악성코드 분석(전라남도 코로나바이러스 대응 긴급 조회.hwp)

By 1q

Published: 2020-04-08 · Archived: 2026-04-05 18:03:01 UTC

[개요]

[1] ASEC 분석팀은 "전라남도 코로나바이러스 대응 긴급 조회.hwp"로 위장한 악성 문서파일을 발견하고 패치했다. 해당 정보를 확인하고 [2] 무료 샌드박스 서비스(any.run)에서 파일을 다운로드 받아 분석을 수행하기로 했다.

해당 악성 문서파일(HWP)은 코로나19 관련 내용으로 정부기관으로 위장하여 유포한 파일이다. CVE-2017-8291 취약점을 이용해 만들어졌으며, Powershell을 이용해 C2 서버에 접근해 2차 유포 파일(EXE)을 다운로드 받은 뒤, 정보유출형 백도어 역할을 수행한다. 현재는 C2가 단절되어 Powershell에서 C2 서버에 접근하지 못하지만, 서버가 다시 살아날 수 있을 가능성도 있기에 주의가 필요하다.

※ 본 게시물에는 단계별로 한글 문서, 쉘코드, 다운로드된 PE 파일의 분석을 수행한 내용이 포함되며, 주관적인 의견이 있을 수 있으니 사실과 다른 내용이 있다면 피드백 부탁드립니다.

※ 참고 : 동일 날짜에 유포된 "인천광역시 코로나바이러스 대응 긴급 조회 (1).hwp", "경찰청 출석요구서.hwp" 2개의 파일과 본 게시물에서 분석하려고 하는 의심 문서와 내부 PostScript Hash 값이 동일한 것으로 보아 Decoy(미끼) 문서만 다르게 활용한 것으로 보임.

인천광역시 코로나바이러스 대응 긴급 조회 (1).hwp : c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b728c

경찰청 출석요구서.hwp : ff4ce7f350b0063c9683499e42028f129195f8d85c372b54f7b52380c64d5ac9

[Hash 값 채증]

총 5가지 파일의 Hash 값을 채증했다.

[1] 악성 문서파일(HWP)

[2] 취약점(CVE-2017-8291)이 존재하는 PostScript 파일

[3] 변환된 PostScript 파일

[4] PostScript 내부에 존재하는 쉘코드 바이너리

[5] 쉘코드에서 다운로드를 수행하는 PE 파일

[악성 문서파일(HWP) 및 쉘코드 분석]

문서파일에는 코로나19 확진자가 발생했다는 허위 내용으로 전라남도 감염병관리지원단을 사칭한 내용이 담겨있다. 최근들어 공격자들은 코로나19 이슈를 활용해 피싱, 랜섬웨어, APT 등을 통해 악용하고 있어 주의가 필요하다.

가상환경에서 한글 파일을 단순히 실행한 결과, 아래와 같이 gbb.exe 프로세스에서 cmd를 이용해 powershell을 직접 수행하는 것을 확인할 수 있다.

[3] hwpscan2를 활용해 문서 파일의 Summary 정보를 확인한 결과, 2020-04-01 15:56분 경에 문서파일이 마지막으로 수정된 것을 확인할 수 있다.

BinData 스토리지의 BIN0005.ps 파일 내부에 "/image <2F78~~~>" 내용이 포함됐다. PostScript는 바이너리를 "< >"로 감싸기 때문에 해당 바이너리가 악성행위를 수행하는 쉘코드라고 의심해 볼 수 있다. 정확한 쉘코드를 얻기 위해서는 한글 파일 자체를 디버깅을 수행하여 추출하는 방법도 존재하지만, 본 게시물에서는 수동으로 진행하도록 하겠다.

위 바이너리를 추출하여 Hxd를 이용해 확인해보면 또 다른 PostScript 파일이 등장한다. 파일의 내용은 CVE-2017-8291 취약점에서 사용되는 것으로, 아래 드래그한 바이너리가 실제 쉘코드이며, 추출하여 분석을 진행하도록 하겠다.

