PC-MEOMEO 침입 사고 분석 보고서 — 공격 타임라인

분석 근거 파일: Security.evtx / System.evtx / Application.evtx / PowerShell.evtx / Prefetch(.pf) / Registry(SAM·SOFTWARE·SYSTEM)

Security.evtx | System.evtx | Application.evtx | PowerShell.evtx | Prefetch(.pf) | Registry | SAM

시스템 설치

2025-10-23 17:24 — Windows 11 25H2 Pro 최초 설치
컴퓨터명: OPENSTACK / 기본 계정: user
System.evtx — 6005 | Reg(SOFTWARE) | SAM

침입 전 사전 준비

2025-12-16 12:06 — 비공식 루트 인증서 조작 (MITM 환경 구성)
certutil + test.certs.us.kg 인증서 — HTTPS 트래픽 가로채기 흔적
PowerShell.evtx | Reg(SOFTWARE) — TypedURLs

2026-04-15 08:02 — Xshell 실행 — SSH 클라이언트
외부 서버(C2) 접속 추정
XSHELL.EXE.pf

2026-04-17 06:02 — RDP Wrapper 설치 + 자동 업데이트 예약 작업 등록 (핵심 포인트)
무제한 동시 RDP 세션 허용 / 재부팅 후에도 유지
PowerShell.evtx — Set-ScheduledTask | RDPCONF.EXE.pf

2026-04-17 19:31~ — 원격제어 도구 4종 설치
Radmin VPN / Radmin Server V3 / DWAgent / Chrome 원격 데스크탑
System.evtx — 7045 | PF 다수 | App.evtx — MsiInstaller

2026-04-17 19:42 — Windows Defender 비활성화 (핵심 포인트)
SECURITY_PRODUCT_STATE_SNOOZED — RDP 침입 약 6시간 전 보안 무력화
App.evtx — SecurityCenter ID 15

2026-04-17 20:19 — RevoltG → Defender 탐지 예외 3중 등록
Add-MpPreference -ExclusionPath / -ExclusionProcess RevoltG.exe
PowerShell.evtx — Add-MpPreference | REVOLTG.INSTALLER.EXE.pf

2026-04-17 21:37~ — MSTSC + MASSSCAN 실행 — 다음 피해자 탐색
원격 데스크탑으로 타 PC 접속 + 대규모 포트 스캔
MSTSC.EXE.pf | MASSSCAN_GUI.EXE.pf

RDP 침입 (2026-04-18 새벽)

04-18 01:06~ — javaw.exe 반복 크래시 (RDP 접속 전)
TLauncher / FISHINGBOTPT_VIP 실행 중 오류 — 새벽 1시부터 게임봇 운용
App.evtx — Application Error ID 1000 | TLAUNCHER.EXE.pf / FISHINGBOTPT.pf

04-18 02:01 — linhhxinhhhyeuuu 계정으로 재부팅 명령 직접 실행
C:\WINDOWS\SysWOW64\shutdown.exe — 접속 10분 전 흔적 세탁
System.evtx — EventID 1074

04-18 02:11 — ★ 최초 RDP 침입 확인 (핵심 포인트)
IP: 14.230.201.161 (베트남) → 계정: linhhxinhhhyeuuu / LogonType 10 — 화면 완전 제어 시작
Security.evtx — EventID 4624 LogonType 10

04-18 02:13~28 — RDP 세션 반복 재연결 (LogonType 7)
02:13 / 02:26 / 02:28 — 네트워크 불안정 또는 의도적 세션 관리
Security.evtx — EventID 4624 LogonType 7

침입 후 행동 — 거점 구축 및 도구 실행

04-18 03:04 — vpnbook VPN 연결 — 신원 세탁 (핵심 포인트)
Dial-in User: vpnbook — 실제 출발지 IP 은닉 후 추가 공격 수행
App.evtx — RasClient 20221~20225

04-18 04:24 — RDPCONF.exe — RDP 설정 강제 변경
지속 RDP 접근 환경 구성 (포트/권한 설정 조작)
RDPCONF.EXE-5722DB7A.pf

04-18 04:32 — DWAgent + Radmin Server 활성화
원격제어 에이전트 — RDP 외 추가 접속 채널 확보
DWAGENT.EXE.pf | RSERVER3.EXE.pf

04-18 05:16~20 — VPSTTT.COM.EXE + CRTIX.EXE 실행
의심 실행파일 — VPS 봇/크립토 관련 도구 추정
VPSTTT.COM.EXE.pf | CRTIX.EXE.pf

