Malware Traffic Analysis - Sputnik House

정지훈

목차

1.개요
2.분석

1. 개요

sputnikhouse.org (192.168.1.95) 에 대한 회사 네트워크의 컴퓨터가 감염되었음을 나타내는 경고가 있습니다 . 일반적인 기간 동안 해당 호스트의 트래픽 한도가 있고 감염된 것과 관련된 경고 목록도 있습니다. 마지막으로 맬웨어 첨부 파일이 포함된 3개의 이메일이 있습니다. 이 3개의 이메일 중 하나의 첨부 파일이 이 컴퓨터를 감염시켰습니다.

2. 분석

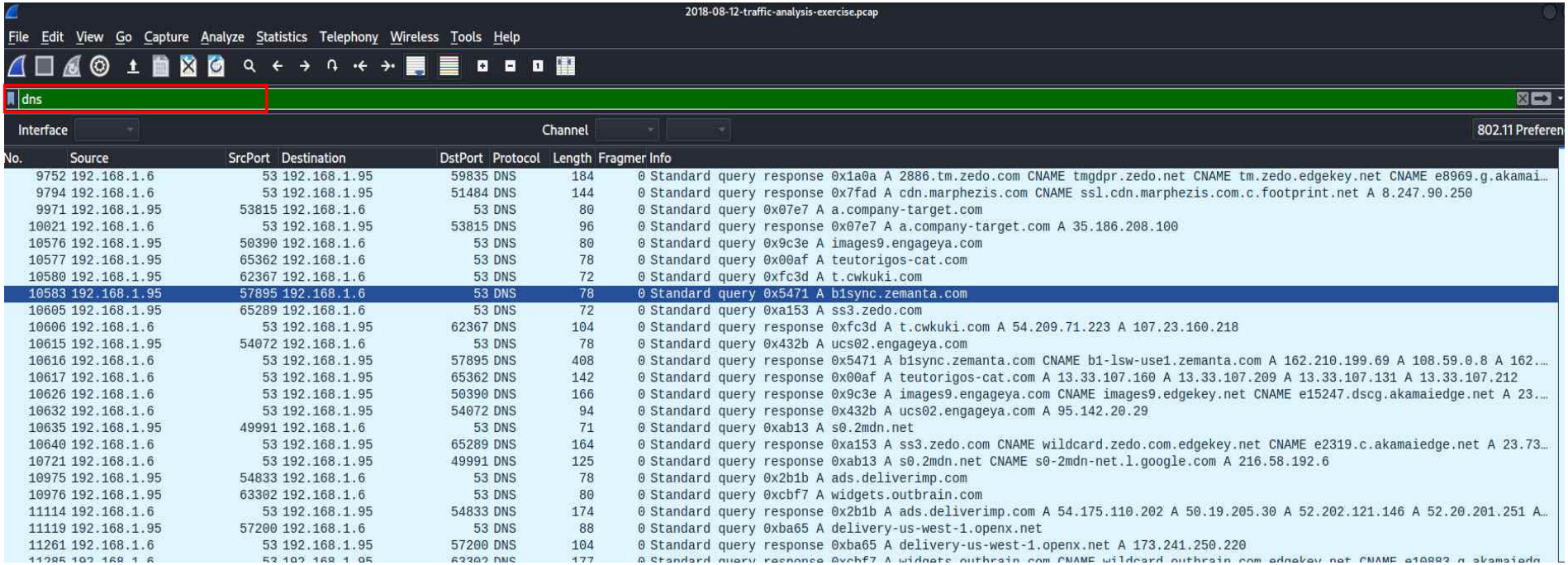
네트워크 특성

LAN Segment : 192.168.1.0/24(192.168.1.0 ~ 192.168.1.255)

