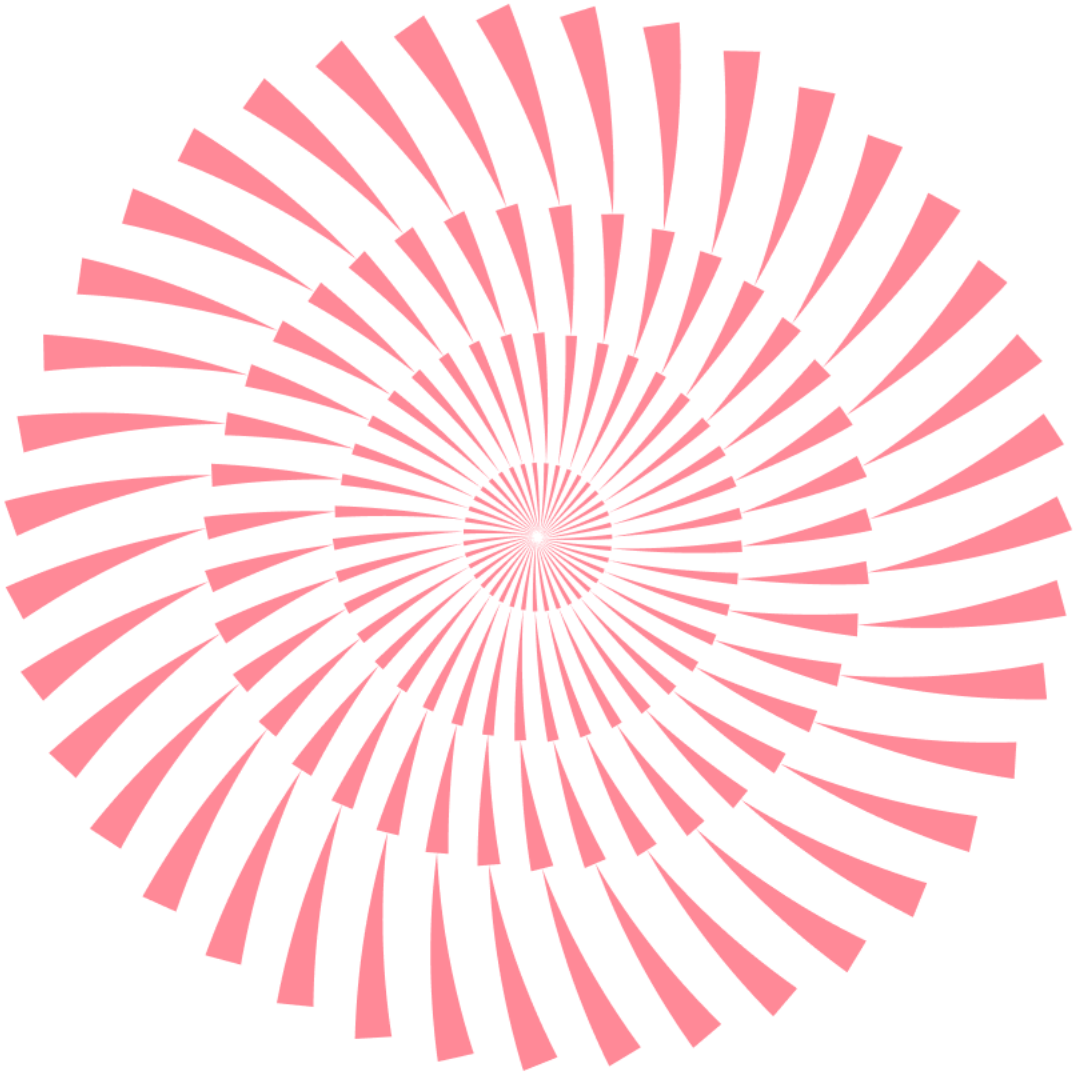
No.180 | 2024.9

ESRC 보안동향보고서

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



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

1. 악성코드 동향

북한 정부가 지원하는 위협그룹 '킴수키(Kimsuky)'가 국내의 대학 직원, 연구원, 교수들을 표적으로 삼는 피싱 캠페인이 연이어 발견되고 있습니다. 공격자는 손상된 호스트를 사용하여 난독화된 Green Dinosaur 웹셸 버전을 배포하고, 합법적인 로그인 포털과 유사한 피싱 페이지가 포함된 가짜 사이트를 만들었습니다.

