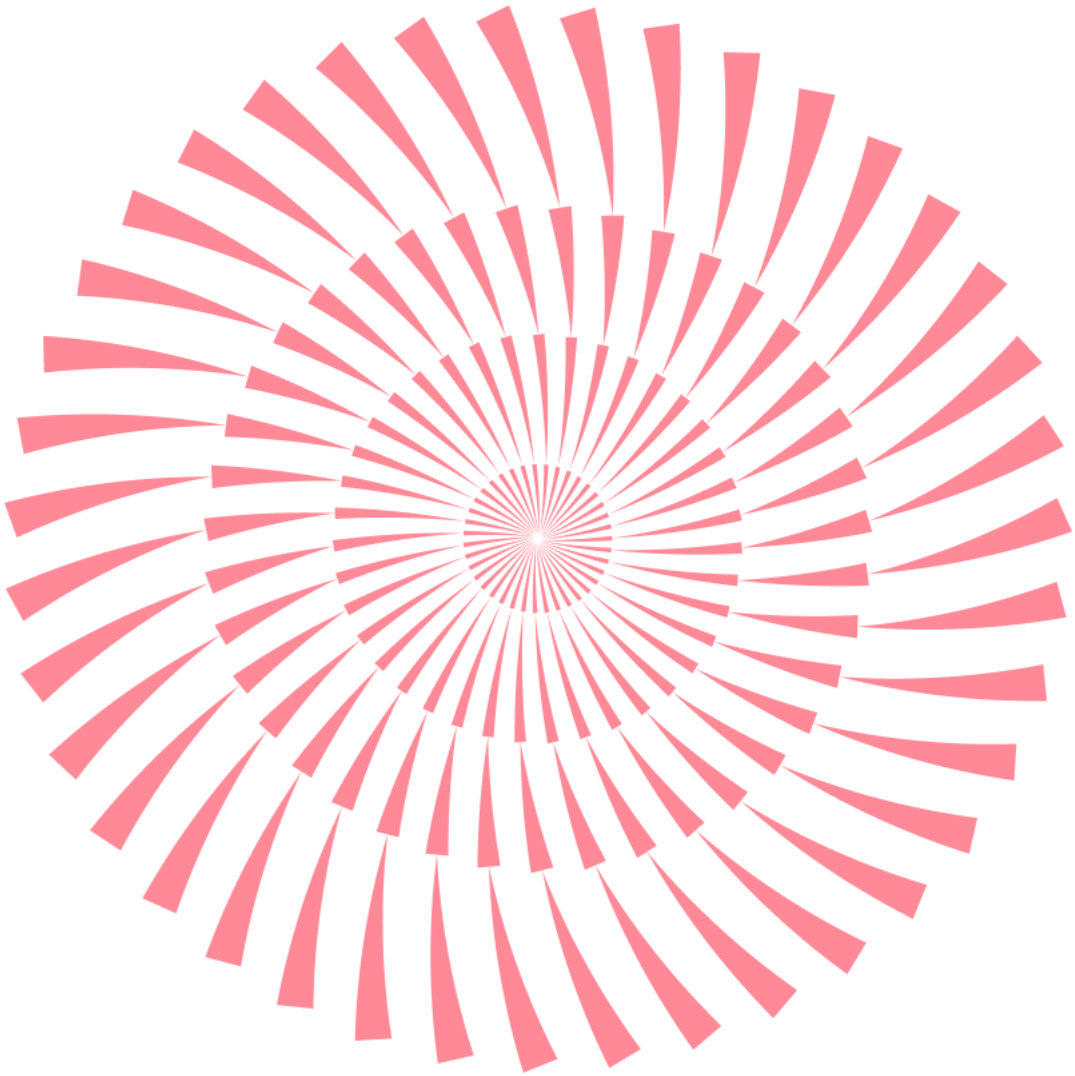
No.202 | 2026.7

ESRC 보안동향보고서

이스트시큐리티가 제공하는 악성코드 동향과 이메일 통계
최근 보안이슈를 확인하세요.



EST SECURITY

ESRC 보안동향보고서

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. 악성 이메일 통계

1. 악성코드 동향

2026 년 6 월 한 달간 발생한 사이버 위협의 핵심은 북한 연계 그룹 Sapphire Sleet(BlueNoroff/APT38)이 국가 배후 조직 최초로 npm 대규모 공급망 공격을 감행한 사건, Shai-Hulud 계열 공급망 웜이 'Miasma'라는 이름으로 Red Hat·node-gyp 생태계를 잇달아 침해한 사건, 그리고 약 74,000 대의 Fortinet 방화벽 관리자 자격 증명이 대규모로 유출된 'FortiBleed' 사태로 요약됩니다. 여기에 랜섬웨어 조직 The Gentlemen 이 자체 EDR 킬러 프레임워크 'GentleKiller'의 실체를 드러내며 478 개 이상의 피해 기업을 발생했고, AI 워크플로 자동화 도구와 브라우징 에이전트를 겨냥한 RCE 취약점이 실제 공격에 악용되면서 AI 인프라가 새로운 공격 표면으로 굳어지는 흐름이 뚜렷해졌습니다.

DPRK 연계 위협 그룹의 npm 공급망 공격 국가 배후화

북한 연계 위협 그룹 Sapphire Sleet(BlueNoroff, APT38 로도 추적)이 2026 년 6 월 17 일, npm 계정 'ehindero'를 탈취해 AI 에이전트 프레임워크 Mastra 의 140 개 이상 패키지(@mastra 스코프)를 약 19 분 만에 오염시키는 공급망 공격을 감행했습니다. 공격자는 정상 dayjs 라이브러리를 사칭한 'easy-day-js' 패키지를 새 의존성으로 주입해 postinstall 훅으로 암호화폐 지갑 정보를 탈취하고 C2 서버로 통신했으며, 마이크로소프트는 6 월 19 일 이를 Sapphire Sleet 의 소행으로 공식 귀속했습니다. 이는 동일 조직이 4 월에 감행한 Axios npm 침해에 이은 두 번째 공급망 공격으로, 국가 배후 조직이 대규모 npm 공급망 공격을 수행한 최초 사례로 평가되었습니다.

Shai-Hulud/Miasma 계열 공급망 웜의 연쇄 확산

npm 생태계를 겨냥한 자가 전파형 공급망 공격이 6 월에도 끊이지 않았습니다. 6 월 1 일, Red Hat 직원의 GitHub 계정이 악성 VS Code 확장을 통해 침해되어 @redhat-cloud-services 네임스페이스 아래 32 개 패키지(주간 다운로드 약 8 만 회)에 'Miasma'로 명명된 악성코드가 유효한 SLSA provenance 서명과 함께 배포되었습니다. 해당 페이로드는 5 월 12 일 TeamPCP 가 오픈소스로 공개한 'Mini Shai-Hulud' 악성코드의 변형으로, GCP·Azure 클라우드 자격 증명 수집 기능이 추가되고 감염마다 고유하게 암호화된 페이로드를 생성하는 등 진화된 형태였습니다. 이 공격은 CI/CD 러너 메모리에서 GitHub Actions 시크릿을 탈취하고, 토큰 무효화 시 홈 디렉터리를 삭제하는 파괴적 안전장치(honeytoken)까지 포함되어 있습니다.

추가적으로 node-gyp/binding.gyp 를 악용한 별도의 자가 전파형 웜이 57 개 패키지, 수백 개의 악성 버전에 걸쳐 확산되었으며, autotel 계열 등 단일 유지관리자 계정을 중심으로 전파되는 패턴이 확인되었습니다. 이 계보의 공격은 이후 6 월 24 일 GitHub Actions('codfish/semantic-release-action')와 Go 모듈(Verana Blockchain)까지 번지며 npm 을 넘어 다른 생태계로 확장되었고, 러시아어 사용자 킬스위치와 559 개 이상의 GitHub 데드드롭 저장소를 운용하는 등 지속적으로 진화했습니다.

Fortinet 대규모 자격 증명 유출과 국가 연계 취약점 악용

'FortiBleed'로 명명된 대규모 자격 증명 유출 사태가 194 개국에서 약 74,000 대의 인터넷 노출 Fortinet FortiGate 방화벽·VPN 게이트웨이에 영향을 미쳤습니다. 러시아어권 사이버 범죄 그룹이 과거 유출된 자격 증명과 브루트포스 공격(GPU 크래킹 인프라 활용)을 결합해 관리자 계정을 확보한 것으로 분석되었으며, Samsung, Siemens, Foxconn, Oracle, Accenture, DHL 등 다수의 대기업과 정부 기관이 영향권에 포함되었습니다. Fortinet 은 이것이 신규 제로데이가 아니라 과거 사고(FG-IR-26-060 등)의 자격 증명 재사용과 취약한 비밀번호 관리에서 비롯되었다고 설명했으며, CISA 는 즉각적인 자격 증명 재설정과 다중 인증 적용을 권고했습니다.

같은 시기 Cisco Catalyst SD-WAN Manager 의 파일 쓰기 취약점(CVE-2026-20262)이 2026 년 들어 7 번째로 실제 악용이 확인된 제로데이로 6 월 15 일 CISA KEV 에 추가되었으며, 이는 앞서 6 월 9 일 KEV 에 추가된 명령 인젝션 취약점(CVE-2026-20245)과 함께 UAT-8616 이라는 위협 행위자가 지속적으로 운용해온 캠페인의 일부로 분석되었습니다. CISA 는 6 월 한 달간 총 23 개의 취약점을 KEV 목록에 추가했고 이 중 6 개가 제로데이였으며, SimpleHelp, Ivanti Sentry, Check Point Security Gateway, PTC Windchill, Oracle PeopleSoft/WebLogic, Splunk Enterprise, Ubiquiti UniFi OS(3 건 모두 CVSS 10.0), Lantronix EDS5000 등 네트워크·엔터프라이즈 인프라 전반에 걸쳐 악용이 확인되었습니다. 특히 PTC Windchill 결함(CVE-2026-12569)은 공개 직후 JSP 웹셸 배포에 악용되었습니다.

AI 워크플로 자동화 도구를 겨냥한 실전 공격

AI 개발 인프라를 직접 겨냥한 취약점이 6 월에도 실전 악용으로 이어졌습니다. 마이크로소프트는 6 월 18 일, AutoGen Studio 기반 AI 브라우징 에이전트를 겨냥한 'AutoJack' 취약점을 공개했는데, 악성 웹페이지가 로컬호스트에서 동작하는 MCP 웹소켓에 접근해 자격 증명 없이도 호스트 수준의 임의 프로세스 실행을 유발할 수 있음을 시연했습니다. 또한 AI 워크플로 자동화 도구 Langflow 에서는 인증 없는 RCE 취약점(CVE-2026-33017)과 크로스 테넌트 IDOR 취약점(CVE-2026-55255)이 결합되어 실전 공격에 악용된 사례가 확인되었습니다. 단일 공격자가 사흘에 걸쳐 인터넷에 노출된 Langflow 인스턴스를 정찰한 뒤, IDOR 로 다른 테넌트의 LLM 제공자 API 키와 AWS 키를 탈취하고 RCE 로 호스트까지 장악한 것으로 분석되었습니다.

랜섬웨어 EDR 킬러의 표준화, 대규모 데이터 유출과 모바일 위협

랜섬웨어 조직 The Gentlemen 은 ESET 조사를 통해 자체 개발한 EDR 킬러 프레임워크 'GentleKiller'의 실체가 공개되었습니다. BYOVD(Bring Your Own Vulnerable Driver) 기법을 활용한 최소 8 종의 변종으로 Microsoft Defender, CrowdStrike, SentinelOne 등 48 개 보안 벤더의 400 개 이상 프로세스를 종료할 수 있으며, 90%라는 파격적인 제휴사 수익 배분 조건을 내걸어 제휴사를 빠르게 끌어모았습니다. 6 월 기준 478 개 이상의 피해 기업이 확인되었고, 호주 2 위 원당 생산업체 Mackay Sugar 를 공격해 제당 공장 가동을 일주일 이상 중단시키는 등 운영기술(OT) 환경까지 실질적 피해가 미쳤습니다.

데이터 유출 측면에서는 6 월 한 달간 다수의 대형 사고가 확인되었습니다. 통신사 Charter 는 비싱(음성 피싱) 공격으로 직원 1 명의 Microsoft Entra 계정이 탈취되며 490 만 건의 고객 기록이 유출되었고, 크루즈 업체 Carnival 도 유사한 방식으로 600 만 고객 정보가 노출되었습니다. Nintendo 는 자사 시스템이 아닌 제 3 자 직원 설문 플랫폼(TinyPulse)이 침해되며 2016 년 이후 누적된 직원 정보가 유출되었고, Kodak(220 만 건), 텍사스주 야생동물국(300 만 명 이상, 운전면허·여권 정보 포함), 제약사 Novo Nordisk(내부 IT 시스템 침해, 임상시험 환자 정보는 비식별 처리) 등이 6 월에 확인·공개된 주요 사고입니다. 모바일 영역에서는 217 개 은행·암호화폐 앱을 표적으로 137 개의 원격 명령을 수행하는 안드로이드 뱅킹 트로이목마 'Rokarolla'가 6 월 16~18 일 보도되었는데, 가짜 TikTok·Chrome 앱으로 유포되며 잠금화면 PIN 탈취, 클립보드 조작(암호화폐 지갑 주소 바꿔치기), Google Play Protect 비활성화 등 기기 완전 장악 수준의 기능을 보였습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

6 월 한 달간 악성코드 탐지 건수는 전월(1,014,016 건) 대비 약 16% 감소한 854,530 건을 기록하며 두 달 연속 감소세를 이어갔습니다. 1 위 Gen:Variant.Application.Miner.2 는 541,005 건으로 전월(710,278 건) 대비 약 24% 줄었으나, 여전히 전체 탐지의 약 63%를 차지하며 코인마이너 계열의 지배력을 유지했습니다.

이번 달 가장 두드러진 변화는 신규 탐지명 Generic.MeadowLocust.A.6277540D 가 곧바로 2 위(91,723 건)에 진입한 점입니다. 기존 2 위였던 Exploit.CVE-2010-2568.Gen 은 탐지 건수 자체는 59,153 건에서 61,154 건으로 소폭 증가했음에도, 신규 항목의 등장으로 순위가 3 위로 밀려났습니다.

크랙·인증 우회 도구 계열의 강세도 계속되었습니다. Misc.HackTool.AutoKMS 는 14,275 건(9 위)에서 15,674 건(7 위)으로 늘며 두 계단 상승했고, Misc.HackTool.KMSActivator 역시 5 계단 상승해 10 위(7,953 건)에 올랐습니다. Trojan.GenericKD 계열 2 종(72973669, 78057588)과 GT:VB.Laburrak.11.6277961D, Trojan.Python.Miner 등 다수의 신규 탐지명이 상위권에 진입하였습니다.

