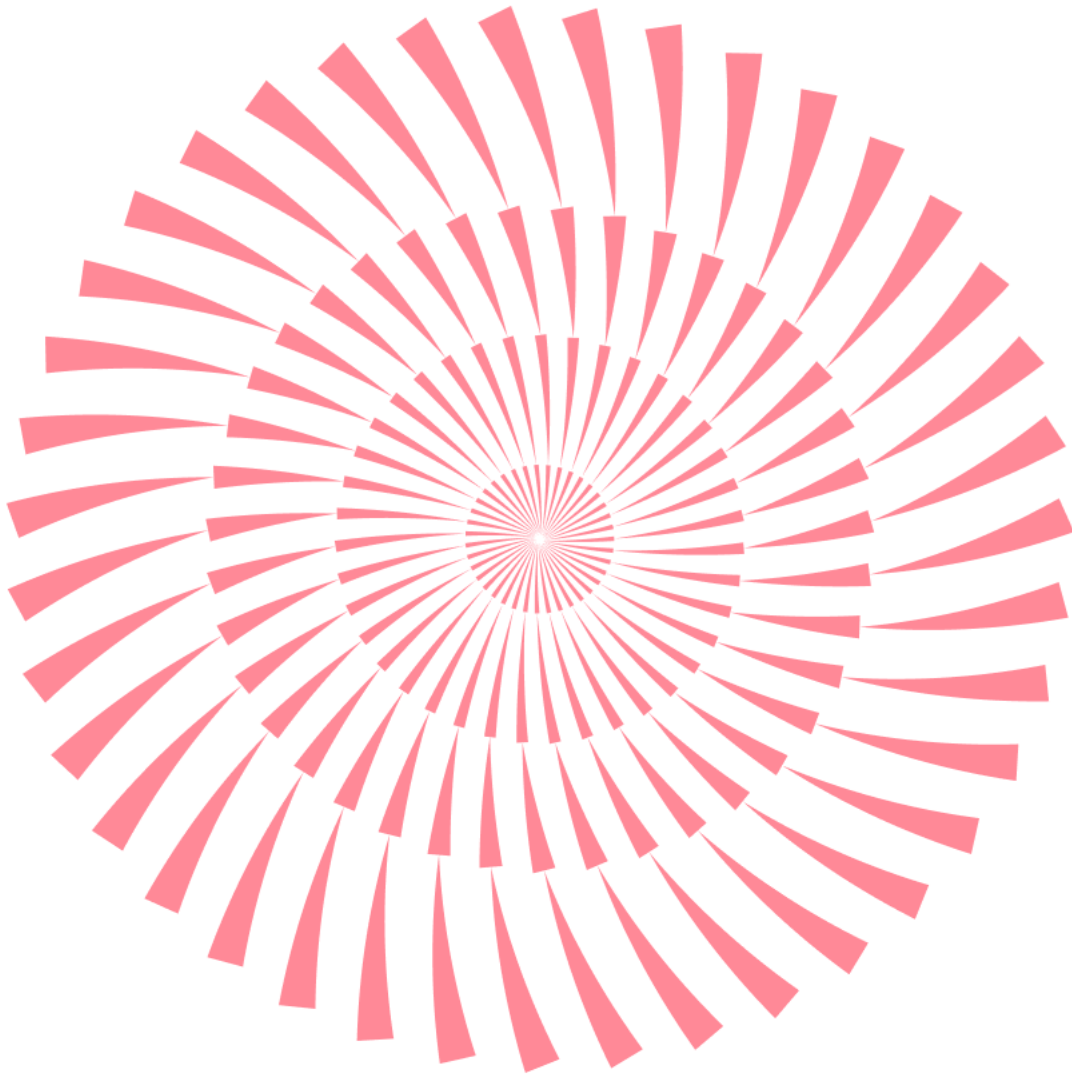


No.178 | 2024.7

# ESRC 보안동향보고서

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



# ESRC 보안동향보고서

# CONTENTS

## 1 악성코드 통계 및 분석

01-05

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

---

## 2 최신 보안 동향

06-09

기업 및 기관의 공식 번호를 사칭하여 유포되는 스미싱 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

북한 위협 그룹인 라자루스(Lazarus)는 LinkedIn 을 통해 블록체인 및 암호화폐 이해 관계자를 타겟으로 대규모 소셜 엔지니어링 Node.js 공격을 수행하였습니다. 공격자는 합법적인 면접관으로 가장하여 이메일과 채팅 앱을 통해 피해자와의 신뢰를 구축했습니다. 신뢰가 구축되면 피해자에게 GitHub 와 같은 오픈 소스에서 채용 테스트로 위장한 소프트웨어를 다운로드하고 실행하도록 요청하였으며, 이 소프트웨어에는 악성 Node.js 페이로드가 포함되어 있습니다. 실행되면 base64 및 XOR 인코딩 페이로드를 디코딩하여 하드코딩된 C2 서버에 연결하여 추가 스크립트를 실행했습니다. 이 스크립트는 시스템 정보를 수집하고 원격 액세스를 허용하여 공격자가 피해자의 시스템에 손상을 입힐 수 있습니다.

