

2026년 1분기 DPRK Operation Kimsuky 분석

 logpresso.com/ko/blog/2026-05-15-1Q-Kimsuky-report

2026년 1분기 DPRK Operation Kimsuky 분석



1. 개요

2026년 상반기에 Kimsuky 공격 그룹이 수행한 스피어피싱 캠페인 중 위장 주제, 초기 침투 벡터, C2 인프라가 구분되는 4건을 분석합니다. 캠페인은 각각 기업 채용 담당자, 암호화폐 투자자, 개발자, 국방 분야 관계자, 대학원 위탁교육 관계자 등을 표적으로 삼았습니다.

본 보고서는 각 캠페인의 초기 침투 경로, 페이로드 동작 방식, C2 인프라, 지속성 확보 기법을 분석하고 탐지·대응에 활용 가능한 IOC와 탐지 포인트를 정리합니다.

분석 대상 네 캠페인은 공통적으로 **미끼 문서 표시 → 페이로드 드롭 → 지속성 확보 → C2 통신 및 원격 제어**의 흐름을 따릅니다. 다만 위장 주제, 초기 실행 벡터(LNK/JSE), C2 인프라(자체 서버·GitHub·VSCode 터널), 타깃 식별 방식(uid/IP/MAC)이 캠페인마다 차별화 되었습니다. 최근에는 정상 서비스(GitHub raw, Microsoft CDN, VSCode 터널)를 C2 채널로 악용하는 경향이 두드러졌으며, 이는 명백히 평판 기반 차단을 우회하기 위한 의도로 판단됩니다.

Kimsuky 스피어피싱 4대 캠페인 공격 흐름 (2026 상반기)



캠페인 비교

구분	Campaign #1	Campaign #2	Campaign #3	Campaign #4
위장 주제	이력서·명함·의료/보험 서류	Pump.fun (Solana 밈코인) 기술 문서	K-ICTC 국제과학화전투경영대회	국내대학원 석사야간과정 위탁교육
주요 타겟	채용 담당자, 거래처, 의료·보험 기관	암호화폐 트레이더·개발자·투자자	육군본부·합참·국방부, 주한 외국 무관부	공공기관·대기업 직원, 대학원 행정 담당자
초기 벡터	LNK (PDF 위장)	LNK (PDF 위장)	LNK (PDF 위장)	JSE (HWPX 위장)
주요 페이로드	PowerShell RAT (a.ps1)	PowerShell Infostealer (bpvme.ps1)	VBE → PowerShell 파일리스	DLL 정찰 모듈 / VSCode CLI
C2 채널	자체 서버 (nelark.icu)	GitHub 저장소 (정상 서비스 악용)	자체 IP (103.67.196.25)	정상 서버 (yespp.co.kr) + GitHub OAuth

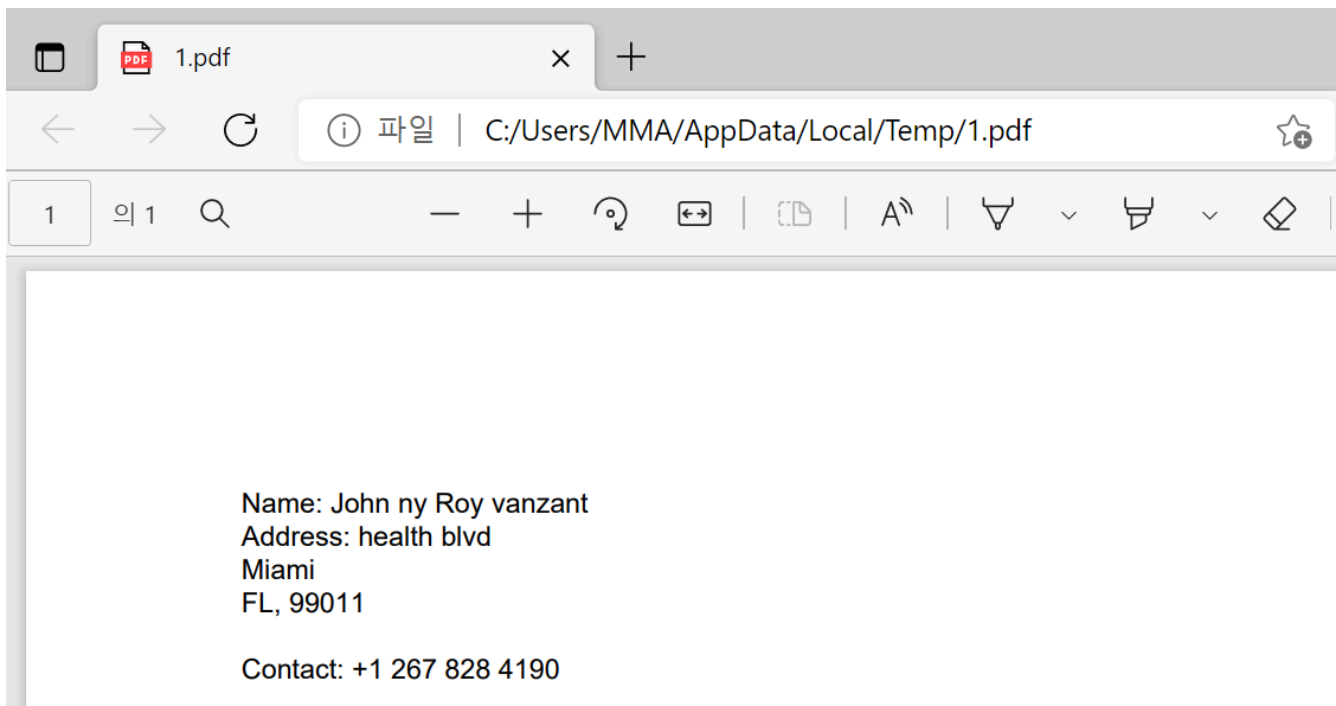
구분	Campaign #1	Campaign #2	Campaign #3	Campaign #4
지속 성 기 법	Startup 폴더 LNK + 작업 스케줄러 (5분 주기)	작업 스케줄러 (OneDrive 위장, 60분 주기)	작업 스케줄러 (15분 주기)	VSCode 터널 (지 속 원격 접속)
방어 우회	UAC 비활성화, Defender 예외 등 특	자가 삭제, 수집 파 일 삭제	다중 난독화 (동물명 변수)	정상 MS CDN 활 용
타겟 식별	uid 기반 폴링	IP-시간 기반 파일 명	MAC 주소 기반 맞춤 페이로드	정찰 정보 일괄 수 집

