

Reference: <https://blueteamlabs.online/home/challenge/network-analysis-malware-compromise-e882f32908>


Download the PCAP from the above link

## Network Analysis – Malware Compromise

A SOC Analyst at Umbrella Corporation is going through SIEM alerts and sees the alert for connections to a known malicious domain.

Wireshark TCPDump TShark

Points	Difficulty	Solves	OS
20	Medium	4922	Windows/Linux

 **Packet Capture**  
982 KB

**Password**  
btlo

**Download File**

In Linux with tcpdump

```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ sudo tcpdump -tt -r traffic-with-dridex-infection.pcap | cut -d " " -f 3
reading from file traffic-with-dridex-infection.pcap, link-type EN10MB (Ethernet), snapshot length 65535
10.11.27.101.65289
10.11.27.1.domain
10.11.27.101.49158
95.181.198.231.http
10.11.27.101.49158
10.11.27.101.49158
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
10.11.27.101.49158
95.181.198.231.http
```

```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ sudo tcpdump -tt -r traffic-with-dridex-infection.pcap | cut -d " " -f 3 | sort |
uniq -c | sort -nr
reading from file traffic-with-dridex-infection.pcap, link-type EN10MB (Ethernet), snapshot length 65535
406 95.181.198.231.http
333 83.166.247.211.cloudvps.regruhosting.ru.https
302 176.32.33.108.http
79 10.11.27.101.49161
77 10.11.27.101.49181
77 10.11.27.101.49159
75 10.11.27.101.49158
39 172.106.33.46.https
38 185.158.251.55.https
38 174.34.253.11.https
37 185.244.150.230.hostsailor.com.https
14 10.11.27.101.49192
13 10.11.27.101.49221
13 10.11.27.101.49218
13 10.11.27.101.49217
13 10.11.27.101.49214
13 10.11.27.101.49209
13 10.11.27.101.49208
12 10.11.27.101.49205
```

Ip addresses used in talking

Ethernet · 1	IPv4 · 9	IPv6	TCP · 51	UDP · 8							
Address A	Address B		Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	E
10.11.27.101	83.166.247.211		711	117 kB	378	53 kB	333	64 kB	99.256729	2424.2444	
10.11.27.101	176.32.33.108		458	405 kB	156	10 kB	302	395 kB	24.283321	5.8906	
10.11.27.101	95.181.198.231		558	546 kB	152	9 kB	406	538 kB	2.123144	537.1739	
10.11.27.101	172.106.33.46		79	28 kB	40	21 kB	39	7 kB	698.722003	1457.7267	
10.11.27.101	174.34.253.11		77	27 kB	39	20 kB	38	6 kB	990.749952	1447.6811	
10.11.27.101	185.244.150.230		76	27 kB	39	21 kB	37	7 kB	524.881874	1466.4519	
10.11.27.101	185.158.251.55		77	27 kB	39	21 kB	38	7 kB	838.328764	1464.5101	
10.11.27.101	10.11.27.1		11	1 kB	5	377 bytes	6	1 kB	0.000000	2118.5054	
10.11.27.101	208.67.222.222		6	575 bytes	3	239 bytes	3	336 bytes	96.715429	0.1224	

We can investigate in these IP addresses

traffic-with-drindex-infection.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.11.27.101 & http.request.method == "GET"

No.	Time	Source	Destination	Destination Port	Protocol	Length	CNameString	Info
6	2018-11-27 16:30:15.190632	10.11.27.101	49158	95.181.198.231	80 HTTP	382		GET /QIC/tewok1.php?i=sptet10.spr HTTP/1.1
289	2018-11-27 16:30:37.364040	10.11.27.101	49159	176.32.33.108	80 HTTP	580		GET /images/ALL8Y6JETT/zN7eSSvSn0_2B/MzmcabxQpNSaFzIPStR/BuMdxGPb7LP1Xk
485	2018-11-27 16:30:38.576934	10.11.27.101	49159	176.32.33.108	80 HTTP	319		GET /fav/icon.ico HTTP/1.1
497	2018-11-27 16:30:39.907792	10.11.27.101	49161	176.32.33.108	80 HTTP	528		GET /images/UC2TjPGPls/FQpYEIaBcTp5xQBL/AUMvvh_2Bfks/KOH9nBaJbga/CF05ee1P
730	2018-11-27 16:30:41.943113	10.11.27.101	49159	176.32.33.108	80 HTTP	507		GET /images/u8xk2MFy8b/hq55JPtBSW8208kV/1z1ZTRdC152/THXW_2Bxk3/h0d4284r1
731	2018-11-27 16:30:42.033388	10.11.27.101	49161	176.32.33.108	80 HTTP	528		GET /QIC/tewok1.php?i=sptet10.spr HTTP/1.1

