Wireshark · 프로토콜 계층 통계 · c11.pcap

프로토콜	패킷 비율	패킷	바이트 비율	바이트	비트/초	최종 패킷	최종 바이트	최종 초당 비트 수	PDU
Frame	100.0	544	100.0	256675	61 k	0	0	0	544
Ethernet	100.0	544	3.4	8742	2084	0	0	0	544
Logical-Link Control	0.2	1	0.0	3	0	0	0	0	1
Internetwork Packet eXchange	0.2	1	0.0	30	7	0	0	0	1
Service Advertisement Protocol	0.2	1	0.1	130	31	1	130	31	1
Internet Protocol Version 6	0.7	4	0.1	160	38	0	0	0	4
User Datagram Protocol	0.2	1	0.0	8	1	0	0	0	1
DHCPv6	0.2	1	0.0	76	18	1	76	18	1
Internet Control Message Protocol v6	0.6	3	0.0	96	22	3	96	22	3
Internet Protocol Version 4	90.4	492	3.8	9840	2346	0	0	0	492
User Datagram Protocol	1.8	10	0.0	80	19	0	0	0	10
Simple Service Discovery Protocol	1.5	8	1.0	2578	614	8	2578	614	8
NetBIOS Datagram Service	0.4	2	0.1	164	39	0	0	0	2
SMB (Server Message Block Protocol)	0.4	2	0.1	238	56	0	0	0	2
SMB MailSlot Protocol	0.4	2	0.0	50	11	0	0	0	2
Microsoft Windows Browser Protocol	0.4	2	0.0	66	15	2	66	15	2
Transmission Control Protocol	88.6	482	5.4	13956	3328	354	10316	2460	482
Hypertext Transfer Protocol	23.5	128	29.9	76693	18 k	87	60395	14 k	128
Media Type	0.2	1	1.7	4371	1042	1	4371	1042	1
Line-based text data	6.4	35	134.8	346082	82 k	35	346082	82 k	35
JPEG File Interchange Format	0.2	1	3.0	7736	1844	1	7736	1844	1
Data	0.2	1	8.1	20742	4946	1	20742	4946	1
Compuserve GIF	0.6	3	0.1	132	31	3	132	31	3
Address Resolution Protocol	8.6	47	0.5	1316	313	47	1316	313	47

대부분 HTTP로 TCP통신 중인 것으로 확인

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
2	0.264221	74.125.127.104	124.137.25.20	TCP	60	80 → 4559 [FIN, ACK] Seq=1 Ack=1 Win=107 Len=0
3	0.997383	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
4	1.997796	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
5	2.487059	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
6	2.919630	74.125.127.118	124.137.25.20	TCP	60	80 → 4564 [FIN, ACK] Seq=1 Ack=1 Win=107 Len=0
7	3.477882	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
8	3.526463	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
9	4.477554	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
10	4.517611	ASUSTekCOMPU_45:8e:…	Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
11	4.814380	124.137.25.20	211.62.35.167	TCP	78	4771 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=0 TSecr=0 SACK_PERM
12	4.818604	211.62.35.167	124.137.25.20	TCP	66	80 → 4771 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
13	4.819481	124.137.25.20	211.62.35.167	TCP	54	4771 → 80 [ACK] Seq=1 Ack=1 Win=262800 Len=0

```
> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: ASUSTekCOMPU_45:8e:42 (00:17:31:45:8e:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ASUSTekCOMPU_45:8e:42 (00:17:31:45:8e:42)
    Sender IP address: 124.137.25.254
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 124.137.25.122
```

3번 패킷

124.137.25.254 IP에서 124.137.25.122 IP를 ARP 프로토콜

dst : broadcast(ff:ff:ff:ff:ff:ff)는 네트워크 상의 모든 노드에게 해당 패킷 전송 의미

Taeget Mac address : 00:00:00:00:00:00은 받는 사람의 MAC주소를 모름을 의미

Opcode : request(1)은 dst에게 내용 요청하는 패킷을 의미

TCP stream

스트림 1

```
  6 2.919630     74.125.127.118      124.137.25.20       TCP      60 80 → 4564 [FIN, ACK] Seq=1 Ack=1 Win=107 Len=0
185 12.920930    74.125.127.118      124.137.25.20       TCP      60 [TCP Retransmission] 80 → 4564 [FIN, ACK] Seq=1 Ack=1 Win=107 Len=0
310 22.921652    74.125.127.118      124.137.25.20       TCP      60 [TCP Retransmission] 80 → 4564 [FIN, ACK] Seq=1 Ack=1 Win=107 Len=0
```

