악성코드 샘플 분석

dgrep.exe

리팩토링 18 주차

목차

개요 2

목적 2

대상 파일 2

테스트 환경 2

분석 도구 2

분석 3

기초분석 3

정적분석 4

패킹(Packing) 여부 4

파일 내부 문자열 분석 4

동적분석 7

실행되는 프로세스 7

각 프로세스의 동작 7

네트워크 분석 9

결론 10

대응 방안 10

개요

목적

본 문서에서는 악성코드 샘플인 dgrep.exe파일을 분석 도구를 이용해 정적, 동적 분석하여 그 결과에 대한 분석을 진행할 것입니다.

대상 파일

(사진 1) dgrep.exe 아이콘

본 문서에서 분석하는 dgrep.exe의 아이콘은 (사진 1)과 같으며 MD5 해시값이 "68af0599e74d36bc2f39a2710754082c"인 파일을 지칭합니다.

테스트 환경

본 문서에서 해당 악성코드를 테스트한 환경은 Windows 7 Home Premium K 64bit 환경에서 Windows 7 서비스 스택 "kb4474419", "kb4490628"을 업데이트한 후 진행하였습니다.

분석 도구

본 문서에서 분석에 사용한 도구들과 그 설명은 하단 표를 참고하십시오.

도구 이름	역할
VirusTotal	무료로 파일 검사를 할 수 있는 웹 서비스
ExeinfoPE	PE(Portable Executable)형식 파일의 속성을 확인할 수 있는 도구로 파일의 패킹 여부와 컴파일러를 확인 가능
PEiD	PE형식 파일의 속성을 확인할 수 있는 도구로 파일의 패킹 여부와 컴파일러를 확인 가능
GUnPacker	패킹되어 있는 파일을 언패킹할 수 있는 도구
PEView	PE형식 파일의 구조와 내부 컴포넌트를 확인할 수 있는 도구
Process	현재 실행 중인 프로세스, DLL 프로세스에 대한 정보를 표시하는 도구

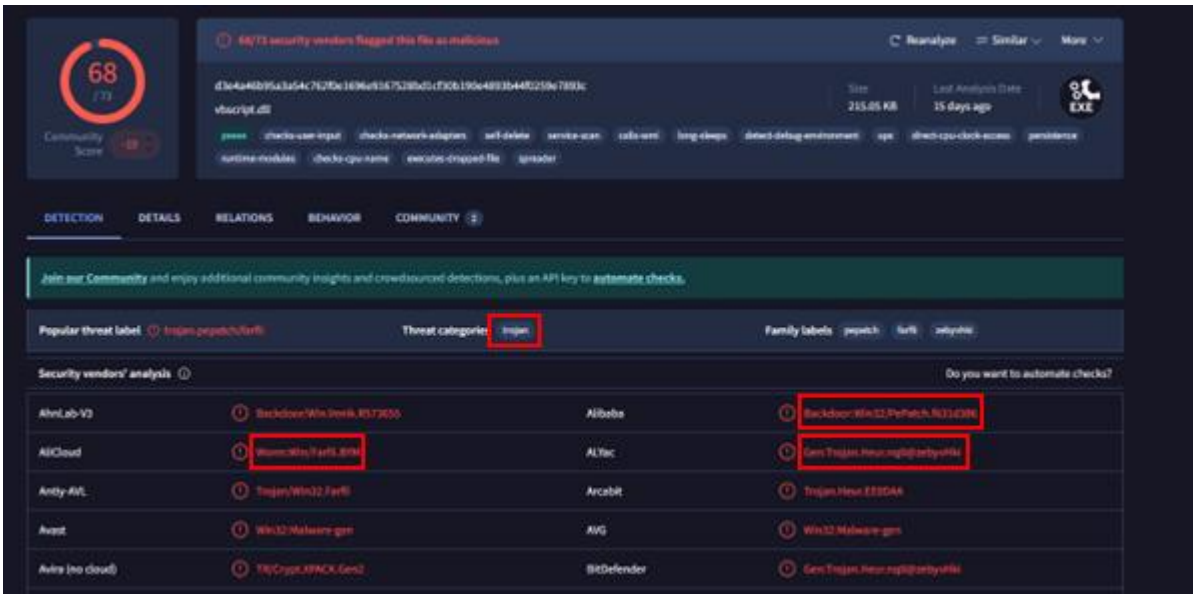
Explorer	
Process Monitor	실시간 파일 시스템, 레지스트리, 프로세스, 스레드 작업을 보여주는 모니터링 도구
System Explorer	의심스러운 파일의 검사, 시스템에 있는 연결, 열린 파일 등의 정보 표시, 스냅샷을 찍어서 악성 파일의 실행 전후를 비교하는 등의 시스템 전반의 정보를 감시, 추적할 수 있는 도구
Autoruns	윈도우 운영체제 부팅 시, 특정 프로그램이 실행될 시 자동으로 실행되는 프로그램에 대한 정보를 표시하는 도구이며 스냅샷을 찍어 악성 파일 실행 전후의 레지스트리 변경 비교 가능
Cport	현재 열려 있는 모든 TCP/IP, UDP 포트 목록을 표시하는 네트워크 모니터링 도구
Wireshark	네트워크 패킷 캡처 및 분석 도구

