

MALWARE TRAFFIC ANALYSIS

WANNACRY SPREADING

2540125384 – BENEDICTO MARVELOUS ALIDAJAYA

2540118933 – JOHN ORLOND

2540124702 – MATTHEW KURNIAWAN



PCAP FILE

Analysis malware menggunakan file pcap yang didapat dari website malware-traffic-analysis.net dengan link pcap sebagai berikut :

<https://www.malware-traffic-analysis.net/2017/05/18/2017-05-18-WannaCry-ransomware-using-ExternalBlue-exploit.pcap.zip>

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays a guest blog post from David Szili titled "PCAP OF WANNACRY SPREADING USING ETERNALBLUE". The post includes a red banner at the top with the text "MALWARE-TRAFFIC-ANALYSIS.NET" and a hand cursor icon. Below the banner, the date "2017-05-18" and author "DAVID SZILI" are mentioned. A section titled "EDITOR'S NOTE" contains three bullet points about the blog's origin. A "ASSOCIATED FILE" section lists two ZIP files: "2017-05-18-WannaCry-ransomware-using-ExternalBlue-exploit.pcap.zip" and "2017-05-18-WannaCry-ransomware-sample.exe.zip". The "TEST ENVIRONMENT" section describes a LAN setup with five Windows hosts. The "MALWARE" section details the WannaCry sample, including its SHA256 hash, SHA1 hash, MD5 hash, file size (3.6 MB), and file type (Win32 EXE). It also lists three URLs for malware analysis. The "ALERTS" section is present at the bottom of the page.

No.	Time	Source	Destination	Protocol	Length	Info
348	2017/138 15:07:13,147251	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
351	2017/138 15:07:13,147772	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
375	2017/138 15:07:20,649359	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
376	2017/138 15:07:20,649698	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
431	2017/138 15:08:28,164604	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
434	2017/138 15:08:28,165176	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
438	2017/138 15:08:35,666640	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
439	2017/138 15:08:35,667047	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
473	2017/138 15:09:56,682176	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
477	2017/138 15:09:56,682983	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
478	2017/138 15:09:56,783978	192.168.116.138	192.168.116.143	SMB_NE_	292	Query for PDC from DFIR-WIN7-X64
480	2017/138 15:09:58,922418	192.168.116.138	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7d403293
485	2017/138 15:10:04,188892	192.168.116.138	192.168.116.255	SMB_NE_	289	SAM LOGON request from client
486	2017/138 15:10:04,181129	192.168.116.138	192.168.116.143	SMB_NE_	289	SAM LOGON request from client
488	2017/138 15:10:04,289889	192.168.116.138	192.168.116.143	SMB_NE_	292	Query for PDC from DFIR-WIN7-X64
490	2017/138 15:10:04,399416	192.168.116.138	192.168.116.255	SMB_NE_	292	Query for PDC from DFIR-WIN7-X64
491	2017/138 15:10:04,399606	192.168.116.138	192.168.116.143	SMB_NE_	292	Query for PDC from DFIR-WIN7-X64

Berikut adalah tampilan pcap saat dibuka dengan Wireshark dengan setting time diubah menjadi yyyy/mm/dd hh//mm/ss.

1111	2017/138	15:12:07,288898	192.168.116.138	192.168.116.149	TCP	66 445 → 49367 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
1114	2017/138	15:12:07,288614	192.168.116.138	192.168.116.149	TCP	68 445 → 49367 [ACK] Seq=1 Ack=2 Win=65536 Len=0
1115	2017/138	15:12:07,288691	192.168.116.138	192.168.116.149	TCP	68 445 → 49367 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1117	2017/138	15:12:07,289827	192.168.116.138	192.168.116.149	TCP	66 445 → 49368 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

Pada jam 15.12.07, IP 192.168.116.138 mencoba melakukan koneksi pada 192.168.116.149 dengan mengirim SYN, ACK. Lalu dibalas dengan mengirimkan ACK, Tetapi IP 192.168.116.138 mengirimkann request RST,ACK.