Storm-1789 라고도 알려진 'Moonstone Sleet'은 Microsoft 가 새로 확인한 북한 사이버 위협 그룹입니다. 이들은 가짜 웹사이트와 소셜 미디어 프로필을 만들고 LinkedIn 을 통해 트로이 목마에 감염된 소프트웨어와 npm 패키지를 배포하고, 'DeTankWar'라는 악성 게임을 통해 악성 코드를 확산시키는 것 뿐만 아니라 660 만 달러 상당의 비트코인을 요구하는 'FakePenny' 랜섬웨어를 유포하기도 하였습니다. 이들은 Lazarus 그룹의 코드 재사용과 악성 게임 개발과 같은 기존 고전적인 전략을 결합하여 소프트웨어, IT, 교육 및 국방 분야를 타겟으로 끊임없이 진화하고 있습니다.

김수키(Kimsuky) 그룹의 한국 정부 및 민간 부문 조직을 타겟으로 한 'Gomir'라는 새로운 Linux 백도어를 발견되었습니다. 트로이 목마 소프트웨어 설치 프로그램을 통해 배포되는 Gomir 는 루트 권한 및 crontab 항목을 통해 지속성을 유지하고, 원격 명령 실행 및 데이터 추출을 위한 직접적인 명령 및 제어(C2) 통신을 활성화합니다. 이는 윈도우 시스템을 타겟으로 하는 GoBear 백도어와 대부분 코드 구성을 공유합니다. Gomir 의 기능에는 셸 명령 실행, 시스템 구성 보고, 파일 조작, 포괄적인 시스템 제어 및 데이터 탈취 등이 포함됩니다. 따라서, 보안 관리자는 강력한 엔드포인트 보안을 구현하고, 신뢰할 수 없는 소프트웨어 소스를 피하고, 이러한 위협에 대응하기 위해 업데이트된 시스템을 유지해야 합니다.

APT 그룹 DarkPeony 가 이끄는 'Operation ControlPlug'는 미얀마, 필리핀, 몽골, 세르비아의 군대 및 정부 조직을 타겟으로 삼는 정교한 사이버 위협 캠페인이 공개되었습니다. 이 캠페인은 MMC(Microsoft Management Console) 파일(.msc)을 사용하여 PowerShell 스크립트를 실행하고 PlugX와 같은 추가 페이로드를 사이드 로드하는 악성 DLL 이 포함된 MSI 파일을 다운로드합니다. 이 캠페인은 공격자가 시스템 관리 도구에 대해 고도로 이해하고 있으며, 탐지를 회피하기 위해 DLL 사이드 로딩을 사용한다는 특징이 있습니다. 최근에는 한국과 일본의 북한 인권 및 반북 운동가들을 겨냥한 공격도 가해졌는데, 이는 김수키(Kimsuky) 조직이 주도한 것으로 보입니다.

2024 년 2 월 EclecticIQ 가 공개한 금융기관 직원의 마이크로소프트 365, 오피스 365 계정을 표적으로 한 서비스형 피싱(Phishing-as-a-Service) 플랫폼 'ONNX Store'이 강세를 보이고 있습니다. 이 플랫폼은 텔레그램 봇을 통해 운영되며, 2 단계 인증을 우회하고 악성 QR 코드를 사용한다. HR 부서에서 보낸 것으로 가장한 피싱 이메일을 통해 가짜 Microsoft 365 로그인 페이지로 유도합니다. 'MRxCODER'가 관리하는 Caffeine 피싱 키트의 리브랜딩 버전으로 추정되는 이 피싱 플랫폼은 민감한 로그인 정보를 실시간으로 탈취합니다. 이에 보안 담당자는 확인되지 않은 PDF/HTML 첨부 파일을 차단하고, 신뢰할 수 없는 HTTPS 사이트에 대한 액세스를 제한하고, FIDO2 하드웨어 보안 키를 구현하는 등의 대응을 통해 나날이 정교하고 진화하는 피싱 공격으로부터 보호해야 합니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

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

2024 년 6 월에는 Gen:Variant.Lazy.266772 와 Trojan.Downloader.MSIL 탐지명이 지난 달과 동일하게 1, 2 위를 차지하였습니다.