Broadcast address: 192.168.1.255

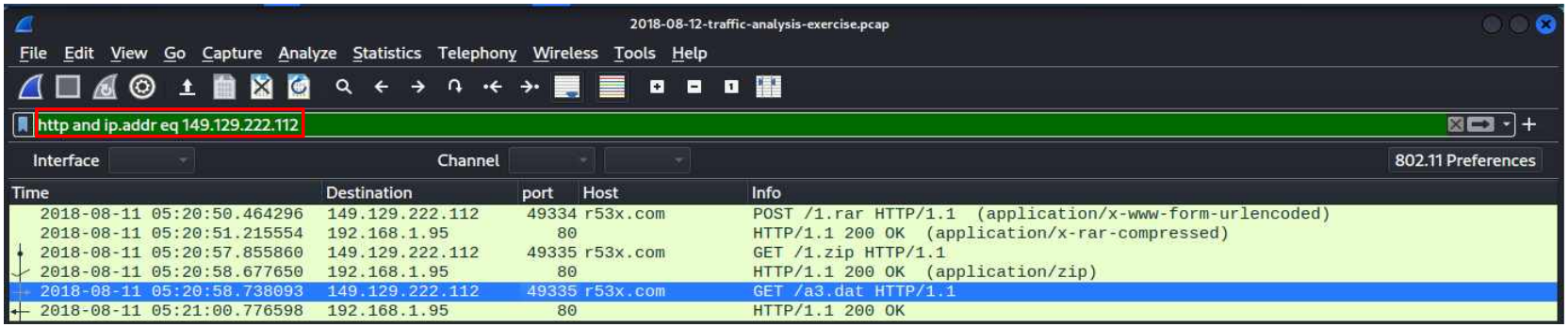
Domain Controller: 192.168.1.6

Domain: sputnikhouse.org



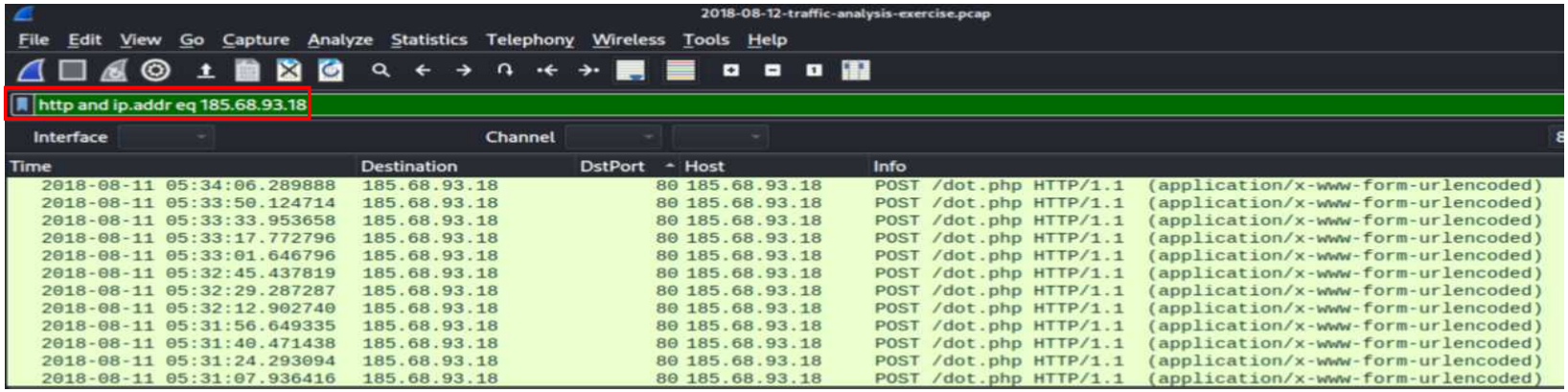
No.	Source	SrcPort	Destination	DstPort	Protocol	Length	Fragmer	Info
9752	192.168.1.6	53	192.168.1.95	59835	DNS	184	0	Standard query response 0x1a0a A 2886.tm.zedo.com CNAME tmgdpr.zedo.net CNAME tm.zedo.edgekey.net CNAME e8969.g.akamai…
9794	192.168.1.6	53	192.168.1.95	51484	DNS	144	0	Standard query response 0x7fad A cdn.marphezis.com CNAME ssl.cdn.marphezis.com.c.footprint.net A 8.247.90.250
9971	192.168.1.95	53815	192.168.1.6	53	DNS	80	0	Standard query 0x07e7 A a.company-target.com
10021	192.168.1.6	53	192.168.1.95	53815	DNS	96	0	Standard query response 0x07e7 A a.company-target.com A 35.186.208.100
10576	192.168.1.95	50390	192.168.1.6	53	DNS	80	0	Standard query 0x9c3e A images9.engageya.com
10577	192.168.1.95	65362	192.168.1.6	53	DNS	78	0	Standard query 0x00af A teutorigos-cat.com
10580	192.168.1.95	62367	192.168.1.6	53	DNS	72	0	Standard query 0xfc3d A t.cwkuki.com
10583	192.168.1.95	57895	192.168.1.6	53	DNS	78	0	Standard query 0x5471 A b1sync.zemanta.com
10605	192.168.1.95	65289	192.168.1.6	53	DNS	72	0	Standard query 0xa153 A ss3.zedo.com
10606	192.168.1.6	53	192.168.1.95	62367	DNS	104	0	Standard query response 0xfc3d A t.cwkuki.com A 54.209.71.223 A 107.23.160.218
10615	192.168.1.95	54072	192.168.1.6	53	DNS	78	0	Standard query 0x432b A ucs02.engageya.com
