2018-Network Traffic Analysis for Ransomware

2018-資訊安全-網路封包分析

Diamond Liu / 劉得民

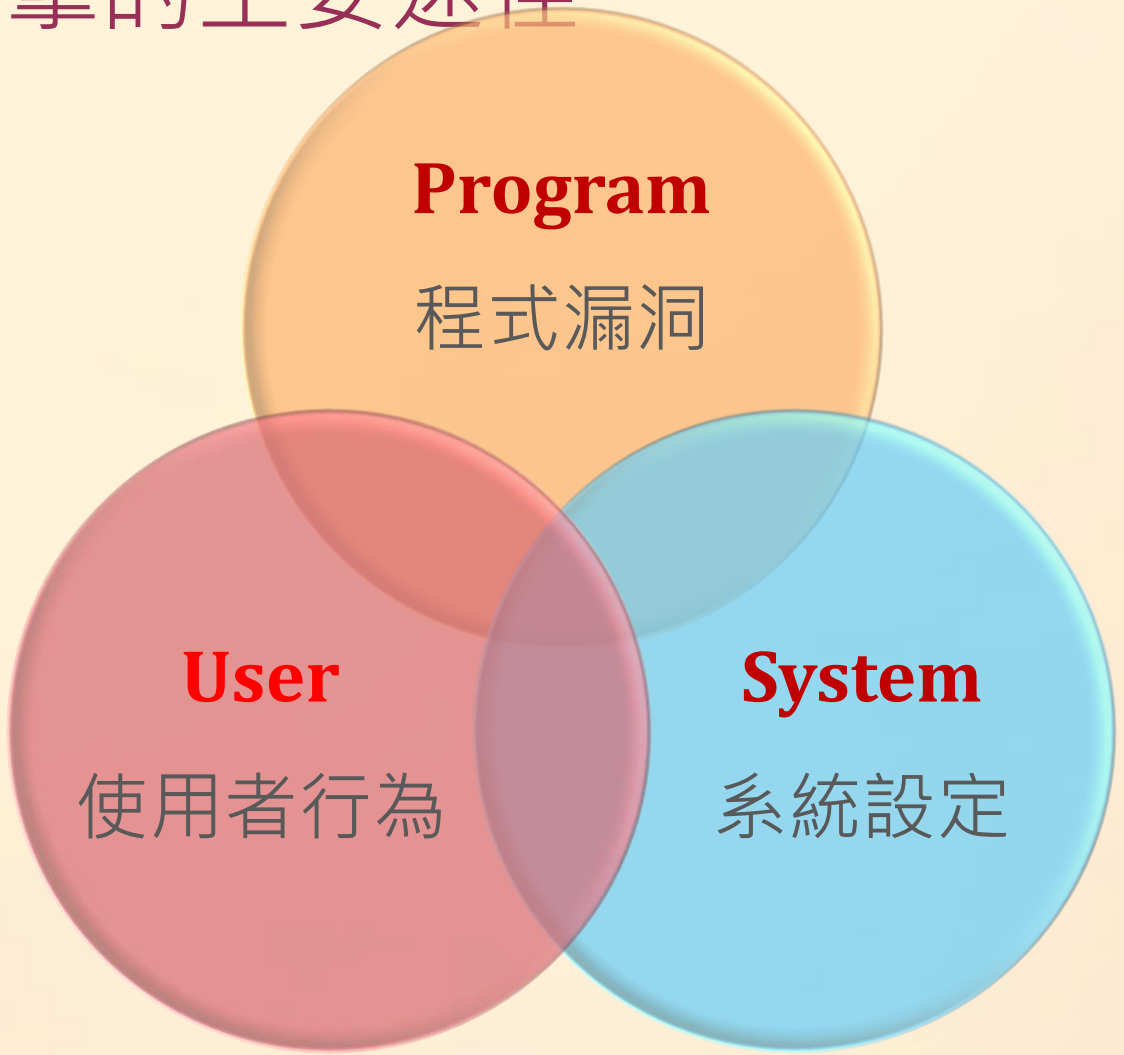
2018-資訊安全-網路封包分析

- 壹、網路封包基本介紹
- 貳、TOR 封包與 HTTPS 封包
- 參、Ransomware
- 肆、其他網路封包
- 伍、封包錄製與分析操作
- 陸、勒索軟體的應對討論
- 柒、問題與討論

基本介紹

- 加密勒索惡意程式簡介
- 網路通訊與Ransomware
- TOR的原理與封包範例

網路駭客攻擊的主要途徑



錄製網路封包的原理

- Method – Local? Switch? or Gateway?
- Physical – Line-Tapping? or Wifi Capturing?
- Software – TcpDump? WireShark? or A-PacketMan?
- Network Knowledge

