USB 전파형 크립토마이너의 프로세스 감시 행위에 대한 API 후킹 기반 역탐지

양시은, 정주연, 박태준*

전남대학교(학부생), *전남대학교(교수)

didtldms2525@jnu.ac.kr, siddl1020@jnu.ac.kr, *taejune.park@jnu.ac.kr

API Hooking-Based Reverse Detection of Process Monitoring Behavior in USB-Propagating Cryptominer

Yang Si Eun, Jeong Ju Yeon, Park Tae June*

Chonnam National Univ., *Chonnam National Univ.

요 약

본 논문에서는 USB 전파형 크립토마이너 PrintMiner의 프로세스 감시 기반 탐지 회피 기법을 분석하고, API 후킹을 통한 역탐지 방법을 제안하였다. 정적 분석을 통해 CreateToolhelp32Snapshot과 Process32NextW API 기반의 프로세스 열거 메커니즘을 확인하고, 시스템 모니터링 도구와 고사양 게임이 탐지 대상에 포함되어 있음을 파악하였다. 탐지 대상 문자열은 런타임 문자열 생성 등 난독화가 적용되어 정적 분석이 어려우나, 악성코드의 감시 행위 자체가 API 호출로 노출되므로 이를 역으로 포착하여 탐지할 수 있음을 Frida 기반 후킹으로 실증하였다.

Ⅰ. 서 론

크립토재킹(Cryptojacking)은 피해자의 컴퓨팅 자원을 무단으로 사용하여 암호화폐를 채굴하는 공격이며, 이를 수행하는 악성코드를 크립토마이너라 한다. 2007년부터 2019년까지 약 450만 개의 악성코드 샘플이 분석될 정도로 그 규모가 지속적으로 증가하고 있다.[1] USB 전파 방식은 네트워크 경계 보안을 우회하여 내부망에 직접 진입할 수 있어, 물리적 매체 공유가 빈번한 교육기관이나 기업 환경에서 감염이 빠르게 확산된다.[2]

크립토마이너가 장기간 은닉 채굴을 유지하기 위해서는 사용자가 시스템 이상을 인지하지 못하도록 하는 것이 중요하다. 이를 위한 기법 중 하나로 프로세스 감시가 있다. 작업 관리자 등 시스템 모니터링 도구가 실행 중일 때 채굴을 중단하고, 해당 도구가 종료되면 채굴을 재개하는 방식이다. 이러한 회피 기법은 문자열 난독화와 결합되어 탐지 대상을 파악하기 어렵게 만들며, 기존 시그니처 기반 탐지의 효과를 저하시킨다.

본 논문에서는 2025년 국내에서 발견된 USB 전파형 크립토마이너 PrintMiner를 대상으로 이러한 프로세스 감시 기반 탐지 회피 기법을 분석한다. 본 연구의 기여는 다음과 같다. 첫째, PrintMiner의 프로세스 감시 메커니즘을 정적 분석을 통해 규명한다. 둘째, 악성코드의 프로세스 감시 행위 자체가 API 호출로 노출되므로, 이를 역으로 포착하여 탐지 지표로 활용할 수 있음을 실증한다. 이는 난독화 기법에 대응하는 행위 기반 탐지 전략으로서 의의를 가진다.

Ⅱ. 본론

1. 분석 대상

본 연구에서 분석한 악성코드는 2025년 11월 전남대학교 공과대학 공용 PC에서 감염된 USB 저장장치로부터 입수하였다. 해당 샘플은 AhnLab ASEC에서 'PrintMiner'로 분류한 USB 전파형 암호화폐 채굴 악성코드와 동일 변종으로 판단되며, 본 연구에서는 ASEC의 분류를 따라 이를 'PrintMiner'로 지칭한다.[3]

PrintMiner는 DLL Sideloading[4]을 통해 정상 시스템 파일(printui.exe)의 컨텍스트에서 XMRig 기반 Monero 채굴 프로그램을 실행한다. Monero는 암호화폐의 일종으로, CPU 채굴이 가능하고 거래 추적이 어려워 크립토재킹에 빈번히 악용된다. 해당 악성코드는 Windows Defender 예외 등록, 전원 설정 조작, 프로세스 감시 등 다중 회피 기법을 사용하며, 본 연구에서는 프로세스 감시 기반 탐지 회피 기법에 초점을 맞춘다.

2. 프로세스 감시 기법 분석

2.1 프로세스 감시 구현 원리

PrintMiner의 프로세스 감시 기능은 채굴 프로그램 실행을 담당하는 스레드 내에 구현되어 있다. 이 스레드는 시스템에서 실행 중인 프로세스 목록을 주기적으로 검사하여 특정 프로세스의 존재 여부에 따라 채굴 프로그램을 동적으로 실행하거나 종료한다.

이는 Windows API의 프로세스 열거 기능을 활용하여 구현되었다. CreateToolhelp32Snapshot 함수로 실행 중인 모든 프로세스의 스냅샷을 생성하고, Process32FirstW와 Process32NextW 함수를 반복 호출하여 프로세스 목록을 순회한다. 각 프로세스의 실행 파일명은 PROCESSENTRY32W 구조체의 szExeFile 필드에서 추출되며, 악성코드 내부의 탐지 대상 목록과 비교한다. 일치하는 프로세스가 발견되면 채굴을 종료하고, 모든 대상 프로세스가 종료될 때까지 재개하지 않는다.

