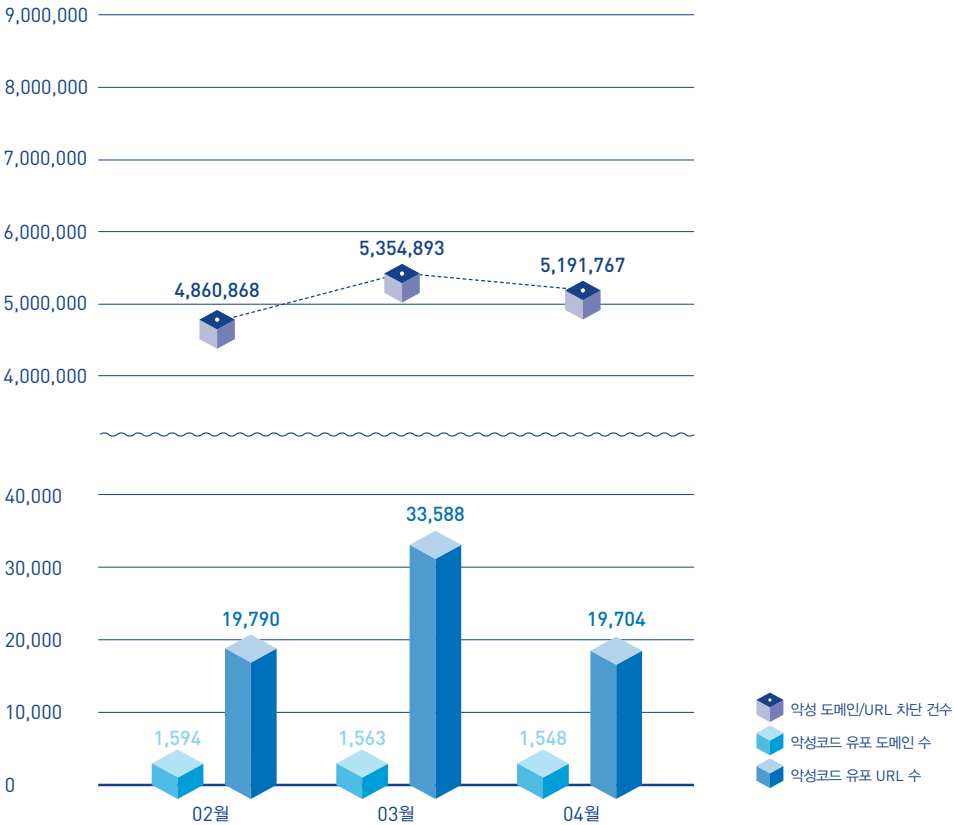
[표 1-1]은 4월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.BrowseFox가 총 186만 5,187건으로 가장 많이 탐지되었고, PUP/ Win32.MywebSearch가 180만 9,795건으로 그 뒤를 이었다.

[표 1-1] 2015년 4월 악성코드 탐지 최다 10건(진단명 기준)

| 순위 | 악성코드 진단명 | 탐지 건수 |
|---|---|---|
| 1 | PUP/Win32.BrowseFox | 1,865,187 |
| 2 | PUP/Win32.MyWebSearch | 1,809,795 |
| 3 | PUP/Win32.MicroLab | 1,482,437 |
| 4 | PUP/Win32.Enumerate | 834,002 |
| 5 | PUP/Win32.Helper | 774,611 |
| 6 | PUP/Win32.CrossRider | 435,549 |
| 7 | PUP/Win32.SubShop | 403,861 |
| 8 | PUP/Win32.InClient | 401,272 |
| 9 | Trojan/Win32.Gen | 353,537 |
| 10 | PUP/Win32.Generic | 352,268 |

# 02
# 웹 통계

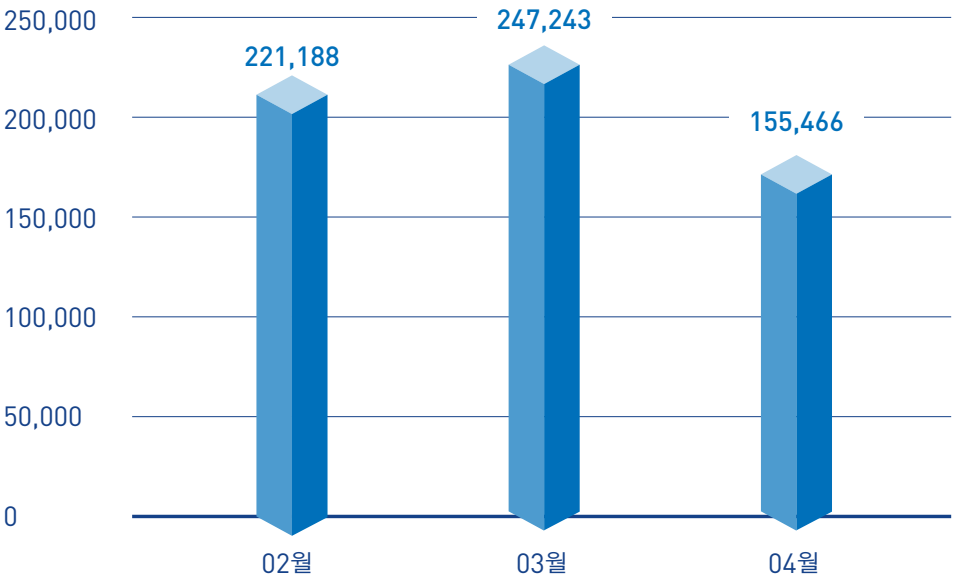
2015년 4월 악성코드 유포지로 악용된 도메인은 1,548개, URL은 1만 9,704개로 집계됐다. 또한 4월의 악성 도메인 및 URL 차단 건수는 총 519만 1,767건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트의 접속을 차단한 수이다.




[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 2월 ~ 2015년 4월)

# 03
# 모바일 통계

2015년 4월 한 달간 탐지된 모바일 악성코드는 15만 5,466건으로 집계됐다.

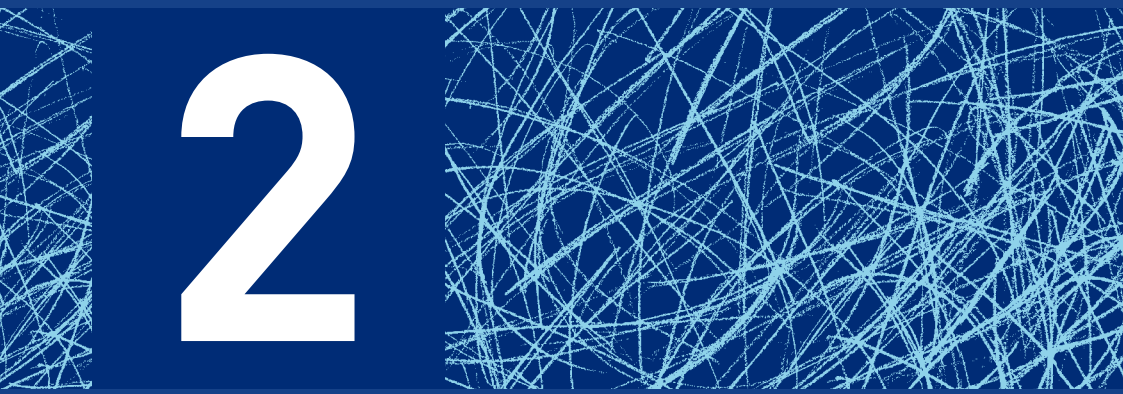



[그림 1-4] 모바일 악성코드 추이(2015년 2월 ~ 2015년 4월)

[표 1-2]는 4월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SMSReg가 지난 3월에 이어 가장 많이 발견되었다.

[표 1-2] 2015년 4월 유형별 모바일 악성코드 탐지 상위 10건

| 순위 | 악성코드 진단명 | 탐지 건수 |
|---|---|---|
| 1 | Android-PUP/SMSReg | 66,134 |
| 2 | Android-PUP/Dowgin | 11,303 |
| 3 | Android-Trojan/FakeInst | 10,701 |
| 4 | Android-PUP/Noico | 10,127 |
| 5 | Android-PUP/Airpush | 6,136 |
| 6 | Android-Trojan/SmsSpy | 3,916 |
| 7 | Android-Trojan/Opfake | 3,352 |
| 8 | Android-Trojan/SmsSend | 2,983 |
| 9 | Android-PUP/Chepa | 2,318 |
| 10 | Android-PUP/Wapsx | 2,193 |



# 2

# 보안 이슈
# SECURITY ISSUE

# 01 DDoS 기능을 포함한 랜섬웨어, 크립토락커

국내 인터넷 사용자를 노린 랜섬웨어가 인터넷 커뮤니티 사이트에서 유포되었다. 러시아, 동유럽 국가 등에서 등장한 랜섬웨어는 서유럽, 미국 등으로 확산되어 피해자가 많았다. 최근 몇 년 사이 국내에서도 랜섬웨어에 감염된 사용자가 증가했으며, ASEC리포트에서는 랜섬웨어 악성코드 감염 예방법(Tip) 등을 소개한 바 있다.

랜섬웨어(Ransomware)란,
Ransom(몸값)과 Software(소프트웨어) 두 단어가 합쳐져 생성된 용어로, PC에 있는 중요한 자료들을 암호화하여 사용하지 못하게 한다. 암호화된 파일을 복구하려면 피해자에게 돈을 지급하도록 강요하는 악성코드이다.

이번에 발견된 랜섬웨어 크립토락커(CryptoLocker)는 국내 유명 커뮤니티 사이트를 통해 유포되었다. 크립토락커는 사용자 PC의 IP 대역을 확인하여 해당 국가의 언어로 페이지를 생성했다. 한글로 보이기 때문에 국내 피해자가 더욱 많았을 것으로 추정된다.