2. 캠페인 분석

Campaign #1 — 이력서·의료 보험 서류·명함으로 위장한 스피어피싱

한 줄 요약

PDF로 위장한 LNK 파일이 미끼 문서를 띄우는 동시에 PowerShell RAT를 설치하고, 5초 간격으로 자체 C2(nelark.icu)에서 명령을 폴링·실행하는 캠페인입니다.



미끼와 타깃

미끼 파일은 단일 LNK 파일로 구성되어 있으며, 미끼 문서는 아래 세 가지 형태로 스피어피싱에 활용되고 있습니다.

- 이력서·지원서 — 이력서처럼 헤더에 이름과 연락처를 기재하여, 채용 담당자를 대상으로 한 스피어피싱에 활용합니다
- 명함 정보 — 거래처나 고객 정보로 위장한 스피어피싱에 활용합니다
- 의료·보험 서류 — 헤더에 기재된 "health blvd"를 오인하게 하여, 의료·보험 기관 종사자를 타깃으로 한 스피어피싱에 활용합니다

공격 흐름

사용자가 1.pdf.lnk를 실행하면 LNK 내부에 은닉된 두 개의 페이로드가 분리됩니다. 20KB 이후 영역에 위치한 미끼 PDF는 %TEMP%\1.pdf로 추출되어 즉시 정상 문서처럼 사용자에게 표시되고, 10~20KB 사이의 LNK 페이로드는 시작 프로그램 폴더의 OneDrive.lnk로 저장되어 재부팅 후에도 C2 서버와 통신하여 스크립트를 다운로드 받고, 실행할 수 있는 지속성을 확보합니다.

곧이어 C2 서버 nelark.icu/xftaswx/res/bb.php에서 스크립트를 다운로드하고 실행합니다. 이 스크립트는 UAC 우회용 배치 파일(1.bat)을 다운로드 및 실행하여 UAC를 비활성화하고, Windows Defender 예외에 자신의 경로를 등록한 뒤, 작업 스케줄러에 RAT 본체(a.ps1)를 등록합니다. 이 일련의 작업은 초기 침투 5분 이내에 모두 완료됩니다.

여기서 등록되는 스케줄러 작업은 단순한 "RAT 재실행" 이상의 의미를 가집니다. 작업명은 Intel(R) Ethernet3 Connection 1219-LM2로 정상 인텔 네트워크 드라이버명을 변형해 위장하며, /ru SYSTEM /rl HIGHEST 옵션으로 **SYSTEM 권한 + 최고 실행 레벨**을 고정 확보합니다. 실행 명령은 Net.WebClient.DownloadString()으로 a.ps1을 메모리에 받아 iex로 즉시 실행하는 파일리스 구조이며, -WindowStyle Hidden으로 콘솔 창도 띄우지 않습니다. 결과적으로 이 한 줄의 스케줄러 등록만으로 ****지속성(5분 마다 부활) + 권한 상승(SYSTEM 고정) + 파일리스 실행(디스크 흔적 제거) + 위장(정상 드라이버명) + 은닉(콘솔 숨김)****의 다섯가지 공격 행위가 동시에 달성됩니다. 이렇게 등록된 스케줄러가 부활시키는 a.ps1 본체는 /get-command.php?uid=<uid> 엔드포인트를 5초 간격으로 폴링하면서 공격자가 내려보낸 명령(gCommand)을 실행합니다. **5분 단위 위치독 위에 5초 단위 RAT가 얹힌 이중 구조**가 완성되며, uid는 피해자별로 고유하게 발급되어 공격자가 다수 감염 PC를 식별·관리할 수 있습니다.