VLAN 802.1P/802.1Q

Wireless 802.11a/802.11b

Wireless 802.11g/802.11n

Network Switch

Network Hub

Network Router

ADSL Modem

Network Address Translator

Network Firewall

NAS, SAN, LAN, WAN,…

Host Name

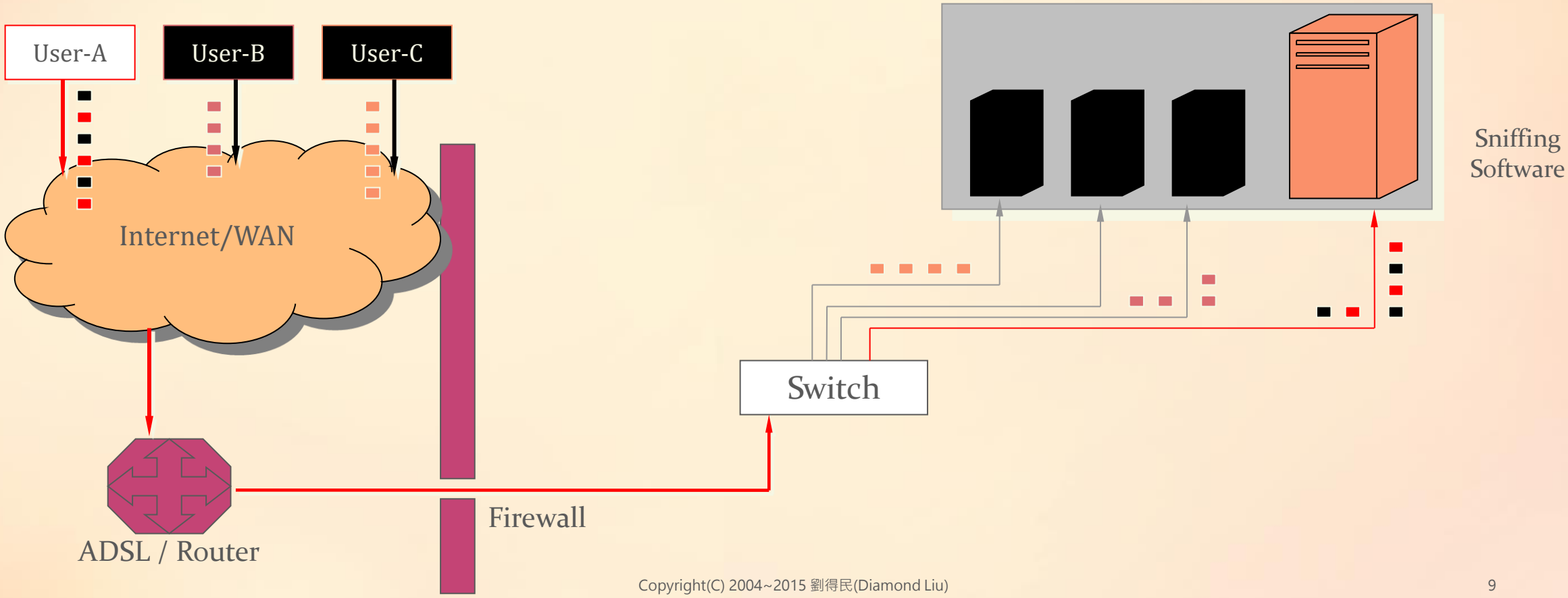
Computer Name

IP Address

MAC Address

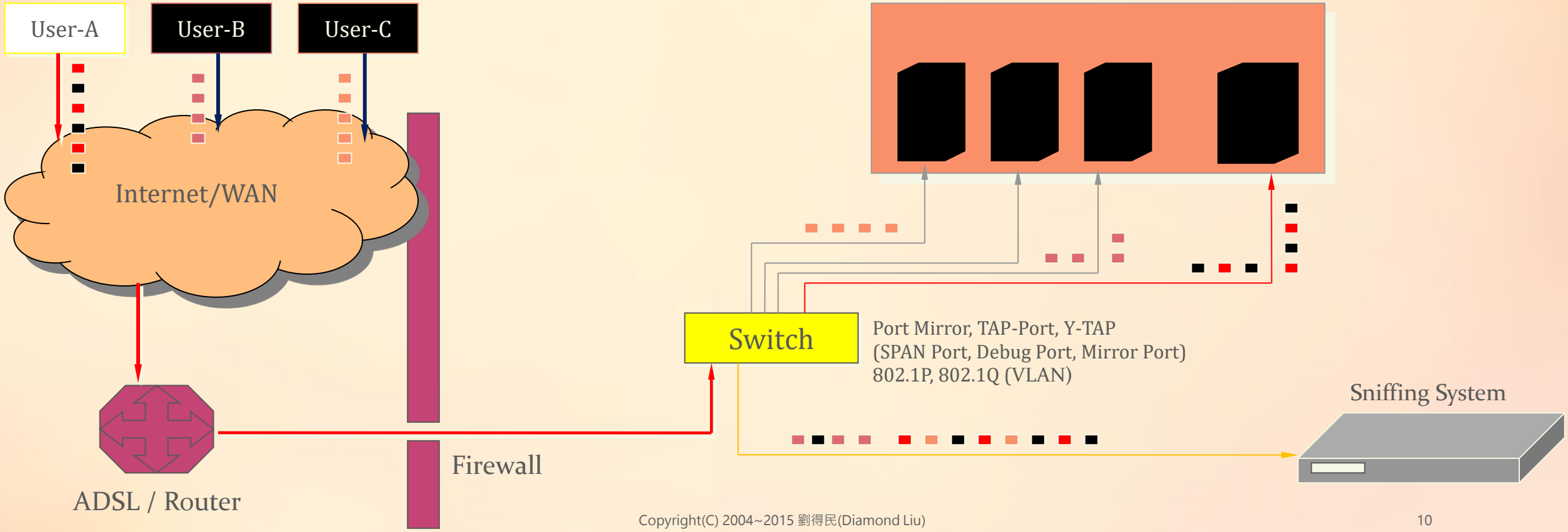
錄製網路封包的原理-方式1

Local-Host Sniffing : We install a sniffing software on local host to capture local I/O traffic.
Advantage : (1) Easy to implement (2) Would not effect other network devices
Weakness : (1) Only capture one computer's activities (2) Can not find a large scale of attack activities
Suitable Status : (1) Have a suitable target host (2) Investigate end user's computer



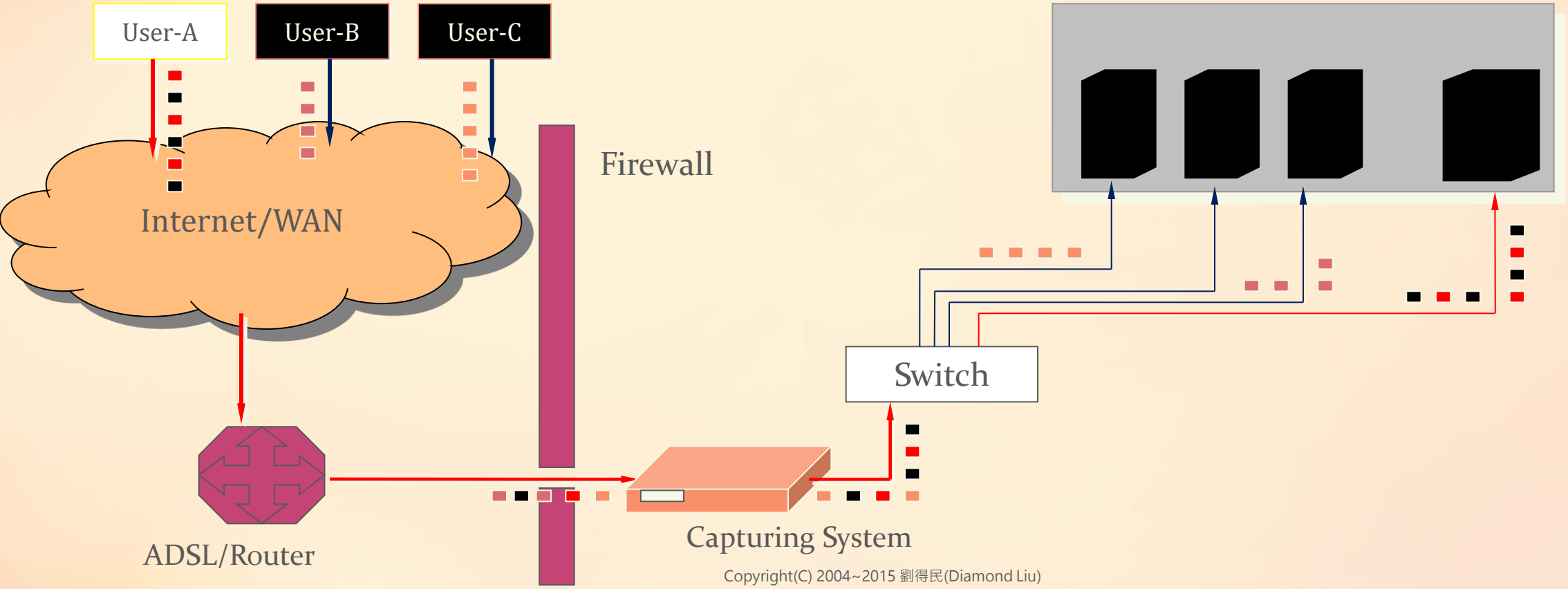
錄製網路封包的原理-2

Net Switch Sniffing : We collect network traffic from a switch' s mirror port and capture them by sniffing software.
Advantage : (1) Capture all computers' activities (2) Narrow down suspects into a small area
Weakness : (1) Can not handle huge traffic (2) Might lost important contents on a busy network
Suitable Status : (1) Early stage to find target host (Investigate) (2) Find out a large scale of attack activities.