(표 1) 분석 도구

분석

기초분석

본격적인 분석에 들어가기 전 virustotal 웹 서비스를 이용하여 기초적인 데이터를 살펴보았습니다.



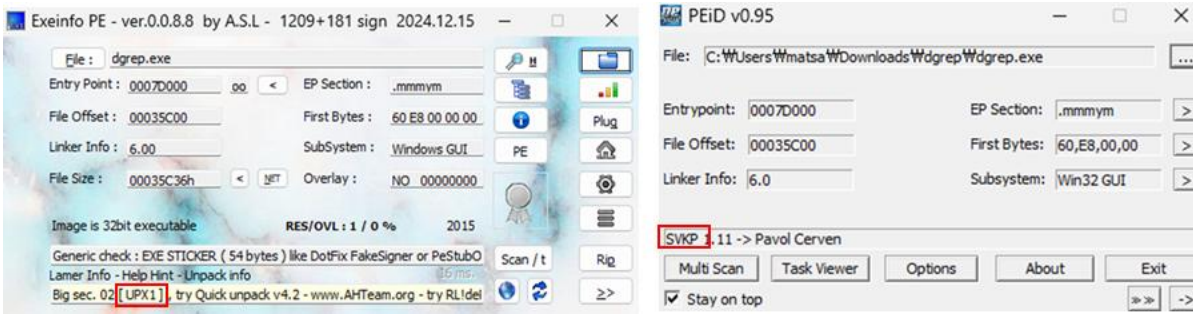
(사진 2) dgrep.exe virustotal 분석 결과

분석 결과를 살펴보면 본 문서에서 분석하는 파일은 트로이목마 계열의 위협이 있다고 판단되고 있습니다. 총 73개의 바이러스 엔진 중에서 68개의 엔진에서 위협을 탐지했으며 트로이 목마, 백도어, 웜 계열의 악성코드로 의심하고 있습니다.

정적분석

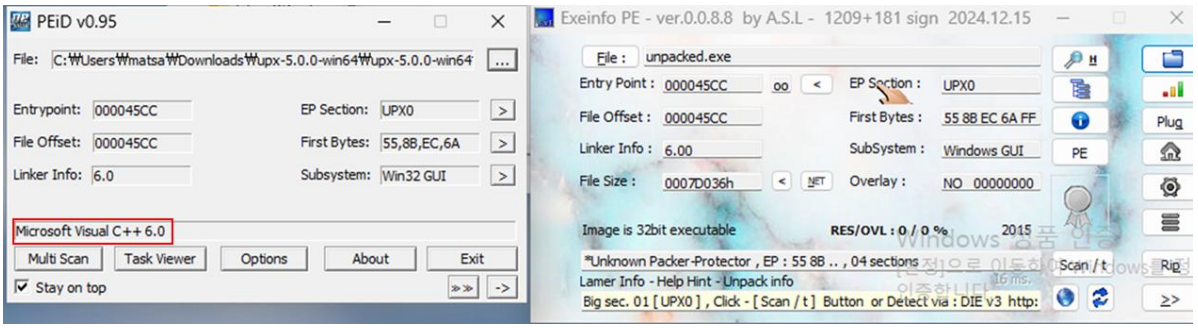
패킹(Packing) 여부

Exeinfo PE와 PEiD를 사용하여 dgrep.exe 파일의 패킹 여부를 확인했습니다.



(사진 3) dgrep.exe Exeinfo PE, PEiD 분석 결과

해당 파일은 UPX1, SVKP 1.11이라는 패킹 도구로 패킹되어 있다는 것을 확인했습니다. 이를 언패킹하기 위해 GUnpacker를 통해 언패킹을 진행했습니다.