크립토락커는 [그림 2-1]과 같이 2013년 9월 처음 발견되었으며, '크립토월(CryptoWall)', '토렌트락커(TorrentLocker)', '크립토그래픽락커(CryptographicLocker)', '테슬라크립트(TeslaCrypt)' 등의 이름으로 변형들이 계속해서 나타났다. 주로 이메일을 통해 유포되던 랜섬웨어가 이번에는 국내 인터넷 커뮤니티 사이트에서 유포되었는데 크립토락커는 과거 발견된 랜섬웨어와 같은 종류이다.

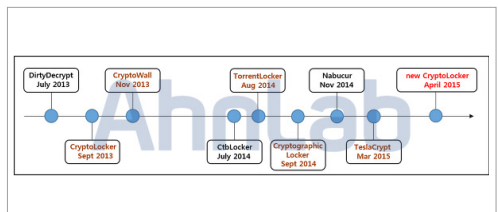



그림 2-1 | 랜섬웨어 타임라인

랜섬웨어에 감염되면 [그림 2-2]와 같은 페이지가 나타난다. 암호화된 파일들을 복원하기 위해 한화 약 43만 8,900원의 비트코인(BitCoin)을 요구한다. 피해자들이 비용 지급을 쉽게 할 수 있도록 결제 방법을 상세하게 설명하고 있으며, 실제 복원됨을 증명하기 위해 암호화된 파일 중 1개의 파일을 무료로 복호화해준다. 이를 통해 악성코드 제작자는 중요한 파일을 암호화하여 사용자에게 금전을 요구한다.

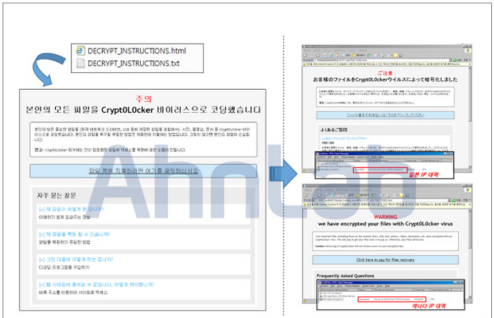



그림 2-2 | 크립토락커 감염 시 보이는 웹 페이지

그리고 사용자 PC의 IP 대역을 확인하여 해당 국가에 맞는 언어로 안내 페이지를 생성하고 실행하여 보여준다. 결제를 진행하기 위해 안내된 링크를 클릭하면 다음과 같은 정보가 기본으로 세팅되어 있다. 토르(Tor), 즉 익명의 네트워크(anonymity network)를 사용하여 네트워크 추적을 어렵게 하였다.

(예제)
http://zoqowm4kzz4cvvvl.torlocator.org/jxt85f9.php
- User-Code : 12lrne9
- User-Pass : 8394

### 1. 감염 경로

[그림 2-3]과 같이 크립토락커의 감염은 사용자 시스템의 취약점을 이용한 전형적인 웹 기반의 DBD(Drive-By-Download) 방식을 통해 이루어졌다. 국내에서 많은 사용자를 보유하고 있는 유명 커뮤니티 사이트에 접속하면 취약한 사이트로 리다이렉션(Redirection)되면서 특정 취약점에 의해 랜섬웨어가 다운로드 및 실행된다.

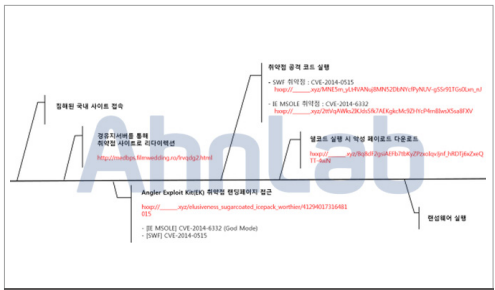



그림 2-3 | 랜섬웨어 감염 경로

#### 1) 최초 유포지 및 경유지

이번 크립토락커 배포에는 국내 3곳의 대표적인 IT 커뮤니티 사이트가 악용되었다.

(1) C 업체
(2) S 업체
(3) R 업체

이들 국내 사이트에는 광고 데이터를 동적으로 받아서 화면에 보여주는 기능이 포함되어 있다. 공격자는 이 기능을 악용하여 [그림 2-4]와 같이 광고 서버에 악의적인 스크립트를 삽입하거나 또는 직접 사이트를 변조하는 방법으로 사용자들이 인지하지 못한 채 악의적인 사이트로 연결되도록 유도하였다.


그림 2-4 | C 업체에 삽입된 악성스크립트

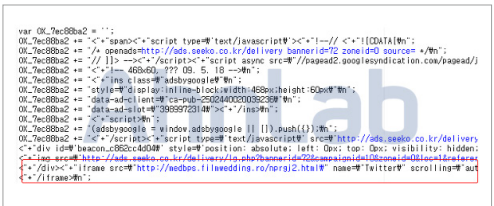


그림 2-5 | S 업체에 삽입된 악성스크립트

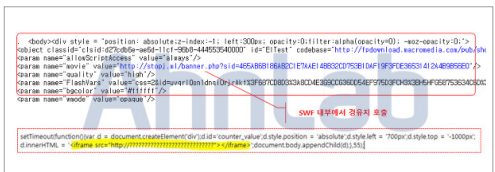


그림 2-6 | R 업체에 삽입된 악성스크립트(SWF 이용)

특히, 삽입된 악성 스크립트들은 경유지 사이트를 거쳐 최종적으로 취약점 공격코드가 탑재된 사이트로 연결된다. 이때 사용자 클라이언트 시스템 상의 취약점을 이용하기 위해 자동화된 웹 공격 툴킷인 '앵글러 EK(Angler Exploit Kit)'가 사용되었다.

### 2) 자동화된 웹 공격 툴킷 - 앵글러 EK

[그림 2-7], [그림 2-8]과 같이 크립토락커에 감염되면 사용자는 최종적으로 난독화된 앵글러 EK의 취약점 랜딩페이지로 연결된다.

그림 2-7 | 앵글러 EK로 난독화된 취약점 랜딩페이지

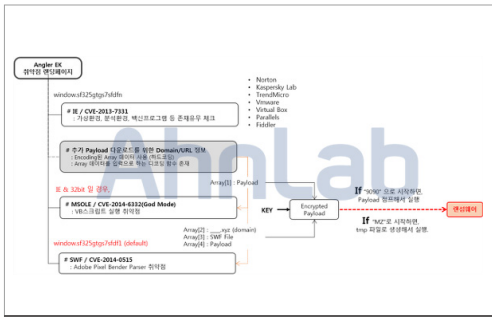


그림 2-8 | 앵글러 EK 동작구조

이때 악성코드의 탐지 우회 기능과 유사하게 스크립트 레벨에서도 취약점 'CVE-2013-7331'을 이용하여 가상 환경, 분석 환경, 백신 프로그램 등의 클라이언트 환경을 체크한다. 만약, 해당 프로그램들이 존재하면 정상으로 공격이 이루어지지 않는다.

또한, [표 2-1]과 같이 특유의 변수를 이용하여 개별 애플리케이션들의 공격 여부를 제어한다.

표 2-1 | 애플리케이션 제어 변수

| 애플리케이션 | 변수 |
|---|---|
| 어도비 플래시 플레이어 | window.sf325gtgs7sfdf1<br>window.sf325gtgs7sfdf2 |
| 마이크로소프트 실버라이트 | window.sf325gtgs7sfds |
| 오라클 자바 | window.sf325gtgs7sfdj |
| 환경 체크 | window.sf325gtgs7sfdfn |

### 3) 취약점 및 페이로드(셸코드)

일반적인 앵글러 EK는 다양한 애플리케이션 취약점을 이용하는 것으로 알려졌다. 그러나 이번 공격에는 '갓모드(God Mode)'로 알려진 'CVE-2014-6332'와 어도비 플래시 플레이어 취약점인 'CVE-2014-0515'가 사용되었다.

| CVE 번호 | CVE-2014-6332(MS14-064) |
|---|---|
| 보안 권고문 | https://technet.microsoft.com/library/security/ms-14-064 |
| 영향 받는 버전 | 마이크로소프트 인터넷 익스플로러(IE) 3.0 이후 모든 버전<br>마이크로소프트 윈도 비스타, 7, 8, 8.1, RT, RT 8.1<br>마이크로소프트 서버 2003, 2008, 2008 R2, 2012, 2012 R2 |

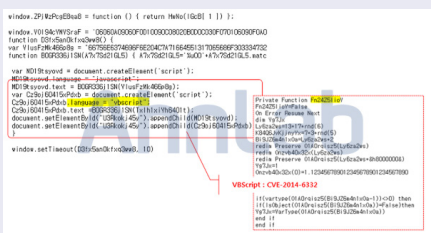


그림 2-9 | CVE-2014-6332 취약점

| CVE Number | CVE-2014-0515(apsb 14-13) |
|---|---|
| 보안 권고문 | https://helpx.adobe.com/security/products/flash-player/apsb14-13.html |
| 영향 받는 버전 | Adobe Flash Player 13.0.0.182 and earlier versions for Windows<br>Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh<br>Adobe Flash Player 11.2.202.350 and earlier versions for Linux |

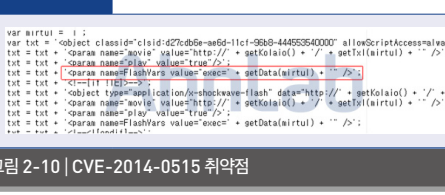


그림 2-10 | CVE-2014-0515 취약점

그림 2-11 | 웹으로부터 전달된 "exec" 파라미터(Base64 인코딩) 처리

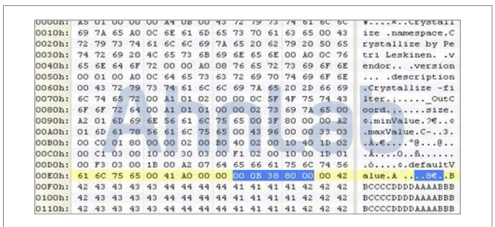


그림 2-12 | CVE-2014-0515 취약점 원인 "픽셀 벤더 바이너리 데이터(Pixel Bender Binary Data)"

그림 2-13 | CVE-2014-0515 취약점 코드

[그림 2-14]와 같이 실제 셸코드 실행 시 공격자 사이트로부터 추가적인 페이로드(Payload)를 다운로드 받는다. 이를 해당 키(KEY) 문자열로 해제한 후 페이로드의 시작이 "9090" 또는 "MZ"인지 구별하여 직접 메모리 상에서 실행하거나 tmp 파일(%temp%폴더)로 생성하여 실행한다.

