

ASEC REPORT

VOL.75

March, 2016



AhnLab

ASEC REPORT

VOL.75 March, 2016

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.

2016년 3월 보안 동향

Table of Contents

1 보안 통계 STATISTICS	01 악성코드 통계	4
	02 웹 통계	6
	03 모바일 통계	7
2 보안 이슈 SECURITY ISSUE	01 금융 정보를 탈취하는 신종 모바일 랜섬웨어, Xbot	10
	02 POS 시스템 노리는 악성코드 국내 유포 주의	14
3 악성코드 상세 분석 ANALYSIS IN-DEPTH	2016년 1분기 주요 랜섬웨어 동향	18

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

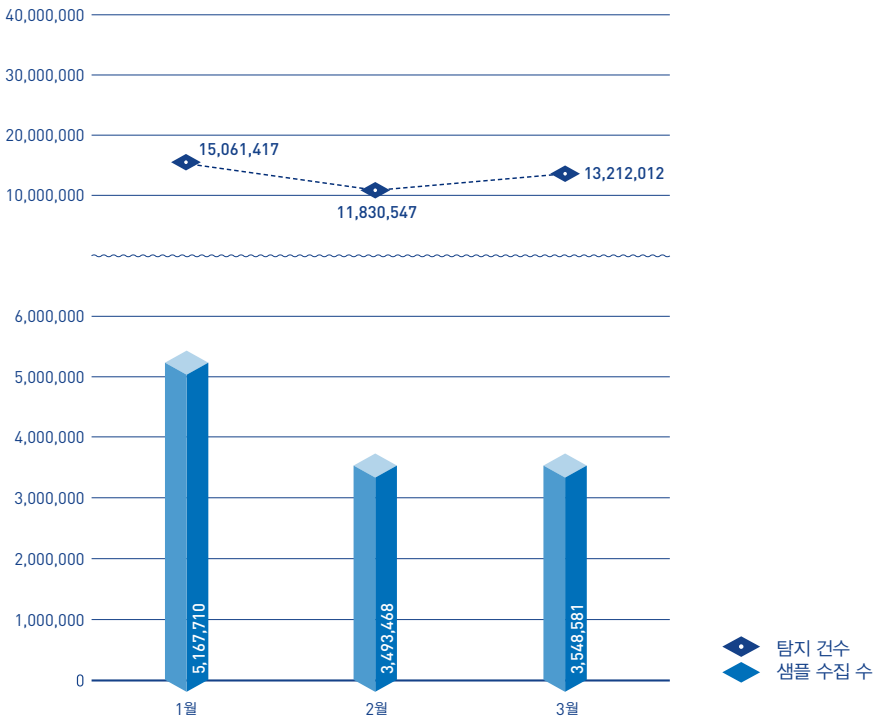
03 모바일 통계

보안 통계

01

악성코드 통계

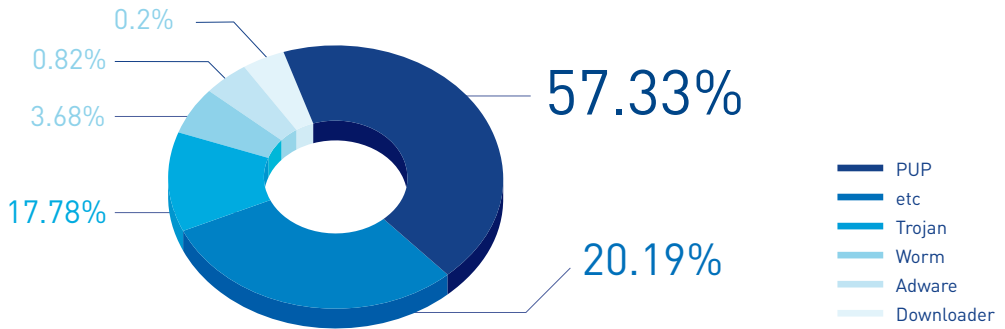
ASEC이 집계한 바에 따르면, 2016년 3월 한 달간 탐지된 악성코드 수는 1,321만 2,012건으로 나타났다. 이는 전월 1,183만 547건에 비해 138만 1,465건 증가한 수치다. 한편 3월에 수집된 악성코드 샘플 수는 354만 8,581건이다.



[그림 1-1] 악성코드 추이(2016년 1월 ~ 2016년 3월)

* '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 1-2]는 2016년 3월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램 램인 PUP(Potentially Unwanted Program)가 57.33%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 17.78%, 웜(Worm)이 3.68%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 3월 주요 악성코드 유형

[표 1-1]은 3월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 28만 7,193건으로 가장 많이 탐지되었고, Malware/Win32.Generic이 12만 9,017건으로 그 뒤를 이었다.