그 밖에 Trojan.GenericKD.72973671, Gen:Variant.Lazy.540900, Trojan.GenericKDZ. 106329, Gen:Variant.Tedy.521942, Trojan.GenericKD.72225706 탐지명이 새롭게 순위권에 자리하였습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.Lazy.266772	ETC	113,329
2	-	Trojan.Downloader.MSIL	Trojan	104,283
3	NEW	Trojan.GenericKD.72973671	Trojan	65,277
4	↑6	Trojan.DDoS.Nitol.gen	Trojan	35,926
5	↓2	Misc.HackTool.AutoKMS	ETC	34,055
6	↓2	Backdoor.Generic.792814	Backdoor	32,003
7	NEW	Gen:Variant.Lazy.540900	ETC	30,747
8	↓2	Gen:Variant.Razy.241020	ETC	25,584
9	↓4	Gen:Variant.Lazy.20522	ETC	25,068
10	NEW	Trojan.GenericKDZ.106329	Trojan	24,032
11	↓2	Gen:Variant.Ulise.144799	ETC	23,463
12	NEW	Gen:Variant.Tedy.521942	ETC	22,712
13	↓5	Application.Hacktool.BBJ	ETC	21,523
14	NEW	Trojan.GenericKD.72225706	Trojan	20,005
15	↓2	Win32.Neshta.A	Virus	18,670

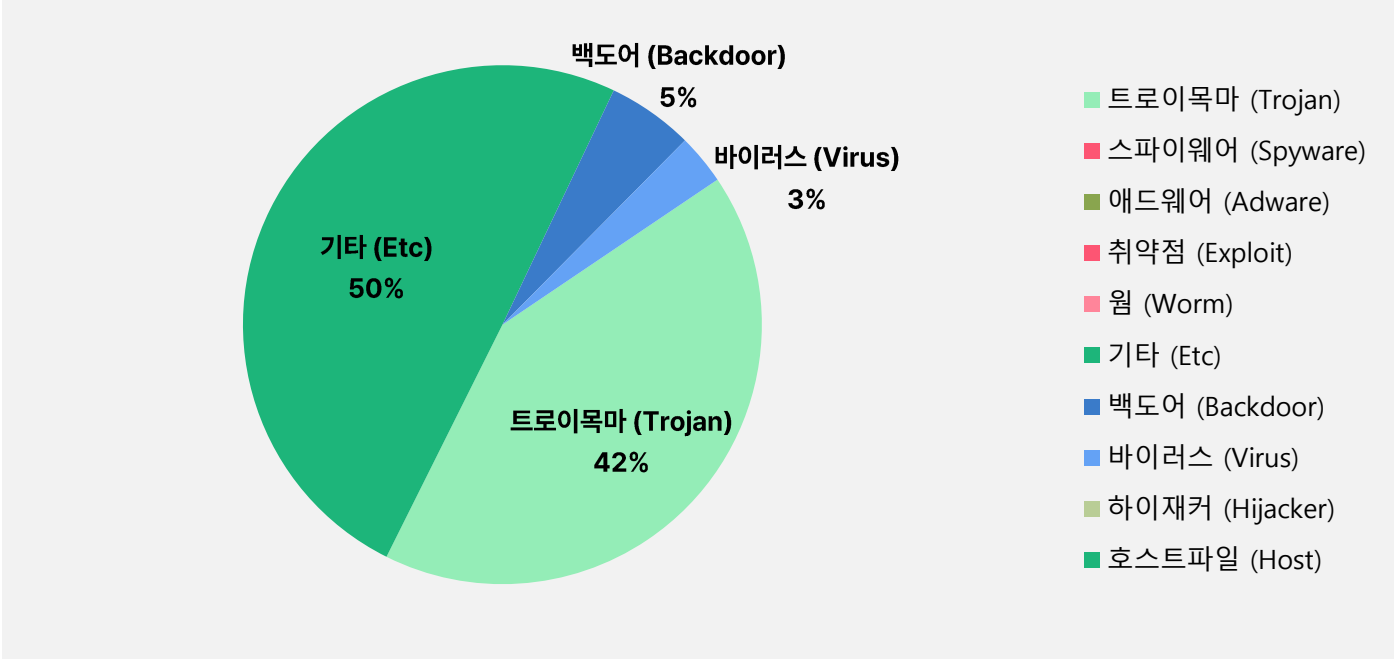
\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024년 6월 1일 ~ 2024년 6월 30일