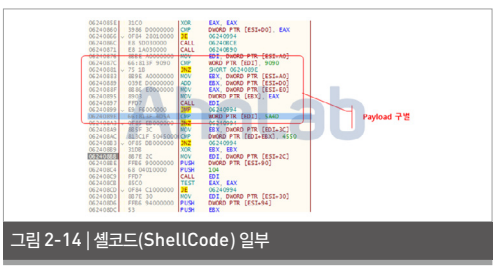



그림 2-14 | 셸코드(ShellCode) 일부

## 2. 기능분석

### 1) 전체 동작 흐름

랜섬웨어가 실행되면 다른 악성코드처럼 자기 자신을 '%WINDOWS%' 폴더에 복사하여 'HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩<랜덤명>'에 등록한다. 해당 키에 실행 파일을 등록해 놓으면 시스템을 재부팅할 때마다 자동 실행된다. 이 경우 해당 파일을 찾아서 삭제하지 않으면 감염된 PC 사용자가 돈을 주고 파일을 복구하더라도 재감염될 가능성이 높다. 랜섬웨어는 자신을 자동 실행으로 등록한 후에는 정상 'explorer.exe' 프로세스를 생성하고 C&C 서버 통신 및 파일을 암호화하는 주요 기능을 포함한 PE 파일을 인젝션(injection)시켜서 동작한다.

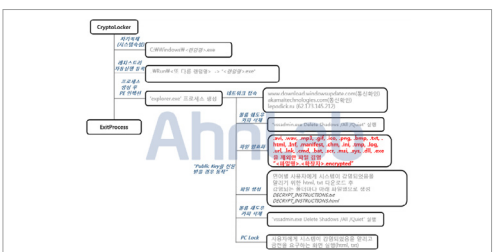



그림 2-15 | 크립토락커 동작 흐름

송한다. 첫 번째는 사용자 PC의 정보를 전달한 후 IP 대역에 따른(나라별)'.txt'와 '.html' 파일을 받아온다. 그리고 두 번째는 앞에서 보낸 정보에 암호화된 파일들을 복호화할 때 필요한 키 정보(256바이트)를 함께 보내고 서버에서 '200 OK' 응답을 받으면 파일들을 암호화하기 시작한다. 서버로부터 받은 'DECRYPT_INSTRUCTIONS.txt'와 'DECRYPT_INSTRUCTIONS.html' 파일은 암호화한 파일이 있는 모든 폴더에 생성되며, 시스템이 감염되었다는 메시지를 사용자에게 보여주고 파일을 정상으로 복원하기 위해 비트코인 결제 방법이 설명되어 있다.

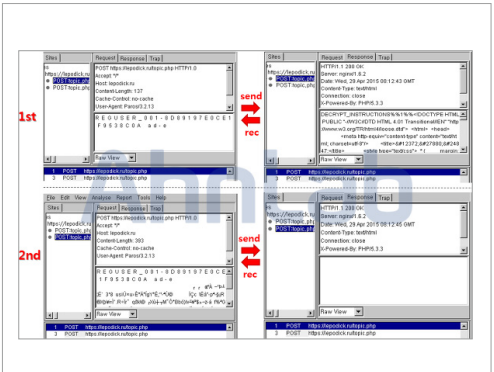



그림 2-16 | C&C 통신 과정

### 2) 세부 내용

a) 네트워크 접속

네트워크 통신 상태를 확인하기 위해 'www.download.windowsupdate.com'과 'akamaitechnologies.com'에 접속한다. 이후 [그림 2-16]과 같이 C&C 서버인 'https://lepodick.ru /topic.php'에 두 번에 걸쳐 'POST' 패킷을 전

b) 볼륨 섀도 카피 삭제

악성코드는 'vssadmin.exe Delete Shadows/All/Quiet' 명령을 실행하여 볼륨 섀도 카피를 삭제한다. 이 경우 윈도 운영체제에서 제공하는 파일 백업 및 복원 기능을 정상적으로 이용할 수 없다. 이 명령은 크립토락커 류에서 공통적으로 확인할 수 있는 기능이다.

c) 파일 암호화

랜섬웨어의 가장 특징적인 기능은 사용자의 중요 파일들을 암호화하는 것이다. [표 2-2]의 목록에 있는 확장자를 가진 파일과 폴더는 암호화 대상에서 제외된다. 암호화 대상 파일은 이동식 드라이브와 네트워크 드라이브에 있는 파일이며 암호화가 완료된 파일의 확장자 뒤에는 '.encrypted' 문자열이 붙는다.

표 2-2 | 파일 암호화에 제외된 확장자와 폴더

**[제외 대상 확장자]**

.avi, .wav, .mp3, .gif, .ico, .png, .bmp, .txt, .html, .inf, .manifest, .chm, .ini, .tmp, .log, .url, .lnk, .cmd, .bat, .scr, .msi, .sys, .dll, .exe

**[제외대상 폴더]**

- %Program Files%
- %ProgramW6432%
- C:₩WINDOWS
- C:₩Documents and Settings₩All Users₩Application Data
- C:₩Documents and Settings₩사용자계정₩Application Data
- C:₩Documents and Settings₩사용자계정₩Local Settings₩Application Data
- C:₩Documents and Settings₩사용자계정₩Cookies
- C:₩Documents and Settings₩사용자계정₩Local Settings₩History
- C:₩Documents and Settings₩사용자계정₩Local Settings₩Temporary Internet Files

[표 2-2]의 암호화 대상 제외 확장자 및 폴더를 제외하고는 파일 외형적으로는 [그림 2-17]과 같이 파일의 확장자에 '.encrypted'가 추가된 것을 확인할 수 있다. 이렇게 암호화된 파일 내부에는 변경된 원본 데이터와 시그니처 그리고 복호화에 필요한 256바이트 공개키가 포함되어 있다.

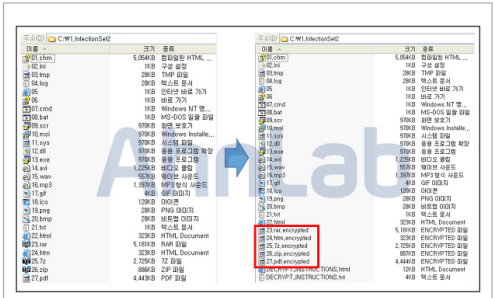


그림 2-17 | 감염 전(좌)/ 감염 후(우)의 변경된 파일명

### 3. 복구 프로그램

최근 이슈가 된 크립토락커의 복구 프로그램은 내부에 감염된 사용자별로 다른 복호화 키 인덱스 정보(0x20바이트)를 포함하고 있다. 실행 시 [그림 2-18]과 같은 화면이 나타나며 "Start Decryption" 버튼을 클릭하면, 감염 조건에 부합하는 드라이브 및 폴더에 대한 스캔과정을 수행한다. ".encrypted" 확장자를 갖는 파일들에 대해 실제 복호화 작업이 진행되는 것을 확인할 수 있다.

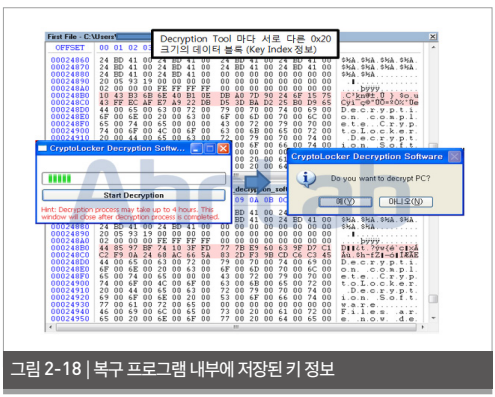



그림 2-18 | 복구 프로그램 내부에 저장된 키 정보

이때 ".encrypted" 로 암호화된 파일은 공통적으로 원래 파일 크기에 0x108(264바이트)이 증가한 것

을 알 수 있다. 파일 끝에 추가된 0x108 크기의 데이터는 다음과 같은 구조를 갖는다.

증가한 264바이트 = 해시 정보(4바이트) + 시그니처(4바이트) + 공개키(256바이트)

[그림 2-19]는 실제 복구툴 내부에 저장된 키 인덱스 정보(0x20바이트)를 통해 생성된 데이터(0x108 바이트)를 ".encrypted" 파일에 존재하는 해시 정보와 비교해 유효한 키인지 검증하는 과정이다.