1252 2017/138 15:12:10,218865	192.168.116.138	192.168.116.149	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
1254 2017/138 15:12:10,218992	192.168.116.138	192.168.116.149	TCP	60 445 → 49419 [ACK] Seq=430 Ack=457 Win=65280 Len=0
1255 2017/138 15:12:10,219044	192.168.116.138	192.168.116.149	TCP	60 445 → 49419 [RST, ACK] Seq=430 Ack=457 Win=0 Len=0
1297 2017/138 15:12:11,232928	192.168.116.138	224.0.0.252	LLMNR	66 Standard query 0xd425 A isatap
1300 2017/138 15:12:11,331776	192.168.116.138	224.0.0.252	LLMNR	66 Standard query 0xd425 A isatap
1318 2017/138 15:12:11,534055	192.168.116.138	192.168.116.255	NBNS	92 Name query NB ISATAP<00>
1354 2017/138 15:12:12,209552	192.168.116.138	255.255.255.255	DHCP	342 DHCP Inform - Transaction ID 0xa8a2bf19

Hal tersebut kembali berulang pada jam 15.12.10 dengan source IP dan Destination IP yang sama.

No.	Time	Source	Destination	Protocol	Length	Info
2119	2017/138 15:12:20,	873312	192.168.116.138	192.168.116.149	TCP	60 445 → 49472 [RST, ACK] Seq=430 Ack=63749 Win=0 Len=0
2120	2017/138 15:12:20,	873433	192.168.116.138	192.168.116.149	TCP	60 445 → 49529 [RST, ACK] Seq=332 Ack=223 Win=0 Len=0
2121	2017/138 15:12:20,	873589	192.168.116.138	192.168.116.149	SMB	253 Session Setup AndX Response
2123	2017/138 15:12:20,	874421	192.168.116.138	192.168.116.149	SMB	114 Tree Connect AndX Response
2125	2017/138 15:12:20,	874700	192.168.116.138	192.168.116.149	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
2127	2017/138 15:12:20,	875378	192.168.116.138	192.168.116.149	TCP	60 445 → 49690 [ACK] Seq=430 Ack=457 Win=63922 Len=0
2128	2017/138 15:12:20,	875460	192.168.116.138	192.168.116.149	TCP	60 445 → 49690 [RST, ACK] Seq=430 Ack=457 Win=0 Len=0
2317	2017/138 15:12:23,	883129	192.168.116.138	192.168.116.149	TCP	66 445 → 49749 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2320	2017/138 15:12:23,	884528	192.168.116.138	192.168.116.149	SMB	185 Negotiate Protocol Response
2450	2017/138 15:12:26,	897212	192.168.116.138	192.168.116.149	TCP	66 445 → 49788 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2453	2017/138 15:12:26,	898111	192.168.116.138	192.168.116.149	SMB	263 Negotiate Protocol Response
2455	2017/138 15:12:26,	882914	192.168.116.138	192.168.116.149	SMB	253 Session Setup AndX Response
2457	2017/138 15:12:26,	131978	192.168.116.138	192.168.116.149	TCP	66 445 → 49791 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2460	2017/138 15:12:26,	145186	192.168.116.138	192.168.116.149	TCP	66 445 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2464	2017/138 15:12:26,	156327	192.168.116.138	192.168.116.149	TCP	66 445 → 49793 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2469	2017/138 15:12:26,	173082	192.168.116.138	192.168.116.149	TCP	66 445 → 49795 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2472	2017/138 15:12:26,	104378	192.168.116.138	192.168.116.149	TCP	66 445 → 49796 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