10616	192.168.1.6	53	192.168.1.95	57895	DNS	408	0	Standard query response 0x5471 A b1sync.zemanta.com CNAME b1-lsw-use1.zemanta.com A 162.210.199.69 A 108.59.0.8 A 162.…
10617	192.168.1.6	53	192.168.1.95	65362	DNS	142	0	Standard query response 0x00af A teutorigos-cat.com A 13.33.107.160 A 13.33.107.209 A 13.33.107.131 A 13.33.107.212
10626	192.168.1.6	53	192.168.1.95	50390	DNS	166	0	Standard query response 0x9c3e A images9.engageya.com CNAME images9.edgekey.net CNAME e15247.dscg.akamaiedge.net A 23.…
10632	192.168.1.6	53	192.168.1.95	54072	DNS	94	0	Standard query response 0x432b A ucs02.engageya.com A 95.142.20.29
10635	192.168.1.95	49991	192.168.1.6	53	DNS	71	0	Standard query 0xab13 A s0.2mdn.net
10640	192.168.1.6	53	192.168.1.95	65289	DNS	164	0	Standard query response 0xa153 A ss3.zedo.com CNAME wildcard.zedo.com.edgekey.net CNAME e2319.c.akamaiedge.net A 23.73…
10721	192.168.1.6	53	192.168.1.95	49991	DNS	125	0	Standard query response 0xab13 A s0.2mdn.net CNAME s0-2mdn-net.l.google.com A 216.58.192.6
10975	192.168.1.95	54833	192.168.1.6	53	DNS	78	0	Standard query 0x2b1b A ads.deliverimp.com
10976	192.168.1.95	63302	192.168.1.6	53	DNS	80	0	Standard query 0xcbf7 A widgets.outbrain.com
11114	192.168.1.6	53	192.168.1.95	54833	DNS	174	0	Standard query response 0x2b1b A ads.deliverimp.com A 54.175.110.202 A 50.19.205.30 A 52.202.121.146 A 52.20.201.251 A…
11119	192.168.1.95	57200	192.168.1.6	53	DNS	88	0	Standard query 0xba65 A delivery-us-west-1.openx.net
11261	192.168.1.6	53	192.168.1.95	57200	DNS	104	0	Standard query response 0xba65 A delivery-us-west-1.openx.net A 173.241.250.220