### 악성코드 유형별 비율

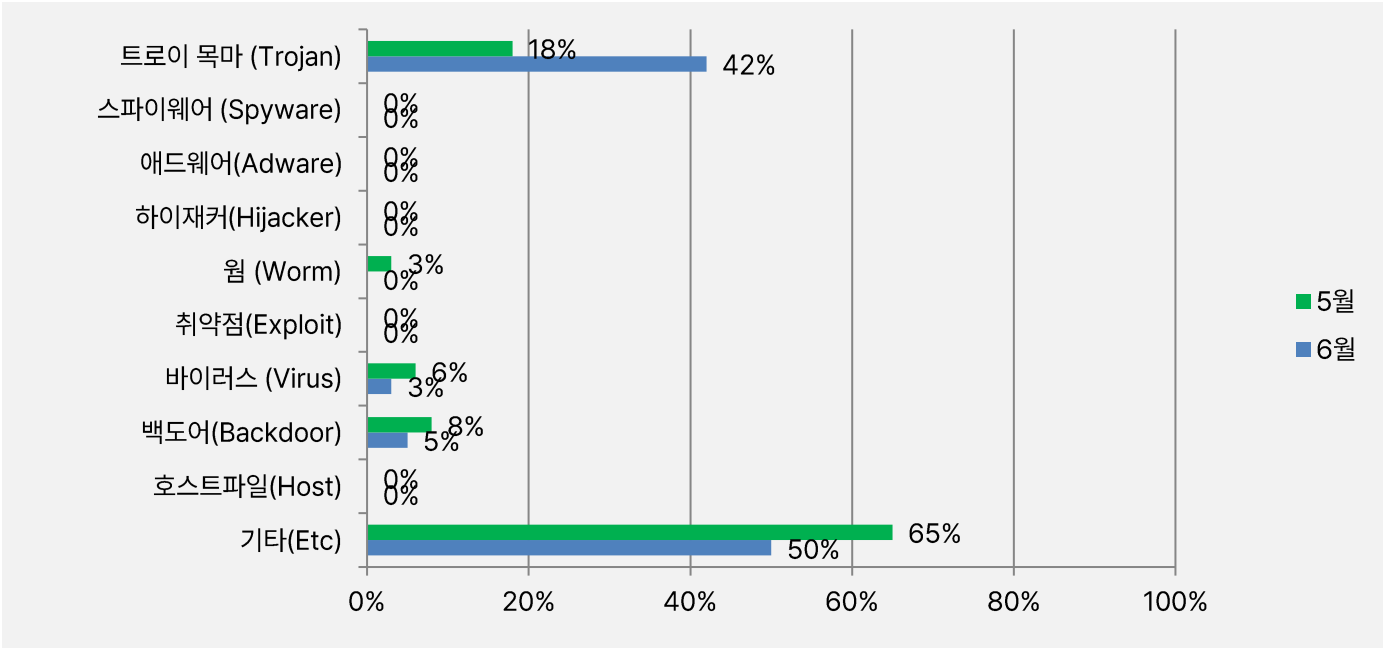
악성코드 유형별 비율에서 기타(ETC) 유형이 50%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마 (Trojan) 유형이 42%, 백도어(Backdoor) 유형이 5%, 바이러스 (Virus) 유형이 3%로 확인되었습니다.

2024 년 5 월과 비교하여 전체 감염 건수는 1.3 배 가량 증가하였습니다.