錄製網路封包的原理-3

Gateway Sniffing : We intercept all traffic NIC-1 and transfer them into another NIC-2.
Advantage : (1) Capture all computers' activities (2) Get the SSL keys to decrypt payload
Weakness : (1) Cause a bottleneck to effect all network traffic or slow down the response time
Suitable Status : (1) Monitor HTTPS or Skype (2) Investigate the VoIP/Streaming session



讀取網路封包的方式

網路

- 直接從網路卡讀取(有線網路/無線網路)
- 要先安裝網路驅動程式(通常是LibPcap程式)

檔案

- 直接開啟封包檔案(標準檔案格式)
- TcpDump/WinDump/Wireshark

批次

- 連續讀取多個檔案或是多個目錄
- 先將光碟資料複製硬碟目錄, 進行批次處理

進階設定與操作

- 相關參數的設定-忽略封包
  - 適用: 尋找惡意程式、BotNet、勒索軟體、TOR(暗網)、主機駭客攻擊 ...
- 相關參數的設定-統計IP位址
  - 適用: 尋找 P2P下載來源、多點通訊(C&C 轉繼站) 、多點發散(機房模式) ....
- 相關參數的設定-IP-MAC對照
  - 適用: 尋找幽靈IP位址、DHCP變動、使用者變更IP位址 ....
- 網路封包分析與剪裁合併
  - 適用: 已取得封包原始檔案(Raw-Data)、消除網路雜訊、整理證據資料 ....
- 網路封包手動儲存與自動儲存

Principle of network traffic data analysis

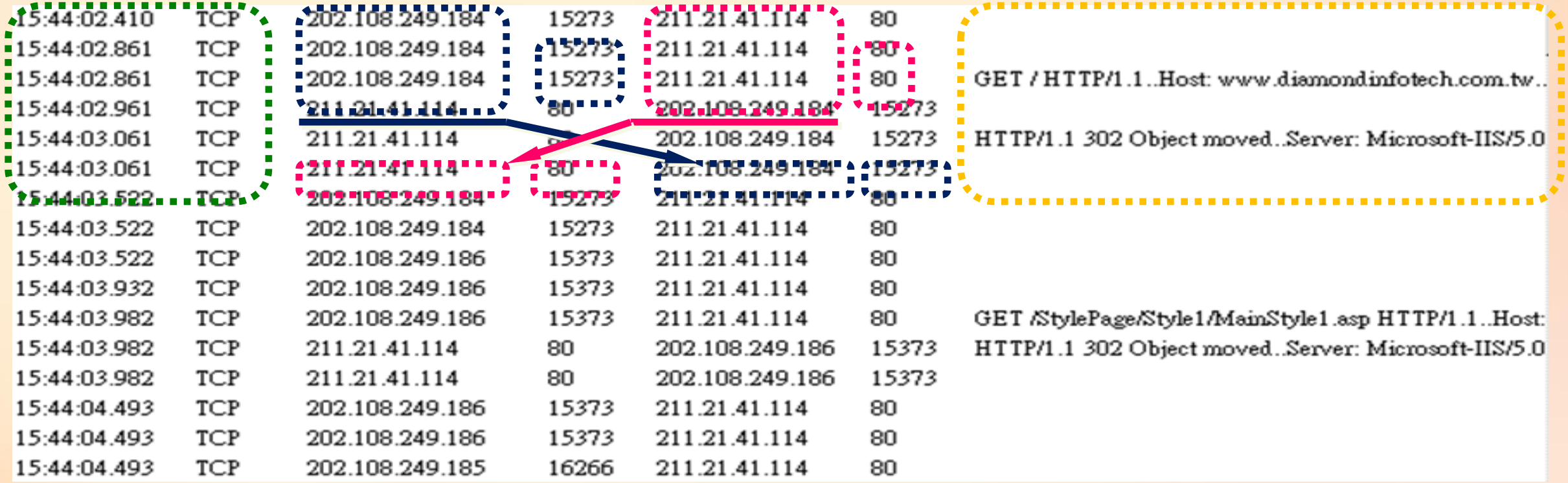
- Well-known Protocol and Plain-Text
- Analyze the interactive of following major data
  - Time and Protocol
  - Source IP Address and Service Port
  - Destination IP Address and Service Port
  - Content (Payload)

TCP? UDP? ICMP? ARP?

TCP 3 way hand-shaking
Only the IP address is can be confirmed in 2-way communication of a TCP session

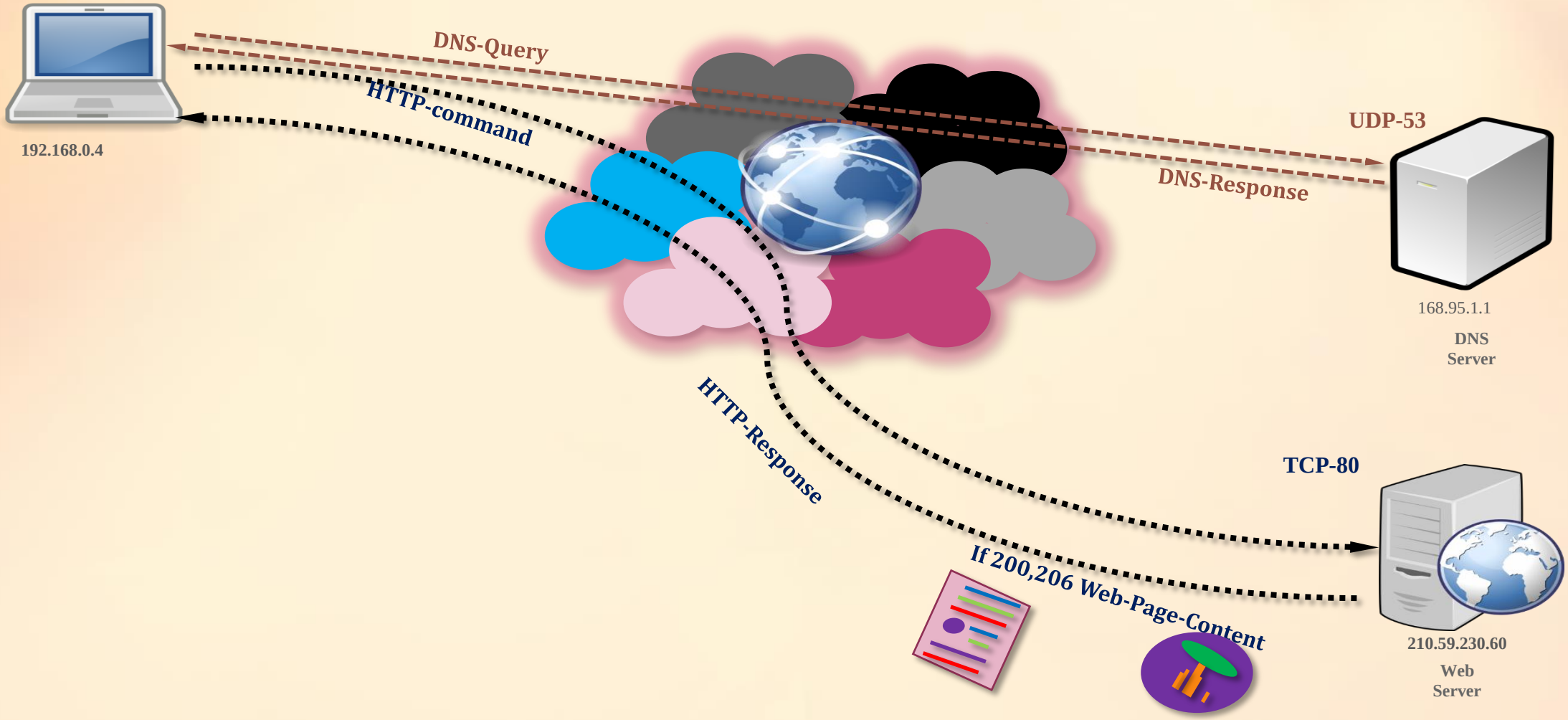
Which Port Number is < 1024 ?

