2024-11-26

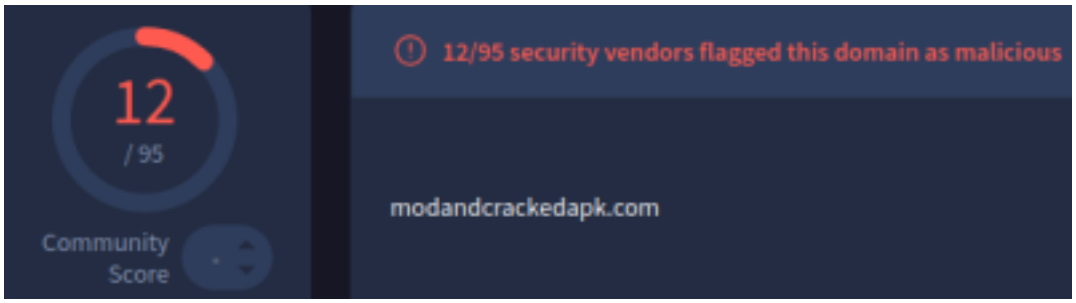
1. alerts 사진을 확인
2. 사진에서 내부 IP가 아닌 주소들을 자세히 확인
- 104[.]117[.]247[.]184 => txt 요청 - S1
- 193[.]42[.]38[.]139 => TLS SNI에 수상한 주소 - S2
- 194[.]180[.]191[.]64 => RAT C2 활동 - S3
- 104[.]26[.]1[.]231 => GeoLocation Lookup 요청 - S4
3. S1과의 패킷 필터링

Protocol	Length	Info
TCP	66	53279 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	66	80 → 53279 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1396 SACK_PERM WS=128
TCP	60	53279 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
HTTP	165	GET /connecttest.txt HTTP/1.1
TCP	60	80 → 53279 [ACK] Seq=1 Ack=112 Win=64256 Len=0
HTTP	241	HTTP/1.1 200 OK (text/plain)
TCP	60	80 → 53279 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
TCP	60	53279 → 80 [ACK] Seq=112 Ack=189 Win=130816 Len=0
TCP	60	53279 → 80 [FIN, ACK] Seq=112 Ack=189 Win=130816 Len=0
TCP	60	80 → 53279 [ACK] Seq=189 Ack=113 Win=64256 Len=0

4. 연결 상태 확인 용도며 악성은 아닌걸로 판단
5. S2와 패킷 필터링
6. 패킷들은 암호화 돼있었지만 SNI를 통해 서버 이름 확인

```
▾ Extension: server_name (len=25) name=modandcrackedapk.com
    Type: server_name (0)
    Length: 25
  ▾ Server Name Indication extension
      Server Name list length: 23
      Server Name Type: host_name (0)
      Server Name length: 20
      Server Name: modandcrackedapk.com
```

7. 바이러스 토탈에 서버 검색



8. 서버를 통해 악성코드를 받았다고 추측 가능
9. S3와 패킷 필터링

No.	Time	Source	Destination	Protocol	Length	Info
20340	67.391300	10.11.26.183	194.180.191.64	HTTP	274	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20341	67.582257	194.180.191.64	10.11.26.183	HTTP	269	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
20342	67.588001	10.11.26.183	194.180.191.64	HTTP	502	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20346	67.789341	194.180.191.64	10.11.26.183	HTTP	360	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
20348	67.889917	10.11.26.183	194.180.191.64	HTTP	328	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20350	68.291089	10.11.26.183	194.180.191.64	HTTP	336	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20572	128.463544	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21145	188.645216	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21153	248.801955	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21246	308.968954	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21295	369.027534	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21337	429.088220	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21352	489.150466	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21364	549.304894	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

10. 여러 패킷을 주고 받는 것을 확인 => 응답이 올 때까지 60초 마다 패킷을 보내며 대기함
11. S4와 패킷 필터링

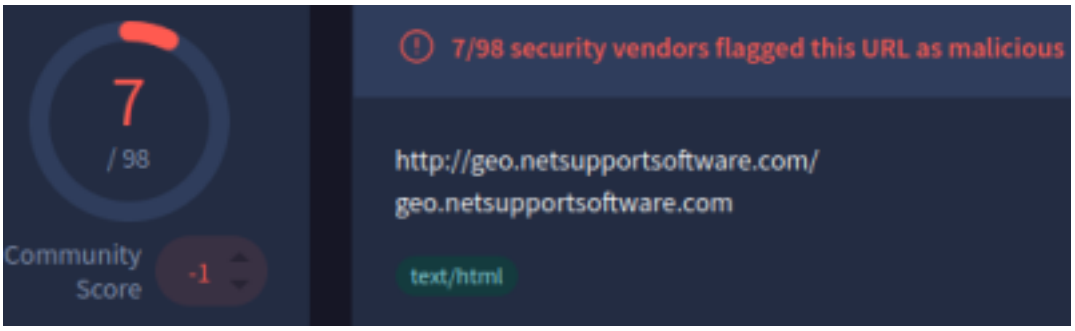
No.	Time	Source	Destination	Protocol	Length	Info
20333	67.229216	10.11.26.183	104.26.1.231	TCP	66	53363 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 S
20334	67.284755	104.26.1.231	10.11.26.183	TCP	66	80 → 53363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=13
20335	67.285017	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
20336	67.286490	10.11.26.183	104.26.1.231	HTTP	172	GET /location/loca.asp HTTP/1.1
20337	67.344368	104.26.1.231	10.11.26.183	TCP	60	80 → 53363 [ACK] Seq=1 Ack=119 Win=65536 Len=0
20343	67.759538	104.26.1.231	10.11.26.183	TCP	1170	80 → 53363 [PSH, ACK] Seq=1 Ack=119 Win=65536 Len=1116 [
20344	67.759632	104.26.1.231	10.11.26.183	HTTP	60	HTTP/1.1 200 OK (text/html)
20345	67.759787	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=119 Ack=1122 Win=260864 Len=0
21140	177.165996	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [FIN, ACK] Seq=119 Ack=1122 Win=260864 Len=0
21141	177.224794	104.26.1.231	10.11.26.183	TCP	60	80 → 53363 [FIN, ACK] Seq=1122 Ack=120 Win=65536 Len=0
21142	177.225106	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=120 Ack=1123 Win=260864 Len=0

