

AI 개발도구 위장 악성코드 감염 헌팅가이드



안내 사항

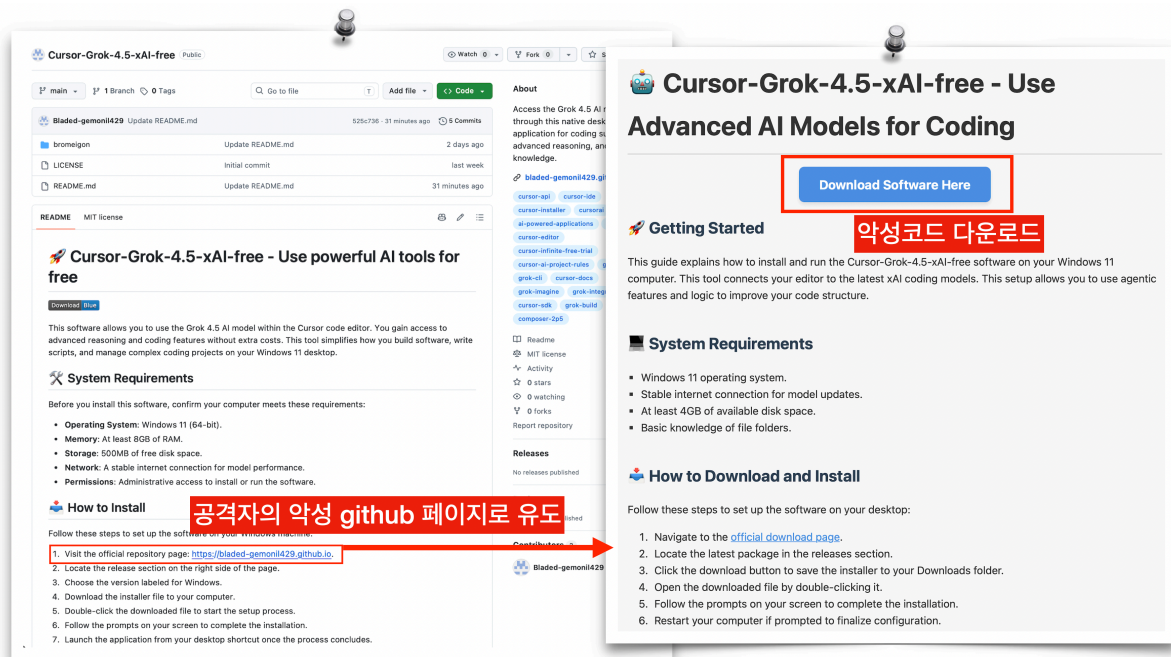
- 본 헌팅가이드(보고서)는 국내에 발생하고 있는 유사 침해사고의 피해 확산 방지를 목적으로 작성되었습니다. 모든 소유권은 한국인터넷진흥원(KISA)에 있습니다.
 - ※ 정보통신망법 제48조의4 제2항(침해사고의 원인분석 및 피해확산 방지 등)
- 또한, 본 가이드를 ▲유관기관에 제공/재배포, ▲온라인 공개/게재, ▲보안제품 활용 등에 있어 발생하는 모든 법적 책임은 귀기관에 있습니다.
- 기타 문의 및 신고는 아래를 참고하여 주시기 바랍니다.
 - 기업 침해사고 신고 : <https://boho.or.kr> (KISA 보호나라)

작성자: 한국인터넷진흥원 위협분석단 AI종합분석팀

작성일: @July 16, 2026

1. 개요

((KST)'26.7.14. 22:02:08~) Gemini, Claude Code, Codex, Grok CLI 등 **AI 개발도구 및 보조도구를 사칭한 악성 유포 사례 49건**이 GitHub 저장소와 GitHub 페이지를 통해 일괄 유포되었다. 공격자는 정상 프로젝트처럼 보이는 README와 랜딩 페이지를 구성하고, 사용자가 정상 도구로 오인해 ZIP 파일을 다운로드 및 악성코드를 실행 유도한다.



실제 악성코드 유포종인 깃허브 저장소 및 페이지

공격자는 처음부터 악성 파일을 노출하지 않고, 정상 도구처럼 보이는 저장소와 소개 페이지를 미리 만들어 둔 뒤 실제 유포 시점에 맞춰 49종 저장소의 다운로드 링크를 악성 ZIP 경로로 전환했다. 이 때문에 저장소 생성 시점만으로는 악성 여부를 식별하기 어렵다.