### 카테고리별 악성코드 비율 전월 비교

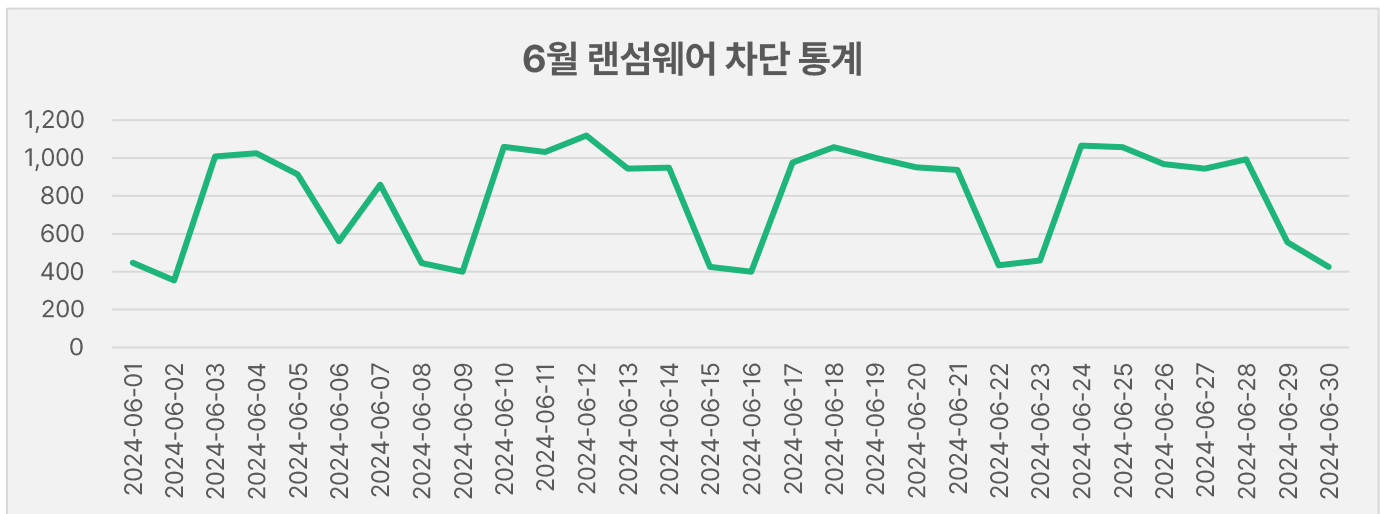
2024 년 6 월에는 지난 5 월과 비교하여 트로이목마(Trojan) 유형이 24% 대폭 증가하였고, 기타(ETC) 유형이 15% 감소하였습니다. 또한, 백도어(Backdoor) 유형과 바이러스(Virus) 유형이 각각 3%씩 감소하였습니다.



### 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 30일까지 23,151건의 랜섬웨어 공격 시도가 차단되었습니다.



#### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 6 월 한 달간 총 7,803,314 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 5 월 한 달간 확인되었던 8,053,634 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.3.% 가량 감소한 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.



# 2

## 최신 보안 동향

## 기업 및 기관의 공식 번호를 사칭하여 유포되는 스미싱 주의!

최근 다양한 내용으로 스미싱이 급증하는 가운데 기업 및 기관의 고객센터번호를 사칭한 스미싱이 지속적으로 발견되고 있어 사용자분들의 각별한 주의가 필요합니다.

스미싱은 다음과 같이 꾸준히 발견되고 있는 '범칙금, 과태료 부과' 등의 내용과 함께 '접근제한 조치'라는 새로운 유형이 추가되어 유포되고 있습니다.