Payload is Plain Text ? Or Mess Text ?

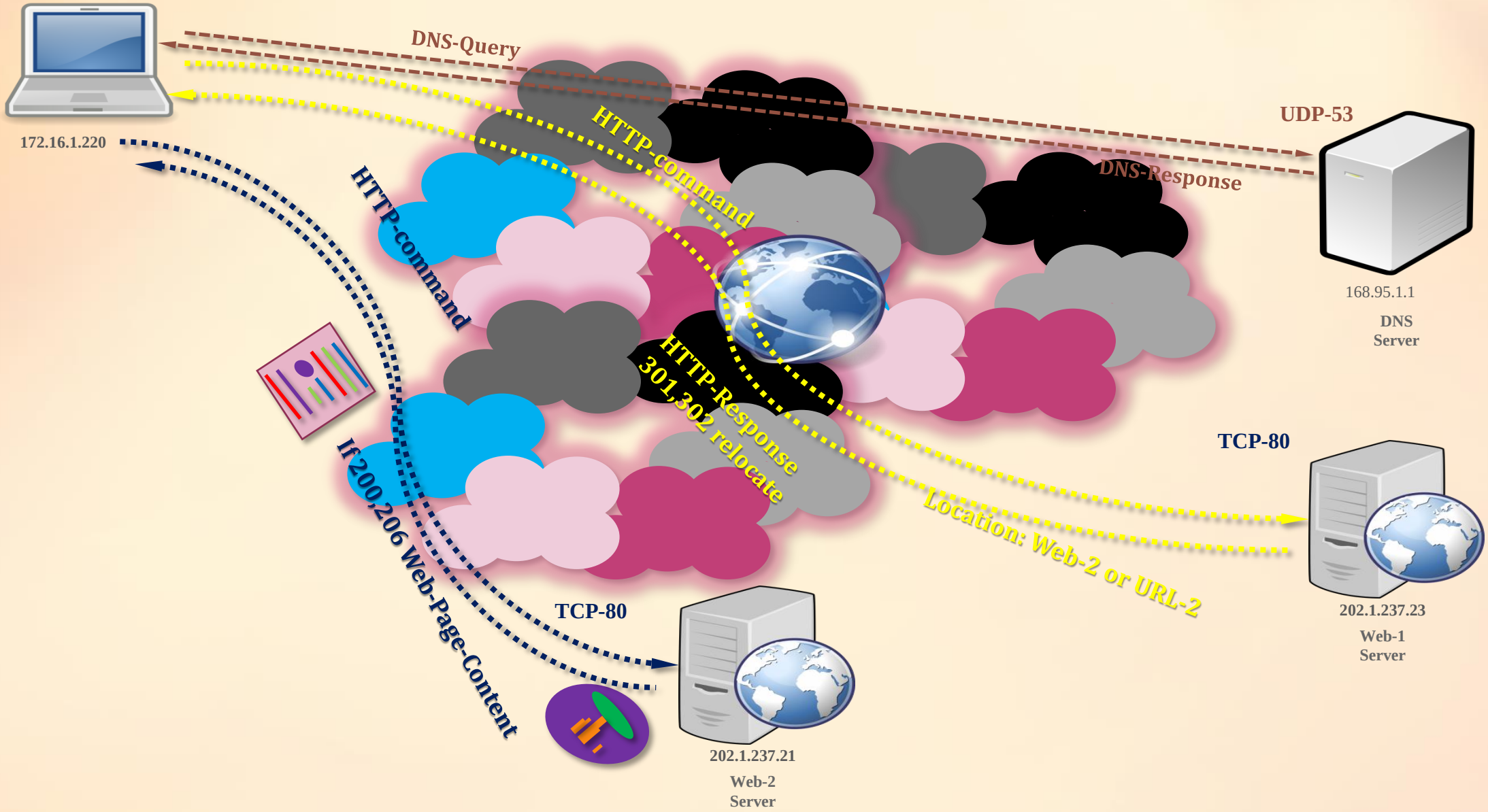


15:44:02.410	TCP	202.108.249.184	15273	211.21.41.114	80	
15:44:02.861	TCP	202.108.249.184	15273	211.21.41.114	80	
15:44:02.861	TCP	202.108.249.184	15273	211.21.41.114	80	GET / HTTP/1.1..Host: www.diamondinfotech.com.tw..
15:44:02.961	TCP	211.21.41.114	80	202.108.249.184	15273	
15:44:03.061	TCP	211.21.41.114	80	202.108.249.184	15273	HTTP/1.1 302 Object moved..Server: Microsoft-IIS/5.0
15:44:03.061	TCP	211.21.41.114	80	202.108.249.184	15273	
15:44:03.522	TCP	202.108.249.184	15273	211.21.41.114	80	
15:44:03.522	TCP	202.108.249.184	15273	211.21.41.114	80	
15:44:03.522	TCP	202.108.249.186	15373	211.21.41.114	80	
15:44:03.932	TCP	202.108.249.186	15373	211.21.41.114	80	
15:44:03.982	TCP	202.108.249.186	15373	211.21.41.114	80	GET /StylePage/Style1/MainStyle1.asp HTTP/1.1..Host:
15:44:03.982	TCP	211.21.41.114	80	202.108.249.186	15373	HTTP/1.1 302 Object moved..Server: Microsoft-IIS/5.0
15:44:03.982	TCP	211.21.41.114	80	202.108.249.186	15373	
15:44:04.493	TCP	202.108.249.186	15373	211.21.41.114	80	
15:44:04.493	TCP	202.108.249.186	15373	211.21.41.114	80	
15:44:04.493	TCP	202.108.249.185	16266	211.21.41.114	80	