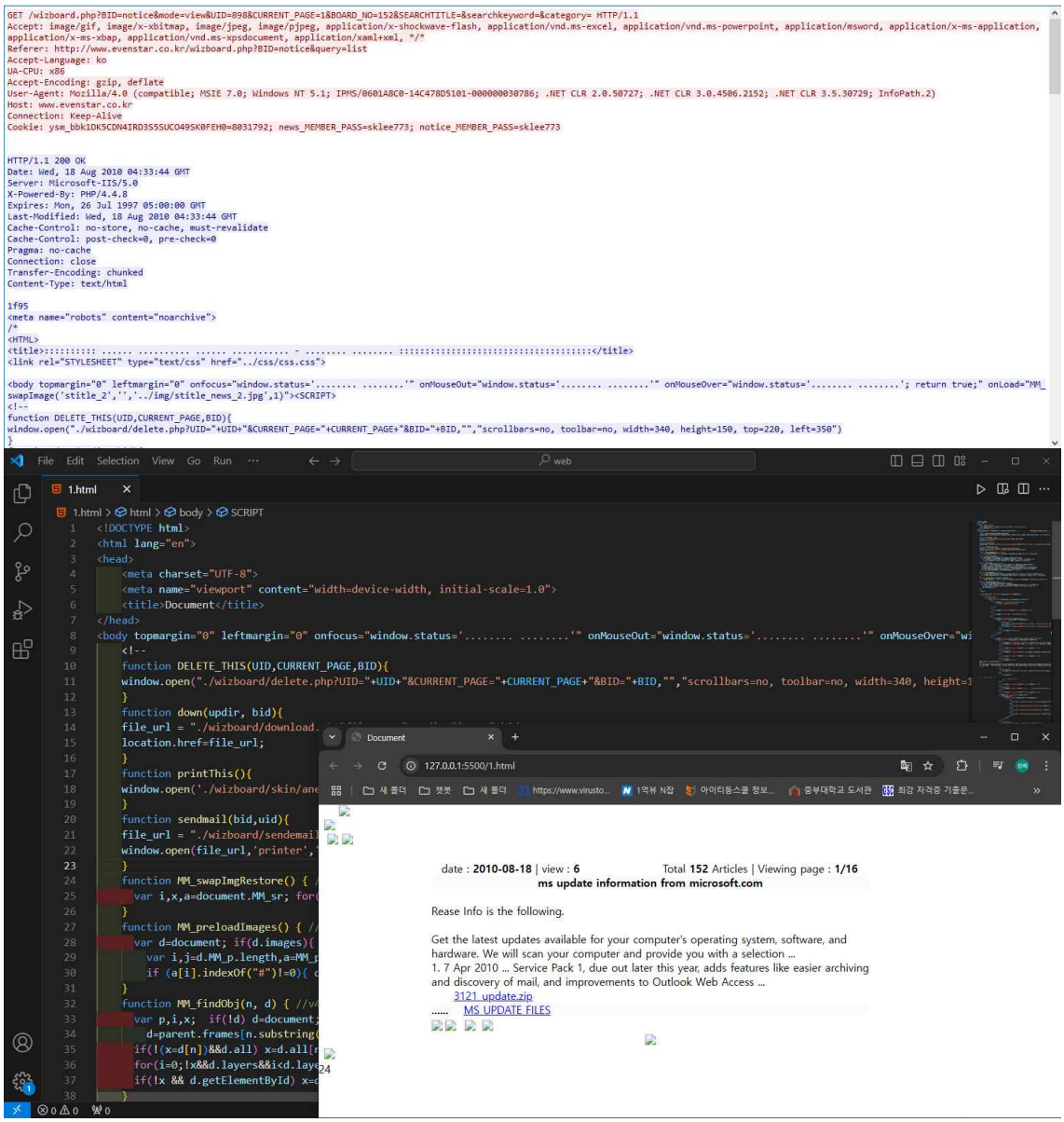
TCP Retransmission : TCP 재전송 패킷

출발지에서 이전 패킷이 목적지로부터 확인되지 않거나 손실되었다고 판단하여 데이터를 다시 전송

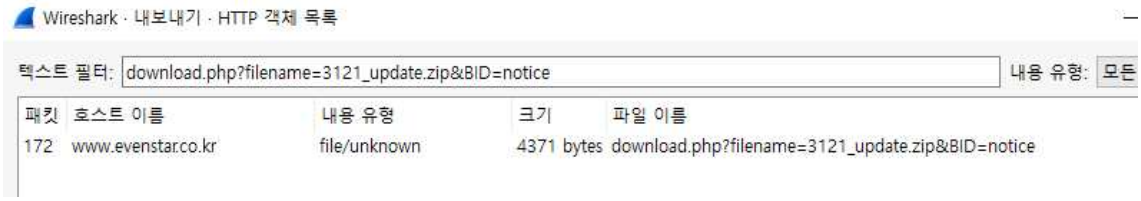
FIN, ACK 플래그가 반복되고 동인한 시퀀스 번호와 확인 응답 번호가 유지