국토교통부(1599-00001) 사칭 스미싱

[Web 발신] 06/02 일 귀하의 범칙금이 1회 미납되었습니다. - 3회 미납시 고발조치 안내: t.\*\*/9Y\*\*\*

[Web 발신] 06/02 일 귀하의 범칙금이 미처리 1건이 있습니다 - 3회 누적 고발조치 내역: t.\*\*/a1\*\*\*

\*\*\*\*시립여성보호센터(\*\*-\*\*\*\*-4502) 사칭 스미싱

[Web 발신][수사중] (제 21-111) 스토킹처벌법에 의거 접근제한 조치되었습니다 - 수사 종결까지 상세: x\*\*

여성긴급전화 1366\*\*여성센터(\*\*-\*\*\*\*-8555) 사칭 스미싱

[Web 발신][경고] (20-12) 스토킹 피해자요청으로 접근제한 조치 - 수사 종결까지 안내: x\*\*.[.]m\*/998

정부 24 콜센터(1588-2188) 사칭 스미싱

[Web 발신] 쓰레기 무단투기 과태료 부과 1회 위반 10만원 부과 예정 입니다 hxxps://s\*\*\*\*\*[.]at/a\*\*\*\*

[Web 발신] \*알림\* 분리수거 미실시 과태료 부과 대상 안내 hxxps://s\*\*\*[.]link/A\*\*\*\*

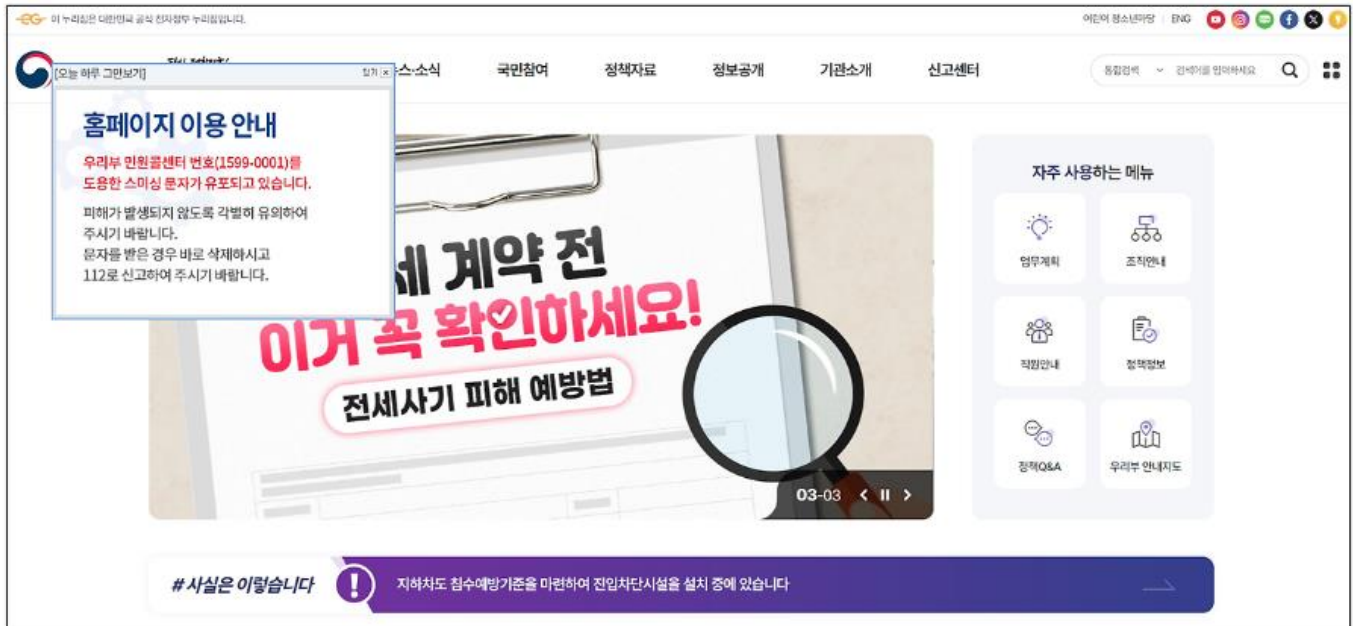
국민건강보험공단(1577-1000) 사칭 스미싱

[Web 발신] 국민건강 검진통지서 자세한 내용 확인 hxxps://b\*\*[.]h\*\*\*\*\*[.]online

[Web 발신] 건강검사 통지서 발송완료,상세보기 hxxps://a\*\*[.]ha\*\*\*\*\*[.]\*\*/

위와 같은 스미싱은 법 위반 관련 키워드를 이용하여 사용자들에게 불안감을 조성하고 문자 내 링크 클릭을 유도하며, 전달된 링크로 연결 시 관련 정부기관의 공식 홈페이지를 위장한 피싱 사이트로 이동된 후 개인정보 입력 또는 악성 앱 설치를 유도합니다.

법 위반 및 각종 벌금과 관련되어 사전 신청을 통한 문자 안내 서비스가 일부 존재하고 있으나 해당 경우를 제외하고는 문자로 안내되는 사항이 없다는 점을 반드시 기억하셔야 합니다. 이러한 법 위반 및 각종 벌금에 대한 내용은 직접 관련 기관 공식 홈페이지로 접속하여 부과 여부를 확인할 수도 있습니다.