Word Count (WCT): 17
Selected Index: 5: NT LM 0.12
> Security Mode: 0x03, Mode, Password
Max Mpx Count: 50
Max VCs: 1
Max Buffer Size: 4356
Max Raw Buffer: 65536
Session Key: 0x00000000
> Capabilities: 0x0001e3fc, Unicode, Large Files, NT SMBs, RPC Remote APIs, NT Status C
System Time: May 18, 2017 15:12:23.427387300 SE Asia Standard Time
Server Time Zone: -120 min from UTC
Challenge Length: 8
Byte Count (BCC): 58
Challenge: b7a8a5a1bc336a50
Primary Domain: TESTDOMAIN
Server: DFIR-WIN7-X64

```

0000 00 25 b3 f5 fa 74 00 19 bb 4f 4c d8 00 45 00 %...t..-OL...E
0010 00 ab 01 5a 40 00 80 06 8e 82 c0 a8 74 8a c0 a8 ...Z@.....t...
0020 74 95 01 bd c2 55 f5 68 1e 9b cf 1e cc 82 50 18 t....U-h.....P-
0030 01 00 73 8a 00 00 00 00 00 7f ff 53 4d 42 72 00 ..s.....-SMBr...
0040 00 00 00 98 53 c9 00 00 00 00 00 00 00 00 00 00 .....S.....-
0050 00 00 00 00 ff fe 00 00 40 00 11 05 00 03 32 00 .....@.....2-
0060 01 00 04 11 00 00 00 00 01 00 00 00 00 00 fc e3 ..... .
0070 01 00 51 c4 89 7a ae cf d2 01 88 ff 08 3a 00 b7 ..Q...z...-....;
0080 a8 a5 a1 bc 33 6a 50 54 00 45 00 53 00 54 00 44 .....3jPT-E-S-T-D
0090 00 4f 00 4d 00 41 00 49 00 4e 00 00 00 44 00 46 -O-M-A-I-N...D-F
00a0 00 49 00 52 00 2d 00 57 00 49 00 4e 00 37 00 2d -I-R...W-I-N-7...
00b0 00 58 00 36 00 34 00 00 00 .....X-6-4-.. .

```

Pada pukul 15.12.23, koneksi berhasil disambungkan lalu IP 192.168.116.128 mengirimkan negotiate protocol response dengan mengirimkan SMB dengan nama Windows 7 Enterprise yang dikoneksikan ke Test Domain

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2119	2017/138 15:12:20,873312	192.168.116.138	192.168.116.149	TCP	60	445 + 49472 [RST, ACK] Seq=430 Ack=63749 Win=0 Len=0
2120	2017/138 15:12:20,873433	192.168.116.138	192.168.116.149	TCP	60	445 + 49529 [RST, ACK] Seq=332 Ack=223 Win=0 Len=0
2121	2017/138 15:12:20,873589	192.168.116.138	192.168.116.149	SMB	253	Session Setup AndX Response
2123	2017/138 15:12:20,874421	192.168.116.138	192.168.116.149	SMB	114	Tree Connect AndX Response
2125	2017/138 15:12:20,874700	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
2127	2017/138 15:12:20,875378	192.168.116.138	192.168.116.149	TCP	60	445 + 49698 [ACK] Seq=430 Ack=457 Win=63922 Len=0
2128	2017/138 15:12:20,875468	192.168.116.138	192.168.116.149	TCP	60	445 + 49698 [RST, ACK] Seq=430 Ack=457 Win=0 Len=0
2317	2017/138 15:12:23,883129	192.168.116.138	192.168.116.149	TCP	66	445 + 49749 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2320	2017/138 15:12:23,884528	192.168.116.138	192.168.116.149	SMB	185	Negotiate Protocol Response
2450	2017/138 15:12:26,057212	192.168.116.138	192.168.116.149	TCP	66	445 + 49788 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2453	2017/138 15:12:26,058111	192.168.116.138	192.168.116.149	SMB	263	Negotiate Protocol Response
2455	2017/138 15:12:26,082914	192.168.116.138	192.168.116.149	SMB	253	Session Setup AndX Response
2457	2017/138 15:12:26,131978	192.168.116.138	192.168.116.149	TCP	66	445 + 49791 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2460	2017/138 15:12:26,145186	192.168.116.138	192.168.116.149	TCP	66	445 + 49792 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2464	2017/138 15:12:26,156327	192.168.116.138	192.168.116.149	TCP	66	445 + 49793 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2469	2017/138 15:12:26,173082	192.168.116.138	192.168.116.149	TCP	66	445 + 49795 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2473	2017/138 15:12:26,104270	192.168.116.138	192.168.116.149	TCP	66	445 + 49796 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

> Ethernet II, Src: HewlettP_4f:4c:d8 (00:19:bb:4f:4c:d8), Dst: HewlettP_f5:fa:74 (00:25:b3:f4) ^

> Internet Protocol Version 4, Src: 192.168.116.138, Dst: 192.168.116.149

> Transmission Control Protocol, Src Port: 445, Dst Port: 49788, Seq: 210, Ack: 223, Len: 199

> NetBIOS Session Service

 SMB (Server Message Block Protocol)

 SMB Header

 Session Setup AndX Response (0x73)

 Word Count (WCT): 3

 AndXCommand: No further commands (0xff)

 Reserved: 00

 AndXOffset: 195

 > Action: 0x0000

 Byte Count (BCC): 154

 Native OS: Windows 7 Enterprise 7601 Service Pack 1

 Native LAN Manager: Windows 7 Enterprise 6.1

 Primary Domain: TESTDOMAIN

0000 00 25 b3 f5 fa 74 00 19 bb 4f 4c d8 00 45 00 .%...t...OL...E...