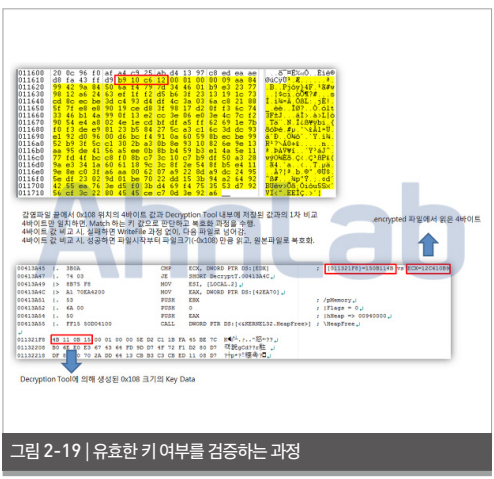


그림 2-19 | 유효한 키 여부를 검증하는 과정

이러한 랜섬웨어는 변종이 다양하다. 그중 DDoS 공격 기능이 포함된 변종도 발견되고 있다. 엑셀 아이콘 모양으로 제작된 악성코드(a.exe)를 실행하면 [그림 2-20]의 ②와 같이 "explorer.exe" 프로세스가 실행되며, 해당 프로세스 메모리에 랜섬웨어 기능의 실행 파일이 인젝션(Injection)되어 동작하는 것을 알 수 있다. 해당 랜섬웨어는 국내 커뮤니티 사이트인 C 업체 배너광고를 통해 유포된 것과 동일한 형태이며, tidisow.ru 사이트에 접속을 시도한다.

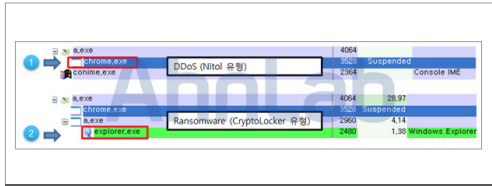



그림 2-20 | 악성 기능별 인젝션 대상 프로세스

- DDoS 기능

기존에 알려진 랜섬웨어 기능 외에 해당 샘플은 DDoS 공격 기능의 실행 파일을 구동하는 특징이 있다. 구체적인 DDoS 공격 방식은 '니톨(Nitol)'이라는 이름으로 알려진 악성코드와 동일하며, 아래의 C&C 주소와의 통신을 통해 공격자의 명령에 따라 파일을 다운로드하고 DDoS 기능을 수행한다.

- b.googlex.me (Port: 22, 23, ...)

[그림 2-21]은 공격자의 명령에 의해 DDoS 공격이 발생하는 부분을 나타내며, DDoS 기능 관련 스레드(Thread)가 반복적으로 생성되는 구조를 보여주고 있다.

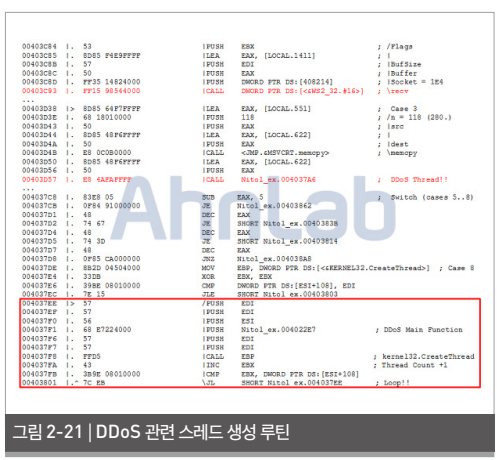


그림 2-21 | DDoS 관련 스레드 생성 루틴

[그림 2-22]는 DDoS 공격 시 사용되는 다양한 HTTP 메시지 내용이다.

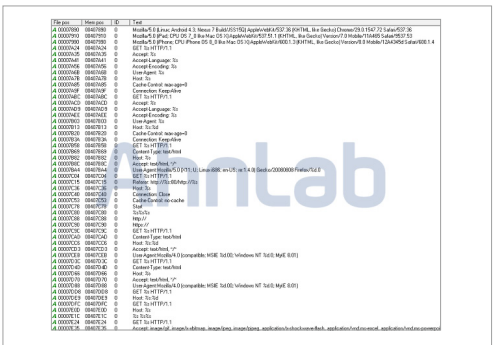


그림 2-22 | DDoS 공격 시 사용되는 HTTP 메시지

DDoS 공격 방식은 랜섬웨어 동작 방식과 유사하게 악성 행위를 하는 실행 파일이 별도의 파일 형태로 생성되는 구조가 아닌, 정상 프로세스 실행 및 인젝션(Injection)을 통해 동작하여 파일 기반의 진단을 우회한다.

또한, 인젝션 대상이 되는 프로세스는 감염 시스템 아래의 레지스트리 정보를 통해 얻은 웹 브라우저이며, 테스트 시스템에서는 'chrome.exe'가 기본 웹 브라우저로 설정되어 있어 [그림 2-20]의 ①과 같이 chrome.exe가 실행됨을 알 수 있다.

- HKCR₩http₩shell₩open₩command

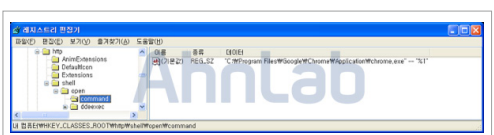


그림 2-23 | 인젝션 대상 웹 브라우저 정보

해당 악성코드가 생성하는 뮤텍스 정보는 다음과 같다.

- "qazwsxedc" (고정)

최초 C&C 주소와 통신할 때 공격자에게 전송되는 정보는 아래 API 호출을 통해 얻는다(최종 전송 시, XOR을 통해 암호화되어 전송).

- KERNEL32.GetComputerNameA
- KERNEL32.GetLocaleInfoW
- ADVAPI32.RegOpenKeyExA ("HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion")
- ADVAPI32.RegQueryValueExA ("ProductName", "ProcessorNameString")
- KERNEL32.GlobalMemoryStatusEx
- KERNEL32.GetSystemInfo

[그림 2-24]와 같이 안티-VM 기능으로 C&C 접속 전 30분 간의 Sleep()을 수행하며, GetTickCount API를 이용하여 정상적으로 30분간 Sleep()을 수행하였는지 여부를 체크하는 코드가 존재한다.

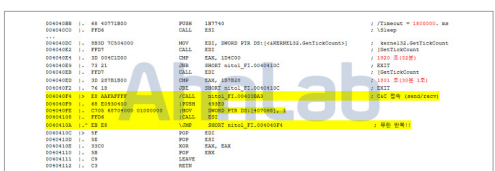


그림 2-24 | 30분 Sleep() 정상 수행 여부 체크

## 4. 결론

이번 크립토락커는 국내 유명 커뮤니티 웹사이트의 광고 배너를 통해 유포되면서 피해자가 많았다. 이에 웹 관리자는 보안에 대한 주의가 필요하며 PC 사용자는 랜섬웨어 예방을 위해 발신자가 불명확한 이메

일 열람에 주의해야 한다. 중요한 파일들은 별도로 백업해둘 필요가 있다. 또한 취약점에 의한 감염 피해를 줄이려면 운영체제와 응용프로그램을 항상 최신 버전으로 유지하는 것이 필요하다. 이 외에도 백신프로그램을 통해 예방할 수 있는데 V3에서는 해당 악성코드를 'Win-Trojan/Cryptolocker.229892', 'Win-Trojan/Cryptolocker.Gen', 'Trojan/Win32. Cryptolocker' 등으로 진단하고 있으며 현재까지 파악된 관련 악성 경유지 및 유포지를 아래와 같이 확보하였다.

한편, ASEC 리포트 이번 호의 상세 분석에서는 최근 유포되고 있는 랜섬웨어 Top 6에 대해 다루고 있다.

[경유지]
- medbps.filmwedding.ro/bkktab2.html (gtdgq2.html, lrvqdg2.html, nprgj2.html)
- guhm.gusg.com.br/pzvjqn2.html
- aker.ktc66.com/tpgop2.html
- lub.liuboya.com/xzrwqh2.html (wvbrrd2.html, gibusn2.html, jibnnm2.html, lxhufq2.html, ubodwx2.html)
- lab.lamo.ro/tpgop2.html

[유포지]
- row.bottomwebsites.xyz/elusiveness_sugarcoated_icepack_worthier/41294017316481015
- gate.moneyslistsarea.xyz/dynasty_sunset_trepidation_guitarists/65630335056125154
- gate.nothaveillinous.xyz/tyrant_absolves_pimply_casualness/16752510507522986
- gate.nothaveillinous.xyz/shirked_edison_gatehouses_springier/47090670725834176

[C&C]
- lepodick.ru/topic.php
- possoqer.ru/topic.php
- koposorer.ru/topic.php
- wosowpe.ru/topic.php

# 02 음악 앱으로 위장한 원격제어 악성코드

음악 애플리케이션으로 위장한 악성 앱이 원격제어 공격에 이용되어 주의가 요구된다.

악성 애플리케이션은 구글 플레이 스토어(Google Play Store) 및 서드파티 앱 스토어(Third Party App Store)를 통해 유포되었다.

그림 2-25 | 구글 플레이 스토어(좌) / 서드파티 앱 스토어(우)
출처 : <ElevenPaths blog> El mes de la RATa en Google Play

서드파티 앱 스토어에서 앱을 설치하면 [그림 2-26]과 같이 개인정보, 요금이 부과되는 서비스, 위치, 메시지 등에 접근할 수 있는 권한을 요구한다. 정상 음악 스트리밍 애플리케이션과 비교해보면 악성 앱에서 요구하는 권한이 더 많다는 것을 알 수 있다.

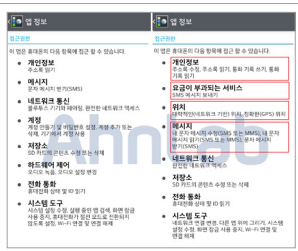


그림 2-26 | 정상 음악 스트리밍 앱(좌) / 악성 음악 스트리밍 앱(우)

[그림 2-27]과 같이 악성 음악 스트리밍 애플리케이션은 사용자의 의심을 피하기 위해 정상적인 음악 스트리밍 애플리케이션의 음악 다운로드, 재생 기능을 갖는다.