이 페이지는 동덕여대, 고려대, 연세대 등의 기관을 타깃으로 로그인 계정 정보를 탈취하기 위해 피싱 이메일이 전송하는 방식을 사용하였습니다. 가짜 로그인 페이지는 매우 정교하게 만들어져 실제 로그인 페이지와 구별하기 어려우며, 피해자가 로그인 정보를 입력하면 사용자 ID, 비밀번호, 로그인 시도 등의 정보가 공격자에게 전송되고 실제 로그인 페이지로 리디렉션되었습니다.

최근에는 앞서 언급한 대학교 외에 연세대, 서울대, 충남대의 사례도 확인되어 지속적인 관찰과 대응이 필요합니다.

지난 7 월 말 버그가 있는 CrowdStrike Falcon 업데이트로 인해 전 세계적으로 Windows 시스템에 블루 스크린이 발생한 이후, 해당 이슈를 악용하여 공격자들의 다양하고 정교한 공격들이 확산되었습니다.

첫 번째 공격은 Microsoft 의 복구 지침을 모방한 Word 문서가 포함된 피싱 이메일이 사용되었는데, 이 문서에는 Chrome, Edge, Firefox 및 베트남 Cốc Cốc 을 포함한 기타 Chromium 기반 브라우저의 데이터를 훔치기 위해 악성 DLL(Daolpu 스틸러)을 실행하는 매크로가 포함되어 있습니다. 두 번째 공격 사례는 이란 해킹 그룹이 CrowdStrike 로 위장한 이메일이 시스템 복구 도구로 위장한 피싱 PDF 메일 공격이 있습니다. PDF 파일 내 "Download The Updater" 링크를 클릭하면 이란 해킹 그룹으로 추정되는 조직이 이스라엘 정부 기관을 표적으로 삼는 Wiper 페이로드가 배포되었습니다. 세 번째 공격은 스페인 BBVA 은행 고객을 표적으로 삼았습니다. 피싱 사이트는 BBVA 인트라넷 포털을 사칭하여 CrowdStrike 핫픽스 업데이트로 위장한 악성 ZIP 파일을 배포하였고, 포함된 "Setup.exe"를 실행하면 Remcos RAT 가 감염되어 시스템 제어 및 민감한 데이터가 탈취되었습니다.

뿐만 아니라, 악성코드를 유포하거나 민감한 정보를 훔치기 위해 사용자를 속여 가짜 결제 사이트나 암호화폐 사이트를 방문하도록 유도하는 'CrowdStrike' 키워드 관련 피싱 도메인도 다수 확인되었습니다.

소프트웨어 개발자를 속여 면접 과정의 일부로 위장하여 GitHub 에 호스팅된 악성 소프트웨어를 다운로드하도록 하는 DEV#POPPER 캠페인이 Windows, Linux, macOS 를 포함한 다양한 운영 체제를 대상으로 확대되었습니다.

이 공격에서 공격자는 개발자를 찾는 면접관으로 가장하여 합법적인 파일과 유해한 파일이 모두 포함된 ZIP 파일을 보내는 사회공학적 방식을 사용합니다. 파일 내부에는 악성 JavaScript 가 숨겨져 있고, Base64 인코딩, 함수명 무작위 등 매우 난독화되어 백신을 통한 탐지가 어려운 특징을 가지고 있습니다. 악성 스크립트가 실행되면 시스템의 OS 를 확인하고 원격 서버에 연결하며, Python 백도어(InvisibleFerret)와 같은 추가 페이로드를 실행하여 브라우저 쿠키 도용, 명령 실행, 파일 추출과 같은 악의적인 작업이 가능해집니다.

최근 샘플에서는 고급 난독화, 원격 모니터링을 위한 AnyDesk 활용, 개선된 FTP 유출, Chrome, Opera 및 Brave 의 민감한 브라우저 정보를 대상으로 하는 특징도 추가로 보이고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2024 년 8 월에는 Gen:Variant.TDss.49 와 Gen:Variant.Lazy.266772 탐지명이 지난 달과 동일하게 1, 2 위를 차지하였습니다. 그 밖에 Trojan.MSIL.Bladabindi, Gen:Variant.Jaik.38715, IL:Trojan.MSILZilla.138369 탐지명이 새롭게 순위권에 자리하였습니다.

