디지털 포렌식 분석 보고서

Windows 아티팩트 기반 Backdoor 실행 흔적 분석

문서 종류	디지털 포렌식 분석 보고서
사건명	Backdoor 실행 흔적 분석
분석 대상	침해 의심 Windows 시스템 아티팩트
사건 발생 시점	2021-06-20 (KST, UTC+09:00)
분석 수행일	2026-07-07
분석 환경	Windows 11 (ARM64) 가상머신 / UTM
사용 도구	WinPrefetchView, REGA v1.6.0.0, NTFS Log Tracker v1.4
분석자	DongGeon

본 보고서는 제공된 아티팩트 추출본에 근거하여 작성된 분석 결과이다.

■ 공개본 안내

본 분석은 CJ Olive Networks AI Security WAVE 교육과정에서 강사가 제공한 인가된 실습용 아티팩트 추출본을 대상으로 수행하였다. 실제 침해사고 대응 건이 아니며, 실존하는 개인·조직의 데이터는 포함되어 있지 않다. 별첨 타임라인 스프레드시트(backdoor_timeline.xlsx)를 함께 공개한다.

목 차

[별첨] Backdoor 침해사고 통합 타임라인 (backdoor_timeline.xlsx)

1. 사건 개요

본 분석은 침해가 의심되는 Windows 시스템에서 확보한 아티팩트를 대상으로, 악성 실행파일 'Backdoor'의 실행 여부와 관련 행위를 규명하기 위해 수행되었다. 단일 아티팩트에 의존하지 않고 서로 다른 메커니즘으로 기록되는 복수의 아티팩트를 교차 검증함으로써 분석 결과의 신뢰성을 확보하는 데 목적을 둔다.

분석 결과, 대상 시스템에서 Backdoor 관련 실행파일이 2021-06-20 두 개 시각대에 걸쳐 실행된 정황이 복수의 독립 아티팩트에서 일관되게 확인되었다.

2. 분석 개요

분석 목적	침해 의심 시스템에서 악성 실행파일(Backdoor)의 실행 여부 및 관련 행위를 아티팩트 기반으로 규명
분석 대상 아티팩트	Prefetch(.pf), 레지스트리 하이브(SYSTEM/NTUSER 등), $MFT · $LogFile
주요 의심 파일	Backdoor.exe, Backdoor.bat, Backdoor - 바로 가기.lnk
주요 시간대	2021-06-20 19:41:59 ~ 20:41:34
분석 방법론	아티팩트별 개별 분석 후 시각·경로 기준 교차 검증(cross-validation)

3. 분석 방법 및 절차

분석은 다음 순서로 수행하였다. 다만 포렌식 분석 순서는 고정된 것이 아니며, 하나의 아티팩트에서 확보한 단서를 다른 아티팩트로 확장·검증하는 반복적 과정으로 진행하였다.

3.1 실행 흔적 분석 — WinPrefetchView

Prefetch(.pf)는 Windows가 프로그램 실행 성능 향상을 위해 자동 생성하는 캐시로, '무엇이 실행되었는가'를 판단하는 근거가 된다. WinPrefetchView로 Prefetch를 분석한 결과, BACKDOOR.EXE 관련 Prefetch 파일 2종을 확인하였다.

3.2 레지스트리 분석 — REGA

레지스트리 하이브(SYSTEM, NTUSER.DAT 등)를 로드하여 시스템 상태 및 사용자 활동을 분석하였다. 특히 UserAssist는 사용자가 GUI를 통해 직접 실행한 프로그램만 기록하므로, 자동 실행과 사용자 의도 실행을 구분하는 근거가 된다. 또한 장치 관리자 정보를 통해 USB 저장장치 연결 이력을 확인하였다.

3.3 파일시스템 분석 — NTFS Log Tracker

$MFT와 $LogFile을 파싱하여 파일의 생성·수정·삭제 이벤트를 시간순으로 재구성하였다. $MFT를 함께 로드하여 각 이벤트의 전체 경로(Full Path)를 확보하였으며, 이를 통해 파일 생성부터 삭제까지의 흐름을 추적하였다.