오프셋	내용	저장 경로
20KB 이후	미끼용 PDF 파일	%TEMP%\1.pdf
10~20KB	지속성 유지용 LNK 파일	Startup\OneDrive.lnk

이는 LNK 파일 포맷의 구조적 특성을 이용한 기법입니다. Windows LNK 파서는 ExtraData 블록의 TerminalBlock(0x00000000)까지만 읽고 파싱을 종료하므로, 그 뒤에 임의 바이트를 단순 concat 방식으로 붙여도 LNK는 정상적으로 실행됩니다. 공격자는 정상 LNK 구조 뒤에 미끼 PDF와 지속성 유지용 LNK를 이어 붙여둔 뒤, PowerShell 명령으로 원본 LNK를 바이너리로 다시 읽어 지정 오프셋 구간을 추출·저장하는 방식으로 페이로드를 분리합니다. 외부 통신 없이 초기 단계가 완결되므로 1차 네트워크 탐지가 어렵고, 정적 분석도 LNK 본체의 명령어 문자열만 봐서는 페이로드 존재를 알 수 없습니다. 그러나 정상 LNK는 보통 1~3KB이며 아이콘을 포함해도 10KB를 넘는 경우가 드물기 때문에, **10KB 이상의 LNK는 그 자체로 페이로드를 은닉했다고 의심할 수** 있습니다.

단계	행위	설명
1단계	LNK 파일 실행, 지속성 확보	PDF 위장 바로가기 파일 실행 → 미끼문서 표시 + 페이로드 추출 + 지속성 확보
2단계	C2 초기 통신	C2 서버에서 초기 스크립트 다운로드 및 실행
3단계	UAC 우회	1.bat 다운로드 및 실행하여 UAC 비활성화
4단계	작업 스케줄러 등록	Defender 예외 등록 + RAT 본체 스케줄러 등록
5단계	C2 원격 제어	RAT 본체가 실행되어 5초 간격으로 C2 서버에서 명령어 수신 및 실행

C2 통신 시도별 행위 요약

순서	C2 엔드포인트	역할	실행 스크립트
1	/xftaswx/res/bb.php	스크립트 다운로드	UAC 확인 + bpersist PS1
2	/xftaswx/res/post_proc.php? fpath=bpersist.ps1	지속성 확보	bpersist.ps1
3	/xftaswx/res/bypass.b	UAC 우회	%TEMP%\1.bat

순 서	C2 엔드포인트	역할	실행 스크립트
4	/xftaswx/res/index.php	UAC 결과 보 고	POST (uid, msg)
5	/xftaswx/res/post_proc.php? fpath=scheduler-once	스케줄러 등 록	scheduler-once.bat
6	/xftaswx/res/post_proc.php?fpath=a.ps1	메인 RAT 루 프	a.ps1 (gCommand 포함)
7	/xftaswx/res/get-command.php?uid=<uid>	원격 명령 수 신	동적 명령 실행

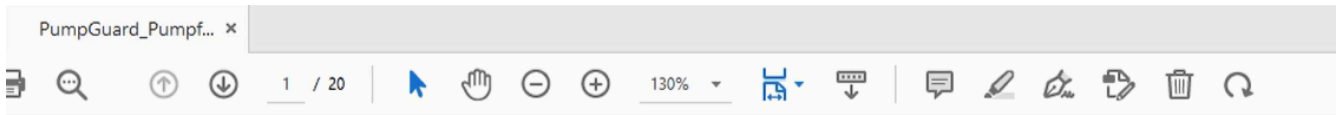
시사점

단일 LNK 파일에 미끼 PDF와 지속성 유지용 LNK를 함께 담아 클릭 한 번으로 두 파일을 드롭하고 실행하는 점이 이 캠페인의 가장 큰 특징입니다. 또한 UAC 비활성화와 Defender 예외 등록을 초기에 일괄 처리해 후속 페이로드의 탐지 가능성을 사전에 차단합니다. uid 기반 폴링 구조는 공격자가 감염 PC를 식별해 선별적으로 명령을 내릴 수 있다는 의미이며, 이는 단발성 정보 탈취가 아니라 장기 침투를 의도한 RAT 운용 패턴입니다.

Campaign #2 — Pump.fun 기술 문서 위장 스피어피싱

한 줄 요약

Solana 기반 밈코인 플랫폼의 "AI 보안 솔루션" 공식 기술 문서로 위장하여 시스템 정보를 탈취하고, 정상 서비스인 GitHub를 C2 채널로 악용하는 캠페인입니다.



PumpGuard

(Pumpfun-AI-Attack-Defence)

미끼와 타겟

미끼 문서는 PumpGuard-Pumpfun-AI-Attack-Defence-Requirements.pdf.lnk로, Solana 기반 밈코인 런치패드 플랫폼인 Pump.fun과 가상의 보안 도구 "PumpGuard"를 결합한 형식입니다. PumpGuard는 실제로 존재하지 않는 가상의 도구이나, 이 문서는 공격/방어 요구사항이 기재된 문서를 흉내내어, 암호화폐 트레이더·개발자·투자자를 표적으로 합니다.

