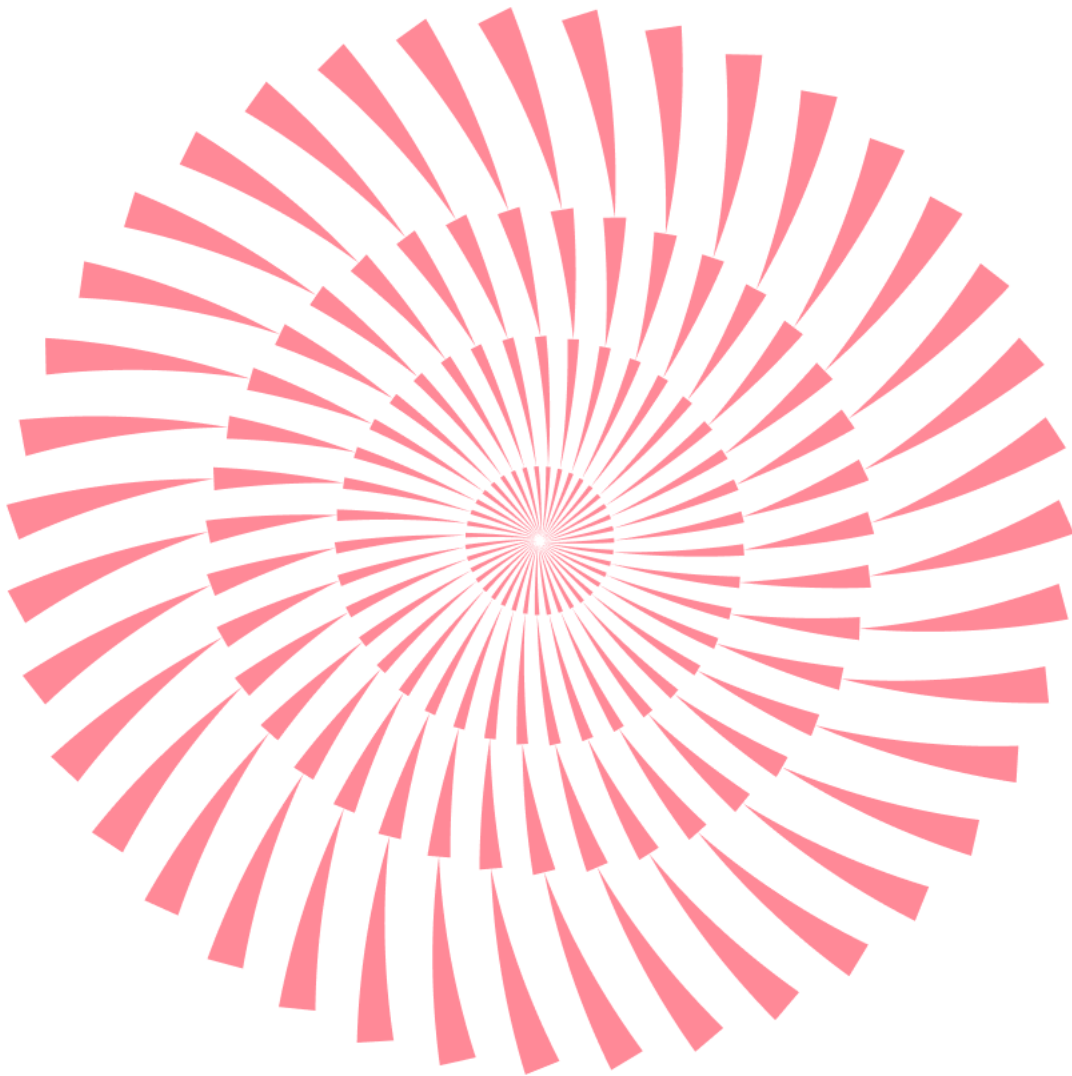


No.198 | 2026.3

# ESRC

이스트시큐리티가 제공하는 악성코드 동향과 이메일 통계  
최근 보안이슈를 확인하세요.



# CONTENTS

## 1 악성코드 통계 및 분석

1. 악성코드 동향
  2. 알약 악성코드 탐지 통계
  3. 알약 M 악성코드 탐지 통계
  4. 랜섬웨어 차단 및 악성코드 유포지 URL 통계
  5. 악성코드 이메일 통계
- 

## 2 최신 악성코드 동향

1. 사회공학적 기법과 지능적 은닉의 결합: Konni 그룹의 'SamsungUpdate' 스케줄러 악용 사례
2. 한국거래소(KRX) 채용 LNK 피싱: PDF 위장 PowerShell 이중 페이로드



# 1

## 악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 알약 M 악성코드 탐지 통계
4. 랜섬웨어 차단 및 악성코드 유포지 URL 통계
5. 악성 이메일 통계

# 1. 악성코드 동향

2026년 2월 한 달간 발생한 사이버 위협의 핵심은 AI 생태계의 급격한 확장에 따른 공격 표면(Attack Surface)의 변화와 북한발 APT 조직의 공격 기법 고도화로 요약됩니다. 특히 생성형 AI를 활용한 악성코드 제작과 더불어 AI 에이전트 플랫폼인 OpenClaw를 겨냥한 대규모 공급망 공격은 기존 보안 체계의 한계를 여실히 드러냈습니다. 또한 국내외에서 발생한 대규모 개인정보 유출 사고는 다크웹을 통한 2차 공격의 자양분이 되고 있어 이에 대한 입체적인 분석이 요구됩니다.

## AI 활용 무기화 및 협업 툴을 이용한 침투 전략과 사회공학적 기법의 진화

북한 배후의 Konni(코니) 그룹은 AI를 이용해 제작한 정교한 PowerShell 백도어를 전면에 내세웠습니다. 블록체인 개발자를 대상으로 한 이번 공격에서는 GSRAT이라는 신규 페이로드가 식별되었는데, 이는 AI 기술이 악성코드의 난독화와 탐지 우회 단계에 깊숙이 개입하고 있음을 시사합니다. Kimsuky(김수키) 조직 역시 국내 사용자의 심리를 교묘히 이용해 한국거래소(KRX) 협업 기획안이나 개인정보 동의서로 위장한 악성 LNK 및 JSE 파일을 유포하며 고전적인 스피어피싱 수법을 병행했습니다.

Lazarus(라자루스) 그룹이 'Prospect Call' 작전을 통해 MS Teams 미팅 제안을 미끼로 macOS 사용자들의 자격 증명을 탈취하는 정밀 타격(Targeted Attack)을 수행했습니다. 이들은 추적을 피하기 위해 공격 인프라 내 데드 드롭(Dead-drop) 지점으로 블록체인을 활용하는 등 인프라 운용의 치밀함을 보였습니다. 또한 VS Code의 악성 프로젝트 파일을 이용해 국내 개발자 PC에 RAT(Remote Access Trojan)을 심으려는 시도가 지속적으로 탐지되었습니다.

## AI 에이전트 생태계 및 SW 업데이트 경로를 통한 침투 고도화

최근의 공급망 공격은 전통적인 소프트웨어 배포 체계를 넘어 신규 AI 에이전트 플랫폼으로 그 범위를 급격히 확장하며 기존의 신뢰 기반 보안 모델을 위협하고 있습니다. 대표적인 사례로 AI 플랫폼 OpenClaw의 스킬 저장소인 'ClawHub'에서 약 1,200개 이상의 악성 스킬이 유포된 'ClawHavoc' 캠페인이 식별되었습니다. 본 공격은 에이전트의 지시 해석 구조를 역이용하는 '에이전트 조작 공학(Agent Engineering)' 기법을 통해 개발자 환경에 AMOS(Atomic macOS Stealer)를 배포하였으며, 이를 통해 API 키, SSH 자격 증명, 가상자산 지갑 등 핵심 인프라 접근 정보를 탈취한 것으로 분석됩니다.