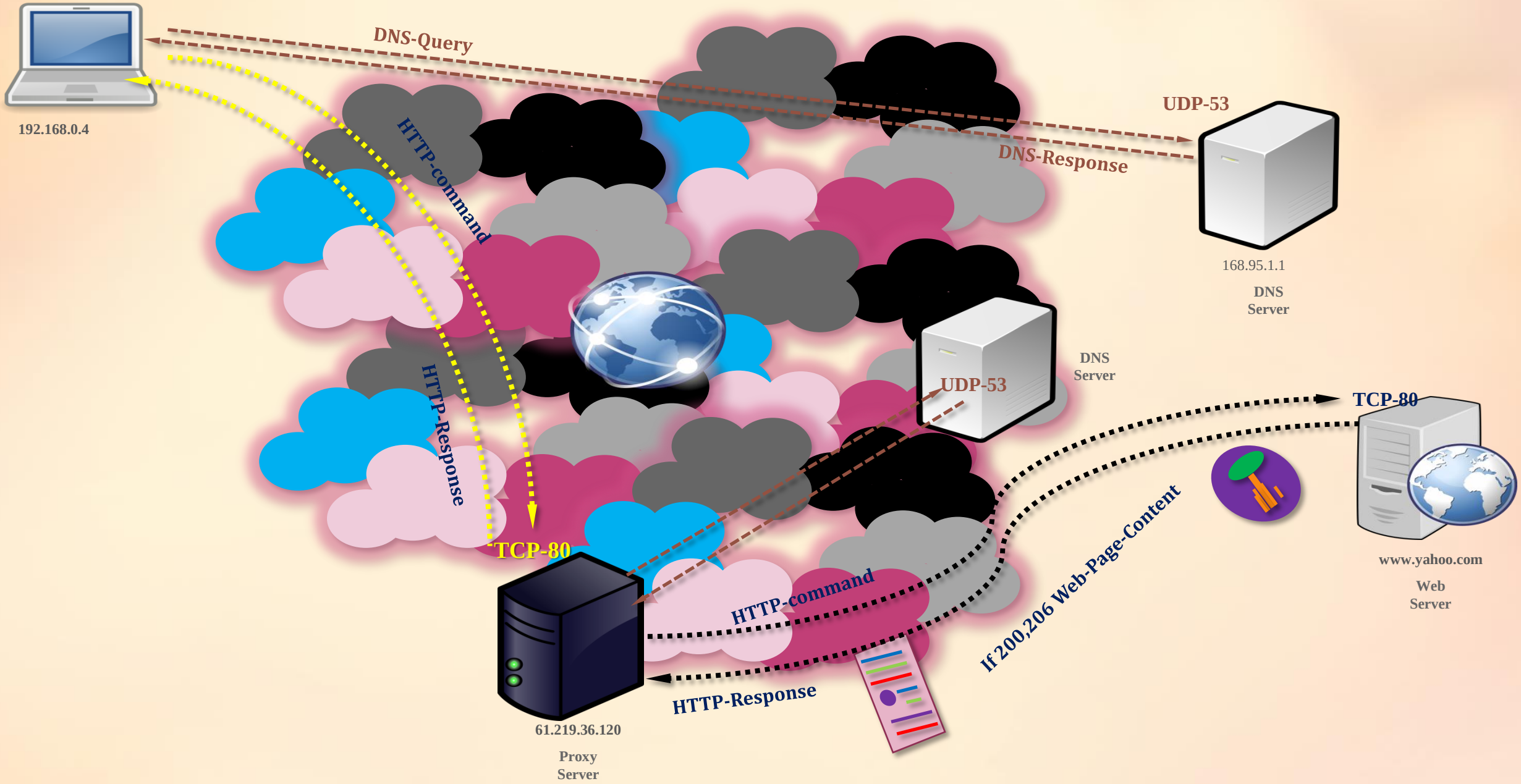
Protocol	Description	Port	Note
ARP	Transfer NIC-MAC Address and IP Address on Local Area Network(LAN). Before NIC sent TCP/UDP/ICMP packet, it will send ARP Packet to ask MAC-Address.	No any Port Number	Only LAN
DNS	Transfer Host Name and IP Address on Internet. Especially, it is the pre-behavior about computer browse the Web or send/receive email.	UDP-53 Normal TCP-53 * (ISP Only)	UPD-53 often
HTTP	At first, it is used for Web page browsing. Now a day, it is used for many Internet service Interface such like Webmail, Facebook, Twitter, …	TCP-80, TCP-8080, TCP-8000, TCP-10000	Very often
HTTPS	Secure web browsing, HTTP+SSL, Web bank or email login would use this.	TCP-443 (Encryption)	Often
SMTP	Sending email. Now a day, users send email by Web-mail so that SMTP is seldom used by end users. However, mail servers still use SMTP to send email.	TCP-25 (Default, no password)	Mail Server Very often
IMAP	Receiving email. This protocol will be more popular than POP3 in cyberspace.	TCP-143 (user-ID, password)	Mail Server Very often
POP3	Receiving email. As same as SMTP, it is rare in end users because Web-mail. Mail servers still use POP3 to receive email.	TCP-110 (user-ID, password)	Mail Server Very often
FTP	Files Transfer Protocol. This protocol also would be replaced by P2P or Cloud Storage (Web, HTTP or HTTPS) but online games still use this to update Apps.	TCP-21 (TCP-20) (user-ID, password)	Online Game Very often
Telnet	It is telecomm command with plain text mode. Mostly it is used for Firewall or Wireless Access Point device by maintenance engineers.	TCP-23 (user-ID, password)	Rare (Night-Fatal)
CIFS	It is used for Network Neighborhood which provides the following purpose, (1) Login/Logout (2) Shared Resource (3) Printing Service.	TCP-139, TCP-445 UDP-135~UDP-138	Very often (WAN-Fatal)
MS-SQL	Microsoft SQL Database Server Service.	TCP-1433 UDP-1434	Rare (DBs – Often)
Remote Desktop	Windows Terminal Service. It provides remote desktop service same as Citrix RDP. Mostly it is used for Servers maintenances from WAN/LAN.	TCP-3389 (user-ID, password)	Rare (Night-Fatal)