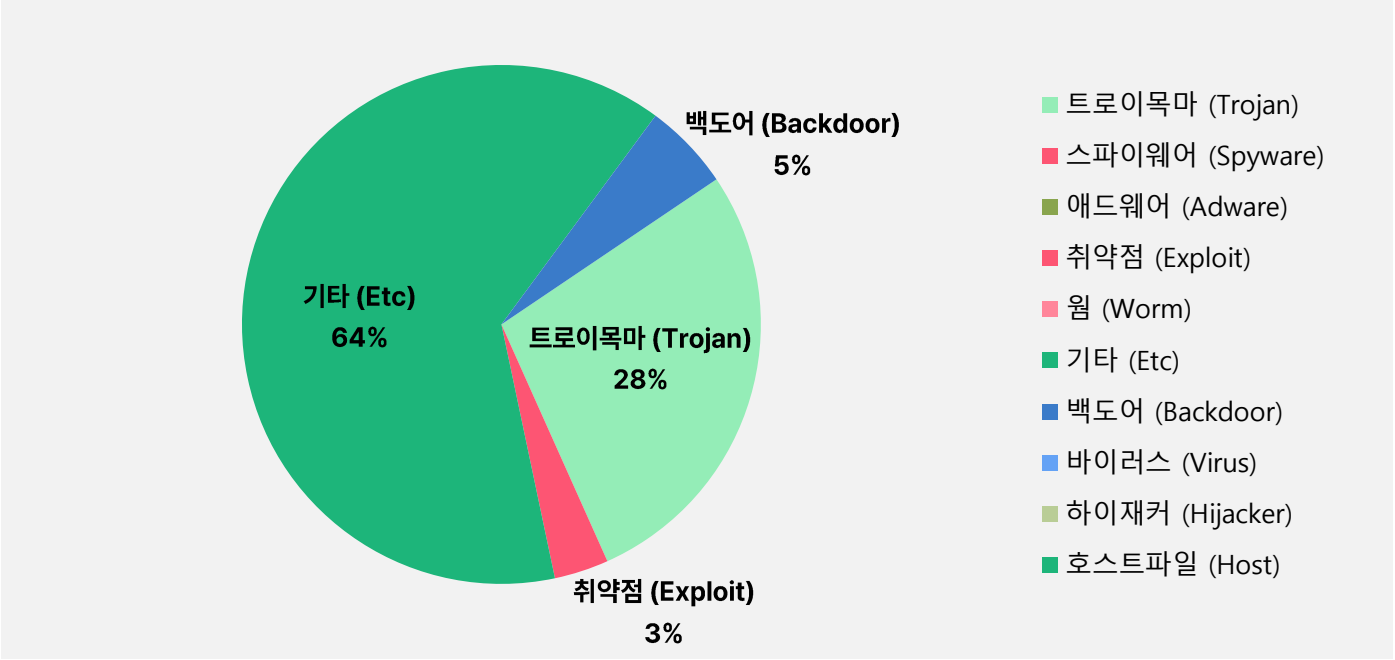
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.TDss.49	ETC	184,800
2	-	Gen:Variant.Lazy.266772	ETC	108,030
3	↑3	Trojan.GenericKD.72973671	Trojan	62,215
4	↑6	Misc.HackTool.AutoKMS	ETC	48,994
5	↓1	Gen:Variant.Lazy.540900	ETC	44,583
6	↑2	Backdoor.Generic.792814	Backdoor	39,795
7	NEW	Trojan.MSIL.Bladabindi	Trojan	35,939
8	NEW	Gen:Variant.Jaik.38715	ETC	34,401
9	↓2	Trojan.Downloader.MSIL	Trojan	32,417
10	↓1	Trojan.DDoS.Nitol.gen	Trojan	26,933
11	NEW	IL:Trojan.MSILZilla.138369	Trojan	26,230
12	↓9	Exploit.CVE-2010-2568.Gen	Exploit	24,840
13	↓2	Gen:Variant.Lazy.20522	ETC	23,348
14	↓1	Application.Hacktool.BBJ	ETC	20,638
15	↓1	Trojan.Acad.Bursted.AK	Trojan	19,574