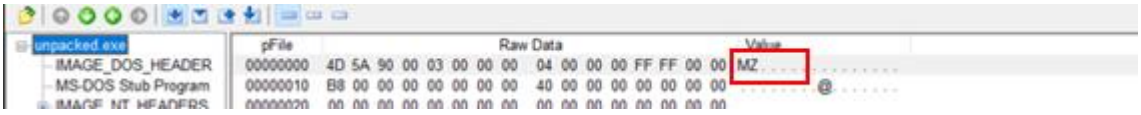


(사진 4) 언패킹 후 Exeinfo PE, PEiD 분석 결과

언패킹 후 다시 분석한 결과 해당 파일은 Microsoft Visual C++ 6.0으로 컴파일된 것을 확인했습니다.

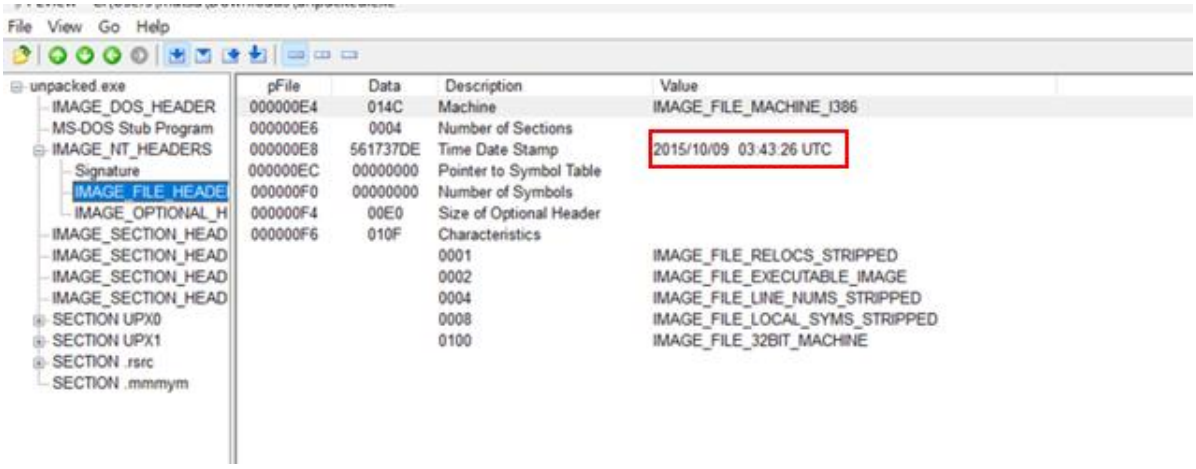
파일 내부 문자열 분석

PE View를 통해 파일의 내부 문자열을 분석했습니다.



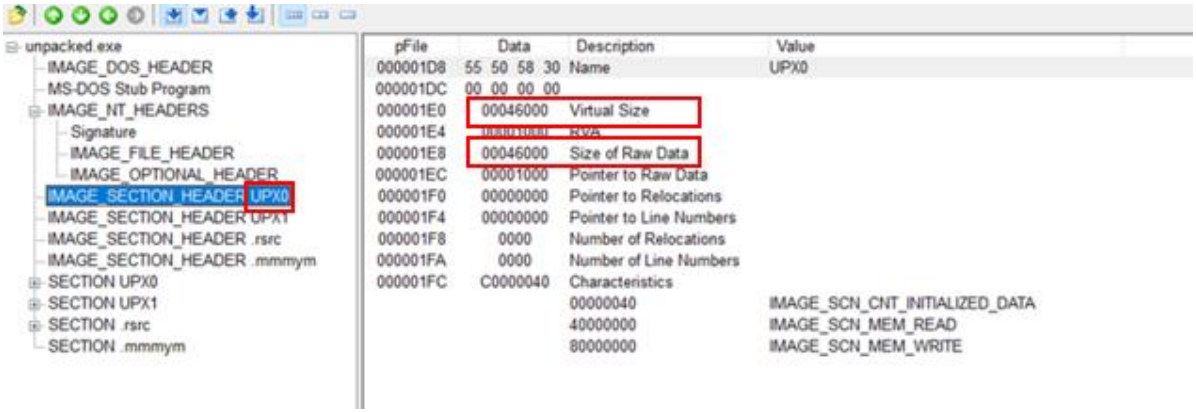
(사진 5) PE View 파일 유형 분석

파일의 유형이 실행 파일임을 확인했습니다.