04-18 09:33 — Wireshark + npcap watchdog 설정
패킷 캡처 실행 + 부팅 시 자동 시작 예약 작업 — 자격증명 스니핑 목적
WIRESHARK.EXE.pf | PowerShell.evtx — Register-ScheduledTask

04-18 09:47 — FISHINGBOTPT_VIP.EXE 실행
게임 자동화 봇 / 피싱 도구 — javaw 크래시와 연동
FISHINGBOTPT_VIP.EXE.pf

04-18 12:31 — MMC.exe — 관리 콘솔 실행
로컬 사용자 및 그룹 관리 — 계정 권한 조작 추정 (4732 직접 로그 미확인)
MMC.EXE.pf

04-18 13:19 — 오후 재접속 (LogonType 7)
14.230.201.161 — 오후에도 지속 접속 확인
Security.evtx — EventID 4624 LogonType 7

04-18 16:30 — 시스템 정보 전수 수집
CPU / GPU / RAM / Disk / BIOS / OS — 채굴 가능 여부 평가 / 봇넷 편입 준비
PowerShell.evtx — Get-CimInstance 다수

04-18 20:13 — 4738 계정 속성 변경
linhhxinhhhyeuuu 계정 설정 조작 (변경 내용 상세 로그 제한)
Security.evtx — EventID 4738

지속성 확보 (2026-04-19 ~ 04-20)

04-19 01:20 — TLauncher 실행 (비공식 Minecraft 런처)
tlauncher.org — 악성코드 유통 경로로 악용되는 크랙 런처
TLAUNCHER.EXE.pf | Reg(SOFTWARE) — TypedURLs

04-19 01:44 — 로컬 콘솔 로그온 + REGEDIT 실행
127.0.0.1 LogonType 2 — 레지스트리 직접 편집
Security.evtx — 4624 LogonType 2 | REGEDIT.EXE.pf

04-19 01:50 — 마지막 확인 원격 RDP 접속
14.230.201.161 → LogonType 7 — Security 로그 기준 최후 원격 세션
Security.evtx — EventID 4624 LogonType 7

04-19 04:47 — RealVNC Viewer 7.15.1 설치
3번째 원격 접속 도구 — Radmin / Chrome 원격 데스크탑에 이어 백업 채널 추가
App.evtx — MsiInstaller 11707 | Reg(SOFTWARE) — TypedURLs

04-19 10:55 — RDPCHECK.exe — RDP 취약점 점검
다음 공격 대상 RDP 취약점 스캔
RDPCHECK.EXE.pf

04-20 03:37 — SCHTASKS + SC.EXE — 예약 작업 + 서비스 조작
재부팅 후에도 공격 도구 자동 실행 — 지속성 확보
SCHTASKS.EXE.pf | SC.EXE.pf

04-20 05:56 — ★ UTILMAN.EXE 백도어 설치 (핵심 포인트)
접근성 도구 교체 — 비밀번호 없이 SYSTEM 권한 CMD 실행 가능 / 현재도 살아있을 가능성 높음
UTILMAN.EXE-47FA7BEF.pf

최종 분석 요약

0. 최초 공격 시점	2026-04-18 02:11 / IP: 14.230.201.161 (베트남)	Security.evtx — 4624 LogonType 10
1. 윈도우 설치	2025-10-23 / Windows 11 25H2 Pro	System.evtx · Reg(SOFTWARE) · SAM
2. 사용자	원래: user (OPENSTACK) / 공격자: linhhxinhhhyeuuu	SAM · System.evtx — 1074
3. 접속 사이트	vpnbook.com / tlauncher.org / wireshark.org / realvnc.com	Reg(SOFTWARE) — TypedURLs · App.evtx — RasClient
4. 실행 도구	MASSSCAN / RDPCONF / RDPCHECK / FISHINGBOTPT / VPSTTT / CRTIX / UTILMAN	Prefetch(.pf) 320개 분석
계정 생성 4720 ②	SAM에 존재 확인 / 생성 로그는 기록 범위 밖	SAM
계정 변경 4738 ④	2026-04-18 20:13 확인	Security.evtx — 4738
지속 접근 ⑤	UTILMAN 백도어 + SCHTASKS + 원격도구 5중 + RDP Wrapper	PF · PowerShell.evtx · App.evtx

