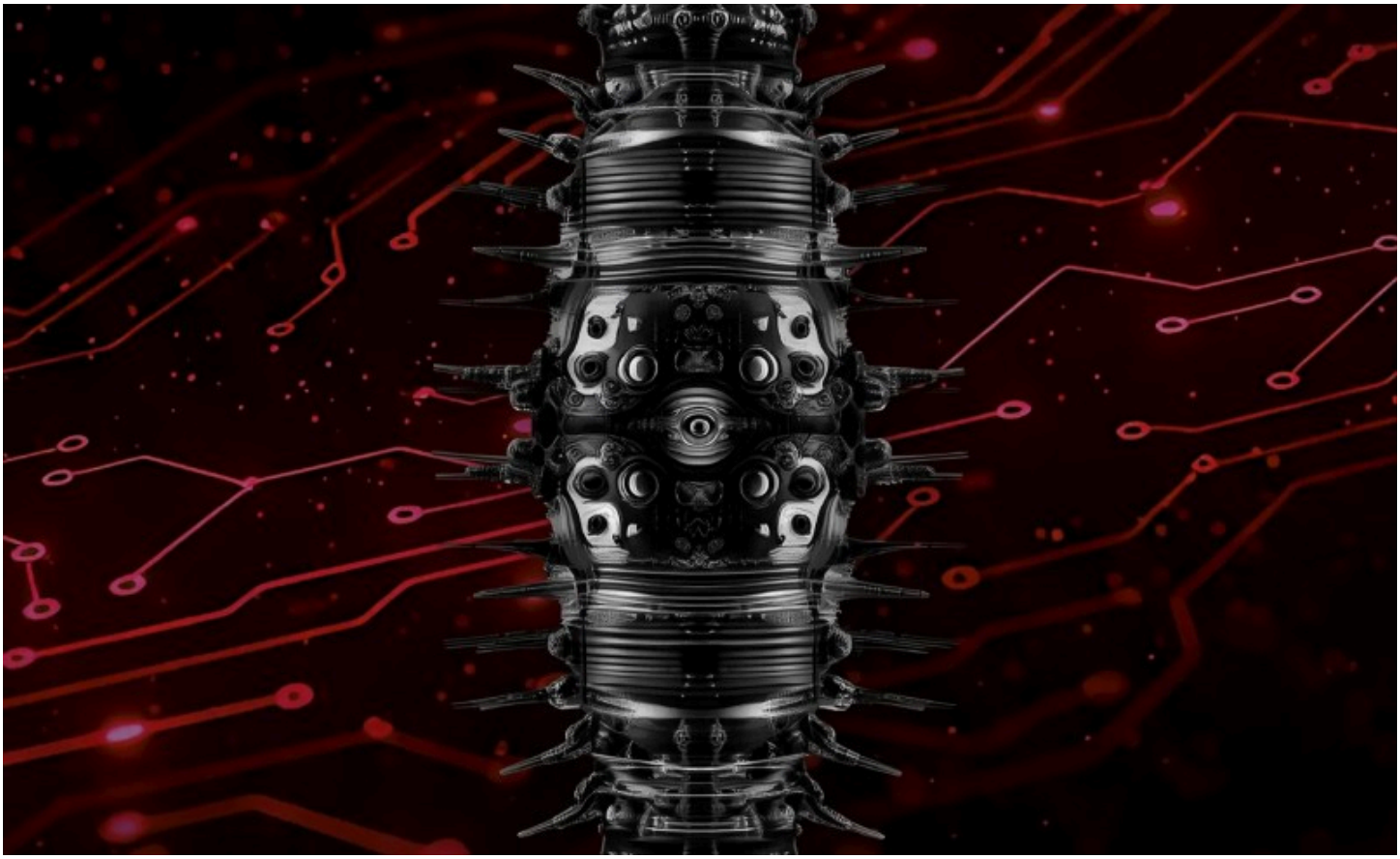
asec.ahnlab.com /ko/90408/

Larva-25010 – APT Down 공격자 PC 분석

⋮ 10/1/2025

APT

- 2025년 10월 02일



본 보고서는 ‘APT Down: the North Korea Files’ 보고서 공개 이후 ‘AhnLab TIP’의 ‘위협 Notes’로 작성된 APT Down의 침해 현황 분석에 대한 7개의 게시글과 추가 분석 내용을 정리한 보고서이다.