클라이언트가 ack 패킷을 서버에 보내지 않아 연결이 끊기지 않은 것 같음

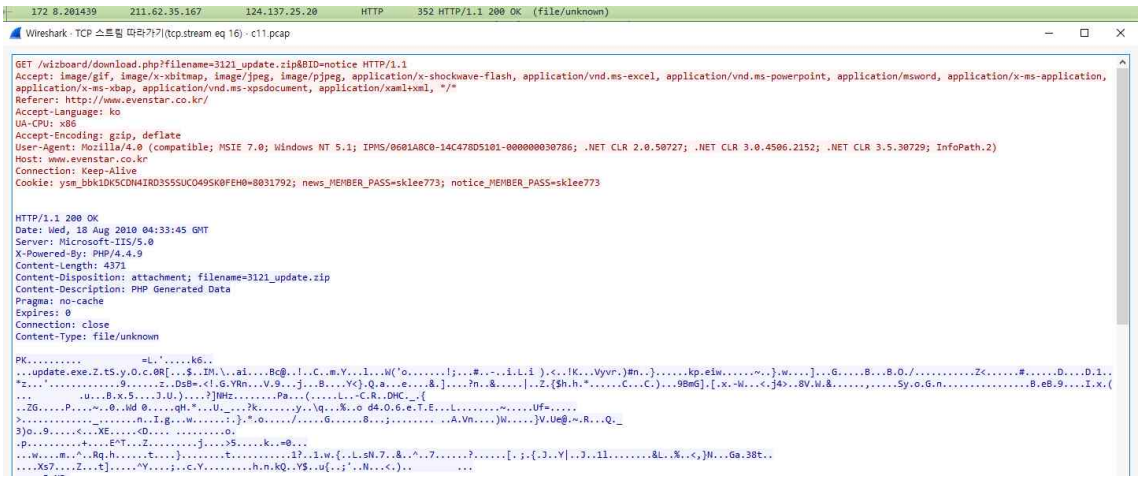
스트림 2



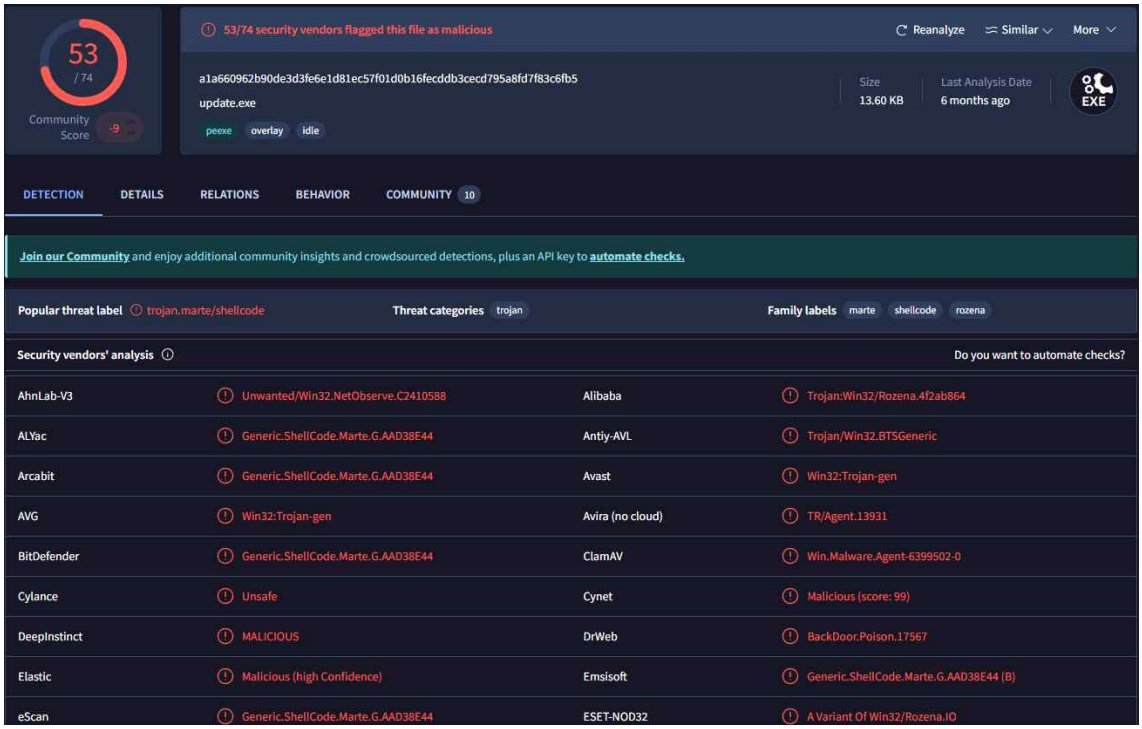
html 코드를 vscode에 입력한 후 사이트의 모습확인
ms 업데이트와 관련된 사이트임을 유추
update.zip 클릭 : wizboard/download.php?filename=3121_update.zip&BID=notice url 주소가 나옴
wireshark 상단의 객체 내보내기에서 패킷 172번임을 확임



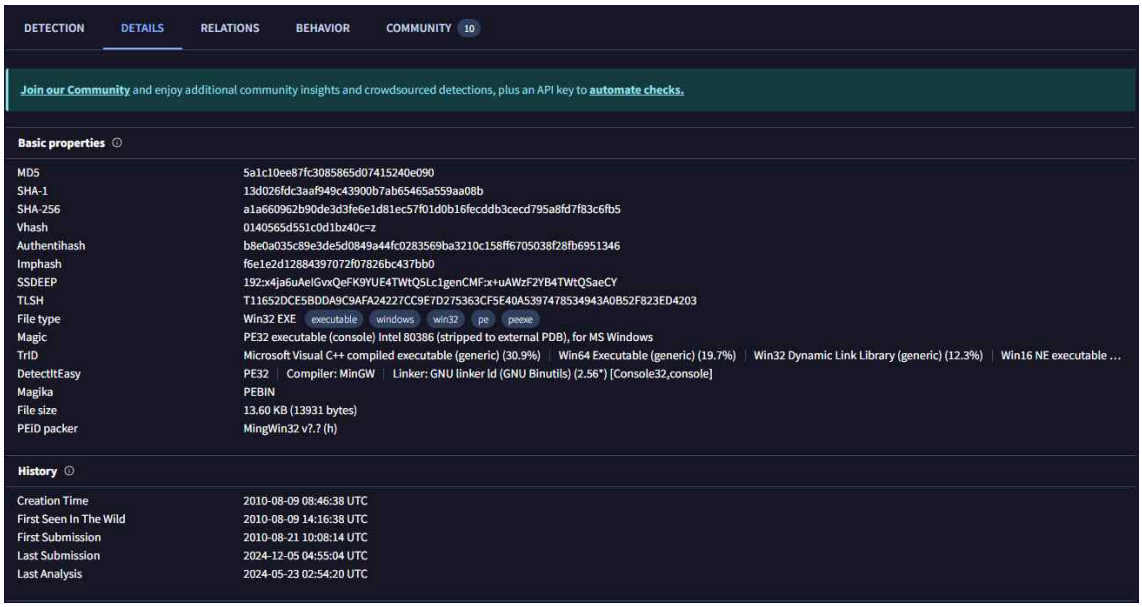
26번 패킷에서 200 = 성공 확인



스트림 16번 패킷 172 번에서 PK = zip 파일 확인
update.exe라는 응용 프로그램 존재



Virus Total에 검색 결과
Trojan을 통해 트로이목마 바이러스검출
= 네트워크 기반의 통신
= 별도의 소프트웨어 설치 후 동작하는 형태임을 유추