0010 00 ef 01 5d 40 00 80 06 8e 3b c0 a8 74 8a c0 a8 ...]@...;...t...

0020 74 95 01 bd c2 7c f1 27 49 75 f9 03 cd 1c 50 18 t....|.'Iu....P...

0030 01 00 ee 5e 00 00 00 00 00 c3 ff 53 4d 42 73 00 ...^.....SMBs...

0040 00 00 00 98 07 c0 00 00 00 00 00 00 00 00 00 00

0050 00 00 00 ff fe 00 08 40 00 03 ff 00 c3 00 00@.....

0060 00 9a 00 11 57 00 69 00 6e 00 64 00 6f 00 77 00 ...W.i..n.d.o.w...

0070 73 00 20 00 37 00 20 00 45 00 6e 00 74 00 65 00 s..-7..-E.n.t-e...

0080 72 00 70 00 72 00 69 00 73 00 65 00 20 00 37 00 r.p.r-i..s.e..-7...

0090 36 00 30 00 31 00 20 00 53 00 65 00 72 00 76 00 6..0..1..-S.e..r.v...

00a0 69 00 63 00 65 00 20 00 50 00 61 00 63 00 6b 00 i.c.e..-P.a..c.k...

00b0 20 00 31 00 00 00 57 00 69 00 6e 00 64 00 6f 00 .1...W..i..n..d..o...

00c0 77 00 73 00 20 00 37 00 20 00 45 00 6e 00 74 00 W.s..-7..-E..n..t...

00d0 65 00 72 00 70 00 72 00 69 00 73 00 65 00 20 00 e..r..p..r..i..s..e..-

00e0 36 00 2e 00 31 00 00 00 54 00 45 00 53 00 54 00 6..-1...T-E-S-T...

00f0 44 00 4f 00 4d 00 41 00 49 00 4e 00 00 00 D..O..M..A..I..N..-

2017-05-18-WannaCry-ransomware-using-ExternalBlue-exploit.pcap

Packets: 46654 · Displayed: 46654 (100.0%)

Profile: Default

Pada waktu yang sama, session juga berhasil terbuat dan siap untuk menerima respond dari IP korban