공격 흐름

초기 실행되는 PowerShell 스크립트는 자체 복호화 루틴을 거쳐 firefox.ps1을 %AppData%에 생성합니다. 복호화는 19자리 키(AB59097(*^zxcvbn)와 단순한 산술 연산을 조합한 방식입니다.

```
# i -> 암호 배열 전체 길이
# j -> 키 길이(19)
pw_num = key[j] + 103

# case 1: pw_num >= encrypted[i]
plain[i] = pw_num - encrypted[i]

# case 2: pw_num < encrypted[i]
plain[i] = encrypted[i]
```

firefox.ps1이 실행되면 세 갈래로 동작이 분기됩니다. 첫째, GitHub 저장소 (brandonleeodd93-blip/doc7)의 /main/view.pdf를 Pumpfun-AI-Attack-Defence-Requirements.pdf 이름으로 띄워 사용자 의심을 차단합니다. 둘째, /main/1.txt를 bpvme.ps1로 실행하여 시스템 정보를 수집·유출합니다. 셋째, wale.ps1을 이용해 작업 스케줄러를 등록하는데, 이 스케줄러는 OneDrive 프로세스로 위장하여 60분 주기로 coks.ps1(/main/2.txt)을 반복 실행합니다.

수집된 시스템 정보는 GitHub Repository의 /report/{IP}-{시간}-0956_info.txt 경로로 업로드되며, 모든 단계가 종료되면 최초 스크립트, firefox.ps1, bpvme.ps1, 수집한 정보를 자가 삭제하여 흔적이 최소화됩니다.

bpvme.ps1(Infostealer) 수집 정보

수집 정보	사용 명령
IP 주소	Win32_NetworkAdapterConfiguration
OS 정보	Win32_OperatingSystem
시스템 정보	Win32_ComputerSystem
마지막 부팅 시간	LastBootUpTime
기기 유형 (노트북/데스크탑)	PCSystemType
안티바이러스 제품명	root\SecurityCenter2
실행 중인 프로세스 목록	Get-Process

공격자 활용 GitHub 정보

항목	값
GitHub 계정	brandonleeodd93-blip
Repository	doc7
GitHub PAT	ghp_4tisPi18exkn0T8jQlKHsVLsZYhF3C0iW0Hp
페이로드 경로	/main/1.txt, /main/2.txt, /main/view.pdf
수집 정보 경로	/report/{IP}-{시간}-0956_info.txt

시사점

C2 채널로 GitHub를 사용한 점이 이 캠페인의 핵심입니다. raw.githubusercontent.com은 대부분의 도메인 평판 시스템에서 정상으로 분류되어 차단·경고 대상에서 제외되며, 외부 트래픽 모니터링에서도 개발 활동과 구분하기 어렵습니다. OneDrive 위장 스케줄러와 자가 삭제 루틴은 감염 이후 흔적을 최소화하려는 의도가 명확합니다.

Campaign #3 — K-ICTC 군사대회 문서 위장 스피어피싱

한 줄 요약

국제과학화전투경영대회(K-ICTC) 안내 문서로 위장한 LNK를 통해 VBE → PowerShell 파일리스 실행으로 진입하며, MAC 주소 기반으로 피해자별 맞춤 페이로드를 배포하는 캠페인입니다.



Republic of Korea Army

26th March 2026

먼저, 대한민국과의 우호증진과 군사협력을 위해 노력해주시는 각국의 군 관계자들에게 감사드립니다.

대한민국 육군에서는 '26년 제4회 국제과학화전투경연대회를 개최할 예정입니다. 이번 대회는 지난 3회차 대회처럼 다자간 연합전투기량과 상호운용성을 향상시키고 국가간 교류협력을 강화하기 위해 시행합니다.

특히, 이번 K-ICTC에는 마일즈 장비를 활용한 소부대 과학화전투훈련 뿐만 아니라 대한민국 육군의 전력화 무기들도 시연할 계획입니다.

K-ICTC는 참가국 간의 상호 신뢰를 구축하고 연합 파트너십을 한층 더 격상시키는 계기가 될 것입니다. '26년 4월 30일까지 참가 의사(미참가 의사 포함)를 회신해주시면 감사하겠습니다.

- 훈련일정 : '26. 9. 14.(월) ~ 18.(금)
- 훈련장소 : 대한민국 육군 과학화전투훈련장(강원도 인제)
- 참가규모 : 소대급 규모(25명)
 - * 인솔·지원인원 포함 30명 이내 * 참관단(옵저버)도 가능

육군본부 정보작전참모부

교육훈련정책과장 대령 김 부 배



Republic of Korea Army

26th March 2026

First, I would like to express my sincere appreciation to all military representatives for your continued efforts in promoting friendship and military cooperation with the Republic of Korea.

The ROK Army is planning to host the **4th Korea-International Combat Training Competition(K-ICTC)** in 2026. As in the previous competition, this event is designed to enhance multinational combined combat capabilities and interoperability, while strengthening exchanges and cooperation among participating nations.

In particular, this year's K-ICTC will feature not only small-unit scientific combat training utilizing MILES equipment, but also demonstration of operational weapon systems of the ROK Army. The K-ICTC will serve as a meaningful opportunity to build mutual trust among participating nations and to further advance combined partnerships.