해시값 (MD5, SHA-1)을 알 수 있음
DETAILS의 File type을 통해 win32 EXE 파일임을 확인

Portable Executable Info ⓘ

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2010-08-09 08:46:38 UTC
Entry Point	4736
Contained Sections	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	2160	2560	5.12	e07bd02041b390f427b7621f37de956d	72917.04
.data	8192	428	512	5.57	7fb135ef07031e75272d68be8e8110a4	9760
.rdata	12288	64	512	1.09	26f16578d4ef8d5ff8e29cecfc97dbc0	100829
.bss	16384	88	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
.idata	20480	528	1024	2.42	5d47ee049f673738d5f9cefbfb79ab22	129187

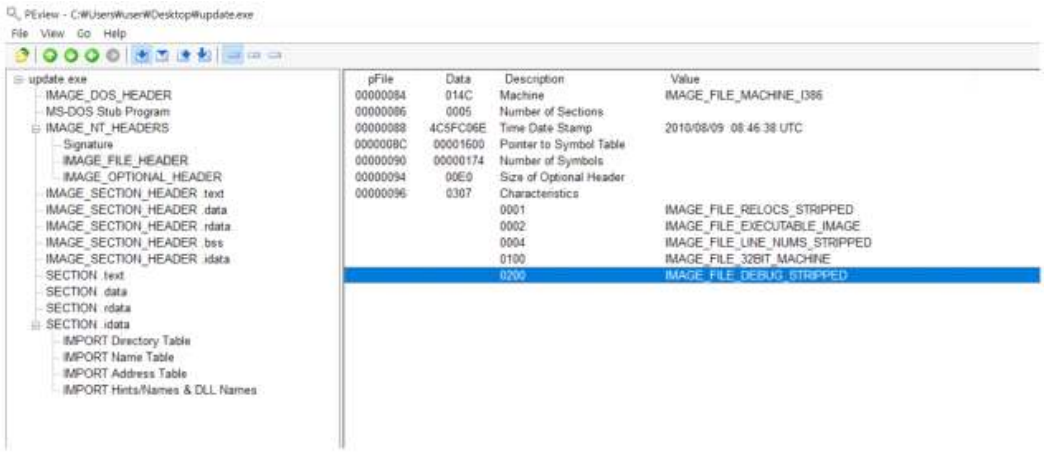
Imports

+ msvcrt.dll
+ KERNEL32.dll

.text, .data, .rdata로 section 구성
imports를 통해 실행파일의 종류가 dll임을 확인

Kernel32.dll : 메모리, 파일, 하드웨어 접근 및 조작
msvcrt.dll : 비주얼 C++ 버전4.2부터 6.0까지의 마이크로소프트 비주얼 C 런타임 라이브러리 비주얼 C++로 컴파일된 프로그램과 C와 C++ 프로그램이 요구하는 일반적인 라이브러리 함수 집합 제공 문자열 처리 및 메모리 할당(C 스타일 입출력 호출 포함)