General Behavior of Visiting Web

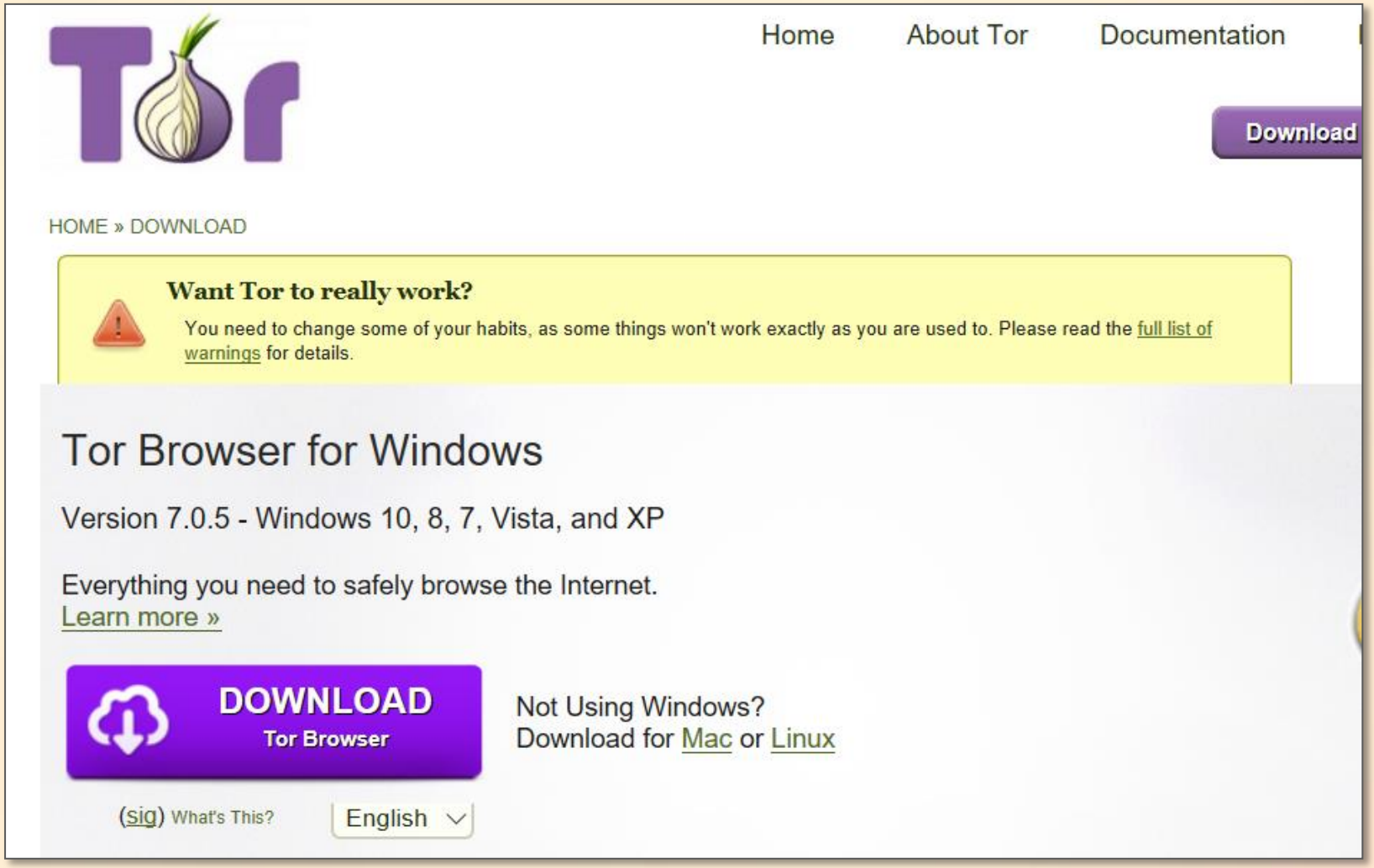


Relocation Behavior of Visiting Web

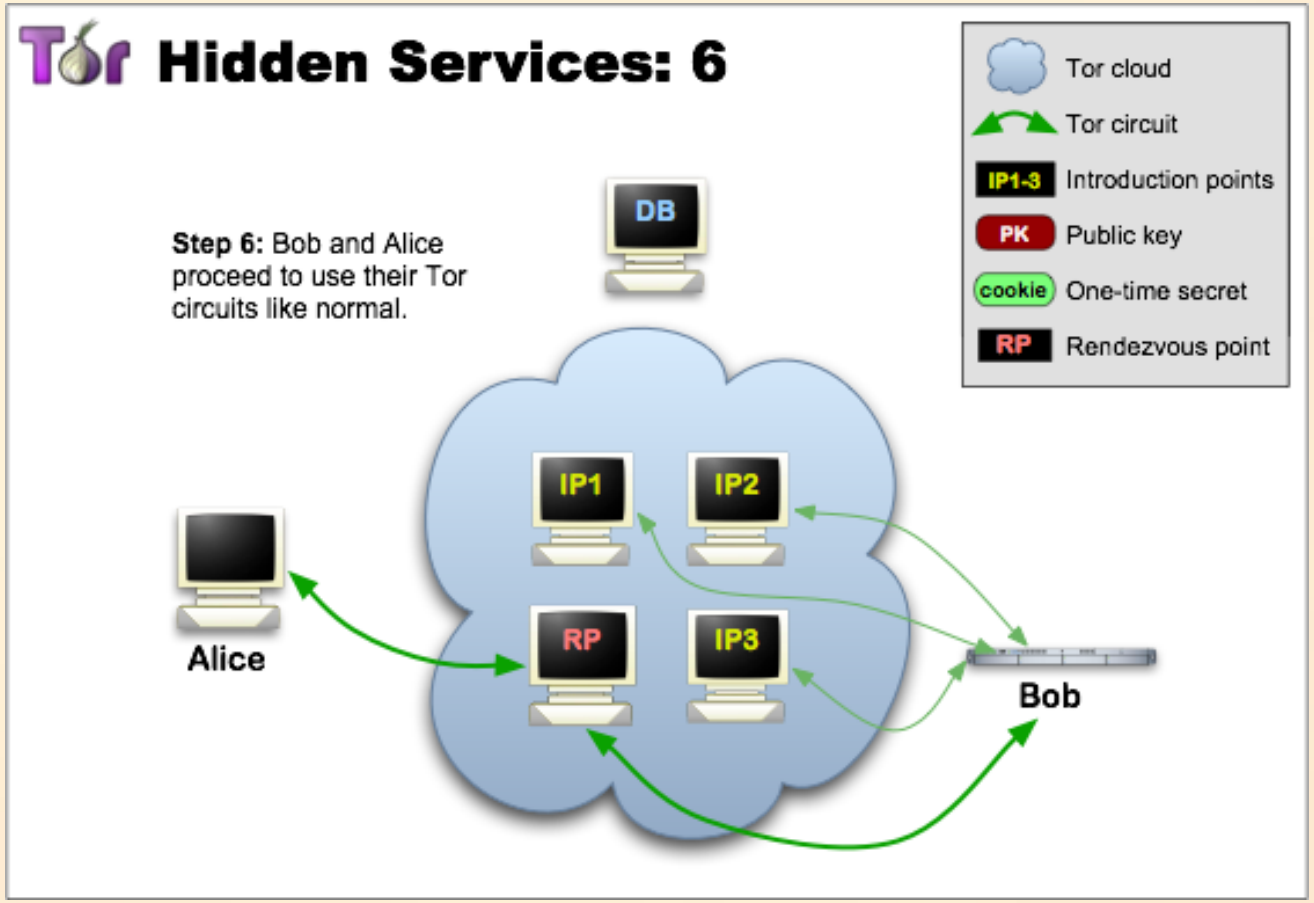


General Behavior of Visiting Web with Proxy

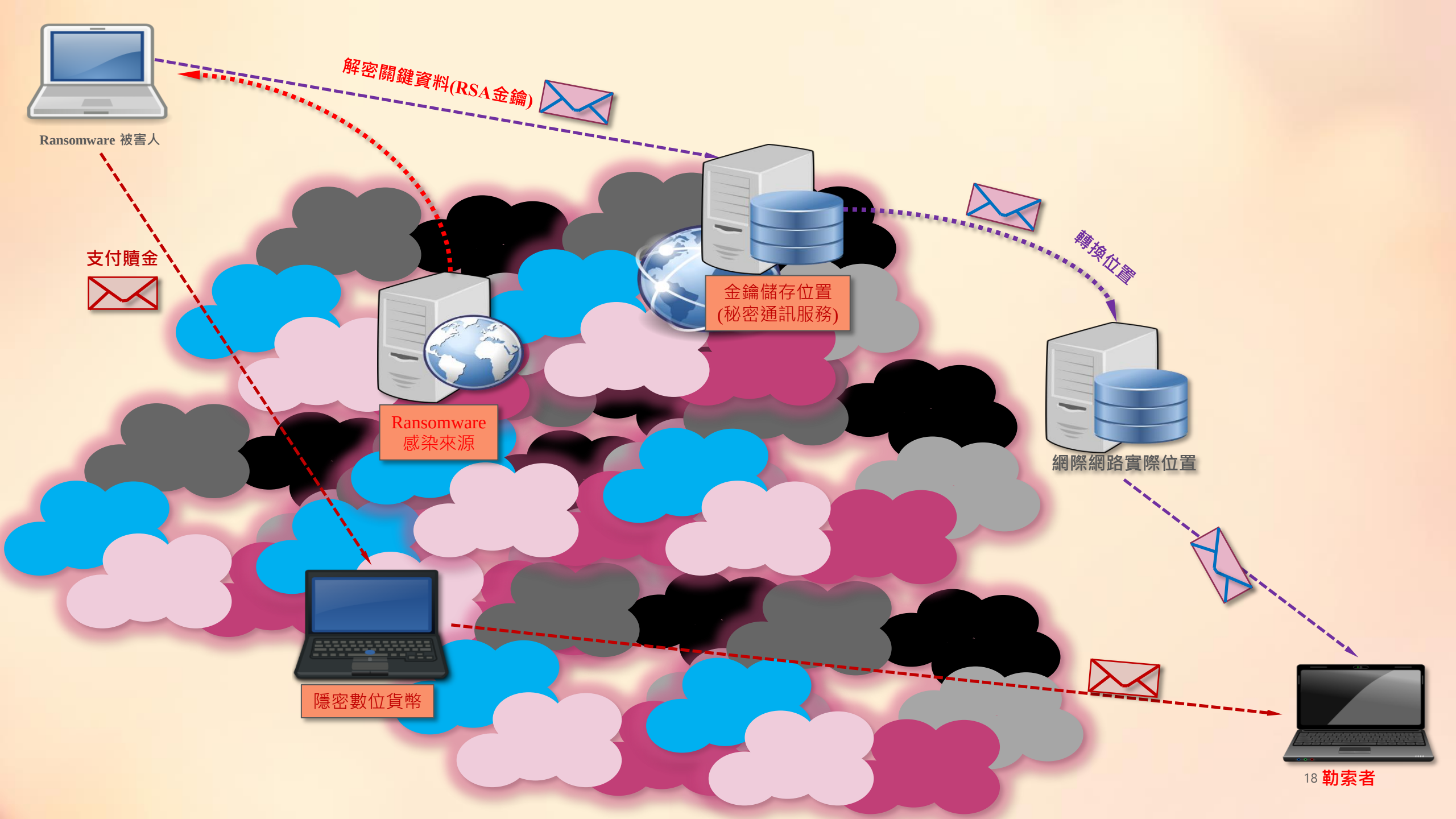
TOR, The Onion Router, 洋蔥路由瀏覽器

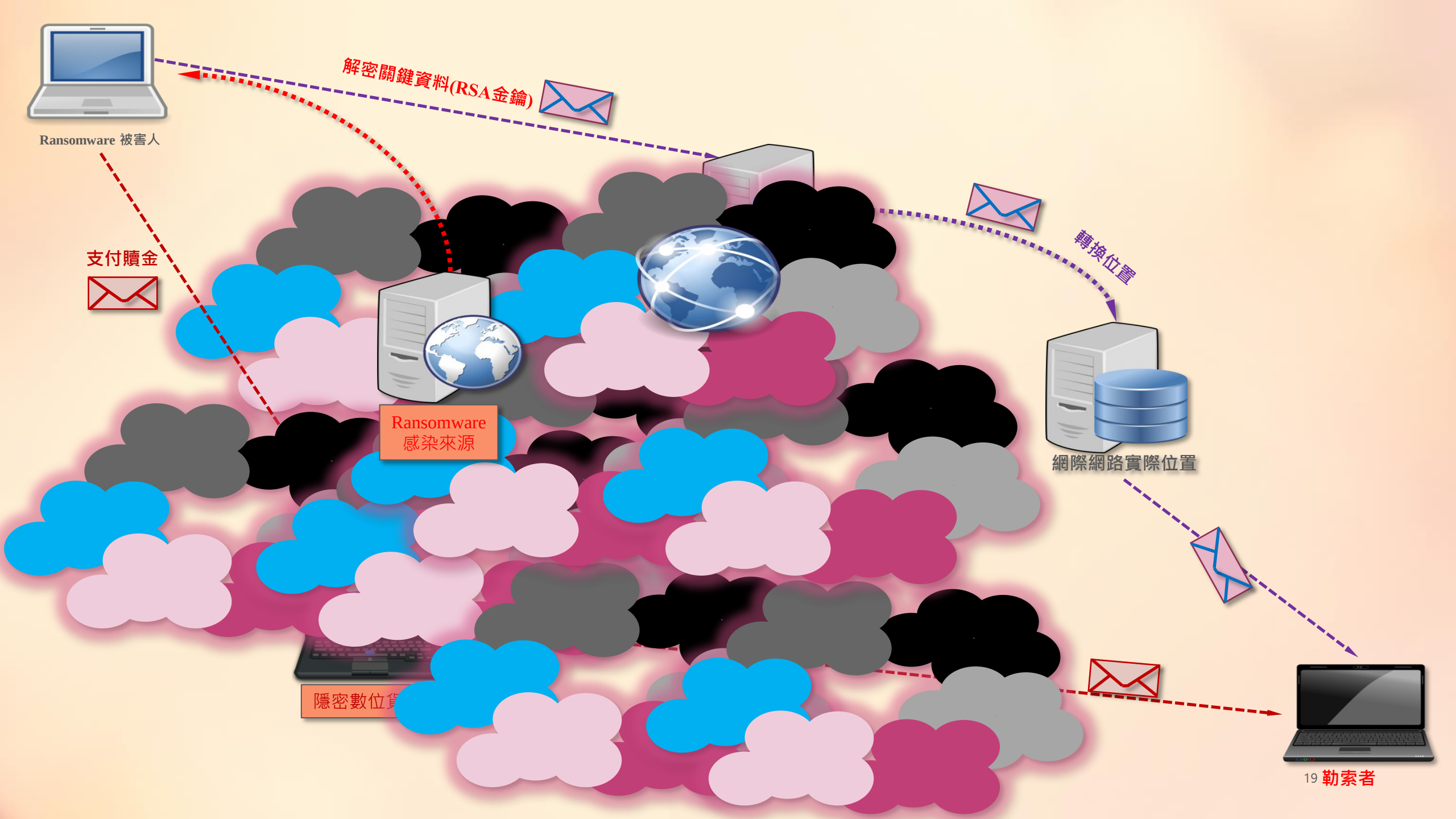


TOR的原理與封包範例



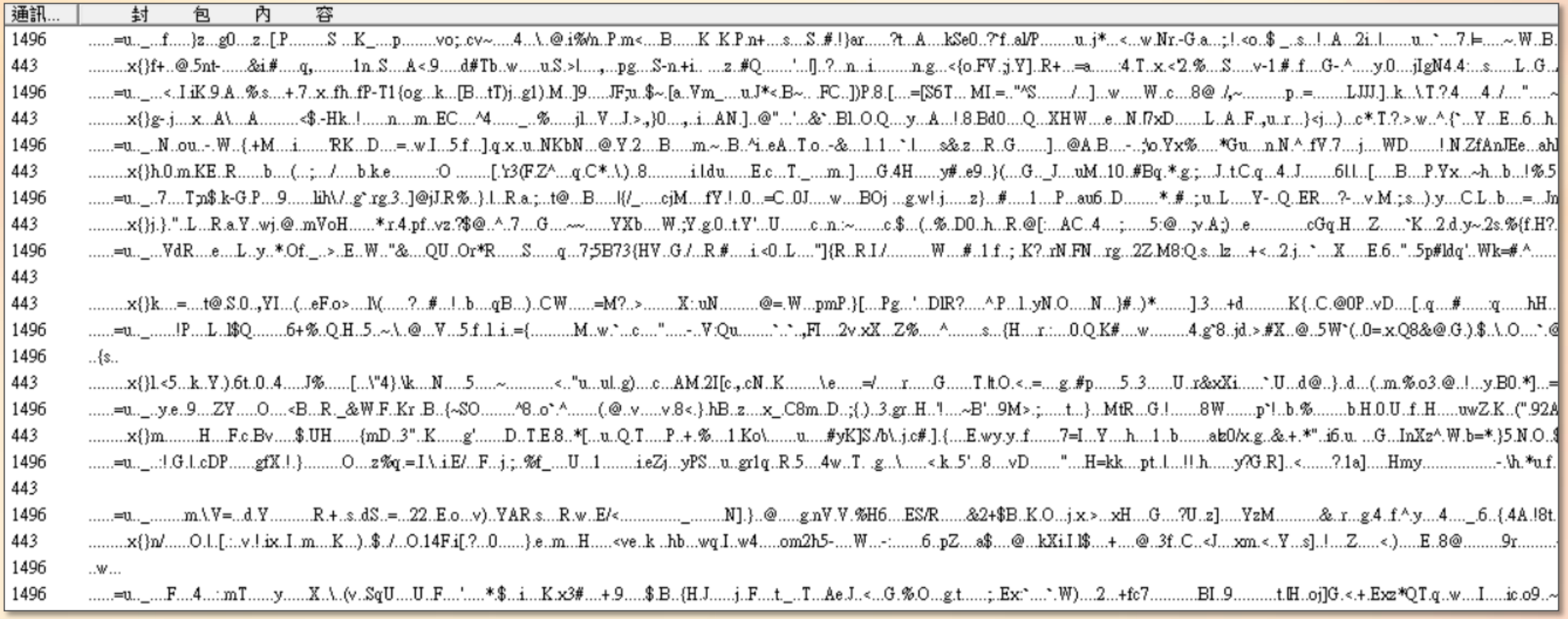
圖片參考來源: https://www.torproject.org/docs/hidden-services.html.en


Ransomware 被害人
解密關鍵資料(RSA金鑰)
支付贖金
金鑰儲存位置
(秘密通訊服務)
轉換位置
Ransomware
感染來源
網際網路實際位置
隱密數位貨幣
勒索者


Ransomware 被害人
解密關鍵資料(RSA金鑰)
支付贖金
轉換位置
Ransomware
感染來源
網際網路實際位置
隱密數位貨
勒索者

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:15:55.676	TCP	192.168.1.117	1496	158.69.204.36	443	
14:15:55.896	TCP	158.69.204.36	443	192.168.1.117	1496	
14:15:55.896	TCP	192.168.1.117	1496	158.69.204.36	443	
14:15:57.236	TCP	192.168.1.117	1496	158.69.204.36	443	.....M....E.{+.f.6b....s..ldp....+./.,0.....3.9./.5.....j.....www.vo4u.com.....#..... .....
14:15:57.464	TCP	158.69.204.36	443	192.168.1.117	1496	....>...:..d...../h....w..E....Z%,0.SM....0.....0...0..0..(.....{-..Z..0...*.H.....0$1"0 ..U....www.z7fkhs57msbtd.
14:15:57.464	TCP	158.69.204.36	443	192.168.1.117	1496	....a.
14:15:57.464	TCP	192.168.1.117	1496	158.69.204.36	443	