국내에는 현재 AI 서비스와 보조도구 활용이 활발한 만큼 정상 도구로 오인한 다운로드·실행에 따른 피해가 우려된다.

2. 위장 AI 도구 49종

공격자는 AI 개발자와 일반 사용자가 실제로 검색할 법한 도구명을 선별하여 위장하고 있으며, 확인된 위장 대상 49종은 다음과 같다.

유포시점(KST)	위장 소프트웨어	GitHub 저장소	위장 유형
2026-07-14 22:02:08	opendw	Carmelyeasty591/opendw	AI agent 모델
2026-07-14 22:05:02	morfeus	Screedrounddance602/morfeus	AI agent control plane
2026-07-14 22:09:16	Cursor-Grok-4.5-xAI-free	Bladed-gemonil429/Cursor-Grok-4.5-xAI-free	AI 코딩 보조도구
2026-07-14 22:09:40	DeepSeek-V4-Flash-DSpark-Abliterated-Uncensored-1M-57toks	naysayingyellowman141/DeepSeek-V4-Flash-DSpark-Abliterated-Uncensored-1M-57toks	LLM 모델
2026-07-14 22:10:00	google-gemini-desktop-app	hale-motorcontrol419/google-gemini-desktop-app	Gemini 데스크톱 앱
2026-07-14 22:11:43	commerce-catalyst-sdk-v2026	HrishiISP/commerce-catalyst-sdk-v2026	AI SDK
2026-07-14 22:13:38	stitch-skills	jairo19993062/stitch-skills	AI agent skill
2026-07-14 22:19:42	vpngrok	unclogged-whiteroom239/vpngrok	Grok CLI
2026-07-14 22:20:44	baidu-unlimited-ocr-local-server	hengmei5074/baidu-unlimited-ocr-local-server	AI OCR 서버
2026-07-14 22:25:38	claude-lens-v2026-hub	krystynaacrid635/claude-lens-v2026-hub	Claude Code 모니터링
2026-07-14 22:27:25	Three.js-Object-Sculptor-Codex-Plugin	Melted-genusagathis664/Three.js-Object-Sculptor-Codex-Plugin	Codex 플러그인
2026-07-14 22:27:34	doc-scraper-rs	I7213798/doc-scraper-rs	LLM 문서 수집 도구
2026-07-14 22:33:35	lingbot-video	Workingmanhediondilla304/lingbot-video	AI 영상 도구
2026-07-14 22:35:27	laurel.dev	Commoncarlinethistleloinooflamb461/laurel.dev	LLM agent API

유포시점(KST)	위장 소프트웨어	GitHub 저장소	위장 유형
2026-07-14 22:39:29	clawk	U90364321/clawk	coding agent VM
2026-07-14 22:42:47	NebuShell	Farhaja4948/NebuShell	AI SSH 클라이언트
2026-07-14 22:42:49	Stable-Diffusion-2026-Free-Local	afifsha4142/Stable-Diffusion-2026-Free-Local	Stable Diffusion 로컬 실행
2026-07-14 22:45:06	gpt-5.6-instruct	Kastradbe9589/gpt-5.6-instruct	LLM 모델/CLI 도구
2026-07-14 22:47:32	claude-skill-router	Jerkinesspotfarm223/claude-skill-router	Claude Code skill 라우터
2026-07-14 22:48:29	ai-job-search	Ergi8957/ai-job-search	AI 취업 도구
2026-07-14 22:51:54	RoboDojo	spartan-nitrogenase831/RoboDojo	AI 로봇틱스 도구
2026-07-14 22:53:01	subjective-zero	Marve6988/subjective-zero	prompt 기반 creative coding
2026-07-14 22:55:18	claude-voice	Mariskak2332/claude-voice	Claude CLI 음성 인터페이스
2026-07-14 22:56:35	sm120-field-guide	fecal-peeler359/sm120-field-guide	AI 워크로드 디버그
2026-07-14 23:01:23	jspace	Swimwearcounterfactuality157/jspace	AI 개발도구
2026-07-14 23:04:16	claudefreemodel	mensal-familyhemiramphidae391/claudefreemodel	Claude 모델 도구
2026-07-14 23:08:34	vox-director	craftsman europeansanicle437/vox-director	AI 음성/영상 도구
2026-07-15 01:09:02	AI-Resume-Analyzer	kalinaredviolet389/AI-Resume-Analyzer	AI 이력서 분석
2026-07-15 01:09:09	Hy3-295B-NVFP4-2x-DGX-Spark	Mecopteragenusmeles123/Hy3-295B-NVFP4-2x-DGX-Spark	LLM 모델
2026-07-15 01:09:09	lingbot-vla-v2	aashmadhungana2005-jpg/lingbot-vla-v2	VLA 모델
2026-07-15 01:12:33	ai-chat-website	Rebeccamari333/ai-chat-website	AI 챗 웹앱
2026-07-15 01:15:07	Nocturne	clusterpinealgland805/Nocturne	AI 개발도구
2026-07-15 01:16:34	edgerag	Northexp3076/edgerag	RAG 도구
2026-07-15 01:22:30	openwebui-generate-documents	Amphoraminingengineer230/openwebui-generate-documents	Open WebUI 확장도구