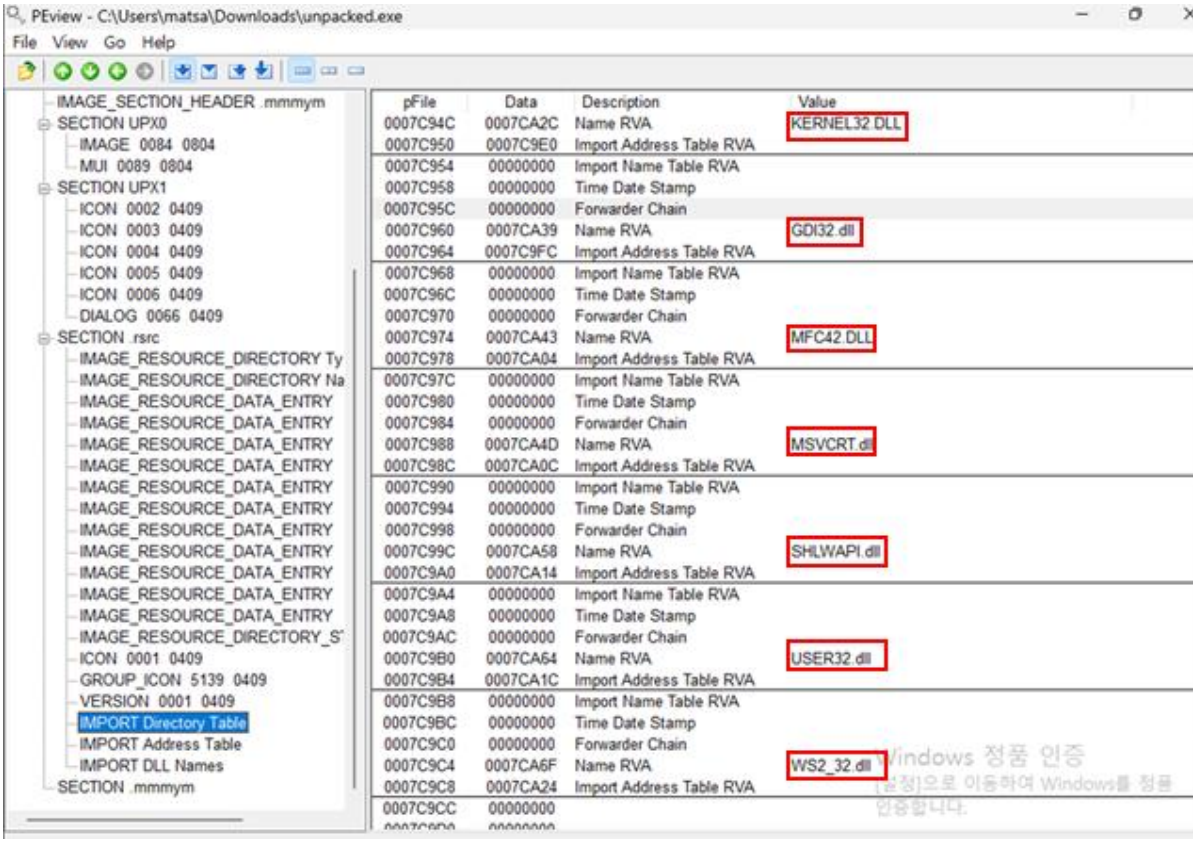
(사진 6) PE View 파일 생성 시간 분석

파일이 2015/10/09에 생성되었다는 것을 확인했습니다.



(사진 6) PE View 패킹여부 분석

Virtual Size, Size of Raw Data 값이 같으므로 파일이 언패킹되었다고 볼 수 있지만 파일 확장자가 UPX0으로 일반적이지 않으므로 GUnPacker를 사용한 언패킹이 일부 되었지만 완전히 안되었다는 것을 확인했습니다.



(사진 7) PE View DLL파일 분석

해당 프로그램이 사용하는 DLL 파일들을 확인했으며 해당 파일들의 동작은 아래 표와 같습니다.