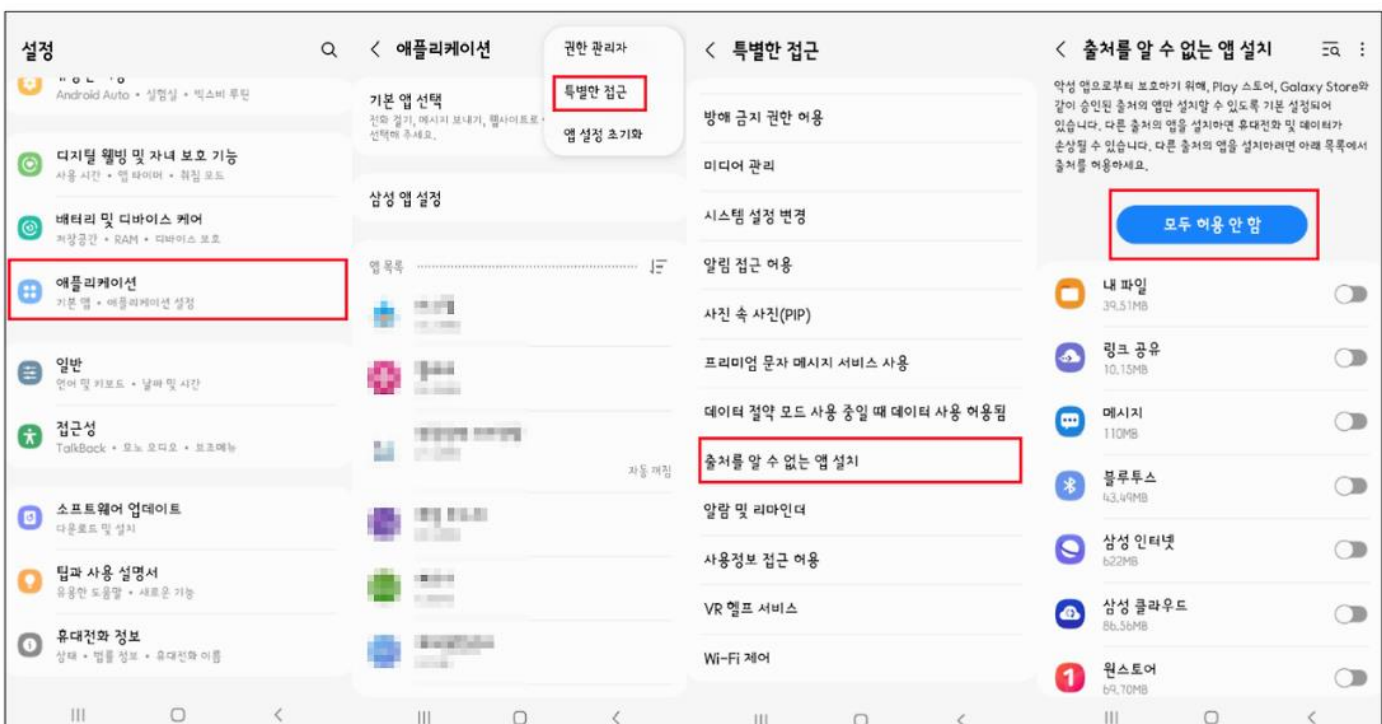
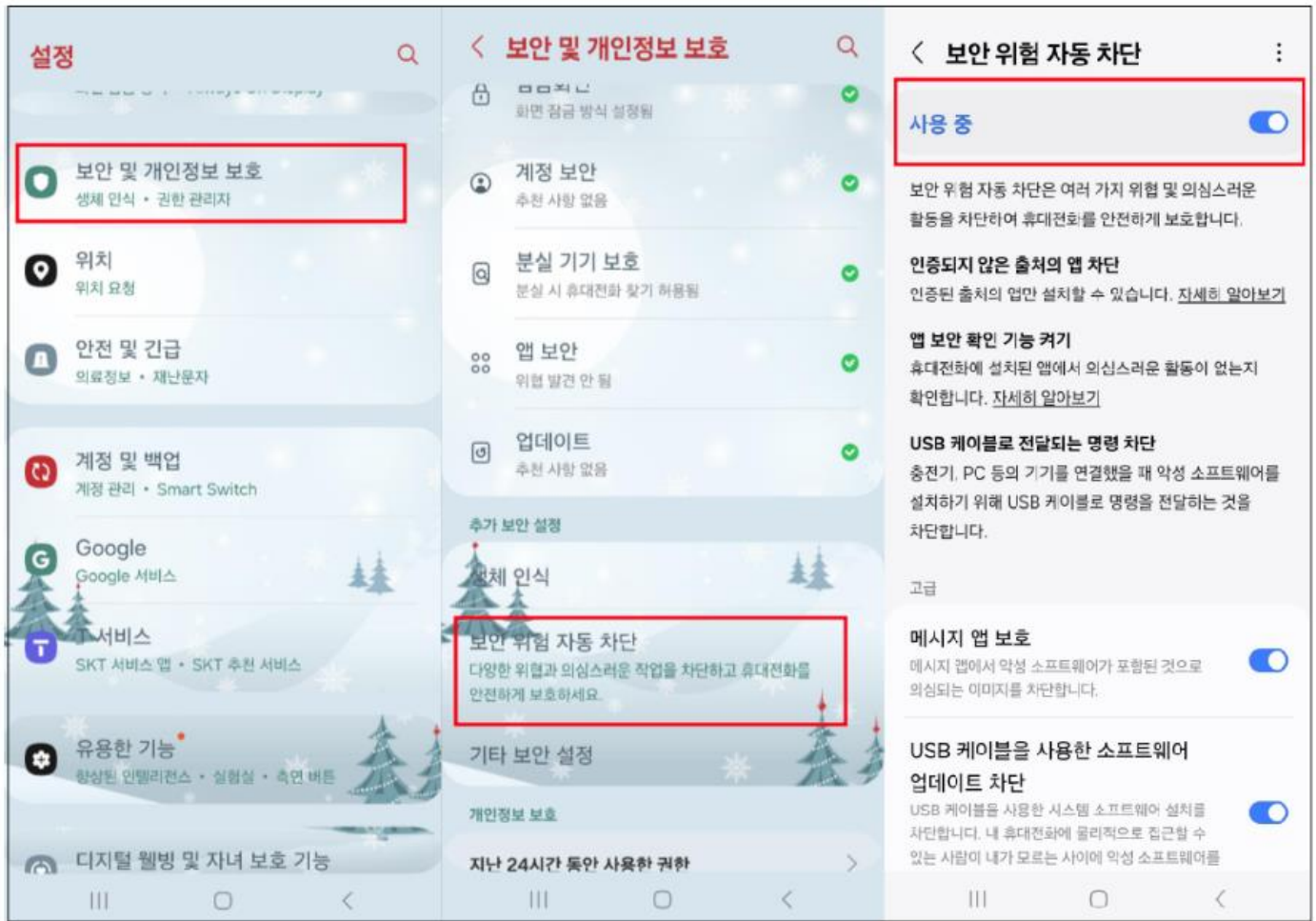