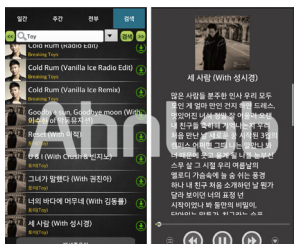


그림 2-27 | 정상 음악 스트리밍 앱 기능

악성 앱의 음악 정보 추출은 중국의 모 음악사이트를 이용한다.

그림 2-28 | 음악 정보 요청

악성 앱은 원격제어 공격을 위해 중국의 클라우드, 검색 포털 사이트 바이두의 푸시 서비스를 이용하였다. 이 푸시 서비스를 사용하여 공격자는 스마트폰에 저장된 연락처, 문자 메시지, 사진 등 개인정보를 공격자의 서버에 전송할 수 있다.

그림 2-29 | 공격자의 바이두 클라우드 접근 키

그림 2-30 | 스마트폰 정보 수집 명령

그림 2-31 | 위치 정보 수집 명령

그림 2-32 | 문자 메시지 정보 수집 명령

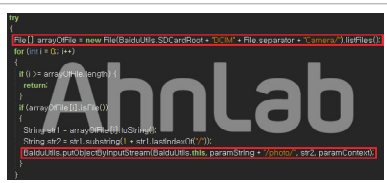


그림 2-33 | 사진앨범 수집 명령

또한, 다운로드 명령을 내려서 추가적인 악성 앱을 다운로드 및 실행하게 할 수 있다.

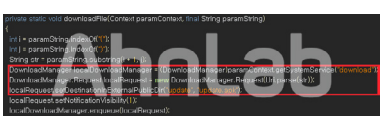


그림 2-34 | 다운로드 명령

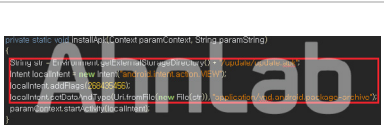


그림 2-35 | 앱 설치 명령

사용자가 보기에는 정상 애플리케이션의 기능을 하지만, 원격제어를 통해 개인정보가 유출될 수 있다. 또한, 추가적인 악성 애플리케이션이 설치되어 피해가 발생할 수 있다.

이러한 악성 앱의 피해를 예방하려면 앱 설치 전에 필요 이상의 과도한 권한을 요구하고 있는지 확인하고 설치하는 습관과, 믿을 수 있는 모바일 백신의 실시간 감시를 활성화하여 사용하기를 권한다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

**<V3 제품군의 진단명>**

Android-Trojan/Fcasino

# 03 스팸메일로 유포되는 'Upatre' 악성코드 기승

전 세계적으로 스팸메일을 통한 악성코드 감염이 문제가 되고 있다.

스팸메일을 통한 악성코드 감염은 메일 본문 내의 링크를 클릭하도록 유도하여 악성 파일을 내려받게 하거나 문서 파일 등으로 가장한 첨부 파일을 실행하도록 유도하여 시스템에 악성코드를 감염시키는 형태를 띠고 있다.

지난 2014년 후반부터는 이러한 '어파트레(Upatre)' 류의 악성코드가 첨부된 스팸메일이 국내에서도 지속해서 대량 유포되고 있어 다시 한 번 스팸메일의 위험성을 강조하고자 한다.

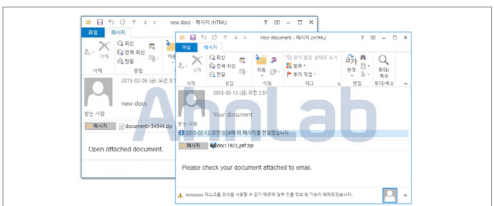


그림 2-36 | 스팸메일 유포 형태

어파트레 류의 악성코드는 변형에 따라 조금씩 다르지만, 공통적으로 다음과 같은 동작을 한다.

- 스팸메일 내 첨부 파일(최초 파일) 실행 시 자기 복제본 생성
- C&C 접속 시도 및 추가 악성코드 다운로드
- 정상 PDF 파일 실행으로 정상처럼 위장
- 지속적인 C&C 통신 및 정보 탈취

이 문서에 다룬 샘플은 최근 접수된 어파트레의 변형으로 'invoice'라는 메일 제목으로 유포되었다. 메일의 첨부 파일에는 [그림 2-37]과 같이 PDF 아이콘으로 위장한 실행 파일 'invoice1212.exe'가 있다.

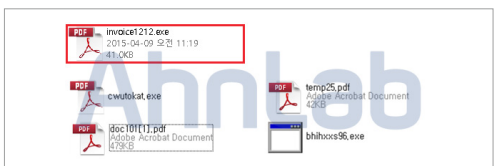



그림 2-37 | 스팸메일 첨부 파일(Dropper) 및 생성 파일(invoice121.exe 외 나머지)

메일에 첨부된 악성 파일 'invoice1212.exe'를 실행하면, [표 2-3]과 같이 파일을 생성하고 C&C 서버로 접속을 시도하여 추가 악성코드를 다운로드한다.

표 2-3 | 생성 파일 목록

| |
|---|
| C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩cwutokat.exe (복사본) |
| C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temporary Internet Files₩Content.IE5₩BR95JRB5₩doc101.pdf (인코딩된 파일) |
| C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩temp25.pdf (정상 PDF) |
| C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩bhihxxs96.exe (디코딩파일) |

그림 2-38 | C&C 서버 연결 정보

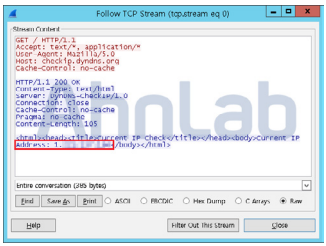



그림 2-39 | IP 주소 확인

감염 후 패킷 정보를 확인하면, [그림 2-39]와 같이 IP 주소를 확인하는 사이트 'checkup.dyndns.org'에 접속하여 감염된 시스템의 IP를 확인한다.

이후 인코딩된 'doc101.pdf' 파일을 [표 2-4]의 주소에서 다운로드를 시도한다.

표 2-4 | 다운로드 주소

| |
|---|
| Electro*****.ro/*****/doc101.pdf (21*.**.**.37:80) |
| electro********.com.**/***/doc101.pdf (66.***.**.28:80) |


그림 2-40 | 정상 PDF 파일 실행 화면

다운로드 시도 후에는 정상 PDF 파일을 실행하여 사용자에게 악성코드에 감염된 사실을 숨긴다.

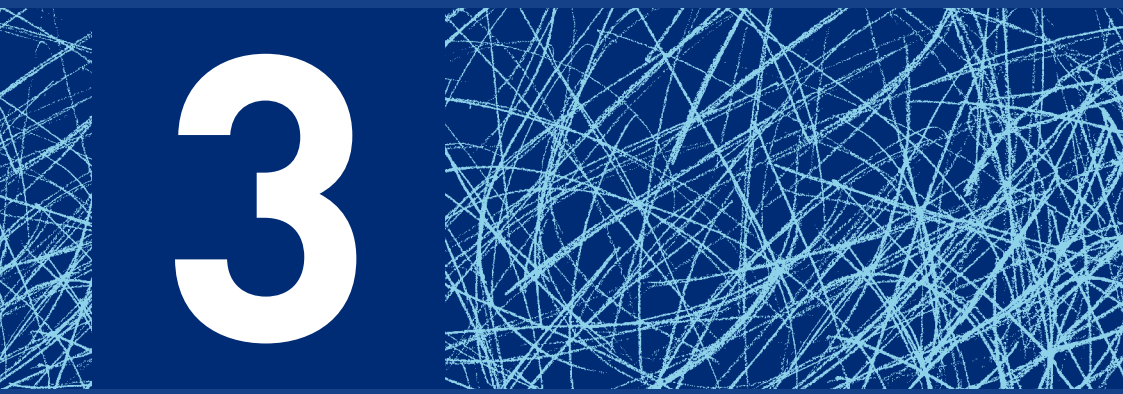
C&C 접속시도 이후 정확한 행위 정보는 확인되지 않았지만, 보통은 금융정보를 탈취하는 '인포스틸러(Infostealer)' 기능을 갖는다. 이러한 스팸메일은 사용자에게 클릭을 유도하기 위해 doc, document, invoice, ticket, photo 등의 문구를 사용하므로 각별한 주의가 필요하다.

어파트레 류의 악성코드 변형은 지속적으로 발견되고 있다. 악성코드 감염을 예방하려면 메일을 열람할 때 위와 같은 문구가 있는지 살펴야 한다. 또한, 위의 문구에 대해 필터링을 설정해둔다면 스팸메일을 통한 악성코드 감염을 대부분 예방할 수 있다. 악성 파일이 첨부된 스팸메일로부터 피해를 최소화하는 방법은 스팸 차단 솔루션으로 스팸메일을 사전에 차단하며, 발신인이 불분명한 메일은 열람하지 않는 것이다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

**<V3 제품군의 진단명>**

Trojan/Win32.Upatre (2015.04.08.01)
Win-Trojan/Agent.516096.EG (2015.04.07.03)
BinImage/Encdata (2015.04.07.05)



# 3

# 악성코드 상세 분석
# ANALYSIS-IN-DEPTH

잔혹한 악의 화신, 랜섬웨어 Top 6

# 잔혹한 악의 화신, 랜섬웨어 Top 6

국내도 랜섬웨어 비상이 걸렸다. 이미 해외에서는 수년 전부터 등장한 공격 수법이었으나 그동안 국내에서는 큰 영향이 없었다. 그러나 최근 랜섬웨어의 일종인 크립토락커(CryptoLocker)의 한글 버전이 국내 웹사이트에서 유포되면서 랜섬웨어에 대한 우려가 높아지고 있다. 이 글에서는 주요 랜섬웨어를 분류해 각각의 특징과 행위를 소개하고자 한다. 분류 및 우선순위는 국내외 이슈 정도(고객사 접수, 보도 기사, 포스팅 등)와 진단 건수를 기반으로 하였으며, 대상 기간은 2014년 10월부터 2015년 3월까지이다.