이러한 지능형 수법은 상용 소프트웨어의 배포 인프라 하이재킹 전략과 결합되어 더욱 치밀해지는 양상을 보입니다. 2 월 중 발생한 Notepad++의 공식 업데이트 경로 탈취 및 Lotus Blossom 조직의 악성코드 유포 사건, 그리고 eScan 백신 서버를 통한 다단계 페이로드 배포 사례는 사용자가 원천적으로 의심하기 어려운 경로를 공격자가 직접 장악하고 있음을 시사합니다. 따라서 기업 보안 담당자는 AI 에이전트 스킬이나 오픈소스 라이브러리와 같은 외부 자산뿐만 아니라, 기존에 신뢰하던 소프트웨어 업데이트 프로세스 전반에 대해서도 제로 트러스트(Zero Trust) 기반의 엄격한 무결성 검증 체계를 수립해야 합니다.

## 대규모 플랫폼 침해 및 개인정보 유출 실태 분석

국내 주요 이커머스 및 금융, 공공 부문에서 발생한 대규모 데이터 유출 사고는 기존 정보보호 관리 체계의 구조적 결함을 여실히 드러냈습니다. 국내 대형 이커머스 업체인 C 사에서는 관리 소홀로 인해 가입자 약 3,367 만 명의 인적 사항과 1 억 건 이상의 배송 데이터가 노출되는 초유의 사고가 발생했습니다. 특히 배송지 정보 수정 페이지의 취약점을 통해 아파트 공동현관 비밀번호가 대량 유출된 점은 디지털 영역의 보안 실패가 실제 물리적 안전 위협으로 전이될 수 있음을 보여주는 상징적 사례로 평가됩니다. 또한, 금융기관 N 사에서는 내부 시스템 감염으로 인해 고객의 신용점수 및 연간 소득 데이터가 다크웹에 유출되었으며, 공공기관 G 사에서도 약 5,000 여 명의 개인정보 노출에 따른 행정 처분 절차가 개시되는 등 민관 전반의 보안 관리 부실 사례가 집중되었습니다.

국외에서도 인지도 높은 글로벌 플랫폼들의 연쇄적인 데이터 유출 사례가 잇따르며 사용자 식별 정보 보호에 비상이 걸렸습니다. 음원 스트리밍 플랫폼인 SoundCloud 에서 약 2,980 만 건의 계정 정보 유출이 식별된 것을 필두로, 핀테크 기업인 Betterment(140 만 건), 뉴스레터 플랫폼 Substack, 그리고 음식 배달 서비스인 Grubhub 등에서 침해 사실이 확인되었습니다. 특히 프랑스 실업청(France Travail)에 대규모 유출 책임으로 500 만 유로의 벌금이 부과된 사례는 데이터 관리 소홀에 대한 법적/사회적 책임이 국제적으로 강화되고 있음을 시사합니다. 이러한 전방위적인 유출 사고는 탈취된 정보를 활용한 크리덴셜 스테핑(Credential Stuffing) 등 2 차 공격의 파급력을 증폭시키는 직접적인 원인이 되고 있습니다.

## 취약점(Exploit) 및 지능형 유포 기술 분석

최근 취약점 무기화 양상은 특정 타겟을 겨냥한 정밀 공격과 엔터프라이즈 소프트웨어의 결함을 이용한 전방위 침투가 병행되는 특징을 보입니다. 러시아 연계 조직인 APT28 은 MS Office 의 최신 제로데이 취약점(CVE-2026-21509)을 지오펜싱(Geofencing) 기술과 결합하여, 특정 지역의 타겟에게만 페이로드를 드롭하는 정교한 탐지 회피 전략을 구사했습니다. 이와 함께 CISA 는 실제

공격 인프라 구축 및 초기 침투 경로로 활발히 소모되고 있는 고위험 결함들을 KEV(Known Exploited Vulnerabilities) 카탈로그에 대거 추가했습니다. 특히 SolarWinds Web Help Desk의 취약점은 공격자들이 인증 없이 시스템 권한을 탈취해 내부망으로 진입하는 핵심 교두보로 활용되었으며, VMware ESXi 및 GitLab의 결함 또한 랜섬웨어 그룹의 액세스 벡터나 소스코드 탈취를 위한 실전 익스플로잇 도구에 통합되어 광범위하게 악용되는 정황이 포착되었습니다.

지능형 유포 기법과 AI 프레임워크의 등장은 보안 솔루션의 자동화 탐지 난이도를 비약적으로 높이고 있습니다. 기존 브라우저 업데이트를 가장해 PowerShell 실행을 유도하던 ClickFix 기법은 가짜 CAPTCHA를 활용한 'CrashFix'로 변모하며 탐지 로직을 교묘히 우회하고 있습니다. 또한, 약 88,000 줄 규모의 AI 생성 Linux 악성코드 프레임워크인 'VoidLink'의 식별은 공격자가 코드 제작 단계부터 AI를 전면 도입하여 변종 생산성과 개발 속도를 혁신적으로 향상시키고 있음을 입증하는 상징적인 사례입니다. 결과적으로 정교한 취약점 공격과 지능형 유포 체계의 결합은 보안 위협의 파괴력을 전방위로 확장하는 직접적인 원인이 되고 있습니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

2월 한 달간 악성코드 탐지 건수는 전월 대비 2배 가까이 급증한 522,077건을 기록했으며, 특히 전월 10위(8,352건)였던 Gen:Variant.Application.Miner.2가 200,319건으로 24배 가까이 증가하며 1위를 차지하였습니다. 해당 악성코드는 시스템 자원을 무단 점유하여 모네로(Monero)화폐를 채굴하는 크립토재킹(Cryptojacking)

변종으로, 백그라운드 상주를 통한 하드웨어 과부하 및 시스템 가용성 저하를 유발하는 기술적 특징을 보입니다.

1월 SmallAsp 계열이 순위권에서 내려가고, Trojan.Rincux.A, Adware.Generic.3303075를 비롯한 다수의 신규 탐지명이 상위권에 진입하는 등 탐지 비중의 변동이 확인되었습니다. 그 외 상위권 항목들은 전월과 유사한 탐지 추이를 유지하고 있으며, 결과적으로 특정 자원 탈취형 공격의 집중 유포가 2월 한 달간 식별된 주요 특징으로 분석됩니다.

