문제: 공격자가 원격데스크톱으로 접근한 후 사용한 도구명과 파일의 해시 값을 적으시오.

(답 양식 - INCO(도구명\_해시 값))

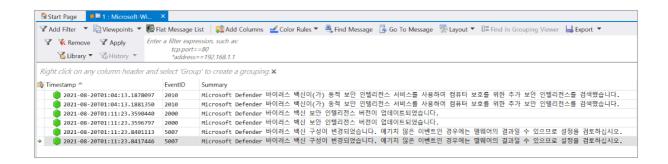
문제에서 제공되는 압축파일에는 실행파일 흔적 분석에 활용될 수 있는 "AmCache", "Prefetch" 등 다양한 아티팩트들이 제공되고 있다. 기본적으로 악성 파일이 분석 대상에 존재하지 않을 경우, 파일의 Hash 값을 확인할 수 있는 아티팩트에는 "AmCache"와 "Windows Defender Log"가 있다.

AmCache에서 "C:₩Temp" 경로에 "JP.exe"라는 도구가 실행된 흔적을 확인할 수 있다. "C:₩Temp" 경로는 공격자들이 악성파일을 은닉할 때 많이 사용하는 경로로 "AmCache"에서 "JP.exe"라는 도구가 실행된 흔적을 통해 해당 파일이 악성 파일이라는 것을 의심할 수 있다. 하지만, 파일명만으로는 해당 파일이 악성 파일이라고 판단할 수만은 없다.

SHA1	Is Os Component	Full Path
*D:	R <b>®</b> C	<b>«□</b> c
d562d36f3f1ab5f1c96d6532dfdbeedc12491ce1	True	c:\windows\system32\compattelrunner.exe
11eba7b1e26cc7d492a2c161ac48370811d0b01e	True	c:\windows\system32\csrss.exe
05d74408a9899054ff5cea5dac98858062e3250e	True	c:\windows\system32\devicecensus.exe
668c40bb6c792b3502b4eefd0916febc8dbd5182	False	c:\temp\jp.exe

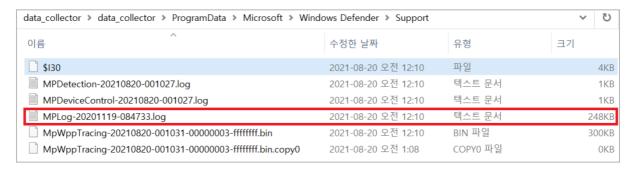
"Windows 10"에서는 "Windows Defender"라는 악성 행위를 탐지하는 백신 기능을 제공하고 있다. "AmCache"에서 의심 파일을 확인한 후, 해당 파일이 "Defender Log"에서 탐지된 이력은 없는지 추가 검증을 통해 공격자의행위를 파악할 수 있다. "Windows Defender" 로그는 이벤트 로그에서도 확인할 수 있으나, 공격자는 이벤트로그를 모두 삭제하여, 이벤트 로그에서 확인할 수 있는 내용은 존재하지 않는 상태이다.

이름	수정한 날짜	크기
Ill Microsoft-Windows-NetworkProvider%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-NetworkProvisioning%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-NlaSvc%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-Ntfs%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-Ntfs%4WHC.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-NTLM%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-OfflineFiles%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-OneBackup%4Debug.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-OOBE-Machine-DUI%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PackageStateRoaming%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-ParentalControls%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-Partition%4Diagnostic.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PerceptionRuntime%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PerceptionSensorDataService%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PersistentMemory-Nvdimm%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PersistentMemory-PmemDisk%4Operational.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PersistentMemory-ScmBus%4Certification.evtx	2021-08-20 오전 12:11	68KB
Microsoft-Windows-PersistentMemory-ScmBus%4Operational.evtx	2021-08-20 오전 12:11	68KB



이벤트로그가 모두 삭제되었지만, 이벤트로그 외에도 "Windows Defender"에서 탐지된 이력을 로깅하는 로그 파일이 따로 존재하고 있다.

해당 파일의 경로는 "C₩ProgramData₩Microsoft₩Windows Defender₩Support"이며, 해당 로그 파일을 이용하여 문제를 풀도록 최대한 유도하여, 문제를 만들었다.



해당 로그 파일을 열어, 내용을 확인해보면 다음과 같이 공격자가 "JuicyPotato" 도구를 실행한 흔적을 다수 확인할 수 있으며, 해당 파일에 대한 탐지명과 해시 값을 모두 확인할 수 있다.