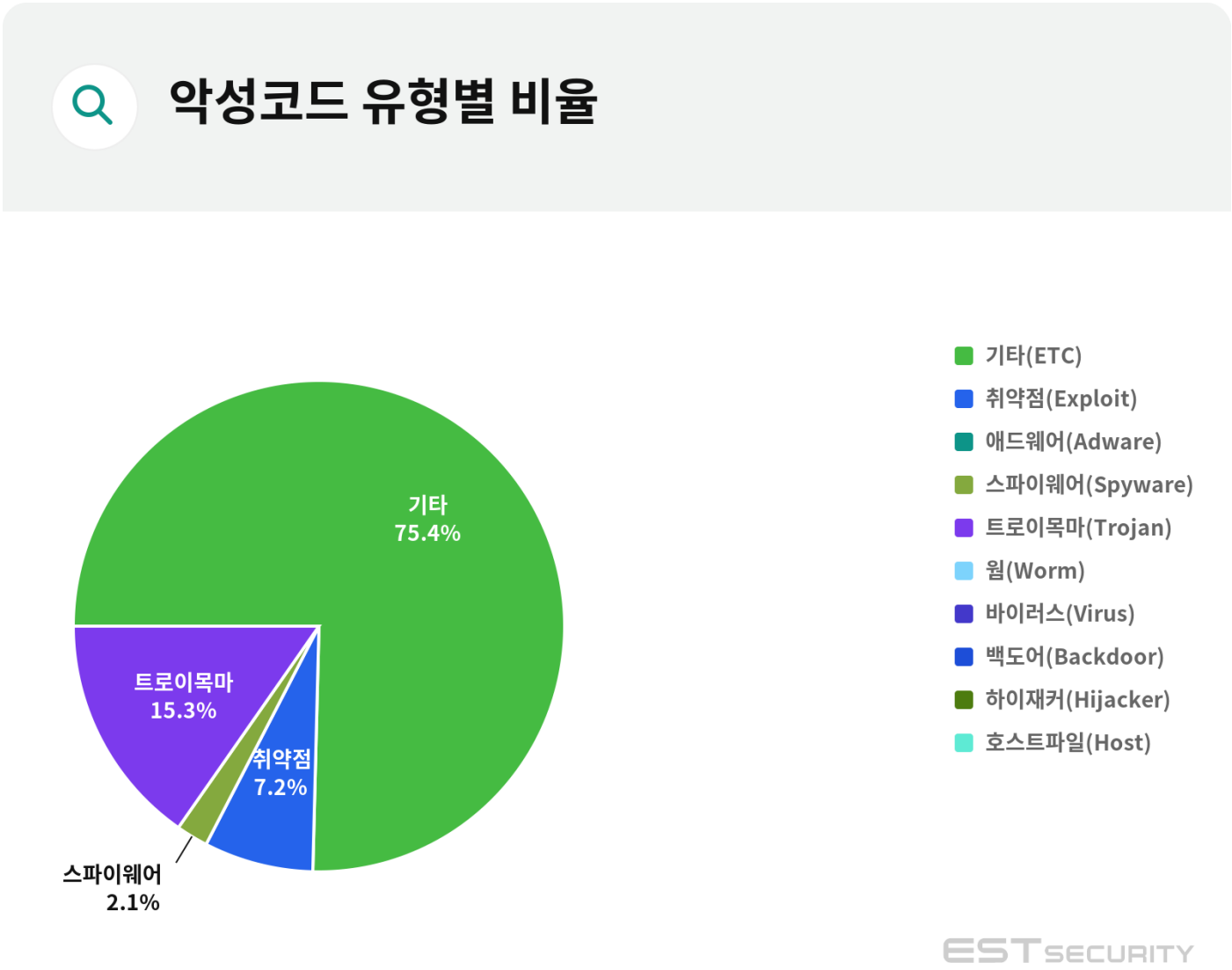
순위	등락	악성코드 진단명	카테고리	합계
1	-	Gen:Variant.Application.Miner.2	ETC	541005
2	NEW	Generic.MeadowLocust.A.6277540D	TROJAN	91723
3	↓1	Exploit.CVE-2010-2568.Gen	EXPLOIT	61154
4	↓1	Gen:Variant.Tedy.675091	ETC	39685
5	↑1	Spyware.Infostealer.Bladabindi	SPYWARE	18288
6	NEW	Trojan.GenericKD.72973669	TROJAN	17148
7	↑2	Misc.HackTool.AutoKMS	ETC	15674
8	NEW	Trojan.GenericKD.78057588	TROJAN	14257
9	NEW	Gen:Variant.TDss.49	ETC	8849
10	↑5	Misc.HackTool.KMSActivator	ETC	7953
11	NEW	GT:VB.Laburrak.11.6277961D	ETC	7938
12	NEW	Misc.Keygen	ETC	7937
13	NEW	Trojan.Python.Miner	TROJAN	7932
14	↓2	Gen:Variant.Jaik.292533	ETC	7896
15	↓10	Gen:Variant.Adware.Barys.61515	ETC	7091

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위

2026 년 6 월 1 일 ~ 2026 년 6 월 30 일

악성코드 유형별 비율

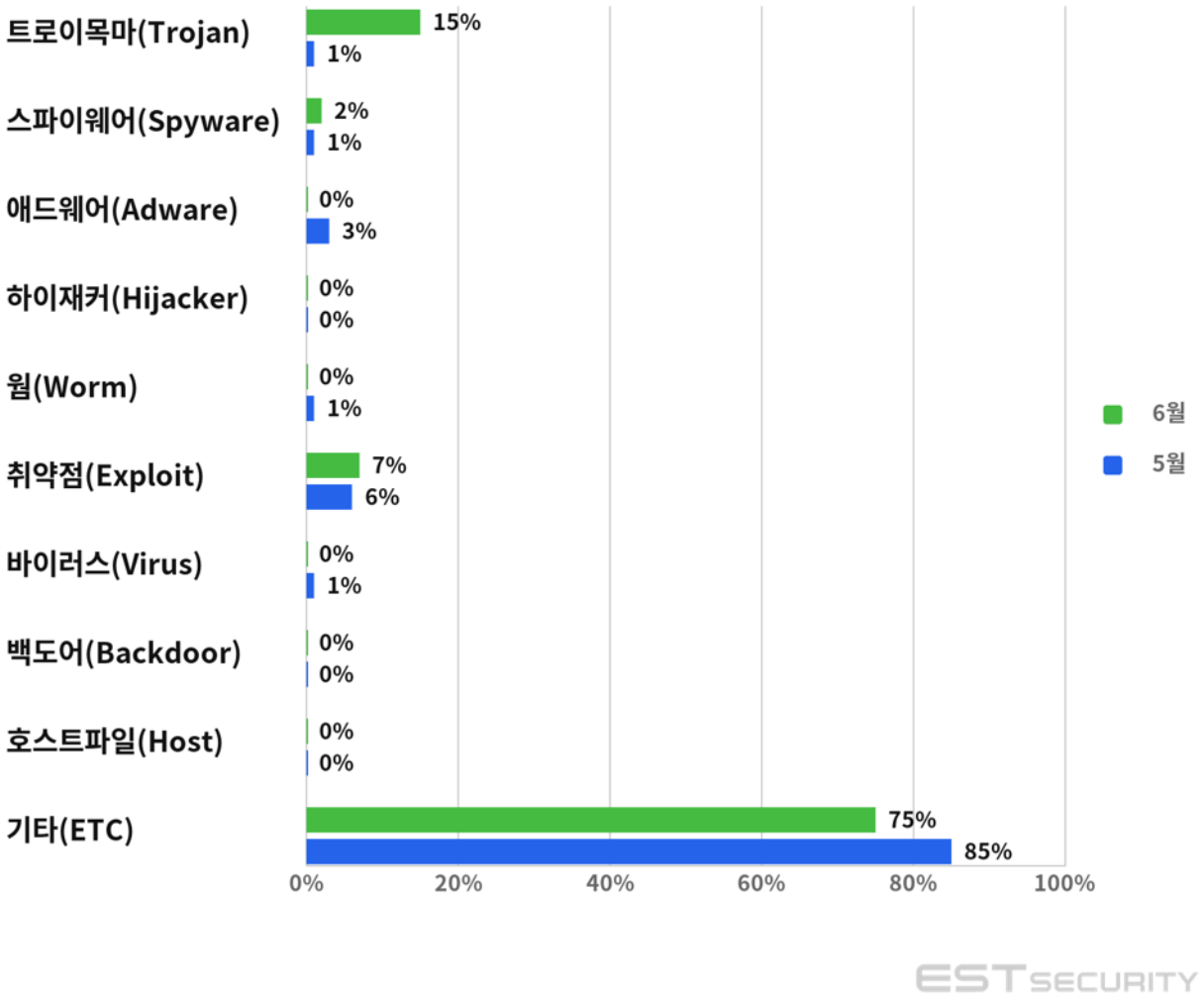
악성코드 유형별 감염 비율을 분석한 결과, 기타(ETC) 유형이 75.4%로 1 위를 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 15.3%, 취약점(Exploit)이 7.2%, 스파이웨어(Spyware)는 2.1%을 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

2026 년 6 월에는 5 월과 비교하여 기타(ETC) 유형이 10% 감소하였습니다. 대신 트로이목마(Trojan) 유형이 14%, 취약점(Exploit) 유형은 1% 증가하였으며, 애드웨어(Adware) 유형은 3%, 바이러스(Virus) 유형은 1% 감소하였습니다. 스파이웨어(Spyware) 유형은 전월과 동일한 수준을 유지하였습니다.

카테고리별 악성코드 비율 전월 비교



3. 알약 M 악성코드 탐지 통계

감염 악성코드 TOP15

6 월 한 달간 모바일 악성코드 탐지 건수는 전월(15,326 건) 대비 약 200.8% 급증한 46,101 건을 기록하며 두 배가 넘는 증가세를 보였습니다. 신규 진입한 Android.Riskware.RogueUrl 이 13,314 건으로 곧바로 1 위에 오르며

전체 탐지량 급증했고, 전달 9 위였던 Android.Adware.Agent 는 13,083 건을 기록하며 7 계단 상승해 2 위에 올랐습니다. 반면 5 월까지 1 위를 유지하던 Android.Riskware.Agent 는 6,380 건으로 3 위로 밀려났습니다.

이번 달에는 신규 진입 항목이 유독 두드러졌습니다. Android.Riskware.FakeApp(2,137 건)이 곧바로 4 위에 올랐고, Android.Adware.Mobby(1,430 건, 6 위), Android.Trojan.SpyAgent(1,170 건, 7 위), Android.Riskware.InfoStealer(970 건, 8 위), Android.Riskware.SpyAgent(445 건, 13 위) 등 절반에 가까운 항목이 새롭게 상위 15 위권에 진입했습니다. 특히 FakeApp·InfoStealer·SpyAgent 등 정보 탈취 및 위장 앱 계열이 신규 진입하면서, 기존 Riskware 중심의 탐지 구도에서 정보 탈취형 위협의 비중이 크게 확대되는 양상을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	NEW	Android.Riskware.RogueUrl	Riskware	13314
2	↑7	Android.Adware.Agent	Adware	13083
3	↓3	Android.Riskware.Agent	Riskware	6380
4	NEW	Android.Riskware.FakeApp	Riskware	2137
5	↓3	Android.Monitor.MSpy	Monitor	2082
6	↓4	Android.Riskware.Packer	Riskware	1498
7	NEW	Android.Adware.Mobby	Adware	1430
8	NEW	Android.Trojan.SpyAgent	Trojan	1170
9	NEW	Android.Riskware.InfoStealer	Riskware	970
10	↓7	Android.Riskware.PackMal	Riskware	931
11	↓4	Android.Adware.Mulad	Adware	917
12	↑2	Android.Trojan.AgentSpy	Trojan	799
13	NEW	Android.Trojan.InfoStealer	Trojan	501
14	NEW	Android.Riskware.SpyAgent	Riskware	445
15	↓10	Android.Riskware.HackTool	Riskware	444

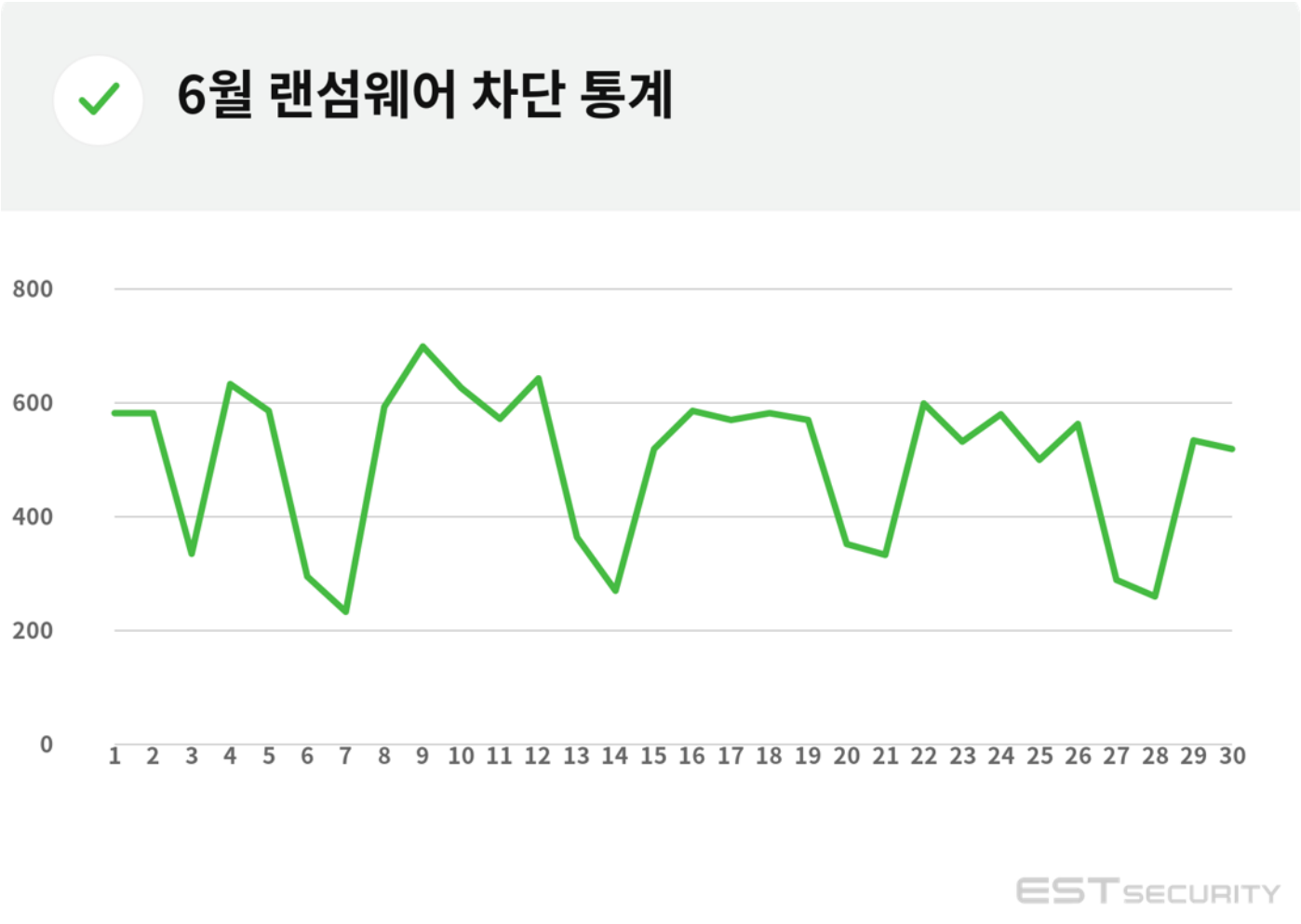
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026 년 6 월 1 일 ~ 2026 년 6 월 30 일

4. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

6 월 랜섬웨어 차단 통계

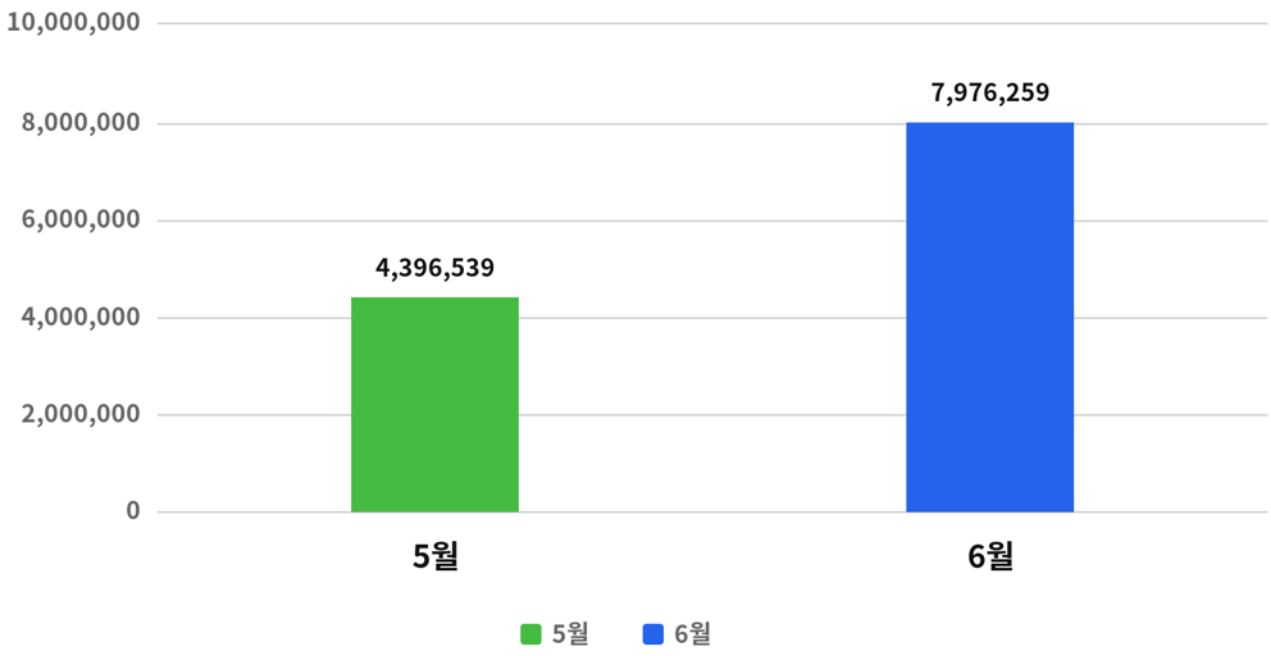
해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 6 월 1 일부터 6 월 30 일까지 15,008 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 26 년 6 월 한 달간 총 7,976,259 건의 URL 이 확인되었습니다. 이 수치는 5 월 한 달간 총 4,396,539 건의 악성코드 유포지 URL 수에 비해 약 81% 증가한 수치입니다.

6월 악성 URL 경유지/유포지 통계

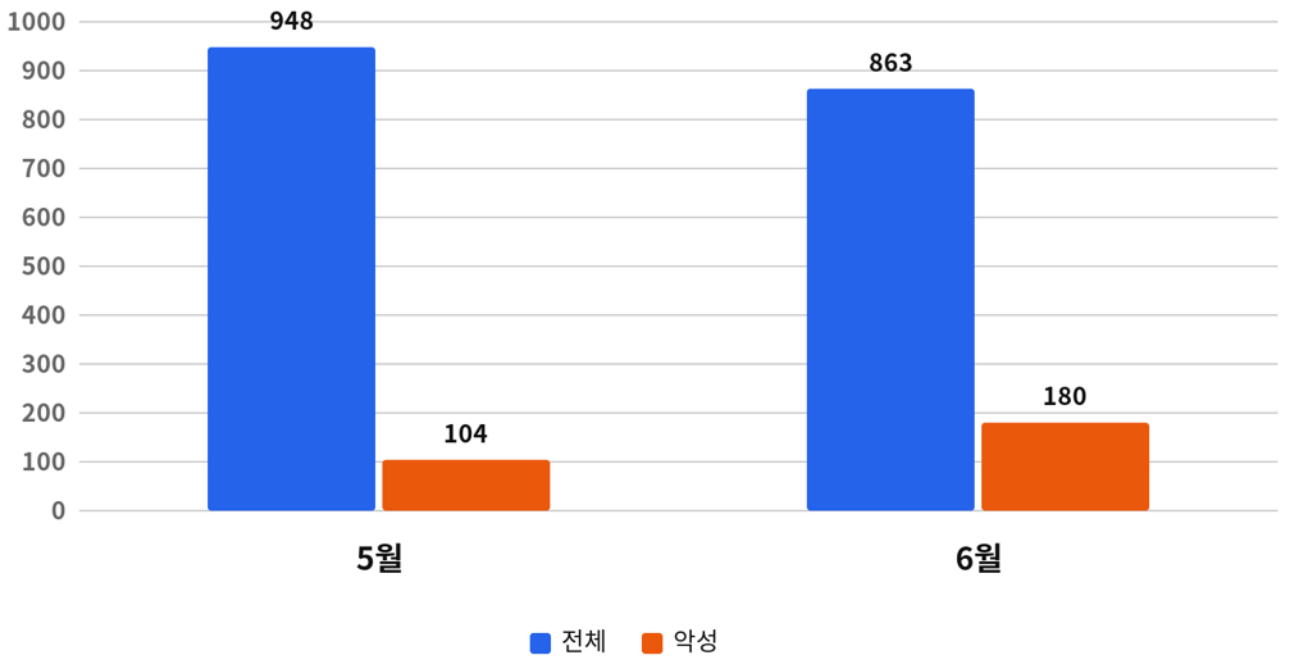


5. 악성 이메일 통계

이메일 유입량

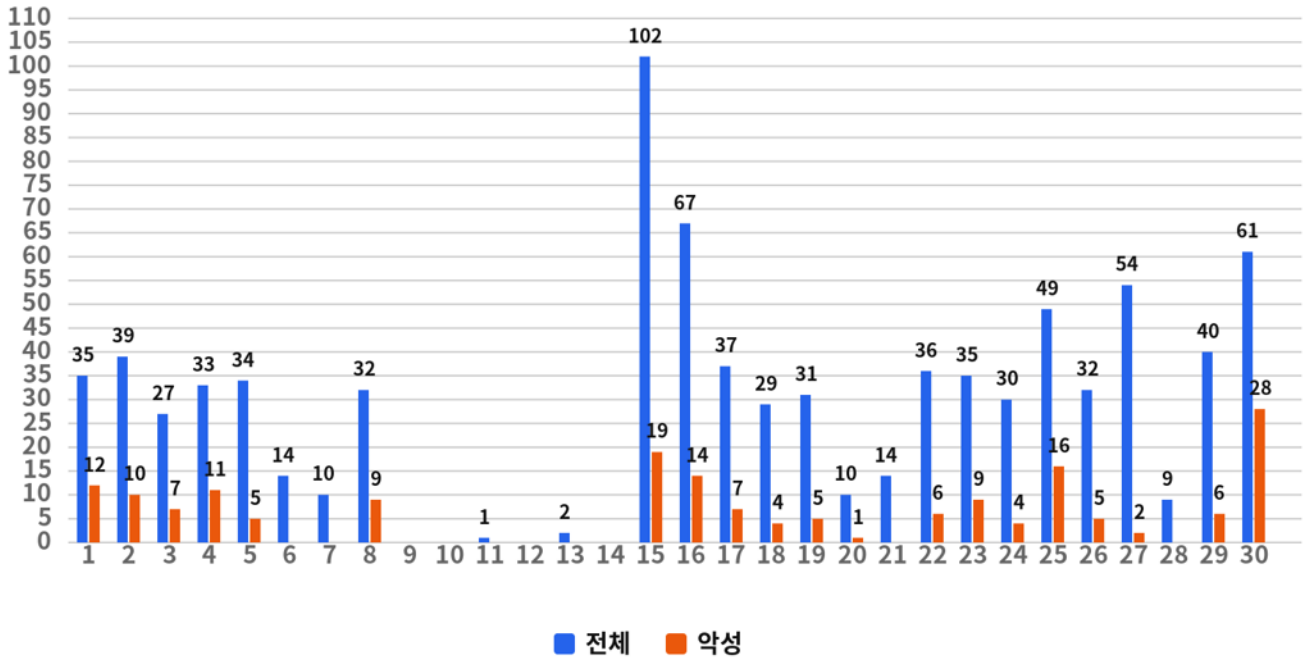
6 월 이메일 유입량은 총 863 건이고 그중 악성은 180 건으로 20.86%의 비율을 보였습니다. 악성 이메일의 경우 전월(5 월) 104 건 대비 180 건으로 76 건이 증가했습니다.

이메일 유입량 전월 비교



일일 유입량은 하루 최저 0 건(악성 0 건)에서 최대 102 건(악성 28 건)으로 일별 편차를 확인할 수 있습니다.

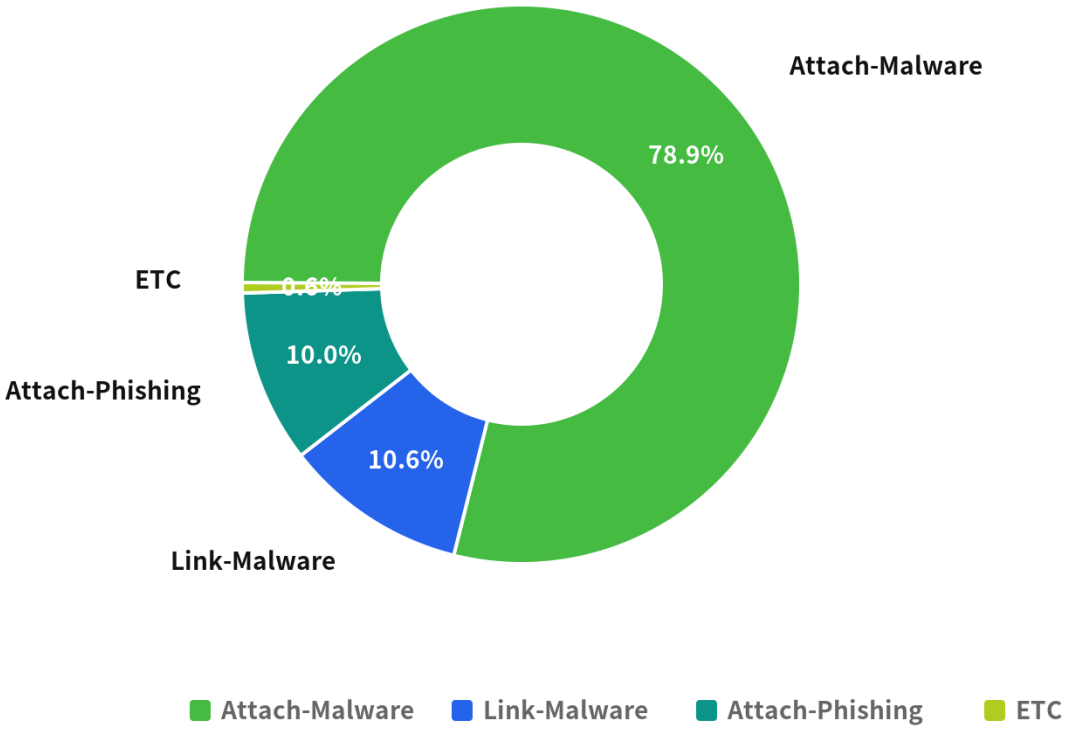
이메일 유입량 일일 비교



이메일 유형

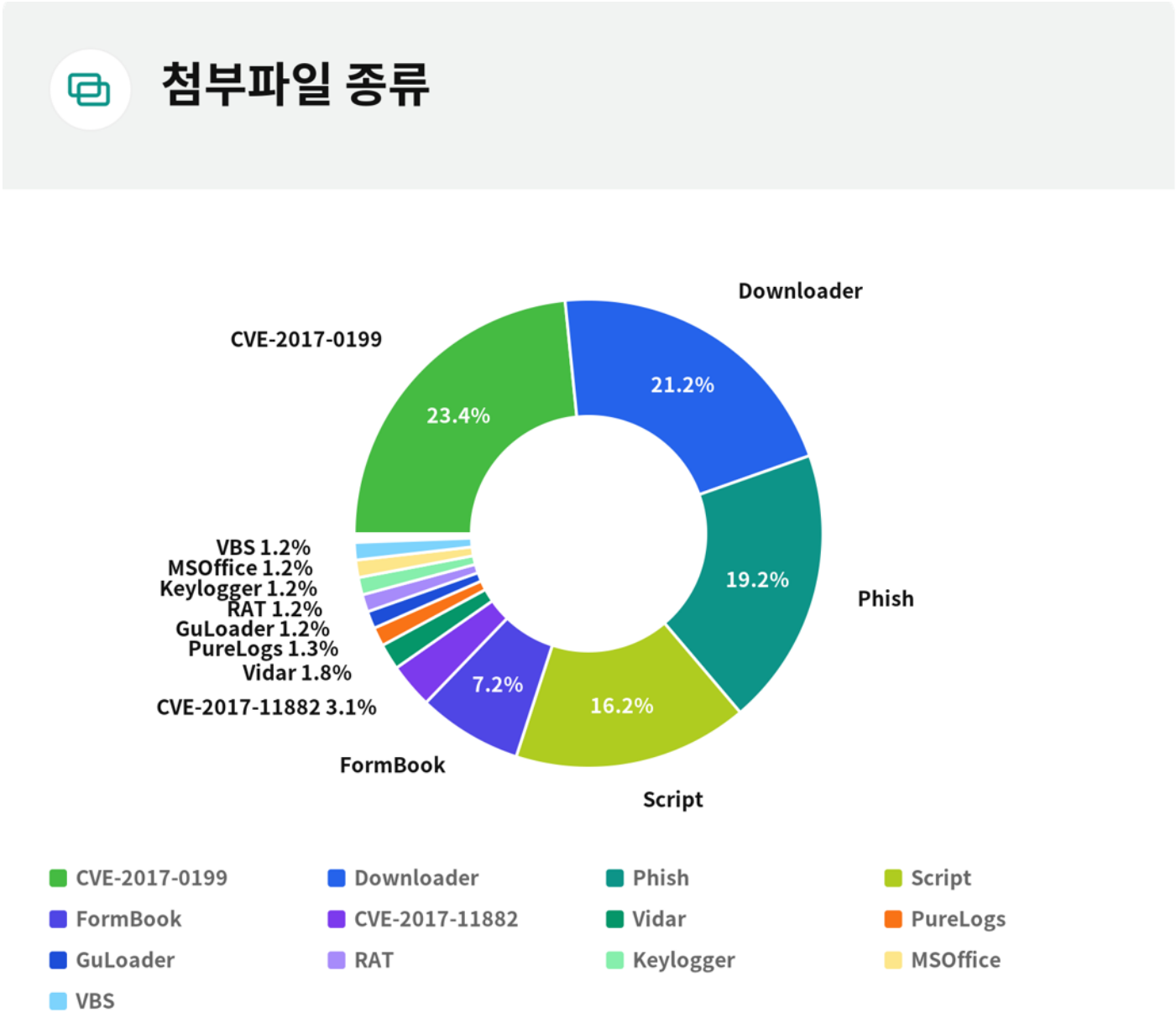
악성 이메일을 유형별로 살펴보면 180 건 중 Attach-Malware 형이 78.9%로 가장 많았고 뒤이어 Link-Malware 형이 10.6%를 나타냈습니다.