http 패킷 분석 (http 요청 및 응답은 149.129.222.112)

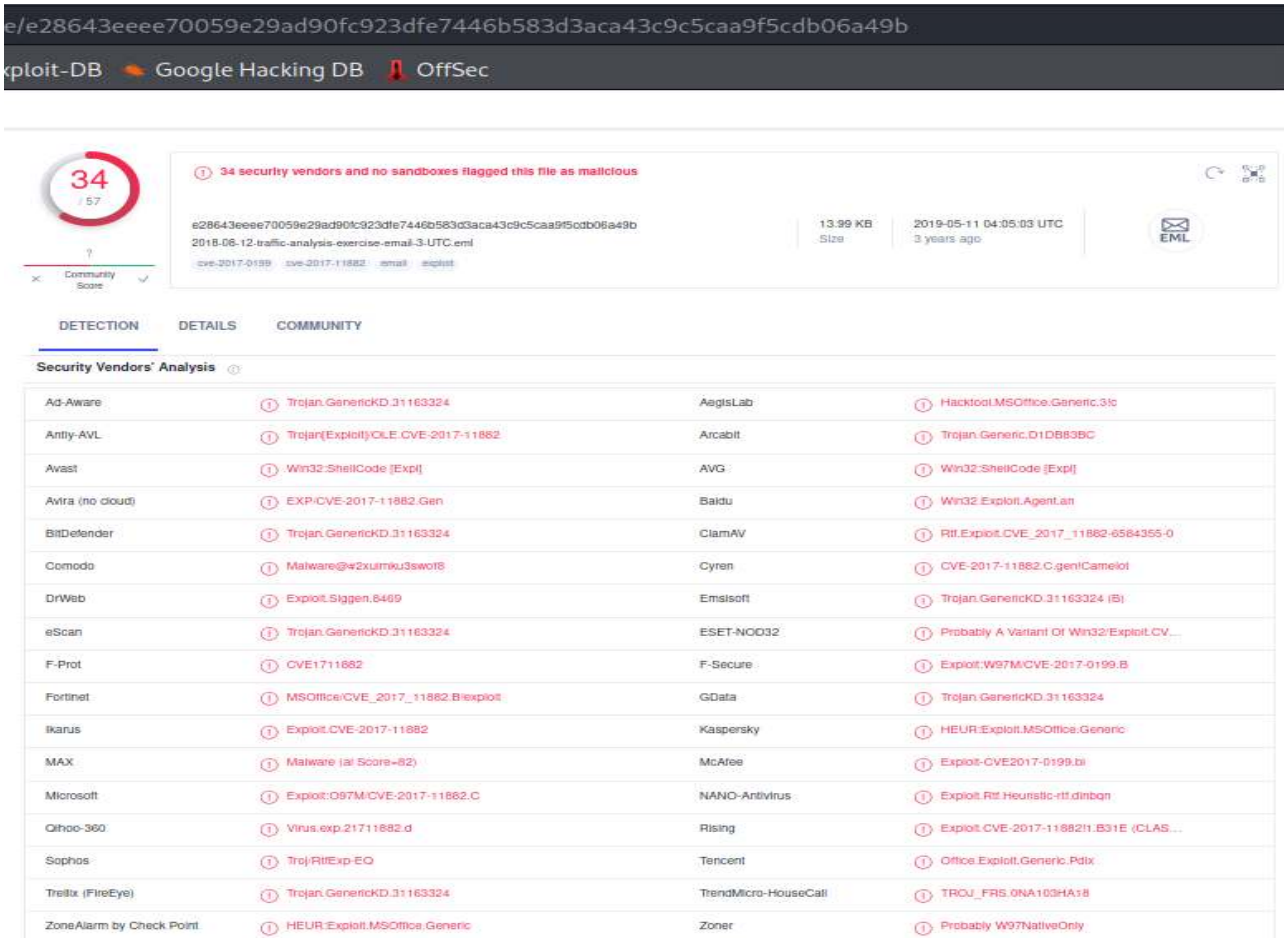


- 첫 번째 HTTP, 두 번째 HTTP 요청은 RAP 또는 ZIP 아카이브를 반환하지 않는다.
- 마지막 HTTP 요청은 “application/octet-stream”이라는 레이블이 지정된 내용으로 200 OK를 반환한다.
- a3.dat에 대한 HTTP요청은 실행 파일을 반환한다.

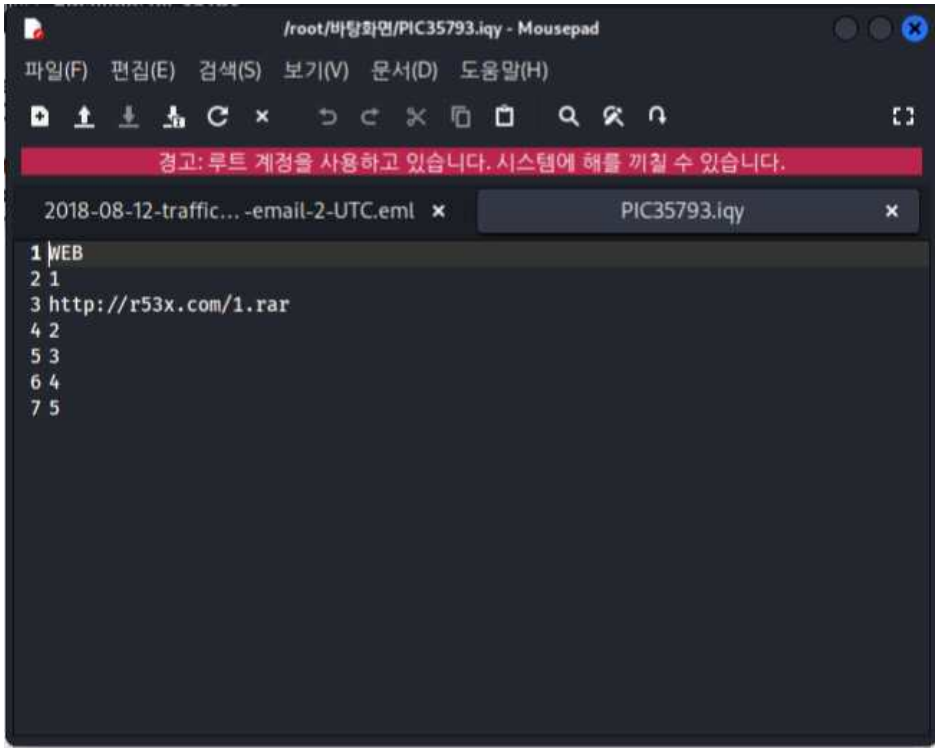
- Wireshark > 185.68.93.18 트래픽 필터링



추출한 값 > VirusTotal 사이트 > 분석결과 확인



취약한 호스트를 감염시키기 위해 몇 가지 경고가 있지만 계속 수행가능
-첫번째 첨부파일> PIC35793.jqy를 텍스트 파일로 열기



-첫 번째 이메일 첨부파일에서 감염된 것을 확인할 수 있다.