유포시점(KST)	위장 소프트웨어	GitHub 저장소	위장 유형
2026-07-15 01:30:34	jlens-qwen36	broddiestretch86/jlens-qwen36	Qwen 모델 도구
2026-07-15 01:30:53	TencentDB-Agent-Memory	mohamamd991/TencentDB-Agent-Memory	AI agent memory
2026-07-15 01:31:21	ai-investment-portfolio-analyzer	tanpresent809/ai-investment-portfolio-analyzer	AI 금융 분석
2026-07-15 01:40:44	awesome_pets	tammyjust719/awesome_pets	AI 앱
2026-07-15 01:41:00	blockout	discomyceteteaparl857/blockout	AI 앱
2026-07-15 01:44:42	chatologist	julianaantic4587/chatologist	AI 챗 도구
2026-07-15 01:51:20	charsheet	Zanetavesicant971/charsheet	AI 캐릭터 도구
2026-07-15 01:51:43	GPT-5.6-Sol-Free-Desktop-App	jagadamba5905/GPT-5.6-Sol-Free-Desktop-App	GPT 데스크톱 앱
2026-07-15 01:55:06	lapian-notes	Deertickpyrrhocoridae427/lapian-notes	AI 노트 도구
2026-07-15 01:56:30	a6b-k-expansion	Imcqu3499/a6b-k-expansion	AI 모델 확장 도구
2026-07-15 01:56:35	fable-5-free-desktop-app	placepacificgiantsalamander20/fable-5-free-desktop-app	AI 데스크톱 앱
2026-07-15 01:58:37	designsight-data-backed-2026	larrystricken940/designsight-data-backed-2026	AI 디자인 도구
2026-07-15 02:05:02	Homekit	Algonkian-seafaring733/Homekit	AI 홈 도구
2026-07-15 02:11:28	Cli-launcher	edwinvar9791/Cli-launcher	AI CLI 런처
2026-07-15 02:59:51	chewy	AyushThapak/chewy	AI 앱

3. 유포 및 감염 방식

1. [공격자] 정상 AI 도구처럼 보이는 GitHub 저장소와 소개 페이지를 미리 생성
↓
2. [유포 시작] 특정 시점에 다운로드 버튼을 악성 ZIP 링크로 변경
↓
3. [피해자] GitHub 검색, 검색엔진 결과, SNS·커뮤니티 공유 링크 등을 통해 저장소 접속
↓
4. [다운로드] 정상 프로그램으로 오인하여 ZIP 파일을 내려받고 실행
↓
5. [감염 시작] 압축 파일 안의 실행 파일이 숨겨진 악성 스크립트를 불러옴

- ↓
6. [서버 연결] 공격자 서버 주소를 확인한 뒤 외부 서버와 통신
- ↓
7. [추가 감염] 후속 악성 파일을 내려받아 추가 기능 실행
- ↓
8. [최종 행위] 시스템 정보 수집, 추가 명령 실행, 재부팅 후에도 동작하도록 설정

- 공격자는 저장소명, 설명, README, Pages 랜딩을 정상 프로젝트처럼 구성하여 육안 식별을 어렵게 만든다.
- 다운로드페이지에서 유포중인 ZIP의 파일명과 hash는 달라지지만, 내부 악성코드(`Application.cmd` , `certificate.txt` , `utility.exe`)는 동일하다.

대표 사례인 `Bladed-gemonil429/Cursor-Grok-4.5-xAI-free` 의 공격 타임라인은 아래와 같다.