악성 이메일 유형



첨부파일 종류

첨부파일은 'CVE-2017-0199'형태가 23.4%로 제일 큰 비중을 차지했고 뒤이어 'Downloader', 'Script'가 각각 21.2%, 16.2%의 비중을 차지했습니다.



대표적인 위협 이메일의 제목과 첨부파일명

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

- Zamówienie na zakup Technomex ZZ-H/25/12/223
- [EPDA REQUEST | Merak] MT. Caribbean 1 / V2506A
- RE: New Order to deliver/Shipping Details
- Request for Quotation – Mid-Year Projects
- MV NAVIOS SPHERA @ PORT KLANG- PROFORMA DA REQ
- RFQ PO # Attached
- [Y*****G Corp.] Request for Quotation
- WIRE CONFIRMATION
- Purchase Order SINO_5700142
- Request for pricing– Mid-Year Projects

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

- zakup Technomex ZZ-H2512223.xls
- Shipping Details&New Order.rar
- PO20260630-0044_RFQ.xls
- Qttn Requirepdf.z
- SWIFT COPY.xls
- PO06292026-0022391_Speifications.xls
- SHIPMENT DOCUMENT ORDER NO - N400..xls
- Order list 7027521.xls
- image_0013pdf.z
- 선적서류 – **증권(BL) 초안.xls

2

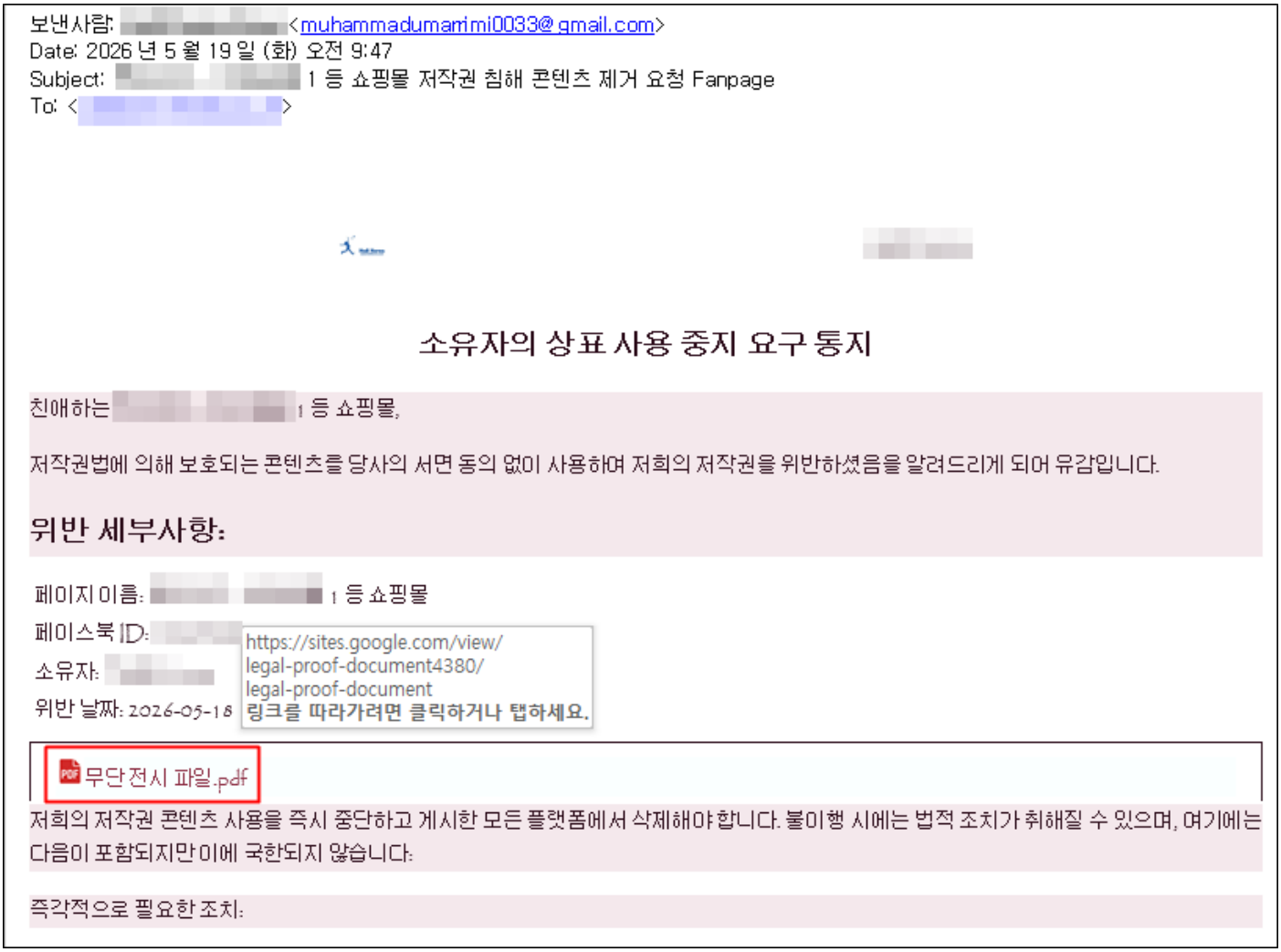
최신 악성코드 동향

1. 디지털 서명 검증을 우회하는 MS Word 변조 악성코드 (CVE-2013-3900)

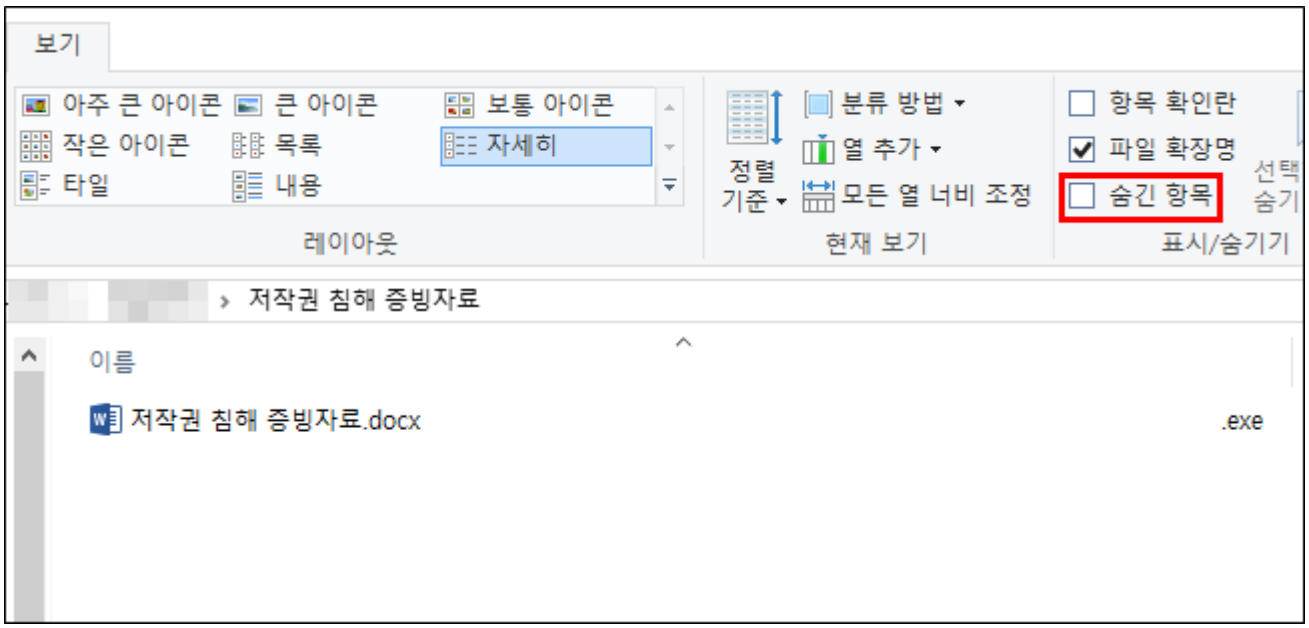
이스트시큐리티 대응센터(ESRC)가 정상 서명된 Microsoft Word 실행 파일로 위장한 다단계 로더 악성코드를 확인했다. 저작권 침해를 사칭한 피싱 메일로 유포되었으며, 정상 서명 파일을 변조했음에도 Windows 가 이를 "정상 Microsoft 파일"로 계속 인식하게 만드는 오래된 취약점 CVE-2013-3900 을 악용한 것이 핵심이다. 취약점 자체는 코드 실행 결함이 아니라, 서명 기반 신뢰 검증(SmartScreen, AppLocker/WDAC 게시자 정책, EDR 의 변조 탐지 등)을 무력화하는 우회 수단으로 사용되었다.

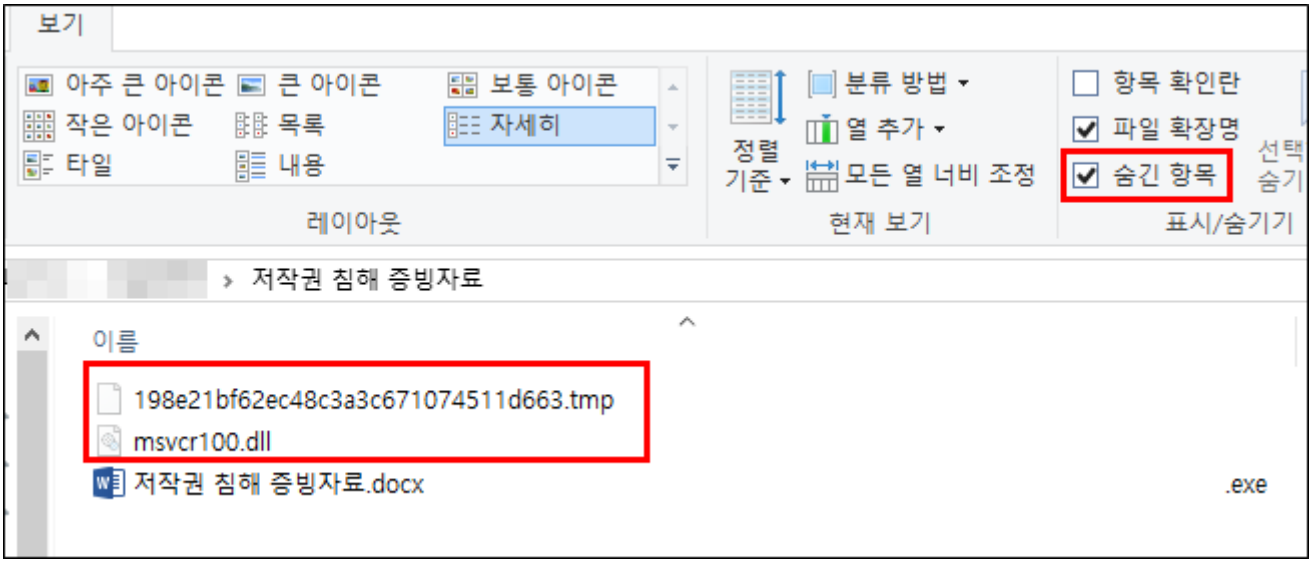
유입 경로

공격자는 국내 여행사를 사칭해 '저작권 침해 콘텐츠 제거 요청' 제목의 메일을 발송했다. 본문 링크를 클릭하면 정상 클라우드(구글 사이트)에 제작해 둔 피싱 페이지로 연결되고, 가짜 CAPTCHA("I'm not a robot")로 정상 보안 확인처럼 위장한다. 체크박스를 누르면 저작권 침해 증빙자료.zip 이 다운로드된다.



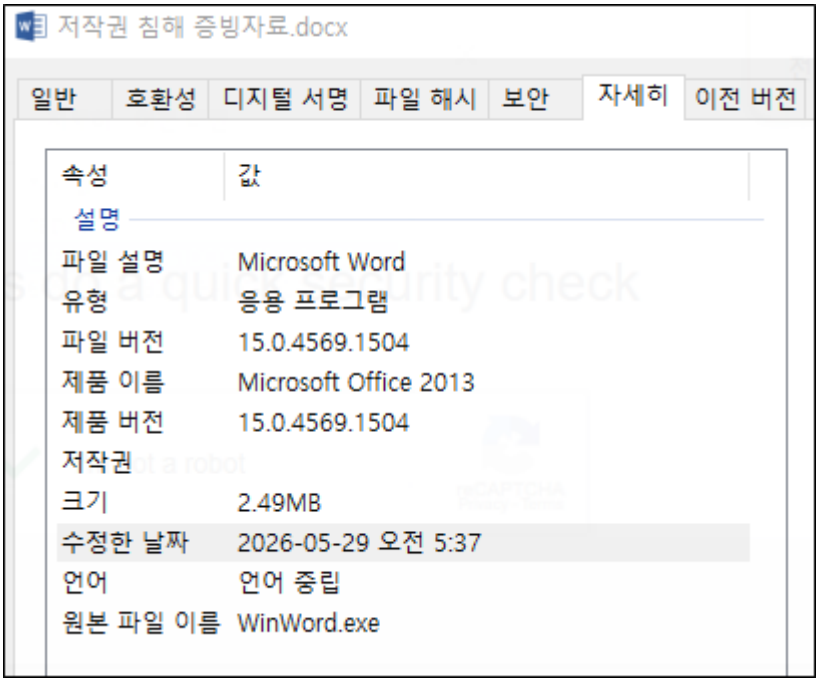
ZIP 내부에는 긴 공백으로 위장한 EXE 만 보이지만, 탐색기 '숨김 항목'을 켜면 악성 DLL 과 TMP 파일이 함께 확인된다. 더미 데이터 TMP 로 압축 크기를 200MB 로 유지해 대용량 파일 검사도 회피한 것으로 추정된다.