### 랜섬웨어 Top 6 분류 및 특징

랜섬웨어 가운데 최근 V3 진단 수량에서 많은 비중을 차지하고 기사화 등으로 이슈가 되는 것에 대해 [표 3-1]과 같이 총 6개로 분류할 수 있다. 좀더 넓게 구분하자면 '나부커(Nabucur)'와 그 외의 랜섬웨어 류로 나눌 수 있다. 그 차이의 기준은 나부커는 인코딩한 원본 파일에 감염 코드를 추가해서 정상 파일을 변경하는 방식으로, V3에서는 해당 파일들을 원본 파일로 복원할 수 있다. 반면, 나머지 종류의 랜섬웨어는 RSA나 AES 같은 암호화 기법을 사용하여 원본 파일로 복원하려면 복호화 키가 필요하다. 그리고 실제 동작을 살펴보면 비슷한 부분이 많다는 것을 알 수 있다.

표 3-1 | 주요 랜섬웨어 분류

| | 랜섬웨어의 종류 | MD5 |
|---|---|---|
| 1 | Nsb락커 / 나부커 | 4DDE0233CD956FAA19FF21B3FB73FBBD<br>ED42954A5824A5DD1E579168480191B2<br>770D3BC32F7ACA8F94DD22209532A352<br>19840868F8D20089BA4CE289F48A6A09<br>DC5BAD327EF50D2594F423A1DF7A6C03<br>FF6CAFE7597BD6FF1521A1A1F817D9BF |
| 2 | Ctb로커 / 크리트로니 | DEFB9614AFA1DA0D0057C80AACBCA7F0<br>D0C3CE7B8B99D4B4278CE3E3CECE33E9<br>E89F09FDDED777CEBA6412D55CE9D3BC<br>F420BDEB156FDB2F874A1E5D51E9D65F<br>FEC68D340ED13292701404E438059FB7<br>14C0558C757C93465ECCBBD77D58BBF3 |
| 3 | 크립토락커 | 0204332754DA5975B6947294B2D64C92<br>6FE47DC2BDB86B0FC28017FC6A67B1F9<br>0E1543914E129FF069D1079695115FE9<br>0DF492989EEA14562EE2E8C880EEDDB6<br>419ECEC2051479609ADED0C173619DF8<br>04FB36199787F2E3E2135611A38321EB |
| 4 | 크립토월 / 크립토디펜스 | 31C2D25D7D0D0A175D4E59D0B3B2EC94<br>0650C9045814C652C2889D291F85C3AE<br>B6C7943C056ACE5911B95D36FF06E0E4<br>A9927372ADB1BBAB4D9FEDA4973B99BB<br>73A9AB2EA9EC4EAF45BCE88AFC7EE87E |
| 5 | 토렌트락커 | 7D1D5E27C1C0CB4ABCC56FA5A4A16744<br>253491AD824E156971C957CD15254844<br>4A96F22E4FFDBCF271FF4EB70B1320ED<br>86296FB3DDD46431DDFE8A48D6FB165C<br>6694617DAB8CD78630AA0A3E002E5197<br>71C066D831A5749685747B33CB9588A8 |
| 6 | 테슬라 크립트 | 01ADE9C90D49AF3204C55D201B466C1B<br>0FF2BE71B46C129EF8905B41E60C2AB0<br>03C1A14C715E3A41F36B026A11A1BCB4<br>0C64ADDB8FE2ED5B029D9337E0E2FBA0<br>0AFBAEE4802BB74F9AC366579921F2B4<br>0C27082138728BC2AACE00263396ADDA |

각 랜섬웨어의 특징은 [표 3-2]와 같이 정리할 수 있다. 가장 큰 특징은 앞서 언급한 것처럼 나부커에서는 암호화 기법을 사용하지 않았으며 공격 대상 파일에 '.exe' 파일이 있다는 것이다. 그리고 공통적으로는 모든 종류의 랜섬웨어에서 비트코인을 이용해 사용자의 결제를 유도하는 것을 확인할 수 있다.

표 3-2 | 주요 랜섬웨어의 특징

| | 랜섬웨어 종류 | 프로토콜 | 암호화 방법 | 주요 대상 파일 | 구현 방식 | 결제 방법 | 복호화 대가 |
|---|---|---|---|---|---|---|---|
| 1 | Nsb락커/ 나부커 | TCP | Polymorphic | Doc/EXE/ 이미지/ 미디어 파일 | Polymorphic | 비트코인 | 250 USD |
| 2 | Ctb로커/ 크리트로니 | HTTPS/ TOR | AES, ECDH | Doc/ 이미지 파일 | OpenSSL | 비트코인 | 0.5 USD |
| 3 | 크립토락커 | HTTP | AES, RSA | Doc/ 이미지 파일 | MS Crypto API | 비트코인 | 300 USD |
| 4 | 크립토월/ 크립토디펜스 | HTTP/ TOR | RSA | Doc/ 이미지 파일 | MS Crypto API | 비트코인 | 500~1000 USD |
| 5 | 토렌트락커 | HTTPS | AES | Doc/ 이미지 파일 | OpenSSL | 비트코인 | 0.8 BTC |
| 6 | 테슬라크립트 | HTTPS/ TOR | AES, ECC | 게임/Doc/ 이미지 파일 | OpenSSL | 비트코인, 페이팔 | 500~1000 USD |

이들 랜섬웨어가 발생한 시기를 타임라인으로 정리하면 [그림 3-1]과 같다. 최근 발견된 '테슬라크립트(TeslaCrypt)'는 공격 대상 파일을 문서나 이미지 파일 뿐만 아니라 게임 관련 파일들도 대상에 포함시킨 것이 특징이며, 이메일로 유포되는 'Ctb락커(CtbLocker)' 류는 최근에 다시 확산되고 있다.

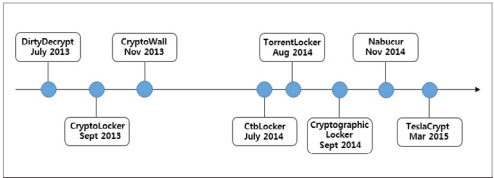



그림 3-1 | 주요 랜섬웨어 타임라인

## 랜섬웨어 Top 6 기능 분석

### Nsb락커 / 나부커(Nabucur)

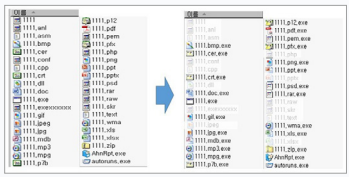
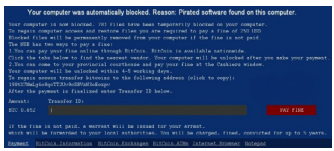
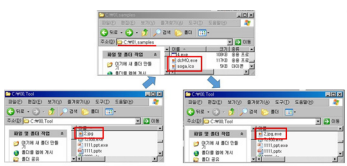
나부커 악성코드에 대해서는 2015년 2월 11일자 안랩 ASEC 블로그(asec.ahnlab.com/1025)에 '원본파일 복원이 가능한 랜섬웨어(NSB: National Security Bureau)'라는 제목으로 소개한 바 있다. 해당 악성코드에 감염되면 시스템에 있는 이미지 파일(*.bmp, *.gif, *.jpg, *.png), 문서 파일(*.doc, *.ppt, *.xls), 미디어 파일(*.mp3, *.wma)뿐만 아니라 실행 파일(*.exe)과 압축 파일(*.rar, *.zip)도 공격 대상이 된다. 이 파일들은 원본 파일을 인코딩된 형태로 백업하고, 이는 실행 파일로 변경되는데 이와 같이 원본 파일들을 'AES', 'RSA'와 같은 암호화 방법으로 변경한 것이 아니므로 백신으로도 복원할 수 있다. 그리고 변경된 실행 파일에는 백업된 원본 파일뿐만 아니라 나부커 감염 코드도 포함되어 있어 그 자체가 다시 다른 파일들을 감염시키는 나부커 랜섬웨어 악성코드가 된다.

그림 3-2 | Nsb락커 / 나부커 동작 흐름

[그림 3-2]에서 볼 수 있듯이 나부커에 감염된 파일은 실행되면 실행 파일 2개를 '%User%'와 '%ALLUser%' 폴더에 생성하는데 이 파일은 스레드 형태로 기능을 수행하면서 C&C 접속과 시스템 내의 특정 확장자를 가진 파일들을 감염시킨다. 그리고 최종적으로 감염된 시스템의 화면을 금전을 요구하는 화면으로 바꾼다.