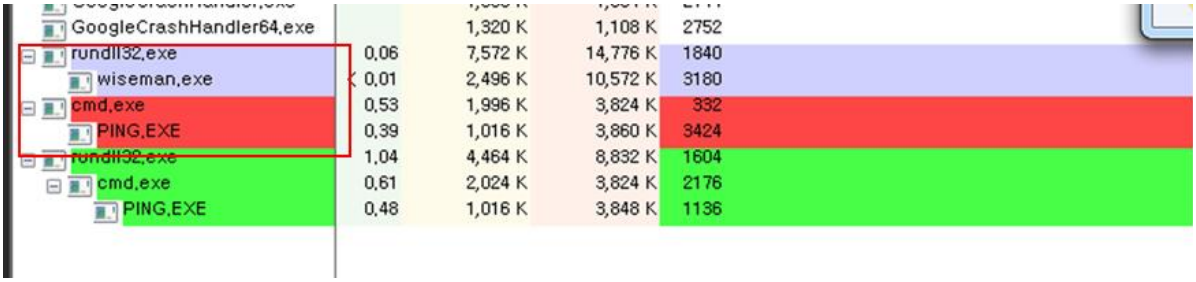
dll파일 이름	역할
Kernel32.dll	하드웨어, 리소스 접근
CGI32.dll	출력장치에 출력
MFC42.dll	윈도우 API 호출
SHLWAPI.dll	파일 경로 조작
USER32.dll	사용자 인터페이스 관련 조작
WS2_32	Windows socket 관리
Vbscript.dll	VBScript를 이용한 PC제어

(표 2) Import된 dll파일

위의 DLL 파일에 import되어 있으므로 해당 dll파일의 동작을 dgrep.exe가 수행할 가능성이 있습니다.

동적분석

실행되는 프로세스



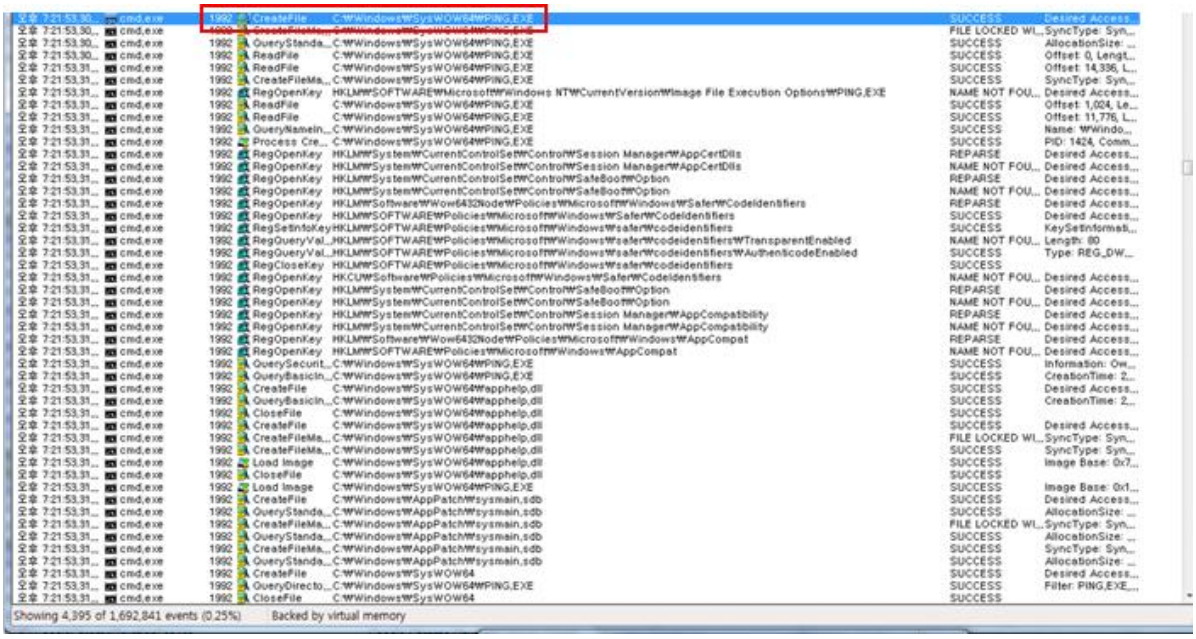
(사진 8) Process Explorer

dgrep.exe를 실행한 직후 Process Explorer를 통해 어떤 프로세스가 생기고 사라지는지를 추적한 결과 dgrep.exe가 cmd.exe, cmd.exe가 PING.exe를 실행하는 것을 확인했으며 rundll32.exe가 실행되고 rundll32.exe가 wiseman.exe를 실행하는 것을 확인했습니다.

그리고 약 1~2초 후 dgrep.exe, cmd.exe, PING.exe가 종료되는 것을 확인했습니다.

각 프로세스의 동작

Process Monitor로 실행되었던 프로세스들의 동작을 살펴봤습니다. 일단 dgrep.exe는 cmd.exe 프로세스를 생성하여 실행시키는 것을 확인했습니다.