순위	등락	악성코드 진단명	카테고리	합계
1	↑9	Gen:Variant.Application.Miner.2	ETC	200319
2	-	Trojan.GenericKD.71882277	Trojan	84259

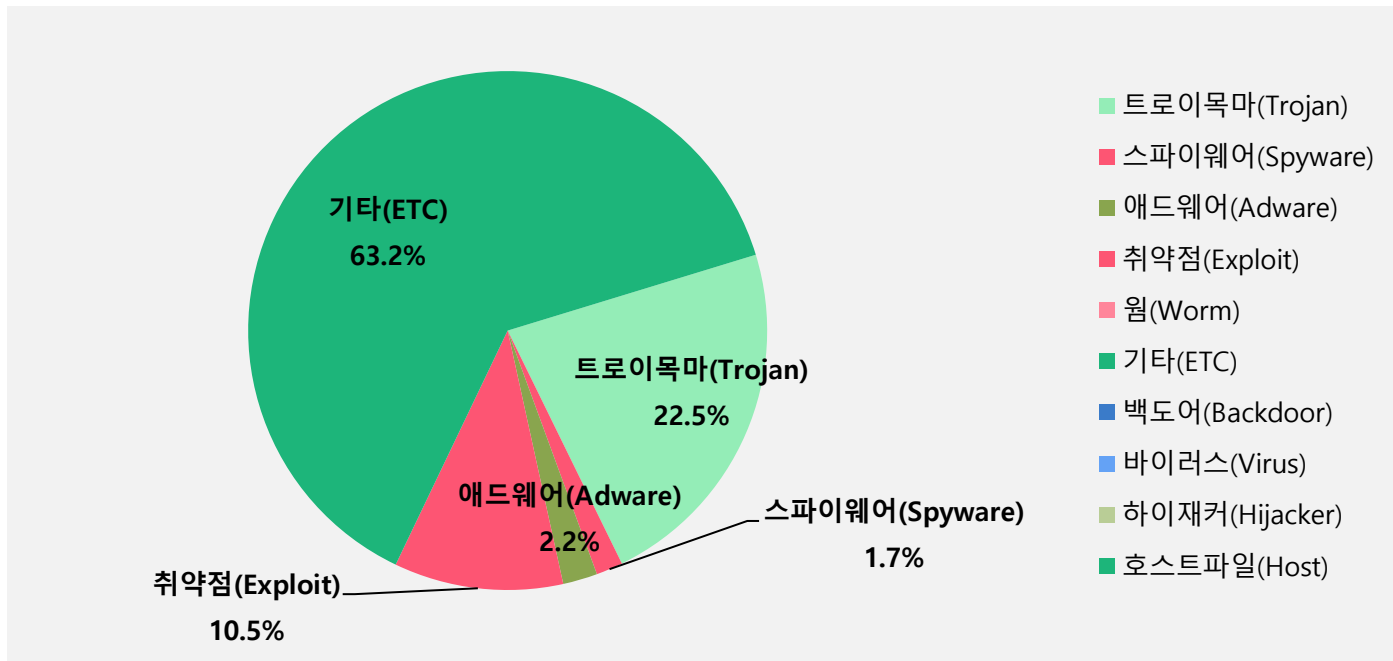
3	↓ 1	Gen:Variant.Tedy.675091	ETC	52104
4	↑ 1	Exploit.CVE-2010-2568.Gen	Exploit	47110
5	↑ 4	Gen:Variant.Jaik.292533	ETC	25924
6	-	Misc.HackTool.AutoKMS	ETC	16042
7	NEW	Trojan.Rincux.AW	Trojan	14349
8	↑ 7	Misc.Riskware.BitCoinMiner	ETC	13733
9	↓ 4	Application.Generic.4092474	ETC	13223
10	NEW	Adware.Generic.3303075	Adware	11236
11	NEW	Trojan.Agent.GDVB	Trojan	10162
12	↓ 7	Spyware.Infostealer.Bladabindi	Spyware	8682
13	↓ 5	JS:Trojan.Cryxos.15301	Trojan	8541
14	↓ 2	Misc.HackTool.KMSActivator	ETC	8483
15	NEW	Exploit.CVE-2020-0601.Gen.1	Exploit	7910

\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026 년 2 월 1 일 ~ 2026 년 2 월 28 일

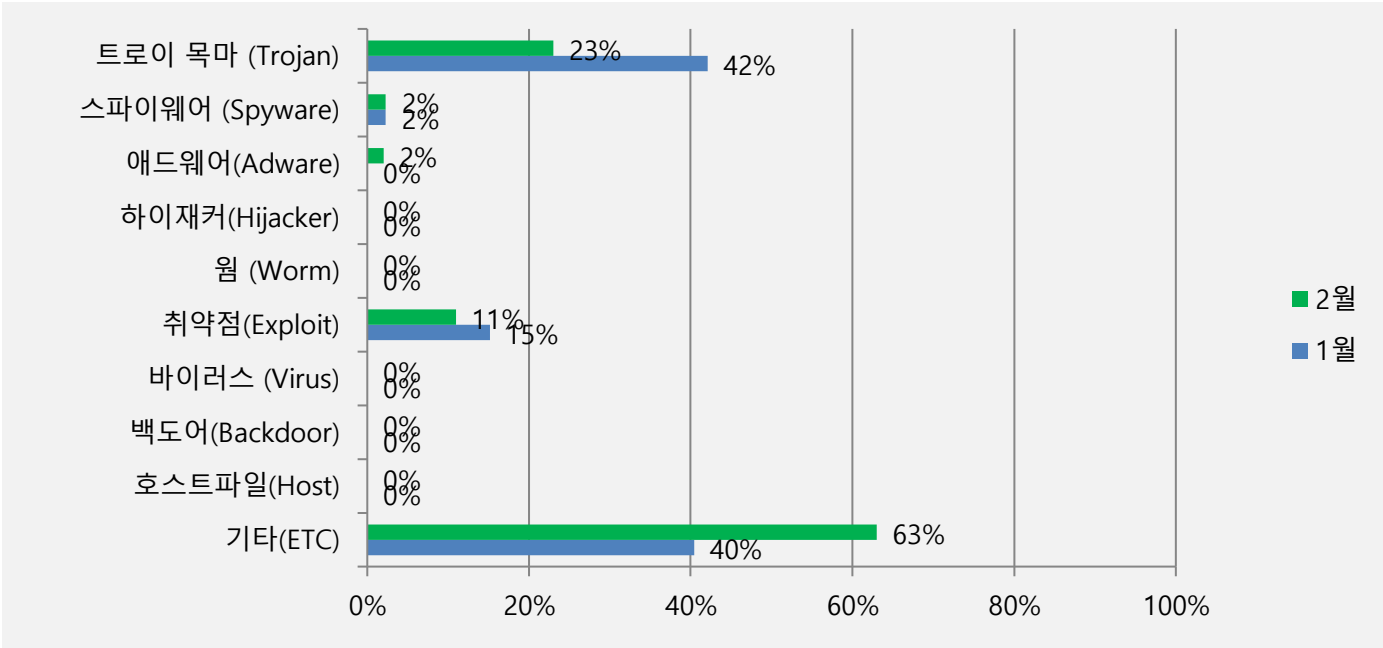
## 악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(ETC) 유형이 63.2%로 1위를 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 22.5%, 취약점(Exploit)이 10.5%, 애드웨어(Adware)가 4.7%를 차지하였습니다.



## 카테고리별 악성코드 비율 전월 비교

2026년 2월에는 1월과 비교하여 기타(ETC) 유형이 23% 큰 폭으로 증가하였습니다. 대신 트로이목마(Trojan) 유형이 19%, 취약점(Exploit) 유형은 4% 감소하였으며, 애드웨어(Adware)는 2% 증가, 스파이웨어(Spyware) 유형은 2%로 1월과 동일하였습니다.