2.2 탐지 대상 프로세스

PrintMiner는 런타임에 문자열을 한 글자씩 붙여서 생성하는 등 문자열 난독화 기법을 적용하고 있어 정적 분석만으로는 탐지 대상 프로세스를 파악하기 어렵다. ASEC 보고서[3]에서 해당 악성코드의 탐지 대상 프로세스 일부가 공개된 바 있으며, 본 연구에서는 이 중 주요 항목을 표 1과 같이 분류하였다.

〈표 1〉 탐지 대상 프로세스 분류

분류	주요 프로세스
시스템 모니터링 도구	Taskmgr.exe, ProcessHacker.exe, procexp64.exe
영상 편집 소프트웨어	Adobe Premiere Pro.exe, AfterFX.exe, vegas200.exe
고사양 게임	sekiro.exe, RustClient.exe, ACOdyssey.exe

시스템 모니터링 도구 실행 중 채굴이 이루어지면 비정상적인 자원 점유가 노출되고, 영상 편집 소프트웨어와 고사양 게임의 경우 성능 저하로 사용자가 이상을 인지할 수 있다. PrintMiner는 이러한 상황을 회피하여 장기간 은닉 채굴을 유지하고자 한다.

3. API 후킹 기반 탐지

3.1 관측 방법론

2장에서 분석한 프로세스 감시 기법은 문자열 난독화 기법로 인해 정적 분석만으로는 전체 동작을 파악하기 어렵다. 그러나 악성코드가 프로세스 목록을 감시하기 위해서는 반드시 CreateToolhelp32Snapshot, Process32NextW 등의 Windows API를 호출해야 한다. 이 API 호출 지점을 후킹하면 악성코드의 감시 행위 자체를 역으로 포착할 수 있다.

본 연구에서는 Frida 기반 동적 계측을 통해 kernel32.dll의 프로세스 열거 API에 후킹을 설치하였다. Process32NextW 후킹 시 PROCESSENTRY32W 구조체의 szExeFile 필드에서 프로세스명을 추출하고, 분석 도구명과의 일치 여부를 실시간으로 기록하였다. 분석 환경은 VMware Workstation 기반 Windows 10 x64 가상머신이며, 네트워크 연결을 허용하여 실제 채굴 동작까지 관측하였다.

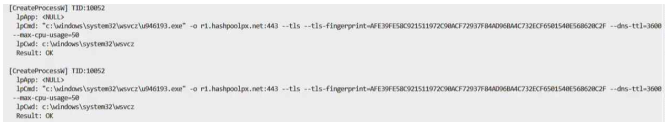
3.2 프로세스 감시 행위 관측

〈그림 1〉 API 후킹을 통한
프로세스 감시 캡처 로그

CreateToolhelp32Snapshot, Process32FirstW, Process32NextW API 후킹 결과, 그림 1과 같이 PrintMiner가 약 3초 주기로 전체 프로세스 목록을 순회하며 탐지 대상을 확인하는 행위를 포착하였다. 후킹 로그에서 Taskmgr.exe, Wireshark.exe 등이 탐지 대상으로 식별되는 것을 확인하였으며, 해당 프로세스 실행 시 채굴 프로그램이 즉시 종료되었다.

이는 악성코드가 분석 환경을 감시하려는 행위가 오히려 API 경계에서 노출됨을 보여준다. 즉, 프로세스 열거 API의 반복 호출 패턴 자체가 탐지 지표로 활용될 수 있다.

3.3 채굴 프로그램 실행 명령 관측



〈그림 2〉 CreateProcessW 후킹으로 캡처된 채굴 프로그램 실행 로그

그림 2와 같이 CreateProcessW API를 후킹하여 채굴 프로그램 실행 시 전달되는 명령줄 인자를 포착하였다. 채굴 풀 주소, TLS 핑거프린트, CPU 사용률 50% 제한 옵션 등 주요 설정이 평문으로 노출되었다. 또한, XMRig 사용과 채굴 풀 주소를 통해 해당 악성코드가 Monero를 채굴함을 확인하였다. 악성코드가 내부적으로 문자열을 난독화하더라도 API 호출 시점에서는 평문이 전달되므로, 이 경계에서의 관측이 효과적임을 확인하였다.

Ⅲ. 결론

본 논문에서는 USB 전파형 크립토마이너 PrintMiner의 프로세스 감시 기반 탐지 회피 기법을 분석하였다. 악성코드가 분석 환경을 감시하려는 행위가 오히려 API 경계에서 노출되며, 이를 역으로 탐지 지표로 활용할 수 있음을 Frida 기반 후킹으로 확인하였다. 본 연구에서 관측한 프로세스 열거 API의 주기적 반복 호출 패턴은 난독화 기법에 대응하는 행위 기반 탐지 전략으로 활용될 수 있다. 다만 본 연구는 단일 샘플 분석에 기반하므로 일반화에 한계가 있다. 향후 연구에서는 정적 분석으로 후킹 대상 API를 사전에 식별할 수 없는 경우에도 적용 가능한 범용적 API 모니터링 기법을 탐구할 예정이다.

ACKNOWLEDGMENT

본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업 및 과학기술정통부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1C1C1006967).

참 고 문 헌

[1] Pastrana, S. and Suarez-Tangil, G., "A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth," ACM Internet Measurement Conference, pp. 73 - 86, 2019.

[2] Nissim, N. Yahalom, R. and Elovici, Y., "USB-based attacks," Computers & Security, vol. 70, pp. 675-688, 2017.

[3] AhnLab ASEC, “USB 꽂는 순간 퍼지는 코인 마이너, 어떻게 침투할까?,” 2025.

(https://www.ahnlab.com/ko/contents/content-center/36027).

[4] Stewart, A. “DLL Side-Loading: A Thorn in the Side of the Anti-Virus Industry,” FireEye, pp. 1 - 12, 2014.