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 8 월 1 일 ~ 2024 년 8 월 31 일

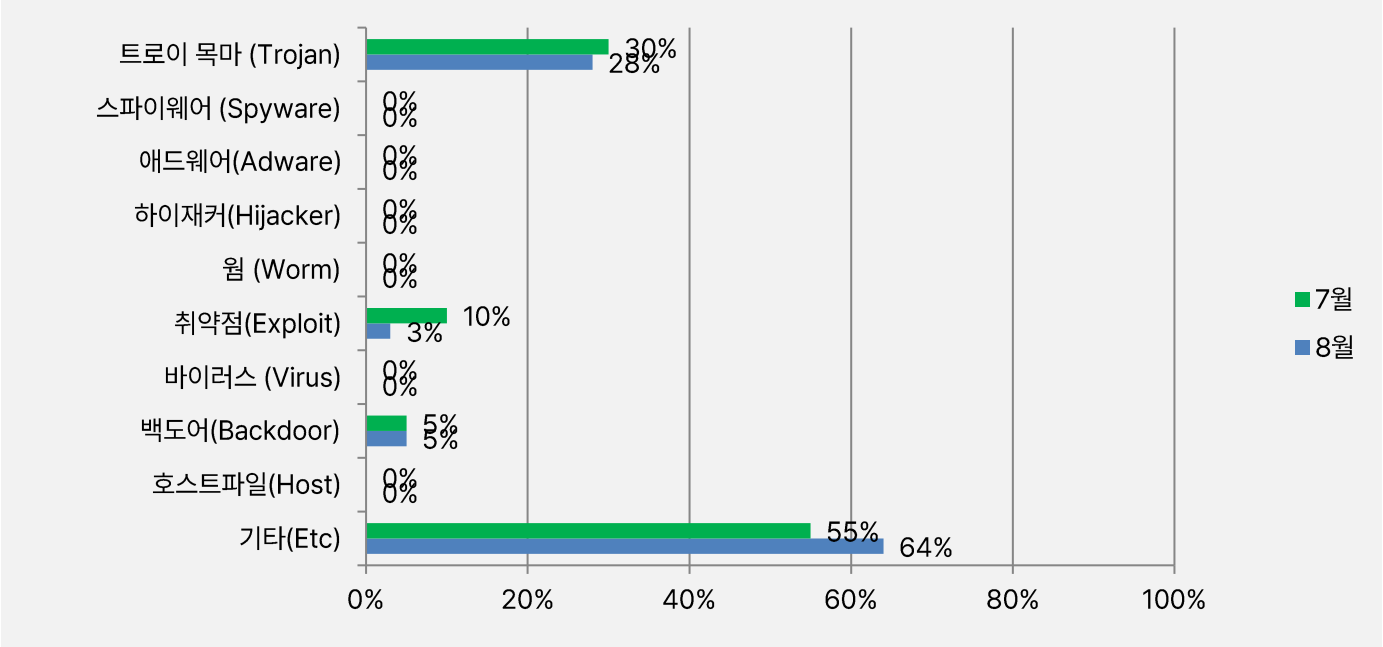
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 64%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 28%, 백도어(Backdoor) 유형이 5%, 취약점(Exploit) 유형이 3%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