### 3. 알약 M 악성코드 탐지 통계

#### 감염 악성코드 TOP15

2월 한 달간 모바일 악성코드 탐지 건수는 전월 대비 36.3% 감소한 16,623 건을 기록하였습니다. Android.Riskware.Agent 는 6,869 건으로 여전히 1위를 차지하였으나 전월 7,664 건 대비 10.4% 감소하였고, Android.Riskware.HiddenAds 또한 3,713 건에서 2,063 건으로 44.4% 감소하였습니다.

Monitor 및 Trojan 계열의 악성코드가 두드러졌습니다. Android.Monitor.Mspy 는 1월 상위권에서 순위 하락 후 2월 1,899 건으로 3위에 진입하였으며, Android.Trojan.Banker 는 724 건에서 1,144 건으로 58% 상승하였습니다.

새롭게 상위권 진입한 악성코드로는 Android.Adware.Andreed, Android.Trojan.SpyAgent, Android.Riskware.SMSSend 등이 확인되었습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	-	Android.Riskware.Agent	Riskware	6869
2	-	Android.Riskware.HiddenAds	Riskware	2063
3	↑ 2	Android.Monitor.Mspy	Monitor	1899
4	↑ 7	Android.Trojan.Banker	Trojan	1144

5	↓ 1	Android.Riskware.PackMal	Riskware	1083
6	NEW	Android.Adware.Andreed	Adware	619
7	NEW	Android.Trojan.SpyAgent	Trojan	586
8	↓ 1	Android.Adware.Agent	Adware	550
9	↓ 1	Android.Adware.Mulad	Adware	388
10	↓ 1	Android.Riskware.HackTool	Riskware	335
11	NEW	Android.Riskware.SMSSend	Riskware	268
12	NEW	Android.Riskware.Adware	Riskware	232
13	-	Android.Riskware.Downloader	Riskware	224
14	NEW	Android.Riskware.Clicker	Riskware	183
15	NEW	Android.Riskware.Porn	Riskware	180

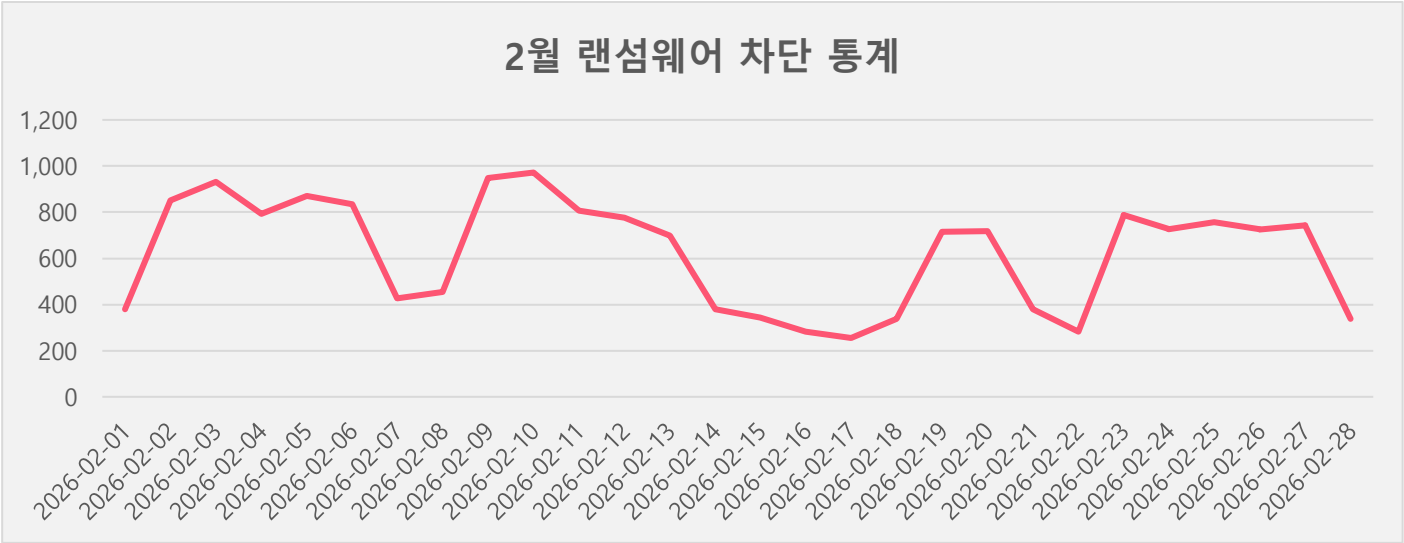
\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026년 2월 1일 ~ 2026년 2월 28일

# 4. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

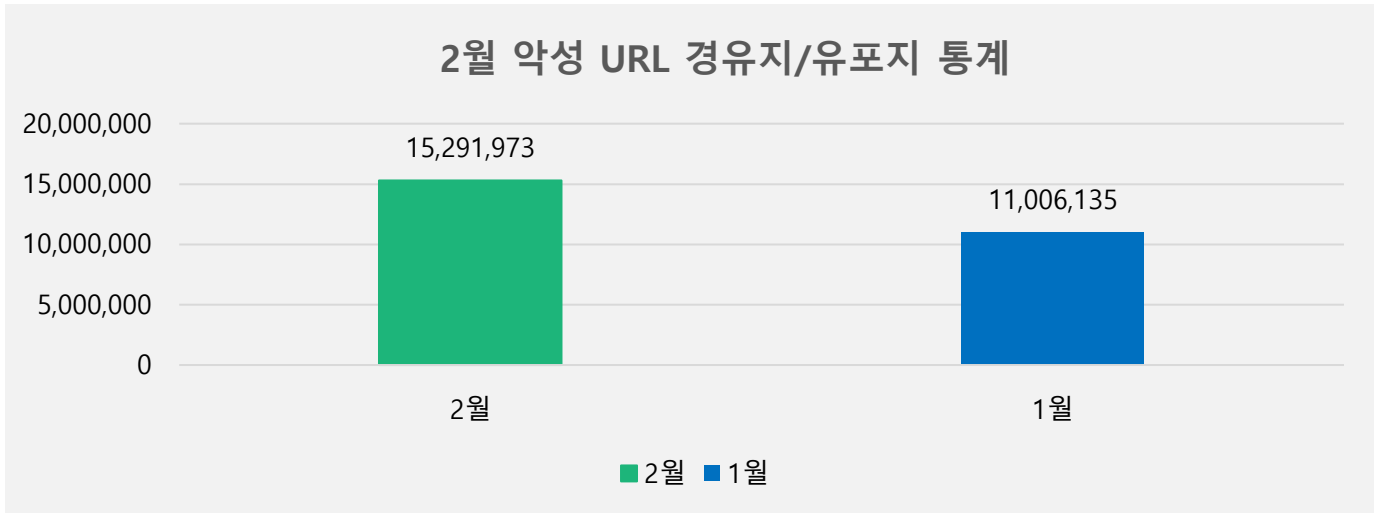
## 2월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 2월 1일부터 2월 28일까지 17,515 건의 랜섬웨어 공격 시도가 차단되었습니다.