Follow the http stream

```

NET /QIC/reowl.php?ts=pet10.spr HTTP/1.1
Accept: */*
Accept-encoding: gzip, deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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: klychenodg.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 27 Nov 2018 16:30:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Disposition: attachment; filename="spet10.spr"
Content-Type: application/octet-stream
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 261120
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

Mz.....@.....f..l..This program cannot be run in DOS mode.....
$.....M.S...S...K.K...T...S...S...S...q...10...J...Rich.S...PE.L...XV.....4.....@.....@.....
.....P.....B...B.....p...@.....@.....text.....f.....
J.....&.....@.....data.....@.....rFC.....
.....h...c...#...Y...h...c...#...Y...h...c...#...Y...DS.V...OcT....V.....^.....DS.TS.H.....TS.....R.P.....
.....DS.H.U.....
.....QV.TS.DS.....TS.....C.E.F.....u.3.QR.....Y.....W.Y...A.U.+QR.....Y.....Q.DS...S.V.....tS...U.J.....
.C...k...AY...PV.....AY.....QV.TS.DS.....B...TS.....C.E.F.....u.3.QR.....Y.....W.Y...A.U.+QR.....Y.....TS.V.....DS.Ot.....
.C...S.....C.S.....S.UVV.....tS.....t.....
.....D.....4.....F.....D.....C.....C.....C.....C.....C.....[S.]jJUS.....
.C.f.S.d.F.dsO.DS\$......u03;u'=.C.....C.....
.C.WSUQ.....j]JTUS.....C.....C.LS.....I.S.UQ.RP.o.....S.C.....C.....LS.U.....f.....C.h6.....S.....
.....k.I.+3;j.U.E.....=f.c.+.....+.....LS.u.....C.[SS.DS.....dsO.DS.7....ds;j.u.tF.....u'.TSVj.W.....DS.....S.C.....DS.=.....|.....LS.....DS.rot.....
.C.f.f.;u;tF.....TSsvj.....DS.....C.DS.....C.DS.....DSOct.....f.....DS(P.xEC.....
.C.....C.B.....C.....
.C.....C.DS..B.....C.f.D.....;.....u.u.J.j3.....
.C.S.C.....C.....nc#n.C.S.C.....nsapu.A.C.....

```

[illegible]

Download the suspicious file and then check its reputation in virustotal

Wireshark · Export · HTTP object list

Text Filter:  Content Type: All Content-Types ▾

Packet ▾	Hostname	Content Type	Size	Filename
280	klychenogg.com	application/octet-stream	261 kB	tewokl.php?l=spet10.spr
483	cochrinato.com	text/html	214 kB	ojw.avi
491	cochrinato.com	image/vnd.microsoft.icon	5,430 bytes	favicon.ico
732	cochrinato.com	text/html	273 kB	6.avi
739	cochrinato.com	text/html	2,352 bytes	timxEQW.avi
1179	95.181.198.231	application/rar	254 kB	oiioiashdqbwe.rar

```
saf-lx@Saf-Ubuntu: ~/Desktop/Hackthebox/Network analysis - Malware Compromise
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ ls
'tewokl.php%3fl=spet10.spr'  traffic-with-dridex-infection.pcap
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ file 'tewokl.php%3fl=spet10.spr'
tewokl.php%3fl=spet10.spr: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ sha256sum 'tewokl.php%3fl=spet10.spr'
aaa41c27d5b4a160ed2a00ba820dd6ada86ed80e76d476a8379543478e608f84  tewokl.php%3fl=spet10.spr
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$
```

Sha 256 Hash -> **aaa41c27d5b4a160ed2a00ba820dd6ada86ed80e76d476a8379543478e608f84**

61 / 72 security vendors flagged this file as malicious

Reanalyze Similar More ▾

aaa41c27d5b4a160ed2a00ba820dd6ada86ed80e76d476a8379543478e608f84

sawwhole.exe

Size: 255.00 KB Last Analysis Date: 6 days ago

peexe detect-debug-environment direct-cpu-clock-access long-sleeps nxdomain runtime-modules calls-wmi spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ursnif/djxi Threat categories trojan spyware Family labels ursnif djxi fqlj

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R246588	Alibaba	TrojanSpy:Win32/Ursnif.d9d29224
AliCloud	Trojan(spy):Win/Ursnif.CW	ALYac	Spyware:Ursnif
Antiy-AVL	Trojan(Spy)/Win32.Ursnif	Arcabit	Trojan.Agent.DJXI
Arctic Wolf	Unsafe	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/AD.Ursnif.nxnua
BitDefender	Trojan.Agent.DJXI	Bkav Pro	W32.AIDetectMalware