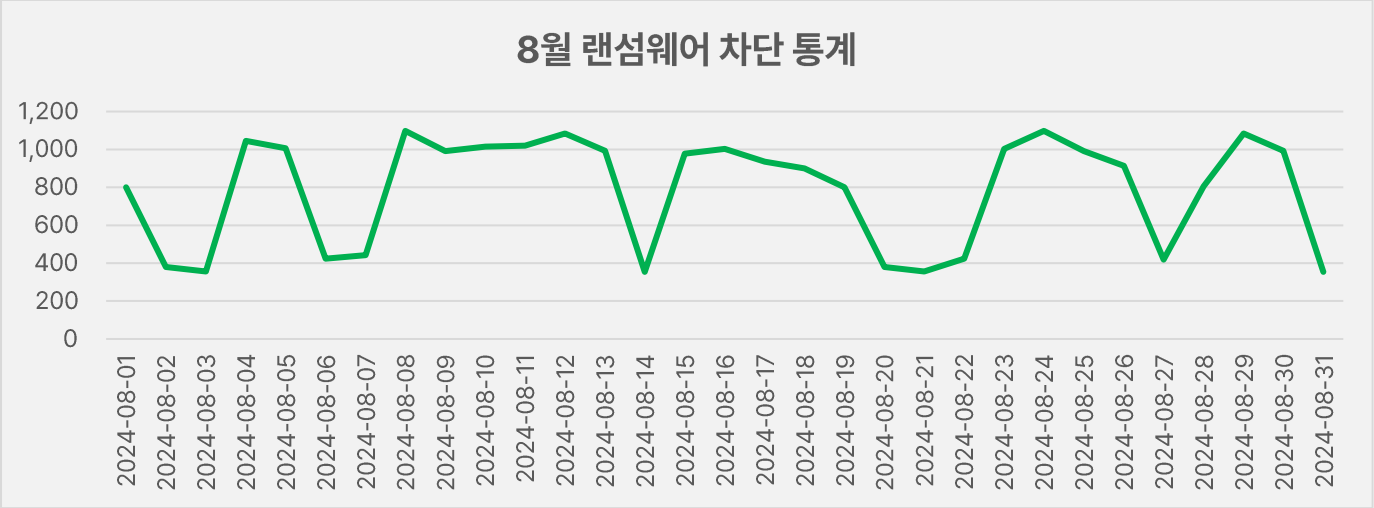
2024년 8월에는 지난 7월과 비교하여 기타(ETC) 유형이 9% 대폭 증가하였고, 트로이목마(Trojan) 유형이 2% 감소하였습니다. 또한 취약점(Exploit) 유형이 7%씩 감소하였고, 백도어(Backdoor) 유형은 동일 수치를 기록하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

8 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. 8 월 1 일부터 8 월 31 일까지 24,447 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한 달간 총 8,135,732 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 7 월 한 달간 확인되었던 8,171,559 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.01% 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

설문조사를 위장하여 개인정보 탈취를 시도하는 스미싱 주의!

최근 공식기관의 설문조사 이벤트를 사칭하여 개인정보 탈취를 시도하는 스미싱이 발견되고 있어 사용자분들의 주의가 필요합니다.

해당 스미싱은 경품지급 또는 급여지원 등의 키워드로 사용자를 현혹하여 설문조사 참여를 유도합니다.