## 악성코드 유포지 URL 통계

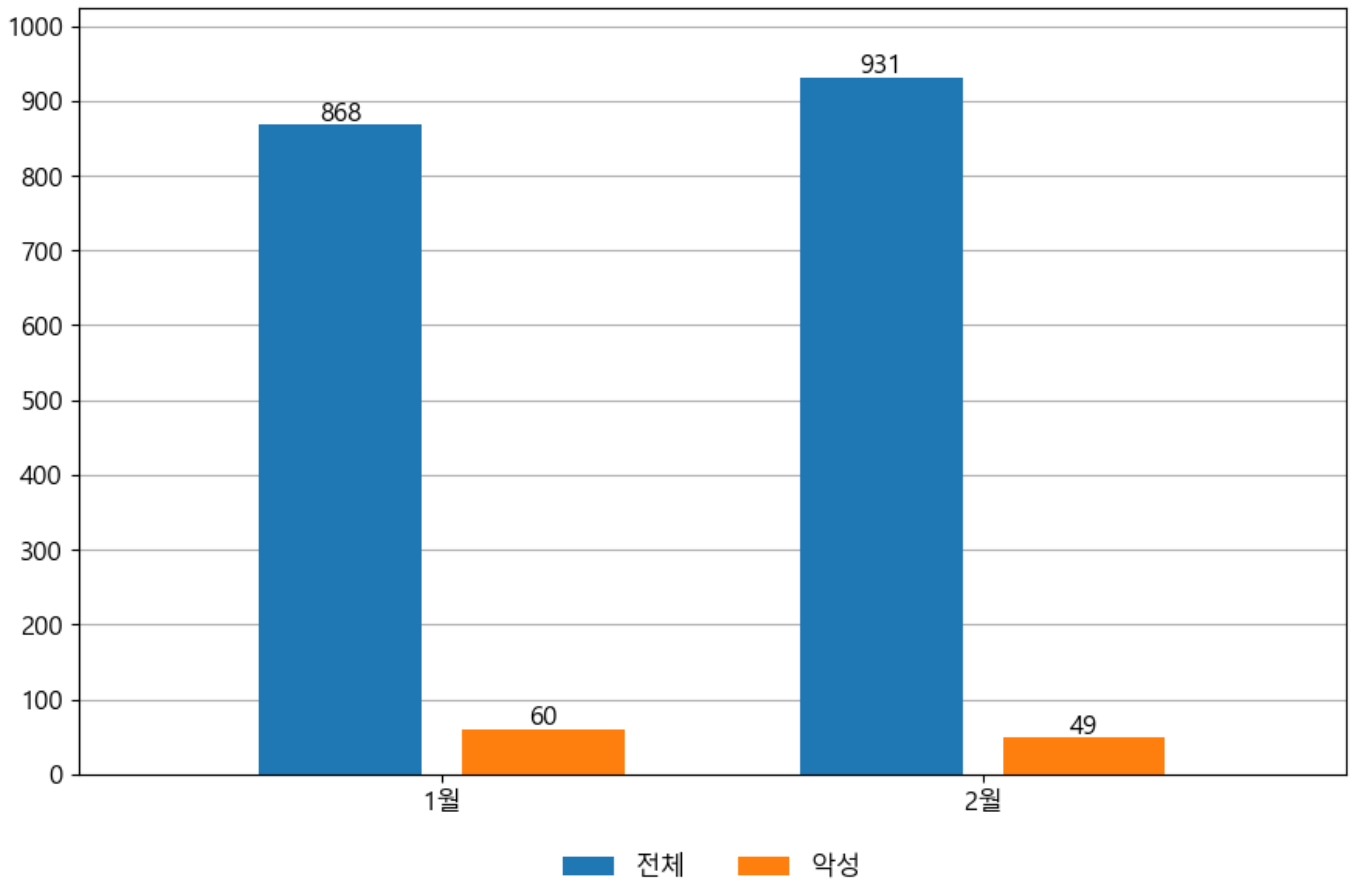
해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 26 년 2 월 한 달간 총 15,291,973 건의 URL 이 확인되었습니다. 이 수치는 1 월 한 달간 총 11,006,135 건의 악성코드 유포지 URL 수에 비해 약 38.9% 증가한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분을 참고하여 보시기 바랍니다.



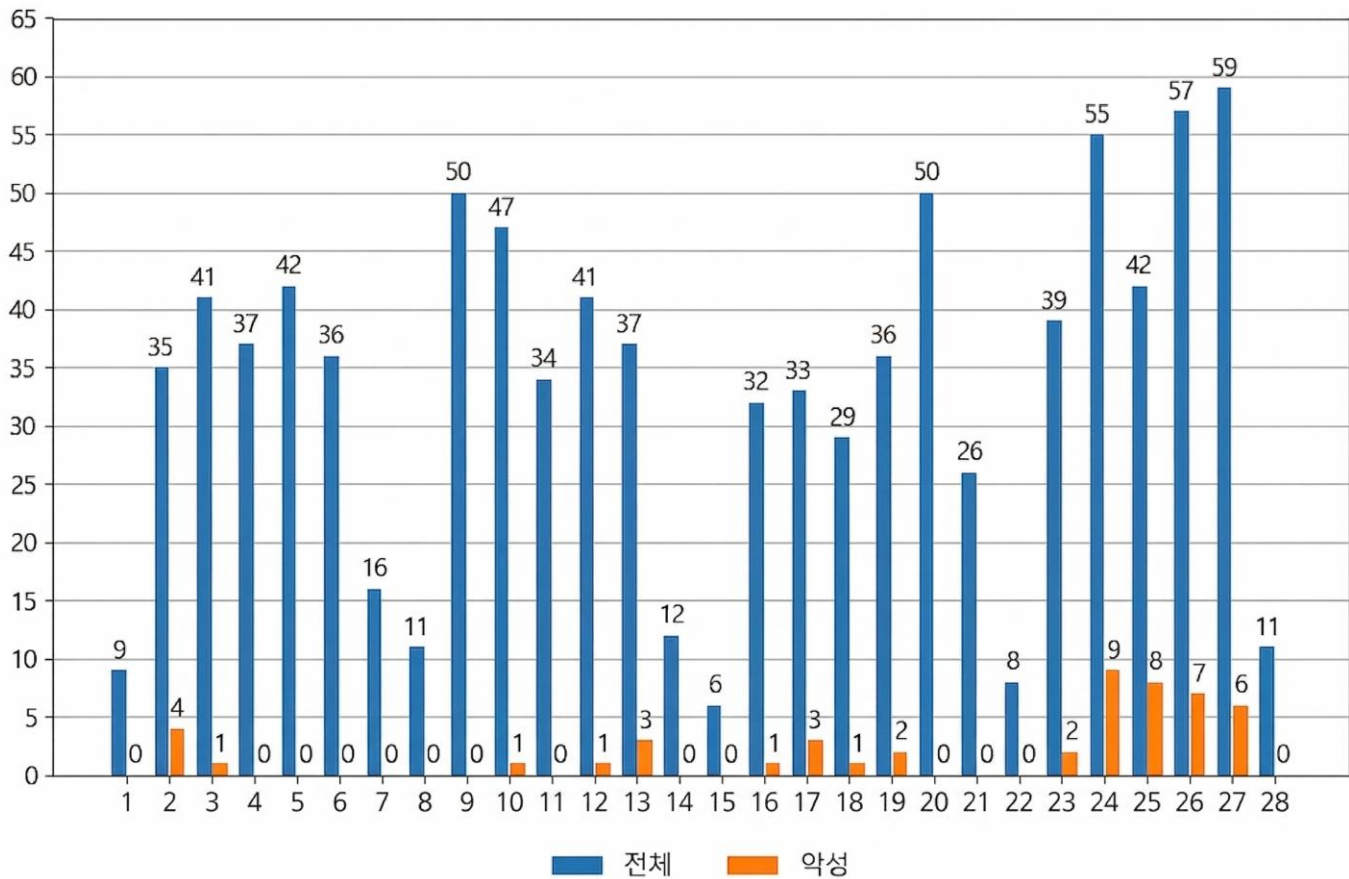
## 5. 악성 이메일 통계

### 이메일 유입량

2 월 이메일 유입량은 총 931 건이고 그중 악성은 49 건으로 5.26%의 비율을 보였습니다. 악성 이메일의 경우 전월(1 월) 60 건 대비 49 건으로 11 건이 감소했습니다.