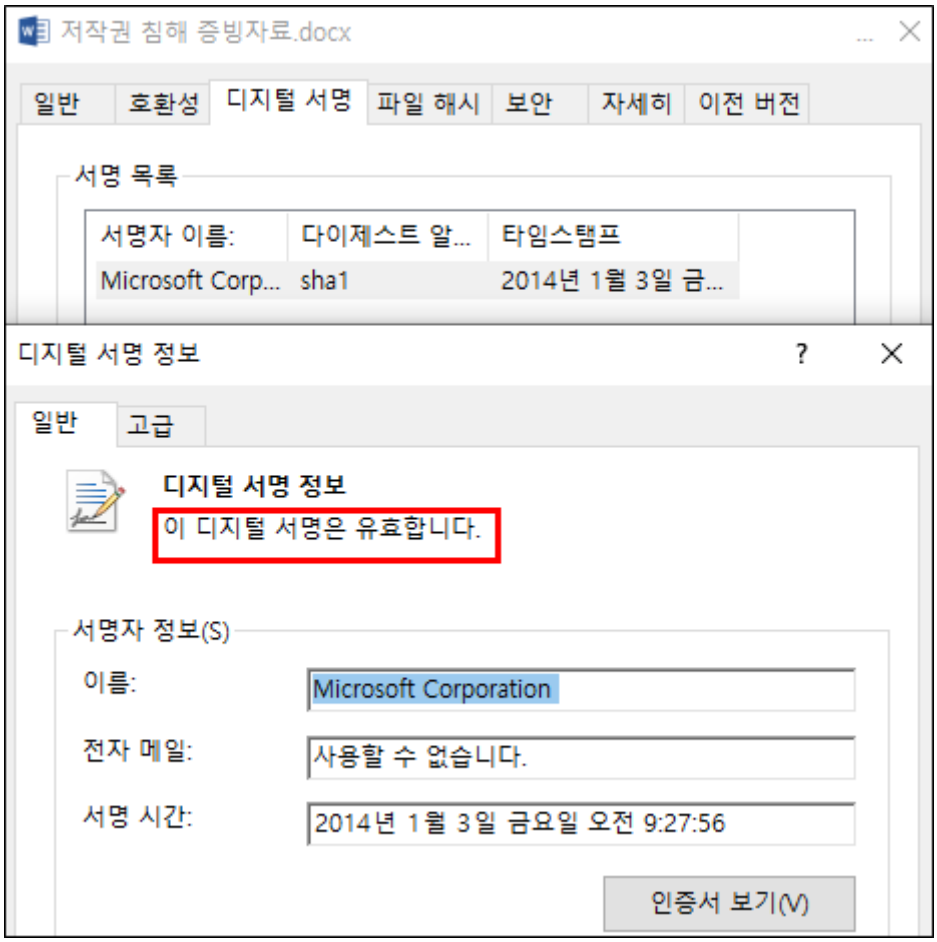




핵심 기법: CVE-2013-3900

Windows 는 PE 파일 무결성을 Authenticode 서명으로 검증하지만, 파일 끝 인증서 테이블(PKCS#7) 영역은 해시 산정 범위에서 제외된다. 공격자는 정상 WinWord.exe 의 디지털 서명 영역에만 암호화된 악성 페이로드를 은닉했고, 실행 코드는 그대로 두어 정품 서명이 유효하게 유지된다. Microsoft 가 MS13-098 로 보완책(레지스트리 EnableCertPaddingCheck)을 제공했으나 호환성 문제로 기본 비활성(옵트인) 상태여서 현재도 악용 가능하다.





공격 흐름 (5 단계)

1 단계 페이로드 은닉 : 정상 Word 서명 영역에 암호화 페이로드 삽입, 서명은 유효 유지(CVE-2013-3900)

2 단계 DLL 사이드로딩 : Word 실행 시 동일 폴더의 msvcr100.dll 이 먼저 로드. 물리 메모리 3GB 이하면 분석 환경으로 보고 종료, 약 315 초 sleep 으로 샌드박스 회피

3 단계 지속성 등록 : %APPDATA%\Microsoft\UpdateServices\에 파일 드롭 후, Run 키(WindowsUpdateCore)와 작업 스케줄러(ONLOGON) 이중 등록. Windows 업데이트로 위장

4 단계 복호화·프로세스 주입 : 인증서 영역의 SIGI 표식으로 페이로드 추출 후 AES-128-CBC 와 16 바이트 롤링 XOR 2 단계 복호화를 거쳐 정상 cvtres.exe 에 프로세스 할로잉(파일리스 실행)

5 단계 최종 모듈 실행 및 C2 통신 : 원격제어·정보탈취형 RAT 로 추정. TLS 암호화 C2 통신, 화면 캡처, WMI 시스템 정보 수집, 파일 스틸러, 키로깅, 관리자 권한 확인, Reflection.Emit 런타임 실행, C2 에서 추가 모듈 다운로드

공격 특징

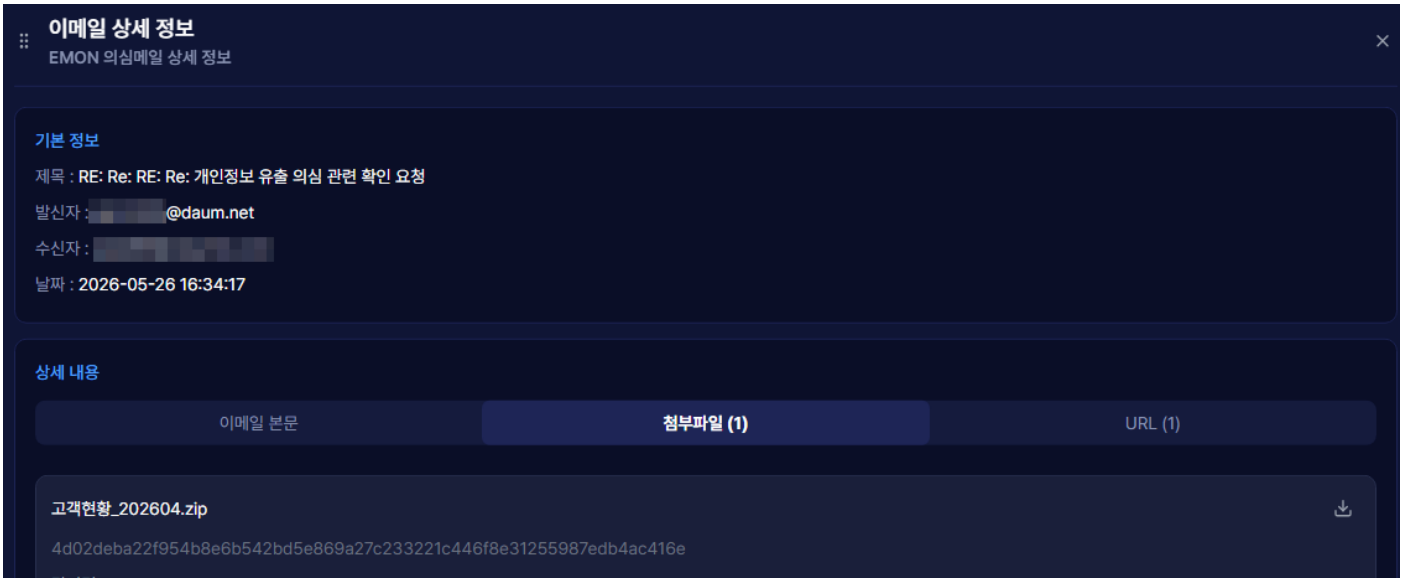
- 사회공학: 저작권 사칭 메일 + 가짜 CAPTCHA + 이중 확장자로 직접 실행 유도
- 신뢰 검증 우회: 정품 서명을 유효하게 유지하며 서명 기반 보안 통제 무력화
- 정상 기능 악용: DLL 사이드로딩·프로세스 할로잉으로 정상 프로그램 뒤에서 실행
- 위장된 지속성: Windows 업데이트로 위장한 폴더·이름으로 재부팅 후에도 생존
- SIGI 표식은 기존 위협 정보에 없던 신규 시그니처로 확인

대응 방안

- 출처 불분명한 메일의 링크 클릭·첨부 실행 자제, 특히 저작권·법무 등 압박형 메일 주의
- 디지털 서명이 정상이어도 파일의 출처와 실행 경로를 함께 확인
- 탐색기에서 "확장명 숨기기" 와 "숨김 파일 표시 안 함" 옵션을 모두 해제해 이중 확장자·숨김 파일 식별

2. 개인정보 유출 의심 문의로 위장한 Kimsuky 스피어피싱 사례 분석

이스트시큐리티 대응센터(ESRC)가 "개인정보 유출 의심 확인 요청"이라는 민감한 소재로 위장한 스피어 피싱 공격을 포착했다. 불특정 다수에게 무작위로 뿌리는 유포형 피싱과 달리, 특정 기업의 실무 담당자를 표적으로 여러 차례 메일을 주고받으며 신뢰를 쌓은 뒤 악성 파일 실행을 유도한 정교한 표적 공격이다. 공격자는 1 차 시도에서 악성 링크가 보안 솔루션에 차단되자 이를 "오탐지"라 둘러대며 같은 악성코드를 암호 걸린 첨부파일로 재전송하는 치밀함까지 보였다. ESRC 는 수집한 악성 샘플 3 종 분석 결과, 이 공격이 북한 연계 조직 Kimsuky 의 전형적 패턴과 매우 높은 유사성을 보인다고 확인했다.



공격 개요

고객을 사칭한 공격자가 국내 기업 정보보호 담당자에게 "내 개인정보가 유출된 것 같으니 확인해 달라"는 문의 메일로 접근을 시작했다. 자연스러운 대화를 이어가다 확인용 자료라는 명목으로 악성 파일을 전달했다. 수집된 샘플 3 종은 동일한 내부 구조와 미끼 문서(고객현황 위장)를 공유하되, 초기 침투는 같고 C2 단계에서 두 갈래로 나뉘었다.

Type A (샘플 1, 2): Dropbox API 기반 C2 — JScript 로더 + RC4 암호화 + 예약된 작업(16 분 주기)

Type B (샘플 3): HTTPS 직접 통신 C2 — VBS 시작프로그램 + 커스텀 시저 암호 + BAT 실행 루프(14 분 주기)

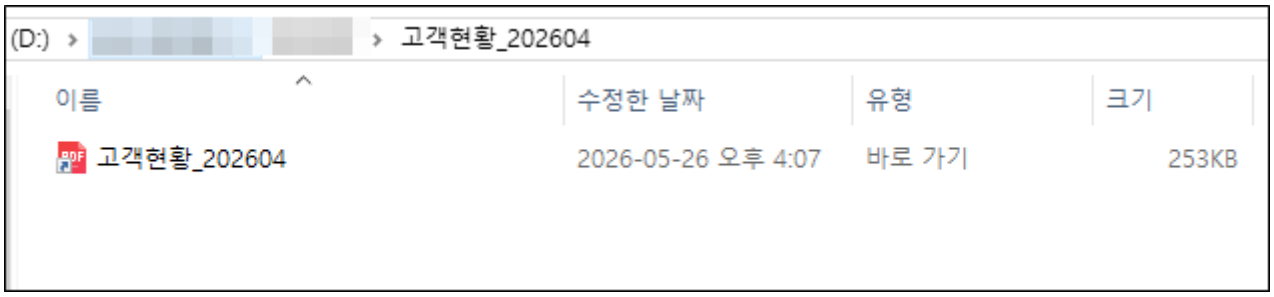
구분	샘플 1	샘플 2	샘플 3
위장 파일명	2603vvip 고객현황.lnk	고객현황_202605.lnk	고객현황_202604.lnk
미끼 문서	XLSX	XLSX	PDF
C2 방식	Dropbox API (Type A)	Dropbox API (Type A)	HTTPS 직접 통신 (Type B)
지속성	예약된 작업 (16 분 주기)	예약된 작업 (16 분 주기)	시작프로그램 VBS (14 분 주기)
캠페인 식별자	Pan05A25	Pd05a28p	Pan

스피어 피싱 메일 분석

단발성이 아니라 여러 차례 오간 메일이었으며, 공격자는 A 사 쇼핑몰 고객으로 위장해 단계적으로 경계심을 허물었다. 흐름은 다음과 같다.

1. 공격자(고객 사칭) → A 사: "당사자·지인 개인정보 유출 정황이 의심된다"며 사내 등록 정보 확인 요청
2. A 사 담당자 → 공격자: 유출 의심 개인정보 목록 공유 요청 회신
3. 공격자 → A 사: "비교·확인용 자료"라며 '고객현황' 문서 다운로드 링크 전달
4. A 사 담당자 → 공격자: 링크에서 악성 파일 탐지되어 확인 어렵다고 통보
5. 공격자 → A 사: "자체 보안팀 검사 결과 이상 없으며 오탐지"라 해명하며 동일 파일을 암호 설정 ZIP 으로 재전송

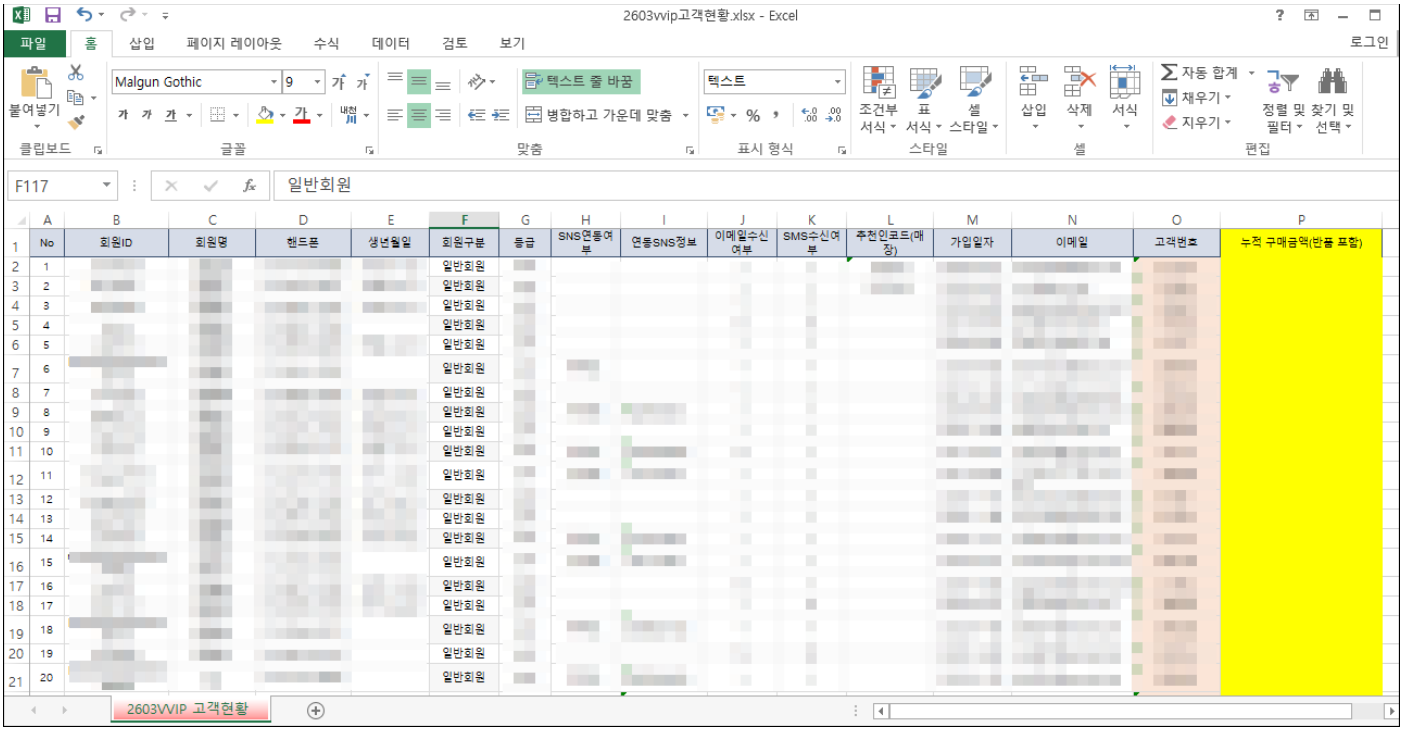
담당자 업무와 직접 관련된 '개인정보 유출 확인' 명분으로 의심을 피했고, 1 차 링크 차단 후에는 암호 압축 파일로 전달 방식을 바꿔 공격을 이어갔다. 압축 내부에는 정상 문서로 위장한 악성 LNK 파일이 들어 있으며, 이를 일반 문서로 오인해 실행하면 감염이 시작된다.