[Web 발신]간단한 설문 참여 하시고 상품 받아가세요 참여시 100% 지급 응모하기 hxxps:vv*.i*/e***

[Web 발신]부모급여지원캠페인 설문시 무조건 급여지원 해드립니다! ▼설문하기▼ hxxps://vv*.i*/캠패인

[Web 발신]부모급여지원캠페인 간단한 설문조사 참여만 해도 경품지급 설문참여 ☞hxxps://vv*.i*/캠페인

[Web 발신]부모급여지원 설문지작성하고 지원받기 설문지작성 ☞hxxps://vv*.i*/부모설문

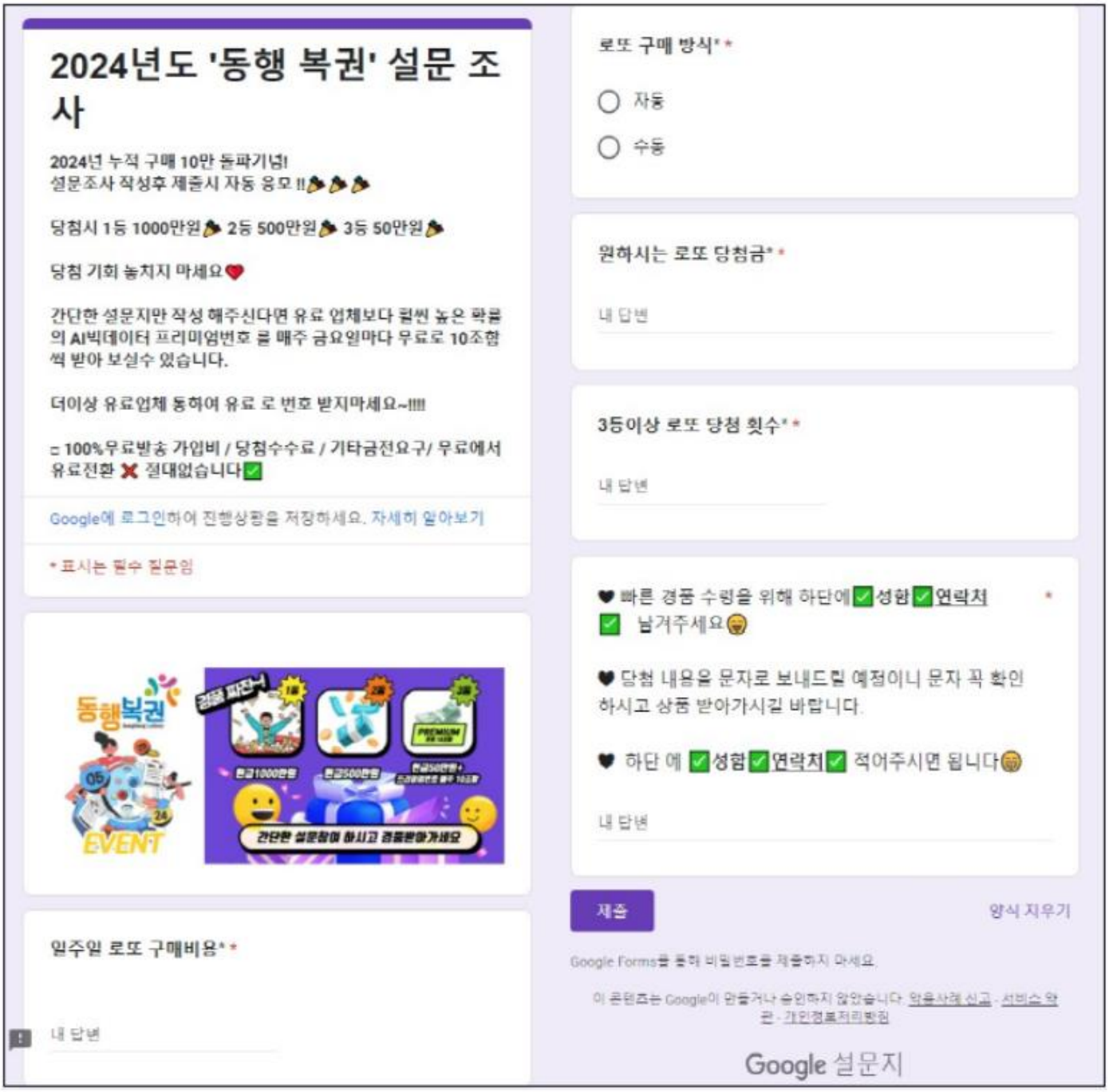
[Web 발신]부모급여지원캠페인 부모라면 누구든 참여가능 설문참여시 경품지급 hxxps://vv*.i*/급여지원

[Web 발신] 키움증권 소비자 만족도 조사 키움증권 소비자 만족도 조사에 참여해주시는 모든분들께 소정의 기프티콘상품권을 발송해드립니다. hxxps://u**.k*/t*mr**

* 소비자 만족도 조사 참여방법 위 URL 을 클릭하여 소비자 만족도 조사 페이지이동 > 설문조사 참여 후 기프트콘 100%지급 받기 > 끝
※ 키움증권 준법감시인심사필 제 24-92714 호(20240312~20250311)