KST	저장소	변화
2026-07-10 03:24:47	<code>Bladed-gemonil429/Cursor-Grok-4.5-xAI-free</code>	메인 저장소 최초 생성
2026-07-12 20:33:14~21:46:40	<code>Bladed-gemonil429/bladed-gemonil429.github.io</code>	GitHub Pages 소개 화면 및 리소스 사전 준비
2026-07-14 19:32:43	<code>Bladed-gemonil429/bladed-gemonil429.github.io</code>	<code>index.html</code> , <code>photo.png</code> , ZIP 추가
2026-07-14 19:32:58	<code>Bladed-gemonil429/Cursor-Grok-4.5-xAI-free</code>	메인 저장소에 ZIP 추가
2026-07-14 22:09:15	<code>Bladed-gemonil429/bladed-gemonil429.github.io</code>	소개 페이지 다운로드 링크를 악성 ZIP으로 변경
2026-07-14 22:09:18	<code>Bladed-gemonil429/Cursor-Grok-4.5-xAI-free</code>	README 다운로드 링크를 GitHub Pages로 변경

4. 감염 징후 및 헌팅 방법

4.1 단말기(Endpoint) 확인

점검 항목	확인 방법
초기 ZIP 내부 조합	다운로드 ZIP 또는 사용자 다운로드 경로에 서 <code>Application.cmd</code> , <code>certificate.txt</code> , <code>utility.exe</code> 3종 동시 존재 여부 확인
초기 실행 체인	<code>cmd.exe</code> 하위에서 <code>utility.exe</code> 가 실행되는 체인 확인
2차 로더 실행	<code>luau.exe dist.lua</code> 실행 여부 확인
후속 실행 파일	<code>%LOCALAPPDATA%\Programs\Chromium\Chromium.exe</code> 생성 및 <code>Chromium.exe</code> "NTE3YjdjNWU1NjYzNjU2YTA1N2Y=" 인자 실행 여부 확인
지속성	<code>C:\Windows\Setup\Scripts\ErrorHandler.cmd</code> 존재 여부 및 <code>OneDriveStandaloneUpdater_7d7752</code> 스케줄러 생성 여부 확인

4.2 네트워크 헌팅

점검 항목	탐지 방법
Polygon 현재 C2 조회	Polygon RPC로의 JSON-RPC 요청 중 HTTP POST 본문에 <code>"method": "eth_call"</code> , contract <code>0x1823A9a0Ec8e0C25dD957D0841e3D41a4474bAdc</code> , selector <code>0x3bc5de30</code> 조합이

점검 항목	탐지 방법
	함께 포함되는지 확인
고정 C2 요청 경로	<code>/api/NTE3YjdjNWU1NjYzNjU2YTA1N2Y=</code> 및 <code>/task/NTE3YjdjNWU1NjYzNjU2YTA1N2Y=</code> 요청 여부 확인
GitHub second-stage	<code>raw[.]githubusercontent[.]com/joao8989/otp/refs/heads/main/80.log</code> , <code>443.log</code> 요청 여부 확인
현재 C2 주소	<code>83[.]97[.]20[.]150</code> 연결 여부 확인 (2026-07-16 08:31 KST 기준)
후속 POST	<code>144[.]31[.]57[.]94/c0e070fa9435429c8ea5.php</code> 요청 여부 확인

5. 위협 평가

5.1 심각성

- **(공격 대상의 특수성)** AI 개발도구와 보조도구는 개발자, 보안분석가, 기술 사용자들이 직접 다운로드·실행할 가능성이 높아 단말 권한과 개발 환경 노출 위험이 큼
- **(대량 활성화)** 2026-07-14 KST 기준 최소 49개는 AI/LLM/agent 도구를 직접 사칭
- **(탐지 우회)** 유포 ZIP파일 해시는 계속 바뀌지만 내부 로더 파일은 동일하여, 단순 해시 차단보다 실제 동작하는 악성코드의 행위 및 네트워크 조합 탐지가 필요
- **(C2 차단의 어려움)** 악성코드에 설정된 C2가 차단돼도 폴리곤 컨트랙트(Polygon contract)를 이용해 C2를 재조회하므로 단일 IP 차단만으로는 대응이 어려움

5.2 탐지 지표 (IOC)