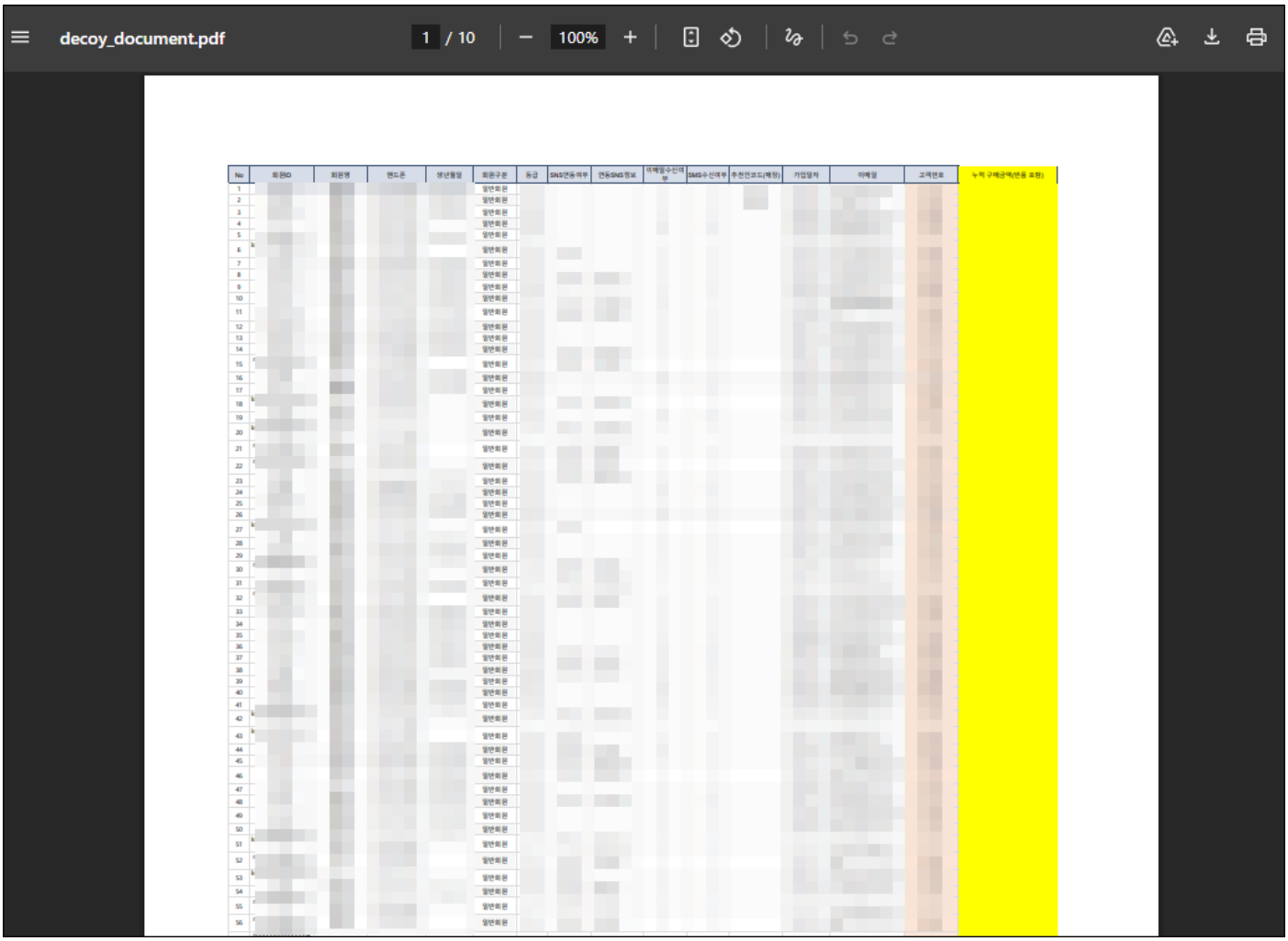


공통 공격 흐름 (1~2 단계)

1 단계 악성 LNK 실행 — LNK 실행 시 백그라운드에서 PowerShell 이 동작한다. 64 비트 대신 SysWOW64 경로의 32 비트 PowerShell 을 강제 호출해 일부 보안 솔루션 감시를 우회하고, PowerShell 위치를 코드에 적지 않고 for /f 구문으로 실행 시점에 검색해 정적 분석을 회피한다. 미끼 문서와 실제 페이로드는 LNK 파일 내부에 오프셋 단위로 이어 붙여져 평문 또는 XOR 인코딩 형태로 저장된다.

2 단계 미끼 문서 표시와 페이로드 드롭 — 의심을 피하기 위해 먼저 미끼 문서를 띄운다. 샘플 1·2 는 '고객현황' 엑셀(XLSX), 샘플 3 은 정상 PDF 를 보여준다. 그 사이 백그라운드에서 XOR 로 숨긴 페이로드를 복원하고, '숨김+시스템' 속성 폴더를 만들어 은닉한 뒤 지속성을 등록하고, 원본 LNK 를 삭제해 흔적을 지운다.





Type A 프레임워크 (샘플 1, 2)

Dropbox를 C2로 악용하는 유형. 복원된 압축에서 자바스크립트 로더와 암호화 페이로드가 함께 풀리고, 로더는 페이로드를 Base64 디코딩과 RC4 복호화(키: Secure20@^)를 거쳐 최종 PowerShell로 복원·실행한다. 약 16분 간격 예약 작업을 등록하되 작업명을 'Intel(R) Ethernet2 Connection' 등 정상 네트워크 드라이버 이름으로 위장한다. 최종 PowerShell은 Dropbox API에 접속해 외부 IP, OS 버전, 실행 프로세스 목록, 사용자·도메인 정보를 수집·암호화해 전송하고, 추가 명령 파일을 내려받아 실행하며 처리한 파일에는 _buy 표식을 붙여 중복 실행을 방지한다. 별도 서버 대신 정상 클라우드 뒤에 숨어 차단·탐지를 우회한 것이 특징이다.

샘플 2는 Type A 업그레이드 버전으로 분석 방해 기능 3가지가 추가됐다. VM/샌드박스 탐지(하드웨어 제조사 정보와 프로세스·네트워크 어댑터 정보가 모두 매칭될 때만 가상환경으로 판정해 오탐 방지), Dropbox 토큰 획득 실패 시 증거 인멸, 임무 완료 후 자가 삭제

Type B 프레임워크 (샘플 3)

클라우드 대신 공격자 직접 운영 서버와 HTTPS로 통신하는 유형. 예약 작업 대신 시작프로그램 폴더에 VBS를 등록해 지속성을 확보하며, 파일명을 'Anlab Auto.vbs'로 만들어 국내 보안 소프트웨어 자동 업데이트처럼 위장했다. 등록된 VBS는 부팅마다 po1ker.bat를 숨긴 창에서 실행하고, po1ker.bat는 sp80poa에 저장된 암호화 명령을 해독한다. 사용된 암호는 공격자가 직접 정의한 79자 알파벳을 5칸씩 밀어 치환하는 커스텀 시저 암호로, 'toopel.shop' 같은 악성 주소를 곧바로 탐지하지 못하게 은닉했다. 해독된 명령은 C2에서 2차 명령 파일을 내려받아 실행하는 것으로, 840초(14분) 대기 후 처음부터 반복하는 무한 루프로 동작한다. 분석 당시 2차 파일은 확인되지 않았으나, C2 게시 내용에 따라 악성 행위를 언제든 교체할 수 있다.

공격 특징

- 정교한 사회공학: 개인정보 유출 확인이라는 담당자 업무 밀착 명분으로 여러 차례 메일을 주고받으며 신뢰 구축
- 공통 침투 체인: 3개 샘플 모두 LNK 기반 동일 초기 실행 방식과 한국어 미끼 문서 사용
- 다중 C2 인프라 운용: 정상 클라우드(Dropbox)와 자체 도메인 병행으로 차단 시 대체 채널 확보
- 국내 표적 정황: 'Pan' 계열 캠페인 식별자, 국내 보안 소프트웨어(안랩) 위장 등 한국 조직 겨냥 흔적 다수

LNK 기반 다단계 침투, 정상 서비스 악용, 표적 업무 맥락을 파고드는 사회공학은 Kimsuky의 전형적 수법과 일치하며, 국내 조직을 겨냥한 표적형 정보 탈취 공격으로 판단된다.

예방 및 대응 방안

- 발신자가 외부인이거나 평소와 다른 주소라면 대화가 자연스럽더라도 첨부파일·다운로드 링크를 함부로 실행하지 말 것

- 보안 솔루션이 악성으로 탐지한 파일을 상대가 "오탐이니 다시 열어보라"며 암호 압축으로 재전송하는 경우는 매우 위험한 신호이므로 절대 압축 해제·실행 금지

- 탐색기의 "확장명 숨기기" 옵션을 해제하고 실행 전 확장자 확인, LNK(바로 가기) 등 의심스러운 파일은 실행하지 않도록 주의

3. Solana SDK 로 위장한 npm 패키지, Telegram Bot API 기반 RAT 유포

이스트시큐리티 대응센터(ESRC)가 Solana 블록체인 공식 SDK 인 @solana/web3.js 를 사칭한 악성 npm 패키지 9 종을 발견했다. 9 개 패키지는 모두 동일한 공격자가 동일한 악성 페이로드를 삽입한 것으로, Telegram Bot API 를 명령제어(C2) 채널로 활용하는 원격 제어 도구(RAT)를 포함한다. 단순 정보 탈취를 넘어 Telegram 채팅 기반 양방향 C2 로 피해 시스템에서 임의의 OS 명령을 실행할 수 있어 심각한 위협이 될 수 있다.

기존 Telegram C2 악용 사례와의 차이점

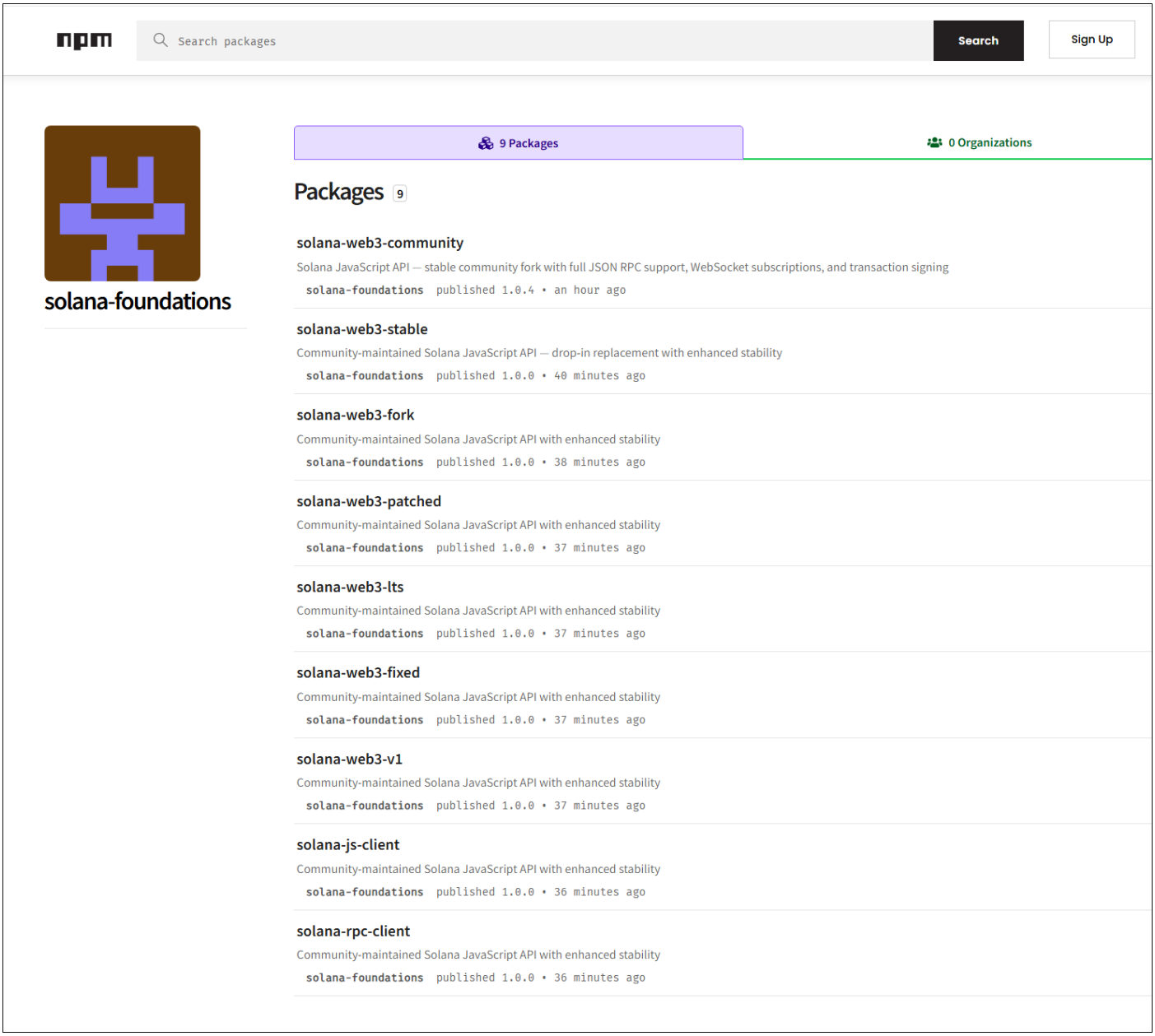
Telegram Bot API 를 C2 로 쓰는 악성 패키지는 기존에도 많았으나, 대부분 정보를 한 방향으로만 빼내고 전송하면 끝나는 단방향 유출 채널이었다. 이번 공격은 SDK 패키지가 자체적으로 Telegram getUpdates 폴링 루프를 구동해 공격자 메시지를 수신하고, 명령을 실행한 뒤 결과를 회신하는 완전한 양방향 C2 구조를 갖춘 점이 다르다. 폴링 주기는 12 초 간격 무한 루프다.