구조

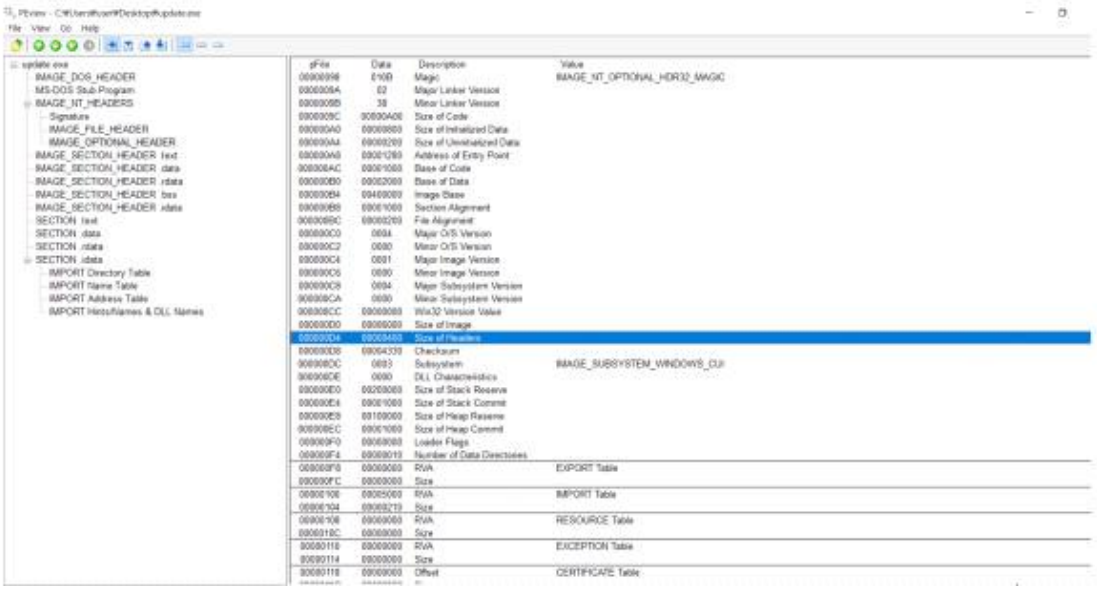


IMAGE_FILE_HEADER = 파일의 전반적인 특성과 실행 환경에 대한 정보

섹션 개수 : 0x0005

time date : 2010/08/09 08:46:38

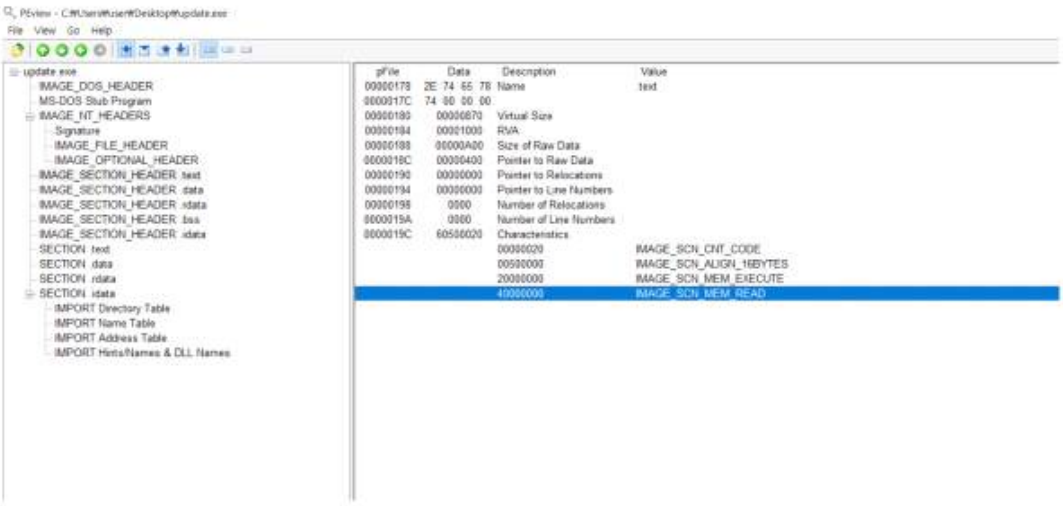
characteristics : 파일 형식 정보, OR연산



IMAGE_OPTION_HEADER = PE 파일 실행에 필요한 세부 정보, 파일의 실행 환경 및 동작 방식을 정의

Magic	0x10B(32구조체), Ox20B(64구조체)
Size Of Code	코드영역(.text)의 크기
Address Of Entry Point	프로그램 시작되는 코드의 주소 RVA값으로 저장 Olly DBG 실행 시 처음 실행하는 주소 (악성코드 시작 지점으로 지정할 수 있다.)
Base Of Code	코드영역이 시작되는 상대 주소(RVA)
Image Base	PE파일이 메모리에 로드되는 시작 주소 EXE(0x400000), DLL(0x10000000)번지로 설정(변경가능), RVA 기준
Section Alignment	메모리에서 섹션의 최소 단위, 시작주소는 이 값의 배수임
File Alignment	파일에서 섹션의 최소 단위, 시작주소는 이 값의 배수임
Size Of Image	PE 파일이 메모리에 로딩될 때 전체 크기
Size Of Header	모든 헤더의 크기
Sub System	1(System Driver), 2(GUI), 3(CUI)
Number of RvaAndSizes	Data Directory의 구조체 멤버 개수
Data Directory	PE파일에서 중요한 역할을 하는 개체들의 위치 및 크기

종류	용도
.text	실행코드
.data	초기화된 전역변수, static 변수
.rdata	Const 변수, 문자열 상수
.bss	전역변수, static변수, 문자열, 기타 상수
.edata	EAT와 관련된 정보
.idata	IAT와 관련된 정보
.rsrc	리소스 정보