- 파일 IOC

파일	SHA-256
<code>Application.cmd</code>	<code>24cdfb100ad9f06798f0c21f5912a98f0c954ffb3477adae9cf86e8521b999f2</code>
<code>certificate.txt</code>	<code>52188dbdebfc8c224ccaac16626b048004ad3447b06ce21d3880fa248cb6db70</code>
<code>utility.exe</code>	<code>e227d47facf0e2f5b9e5c54a23a86b31272696b64bbb9932a31fe06973677bd</code>
<code>80.log</code>	<code>e200c7cabdc778845cce27bdf1a917d7f7bda394b6d5a8f21ebe8f536c248f84</code>
<code>dist.lua</code>	<code>54e1a69f1921fbf1942f59cabd44a8206f9bcad89a3de7434e81120adf2ce8</code>
<code>443.log</code>	<code>14bde4b6a8bcdce7234ce6edf4acd203b9ab0f58a4117e4e99c4758ce041fa8a</code>
<code>443.log</code> 디코딩 PE	<code>e17040d9f2841d2523d759a6e81e77bd7cd180125b960fccaa7291cc008b56df</code>

- AI 위장 49종 유포 ZIP

49종 유포 ZIP은 서로 다른 SHA-256을 사용하지만, 내부에는 위 공통 파일 `Application.cmd` , `certificate.txt` , `utility.exe` 가 동일하게 포함되어 있다.

#	SHA-256
1	<code>7165285109f90fe06d8b388c7319b68956c695393843bcea41836cd9539806cd</code>
2	<code>c93f09133d39dd3454dfa682e0277674e32a44a1e383b14d5e0f4e2d8f97a2e2</code>
3	<code>2391d46a8c2ff15d9e0662266b510a541dde58a901ccdf4f5a8b182a064067</code>

#	SHA-256
4	8f7a730f2e1798e2413e420887e30693496d15c4414a9d59c5f6e38e7b88c33f
5	56f0030b3d1d01eaf2aab8a959e5b14cbcba18c549a81303b4f9a4c06a88532b
6	09de877a6a65eff4ebbf06753872d56217a6ae6bd5d7b5fb1209adb6c2d57ee7
7	ab94bf77f9bad202adb0ac25aa32240946f1ed5365edcd25a6e2f65236f78865
8	d2b079d705fd76b7cb4157d7619c38bde8dfcb1f100bcb77bdf8d6037eb7a5d3
9	374afe05450c8cafd685b61e412df2af0c044821e2750278e9ea987d2d97dea9
10	991ffce7918435a9647068b646957f34cdc0269710e7c84fee4d3062e9f75c3
11	ca25e970ebe373ecc88a15d997e16651b25beda7b9d074cc02850166b24db2ec
12	90208db8e1836aa3bf46d1c5db78ef5c96dd119580fc7cf4370f44f30667ad2a
13	8b09b094fb2c8549f1e083a981f150c6e2c89f9b05742dcf24fa5f16335bb42d
14	a792e152da60c6ef878226413776b9e2303f537af55932996ea267c3721144d2
15	0dfad8abcafd1c878903a2da6f299d916f87957458ea06271a18b9e2285d36c3
16	8f1c87350e8f907ab77cfc4ef28e0419611e50e3fc68ae3f886637927a1d00cd
17	09449cccab5e2b808460bd0cac3b0767a34edcea9a0181c48c68244260c863da
18	f58811706171b9fddc65d72ea7381bea298457b1d043870f088e7b90e7849299
19	dedd4c6c8f94a7bdc2e9a91aa434c8a03be54764190389ddaa9cf42f16241994
20	fe1e3ff3201521dd2863e62ab312b5dc720458fbc4e93695f80fd80645f29714
21	f817d6fefa0fa806f91307824ea2bfd2adadc3d22d11d91b605923a846e616bb
22	049abe9b19ec1aae891d340e5528e58a43f07b49e5bd448f97eb359fb101135a
23	d1b559bf2d8596e4837703ce92afc79c325dff1509c41f624fffc516ce8c88dd
24	a8c4ff71ab75c0f03dcd5ad2611ffc7d4a3afefd7a4de3efd2b84d4cd63cac1d
25	7d0e82101b5b18ba6f0ffb764ac73c223de92643710a243ba93e30d673cfeb38
26	d9ea21f1c464c5263455103a6df05c3d2b163b946b1202231c19b43b0e271a79
27	fbcb5e52a96b456ce431cd9fc31ca9a12e068d8468ffce2829b505d9527cd349
28	b2c87dfad4470a6a6da5211cb34516d5a5ae80db0d1a564156ad26f11fe4f1a0
29	1475c24bdc7a99a2cd7e2bb993d7f094abaf4328f6777a3348979336d112c6bd
30	b5859b7e347146f503d8dad27ce99112a3f1bcd137c70bad186caa28ab05206c
31	4997147bd01e785d018fbb982a45f7dccfa70d43dc7f46908519aa41bf460381
32	947583716be058fa515f423c539885e7ba38c97351a13985e27338db32342cac
33	8d72ebe9a0dbdec37685aa02abda977e69d948662bbf8040191f07a491b87f0b
34	cf38ea7285a84691003694495b05cd892464114487408cbbe6a5514cd29ab463
35	a9de206678821d1d296a39b577d3febd787a772828487323105ef89362096a95
36	7c73e4a74e1388b0e3e6941fee4f6bfcdb32a8a380536ee9187e069099fa1c40
37	c5c3dd7efb5d486092a705fcbeae86b24712be5ac8ed6626351fbec5d87e4f8e
38	d376f5c2119e9499ceea4955cfd265c7198500d4beaa69574fbe2e9fb56fd35d
39	4c7c2c0a4c779bdb89f0055b3b298dad84ffcdc0fc3a8e9f09da379fba1ce9e3