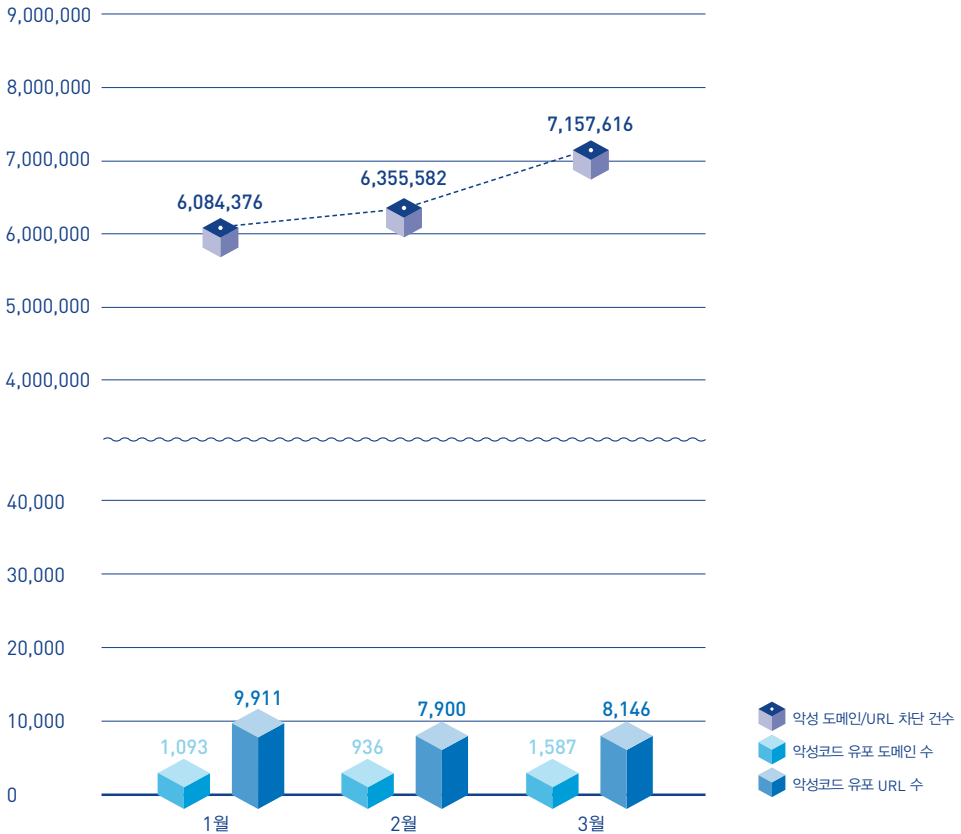
[표 1-1] 2016년 3월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	287,193
2	Malware/Win32.Generic	129,017
3	Trojan/Win32.Agent	110,699
4	Unwanted/Win32.HackTool	101,161
5	Trojan/Win32.Banki	89,940
6	Trojan/Win32.Teslacrypt	85,658
7	Trojan/Win32.Injector	78,698
8	Trojan/Win32.Neshta	78,147
9	Unwanted/Win32.Keygen	74,648
10	HackTool/Win32.Crack	74,607

보안 통계

02
웹 통계

2016년 3월에 악성코드 유포지로 악용된 도메인은 1,587개, URL은 8,146개로 집계됐다([그림 1-3]). 또한 3월의 악성 도메인 및 URL 차단 건수는 총 715만 7,616건이다.



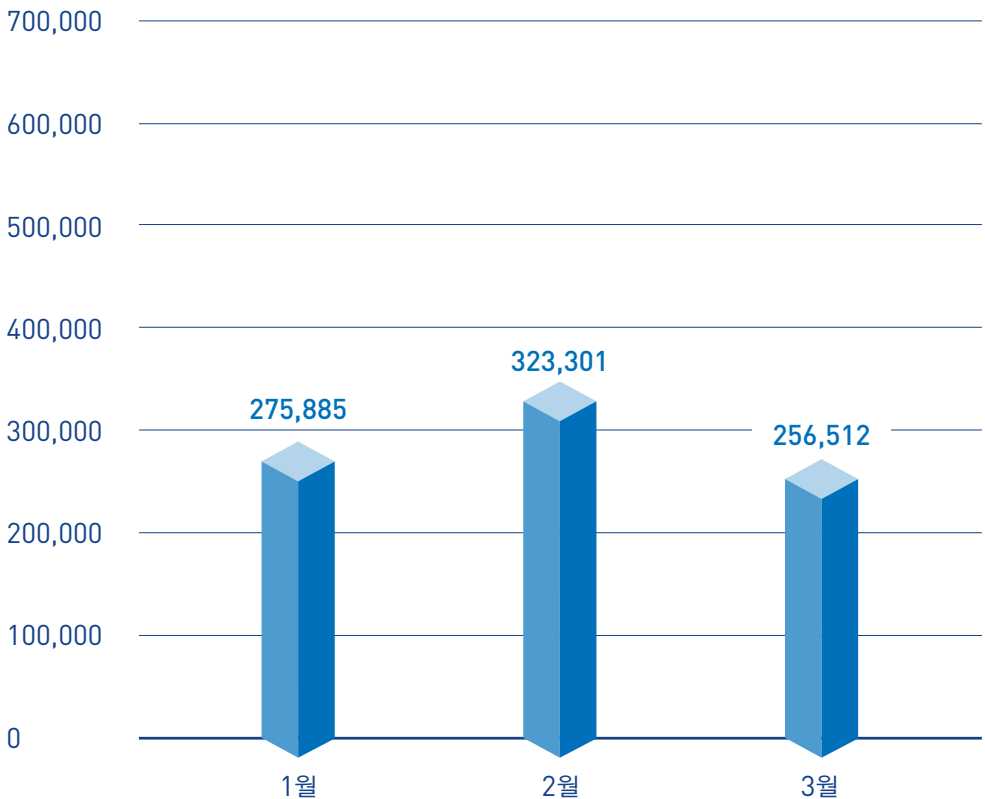
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 1월 ~ 2016년 3월)

* 악성 도메인 및 URL 차단 건수란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03

모바일 통계

2016년 3월 한 달간 탐지된 모바일 악성코드는 25만 6,512건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이(2016년 1월 ~ 2016년 3월)

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

[표 1-2] 2016년 3월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	47,039
2	Android-PUP/SmsReg	35,088
3	Android-PUP/Noico	18,872
4	Android-PUP/Dowgin	15,098
5	Android-Trojan/Moavt	8,782
6	Android-PUP/Shedun	8,302
7	Android-PUP/Zdpay	6,627
8	Android-PUP/Kuguo	5,771
9	Android-PUP/Wapsx	5,313
10	Android-Trojan/FakeInst	5,066

2

보안 이슈 SECURITY ISSUE

- 01 금융 정보를 탈취하는 신종 모바일 랜섬웨어, Xbot
- 02 POS 시스템 노리는 악성코드 국내 유포 주의

01

금융 정보를 탈취하는 신종 모바일 랜섬웨어, Xbot

윈도우(Windows) 기반의 랜섬웨어로 인한 피해가 다수 보고되고 있는 가운데, 최근 랜섬웨어 기능을 가진 신종 안드로이드 악성 앱 Xbot이 발견됐다. 지난 2015년 5월경부터 발견되고 있는 Xbot은 사용자의 신용카드 및 은행 계좌 정보를 탈취하고, 기기 내의 데이터를 암호화한다. 또한 정기적인 업데이트를 통해 꾸준히 진화하고 있어 모바일 랜섬웨어로 인한 금융 피해가 우려된다.