IMAGE_SECTION_HEADER .text

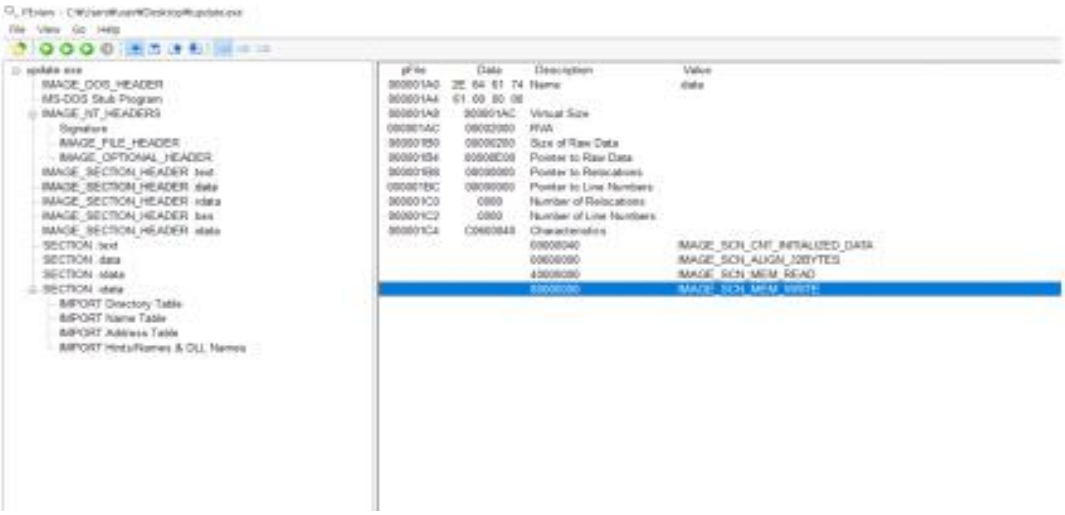
Name : 섹션 이름

RVA : 메모리 섹션의 시작 주소

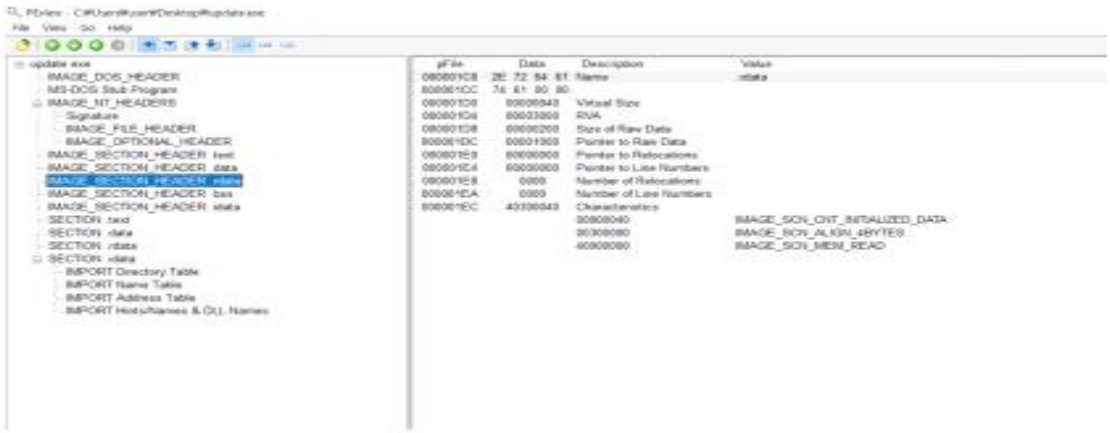
Size Of Raw Data : 파일에서의 섹션 크기

Pointer To Raw Data : 파일에서의 섹션의 시작 위치

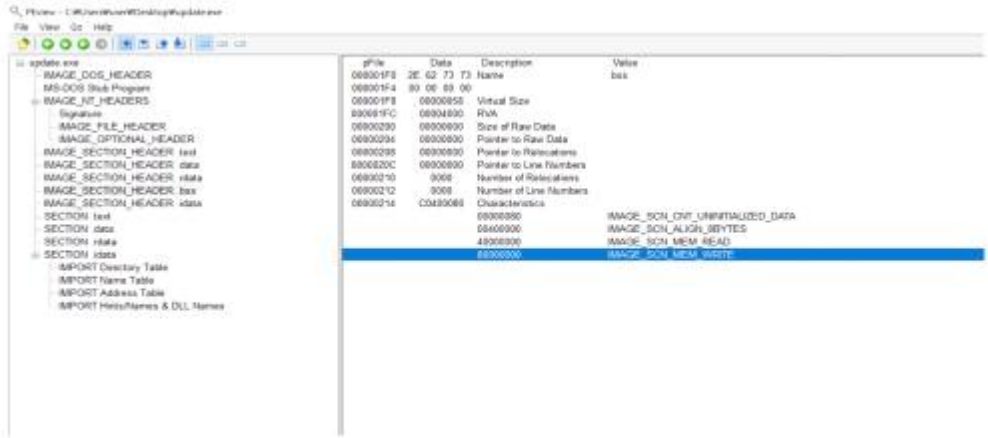
Characteristics : 읽고 쓰기가 가능한 코드 섹션 정보 표시, OR 연산으로 표시 20000000(실행), 40000000(읽기), 20(코드)