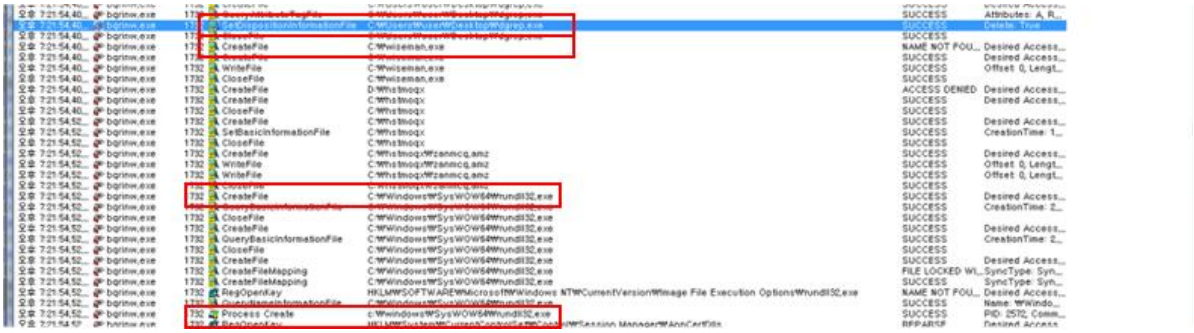


(사진 9) Process Monitor cmd.exe 동작1

dgrep.exe로부터 실행된 cmd.exe는 PING.exe 프로세스를 생성하고 실행하는 것을 볼 수 있습니다.

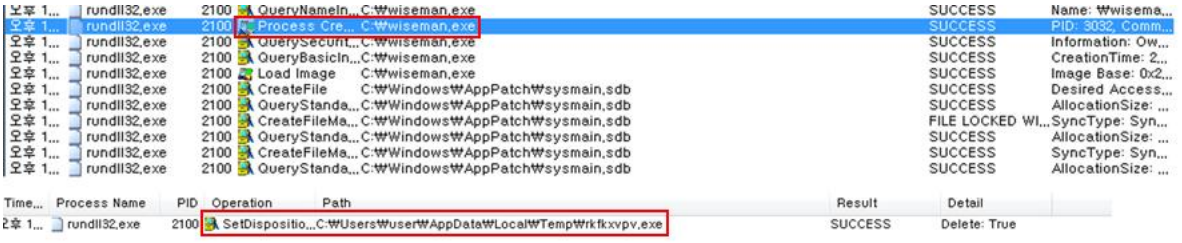
(사진 10) Process Monitor cmd.exe 동작2

또한 cmd.exe는 C:₩Users₩user₩AppData₩Local₩Temp(현재 로그인하고 있는 윈도우 유저의 ₩AppData₩Local₩Temp 디렉토리) 디렉토리에 bqrinw.exe라는 랜덤한 이름의 exe 형식 파일을 생성하고 해당 프로그램의 프로세스를 생성하고 실행하는 것을 확인할 수 있습니다.



(사진 11) Process Monitor bqrinw.exe 동작

cmd.exe에 의해 생성된 bqrinw.exe(파일명은 무작위입니다.)는 SetDispositionInformationFile Operation을 통해 실행된 dgrep.exe파일을 삭제하며 C:₩ 디렉토리에 wiseman.exe라는 파일을 생성합니다. 또한 C:₩Windows₩SysWOW64 디렉토리에 rundll32.exe라는 파일을 생성하며 해당 프로그램의 프로세스를 생성하고 실행하는 것을 확인할 수 있습니다.