No.	Time	Source	Destination	Protocol	Length	Info
3159	2017/138 15:12:41,545050	192.168.116.138	192.168.116.143	SMB_NEGOTIATE	316	SAM LOGON request from client
3171	2017/138 15:12:42,118707	192.168.116.138	192.168.116.149	TCP	66	445 → 50164 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3174	2017/138 15:12:42,119191	192.168.116.138	192.168.116.149	SMB	185	Negotiate Protocol Response
3176	2017/138 15:12:42,119394	192.168.116.138	192.168.116.149	TCP	60	445 → 49806 [RST, ACK] Seq=332 Ack=223 Win=0 Len=0
3177	2017/138 15:12:42,119606	192.168.116.138	192.168.116.149	SMB	253	Session Setup AndX Response
3179	2017/138 15:12:42,120172	192.168.116.138	192.168.116.149	SMB	114	Tree Connect AndX Response
3181	2017/138 15:12:42,120628	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
3183	2017/138 15:12:42,121120	192.168.116.138	192.168.116.149	TCP	60	445 → 50164 [ACK] Seq=430 Ack=457 Win=65280 Len=0
3184	2017/138 15:12:42,121239	192.168.116.138	192.168.116.149	TCP	60	445 → 50164 [RST, ACK] Seq=430 Ack=457 Win=0 Len=0
3390	2017/138 15:12:45,129666	192.168.116.138	192.168.116.149	TCP	66	445 → 50240 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3393	2017/138 15:12:45,130281	192.168.116.138	192.168.116.149	SMB	185	Negotiate Protocol Response
3395	2017/138 15:12:45,160822	192.168.116.138	192.168.116.149	SMB	253	Session Setup AndX Response
3397	2017/138 15:12:45,180745	192.168.116.138	192.168.116.149	SMB	114	Tree Connect AndX Response
3399	2017/138 15:12:45,205281	192.168.116.138	192.168.116.149	SMB	93	NT Trans Response, <unknown (0)>
3402	2017/138 15:12:45,230229	192.168.116.138	192.168.116.149	TCP	60	445 → 50240 [ACK] Seq=430 Ack=4374 Win=65536 Len=0
3405	2017/138 15:12:45,245775	192.168.116.138	192.168.116.149	TCP	60	445 → 50240 [ACK] Seq=430 Ack=7067 Win=65536 Len=0
3400	2017/138 15:12:45,247201	192.168.116.138	192.168.116.149	TCP	60	445 → 50240 [ACK] Seq=430 Ack=71447 Win=65536 Len=0
Word Count (WCT): 17 Selected Index: 5: NT LM 0.12 > Security Mode: 0x03, Mode, Password Max Mpx Count: 50 Max VCs: 1 Max Buffer Size: 4356 Max Raw Buffer: 65536 Session Key: 0x00000000 > Capabilities: 0x0001e3fc, Unicode, Large Files, NT SMBs, RPC Remote APIs, NT Status C System Time: May 18, 2017 15:12:41.663819400 SE Asia Standard Time Server Time Zone: -120 min from UTC Challenge Length: 8 Byte Count (BCC): 58 Challenge: dcada83586aaca09 Primary Domain: TESTDOMAIN Server: DFIR-WIN7-X64						
<pre>0000 00 25 b3 f5 fa 74 00 19 bb 4f 4c d8 00 45 00 .%..t...OL..E. 0010 00 ab 01 8a 40 00 80 06 8e 52 c0 a8 74 8a c0 a8 ..@...R.t... 0020 74 95 01 bd c3 f4 79 68 7b e1 ff e1 de 96 50 18 t...yh {....P. 0030 01 00 04 c9 00 00 00 00 00 7f ff 53 4d 42 72 00S.....SMBr. 0040 00 00 00 98 53 c0 00 00 00 00 00 00 00 00 00 00S..... 0050 00 00 00 ff fe 00 00 40 00 11 05 00 03 32 00@....2. 0060 01 00 04 11 00 00 00 00 01 00 00 00 00 fc e3 0070 01 00 f2 6c 68 85 ae cf d2 01 88 ff 08 3a 00 dc ...lh..... 0080 ad a8 35 86 aa ca 09 54 00 45 00 53 00 54 00 44 ..5....T.E.S.T.D 0090 00 4f 00 4d 00 41 00 49 00 4e 00 00 00 44 00 46 ..O.M.A.I.N..D.F 00a0 00 49 00 52 00 2d 00 57 00 49 00 4e 00 37 00 2d ..I.R...W.I.N.7.. 00b0 00 58 00 36 00 34 00 00X.6.4...</pre>						

Lalu pada 15.12.43, IP 192.168.116.138 mengirimkan file Windows 7 Enterprise X64 dengan protocol SMB.

3344 2017/138 15:12:43,489253 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3347 2017/138 15:12:43,788303 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3349 2017/138 15:12:43,788861 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	202 Close Response
3351 2017/138 15:12:43,905325 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3353 2017/138 15:12:43,905632 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3355 2017/138 15:12:43,905920 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3357 2017/138 15:12:43,954298 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3359 2017/138 15:12:43,954909 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	202 Close Response
3361 2017/138 15:12:43,978280 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3363 2017/138 15:12:43,978283 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3365 2017/138 15:12:43,978286 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3367 2017/138 15:12:44,120773 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3369 2017/138 15:12:44,121246 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	202 Close Response
3371 2017/138 15:12:44,140684 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3373 2017/138 15:12:44,141141 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 GetInfo Response, Error: STATUS_FILE_CLOSED
3375 2017/138 15:12:44,142346 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3376 2017/138 15:12:44,142346 fe80::6992:5661:9d8.. fe80::2409:fcbd:1be.. SMB2	151 Ioctl Response, Error: STATUS_FILE_CLOSED

Kemudian, IP 192.168.116.138 melakukan bruteforce IP pada local LAN (informasi didapat dari malware-traffic-analysis.net) hingga 15.12.42, Lalu pada 15.12.43 IP 192.168.116.138 melakukan create response file untuk Administrator.TESTDOMAIN\Desktop\Share