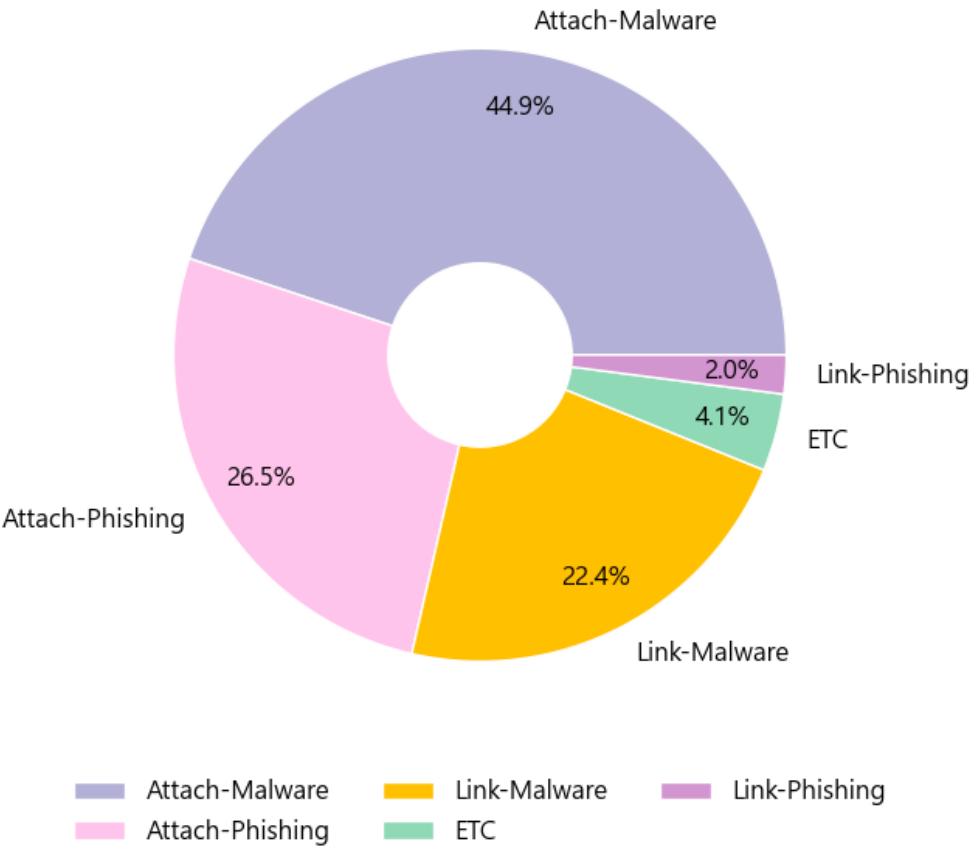


일일 유입량은 하루 최저 6 건(악성 1 건)에서 최대 59 건(악성 9 건)으로 일별 편차를 확인할 수 있습니다.



## 이메일 유형

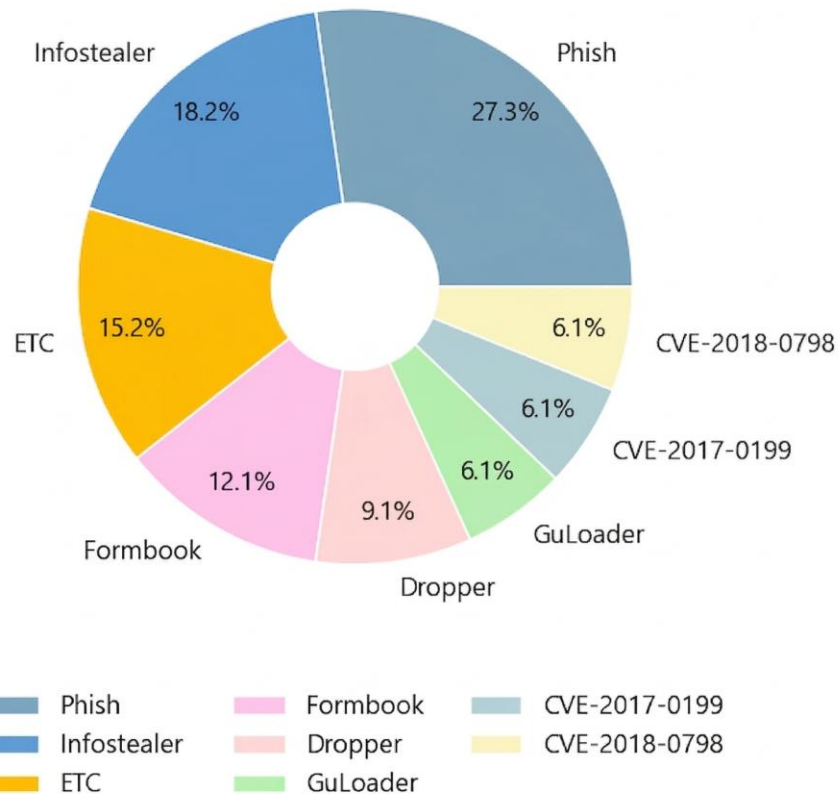
악성 이메일을 유형별로 살펴보면 49 건 중 Attach-Malware 형이 44.9%로 가장 많았고 뒤이어 Attach-Phishing 형이 26.5%를 나타냈습니다.



이메일 유형	상세 설명
Attach – Phishing	첨부파일을 통해 개인정보를 입력하게 하는 유형
Attach – Malware	첨부파일에 악성코드가 존재하는 유형
Link - Phishing	링크 클릭 시 피싱사이트로 연결되는 유형
Link - Malware	링크 클릭 시 악성코드가 다운로드되는 유형
Img Tag	이메일 본문 악성 'img' 태그를 이용하는 유형
Hoax	거짓 내용으로 상대방에게 송금을 유도하는 유형

첨부파일 종류

첨부파일은 'Phish'형태가 27.3%로 제일 큰 비중을 차지했고 뒤이어 'Infostealer', 'ETC'가 각각 18.2%, 15.2%의 비중을 차지했습니다.



## 대표적인 위협 이메일의 제목과 첨부파일명

2 월 같은 제목으로 다수 유포된 위협 이메일의 제목들은 다음과 같습니다.

- 이 이메일은 발행 및 발송된 전자 세금계산서입니다.
- RE: KHN250045 Booking 1-case//305kgs//2.53cbm ETD
- Approval requested:[EXTERNAL] - Fw; Deliberations from the meeting with FAB.../NRS
- 계정 보호 조치가 실행되었습니다
- RE: HK 121437: [INQUIRY] LDC-KOREA, (NEW TIMES-0311503), RFQ.NO. T-251223013
- ADVICE OF REMITTANCE
- 2026 년 1 월 직원 성과 보고서
- 확인을 위한 수정된 BL & AWB

- 문의가 들어왔습니다.

2 월 유포된 위협 이메일 중 대표적인 악성 첨부파일 명은 다음과 같습니다.