#	SHA-256
40	6f5499fc2bcdcf86302a594ddec6c7c1d9b67d100cd762ef18daf99d7de72cc
41	b130c8815218b1d265feafa5f3c923df72a1938d0a6eebfaaf4afc29ff001164
42	1defbe31306d0bafbd60f907fe3e0088ba1641597f2ca202042a8b31e003f69b
43	c60a68df6f1757ae026a6e55e0294948365b02403cbdc9d5d3be141ea993fe48
44	3af2a4c7fca829dd66756787f8a67c909b20cc77200c94d5ffc78cf92ae57d19
45	0bab79905f8f9a27daa727417388f5a6eb44b366774085f390c9392cb85e5618
46	504ec31ca1bcdcfb8163704879361839234fd163bff238c885a53344854c4762c
47	adfc8c16082b94adbd76ecd78c927effb88ca2d68cc4763d7a3f7a5b147ca517
48	434adee1abb3ac72af197d0d7c6a3c96530e1aecb31cb1bd278c12baa8357562
49	b62717a505480a34927ebfc19b03aa04ee21c9432d70bad1cd7f2d849cafd7ab

• 네트워크 IOC

유형	값
initial bootstrap C2	213[.]176[.]72[.]221
second-stage bootstrap C2	2[.]27[.]14[.]165
current on-chain C2	83[.]97[.]20[.]150
follow-on POST	144[.]31[.]57[.]94/c0e070fa9435429c8ea5.php
API path	/api/NTE3YjdjNWU1NjYzNjU2YTA1N2Y=
task path	/task/NTE3YjdjNWU1NjYzNjU2YTA1N2Y=
second-stage URL	raw[.]githubusercontent[.]com/joao8989/otp/refs/heads/main/80.log
second-stage URL	raw[.]githubusercontent[.]com/joao8989/otp/refs/heads/main/443.log

• Polygon(contract : 0x1823A9a0Ec8e0C25dD957D0841e3D41a4474bAdc) C2 이력

최초 반영 UTC	C2
2025-11-16 11:37:19	93[.]123[.]39[.]74
2025-12-27 21:28:31	151[.]243[.]113[.]70
2026-01-01 17:17:43	144[.]31[.]219[.]15
2026-01-26 07:11:28	213[.]176[.]72[.]204
2026-02-08 20:22:31	89[.]169[.]12[.]160
2026-04-05 11:07:17	144[.]31[.]57[.]65
2026-04-22 13:39:02	89[.]169[.]12[.]149
2026-05-03 15:48:58	89[.]169[.]12[.]140
2026-05-14 08:55:52	144[.]31[.]57[.]67
2026-06-04 13:44:03	213[.]176[.]73[.]139
2026-06-04 22:00:34	85[.]137[.]52[.]21
2026-06-21 07:01:41	185[.]10[.]68[.]98
2026-07-13 18:59:01	83[.]97[.]20[.]150

6. 권고 사항

1. **(공식 배포처 이용)** AI 보조도구, Claude/Codex/Gemini/Grok 관련 도구는 공식 프로젝트 페이지와 공식 배포처만 이용
2. **(GitHub 저장소 검증)** Star 수, 기여자 이력, 계정 생성 시점 등을 확인
3. **(IoC 즉시 점검)** 위 해시, 도메인, 레지스트리 경로에 대한 즉시 스캔