[그림 1] 공식 홈페이지 방문 시 보여지는 스미싱 주의 공지

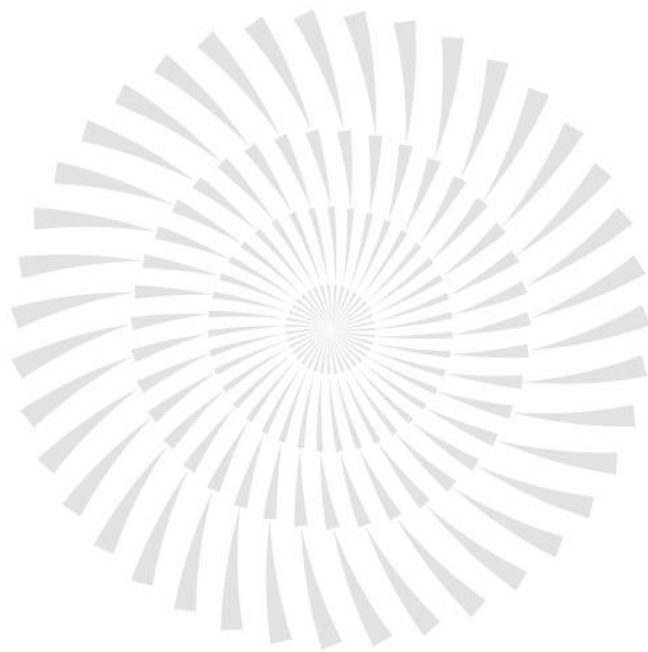
스미싱 수법이 갈수록 교묘해지는 가운데 기업이나 공공기관의 공식 번호를 사칭하는 스미싱까지 발견되고 있어 피해 사례가 늘어나고 있습니다. 공식 번호를 통해 전송된 문자라도 링크가 포함되어있거나 콜백을 유도하는 등의 문자는 스미싱 여부를 의심해 보시고 직접 발신번호로 연락하거나 링크를 클릭하지 않도록 각별히 주의하시기 바랍니다.

만약 실수로 악성 링크로 접속하여 개인정보를 입력하거나 악성 앱이 설치되었다면 즉시 휴대폰 기기를 비행기 모드로 전환하여 인터넷 연결을 차단하시고 관련 기관에 스미싱 피해신고 및 계좌 출금/지급 정지, 명의도용 차단 등을 진행하여 2차 피해를 최소화하는 것이 중요합니다.

또한 스미싱으로 전파되는 악성 앱은 대부분 안드로이드 공식마켓에 업로드 된 앱이 아니므로 출처가 불분명한 앱이 설치되지 않도록 휴대폰 기기 내 보안 설정을 확인하시어 아래와 같이 차단설정 진행을 권해드립니다.



[그림 2] 휴대폰 기기 내 보안 설정 화면 (Android 14 - 위 / Android 14 이하 - 아래)



(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

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