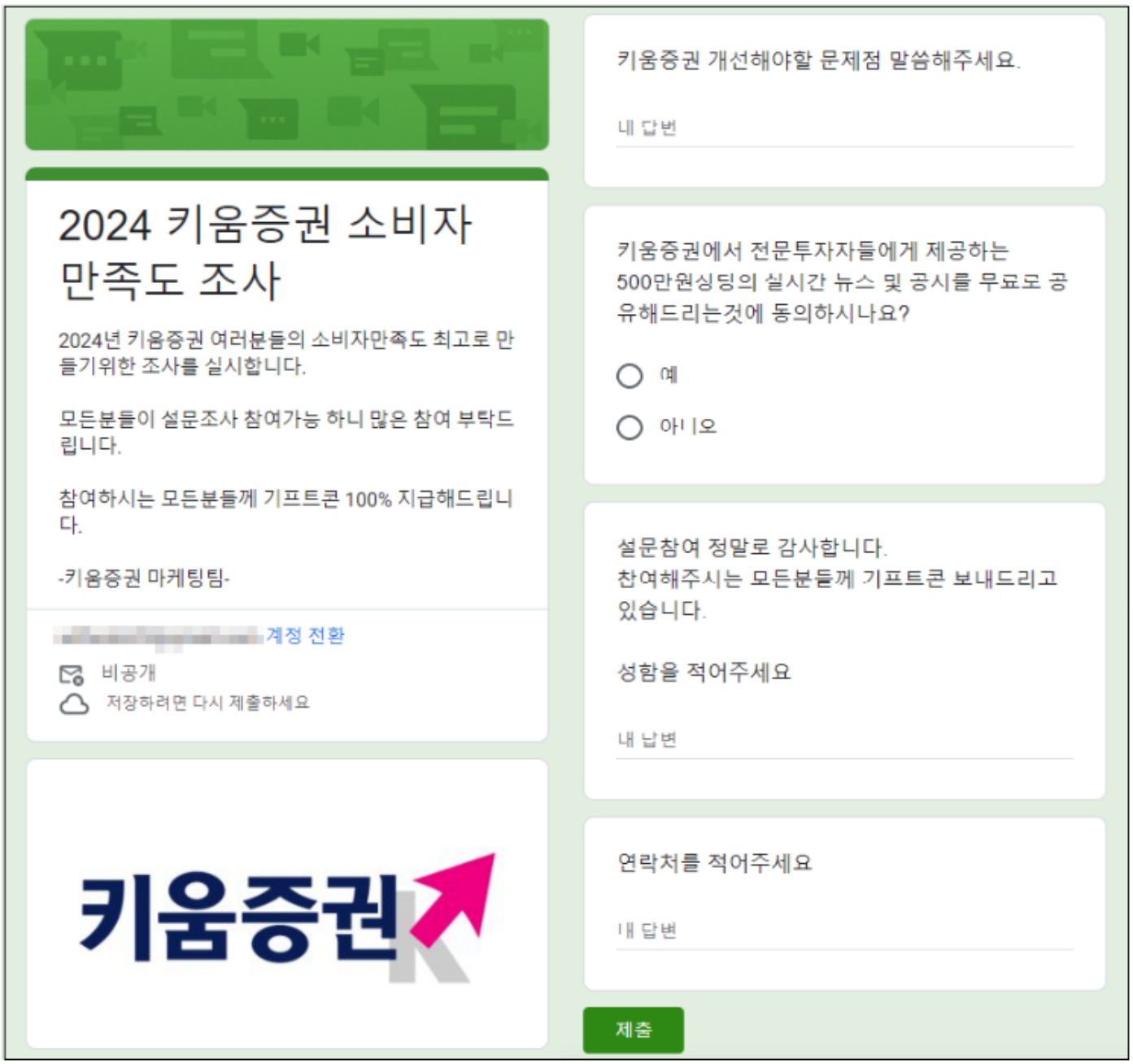
설문조사 참여를 위해 문자 내 링크를 클릭하면 구글폼으로 작성된 설문 페이지로 접속되고, 몇 가지 설문 항목과 이름, 연락처를 기재하여 제출하도록 유도합니다.

[그림 1] 동행복권 설문조사 링크 페이지 1



[그림 2] 동행복권 설문조사 링크 페이지 2

[그림 3] 부모급여지원캠페인 설문조사 링크 페이지



[그림 4] 키움증권 소비자만족도조사 링크 페이지

사용자가 해당 설문조사에 참여하여 개인정보를 기재한 후 제출하게 되면 입력된 개인정보는 해당 설문지를 만든 공격자에게 그대로 전달되며, 공격자는 구글폼 응답페이지를 통해 수집된 개인정보를 확인할 수 있습니다.