다음은 구글 플레이 아이콘으로 위장하고 있는 Xbot을 분석한 내용이다. 먼저 해당 안드로이드 악성 앱의 manifest 정보를 통해 권한 정보를 확인하면 다음 [표 2-1]과 같이 악성 행위에 필요한 다수의 권한을 요구하고 있다.

표 2-1 | manifest 정보

```
<manifest android:versionCode="1" android:versionName="1.0"
package="com.replayroll.core" platformBuildVersionCode="15"
platformBuildVersionName="4.0.4-1406430"
xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:allowBackup="true" android:icon="@drawable/icon" android:label="Installer">
        <activity android:label="Installer"
        android:launchMode="singleTop" android:name="com.replayroll.
core.MainActivity">
            <intent-filter>
```

```
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.
LAUNCHER" />
    </intent-filter>
</activity>
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.BrowserActivity" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.Browser" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.lck.Lock" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.GoogleCC" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.Inject" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.BankApp" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.activities.RunScript" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.AdminActivity" />
    <activity android:label="" android:launchMode="singleTop"
    android:name="com.replayroll.core.
CCNotificationResultActivity" />
    <service android:name="com.replayroll.core.RunService" />
    <receiver android:name="com.replayroll.core.
OnBootHandler">
        <intent-filter>
            <action android:name="android.intent.action.BOOT_
COMPLETED" />
        </intent-filter>
    </receiver>
    <receiver android:name=".SMSHandler">
        <intent-filter android:priority="2147483647">
            <action android:name="android.provider.Telephony.
```

```

SMS_RECEIVED" />
</intent-filter>
</receiver>
<receiver android:label="Admin" android:name="com.
replayroll.core.AdminReceiver" android:permission="android.
permission.BIND_DEVICE_ADMIN">
    <meta-data android:name="android.app.device_admin"
android:resource="@xml/ok" />
    <intent-filter>
        <action android:name="android.app.action.DEVICE_
ADMIN_ENABLED" />
    </intent-filter>
</receiver>
<receiver android:name=".sms.SentReceiver">
    <intent-filter>
        <action android:name="SMS_SENT" />
    </intent-filter>
</receiver>
<receiver android:name=".sms.DeliveredReceiver">
    <intent-filter>
        <action android:name="SMS_DELIVERED" />
    </intent-filter>
</receiver>
</application>
<uses-permission android:name="android.permission.
INTERNET" />
<uses-permission android:name="android.permission.WAKE_
LOCK" />
<uses-permission android:name="android.permission.READ_
SMS" />
<uses-permission android:name="android.permission.
RECEIVE_SMS" />
<uses-permission android:name="android.permission.READ_
EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_
EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_
PHONE_STATE" />
<uses-permission android:name="android.permission.SEND_
SMS" />
<uses-permission android:name="android.permission.
RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.READ_
CONTACTS" />
<uses-permission android:name="android.permission.
ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.
ACCESS_MOCK_LOCATION" />

```

```

<uses-permission android:name="android.permission.
ACCESS_LOCATION_EXTRA_COMMANDS" />
<uses-permission android:name="android.permission.BIND_
DEVICE_ADMIN" />
<uses-permission android:name="android.permission.GET_
TASKS" />
<uses-permission android:name="android.permission.
ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.
MODIFY_AUDIO_SETTINGS" />
<uses-permission android:name="android.permission.
DEVICE_POWER" />
<uses-permission android:name="android.permission.
SYSTEM_ALERT_WINDOW" />
</manifest>

```

해당 앱의 설치 과정을 살펴보면 [그림 2-1]과 같이 주소록 및 메시지 접근, SD 카드 내의 콘텐츠 수정 등의 권한을 갖고 있는 것을 확인할 수 있다.

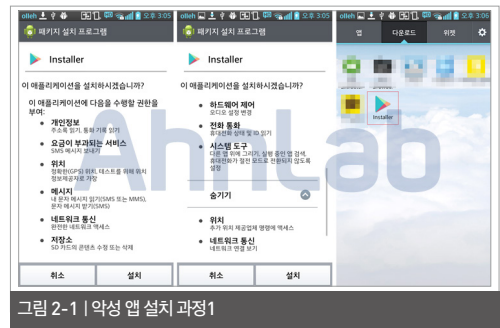
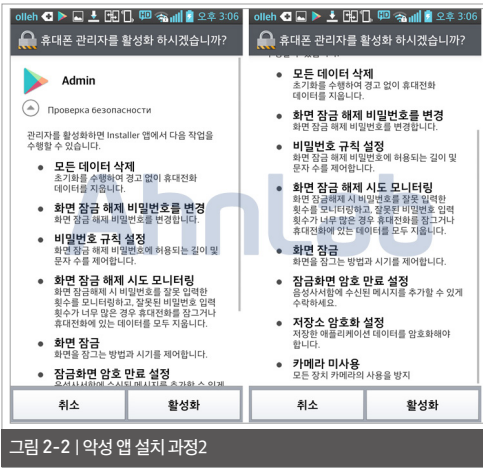


그림 2-1 | 악성 앱 설치 과정1

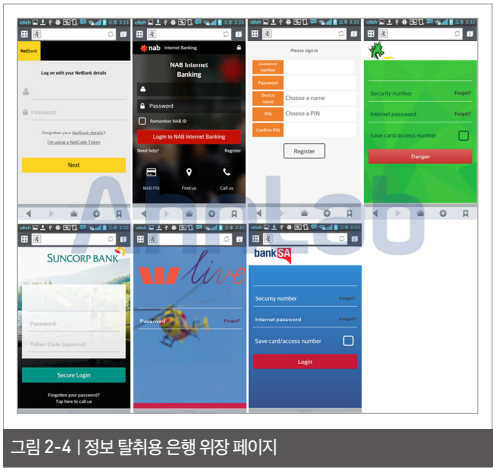
설치가 완료되면 [그림 2-1]의 오른쪽 화면과 같이 사용자의 스마트폰에 구글 플레이 스토어 아이콘이 생성되며, 해당 앱을 실행하면 관리자 권한을 획득하기 위해 휴대폰 관리자 활성화를 요구한다. 대다수의 악성 안드로이드 앱은 휴대폰 관리자 권한을 요구하는데, 사용자가 관리자 권한을 활성화하면 악성 앱은 스스로를 보호하기 위해 사용자가 다시 활성화 해제하는 것을 방해한다.