12. 연결 도메인 확인

```
Frame 20336: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits
Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Cisco_b8:29:5e
Internet Protocol Version 4, Src: 10.11.26.183, Dst: 104.26.1.231
Transmission Control Protocol, Src Port: 53363, Dst Port: 80, Seq: 1, Ack
Hypertext Transfer Protocol
▾ GET /location/loca.asp HTTP/1.1\r\n
    Request Method: GET
    Request URI: /location/loca.asp
    Request Version: HTTP/1.1
  Host: geo.netsupportsoftware.com\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Response in frame: 20344]
  [Full request URI: http://geo.netsupportsoftware.com/location/loca.asp]
```

hxxp[://]geo[.]netsupportsoftware[.]com/location/loca[.]asp

13. 바이러스 토탈에서 악성 도메인 확인



14. 시간대 별로 패킷들 확인

필터: ip.addr == 104[.]26[.]1[.]231 or (ip.addr ==194[.]180[.]191[.]64 and http) or (ip.addr == 193[.]42[.]38[.]139)

20324	66.684321	10.11.26.183	193.42.38.139	TCP	60	53360 → 443 [ACK] Seq=1196 Ack=5284679 Win=523520 Len=0
20325	66.684442	193.42.38.139	10.11.26.183	TLSv1.3	1411	Application Data, Application Data
20326	66.684442	10.11.26.183	193.42.38.139	TCP	60	53360 → 443 [ACK] Seq=1196 Ack=5286055 Win=524800 Len=0
20327	66.684462	10.11.26.183	193.42.38.139	TCP	60	53360 → 443 [ACK] Seq=1196 Ack=5287412 Win=523520 Len=0
20328	67.175981	10.11.26.183	193.42.38.139	TCP	60	53360 → 443 [RST, ACK] Seq=1196 Ack=5287412 Win=0 Len=0
20333	67.229216	10.11.26.183	104.26.1.231	TCP	66	53363 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
20334	67.284755	104.26.1.231	10.11.26.183	TCP	66	80 → 53363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM WS=8192
20335	67.285017	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
20336	67.286490	10.11.26.183	104.26.1.231	HTTP	172	GET /location/loca.asp HTTP/1.1
20337	67.344368	104.26.1.231	10.11.26.183	TCP	60	80 → 53363 [ACK] Seq=1 Ack=119 Win=65536 Len=0
20340	67.391300	10.11.26.183	194.180.191.64	HTTP	274	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20341	67.582257	194.180.191.64	10.11.26.183	HTTP	269	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
20342	67.588001	10.11.26.183	194.180.191.64	HTTP	502	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20343	67.759538	104.26.1.231	10.11.26.183	TCP	1170	80 → 53363 [PSH, ACK] Seq=1 Ack=119 Win=65536 Len=1116 [TCP PDU reassembled in 20344
20344	67.759632	104.26.1.231	10.11.26.183	HTTP	60	HTTP/1.1 200 OK (text/html)
20345	67.759787	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=119 Ack=1122 Win=260864 Len=0
20346	67.789341	194.180.191.64	10.11.26.183	HTTP	360	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
20348	67.889917	10.11.26.183	194.180.191.64	HTTP	328	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20350	68.291089	10.11.26.183	194.180.191.64	HTTP	336	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20572	128.463544	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21140	177.165996	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [FIN, ACK] Seq=119 Ack=1122 Win=260864 Len=0
21141	177.224794	104.26.1.231	10.11.26.183	TCP	60	80 → 53363 [FIN, ACK] Seq=1122 Ack=120 Win=65536 Len=0
21142	177.225106	10.11.26.183	104.26.1.231	TCP	60	53363 → 80 [ACK] Seq=120 Ack=1123 Win=260864 Len=0
21145	188.645216	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21153	248.801955	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21246	308.968954	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21295	369.027534	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21337	429.088220	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21352	489.150466	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21364	549.304894	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21415	609.360011	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
21608	669.564727	10.11.26.183	194.180.191.64	HTTP	288	POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

15. S2으로부터 명령을 받은 후 다른 두 IP에 연결

16. 호스트 이름과 계정 이름을 찾기 위해 kerberos로 필터링

```
▾ cname
    name-type: kRB5-NT-PRINCIPAL (1)
  ▾ cname-string: 1 item
      CNameString: oboomwald
  realm: NEMOTODES
▸ sname
  till: Sep 12, 2100 22:48:05.000000000
  rtime: Sep 12, 2100 22:48:05.000000000
  nonce: 155140912
▸ etype: 6 items
▸ addresses: 1 item DESKTOP-B8TQK49<20>


▾ Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7
  ▸ Destination: Dell_7f:09:5d (00:24:e8:7f:09:5d)
  ▸ Source: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
```