4. 사건 타임라인

아래 표는 Backdoor.exe 와 직접 관련된 증거를 시간순으로 정리한 것이다. 일반 Windows 시스템 프로세스 등 사건과 직접 관련성이 낮은 항목은 제외하였다. 동일 시각(19:42:18 / 20:41:07 / 20:41:17)에 서로 다른 도구가 같은 실행 사건을 독립적으로 기록하고 있어, 아티팩트 간 교차 검증이 성립한다.

시간	출처(도구)	아티팩트	확인 내용	관련 파일 / 경로
2021-06-20 19:41:59	NTFS Log Tracker	$LogFile	Backdoor - 바로 가기.lnk 생성	\Users\Bum\Desktop\Backdoor - 바로 가기.lnk
2021-06-20 19:42:18	NTFS Log Tracker	$LogFile	Backdoor.bat 생성·기록 후 삭제	Backdoor.bat
2021-06-20 19:42:18	NTFS Log Tracker	$LogFile	BACKDOOR.EXE-500565FB.pf 생성	\Windows\Prefetch\BACKDOOR.EXE-500565FB.pf
2021-06-20 19:42:18	WinPrefetchView	Prefetch	BACKDOOR.EXE 실행 흔적 (Run Counter 1)	BACKDOOR.EXE-500565FB.pf
2021-06-20 20:41:07	NTFS Log Tracker	$LogFile	Backdoor.bat 생성·기록 후 삭제	Backdoor.bat
2021-06-20 20:41:07	NTFS Log Tracker	$LogFile	BACKDOOR.EXE-D0C8C9F8.pf 생성	\Windows\Prefetch\BACKDOOR.EXE-D0C8C9F8.pf
2021-06-20 20:41:07	WinPrefetchView	Prefetch	BACKDOOR.EXE 실행 흔적 확인	BACKDOOR.EXE-D0C8C9F8.pf
2021-06-20 20:41:17	REGA	UserAssist	Backdoor.exe 최종 실행 시각 및 실행 횟수 3 회 확인	Backdoor.exe
2021-06-20 20:41:17	REGA	UserAssist	Backdoor - 바로 가기.lnk 실행 횟수 3 회 확인	\Users\Bum\Desktop\Backdoor - 바로 가기.lnk
2021-06-20 20:41:19	WinPrefetchView	Prefetch	BACKDOOR.EXE 실행 흔적 (Run Counter 2)	BACKDOOR.EXE-D0C8C9F8.pf
2021-06-20 20:41:19	NTFS Log Tracker	$LogFile	Backdoor.bat 생성·기록 후 삭제	Backdoor.bat
2021-06-20 20:41:17~20:41:34	NTFS Log Tracker	$LogFile	Backdoor - 바로 가기.lnk 업데이트 흔적	\Users\Bum\Desktop\Backdoor - 바로 가기.lnk
(상시 누적)	REGA	SYSTEM 하이브 (장치관리자)	USB Mass Storage Device 연결 이력 확인	USB Mass Storage Device

※ 각 행의 '해석'을 포함한 전체 타임라인은 별첨 스프레드시트(backdoor_timeline.xlsx)에 상세 수록하였다.

5. 핵심 증거 요약

아티팩트별로 확인된 핵심 증거는 다음과 같다. 각 증거는 서로 독립적인 기록 메커니즘에서 도출되었다.

구분	분석 도구	확인 내용	확인 시각
실행 흔적	WinPrefetchView	BACKDOOR.EXE-500565FB.pf (Run Counter 1)	2021-06-20 19:42:18
재실행 흔적	WinPrefetchView	BACKDOOR.EXE-D0C8C9F8.pf (Run Counter 2)	2021-06-20 20:41:07
사용자 활동	REGA (UserAssist)	Backdoor.exe / 바로가기.lnk, 실행 횟수 3	2021-06-20 20:41:17
파일시스템	NTFS Log Tracker	Backdoor.bat 생성·수정·삭제, Prefetch 생성	2021-06-20 19:42 / 20:41
매체 이력	REGA (장치관리자)	USB Mass Storage Device 연결 이력	(상시 누적)

6. 종합 분석

확보된 증거를 종합하면 다음과 같은 정황이 도출된다.