표 3-3 | Nsb락커 / 나부커 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **%User%₩₩〈랜덤폴더명1〉₩〈랜덤파일명1〉.exe**<br>**%ALLUser%₩₩〈랜덤폴더명2〉₩〈랜덤파일명2〉.exe**<br>⇒ 실제 랜섬웨어 기능을 하는 파일<br>**%TEMP%₩₩〈랜덤파일명3〉.bat**<br>⇒ 원본 파일 디코딩에 필요한 4바이트 키값, 원본 파일 생성 후 삭제<br>**%TEMP%₩₩〈원본파일명〉.exe**<br>⇒ 디코딩된 원본 파일 |
| 레지스트리 등록 | **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩〈랜덤파일명1〉.exe**<br>→ %User%₩〈랜덤폴더명1〉₩〈랜덤파일명1〉.exe<br>**HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩〈랜덤파일명2〉.exe**<br>→ %ALLUser%₩〈랜덤폴더명2〉₩〈랜덤파일명2〉.exe<br>⇒ 자동 실행 등록<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced₩Hidden**<br>→ "0x2"<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced₩HideFileExt**<br>→ "0x1"<br>⇒ 폴더 및 확장자 보기 속성 변경<br>**HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩policies₩system₩EnableLUA**<br>→ "0x0"<br>⇒ 윈도 사용자 계정 설정 변경 |
| 네트워크 접속 | 200.87.164.69:9999(또는 666포트)<br>200.119.204.12:9999(또는 666포트)<br>190.186.45.170:9999(또는 666포트) |

| | |
|---|---|
| 대상 파일 | .bmp, .cer, .crt, .doc, .exe, .gif, .jpg, .mdb, .mp3, .mpg, .p12, .p7b, .pdf, .pem, .pfx, .png, .ppt, .psd, .rar, .wma, .xls, .zip |
| 파일 상태 | 파일의 원래 확장자 뒤에 '.exe' 추가. 단, 실행 파일(.exe)인 경우에는 확장자를 추가하지 않음<br>예) test.jpg.exe, compress.zip.exe 등<br>  |
| 감염 화면 |  |
| 기타 | 아래 그림은 파일을 감염시키는 과정이다. 먼저 감염시키려는 파일의 아이콘 정보를 가져와 〈랜덤4문자.ico〉를 만든다. '원본 파일의 아이콘 + 인코딩된 원본 파일 + 감염 코드'를 포함하고 있는 〈랜덤4문자.exe〉 파일을 생성한다. 그리고 이 파일을 '원본 파일명 + .exe'로 복사하고 원본 파일은 삭제한다.<br>  |

## Ctb락커 / 크리트로니

2014년 7월 공개된 랜섬웨어 Ctb락커(CtbLocker)는 '크리트로니(Critroni)'라는 이름으로도 알려졌으며 스팸메일로 유포되는 다운로더(downloader)에 의해 생성 및 실행된다. 첨부 파일로 포함되어 있는 다운로더는 '.zip' 또는 '.cab' 형태로 압축되어 유포된다. 압축 해제된 파일은 '.scr'

확장자를 가진다. 실행하면 '%TEMP%' 폴더에 정상 '.rtf' 파일을 생성 및 실행하여 마치 문서 파일처럼 위장하지만 백그라운드에서는 사용자 몰래 악성코드를 다운로드한다.

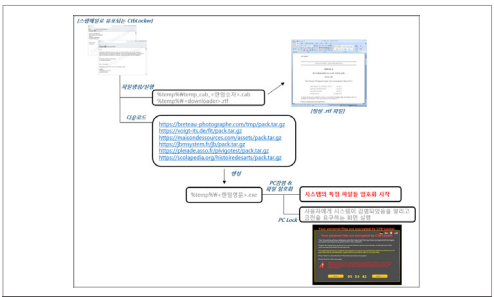
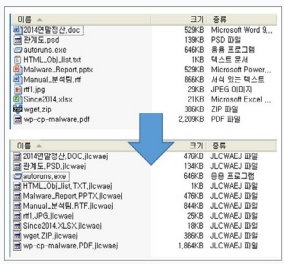
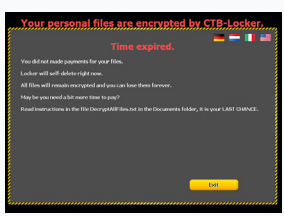


그림 3-3 | Ctb락커 / 크리트로니 동작 흐름

다운로드된 파일은 랜섬웨어 악성코드로 오피스 문서 파일들뿐만 아니라 이미지와 소스 파일 그리고 기타 다양한 파일을 암호화 대상으로 하고 완료 후에는 Ctb락커에 대한 메시지와 비트코인을 요구하는 페이지를 화면에 보여준다.

표 3-4 | Ctb락커 / 크리트로니 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **%temp%₩temp_cab_〈랜덤숫자〉.cab**<br>**%temp%₩〈downloader〉.rtf**<br>⇒ 사용자를 속이기 위한 정상 문서 파일<br>**%temp%₩〈랜덤문자〉.exe**<br>⇒ 실제 랜섬웨어 기능 실행 |
| 레지스트리 등록 | 없음 |
| 네트워크 접속 | https://breteau-photographe.com/tmp/pack.tar.gz<br>https://voigt-its.de/fit/pack.tar.gz<br>https://maisondessources.com/assets/pack.tar.gz<br>https://jbmsystem.fr/jb/pack.tar.gz<br>https://pleiade.asso.fr/pivigotest/pack.tar.gz<br>https://scolapedia.org/histoiredesarts/pack.tar.gz<br>⇒ 파일 다운로드 주소 |
| 대상 파일 | .pwm, .kwm, .txt, .cer, .crt, .der, .pem, .doc, .cpp, .c, .php, .js, .cs, .pas, .bas, .pl, .py, .docx, .rtf, .docm, .xls, .xlsx, .safe, .groups, .xlk, .xlsb, .xlsm, .mdb, .mdf, .dbf, .sql, .md, .dd, .dds, .jpe, .jpg, .jpeg, .cr2, .raw, .rw2, .rwl, .dwg, .dxf, .dxg, .psd, .3fr, .accdb, .ai, .arw, .bay, .blend, .cdr, .crw, .dcr, .dng, .eps, .erf, .indd, .kdc, .mef, .mrw, .nef, .nrw, .odb, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c, .pdd, .pdf, .pef, .pfx, .ppt, .pptm, .pptx, .pst, .ptx, .r3d, .raf, .srf, .srw, .wb2, .vsd, .wpd, .wps, .7z, .zip, .rar, .dbx, .gdb, .bsdr, .bsdu, .bdcr, .bdcu, .bpdr, .bpdu, .ims, .bds, .bdd, .bdp, .gsf, .gsd, .iss, .arp, .rik, .gdb, .fdb, .abu, .config, .rgx |
| 파일 상태 | 암호화된 파일들은 아래 그림과 같이 확장자 뒤에 7자리 랜덤 문자열이 추가된다.<br>예) test.jpg.[7자리랜덤 문자열], compress.zip.[7자리 랜덤문자열] 등<br>  |
| 감염 화면 |  |
| 기타 | 96시간 안에 돈을 주지 않으면 데이터를 복구할 수 없다는 메시지를 보여주고 해당 시간이 모두 지나거나 컴퓨터 시간을 임의로 이후 시간으로 조작하면 아래와 같이 만료(expire)되었다는 화면이 나타난다.<br>  |

## 크립토락커

2013년 9월 처음 발견된 크립토락커(CryptoLocker)는 Ctb락커처럼 스팸메일의 첨부 파일 형태 또는 P2P 방식의 '게임오버 제우스(Gameover Zeus)' 봇넷 악성코드를 통해 유포되며 문서와 이미지 파일들을 암호화하였다. 이를 정상화하려면 머니팩(MoneyPak)이나 비트코인 결제를 요구한다.

이 랜섬웨어는 자신을 레지스트리에 자동 실행하도록 등록해 놓는데 등록된 이름이 '크립토락커(CryptoLocker)'로 되어 있는 것이 특징이다. C&C 서버에 접속해서 공개키(Public Key)를 받아온 후 시스템의 파일들을 암호화한다. 현재는 해당 서버들이 다운되어 있는 상태이므로 랜섬웨어 기능이 동작하지는 않는다.

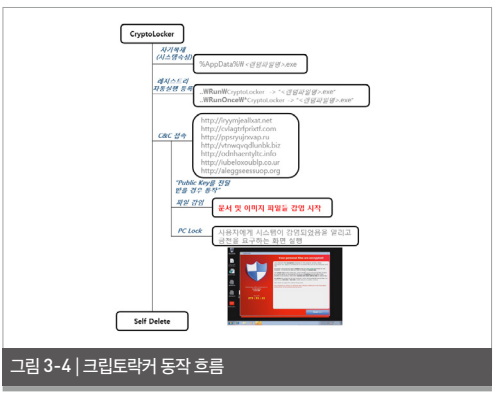
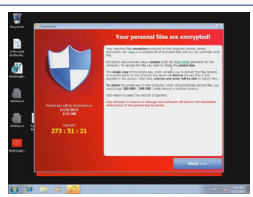
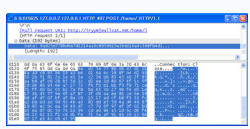



그림 3-4 | 크립토락커 동작 흐름

2014년 8월, 글로벌 보안 전문가들이 'Tovar' 오퍼레이션을 통해 이 악성코드 제작자의 C&C 서버를 다운시키고 서버에 저장된 복호화 키를 다수 획득했다. 현재는 암호화된 파일 상당수를 이전의 상태로 복구할 수 있다. 해당 기간까지 전 세계 약 50만 대의 시스템이 크립토락커에 감염된 것으로 보고되었다.

표 3-5 | 크립토락커의 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **%AppData%₩<랜덤파일명>.exe**<br>⇒ [Windows XP]<br>**%AppData%₩Loca₩<랜덤파일명>.exe**<br>⇒ [Windows 7]<br>⇒ 자기 복제 |
| 레지스트리 등록 | **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩CryptoLocker**<br>→ %AppData%₩<랜덤파일명>.exe<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩*CryptoLocker**<br>→ %AppData%₩<랜덤파일명>.exe<br>⇒ 자동 실행 등록 |
| 네트워크 접속 | http://iryymjeallxat.net<br>http://cvlagtrfprixtf.com<br>http://ppsryujrxvap.ru<br>http://vtnwqvqdlunbk.biz<br>http://odnhaentyltc.info<br>http://iubeloxoublp.co.uk<br>http://alegqseessuop.org<br>⇒ C&C 서버 주소 |
| 대상 파일 | .odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx, .pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .eps, .indd, .cdr, .jpg, .dng, .3fr, .arw, .srf, .sr2, .bay, .crw, .cr2, .dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .der, .cer, .crt, .pem, .pfx,.p12, .p7b, .p7c |
| 파일 상태 | C&C 서버와 통신 성공 후 동작 |
| 감염 화면 |  |
| 기타 | [C&C 서버에 특정 데이터를 암호화하여 POST 전송]<br>C&C 접속에 성공하면 해당 서버의 /home/ 경로에 실행 파일과 피해 시스템의 정보가 포함된 데이터를 POST 전송한다.<br>  |

## 크립토월/크립토디펜스

크립토월은 전체적인 동작 흐름이 앞서 설명한 크립토락커와 비슷하다. 둘 다 하위 프로세스를 생성한 후 PE 이미지를 인젝션시켜 동작하며, C&C 서버로부터 공개 키를 받아온 후 랜섬웨어 기능을 실행한다.