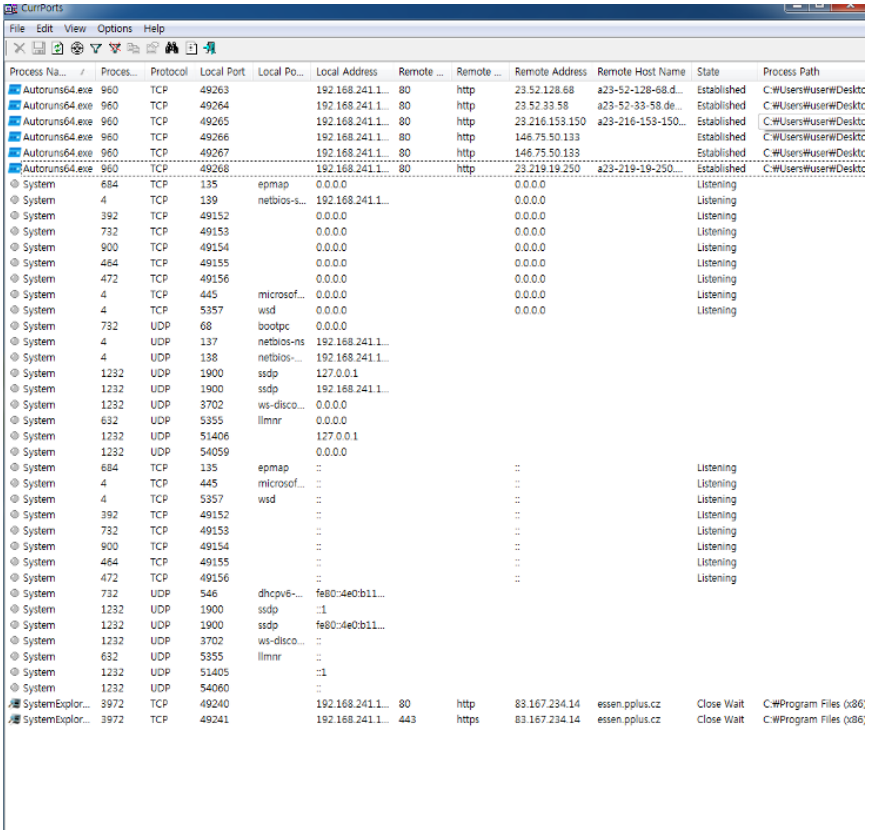
(사진 12) Process Monitor rundll32.exe 동작

Rundll32.exe는 bqrinw.exe가 생성했던 wiseman.exe의 프로세스를 생성하고 실행하는 것을 확인할 수 있으며 자신을 생성하고 실행했던 bqrinw.exe(사진 12의 이름이 다른 것은 2회차 테스트의 사진이기 때문입니다.)를 삭제합니다.

마지막으로 wiseman.exe는 레지스트리를 변경하는 것 외에 특이 사항은 없었습니다.

네트워크 분석

Cport를 사용하여 현재 실행 중인 프로세스가 사용중인 port를 확인했습니다.



(사진 13) Cport

의심되는 port는 없었습니다.

또한 Wireshark를 사용하여 악성코드 실행 후의 패킷을 분석했습니다.

(사진 14) Wireshark

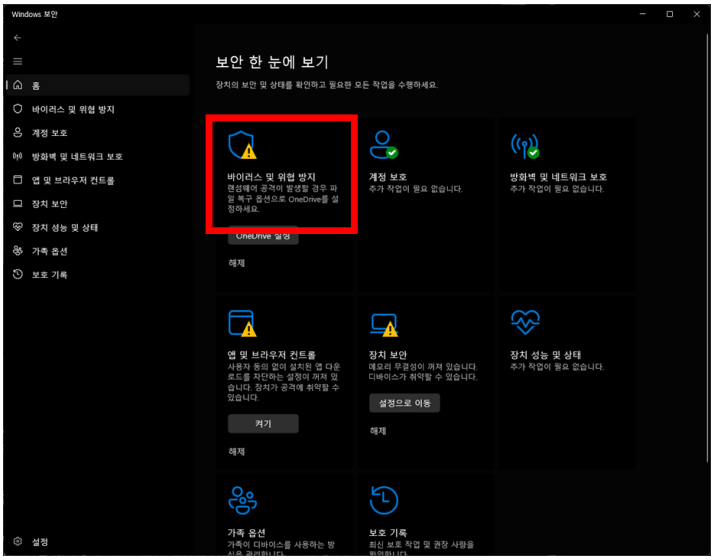
악성코드를 실행한 후 107.163.241.197, 107.163.241.198로 요청을 TCP 연결 요청을 보냈으며 해당 주소에서 답변이 없어서 Retransmission된 것을 볼 수 있습니다.

결론

본 문서에서 분석한 dgrep.exe는 기초분석에 따르면 32비트 환경에서 트로이목마, 웜, 백도어로 동작할 가능성이 있는 악성코드이며 윈도우 7 64bit 환경에서 하드웨어, 출력장치, 윈도우 API, 파일, 사용자 인터페이스, windows socket에 접근할 수 있으며 실행 시 cmd.exe, PING.exe, bqrinw.exe, rundll32.exe, wiseman.exe가 실행되며 dgrep.exe, bqrinw.exe가 삭제됩니다. 그리고 107.163.241.197, 107.163.241.198 TCP 연결 요청을 보내는 것으로 확인되었습니다. 해당 서버가 응답하지 않아 악성 행위를 하는 것은 확인되지 않았지만, 만약 107.163.241.197, 107.163.241.198 주소의 서버가 활성화된다면 언제든지 다시 동작할 수 있는 악성코드입니다.