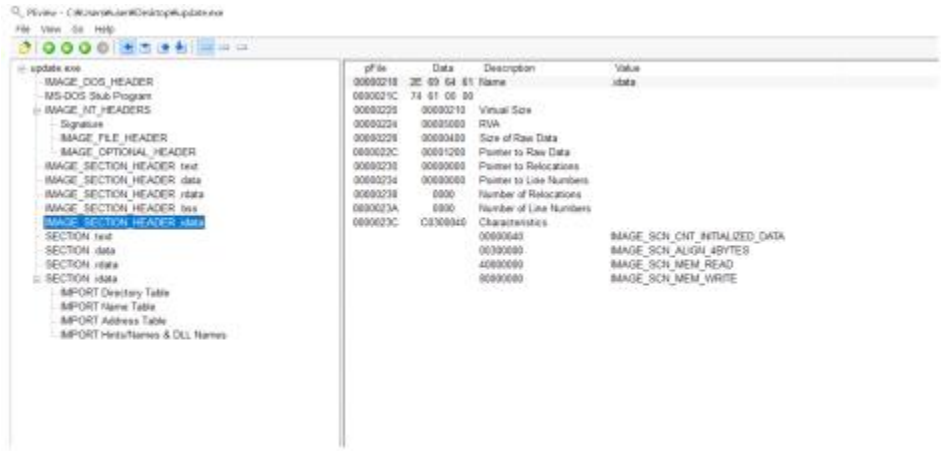
data



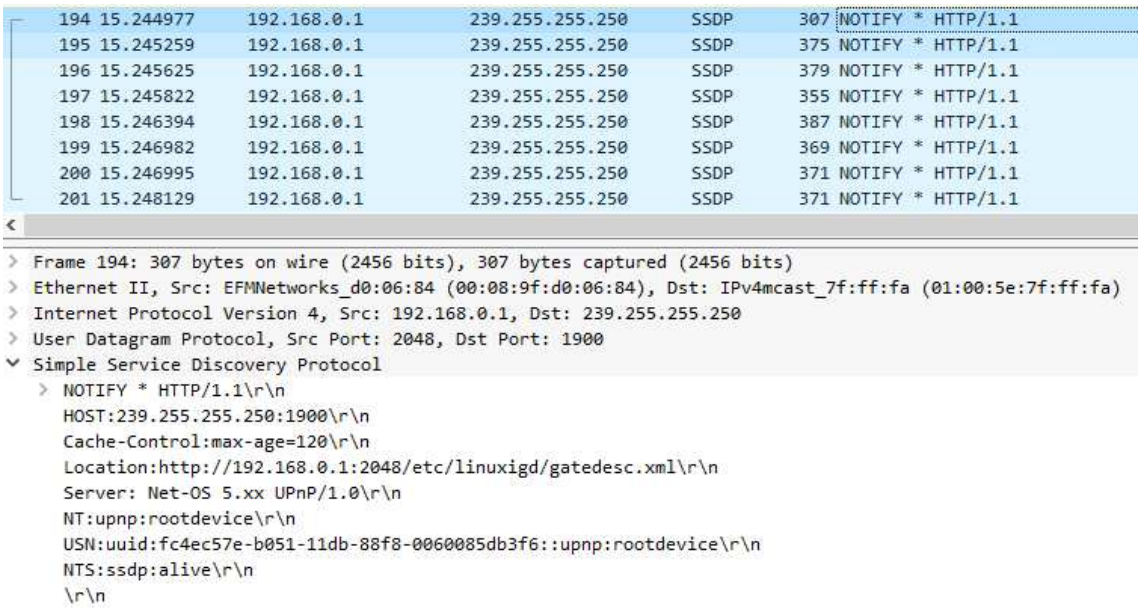
rdata



bss



idata



```
194 15.244977    192.168.0.1     239.255.255.250    SSDP    307 NOTIFY * HTTP/1.1
195 15.245259    192.168.0.1     239.255.255.250    SSDP    375 NOTIFY * HTTP/1.1
196 15.245625    192.168.0.1     239.255.255.250    SSDP    379 NOTIFY * HTTP/1.1
197 15.245822    192.168.0.1     239.255.255.250    SSDP    355 NOTIFY * HTTP/1.1
198 15.246394    192.168.0.1     239.255.255.250    SSDP    387 NOTIFY * HTTP/1.1
199 15.246982    192.168.0.1     239.255.255.250    SSDP    369 NOTIFY * HTTP/1.1
200 15.246995    192.168.0.1     239.255.255.250    SSDP    371 NOTIFY * HTTP/1.1
201 15.248129    192.168.0.1     239.255.255.250    SSDP    371 NOTIFY * HTTP/1.1
```

```
> Frame 194: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits)
> Ethernet II, Src: EFMNetworks_d0:06:84 (00:08:9f:d0:06:84), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 2048, Dst Port: 1900
v Simple Service Discovery Protocol
  > NOTIFY * HTTP/1.1\r\n
    HOST:239.255.255.250:1900\r\n
    Cache-Control:max-age=120\r\n
    Location:http://192.168.0.1:2048/etc/linuxigd/gatedesc.xml\r\n
    Server: Net-OS 5.xx UPnP/1.0\r\n
    NT:upnp:rootdevice\r\n
    USN:uuid:fc4ec57e-b051-11db-88f8-0060085db3f6::upnp:rootdevice\r\n
    NTS:ssdp:alive\r\n
    \r\n
```

SSDP

Simple Service Discovery Protocol

네트워크 서비스나 정보를 찾기 위해 사용하는 네트워크 프로토콜

SSDP를 이용해 DHCP나 DNS와 같은 네트워크 서버 혹은 정적인 호스트 설정 없이 수행 가능

IPv4의 dst : 239.255.255.250

SSDP에서 사용하는 멀티 캐스트의 site-local 주소

SSDP는 UDP 사용 NOTIFY * HTTP/1,1 : SSDP Message는 하나의 시작줄을 가져야 하며 적어도 3개 중에 하나는 포함 하고 있어야 함

NOTIFY * HTTP/1.1

M-SEARCH * HTTP/1.1

HTTP/1.1 200 OK

스트림 17

```
GET /url?q=http://windowsupdate.microsoft.com&sa=X&ei=kWFrTPf_C4H6swPzjdnmBQ&ved=0CDAQ7AgoADAA&usg=AFQjCNE_Wy_qKvouYCkrtFXViIWqcT3BXQ HTTP/1.1
Accept: */*
Referer: http://www.google.co.kr/search?complete=1&hl=ko&q=ms+update&aq=f&aqi=g3g-m1&aql=&oq=&gs_rfai=
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/0601A8C0-14C478D5101-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: www.google.co.kr
Connection: Keep-Alive
Cookie: PREF=ID=b8f32f16fdf21849:U=2f180ad4b4f5c33c:NW=1:TM=1281932300:LM=1281932300:S=RI-_odCc24cVmZGS; NID=37=ZoIEumKkorbPQKpsI1KRTFpxLVEL3wpkgloIfuB3R7RVp4o3WRJpRms2thIsWRkKiJ4oeG9WgEYIro2ERQBvbO45W
6T6yWEUtHrQItkErXyrh5aKkiV_4fXlHbgrdLZo


HTTP/1.1 302 Found
Location: http://windowsupdate.microsoft.com
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Wed, 18 Aug 2010 04:34:02 GMT
Server: gws
Content-Length: 231
X-XSS-Protection: 1; mode=block

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://windowsupdate.microsoft.com">here</A>.
</BODY></HTML>
```

클라이언트가 http://windowsupdate.microsoft.com/에 대해 HTTP GET 요청을 보낸 상황
http://www.google.co.kr/ 사용자가 구글 검색 결과에서 이 URL을 클릭했음
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; ...)
이 요청이 Internet Explorer 7을 실행하는 Windows XP 환경에서 발생했음

HTTP 상태 코드 302 리다이렉션 상태
http://windowsupdate.microsoft.com/ 클라이언트가 이동해야 할 새 URL을 명시

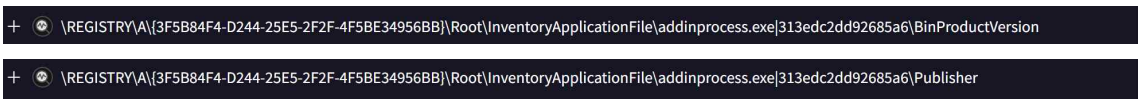
Temp에서 update.exe 실행되고 있음
update.ext 같은 이름은 악성코드가 업데이트 프로그램으로 위장하는 데 자주 사용됨
공격자가 악성 페이로드를 update.exe로 위장하고 임시 폴더에 드롭한 후 실행했을 거라고 추측