14:15:57.467	TCP	192.168.1.117	1496	158.69.204.36	443	....F...BA.O@.T...&..*.N-.W.....C7n.@..^.{.!...r/..c&...v:..`.=$v...DG.....g.....(....x{}b,g...Bl..c....7.....%...x.
14:15:57.687	TCP	158.69.204.36	443	192.168.1.117	1496	.....(.=u._....Rh.R.o.....vR:..o..}s..F.]..o^
14:15:57.687	TCP	192.168.1.117	1496	158.69.204.36	443	....!....x{}c....)]p.....97..r4....
14:15:57.908	TCP	158.69.204.36	443	192.168.1.117	1496	.....=u._..D.....i."..._...m6..8gd...W{....P.M...?%D...i....J.....t.!...#....F...\Kz..=i.....R.....;4:9.....Q.d,hNE....}.R.Ul_..r~..
14:15:57.908	TCP	158.69.204.36	443	192.168.1.117	1496	.I..6KsX....T.jl...w..[1...K..aa...E<G.p._Q...e.uU-...
14:15:57.908	TCP	192.168.1.117	1496	158.69.204.36	443	
14:15:57.910	TCP	192.168.1.117	1496	158.69.204.36	443	....x{}d...f..*Jr.l.`.....G.....WQ..R0.9.{.x..Y.`C..v.....#.~i....*.+.X.Z.).....l7...L.`8..S..#.9H.<....(.....[....[.....3..de....8...A.S..
14:15:57.910	TCP	192.168.1.117	1496	158.69.204.36	443	.....kRhU.#...\.`=..#....]..."..o...yL.....o.....".(...l...QQ.?,A W\(....+.Q..H..W..VX..uw.....?"....<.6U5r1..B...o}.&.xu....g,_v..'
14:15:58.132	TCP	158.69.204.36	443	192.168.1.117	1496	..T...
14:15:58.140	TCP	158.69.204.36	443	192.168.1.117	1496	.....=u._...N.+.<m....PQ.4.QMYT/...Z....>..].4....@e....."..j^....*4..<.....G.aWL'.....&..a.J.u@..;?...9.N..D..e.c....d....P....D..Z..