46.. 2017/138 15:17:25,268886 fe80::6992:5661:9d0.. ff02::1:2	DHCPv6	173 Solicit XID: 0xb680fa CID: 000100011f5a2cd00000000e73a14
46.. 2017/138 15:17:40,380891 fe80::6992:5661:9d0.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46.. 2017/138 15:17:40,385382 fe80::6992:5661:9d0.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46.. 2017/138 15:17:40,386741 fe80::6992:5661:9d0.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46.. 2017/138 15:17:40,386892 fe80::6992:5661:9d0.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46.. 2017/138 15:17:40,387842 fe80::6992:5661:9d0.. ff02::1:3	LLMNR	93 Standard query 0x1fb4 ANY WIN-2012-R2-1
46.. 2017/138 15:17:40,800033 fe80::6992:5661:9d0.. ff02::1:3	LLMNR	93 Standard query 0x1fb4 ANY WIN-2012-R2-1
46.. 2017/138 15:17:40,877701 fe80::6992:5661:9d0.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
675 2017/138 15:11:39,544551 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
676 2017/138 15:11:40,558732 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
677 2017/138 15:11:42,574101 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
678 2017/138 15:11:46,574610 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
712 2017/138 15:11:54,589751 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
1265 2017/138 15:12:10,604771 fe80::ed0e:fee3:804.. ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
2423 2017/138 15:12:24,833879 fe80::ed0e:fee3:804.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
2425 2017/138 15:12:24,833956 fe80::ed0e:fee3:804.. ff02::16	ICMPv6	90 Multicast Listener Report Message v2
2427 2017/138 15:12:34,833961 fe80::ed0e:fee3:804.. ff02::1:3	LLMNR	87 Standard query 0xd0a6 ANY TactDC1

Pada 15.17.40, file tersebut mulai digunakan sebagai listener hingga hari setelahnya.

No.	Time	Source	Destination	Protocol	Length	Info
120	2017/138 15:06:32,983856	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	366	Create Request File: Administrator.TESTDOMAIN\Desktop\Share
122	2017/138 15:06:32,983964	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	174	Notify Request File: Administrator.TESTDOMAIN\Desktop\Share
123	2017/138 15:06:32,983969	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	446	Create Request File: Administrator.TESTDOMAIN\Desktop\Share\desktop.ini
127	2017/138 15:06:33,021268	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	TCP	74	49166 → 445 [ACK] Seq=3753 Ack=1769 Win=66048 Len=0
128	2017/138 15:06:33,021320	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	398	Create Request File: Administrator.TESTDOMAIN\Desktop\Share
130	2017/138 15:06:33,021325	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	280	Find Request File: Administrator.TESTDOMAIN\Desktop\Share SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern
133	2017/138 15:06:33,021329	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	TCP	74	49166 → 445 [ACK] Seq=4283 Ack=3529 Win=66048 Len=0
134	2017/138 15:06:33,021330	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	166	Close Request File: Administrator.TESTDOMAIN\Desktop\Share
136	2017/138 15:06:33,021333	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	559	Create Request File: Administrator.TESTDOMAIN\Desktop\Share;GetInfo Request FS_INFO/FileFsVolumeI
138	2017/138 15:06:33,021335	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	166	Close Request File: Administrator.TESTDOMAIN\Desktop\Share
140	2017/138 15:06:33,141764	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	TCP	74	49166 → 445 [ACK] Seq=4952 Ack=4165 Win=65536 Len=0
141	2017/138 15:06:33,416586	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	182	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO
143	2017/138 15:06:33,416896	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	182	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO
145	2017/138 15:06:33,417260	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	228	Ioctl Request FSCTL_PIPE_WAIT Pipe: MsFteWds
147	2017/138 15:06:33,626579	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	TCP	74	49166 → 445 [ACK] Seq=5322 Ack=4396 Win=65280 Len=0
179	2017/138 15:06:44,882143	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	SMB2	146	Tree Disconnect Request
181	2017/138 15:06:44,882143	fe80::ed6a:d848:605:	fe80::6992:5661:9d0:	TCP	74	40166 → 445 [ACK] Seq=4007 Ack=1957 Win=66048 Len=0
> Frame 130: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits)						
> Ethernet II, Src: HewlettP_33:c6:dd (00:1c:c4:33:c6:dd), Dst: WIN-2012-R2-1 (00:08:83:e7:3a:14)						
> Internet Protocol Version 6, Src: fe80::ed6a:d848:6059:3c0e, Dst: fe80::6992:5661:9d0d:3f96						
> Transmission Control Protocol, Src Port: 49166, Dst Port: 445, Seq: 4077, Ack: 1957, Len: 206						
> NetBIOS Session Service						
> SMB2 (Server Message Block Protocol version 2)						
> SMB2 (Server Message Block Protocol version 2)						
0000 00 08 83 e7 3a 14 00 1c c4 33 c6 dd 66 00 3 . . .						
0010 00 00 00 e2 06 80 fe 80 00 00 00 00 00 ed 6a j .						
0020 d8 48 60 59 3c 0e fe 80 00 00 00 00 00 69 92 H'Y< i .						
0030 56 61 9d 0d 3f 96 c0 0e 01 bd 12 67 d5 aa 6f fe Va . ? . . g o .						
0040 10 21 50 18 01 01 f2 83 00 00 00 00 ca fe 53 !P S .						
0050 4d 42 40 00 01 00 00 00 00 00 0e 00 01 00 00 00 MB@						
0060 00 00 68 00 00 00 0d 00 00 00 00 00 00 ff fe . h						
0070 00 00 05 00 00 00 05 00 00 00 00 68 00 00 00 00 . h						
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 . !						
0090 25 00 00 00 00 10 00 00 00 1a 00 00 00 09 00 %						
00a0 00 00 1a 00 00 00 60 00 02 00 00 00 01 00 2a 00						
00b0 00 00 00 00 03 00 fe 53 4d 42 40 00 01 00 00 00 5 MB@						
00c0 00 00 0e 00 01 00 04 00 00 00 00 00 00 00 0e 00						
00d0 00 00 00 00 00 ff fe 00 00 05 00 00 00 05 00						
00e0 00 00 00 68 00 00 00 00 00 00 00 00 00 00 00 00 . h						
00f0 00 00 00 00 00 21 00 25 00 00 00 00 00 10 00 . ! % . . .						
0100 00 00 1a 00 00 00 09 00 00 00 1a 00 00 00 60 00						
0110 02 00 00 00 00 00 2a 00						