- NTS\_eTaxInvoice.html
- KHN250045 Booking 1case305kgs2.53cbm ETD.zip
- T-251223013 packing.zip
- T-251223013 DN.zip
- Request for Quotation.rar
- RFQ - Purchase Order #POTT40494820.Tar.001
- 첨부파일(보안).html
- 2026 년 1 월 보고서.rar
- Fedex Korea Delivery.html
- Payment-Advise-Pdf.gz



## 최신 악성코드 동향

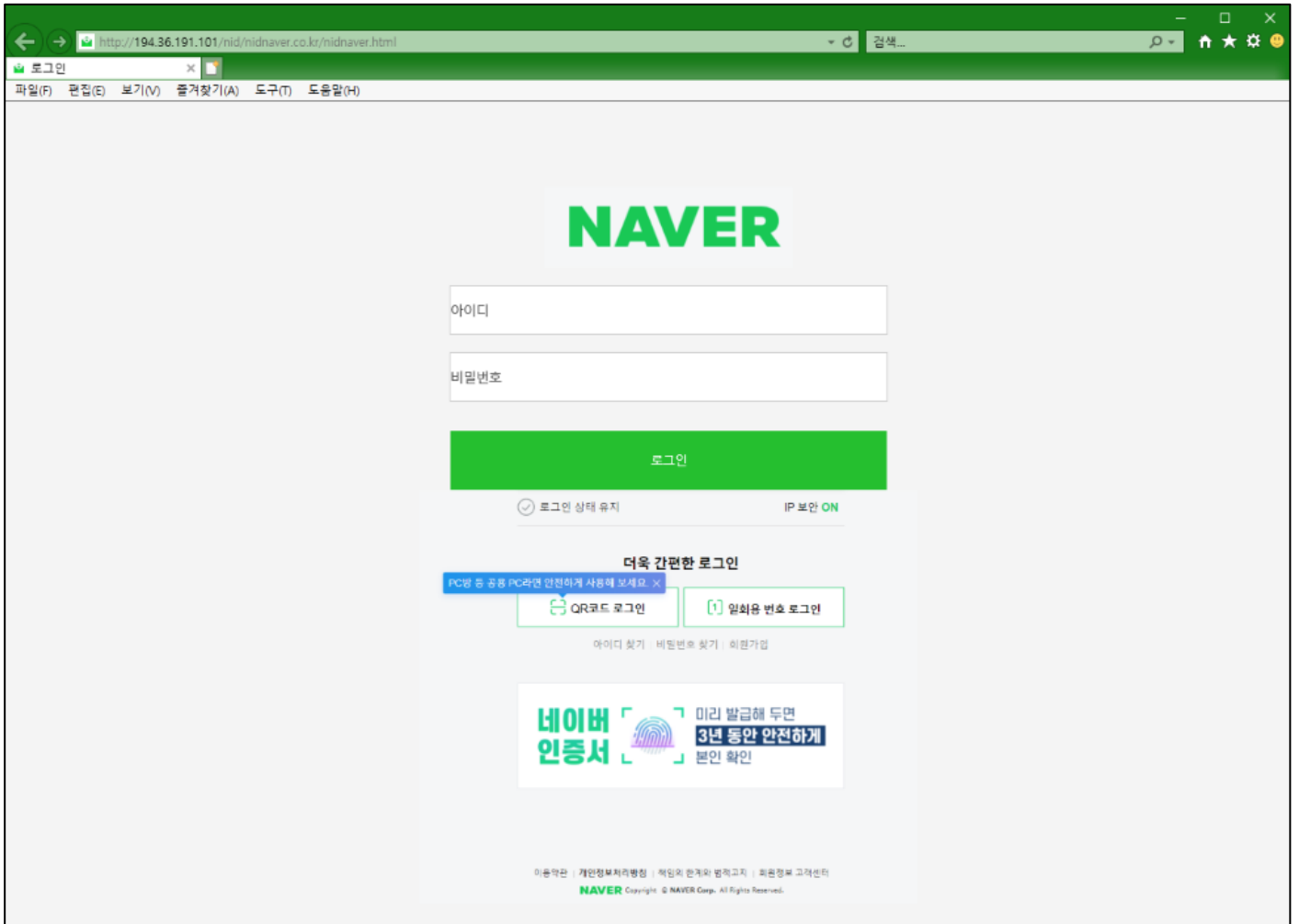
## 사회공학적 기법과 지능적 은닉의 결합: Konni 그룹의 'SamsungUpdate' 스케줄러 악용 사례

네이버 로그인 화면처럼 보이게 꾸민 파일 "210930-001.png.lnk"를 통해 진행되는 북한 Konni 그룹의 피싱 공격을 발견했습니다. 이번 공격은 '네이버 로그인 화면'을 위장한 사회공학적 기법으로 시작되며, "210930-001.png.lnk"라는 파일명의 바로가기(LNK) 파일을 초기 침투 경로로 활용합니다. 사용자가 이 파일을 실행하면 백그라운드에서 PowerShell 스크립트가 은밀히 구동되며, 사용자를 안심시키기 위해 정상적인 PNG 이미지 파일을 전면에 표시하는 기만 전술을 구사합니다. 이와 동시에 LNK 내부에 은닉된 CAB 아카이브가 %public%\WLibraries 경로에 해제되어 VBScript, 배치 파일 등 다수의 악성 스크립트가 드롭됩니다.

감염 체인은 매우 치밀하게 설계되어 있습니다. 드롭된 vxnlcn989.vbs 가 실행되어 avtue483.bat 을 호출하면, 해당 배치 파일은 시스템의 지속성(Persistence) 확보를 위해 SamsungUpdate 라는 명칭으로 작업 스케줄러를 등록합니다. 이후 실행되는 bxcyv197.bat 은 시스템 내 주요 폴더 구조(다운로드, 문서, 바탕화면)를 전수 조사하고 설치된 프로그램, 공인 IP, 현재 실행 중인 프로세스 목록 및 레지스트리 자동 실행 항목 등 포괄적인 시스템 정찰 정보를 수집합니다. 수집된 데이터는 uplokli567.bat 을 통해 정상적인 워드프레스 경로로 위장한 C2 서버(atlasstours.com)로 전송됩니다.

특히 이번 캠페인은 공격의 흔적을 지우기 위해 업로드 완료 후 특정 배치 파일을 자동 삭제하고, chbbie400.bat 을 avtue483.bat 으로 이름을 변경하여 2 단계 공격을 준비하는 지능적인 파일 스왑 기법을 사용합니다. C2 서버와 통신할 때 URL 파라미터에 컴퓨터 이름을 포함하여 피해 단말을 개별 식별하는 방식은 전형적인 Konni 그룹의 특성으로, 이를 통해 선별적인 추가 페이로드 배포가 가능해집니다. 이는 단순한 정보 탈취를 넘어 장기적인 침투와 추가 악성 행위를 염두에 둔 숙련된 공격자의 수법임을 보여줍니다.

이러한 위협에 대응하기 위해서는 우선적으로 210930-001.png.lnk 파일과 %public%\WLibraries 경로 내 생성된 모든 스크립트 파일을 즉시 격리 조치해야 합니다. 보안 관리자는 atlasstours.com 도메인에 대한 전역 차단을 시행하고, PowerShell 및 WScript 의 자식 프로세스 생성을 로깅하여 SamsungUpdate 와 같은 비정상적인 스케줄러 등록 행위를 실시간 탐지해야 합니다. 또한 네트워크 및 EDR 시스템에서 dir /s /od 명령의 과도한 실행이나 locale 파라미터가 포함된 multipart POST 요청을 모니터링 규칙에 반영하여 유사한 변종 공격을 사전에 차단하는 종합적인 방어 체계 구축이 시급합니다.