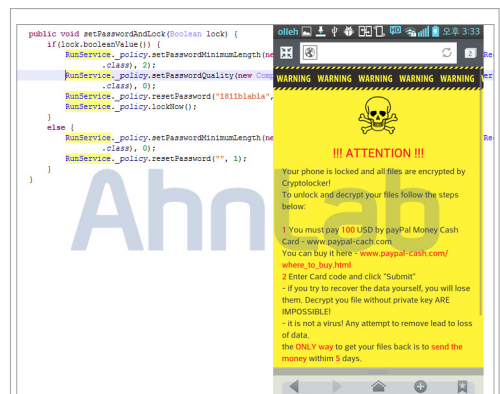
악성 앱이 동작하면 [그림 2-3]과 같이 RunService 클래스를 통해 카드 정보 수집 페이지로 이동한다.



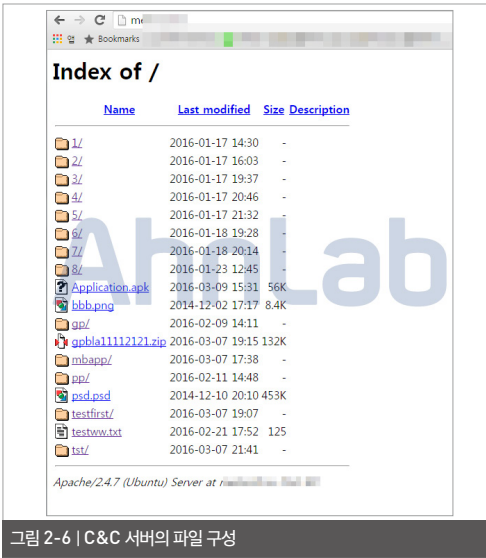
해당 악성 앱은 명령을 받아 [그림 2-4]와 같이 사용자에게 위조된 은행 페이지를 보여준 다음 사용자가 입력한 금융 정보를 탈취한다.



또한, [그림 2-5]와 같이 잠금 패스워드를 '1811bla-bla'로 재설정하는 코드도 확인된다. 해당 코드가 정상적으로 실행되면 랜섬웨어 기능이 동작할 것으로 보인다.



한편, 해외에 존재하는 C&C서버에서 [그림 2-6]과 같은 파일 구성이 확인되었으며, 현재도 지속적으로 악성 앱을 제작 중인 것으로 보인다.



거래가 증가할수록 이를 노린 악성 안드로이드 앱 또한 더욱 교묘하게 고도화되고 있다.

기본적으로 앱은 공식 마켓에서 다운로드하여 설치하는 것이 안전하다. 그러나 공식 마켓에도 악성 앱이 등록되어 있을 가능성이 있으므로 앱 설치 시에는 반드시 평판 정보를 확인하고 다운로드하는 습관이 필요하다. 또한 문자에 포함된 URL을 무심코 클릭하면 악성 앱이 설치될 수도 있기 때문에 확인되지 않은 URL 및 앱은 설치하지 않도록 주의해야 한다. V3 Mobile Security 등의 모바일 전용 보안 앱을 이용하는 것도 안전한 스마트폰 이용에 도움이 된다.

V3 모바일 제품에서는 해당 악성 앱을 다음과 같은 진단명으로 탐지하고 있다.

<V3 모바일 제품군 진단명>

Android-Trojan/XBot

지금까지 살펴본 것처럼 Xbot은 구글 플레이 스토어의 지불 정보 페이지와 은행 앱의 로그인 페이지를 도용한 피싱을 이용하여 사용자의 금융 정보를 탈취하고, SD 카드 내의 사용자 데이터를 암호화하여 금전을 요구하고 있다. 스마트폰에서 बैं킹, 쇼핑 등 금융

02

POS 시스템 노리는 악성코드 국내 유포 주의

POS(Point of Sales) 시스템은 주로 백화점, 마트, 음식점 등과 같이 판매와 관련된 데이터를 관리하는 시스템으로, PC에 바코드 리더기, 카드 입력기, 영수증 프린터가 추가된 형태다. POS 시스템은 대부분 결제 시 신용카드의 정보 및 고객 정보를 일시적으로 저장하고 있는데, 일반 PC에 비해 OS나 응용 프로그램의 업데이트가 제대로 이뤄지지 않는 등 상대적으로 보안 위협에 취약한 편이다.

이러한 이유로 POS 시스템의 취약점을 노리는 악성코드가 지속적으로 나타나고 있다. POS 시스템의 데이터 유출을 위한 다양한 공격 기법이 존재하는데, 대표적으로 시스템에 입력되는 값들을 가로채는 키로깅(Keylogging)과 메모리에 접근하여 특정 값을 유출하는 메모리 스크래핑(Memory Scraping) 등이 있다. 체리피커(Cherry Picker)를 비롯한 대부분의 POS 악성코드들은 메모리 스크래핑 공격 기법을 이용한다.

최근에도 메모리 스크래핑 공격 기법을 이용한 POS 악성코드가 발견돼 POS 시스템 보안 관리에 더욱 주의가 요구된다.