- 실행 파일 하이재킹

이 키는 .exe 파일 확장자가 어떤 프로그램과 연결되는지를 정의
.exe 파일은 exefile 프로그래밍 id로 연결, 이는 windows에서 실행 파일로 처리됨을 의미

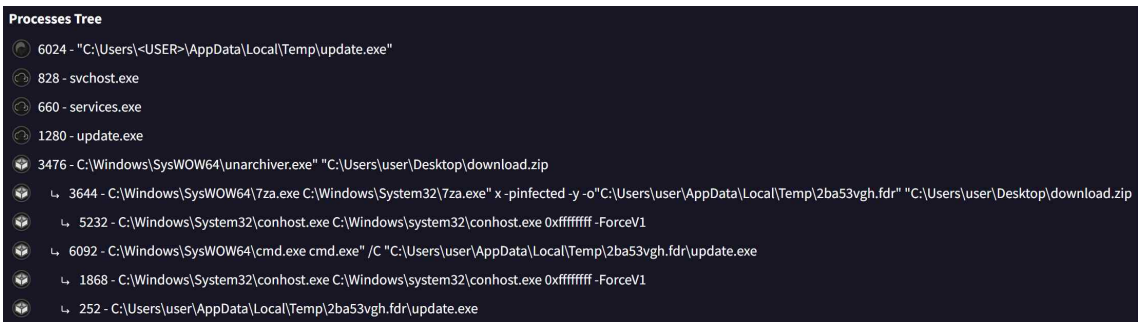
이 키를 조작하여 .exe 파일 실행을 악성 코드로 리디렉션하여 지속성을 확보하는 공격

- 백도어



이러한 키는 일반적인 windows 레지스트리 경로와 다름. addinprocess.exe 및 addinprocess32.e는 실행 파일로 보이고 인벤토리 어플리케이션 파일로 등록되어 있음.

공격자가 addinprocess.exe와 같은 악성 파일을 특정 경로에 배치, 해당 파일을 레지스트리에 등록
BinProductVersion, Publisher 항목을 위조하여 합법적인 소프트웨어처럼 보이게 하여 백도어가 설치되면 공격자가 원격으로 시스템에 접근하고 명령 실행 가능.



processes Tree 분석
cmd.exe를 통해 update.exe가 실행되었으며, 이는 자동화된 백도어 실행 흐름을 나타냄
conhost.exe와 연계된 실행은 명령어 실행 및 제어 기능을 암시

HTTP 상태 코드
1xx : Informational (정보성 응답)
요청이 처리 중임을 알리는 응답
100 Continue : 클라이언트가 요청을 계속 진행해도 된다는 의미
101 Switching Protocols : 클라이언트 요청에 따라 프로토콜을 변결 중임을 알림
102 Processing (WebDAV) : 요청이 처리 중이지만 완료되지 않았음을 나타냄

2xx : Success (성공)
요청이 성공적으로 처리되었음을 나타냄
200 OK: 요청이 성공적으로 처리. (예: GET 요청에 대한 응답 데이터 반환)
201 Created : 요청으로 인해 리소스가 성공적으로 생성. (예: POST 요청)
202 Accepted : 요청이 수락되었지만, 아직 처리되지 않음.
204 No Content : 요청이 성공했으나 응답 본문이 없음.
206 Partial Content : 요청한 데이터의 일부만 제공되었음을 나타냄. (예: 파일 다운로드 중 분할 데이터 전송)

3xx : Redirection (리다이렉션)
클라이언트가 요청한 리소스의 위치가 변경되었음을 나타냄.
301 Moved Permanently : 리소스가 영구적으로 이동했으며, 새로운 URL이 제공.
302 Found : 리소스가 임시로 다른 위치에 있음.
303 See Other : 클라이언트는 다른 URL을 통해 요청을 이어감.
304 Not Modified : 캐시된 리소스가 변경되지 않았음을 알립니다. 클라이언트는 캐시된 데이터를 사용할 수 있음.
307 Temporary Redirect : 리소스가 임시로 이동했으며, POST 방식은 유지됨.
308 Permanent Redirect : 리소스가 영구적으로 이동했으며, POST 방식도 유지.

4xx : Client Error (클라이언트 오류)
클라이언트 요청에 문제가 있음을 나타냄
400 Bad Request : 요청이 잘못되었거나 이해할 수 없음.
401 Unauthorized : 인증이 필요하지만 제공되지 않았거나 실패.
403 Forbidden : 요청이 거부. (권한 없음)
404 Not Found : 요청한 리소스를 찾을 수 없음.
405 Method Not Allowed : 요청한 HTTP 메서드가 지원되지 않음.
408 Request Timeout : 서버가 클라이언트의 요청을 기다리다가 시간 초과.
429 Too Many Requests : 클라이언트가 너무 많은 요청을 보냄.

5xx : Server Error (서버 오류)
서버가 요청을 처리하지 못했음을 나타냄.
500 Internal Server Error : 서버에서 예기치 못한 오류가 발생.
501 Not Implemented : 서버가 요청을 처리할 기능을 지원하지 않음.
502 Bad Gateway : 서버가 잘못된 응답을 받았음. (게이트웨이 문제)
503 Service Unavailable : 서버가 일시적으로 요청을 처리할 수 없음. (과부하, 유지보수 등)
504 Gateway Timeout : 게이트웨이나 프록시 서버가 요청에 대한 응답 시간을 초과.
505 HTTP Version Not Supported : 서버가 요청에서 사용된 HTTP 버전을 지원하지 않음