We would appreciate it if you could kindly confirm your participation, including non-participation, **by April 30, 2026.**

- Training Period : September 14(Mon) ~ 18(Fri), 2026
- Location : Korea Combat Training Center, ROKA (Inje-gun, Gangwon Province)
- Participation : 1 platoon level (25x Pax)
 - * Maximum of 30, including escort and support personnel(Observers allowed)

Sincerely,

Colonel Kim, Boo-bae
Chief of Training Policy, G-2/3
Republic of Korea Army

미끼와 타깃

미끼 문서는 2026 4th K-ICTC Information.pdf로, 국문본과 영문본 두 종이 확인되었습니다. 국문본은 육군본부 훈련정책 부서, 합참 국제협력·훈련 담당 장교, 국방부 정책 실무자를 표적으로 삼으며, 영문본은 주한 외국 무관부, 과거 K-ICTC 참가국 군 담당자, 미군·호주군·영국 군 연합훈련 연락장교를 표적으로 합니다. 미끼 주제의 전문성과 표적 분리(국문/영문)로 보아 사전 정찰이 충분히 이루어진 캠페인으로 판단됩니다.

공격 흐름

사용자가 2026 4th K-ICTC Information.pdf.lnk를 실행하면, curl을 이용해 자체 C2 IP(103.67.196.25)의 /conf.dat을 다운로드해 C:\Users\Public\Music\ant.vbe로 저장합니다. VBE는 VBScript Encoded 형식의 백그라운드 실행용 스크립트로, WMI를 경유해 PowerShell을 호출하는 역할만 수행합니다.

이어 실행되는 PowerShell은 다중 난독화 해제 루틴을 거치는데, 변수명이 모두 \$tiger, \$bear, \$puma 같은 동물명으로 난독화되어 있습니다. 난독화가 풀리면 최종적으로 (New-Object Net.WebClient).DownloadString() 형식의 페이로드 다운로드 명령이 조립되며, 이때 getmac 명령으로 시스템 MAC 주소를 수집해 피해자 고유 식별자를 만듭니다.

이 MAC 주소를 시드로 사용해 C2 서버에 hxxp://103.67.196.25/view1.php?type=apple&seed=<MAC> 요청을 보내고, 공격자 서버는 해당 MAC에 매칭되는 맞춤 페이로드를 응답합니다. 페이로드는 iex를 두 차례 호출해 실행되는데, 1차 iex는 원격 스크립트 요청을 수행하고, 2차 iex는 디스크에 파일을 저장하지 않는 파일리스 방식으로 최종 코드를 실행합니다. 이후 작업 스케줄러를 통해 15분 주기로 C2 서버에서 명령을 수신·실행하며 지속성을 유지합니다.

시사점

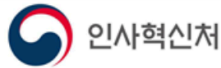
MAC 주소 기반 맞춤 페이로드 배포 방식은 공격자가 표적 환경의 식별 정보를 사전에 확보하고 있어 특정 PC에만 본 페이로드를 내려보낼 수 있다는 의미입니다. 이는 동물명 변수 난독화와 결합되어 정적·동적 분석 모두를 어렵게 만드는 구조입니다.

Campaign #4 — 위탁교육 서류 위장 스피어피싱

한 줄 요약

하나의 ZIP 파일 안에 이중 확장자(.hwpj.jse)로 위장한 JSE 스크립트 두 종을 담아 배포한 캠페인으로, 하나는 DLL 정찰 모듈을 로드하고 다른 하나는 정상 VSCode CLI로 터널링하여 피해자 PC를 원격 제어합니다.

2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류



【 복 자 】

【별첨 1】 부처별 자체 국내위탁 교육훈련 심의위원회 개최관련 양식

- (1-1) 국내대학 석사야간과정 위탁교육대상자 추천서
- (1-2) 훈련과제 세부연구계획서
- (1-3) 공무원 국내위탁 교육훈련 심의의결서

【별첨2】 입학시험 대상자 추천 (각 부처→각 대학원)

- (2-1) 입학전형 대상자 추천 공문(예시)
- (2-2) 입학시험 전형대상자 추천명단
- (2-3) 국내대학원 석사(야간)과정 정부위탁교육 진행안내
- (2-4) 국내대학원 석사(야간)과정 위탁교육 추천자 전형결과 통보서식

【별첨3】 위탁교육 최종 선발명단 통보 서식 (각 부처→인사처)

- (3-1) 선발명단
- (3-2) 서약서
- (3-3) 연구윤리 준수 서약서

【별첨4】 교육비 청구 서식

미끼와 타깃

배포 파일명은 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류.hwp.x.jse와 동일 이름에 (1)이 붙은 또 다른 미끼 파일로, Windows 기본 설정상 .jse 확장자가 숨겨지므로 사용자에게는 한글 문서(.hwp.x)처럼 보입니다. 표적은 중앙부처·지방자치단체 공무원, 기업·준정부기관 재직자, 임직원 위탁교육 제도를 운영하는 대기업 재직자, 그리고 위탁교육생을 받는 대학원의 입학처·행정실 담당자입니다.