Pada hari setelahnya pada pukul 15.06.32. file tersebut kembali diakses.

No.	Time	Source	Destination	Protocol	Length	Info
601	2017/138 15:11:12,568125	fe80::f5b3:851:d70b..	ff02::1:2	DHCPv6	173	Solicit XID: 0x07c04c CID: 000100011f203ee00019bb4f4cd8
611	2017/138 15:11:28,573482	fe80::f5b3:851:d70b..	ff02::1:2	DHCPv6	173	Solicit XID: 0x07c04c CID: 000100011f203ee00019bb4f4cd8
907	2017/138 15:12:00,582999	fe80::f5b3:851:d70b..	ff02::1:2	DHCPv6	173	Solicit XID: 0x07c04c CID: 000100011f203ee00019bb4f4cd8
1282	2017/138 15:12:10,781966	fe80::f5b3:851:d70b..	ff02::1:ff0d:3f96	ICMPv6	86	Neighbor Solicitation for fe80::6992:5661:9d0d:3f96 from 00:19:bb:4f:4c:d8
1285	2017/138 15:12:10,782511	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	TCP	86	[TCP Keep-Alive ACK] 1034 → 445 [ACK] Seq=1 Ack=2 Win=254 Len=0 SLE=1 SRE=2
1296	2017/138 15:12:11,232232	fe80::f5b3:851:d70b..	ff02::1:3	LLMNR	86	Standard query 0xd425 A isstatp
1299	2017/138 15:12:11,331251	fe80::f5b3:851:d70b..	ff02::1:3	LLMNR	86	Standard query 0xd425 A isstatp
11..	2017/138 15:13:20,640991	fe80::f5b3:851:d70b..	ff02::1:ff0d:3f96	ICMPv6	86	Neighbor Solicitation for fe80::6992:5661:9d0d:3f96 from 00:19:bb:4f:4c:d8
11..	2017/138 15:13:20,641380	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	SHB2	342	Create Request File: Administrator.TESTDOMAIN\Desktop\Share
11..	2017/138 15:13:20,641428	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	ICMPv6	86	Neighbor Advertisement fe80::f5b3:851:d70b:6d4 (sol, ovr) is at 00:19:bb:4f:4c:d8
11..	2017/138 15:13:20,645080	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	SHB2	166	Close Request File: Administrator.TESTDOMAIN\Desktop\Share
11..	2017/138 15:13:20,861139	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	TCP	74	1034 → 445 [ACK] Seq=361 Ack=318 Win=258 Len=0
46..	2017/138 15:15:20,862578	fe80::f5b3:851:d70b..	ff02::1:ff0d:3f96	ICMPv6	86	Neighbor Solicitation for fe80::6992:5661:9d0d:3f96 from 00:19:bb:4f:4c:d8
46..	2017/138 15:15:20,863084	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	TCP	86	[TCP Keep-Alive ACK] 1034 → 445 [ACK] Seq=361 Ack=318 Win=258 Len=0 SLE=317 SRE=318
46..	2017/138 15:17:20,863097	fe80::f5b3:851:d70b..	ff02::1:ff0d:3f96	ICMPv6	86	Neighbor Solicitation for fe80::6992:5661:9d0d:3f96 from 00:19:bb:4f:4c:d8
46..	2017/138 15:17:20,863176	fe80::f5b3:851:d70b..	fe80::6992:5661:9d0..	TCP	86	[TCP Keep-Alive ACK] 1034 → 445 [ACK] Seq=361 Ack=318 Win=258 Len=0 SLE=317 SRE=318