- 2025/08/12 게시, ‘APT DOWN – 한국 기관 침해 현황 분석’
- 2025/08/13 게시, ‘APT DOWN – 한국 기관 침해 현황 분석(2)’
- 2025/08/20 게시, ‘APT DOWN – 한국 기관 침해 현황 분석(3): 정부기관 공용 패스워드 (추정) 보안 경고’
- 2025/08/25 게시, ‘APT DOWN – 한국어를 모르는 공격자, 중국인 가능성 짙다’
- 2025/08/27 게시, ‘APT DOWN – 대만과 일본을 대상으로 한 정찰 행위 식별’
- 2025/08/29 게시, ‘APT DOWN – APPM제품 유출 및 데이터 복호화 시도 정황’
- 2025/09/08 게시, ‘APT DOWN – 네이버와 카카오 로그인 페이지 피싱 공격 준비 정황’

‘APT Down: the North Korea Files’ 보고서는 지난 8월 세계적인 해킹 대회 Defcon 33에서 보고서와 관련 자료가 공개됐다. 해당 보고서는 해외 화이트 해커 saber와 cyb0rg가 작성해 해킹 기술 관련 간행물 Phrack Magazine 40주년 기념호에 수록됐다.

보고서의 저자인 saber와 cyb0rg는 APT 공격자 워크스테이션에 유출한 데이터 덤프의 분석 결과를 공개했다. 이들은 해당 자료를 통해 대한민국 주요 행정기관, 군 기관, 통신사를 대상으로 한 지속적 공격 흔적을 확인했으며, 분석 대상이 북한 연계 공격 그룹인 Kimsuky 소속원의 PC이라고 주장했다.

ASEC(AhnLab Security Intelligence Center)은 저자들이 공개한 보고서와 데이터를 토대로 추가 분석을 진행했으며, 그 결과 공개된 자료보다 더 구체적인 사실을 확인했다.

구분	내용

공격자	• 중국어에 능통한 중국 국적의 공격자
	  ◦ Kimsuky 공격 그룹과 협업 관계를 형성
	  ◦ 한국어를 이해하지 못하며, 중국어를 주언어로 사용
	• 기업형 조직의 일원
	  ◦ 평일 주중 9-6 근무 수행
	  ◦ 주말/공휴일 활동이력 없음

주요 공격 내용	• 한국, 일본, 대만 지역을 대상으로 공격 수행
	  ◦ 한국: 피싱 공격 정황 확인
	  ◦ 일본: Sophos 제품 취약점을 노린 공격 대상 스캔 행위
	  ◦ 대만: JBoss(Wildfly), Paloalto 제품 취약점을 노린 공격 대상 스캔 행위

공격자 사용 도구	• Ivanti CVE-2025-0282 Exploit • Rootkit (Syslogk) • Backdoor (TinyShell) • CobaltStrike Beacon • Phishing 인프라
사건 TAG	#APT Down #Larva-25010 #APT41 #UNC3886 #UNC5221 #인증서유출 #정보유출 #Ivanti Exploit #syslogk #Tinyshell #Phishing #CobaltStrike

표 1. 분석 요약

MD5

00dfce9ad207f77397dbbb6791d64a9e

1d475427100ad95edca070d75fa3b267

2c0fbdb97439e079bbd8919c39598508

36d2be6eb548aee37852f7fbf38dcf30

3b76316810d61e114015af617c5d0408

추가 IoC는 ATIP에서 제공됩니다.
FQDN

websecuritynotices[.]com

추가 IoC는 ATIP에서 제공됩니다.

IP

104[.]167[.]16[.]97

추가 IoC는 ATIP에서 제공됩니다.