

[INCOGNITO CTF WriteUp]

팀명: F-Active

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
d562d36f3f1ab5f1c96d6532dfdbeedc12491ce1	True	c:\windows\system32\compattelrunner.exe
11eba7b1e26cc7d492a2c161ac48370811d0b01e	True	c:\windows\system32\csrss.exe
05d74408a9899054ff5cea5dac98858062e3250e	True	c:\windows\system32\devicecensus.exe
668c40bb6c792b3502b4eefdb0916febcb8dbd5182	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 공격자의 행위를 파악할 수 있다. “Windows Defender” 로그는 이벤트 로그에서도 확인할 수 있으나, 공격자는 이벤트 로그를 모두 삭제하여, 이벤트 로그에서 확인할 수 있는 내용은 존재하지 않는 상태이다.

이름	수정된 날짜	크기
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-Nvdimmm%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

Start Page

1 : Microsoft Wi...

Add Filter

Viewpoints

Flat Message List

Add Columns

Color Rules

Find Message

Go To Message

Layout

Find In Grouping Viewer

Export

Remove







Apply

Enter a filter expression, such as:
tcp.port==80
*address==192.168.1.1

Library

History

Right click on any column header and select 'Group' to create a grouping.

Timestamp	EventID	Summary
 2021-08-20T01:04:13.1878097	2010	Microsoft Defender 바이러스 백신이(가) 동적 보안 인텔리전스 서비스를 사용하여 컴퓨터 보호를 위한 추가 보안 인텔리전스를 검색했습니다.
 2021-08-20T01:04:13.1881350	2010	Microsoft Defender 바이러스 백신이(가) 동적 보안 인텔리전스 서비스를 사용하여 컴퓨터 보호를 위한 추가 보안 인텔리전스를 검색했습니다.
 2021-08-20T01:11:23.3590440	2000	Microsoft Defender 바이러스 백신 보안 인텔리전스 버전이 업데이트되었습니다.
 2021-08-20T01:11:23.3596797	2000	Microsoft Defender 바이러스 백신 보안 인텔리전스 버전이 업데이트되었습니다.
 2021-08-20T01:11:23.8401113	5007	Microsoft Defender 바이러스 백신 구성이 변경되었습니다. 예기치 않은 이벤트인 경우에는 맬웨어의 결과일 수 있으므로 설정을 검토하십시오.
 2021-08-20T01:11:23.8417446	5007	Microsoft Defender 바이러스 백신 구성이 변경되었습니다. 예기치 않은 이벤트인 경우에는 맬웨어의 결과일 수 있으므로 설정을 검토하십시오.

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.

data_collector > data_collector > ProgramData > Microsoft > Windows Defender > Support				▼	↺
이름	수정된 날짜	유형	크기		
\$I30	2021-08-20 오전 12:10	파일	4KB		
MPDetection-20210820-001027.log	2021-08-20 오전 12:10	텍스트 문서	1KB		
MPDeviceControl-20210820-001027.log	2021-08-20 오전 12:10	텍스트 문서	1KB		
MPLLog-20201119-084733.log	2021-08-20 오전 12:10	텍스트 문서	248KB		
MpWppTracing-20210820-001031-00000003-ffffffff.bin	2021-08-20 오전 12:10	BIN 파일	300KB		
MpWppTracing-20210820-001031-00000003-ffffffff.bin.copy0	2021-08-20 오전 1:08	COPY0 파일	0KB		

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.

MPLLog-20201119-084733.log - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
<div> <div>FileName:C:\Temp\WJP.exe</div> <div>SHA1:668c40bb6c792b3502b4eefd0916fbc8dbd5182</div> </div> <div> Internal signature match:subtype=Lowfi, sigseq=0x00001080F7BAEC99, sigsha=f66aaf765db759aeb82a1a4346833b819eea938, cached=true, source=0, resourceid=0x91f62da7 Internal signature match:subtype=Lowfi, sigseq=0x00007E786A9CA8C2, sigsha=b7c41d9d009e08a4f7ea849b913750706228ccb5, cached=true, source=0, resourceid=0x91f62da7 FP supression checks: 2021-08-19T15:08:20.645Z CheckTrusted=true (Sigseq=0x1667b3a21a00), CheckLimit=true, IsNotRevokedCertSig=true, IsNotFpCheckDisabledSig=true, IsSignedFileCheck=false, IsNotExcludedCertificate=true (FriendlySigSeq=0x0) 2021-08-19T15:08:20.645Z DETECTION_CLEANEVENT MPSOURCE_REALTIME MP_THREAT_ACTION_QUARANTINE 0x0 HackTool:Win64/JuicyPotato file:C:\Temp\WJP.exe; 2021-08-19T15:08:20.645Z [Cloud] SubmitReport(CMpSpyNetReportContext - post clean) 2021-08-19T15:08:20.645Z [Cloud] Start of cloud request. 2021-08-19T15:08:20.645Z [Cloud] Queued cloud request. 2021-08-19T15:08:20.645Z [Cloud] Queued cloud request. 2021-08-19T15:08:20.645Z DETECTIONEVENT MPSOURCE_REALTIME HackTool:Win64/JuicyPotato file:C:\Temp\WJP.exe; Beginning threat actions Start time:08-20-2021 00:08:20 Threat Name:HackTool:Win64/JuicyPotato Threat ID:2147740472 Action:quarantine </div>