그림 2-7 | 2016년 국내 POS 해킹 사고(출처: KBS뉴스(좌) 기호일보(우))

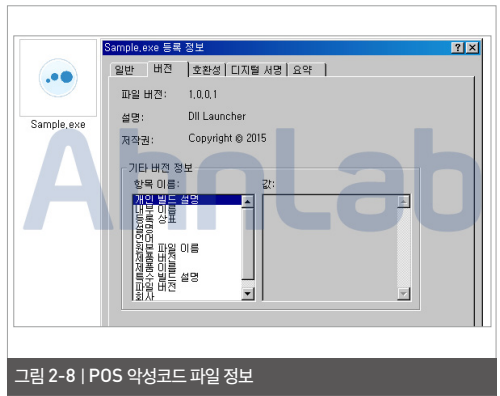
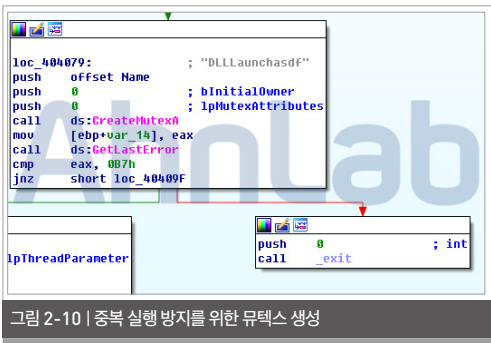


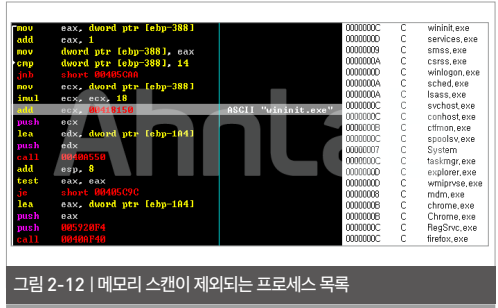
그림 2-8 | POS 악성코드 파일 정보

최근 발견된 POS 악성코드는 [그림 2-8]과 같이 위조된 디지털 서명과 함께 DLL Launcher로 위장하고 있으며, 실행 시 레지스트리를 통해 'LogMeInServer' 서비스로 등록된다.

[그림 2-9]와 같이 서비스로 등록된 악성코드는 시스템 시작 시 자동 실행되며, 'DLLLaunchasd' 모듈을 생성하여 중복 실행을 방지한다.



이 POS 악성코드는 CreateToolhelp32Snapshot API를 이용하여 시스템 정보 및 실행 중인 프로세스(특정 프로세스 제외) 메모리의 트랙 데이터(Track Data)를 스캔한다.



이 악성코드는 감염된 시스템 내 POS 프로세스의 메모리 값을 읽어 이를 암호화하여 ‘[랜덤문자열].dat’ 파일에 저장한다. 또한 bot ID 값으로 추정되는 문자열을 ‘dpsvc.bid’에 저장한다.



이어 POS 프로세스를 스캔한 메모리 내 데이터를 C&C 서버로 전송한다. 이에 앞서 네트워크 연결 상태를 확인하기 위하여 45.63.71.150:80 /index.php HTTP Request 패킷을 보내는데, 응답이 오면 탈취한 금융 정보를 C&C 서버로 전송할 것으로 추측된다.

최근 국내에서도 POS 악성코드로 인한 피해가 지속적으로 발생하고 있으나, 이에 대한 대처는 미흡한 상황이다. POS 시스템은 신용카드 등 민감한 정보를 다루고 있는 만큼, POS 시스템에 대한 지속적인 관리와 확실한 보안 조치가 필요하다. 특히 POS 악성코드에 의한 피해를 예방하기 위해서는 POS 시스템

로그인 암호를 주기적으로 변경하고 웹 서핑, 메신저 등 POS 시스템 운영과 무관한 프로그램이나 서비스 사용은 지양해야 한다. 또한 POS 시스템 전용 보안 프로그램을 사용하는 것도 바람직하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군 진단명>

Spyware/Win32.Poscard (2016.02.25.09)

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

2016년 1분기 주요 랜섬웨어 동향

2016년 1분기 주요 랜섬웨어 동향

최근 랜섬웨어 피해가 잇따라 발생하고 있는 가운데, 다양한 공격 기법을 이용한 신·변종 랜섬웨어가 지속적으로 유포되고 있다. 이 글에서는 2016년 1분기 주요 랜섬웨어의 특징을 상세히 살펴본다.

1. 록키(Locky) 랜섬웨어의 진화

1.1. 매크로 기능을 이용한 록키 랜섬웨어

MS 오피스 문서의 매크로 기능을 이용한 록키 랜섬웨어가 발견됐다.

사용자가 감염된 사이트를 접속하면 감염되는 기존의 랜섬웨어와 달리, 최근 발견된 록키 랜섬웨어는 [그림 3-1]과 같이 지급(payment), 송장(invoice), 계약서(contract) 등의 제목으로 위장한 스팸 메일을 통해 불특정 다수에게 유포되었다.

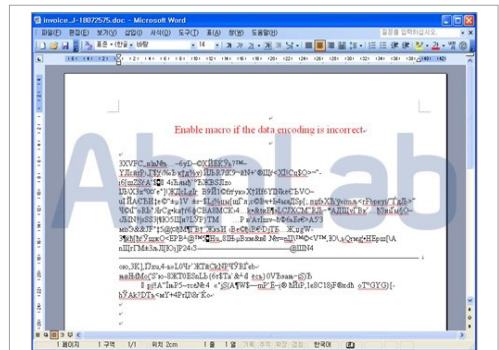


그림 3-2 | 첨부된 워드 파일 실행화면

스팸 메일에 첨부된 워드 파일을 실행하면 [그림 3-2]와 같이 인코딩되어 있는 내용을 풀기 위해 매크로 기능을 사용하도록 유도하고 있다.