미끼파일 #1 — DLL 정찰 모듈 로딩

JSE 스크립트가 실행되면 먼저 정상 한글 문서를 드롭·실행해 피해자의 의심을 차단합니다. 이후 Base64로 인코딩된 1차 페이로드를 iIdypWi.zgyY 이름으로 저장하고, certutil -decode 명령을 통해 최종 악성 DLL인 ke2I3TP.crqn을 생성합니다. 이 DLL은 rundll32.exe의 load 함수로 로드되어 즉시 백신·네트워크·사용자·프로세스 등 시스템 전반에 대한 초기 정찰을 수행합니다.

DLL 수집 정보

명령어

수집 정보

Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct 설치된 백신 제품명, 버전, 상태

명령어	수집 정보
<code>dir C:\</code>	C 드라이브 루트 디렉토리 목록
<code>dir C:\programdata</code>	ProgramData 폴더 내 파일/폴더 목록
<code>dir C:\Users</code>	사용자 계정 목록
<code>tasklist</code>	현재 실행 중인 프로세스 전체 목록
<code>dir "C:\program files"</code>	설치된 프로그램 목록
<code>dir "%USERPROFILE%\Desktop"</code>	바탕화면 파일 목록
<code>ipconfig /all</code>	IP 주소, MAC 주소, DNS 서버, 게이트웨이, DHCP 정보
<code>route print</code>	라우팅 테이블 전체
<code>net user</code>	로컬 사용자 계정 목록 및 그룹 정보
<code>netstat -nao</code>	현재 활성 네트워크 연결, 포트, 연결된 PID
<code>systeminfo</code>	OS 버전, 패치 수준, 아키텍처, 도메인, 부팅 시간, 메모리 등
<code>reg query HKCU\...\CurrentVersion\Run</code>	현재 사용자 시작프로그램 레지스트리 항목

수집된 정보는 C2 서버(yespp.co.kr/common/include/code/out.php)로 전송됩니다.

미끼파일 #2 — VSCode 터널링 원격 제어

동일한 미끼 문서로 피해자를 속인 뒤, Microsoft 공식 CDN에서 VSCode CLI ZIP을 다운로드 합니다. 압축 해제 후 `code.exe`를 `C:\ProgramData\`에 복사하고, 중복 실행을 방지하기 위해 기존에 실행 중인 `code.exe` 프로세스를 종료한 다음 터널링 단계로 진입합니다.

이 파일의 핵심은 정상 도구인 VSCode의 터널 기능을 그대로 활용한다는 점입니다. 피해자 PC에서 `code.exe tunnel --name bizeugene` 명령이 실행되면, `code.exe`는 GitHub에 Device

Code 발급을 요청하고 일회용 디바이스 코드를 받아 로컬 out.txt에 기록한 뒤 github.com/login/oauth/access_token 엔드포인트로 인증 폴링을 시작합니다.

이때 JSE 스크립트는 out.txt의 내용을 C2 서버 (yespp.co.kr/common/include/code/out.php)로 POST 전송합니다. 공격자는 이 디바이스 코드를 자신의 GitHub 계정으로 github.com/login/device에 입력해 인증을 완료하며, 그 결과 access token이 피해자 PC로 반환됩니다. 인증이 완료되면 vscode.dev/tunnel/bizeugene 주소로 터널이 활성화되어, 공격자는 자신의 브라우저에서 해당 URL로 접속해 피해자 PC를 원격 제어합니다.

단 계	주체	동작	통신 대상
1	피해자 PC	code.exe tunnel -- name bizeugene 실행	-
2	code.exe	GitHub에 Device Code 발급 요청	github.com
3	GitHub	일회용 디바이스 코드 발급	→ 피해자 PC
4	code.exe	디바이스 코드를 out.txt에 기록	로컬
5	code.exe	access_token 엔드포인트 반복 폴링	github.com/login/oauth/access_token
6	JSE 스크립트	out.txt 내용을 C2 서버로 POST 전송	yespp.co.kr/common/include/code/out.php
7	공격자	C2에서 디바이스 코드 확인	yespp.co.kr
8	공격자	공격자의 GitHub 계정으로 코드 입력	github.com/login/device
9	GitHub	인증 완료 → access token 반환	→ 피해자 PC (code.exe)
10	code.exe	터널 활성화	vscode.dev/tunnel/bizeugene

단 계	주체	동작	통신 대상
11	공격자	터널 접속 → 피해자 PC 원격 제어	vscode.dev/tunnel/bizeugene

시사점

이 캠페인이 위협적인 이유는 두 미끼 파일 모두 합법적인 도구·서비스를 핵심에 두기 때문입니다. 미끼파일 #1은 Windows에 기본 내장된 certutil을 페이로드 디코딩에 사용하고 rundll32.exe로 DLL을 로드하는 LotL(Living off the Land) 방식이며, 미끼파일 #2는 Microsoft가 직접 서명·배포하는 정상 VSCode 바이너리와 GitHub OAuth 인증 흐름을 그대로 활용합니다. 결과적으로 트래픽은 Microsoft CDN과 GitHub로 향하고, 실행 파일은 정상 서명되어 있어 평판·해시 기반 차단이 어렵습니다. 또한 .hwpj.jse 이종 확장자는 Windows 기본 설정에서 두 번째 확장자가 숨겨지므로 사용자 시점에서는 한글 문서로 인식됩니다.