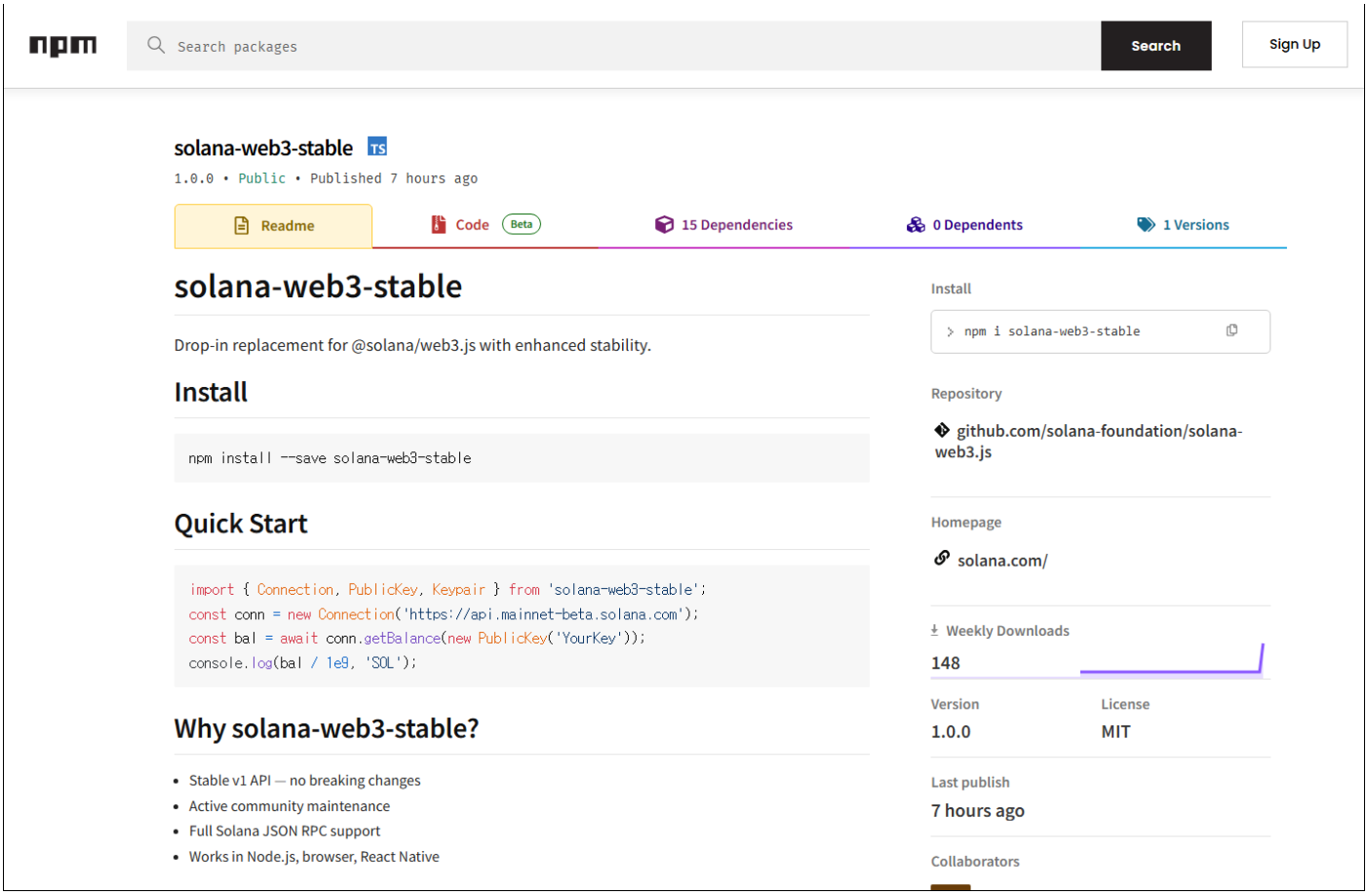
구분	단순 Infostealer	본 샘플 (Telegram RAT)
데이터 유출	수집 → 전송 (1 회성)	수집 → 전송 (1 회성) + 온 디맨드(On-Demand) 재수집
명령 수신	없음	getUpdates 폴링으로 공격자 메시지 수신
명령 실행	없음	/sh, /cmd, 일반 텍스트를 OS 명령으로 실행
결과 회신	없음	실행 결과를 sendMessage 로 회신
폴링 주기	-	12 초 간격 무한 루프
양방향 통신	단방향 (피해자→공격자)	양방향 (피해자↔공격자)

악성 패키지 구성

공격자는 @solana/web3.js 를 사칭한 9 개 타이포스쿼팅 패키지를 동일 작성자명(Solana Labs Maintainers)으로 npm 에 등록했으며, 모두 파일 구조와 바이트 단위 페이로드가 일치한다. 패키지명은 solana-web3-community / -stable / -fixed / -fork / -lts / -patched / -v1, solana-js-client, solana-rpc-client 로,

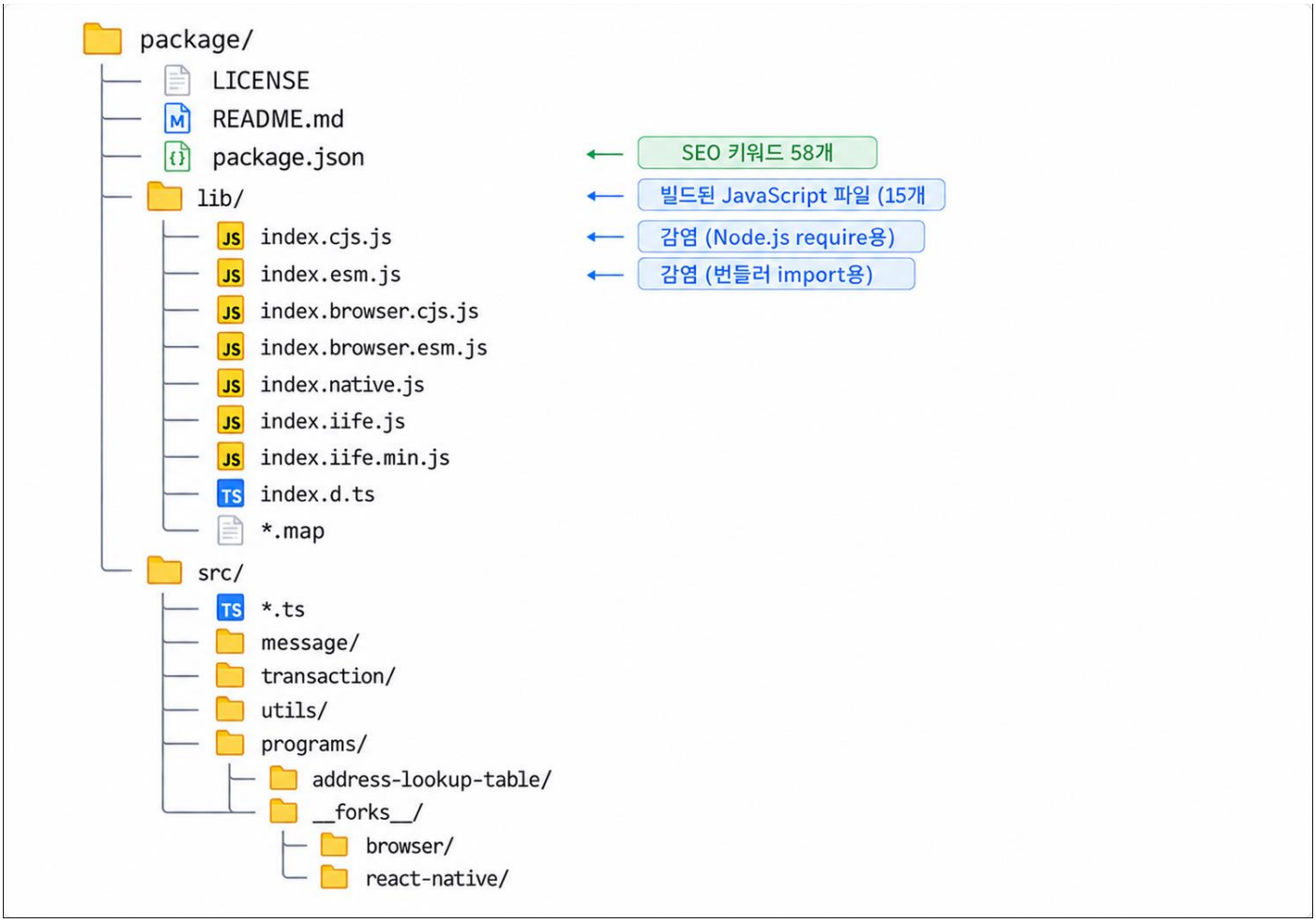
community·stable·lts·fixed·patched 등 개발자가 신뢰할 만한 키워드를 조합했다.





각 package.json 에는 검색 노출을 높이기 위한 58 개 SEO 키워드가 등록됐다. 일반 Solana/Web3 키워드 외에 MEV, 차익거래 봇, 샌드위치 공격 봇, 트레이딩 봇 개발자를 노리는 고가치 타겟 키워드가 포함됐는데, 이런 키워드로 검색하는 개발자는 고액 암호화폐 자산을 다룰 가능성이 높아 가장 가치 있는 표적이 된다.

9 개 패키지는 모두 정상 @solana/web3.js 전체 소스를 포함하면서 빌드 결과물 JS 파일 끝에 악성 코드를 삽입한 동일 구조다. 실제 악성 파일은 Node.js 서버용 index.cjs.js 와 index.esm.js 2 개뿐이며, 브라우저용 파일은 정상이다(악성 코드가 require('fs'), require('child_process') 등 Node 전용 기능을 써서 브라우저에 넣으면 오류로 정체가 드러나기 때문). require 와 import 양쪽 모두를 감염시켜 어떤 방식으로 불러와도 실행되게 했고, 삽입 위치도 소스맵 주석 직후 최하단이라 코드 리뷰에서 지나치기 쉽다.



악성 행위 상세 (8 단계)

1 단계 실행 환경 확인·분석 회피 : Node.js 환경이 아니면 즉시 종료, 전역 플래그(SF)로 중복 실행 방지. 공격자 인프라 IP(104.239.66.223)나 ubuntu2204·vps·server 등 의심 호스트명에서는 실행하지 않아 테스트·분석 환경 회피

2 단계 민감 파일 탈취 : Solana 지갑 비밀키, SSH 비밀키, AWS 자격증명, .env 등 수집. Linux/macOS 대상 경로(10 개)가 Windows(6 개)보다 많고 Docker 컨테이너 경로까지 포함해 서버 환경이 주요 타겟임을 보여준다.

3 단계 환경 변수 수집 : KEY, SECRET, PRIVATE, TOKEN, PASSWORD 등 16 개 키워드가 든 환경 변수를 선별 수집. example·test·placeholder 같은 테스트 값은 걸러 유효한 비밀 정보만 추린다.

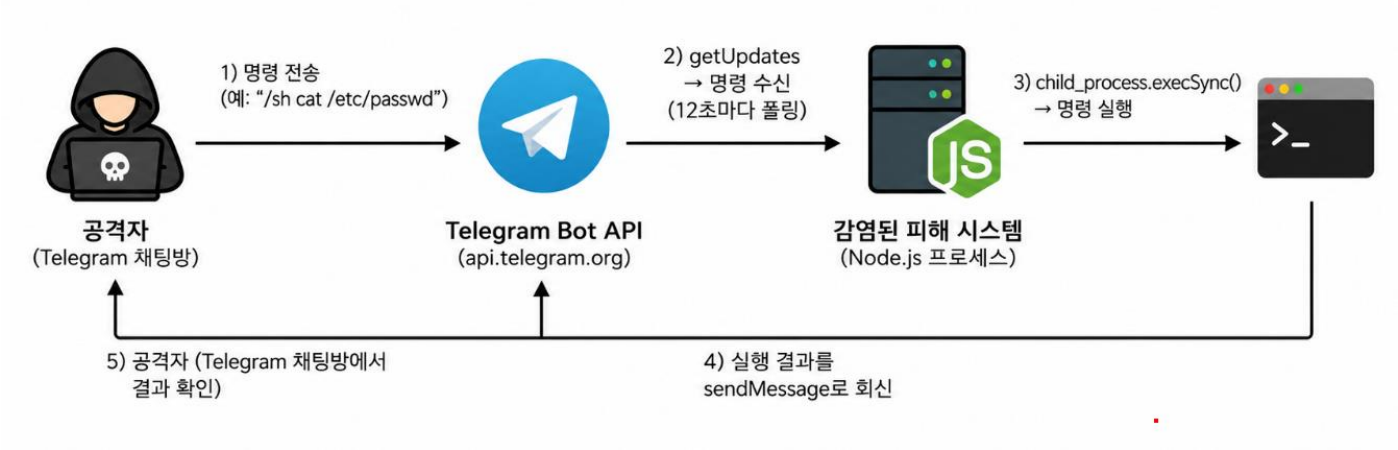
4 단계 Solana CLI 설정 변조(RPC 하이재킹) : 가장 위험한 단계. CLI 설정 파일(config.yml)의 json_rpc_url 을 공격자 서버(http://104.239.66.223:8899)로 덮어쓴다. 이후 피해자의 solana transfer·balance, spl-token transfer 등 모든 요청이 공격자 서버를 경유해, 트랜잭션 가로채기·송금 주소 바꿔치기·거짓 잔액 응답 등이 가능해진다. config.yml 은 평소 잘 안 보는 파일이라 무증상으로 감염이 지속되고, npm uninstall 로 패키지를 지워도 RPC 주소는 복구되지 않아 수동으로 되돌려야 한다. 또 HTTPS 대신 평문 http 로 바꿔 도청 위험까지 생긴다.

5 단계 피해자 식별 해시 생성 : 호스트명+사용자명을 sf-v6 키로 HMAC-SHA256 해싱해 16 자리 식별자를 만든다. 같은 PC·계정은 항상 동일 값이라 공격자가 감염 시스템을 구분·관리할 수 있다.

6 단계 탈취 데이터 즉시 전송 : 수집 데이터를 식별자와 함께 Telegram sendMessage 로 즉시 전송. HTML 포맷, 길이 제한(4,096 자)을 고려해 3,800 자 단위 분할 전송하며 실제 탈취 데이터가 있을 때만 전송

7 단계 지속성 확보(Linux 한정) : crontab 에 재부팅 자동 실행 항목 추가, 네트워크 초기화를 위해 90 초 대기 후 재실행. 설정용 임시 파일은 즉시 삭제

8 단계 양방향 C2 폴링 루프 : 12 초마다 getUpdates 로 공격자 명령을 확인해 실행하고 sendMessage 로 회신. 지원 명령은 /keys·/grab(민감 파일 재수집), /info(시스템 정보), /ssh, /env, /wallet, /sh·/cmd(임의 OS 명령), /die(자가 종료), /help 등이며, 슬래시로 시작하지 않는 일반 텍스트까지 모두 셸 명령으로 실행한다. 명령 실행은 child_process.execSync()(최대 30 초, 50MB 출력 버퍼)



동일 공격자의 이전 캠페인

공격자 서버 IP 와 Telegram Chat ID 를 추적한 결과 이전 공급망 공격 캠페인도 확인됐다. 정상 스코프 @solana 를 사칭한 가짜 스코프 @solana-labs 와 비스코프 패키지를 배포한 사례로, @solana-labs/web3.js, @solana-labs/web3js, @solana-labs/ancor(@coral-xyz/anchor 를 노린 이중 타이포스쿼팅), solana-dev-tools, solana-rpc-pool 5 종이다(모두 npm 에서 삭제됨). 이번 캠페인은 봇 토큰을 교체하면서도 동일한 Chat ID(8346336575)와 C2 서버(104.239.66.223:8899), 동일 운영자(@B4ck7p)를 유지했고, 난독화를 제거하는 대신 RAT 명령 체계를 대폭 확장하고 install hook 방식을 버려 lib 삽입 방식으로 통일했다. HMAC 키 버전(sf-v6)도 반복적 개선을 뒷받침한다.