위 바이너리를 확인한 결과, 텍스트(오른쪽) 화면을 육안상으로 봤을 때, Powershell의 DownloadFile API를 활용해 C2 서버에 접근하는 것을 확인할 수 있다.

자세한 내용을 알기 위해 디버깅을 통해 쉘코드를 분석한 결과 아래와 같은 순서로 진행됐다.

1. msvcrt.dll을 로드
2. system() 함수 호출
3. system() 함수의 인자로, powershell의 DownloadFile API를 통해 특정 C2 서버에서 "h1.jpg" 파일을 %temp% 경로에 svchost.exe 파일로 다운로드 및 실행

※ 1차 C2 주소 : http://www.sofa[.]rs/wp-content/themes/twentynineteen/sass/layout/h1[.]jpg (워드프레스 서버 악용)

VirusTotal에서 해당 C2 주소를 확인한 결과, 2개의 파일(h1.jpg와 h2.jpg)이 스캔된 것을 확인할 수 있었다. 32bit와 64bit로 추정은 되지만, 확실하지는 않다. 본 게시물에서는 h2.jpg에 대한 분석을 진행한다.

[유포된 PE 파일 분석]

※ IDA를 통해 정적분석에 치중한 분석 내용입니다.

해당 파일은 C++로 컴파일된 32bit 파일로 확인됐다.

IDA를 이용해 스트링을 확인한 결과, 4개의 C2 주소를 발견할 수 있었다. 3개의 주소는 워드프레스 주소 하위의 server_test.php 파일로 동일했으며, 1개의 파일은 index.php가 존재했다. 이를 활용해 C2 통신을 수행할 수도 있겠다는 생각을 할 수도 있을 것이다.

"Microsoft\\Windows\\WinX\\config.txt" 경로의 파일이 존재하는지 확인 및 새로 생성하여 특정 데이터(0xCF 사이즈)를 덮어씌운다. (데이터가 어떻게 생성되는지는 상세 분석이 필요할 것으로 보임.. 상세 디버깅은 나중에 시간이 남으면 추가적으로...)

위에서 작성한 config.txt 파일에 들어가는 내용이며, 특정 인코딩을 통해 평문을 변조한 것으로 보인다.

네트워크 행위는 IDA에서 잘 해석하지 못하여 디버깅을 통해 잠시 확인해본 결과, C2 서버(kingsvc.cc)에 id, content를 raw 데이터 형태로 timestamp 파라미터를 추가하여 POST 형식으로 전송하는 것을 보인다.

ex) hxxp://kingsvc[.]cc/index.php?timestamp={} | 전송하려는 raw 데이터 : &id={}&content={}

WQL을 사용하여 "ROOT\\CIMV2"의 "Win32_OperatingSystem"에 존재하는 {Caption, CSName, MUILanguages, Version, OSArchitecture} 정보를 쿼리한다. 결과 값은 아래 로그 형태로 만들어진다.

[Operating System Information] - 시스템 관련 정보 탈취

OS Name:{}

Host Name:{}

MUI Lacale:{}

OS Version:{}

OS Type:{}

WQL을 사용하여 "ROOT\\CIMV2"의 "Win32_NetworkAdapterConfiguration"에 존재하는 {Description, DefaultIPGateway, DHCPEnabled, DNSServerSearchOrder, IPAddress, IPEnabled, IPSubnet} 정보를 쿼리한다. 결과 값은 아래 로그 형태로 만들어진다.

[Network Information] - 네트워크 관련 정보 탈취

Description:{}

Default Gateway:{}

DHCP Enabled:{}

DNS Server:{}

IP Address:{}

MAC Address:{}

WQL을 사용하여 "ROOT\\SecurityCenter2" or "ROOT\\SecurityCenter"의 "AntivirusProduct"에 존재하는 {DisplayName, TimeStamp} 정보를 쿼리한다. 결과 값은 아래 로그 형태로 만들어진다.

[Installed Anti Virus Programs] - 설치된 백신 정보 탈취

Name:{}

Update Date:{}

WQL을 사용하여 "ROOT\\CIMV2"의 "Win32_Process"에 존재하는 {Caption, ProcessID, Description} 정보를 쿼리한다. 결과 값은 아래 로그 형태로 만들어진다.