PC-MEOMEO 침입 사고 분석 보고서 — 공격자 의도 분석

공격자: linhhxinhhhyeuuu / 출발지 IP: 14.230.201.161 (베트남) / 경유: vpnbook.com VPN

공격자 프로파일

계정명	linhhxinhhhyeuuu (베트남어: "예쁜 사랑스러운 Linh" 의미)
출발지 IP	14.230.201.161 (베트남 호스팅 추정)
신원 은닉	vpnbook.com 무료 익명 VPN 경유 — 실제 IP 숨김
공격 유형	기회주의적 개인/소규모 그룹 (정교한 APT 아님)
주요 언어	베트남어 (계정명, 시스템 환경 기반 추정)

공격 목적 분석 — 3가지 의도가 혼재

목적 1 | 게임 자동화 봇 운용 (가장 강한 증거)

- FISHINGBOTPT_VIP.EXE — Minecraft 자동 낚시봇 — 아이템 자동 수집 후 현금화
- AUTOCLICKER.EXE / AUTO.CLICK — 마우스/키보드 자동화 — 반복 작업 자동 수행
- AUTOHOTKEYU64.EXE — 스크립트 기반 게임 자동화
- TLAUNCHER.EXE — 비공식 Minecraft 런처 (무료 서버 접근)
- REVOLTG.EXE — 게임 핵/봇 (Defender 예외 3중 등록으로 탐지 우회)
- javaw.exe 하루 21회 크래시 — Java 봇을 하루 종일 돌린 직접 증거

피해자 PC의 전기/자원을 무단 사용해 게임 재화를 파밍, 이를 현금화하는 구조. 봇이 크래시 나도 계속 재실행 — 장시간 무인 운용이 목표.

목적 2 | 피벗 공격 (다음 피해자 탐색)

- MASSSCAN_GUI.EXE — 대규모 인터넷 포트 스캔 — 다음 RDP 취약 대상 탐색
- MSTSC.EXE — 이 PC에서 다른 PC로 RDP 접속 시도
- RDPCHECK.EXE — 다음 공격 대상의 RDP 취약점 점검
- XSHELL.EXE — SSH로 외부 C2 서버 접속
- vpnbook VPN — 스캔 출처 IP 은닉 — 차단 우회

이 PC를 "중간 거점"으로 사용해 자신의 실제 IP를 숨기고 다음 피해자를 공격. 공격자 IP가 차단되어도 피해자 PC의 IP를 이용해 계속 스캔 가능.

목적 3 | 장기 지속 수익화 인프라 구축

- Radmin VPN / Server — 원격 접속 채널 1
- DWAgent — 원격 접속 채널 2
- Chrome 원격 데스크탑 — 원격 접속 채널 3
- RealVNC Viewer — 원격 접속 채널 4
- RDP Wrapper — 원격 접속 채널 5 (무제한 동시 세션)
- UTILMAN.EXE 백도어 — 비밀번호 없이 SYSTEM 권한 접근 — 최후 수단
- npcap watchdog 예약 작업 — 부팅마다 패킷 캡처 자동 시작
- SCHTASKS 예약 작업 — 재부팅 후 봇 자동 재시작

5중 원격 접속 채널 + 로그인 없이 접근 가능한 백도어 = 어떤 상황에서도 재진입 가능. 조용히 장기간 기생하면서 지속 수익을 내는 구조.

반증 근거 — 공격자가 의도하지 않은 것

랜섬웨어 목적이었다면 있어야 할 것

- ☒ 파일 암호화 도구 실행 (미발견)
- ☒ 볼륨 섀도 삭제 (vssadmin) (미발견)
- ☒ 백업 폴더 삭제 (미발견)
- ☒ 몸값 메모(.txt) 생성 (미발견)

데이터 탈취 목적이었다면 있어야 할 것

- ☒ 대용량 파일 압축/외부 전송 (미발견)
- ☒ mimikatz 자격증명 덤프 (미발견)
- ☒ 문서/DB 대량 접근 흔적 (미발견)
- ☒ 클라우드/FTP 업로드 (미발견)

종합 결론

주목적	피해자 PC를 게임 봇 농장으로 장기 운용 → 전기·자원 비용 없이 게임 재화 파밍 후 현금화
부목적	피벗 포인트 활용 → 이 PC에서 다음 피해자 스캔·공격 (자신의 IP 은닉)
수법	5중 백도어로 장기 지속 접근 확보 → 피해자가 눈치채도 다른 경로로 재진입
특이점	Wireshark + npcap 상시 실행 → 피해자가 입력하는 계정·비밀번호 가로채기 시도 가능
결론	저비용 고수익을 노린 기회주의적 공격자 / 정교한 APT가 아닌 개인 또는 소규모 그룹