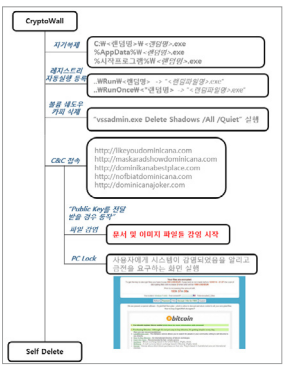



그림 3-5 | 크립토월 동작 흐름

표 3-6 | 크립토월의 주요 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **C:₩<랜덤명>₩<랜덤명>.exe**<br>**%AppData%₩<랜덤명>.exe**<br>**%시작프로그램%₩<랜덤명>.exe**<br>⇒ 자기 복제 |
| 레지스트리 등록 | **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩ <랜덤명-1>**<br>→ C:₩<랜덤명>₩<랜덤명>.exe<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩*<랜덤명-1>**<br>→ C:₩<랜덤명>₩<랜덤명>.exe<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩ <랜덤명>**<br>→ %AppData%₩<랜덤명>.exe<br>**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩*CryptoLocker**<br>→ %AppData%₩<랜덤명>.exe<br>⇒ 자동 실행 등록<br><랜덤명-1>은 7문자 랜덤한 파일명에서 마지막 문자를 제외한 6자리<br>⇒ 랜덤한 파일명 |
| 네트워크 접속 | http://likeyoudominicana.com<br>http://maskaradshowdominicana.com<br>http://dominikanabestplace.com<br>http://nofbiatdominicana.com<br>http://dominicanajoker.com<br>⇒ C&C 서버 주소 |
| 대상 파일 | *.doc, *.ppt, *.rtf 등의 문서와 이미지 파일 |
| 파일 상태 | C&C 서버와 통신 성공 후 동작 |
| 감염 화면 |  |
| 기타 | C&C 서버로부터 키 값을 가져와 크립토월이 시스템을 감염시킨다면 모든 폴더에 아래 3개의 파일을 생성하고 내부에는 파일 복구를 위한 절차가 명시되어 있다.<br><br>DECRYPT_INSTRUCTION.HTML<br>DECRYPT_INSTRUCTION.TXT<br>DECRYPT_INSTRUCTION.URL |

## 토렌트락커

토렌트락커(TorrentLocker) 역시 앞에 설명한 크립토락커, 크립토월과 비슷한 동작을 하며 코드가 진행되는 부분도 매우 비슷하다. 단 "HKCU₩Software₩Bit Torrent Application₩configuration" 레지스트리에 암호화한 파일 리스트를 등록하는 특징이 있어 토렌트락커로 명명되었다고 한다.

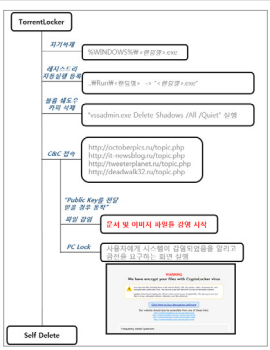



그림 3-6 | 토렌트락커 동작 흐름

표 3-7 | 토렌트락커의 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **%WINDOWS%₩〈랜덤명〉.exe**<br>⇒ 자기 복제 |
| 레지스트리 등록 | **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩ 〈랜덤명〉**<br>→ %WINDOWS%₩〈랜덤명〉.exe<br>⇒ 자동 실행 등록 |
| 네트워크 접속 | http://octoberpics.ru/topic.php<br>http://it-newsblog.ru/topic.php<br>http://tweeterplanet.ru/topic.php<br>http://deadwalk32.ru/topic.php<br>⇒ C&C 서버 주소 |
| 대상 파일 | *.doc, *.ppt, *.rtf 등의 문서와 이미지 파일 |
| 파일 상태 | C&C 서버와 통신 성공 후 동작 |
| 감염 화면 |  |
| 기타 | C&C 서버에서 키를 받아와 파일들을 암호화하는 랜섬웨어 기능을 한다면, '%AppData%₩〈16자리소문자랜덤명〉' 폴더에 암호화된 파일들을 저장해 놓음 |

## 테슬라크립트

테슬라크립트(TeslaCrypt)는 게임 기능과 저장 데이터를 공격하는 랜섬웨어 류로, 아이프레임(iframe) 대신 태그(div)를 이용한 플래시 플레이어 취약점을 통해 일반 사용자 PC에 설치된다. 구조는 앞의 크립토락커(CyptoLocker)와 유사하지만, 문서 파일뿐만 아니라 게임 관련 파일(프로필, 세이브, 데이터, 지도, 모드 등)도 암호화한다는 것이 특징이다.

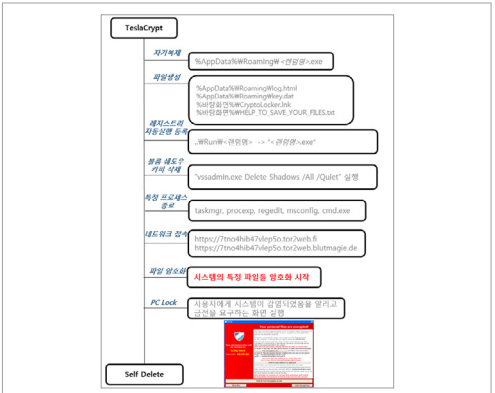



그림 3-7 | 테슬라크립트 동작 흐름

테슬라크립트는 크립토락커와는 달리 네트워크 접속은 사용자 PC의 비트코인 접속 주소를 전달하기 위해 사용되며, %AppData% 폴더에는 암호화한 파일 리스트를 가지고 있는 'log.html' 파일과 복호화할 때 사용하는 'key.dat' 파일이 저장된다. 그리고 바탕화면에 생성되는 'HELP_RESTORE_FILES.txt' 파일에는 암호화된 파일을 풀기 위해 비트코인을 지급하는 과정이 설명되어 있다.

표 3-8 | 테슬라크립트 특징

| 동작 | Log |
|---|---|
| 파일 생성 | **%AppData%₩Roaming₩〈랜덤명〉.exe**<br>⇒ 자기 복제<br>**%AppData%₩Roaming₩log.html**<br>⇒ 암호화된 파일 리스트<br>**%AppData%₩Roaming₩key.dat**<br>⇒ 복호화 시 사용되는 파일<br>**%바탕화면%₩CryptoLocker.lnk**<br>⇒ 바로가기 파일<br>**%바탕화면%₩HELP_RESTORE_FILES.txt**<br>⇒ 시스템이 감염되었으니 비트코인으로 결제하여 해결하라는 안내 텍스트 |
| 레지스트리 등록 | **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩** 〈랜덤명〉<br>→ %AppData%₩Roaming₩〈랜덤명〉.exe<br>⇒ 자동 실행 등록 |

| | |
|---|---|
| 네트워크 접속 | https://7tno4hib47vlep5o.tor2web.fi<br>https://7tno4hib47vlep5o.tor2web.blutmagie.de |
| 대상 파일 | .d3dbsp, .icxs, .menu, .mpqge, .wotreplay, .pptx, .sc2save, .hvpl, .layout, .DayZProfile, .desc, .xlsb, .ibank, .hplg, .blob, .rofl, .jpeg, .xlsm, .pkpass, .hkdb, .dazip, .litemod, .mrwref, .xlsx, .sidn, .mdbackup, .arch00, .asset, .indd, .docm, .sidd, .syncdb, .vpp_pc, .forge, .dbfv, .docx, .mddata, .mcgame, .mcmeta, .rgss3a, .accdb, .itdb, .ztmp, .vfs0, .unity3d, .pptm |
| 파일 상태 | 파일 확장자 뒤에 '.ecc' 추가, 그리고 모든 폴더에 'HELP_RESTORE_FILES.txt' 파일이 생성됨<br>예) test.jpg.ecc, compress.zip.ecc 등<br>  |
| 감염 화면 |  |
| 기타 | C&C 서버로부터 키를 받아와 파일들을 암호화하는 랜섬웨어 기능을 한다면, '%AppData%₩〈16자리 소문자랜덤명〉' 폴더에 암호화된 파일들을 저장해 놓음 |

랜섬웨어에 감염되면, 화면으로 PC가 감염되었음을 사용자에게 알려주고 이를 정상화하려면 돈을 내라는 내용에 사용자들은 혼란을 겪는다. 당장 PC를 사용할 수 없을 뿐만 아니라 내부에 중요한 파일들이 있다면 다른 뚜렷한 해결책이 없는 상황에서는 사용자들이 결제를 선택할 수밖에 없을 것이다. 그렇다고 대가를 지급한다고 해서 시스템이 원래대로 돌아온다고 확신할 수도 없다. 그러므로 해당 악성코드에 PC가 감염되는 것을 사전에 방지하는 것이 가장 좋은 방법이다. 그러려면 발신자가 명확하지 않은 이메일에 포함된 의심스러운 파일들을 실행하지 말아야 한다. 또한 PC에 사용 중인 백신을 항상 최신의 상태로 업데이트하고, OS와 애플리케이션 공급 업체에서 제공하는 패치를 최신 버전으로 유지하는 것이 중요하다.

AhnLab

# ASEC REPORT

VOL.64
April, 2015

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 UX디자인팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901