- WinPrefetchView 에서 BACKDOOR.EXE 관련 Prefetch 파일 2 종(500565FB, D0C8C9F8)이 확인되어, 동일 실행파일이 반복 실행된 정황이 존재한다.
- REGA 의 UserAssist 기록에서 Backdoor.exe 의 실행 횟수 3 회가 확인되었다. UserAssist 는 사용자 직접 실행분만 기록하므로, 이는 자동 실행이 아닌 사용자 조작에 의한 실행 정황을 시사한다.
- NTFS Log Tracker 에서 Backdoor.bat 의 생성·수정·삭제 및 Prefetch 파일 생성 이벤트가 시간대별로 확인되었으며, .bat 파일이 반복적으로 생성 후 삭제된 점은 흔적 인멸 시도 정황으로 해석된다.
- 특히 Prefetch 의 실행 시각, NTFS 로그의 Prefetch 생성 시각, UserAssist 의 최종 실행 시각(20:41 시각대)이 상호 일치하거나 근접한다. 이는 서로 다른 아티팩트가 동일 사건을 독립적으로 뒷받침함을 의미한다.

이상을 종합하면, 분석 대상 시스템에서 Backdoor 관련 실행파일이 실행된 정황이 복수 아티팩트에서 일관되게 확인된다. 육하원칙 기준 정리는 다음과 같다.

요소	분석 결과	근거 아티팩트
무엇을	Backdoor.exe / Backdoor.bat 실행	Prefetch, UserAssist, $MFT
언제	2021-06-20 19:42 (1 차), 20:41 (2 차)	3 종 아티팩트 시각 일치
몇 회	직접 실행 3 회 / Prefetch 2 종 생성	UserAssist, Prefetch
어디서	사용자 계정 Bum 바탕화면 경로에서 구동	UserAssist, $MFT 경로
은폐 정황	.bat 파일 반복 생성 후 삭제	NTFS Log Tracker

7. 결론

서로 다른 기록 메커니즘을 갖는 세 종류의 아티팩트(Prefetch, UserAssist, $MFT/$LogFile)에서 Backdoor 실행에 관한 정황이 상호 일치하게 확인되었다. 복수의 독립 근거가 동일한 결론을 지지하므로, 대상 시스템에서 해당 실행파일이 실행되었을 개연성이 높다고 판단된다.

한편, 공격자가 Backdoor.bat 파일을 반복적으로 삭제하였음에도 Prefetch·UserAssist·$LogFile 등에 실행 및 삭제 흔적이 잔존하였다. 이는 단일 파일 삭제만으로는 침해 흔적이 완전히 제거되지 않으며, 오히려 삭제 행위 자체가 아티팩트에 기록되어 인멸 정황의 근거가 됨을 보여준다.

8. 분석의 한계 및 유의사항

- 본 보고서의 표현은 '공격자가 실행하였다'와 같은 단정이 아니라 '실행 정황이 확인된다'는 개연성 판단에 기반한다. 행위 주체의 특정을 위해서는 계정 인증 로그, 네트워크 로그 등 추가 증거가 필요하다.
- $UsnJrnl 은 확보된 데이터가 비어 있어(0KB) 분석에 활용하지 못하였다. 향후 정상 확보 시 파일 변경 저널을 통한 보강 분석이 가능하다.
- USB Mass Storage Device 연결 이력은 확인되었으나 정확한 연결 시각은 별도 분석이 필요하며, 반입 경로로 단정하지 않는다.
- 분석은 제공된 아티팩트 추출본을 기반으로 하였으며, 원본 디스크 전체에 대한 무결성 검증(해시 비교)은 본 분석 범위에 포함되지 않았다.

9. 대응 권고사항

- EDR 등 상시 모니터링을 통해 Prefetch·UserAssist·파일시스템 변경 이벤트를 지속 수집하여 유사 실행 행위를 조기 탐지한다.
- 일반 사용자 계정이 임의 실행파일을 바탕화면 등에서 구동하지 못하도록 애플리케이션 실행 통제(AppLocker 등)를 적용한다.
- USB 등 외부 저장매체 연결 정책을 수립하여 악성코드 반입 경로를 차단한다.
- 침해 의심 시 원본 디스크 이미지를 확보한 뒤 사본으로 분석하여 증거 보존(chain of custody)을 유지한다.