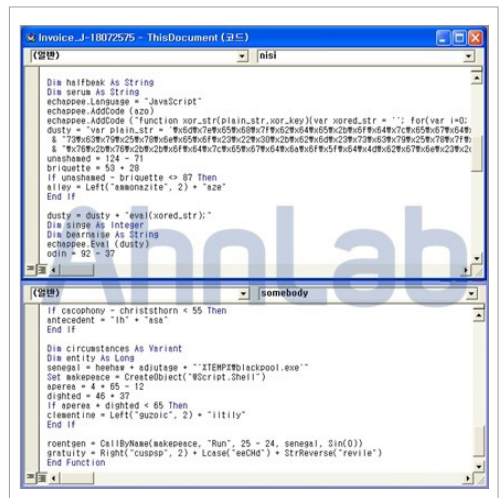


그림 3-3 | 워드 파일에 삽입된 매크로 내용

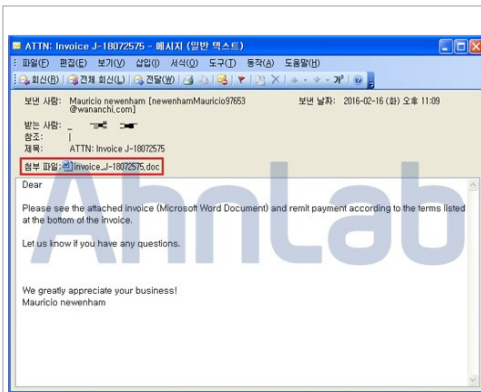


그림 3-1 | 스팸 메일을 통해 유포되는 록키 랜섬웨어

해당 매크로 내용을 살펴보면 난독화된 자바스크립트 구문이 확인되며, 시스템 [%Temp%] 폴더에 생성된 파일에 의해 [그림 3-4]와 같이 특정 URL에 접속해 추가로 악성 파일 다운로드를 시도한다. 해당 URL은 실제 암호화 행위를 하기 위해 필요한 키(Key)를 받아오는 C&C 서버 주소로 추정되나, 분석 당시에는 정상적으로 접속되지 않았다.

Source	Destination	Info
1114-80	[SYN]	Seq=0 Win=64240 Len=0 MSS=3460 SACK_PERM=1
80-1114	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1114-80	[ACK]	Seq=1 Ack=1 Win=64240 Len=0
80-1114	[ACK]	Seq=293 Ack=1 Win=63783 Len=0
80-1114	[FIN, ACK]	Seq=293 Ack=1 Win=63783 Len=0
80-1114	[ACK]	Seq=459 Ack=294 Win=64239 Len=0

그림 3-4 | 매크로 기능에 의해 악성 파일 추가 다운로드

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

W97M/Downloader (2016.02.18.00)

1.2. ‘js’ 파일 형식의 록키 랜섬웨어

최근에는 자바스크립트(js)를 zip 파일로 첨부해 이를 실행하면 외부에서 랜섬웨어 본체를 다운로드 받아오는 변종 형태도 발견되었다. 웹 서버가 아닌 사용자 PC에 설치된 웹 브라우저에서 동작하도록 작성된 자바스크립트(JavaScript) 언어를 이용한 것으로, 기존의 exe, pdf, doc 등의 첨부 파일 형태를 이용한 형태와 차이를 보인다. 기존의 랜섬웨어들이 사용한 파일 포맷은 다양한 PC 환경에 구매받지 않을 뿐만 아니라 사용자들이 익숙한 파일 아이콘을 보고 별다른 의심 없이 실행하도록 유도하기 위함이었다.

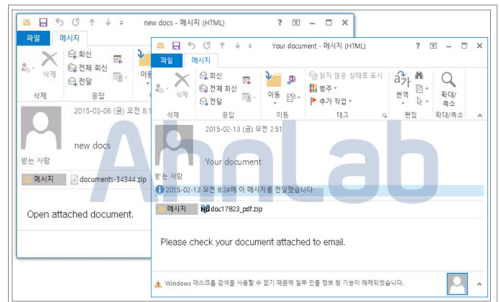


그림 3-5 | 일반적인 형태의 스팸 메일



그림 3-6 | 일반적으로 스팸 메일 내부에 존재하는 exe, pdf 파일

그러나 최근 발견된 록키 랜섬웨어 변종은 일반 사용자들에게는 익숙하지 않은 js 파일이 스팸 메일의 첨부 파일로 포함되어 있다.

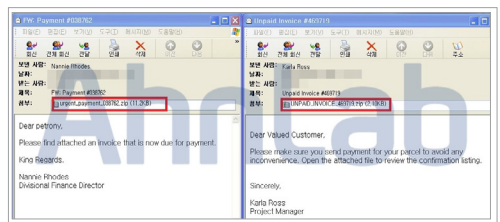


그림 3-7 | 기존과 동일한 형태의 스팸 메일

[그림 3-7]과 같이 스팸 메일에 압축 파일 형태로 첨부되어 있으며 지급(payment), 송장(invoice), 계약서(contract) 등을 사칭하고 있는 점도 기존 랜섬웨어 유포 방식과 동일하다. 그러나 압축 파일의 내부를 확인해보면 기존과 다른 것을 알 수 있다.

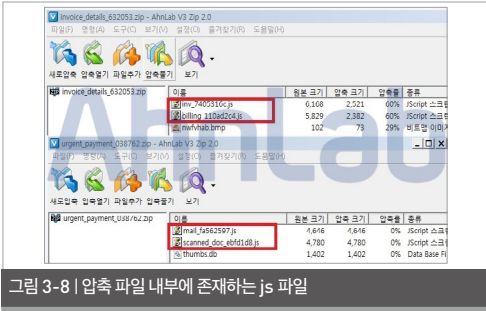


그림 3-8 | 압축 파일 내부에 존재하는 js 파일

[그림 3-8]과 같이 압축 파일 내부에 js 파일이 존재하며, 파일 종류 또한 JScript 스크립트로 구분되어 있다.

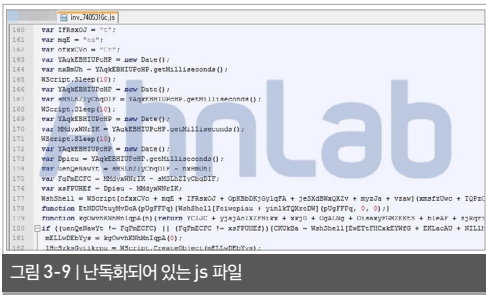


그림 3-9 | 난독화되어 있는 js 파일

해당 첨부 파일을 다운로드하여 압축을 해제한 뒤 js 파일을 확인해보면 [그림 3-9]와 같이 난독화되어 있다. 최근 신고되는 js 파일들을 살펴보면 난독화된 형태는 비슷하지만 랜덤한 문자열이 각기 다른 것으로 보아 자동 생성 프로그램을 활용하고 있는 것으로 추측된다.