대응 권고 및 결론

- 감염 확인: package.json / package-lock.json 에서 이번 9 종 및 이전 5 종 패키지 사용 여부 확인, 하나라도 있으면 즉시 제거

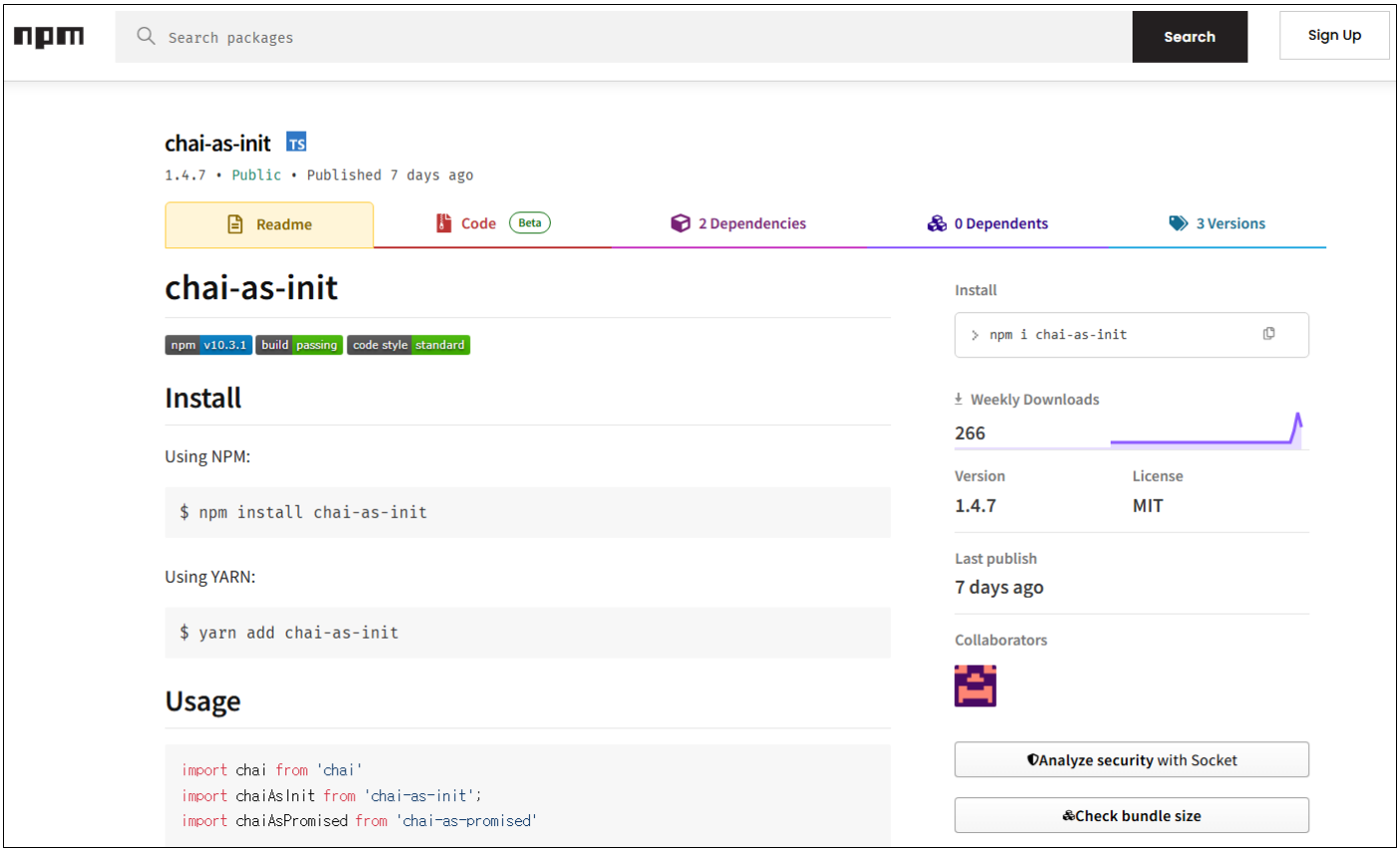
- 감염 시 조치 : 정상 패키지(@solana/web3.js)로 교체, Solana 지갑 키 교체 및 자산 이전, SSH 키 재생성, AWS 자격증명 교체, 환경 변수 비밀값 전면 교체, CLI config.yml 의 RPC URL 복원, Linux crontab 의심 항목 제거, npm/GitHub 토큰 revoke

- 조직 차원 : 전사 npm 의존성 일괄 스캔, 네트워크 로그에서 104.239.66.223 및 api.telegram.org 접속 이력 확인, crontab 에서 csf6·csync·psync 키워드 검색, CI/CD 환경 변수 노출 점검

이번 사례는 신뢰성 키워드를 조합한 9 개 패키지를 동시 배포해 개발자가 어떤 검색어로 찾아도 노출되도록 한 조직적 타이포스쿼팅 공급망 공격이다. 정보 유출에 그친 기존 Telegram C2 악성 패키지와 달리 명령 수신·실행·회신을 갖춘 완전한 양방향 C2 구조라 RAT 로 분류하는 것이 적절하며, 동일 인프라를 유지한 채 페이로드를 계속 발전시켜 온 정황상 추가 캠페인 가능성도 있다. npm 설치 시 반드시 공식 스코프(@solana/) 패키지인지 확인하고 이름이 유사한 비공식 패키지에 주의해야 한다.

4. Chai.js 플러그인으로 위장한 북한발 npm 악성 패키지 'chai-as-init' 분석

이스트시큐리티 대응센터(ESRC)가 유명 테스트 프레임워크 Chai.js 의 플러그인으로 위장한 악성 npm 패키지 chai-as-init 가 v1.4.5~v1.4.7 총 3 개 버전으로 배포된 사실을 확인했다. 이 패키지는 설치 또는 코드에서 불러오는 즉시 외부 서버에서 악성 코드를 내려받아 실행하며, 자격증명을 탈취하는 인포스틸러와 원격 명령을 수행하는 RAT 기능을 함께 갖췄다.



패키지 개요

chai-as-init 은 인기 패키지 chai 및 chai-as-promised 를 모방한 타이포스쿼팅 기법을 썼으나 내부 코드는 전혀 다르다. 공격자는 정상 Node.js 로깅 라이브러리 pino 의 전체 소스·문서·타입 정의를 통째로 복사해 정상 패키지처럼 위장했으며, 총 42 개 파일 중 실제 악성 코드는 index.js 와 lib/initializeCaller.js 단 2 개에만 존재한다. 함수명을 initializeCaller, runBackgroundTask 처럼 일반 초기화 코드처럼 짓고, 탈취 데이터를 cookie·level·timestamp 같은 로그·쿠키 형식 필드명에 담아 정상 데이터로 오인하게 만들었다. README 는 chai 를 설명하지만 실제 코드는 pino 이고, 선언된 버전(1.4.7)과 달리 내부 버전 정보가 pino 의 9.6.0 으로 남아 있는 등 곳곳에 위장 흔적이 확인됐다.

감염 체인

모든 버전이 동일한 초기 실행 구조를 사용한다. 진입점 index.js 는 정상 Express 미들웨어처럼 보이지만, 패키지를 불러오는 순간 백그라운드에서 악성 스크립트를 실행한다. 이때 자식 프로세스를 부모와 분리(detached)하고 출력을 숨기며(stdio: 'ignore'), 부모가 종료돼도 살아남도록(child.unref()) 설정해 추적을 어렵게 한다. 이후 2 단계 로더(initializeCaller.js)가 C2 와 통신해 최종 페이로드를 받아 실행하고, 이 페이로드가 시스템 정보 수집·파일 탐색·데이터 암호화 전송·원격 명령 실행을 수행한다. v1.4.5 는 정적 호스팅에서 페이로드만 내려받는 단방향 구조인 반면, v1.4.6 이후는 환경변수를 먼저 전송하고 응답 본문 전체를 코드로 실행하는 양방향 구조다. v1.4.6/v1.4.7 이 즉시 탈취하는 고위험 환경변수에는 AWS 액세스 키, GITHUB_TOKEN·NPM_TOKEN, DATABASE_URL·REDIS_URL, STRIPE_SECRET_KEY, CI/CD 시크릿 등이 포함된다.

버전별 공격 기법의 진화 (v1.4.5 → v1.4.7)

초기 버전 v1.4.5 는 C2 주소가 평문으로 하드코딩된 단순 단방향 다운로더에 가까웠다(HTTP GET, 환경변수 탈취 없음, C2 호스팅 tiiny.site). v1.4.6 이후부터는 C2 주소를 Base64 로 숨기고 요청 방식을 GET 에서 POST 로 바꾸면서 process.env 전체를 함께 전송하고, C2 응답 본문 전체를 코드로 실행하는 양방향 구조로 변경됐다(인증 헤더 x-secret-header 추가, C2 호스팅 Vercel). 이는 단순 코드 정리가 아니라 질적 도약으로, 환경변수를 먼저 받아 분

석한 뒤 피해자별 맞춤형 페이로드를 내려보내는 구조가 됐다. 특히 정적 호스팅에서 Vercel 서버리스로 인프라를 옮기면서 보안 분석가·샌드박스 접근 시 정상 응답을 돌려주어 탐지를 회피하는 것도 가능해졌다.

v1.4.5 페이로드(data.json) 분석

ESRC는 v1.4.5의 C2에서 최종 페이로드 data.json을 확보해 분석했다. 약 3.8MB JSON 객체로, cookie 필드 안에 난독화된 자바스크립트 전체가 문자열로 담겼으며 cookie라는 이름은 네트워크 모니터링·로그에서 정상 쿠키 데이터로 오인하게 하려는 위장이다(v1.4.5 로더는 이 필드를 Function.constructor로 실행). v1.4.6/v1.4.7은 분석 시점에 C2 동적 응답이 확인되지 않아 실제 페이로드는 파악하지 못했으나, 로더 구조상 v1.4.5와 동일 페이로드를 JSON 래핑 없이 응답 본문으로 직접 반환했을 가능성이 높다.

난독화 해제 후 페이로드는 시스템 정보 수집 → 파일 탐색·명령 실행 → 암호화 후 C2 전송 순으로 동작한다. 시스템 정보는 os 모듈로 호스트명·OS 종류/버전·사용자명을 수집하고 WSL 환경 여부도 자체 함수로 탐지한다. 파일 시스템은 fs.readdirSync()로 특정 4개 디렉터리를 제외한 재귀 탐색, child_process.execSync()로 동기 명령 실행(maxBuffer로 대량 출력 캡처), spawn()으로 비동기 프로세스 생성을 수행한다. 수집·캡처 데이터는 crypto 모듈로 암호화한 뒤 JSON으로 구성해 axios.post로 공격자 서버(144.172.89.180:8086/upload)에 전송한다.

```
{
  ukey: 304,                          // 캠페인/피해자 식별 키
  t: 3,                               // 데이터 타입 코드
  host: '304_<hostname>',             // 식별키_호스트명
  os: '<os.type> <os.release>',       // OS 정보
  username: '<username>',             // 사용자명
  message: '<상태 메시지>',           // 작업 상태/설명
  level: '<데이터 유형>',             // 전송 데이터 분류 (시스템 정보/파일 목록/명령 결과 등)
  data: '<암호화된 데이터>',          // crypto 모듈로 암호화된 실제 탈취 데이터
  timestamp: '<시간>'                 // 전송 시각
}
```

위협 귀속: 북한 Contagious Interview 캠페인

이전에 보고된 다수의 chai-as-* 패키지가 북한 연계 'Contagious Interview' 캠페인의 일환으로 확인된 바 있으며, 이번 chai-as-init도 기존 패키지들과 공격 기법(TTP) 및 인프라 구성 패턴 양면에서 일치했다. 구체적으로 Base64로 C2 주소를 인코딩하고 process.env 전체를 유출하며 new Function()으로 원격 코드를 실행하는 방식, 인기 패키지 타이포스쿼팅과 Vercel 서버리스 C2 활용 등이 기존 캠페인과 일치한다. 또 ipcheck-hashed.vercel.app 도메인 패턴과 ipcheck 키워드, /api/auth/ 형태 API 경로는 기존 북한 OtterCookie 인프라 패턴과도 부합한다. ESRC는 이를 Contagious Interview 캠페인의 연장선으로 판단하고 추가 연관성 분석을 진행 중이다.

참고로 Contagious Interview 는 북한 연계 위협 그룹이 IT 개발자를 표적으로 가짜 채용·면접이나 정상 라이브러리 위장 악성 패키지를 통해 침투하는 대규모 공급망 공격 캠페인으로, npm·PyPI 등에서 1,700 개 이상의 악성 패키지가 보고됐다. 대표 악성코드로 BeaverTail(정보 탈취), InvisibleFerret(백도어), OtterCookie(인포스틸러·RAT) 등이 있다.

기법	chai-as-init	Contagious Interview TTP
Base64 C2 URL 인코딩	O (v1.4.6/v1.4.7)	O
process.env 전체 유출	O (v1.4.6/v1.4.7)	O
new Function(require, code) RCE	O (모든 버전)	O
axios HTTP 클라이언트 C2 통신	O (모든 버전)	O
분리된 자식 프로세스 생성	O (모든 버전)	O
Vercel C2 호스팅	O (v1.4.6/v1.4.7)	O
정적 호스팅 페이로드 배포	O (v1.4.5, tiiny.site)	O
인기 패키지 타이포스쿼팅	O (모든 버전)	O

대응 권고

해당 패키지가 설치된 환경은 모든 비밀 값이 침해된 것으로 간주하고 즉시 대응해야 한다.

- 감염 시 조치 : 로드된 환경의 시크릿·API 키·토큰·비밀번호 전면 교체, chai-as-init 제거 및 모든 프로젝트 package-lock.json 에서 chai-as-* 패키지 존재 여부 확인, CI/CD 빌드 로그에서 설치 흔적 확인, 방화벽·프록시 로그에서 ipcheck-hashed.vercel.app 및 144.172.89.180 연결 이력 확인·차단, 영향받은 시스템 전반 정밀 조사 (원격 코드 실행 단계에서 추가 악성코드 배포 가능성)

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616
(주)이스트시큐리티
www.estsecurity.com