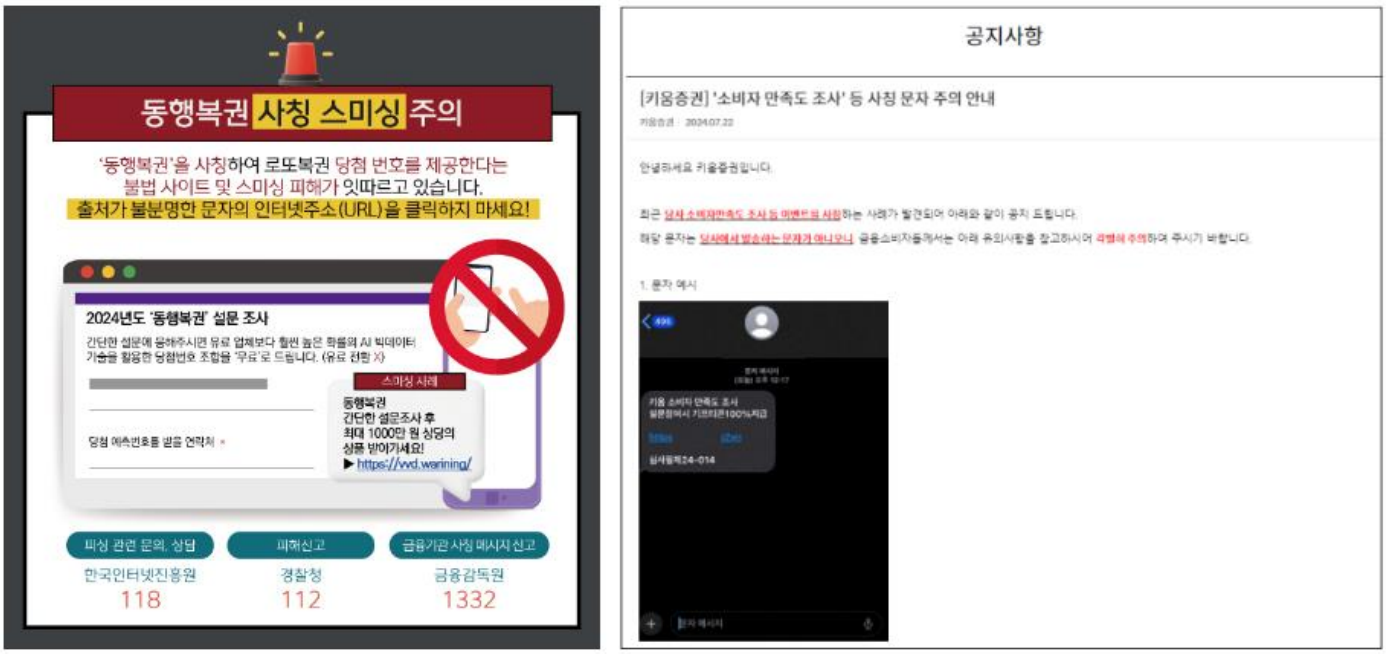
부모급여란 출산과 양육에 따른 부모의 경제적 부담을 덜고 영아기 돌봄을 지원하기 위하여 기존의 영유아 수당을 확대 개편하여 23 년 1 월 25 일부터 시행된 정책으로, 공격자들은 이러한 키워드를 악용하여 사용자들의 설문조사 참여를 유도하고 있습니다.

정상적인 설문조사처럼 보이지만, 자세히 살펴보면 경품내용에 주제와 관련 없는 '로또 10 조합' 이라는 엉뚱한 내용 혹은 '문제지 제출시 100%경품지원' 이라는 어색한 부분들이 포함되어 있습니다.

만일 문자 수신자들이 실제 설문조사로 오인하여 개인정보를 입력 후 제출을 누르면, 입력된 개인정보는 공격자에게 전송되게 됩니다.

이렇게 수집된 개인정보를 활용해 실제 설문조사 참여자에게 당첨 문자를 발송하여 카카오톡 채널을 통한 로또 사이트 가입 및 1:1 채팅을 유도하는 사례도 확인되었습니다.

> [Web 발신] 000 부모 급여지원 캠페인 ★당첨 축하드립니다★ 경품 안내받기 ☞hxxps://vv*.i*/안내봇



[그림 5] 동행복권/키움증권 공식 홈페이지 스미싱 주의 공지 화면

이번 공격의 특징은 대형 포털 사이트에서 제공하는 설문조사 양식을 사용하여 사용자들의 신뢰를 얻고자 하였고, 일반적으로 악성앱 설치를 유도하는 스미싱과는 다르게 정보 기입만을 요구하여 사용자들이 스미싱 공격임을 인지하기 어렵도록 했습니다.

이렇게 불법적으로 수집된 개인정보는 2 차 피해를 야기할 수 있어 각별한 주의가 필요합니다.

사용자 여러분들께서는 출처가 불분명한 사용자에게서 전달받은 링크 접속을 지양하시고, 설문조사의 경품이 고가이거나 당첨금이 고가일 경우 혹은 이름과 연락처와 같은 민감한 정보를 요구할 경우 공격임을 의심하고 공식 홈페이지를 통해 이벤트 진행 여부를 확인하시기를 권고 드립니다.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com