그림 3-10 | js 파일을 더블클릭할 경우 연결되는 프로그램

해당 js 파일의 연결 프로그램을 확인하면 Microsoft

Windows Based Script Host (WBSH)라는 프로그램으로 연결된다. 해당 프로그램은 윈도우 운영체제에서 스크립트 파일을 구동하기 위한 프로그램으로, 일반적으로 wscript.exe 프로그램이 실행되면서 js 파일을 실행하는 구조로 되어있다. 사용자가 .js 파일을 더블클릭하면 wscript.exe 프로그램을 통해 js 파일이 실행되면서 악성코드를 다운로드한다. 일반적으로 js 파일의 역할은 악성코드를 다운로드하고 실행하는 것까지만 수행한다.

표 3-1 | 생성되는 파일

[생성되는 파일]

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\V3Z9E5F.tmp\accent.270847031.js
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\qualifier.scr

압축 파일의 압축을 해제하지 않고 열려 있는 상태로 내부의 js 파일을 더블클릭하면 임시 폴더에 js 파일이 복사되어 실행된다. 이후 임시 폴더에 qualifier.scr 파일을 다운로드한 뒤 실행하는데, [그림 3-11]과 같이 Windows 작업 관리자에서 해당 프로세스를 확인할 수 있다. 이 프로세스가 실행되면서 사용자의 문서를 암호화한다.

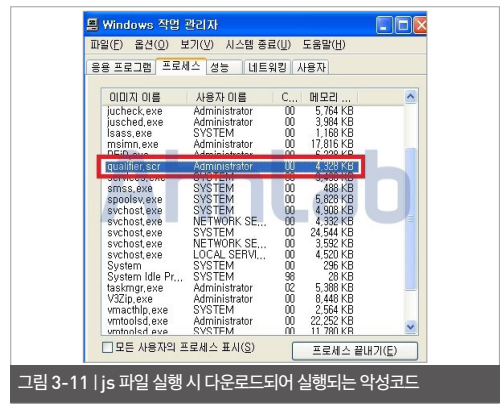


그림 3-11 | js 파일 실행 시 다운로드되어 실행되는 악성코드

V3 제품에서는 해당 록키 랜섬웨어 변종을 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/JS.Downloader (2016.03.08.08)

Trojan/Win32.Locky.R175959 (2016.03.08.04)

2. 테슬라크립트(Tesla Crypt) 4.0 등장

2015년에 악명을 떨쳤던 테슬라크립트(Tesla-Crypt) 랜섬웨어가 지난 2016년 3월 중순 경, 4.0 버전으로 업그레이드되어 나타났다. 새롭게 발견된 테슬라크립트 4.0은 기존 3.0 버전에 비해 한층 진화한 형태를 하고 있다.

먼저, 테슬라크립트 3.0과 4.0의 가장 큰 차이점은 감염 후 암호화된 파일의 확장자명이다. 테슬라크립트 3.0은 [그림 3-12]와 같이 기존 파일명 뒤에 '.micro, .mp3' 등의 문자열이 추가되는 형태로, 어떤 파일이 암호화되었는지 짐작이 가능하다.

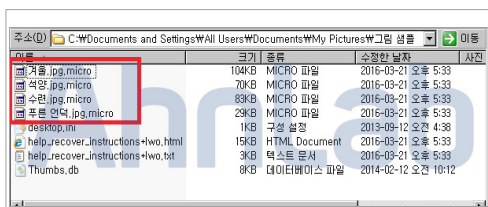
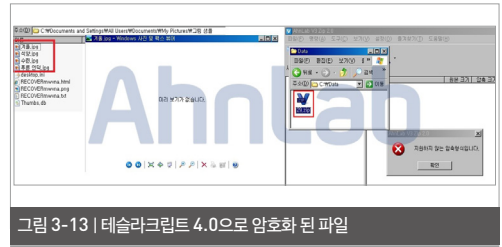


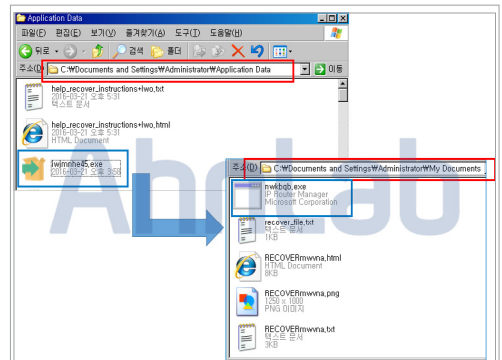
그림 3-12 | 테슬라크립트 3.0의 암호화된 파일 확장자명

그러나 테슬라크립트 4.0은 [그림 3-13]과 같이 암호화된 파일명의 변경이 없어 파일명만으로는 암호화 여부를 알 수 없으며, 해당 파일을 실행한 후 나타나는 에러 메시지를 통해서만 암호화 여부를 확인할 수 있다. 이로 인해 사용자가 랜섬웨어 감염 사실을

인지하기까지 더 많은 시간이 소요되어 적절한 조치를 취하기 어렵게 된다.



테슬라크립트가 실행되면 대부분의 악성코드와 마찬가지로 자가복제 및 자가삭제 행위를 수행한다. 테슬라크립트 3.0과 4.0 버전의 또 다른 차이점은 이 자가복제 파일이 위치하는 경로이다. [그림 3-14]와 같이 3.0 버전은 %Application Data% 경로에, 4.0 버전은 %My Documents% 경로에 자가복제 파일을 저장한다. 이때 '숨김 속성'으로 자가복제하는 것도 이전 버전과 달라진 점이다.



암호화를 완료한 테슬라크립트는 html, png, txt 파일 등을 이용해 사용자에게 PC가 랜섬웨어 감염되었음을 공지하고, 복호화의 대가로 금전을 요구한다.

테슬라크립트 4.0 버전의 결제 유도 파일명 또한 이전 버전과 다르게 변경되어 있는데, [그림 3-15]와 같이 3.0 버전은 help_recover_instructions+xxx, 4.0 버전은 RECOVERxxxxxx로 경고문 페이지의 문자열이 다르다.