[그림] 악성 LNK 파일 실행 시 보여지는 미끼 HWP

## 한국거래소(KRX) 채용 LNK 피싱: PDF 위장 PowerShell 이중 페이로드

한국거래소(KRX) 채용 제안서를 교묘하게 위장한 정교한 LNK 파일 기반 피싱 공격을 새롭게 포착했습니다. "2026 년 KRX 유튜브 메인 MC 초빙 및 콘텐츠 협업 기획안.pdf.lnk"는 실행 즉시 내장된 PowerShell 명령어를 통해 현재 경로와 TEMP 폴더를 재귀 검색하여 동일 파일을 자동 탐지하고, LNK 내부 오프셋 4096(92,975 바이트)과 97071(25,166 바이트)에서 데이터를 추출한 뒤 단일 바이트 XOR 복호화를 거쳐 정상 PDF 문서와 악성 PS1 스크립트를 %TEMP%에 동시 생성하는 이중 페이로드 구조를 구현했습니다. 이 설계는 파일 위치 변경에도 안정적으로 동작하며, PDF 자동 실행으로 사용자가 실제 제안서를 검토하는 것처럼 자연스럽게 보이게 해 의심을 완전히 차단합니다.

복호화된 PS1 파일은 임의 파일명으로 저장된 후 powershell.exe -nopprofile -windowstyle hidden -executionpolicy bypass 옵션으로 완전 은폐 상태에서 실행되며, 외부 C2 서버 (midp.wuaze[.]com/aes.js, /maith.php 등)와 활발한 통신을 시도합니다. 드롭 파일 (\_PSScriptPolicyTest\*.psm1, StartupProfileData-NonInteractive-..., powershell.exe.log)을 통해 PowerShell 실행 정책 테스트, 비대화식 프로파일 데이터 수집, 실행 로깅 활동이 확인되며, PS1 실행 완료 후 즉시 자체 삭제로 포렌식 분석을 어렵게 만드는 세심한 설계가 돋보이는 'LNK→PowerShell→동시 드롭 및 실행'의 핵심 공격 흐름이 명확합니다.

이에 따라 즉시 "2026 년 KRX 유튜브 메인 MC 초빙 및 콘텐츠 협업 기획안.pdf.lnk" 관련 파일을 전 시스템에서 검색·격리하고 %TEMP% 경로의 PDF·PS1 생성 이력을 집중적으로 조사해야 합니다. PowerShell Module/Script Block/Transcription 로깅을 활성화하여 ExecutionPolicy Bypass, Hidden Window 실행, Get-ChildItem -Recurse, Set-Content -Encoding Byte 등의 패턴을 실시간 EDR 규칙으로 탐지하며, midp.wuaze[.]com 도메인과 모든 하위 경로(/aes.js, /maith.php 포함)를 방화벽·프록시에서 즉각 차단하는 것이 필수입니다. 또한 LNK 첨부 스피어피싱 대응 강화를 위해 이메일 게이트웨이에서 LNK 확장자 격리 정책을 적용하고, LNK→PowerShell 자식 프로세스 생성 및 비정상 LNK 메타데이터를 탐지하는 SIEM 규칙을 배포하여 유사 공격을 사전에 차단해야 합니다.

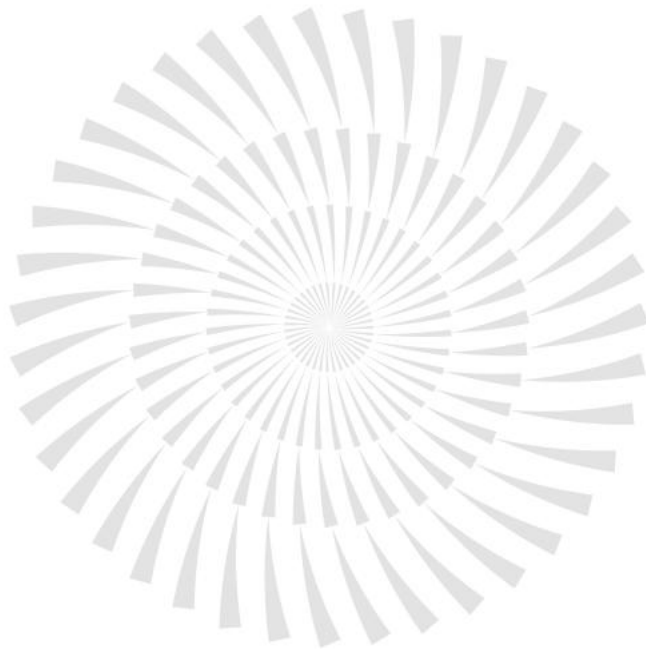
2026년 KRX 유튜브 메인 MC 초빙 및 콘텐츠 협업 기획안

1. 프로젝트 개요
  - 프로젝트명: KRX 밸류업 인사이트 시리즈 (가제)
  - 주관/시행: 한국거래소(KRX) / 엣지랭크(EDGERANK)
  - 추진 배경:
    - 정부 및 유관기관 주도의 '기업 밸류업 프로그램' 대국민 홍보 필요성 증대
    - 개인 투자자들의 시장 인식 개선 및 건전한 투자 문화 정착
    - 실전 투자 전문가와의 협업을 통한 콘텐츠 신뢰도 및 도달률 극대화
2. 협업 모델
  - 초빙 대상: 유튜브
  - 선정 사유:
    - 투자 철학이 거래소의 건전 투자 지향점과 일치
    - 크몽 만족도 99% 등 데이터로 증명된 교육적 역량 및 대중적 소구력
  - 주요 역할:
    - 메인 호스트로서 프로그램 진행 및 패널 토크 리딩
    - 투자자 관점에서의 정책(밸류업 등) 해석 및 실전 멘토링 세션 운영
3. 제작 및 마케팅 지원 (EDGERANK 역량)
  - VISUAL-E 솔루션: 자체 4K 스튜디오 및 전문 시네마틱 제작팀 투입으로 방송국 수준의 퀄리티 보장
  - 데이터 기반 최적화: 빅데이터 분석을 통해 타겟 오디언스의 유입 경로와 썸네일 클릭률(CTR) 실시간 관리
  - 퍼포먼스 마케팅: 엣지랭크의 운영 노하우를 바탕으로 한국거래소 채널 구독자 및 조회수 목표 달성 지원 (예산 약 10억 원 규모의 대행 이력 기반)
4. 계약 조건 및 출연료 (Strictly Confidential)

본 섹션은 보안 유지가 필수적이며, 협의에 따라 변동될 수 있습니다.

항목	세부 내용	비고
기본 출연료	회당 10만 원 (VAT 별도)	구독자 수 및 영향력 기반 산정
기획 자문료	프로젝트 전체 기간 내 만 원	콘텐츠 기획 참여 및 자문비
성과 인센티브	목표 조회수 달성 시 회당 출연료의 10~20% 추가 지급	성과 중심 퍼포먼스 관리

[그림] "2026년 KRX 유튜브 메인 MC 초빙 및 콘텐츠 협업 기획안.pdf.lnk" 실행 시 보여지는 미끼 PDF 파일



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

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