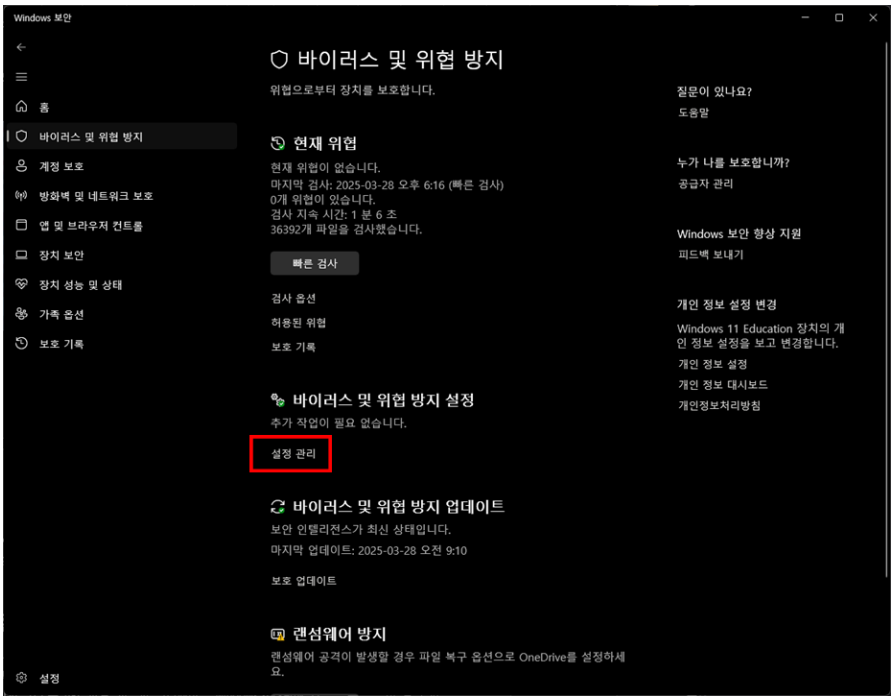
대응 방안

Microsoft Defender를 이용하여 해당 악성코드에 대응할 수 있습니다.



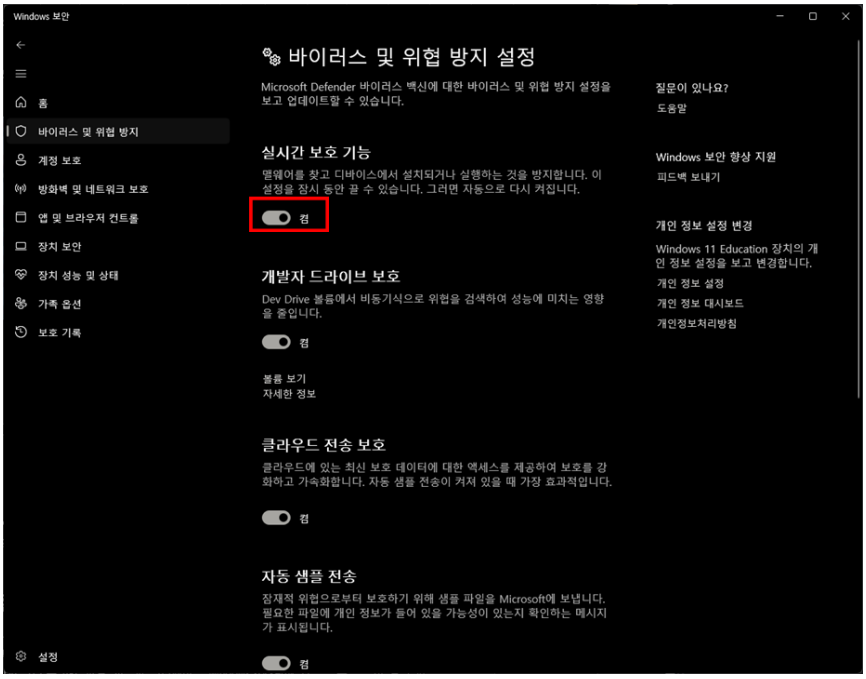
(사진 15) Windows 보안

Windows 11 64비트 환경을 기준으로 "Windows 보안"을 실행하여 (사진 15)의 빨간색 네모 박스로 표시되어 있는 "바이러스 및 위협 방지"를 클릭하여 들어갑니다.



(사진 16) 바이러스 및 위협 방지

다음으로 "바이러스 및 위협 방지 설정" 하단의 "설정 관리" 버튼을 눌러 이동합니다.



(사진 17) 바이러스 및 위협 방지 설정

마지막으로 "실시간 보호 기능" 설정을 "켬"으로 변경하면 됩니다.