3. 위협 캠페인 종합 결론

분석된 네 캠페인은 위장 주제, 초기 벡터, C2 인프라가 각기 다르지만, 전술·기법·절차(TTP) 측면에서는 스피어피싱 초기 접근 + 정상 도구·서비스 악용(LotL/Legitimate Service Abuse) + 스크립트 다단계 난독화 + 작업 스케줄러 기반 지속성이 결합된 동일한 침투 프레임워크 위에서 운영되고 있습니다. 단일 IOC(도메인·해시·파일명)는 캠페인 간에 거의 공유되지 않으나, 공격 행위의 흐름은 일관되어 있습니다. 따라서 IOC 기반 차단만으로는 한계가 명확하며, 공격 단계별 행위와 그 상관관계를 통합적으로 탐지하는 체계가 필요합니다.

본 분기 캠페인 전반에서 관찰된 공통 TTP는 다음과 같습니다.

- 이종 확장자 LNK·JSE 첨부를 통한 초기 실행 (.pdf.lnk, .hwpj.jse)
- 미끼 문서 표시와 악성 페이로드 실행의 동시 수행으로 사용자 의심 차단
- 정상 OS 구성요소 악용(LotL): curl, certutil, rundll32, wscript, schtasks
- 정상 서비스 C2 채널 악용: GitHub raw·API, Microsoft CDN, VSCode 터널
- 단계별 스크립트 난독화: 환경변수 치환, Base64 인코딩, 동물명 변수, MAC 시드 기반 분기 페이로드
- 작업 스케줄러 기반 지속성: OneDrive·Update·Intel 등 정상 서비스명 위장, 1~60분 주기 폴링
- UAC 비활성화 및 Defender 예외 등록으로 후속 페이로드 탐지 차단
- uid/IP/MAC 기반 피해자 식별으로 표적 환경에만 페이로드 회신 (분석 환경 회피)
- LNK 트레일링 데이터에 미끼·페이로드 동시 은닉으로 초기 단계 외부 통신 제거

도메인, IP, 파일명, 확장자는 단기간에 교체되는 가변 지표이므로, 프로세스 실행 관계, 명령행 패턴, 파일 생성 위치, 예약 작업 생성, 정상 도구 악용 행위 간의 상관관계를 기반으로 한 탐지·헌팅 체계를 병행해야 합니다.

4. 침해 지표(IOC)

Campaign #1

MD5

80088af673b0117dbd5cf528021dd970	1.pdf.lnk
c499e415f7e07f513d8319013a8b2e86	1.pdf.lnk.zip
0331a83b58231cb0cd3bfe319003ed1a	OneDrive.lnk
806fb7876b63ba89d2432cb831be01ba	a.ps1
c57a8b40d2ca402656ff3d778f42708c	bb.ps1
2689f58b803364bbfba2edb423a3b572	bpersist.ps1
552ca91696fedd387e1ea47f50f18344	scheduler-once.bat

C2

hxxps://nelark.icu/xftaswx/res/post_proc.php?fpath=a.ps1
hxxps://nelark.icu/xftaswx/res/post_proc.php?fpath=bpersist.ps1
hxxps://nelark.icu/xftaswx/res/index.php
hxxps://nelark.icu/xftaswx/res/post_proc.php?fpath=scheduler-once
hxxps://nelark.icu/xftaswx/res/bypass.b

Campaign #2

MD5

aa9d5dd632bb90addca480eaa5ff4382	PumpGuard-Pumpfun-AI-Attack-Defence-Requirements.pdf
5c2857913efc6007b3ee7028a132baa4	PumpGuard-Pumpfun-AI-Attack-Defence-Requirements.pdf
6869766741b40825e31fd8bbff688bd3	bpvme.ps1
3fdce08723365d5c06e1183585164118	PumpGuard_Pumpfun_AI_Attack_Defence_Requirements_v2_
a3363e0c22c0356fdbcdc37f502bbcd	firefox.ps1
471faa43f4811a0250648d586cb3eebf	bpvme.ps1
8301fc2c740f6309864e68b6e429d0f0	whale.vbs
af7330af68a8f79b5a28fcc242e54a7e	doc_2026-03-26_08-58-03.NetAngular.pdf.zip
450774df6785e6eeb6ea906490905888	firefox.ps1
831d7c614ba32aa5d70ff9b0f259ee1d	wale.ps1

C2 (정상 GitHub 서비스 악용)

hxxps://raw.githubusercontent.com/brandonleeodd93-blip/doc7/main/1.txt
hxxps://raw.githubusercontent.com/brandonleeodd93-blip/doc7/main/view.pdf
hxxps://api.github.com/repos/brandonleeodd93-blip/doc7/contents/report/{IP}-{시간}-0956

Campaign #3

MD5

b3c90f52e4b86a94ec637fee4354bb84 2026 4th K-ICTC Information.pdf.lnk
0dd1cf2d9a72fdbef19e77af59ba9d1f 2026 4th K-ICTC Information.pdf.zip
cbb059bd691d846e8279d617134d3129 conf.dat