> Frame 46628: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
 > Ethernet II, Src: HewlettP_4f:4c:d8 (00:19:bb:4f:4c:d8), Dst: WIN-2012-R2-1 (00:00:83:e7:3a:14)
 > Internet Protocol Version 6, Src: fe80::f5b3:851:d70b:6d4, Dst: fe80::6992:5661:9d0d:3f96
 > Transmission Control Protocol, Src Port: 1034, Dst Port: 445, Seq: 361, Ack: 318, Len: 0

```

0000 00 00 83 e7 3a 14 00 19 bb 4f 4c d8 86 dd 60 00  ....:...OL...
0010 00 00 00 20 86 80 fe 80 00 00 00 00 00 f5 b3  .....
0020 00 51 d7 0b 86 d4 fe 80 00 00 00 00 00 69 92  Q.....
0030 56 61 9d 0d 3f 96 04 0a 01 bd 0d 8d 29 34 38 93  Va...?)48...
0040 8c 5b 80 10 01 02 77 ea 00 00 01 01 05 0a 38 93  .[....w....8...
0050 8c 5a 38 93 8c 5b 28 .....
```

2017-05-18-WannaCry-ransomware-using-ExternalBlue-exploit.pcap

Packets: 46654 · Displayed: 46654 (100.0%)

Profile: Default

Kemudian pada pukul 15.17.20 melakukan stay alive pada malware agar tetap meninfeksi system sampai dibayar oleh korban.

Σ | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c | | | | | Sign in | Sign up

70 / 72

Community Score

① 70 security vendors and 5 sandboxes flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
hdfrgui.exe

Size: 3.55 MB | Last Analysis Date: 1 day ago | EXE

peexo malware macro-create-ole runtime-modules detect-debug-environment checks-network-adapters exploit cve-2017-0147 long-sleeps direct-cpu-clock-access checks-user-input cve-2017-0144

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30 +

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

Popular threat label ① trojan.wannacry/wanna Threat categories trojan ransomware worm Family labels wannacry wanna wannacryptor

Security vendors' analysis ①

Acronis (Static ML)	① Suspicious	AhnLab-V3	① Trojan/Win32.WannaCryptor.R200572
Alibaba	① Ransom:Win32/WannaCry.398	ALYac	① Trojan.Ransom.WannaCryptor
Antiy-AVL	① Trojan[Ransom]/Win32.Wanna	Arcabit	① Trojan.Ransom.WannaCryptor.H
Avast	① SF-WNCrypt.Rr-A [Tril]	AVG	① SF-WNCrypt.Rr-A [Tril]

Do you want to automate checks?

File windows 7 enterprise juga memiliki isi berupa file exe yang bernama 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022clhdfrgui.exe yang ketika diupload ke virustotal merupakan virus dengan angka 70/72.

**THANK
YOU VERY
MUCH!**