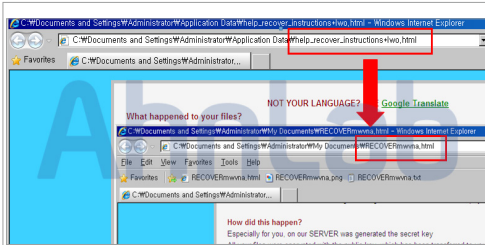


그림 3-15 | 경고문 페이지 문자열 변경

V3 제품에서는 테슬라크립트 4.0을 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Teslacrypt (2016.03.18.01)

3. 맥(Mac) OS X 랜섬웨어 'KeRanger' 등장

최근에는 맥 OS X 사용자들을 노린 랜섬웨어가 처음으로 발견됐다. KeRanger 랜섬웨어가 맥 OS X 전용 토렌트 클라이언트 프로그램인 '트랜스미션 (Transmission)'의 2.90 버전과 함께 배포돼 맥 OS 사용자들 또한 랜섬웨어에 대한 각별한 주의가 필요하다. 트랜스미션 프로그램 설치부터 파일 암호화까지, KeRanger의 일련의 동작 과정을 자세히 살펴보자.

[그림 3-16]과 같이 KeRanger는 Transmission-2.90.dmg 설치 파일을 통해 배포되었다. 실

제 실행되는 Transmission.app에는 유효한 코드 서명이 존재하기 때문에 맥 OS의 게이트키퍼 (GateKeeper)를 우회할 수 있었다.

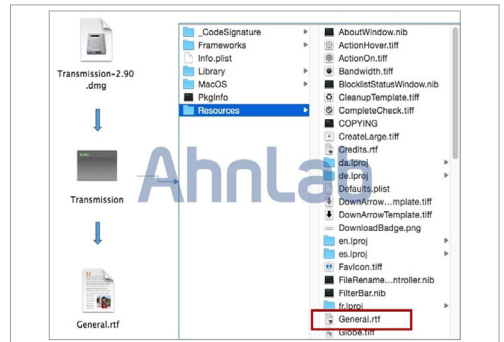


그림 3-16 | 트랜스미션(Transmission) 프로그램 설치

트랜스미션 프로그램이 실행되면 [그림 3-17]과 같이 ~/Library 경로에 .kernel_pid 파일과 .kernel_time 파일이 생성되며, Resources 경로에 있는 General.rtf 파일이 실행된다. General.rtf 파일은 문서 파일 형태로 위장하고 있지만, 실제로는 맥에서 실행될 수 있는 Mach-O 포맷 파일이다.

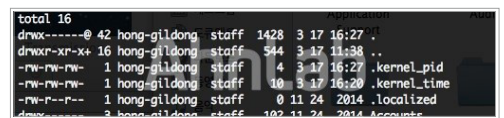


그림 3-17 | ~/Library 경로에 생성된 파일



그림 3-18 | Transmission.app

그 다음, [그림 3-18]에서 확인할 수 있는 바와 같이 pid와 time 파일을 이용하여 3일 동안은 슬립(sleep) 상태로 있다가 3일간의 잠복기를 끝내면 파일 암호화를 진행하고 C&C 서버에 연결을 시도한다. 암호화되는 파일들은 문서 및 그림 파일들을 포함한 수백 개 종류의 파일들이다.



그림 3-19 | 네트워크 정보 및 General.rtf Time Check

암호화가 완료된 파일들은 [그림 3-20]과 같이 .encrypted 확장자가 붙는다.



그림 3-20 | General.rtf Time Check



그림 3-21 | 트랜스미션 홈페이지

KeRanger 랜섬웨어와 관련하여 트랜스미션 공식 홈페이지에는 긴급 공지문과 함께 사용자의 맥 시스템이 KeRanger에 감염됐는지를 확인하고, 만약 감염되었을 경우 해당 랜섬웨어를 제거하는 기능이 포함된 2.92 버전이 게시됐다. 애플(Apple) 또한 OS X의 보안 기능인 XProtect 블랙리스트에 관련 시그니처를 업데이트했다.

이번 사례와 같이 오픈소스를 이용해 코드 인증이 된 경우에는 보안 솔루션의 탐지를 우회할 수 있기 때문에 사용자들의 각별한 주의가 필요하다.

V3 제품에서는 KeRanger 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

OSX64/Keranger.139264

OSX64/Keranger.1269584

BinImage/Keranger

지금까지 살펴본 바와 같이 최근 악성코드 제작자들은 사용자들을 속이고 보안 솔루션의 탐지를 회피하기 위해 다양한 기법과 기능을 추가한 랜섬웨어 변종을 지속적으로 제작 및 유포하고 있다. 특히 랜섬웨어는 암호화 알고리즘을 이용하여 시스템 내의 파일을 암호화하기 때문에 감염된 이후에는 사실상 파일 복구가 어렵다. 따라서 랜섬웨어에 감염되지 않도록 의심스러운 이메일 등을 주의하고 백신 및 주요 프로그램의 최신 업데이트 적용 등 기본적인 보안 수칙을 준수하는 습관이 필요하다. 또한 중요한 데이터는 주기적으로 별도 백업을 해두는 것도 방법이다.

랜섬웨어 감염을 예방하기 위한 보안 수칙은 다음과 같다.

1. 발신인이 불분명한 이메일은 가급적 열어보지 않는다.
2. 악성코드를 첨부한 영문 스팸 메일은 대부분 Payment, Invoice, Shipping, Order와 같은 단어들을 포함하고 있는 점을 참고한다.
3. 업무상 송장이나 대금 결제 등을 영문 메일로 하는 경우에는 발신자를 확인하고, 거래 업체에 확인하는 등의 과정을 거친다.
4. 첨부 파일 또는 첨부된 압축 파일 내에 js 확장자명을 가진 파일이 존재하면 실행하지 않는다.
5. 백신 프로그램을 최신 엔진으로 항상 유지하고, 실시간 감시 기능을 활성화한다.
6. 첨부 파일은 바탕화면에 저장하여 백신으로 검사한 다음, 실행하거나 열람한다.
7. 메일 본문에 언급된 URL이나 IP 주소는 가급적 접속하지 않는다.
8. 확장명 숨기기 기능을 해제하여 .exe 등의 확장명을 숨기는 파일에 속지 않는다.

AhnLab

ASEC REPORT VOL.75

March, 2016

집필 **안랩 시큐리티대응센터 (ASEC)**
편집 **안랩 콘텐츠기획팀**
디자인 **안랩 디자인팀**

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

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.