C2

hxxp://103.67.196.25/conf.dat
hxxp://103.67.196.25/payload.dat
hxxp://103.67.196.25/view1.php?type=apple&seed=<MAC>

Campaign #4

MD5

bb5040d54135b0999cc491b41a0a45e2 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류
9fe43e08c8f446554340f972dac8a68c 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류
52f1ff082e981cbdfd1f045c6021c63f 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류
bb9e9c893b170b3774c150b1d0b93a73 iIdypWi.zgyY
08160acf08fccecd7b34090db18b321 kE2I3TP.crqn

C2

hxxps://www.pyrotech.co.kr/common/include/tech/default.php
hxxps://www.yespp.co.kr/common/include/code/out.php



F5 BIG-IP APM
원격 취약점(RCE)
대응 권고

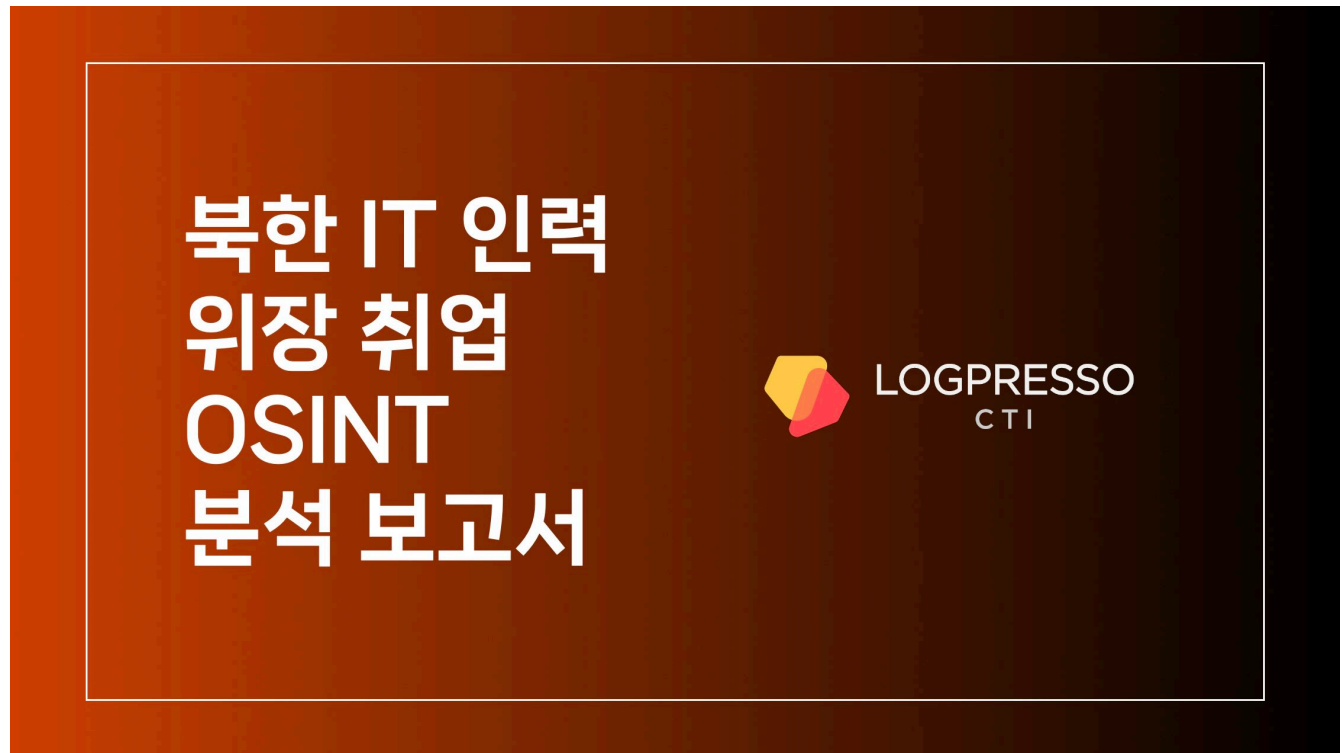


LOGPRESSO

F5 BIG-IP APM 원격 취약점 대응 권고

F5 BIG-IP APM은 F5 Networks의 접근 제어 솔루션으로, 인증되지 않은 공격자가 원격 코드를 실행(RCE) 할 수 있는 심각한 보안 취약점이 확인되었습니다.

2026-04-02



[로그프레소 CTI] 북한 IT 인력 위장 취업 OSINT 분석 보고서

인포스틸러 로그로 추적한 북한 IT 노동자 위장 취업 분석 - 100만 건 봇넷 텔레메트리로 밝혀낸 조직적 다중신원 운영 구조

2026-03-09

2026년 1분기 Chinese-nexus PlugX 공격 분석 보고서



LOGPRESSO
CTI

Chinese-nexus PlugX 공격 2026년 1분기 분석 보고서

PlugX 멀티캠페인 변종 심층 분석 - 동남아·중동·중앙아 외교 타깃 맞춤형 트리거·암호화 커스터마이징 전술 비교

2026-04-08

새로운 위협보다 앞서나가세요

(필수)개인정보 수집 및 이용에 동의합니다.

© 2022 Logpresso Inc. All rights reserved.