[Running Processes] - 실행되고 있는 프로세스 정보 탈취

Caption:{}

Process ID Description:{}

Command:{}

위 정보들은 아래 코드의 WQL을 통해 쿼리가 수행된다.

WQL : Windows Management Instrumentation 쿼리 언어는 Microsoft의 CIM 쿼리 언어 구현으로, 분산 관리 태스크 포스의 공통 정보 모델 표준에 대한 쿼리 언어

사용자 계정, 컴퓨터 계정, 국가별지역 정보를 탈취

해당 악성코드에서 Thread 함수를 분석한 결과, 총 5개의 함수가 존재했다. 각 세부내용은 아래와 같다.

StartAddress : ReadFile API를 통해 연결된 Pipe에서 데이터를 읽은 뒤 버퍼에 저장하고, SetEvent API를 통해 이벤트를 생성한다.

sub_40B530 : 인자로 받은 특정 스레드 핸들을 종료시킨 후, CreateToolhelp32Snapshot API 함수를 통해 특정 프로세스를 탐색한다.

sub_4021E0 : 4개의 C2 주소를 특정 버퍼에 저장한 후 kingsvc.cc 주소에 3개의 파라미터(id, content, timestamp)를 추가적으로 생성하고 POST 형태로 전송한다.

sub_40CAB0 : URLDownloadToFileW API 함수를 통해 C2 서버로부터 악성코드를 다운로드 받은 뒤, CreateProcessW API 함수를 통해 받은 파일을 실행한다. 그 이후 프로세스, 스레드 핸들 종료 및 파일을 삭제한다.

sub_40E770 : GetAsyncKeyState, GetKeyState, GetWindowTextW API 함수를 통해 키로깅 관련 행위를 수행하는 것으로 예상된다.

Exports 함수 확인결과, ReflectiveLoader, getVersion 함수가 확인됐다. ReflectiveLoader 함수는 파일로 존재하는 바이너리(보통 DLL)를 메모리에서 바로 실행하는 기능을 가지고 있다고 한다. 내/외부 벤더 보고서에도 악성코드에서 주로 사용하는 방법이라고 명시되어 있다. 주관적인 의견으로, C2 서버에서 추가적으로 추가 파일(DLL)을 다운로드 받아 해당 Exports 함수를 수행할 것으로 예상된다.

[결론]

본 게시물에서는 "전라남도 코로나바이러스 대응 긴급 조회.hwp" 분석을 수행했다. 내부적으로 한글 문서 구조, PostScript, 쉘코드, PE 파일 등을 분석하는 시간을 가졌다. 5개의 C2 주소를 확인했으며, 2개의 주소

만 이용됐다. 나머지 3개의 C2는 테스트 목적으로 만들어진 것인지는 확실하진 않다. 결론적으로, 정보유출형 백도어로 확인됐으며, 해당 내용 관련 메일을 수신 받았을 경우 주의할 필요가 있다.

[IOC]

-
- **hxxp://www.kingsvc[.]cc/index[.]php**
- **hxxp://www.sofa[.]rs/wp-admin/network/server_test[.]php**
- **hxxp://www.afuocolento[.]it/wp-admin/network/server_test[.]php**
- **hxxp://www.mbrainingevents[.]com/wp-admin/network/server_test[.]php**
- **Microsoft\\Windows\\WinX\\config.txt**
- **3edd95d6ecf200ecbafd259e15f321353e4c4b7b15a536b0b8066a2ad647460f**
- **a1d59162664163a16502e33286cd8d54b9f5c713325b570e8db493edf55d99f9**
- **88c168cd261dabea1b7223e8c05042be7e0505dedf6fd5effea90ae42e127968**
- **7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26**
- **ca47eb3a62a19e378b15b5714fcf61cfec528d8e27a71ed414d1128658671c8c**
- **c0bd35a36ea5227b9b981d7707dff0e2c5ca87453a5289dc4a5cd04c7e8b728c**
- **ff4ce7f350b0063c9683499e42028f129195f8d85c372b54f7b52380c64d5ac9**

[Reference]

-
-
-