14:15:58.140	TCP	158.69.204.36	443	192.168.1.117	1496	...:t.....og.^?.Z....)O..N.k.f.BXnf.S..YTv.pb.:."g...S.W...9..$9..)..p*bla...S.g.8{..=...6.X$&.....t.,
14:15:58.140	TCP	192.168.1.117	1496	158.69.204.36	443	
14:15:58.154	TCP	192.168.1.117	1496	158.69.204.36	443	.....x{}e.W..N...).i....^V4.o..B...*..k..t..)W.....~....:a.,.....y._.....&&}..1..5_.1...l.Kn.....s.?.....,.rf...5f.1xRh..5B.._.c..
14:15:58.154	TCP	192.168.1.117	1496	158.69.204		
14:15:58.376	TCP	158.69.204.36	443	192.168.1.1		

通訊...	封　包　內　容
443	
1496	
443	
443	.....M....E.{+.f.6b....s..ldp....+./.,0.....3.9./.5.....j.....www.vo4u.com.....#..... .....
1496	....>...:..d...../h....w..E....Z%,0.SM....0.....0...0..0..(.....{-..Z..0...*.H.....0$1"0 ..U....www.z7fkhs57msbtd.5zme.com0...1704060000000Z..18010600000000Z0.1.0...U....www.n6ii4jed.5bsr.net0..0...*.
1496	....a.
443	
443	....F...BA.O@.T...&..*.N-.W.....C7n.@..^.{.!...r/..c&...v:..`.=$v...DG.....g.....(....x{}b,g...Bl..c....7.....%...x.
1496	.....(.=u._....Rh.R.o.....vR:..o..}s..F.]..o^
443	....!....x{}c....)]p.....97..r4....
1496	.....=u._..D.....i."..._...m6..8gd...W{....P.M...?%D...i....J.....t.!...#....F...\Kz..=i.....R.....;4:9.....Q.d,hNE....}.R.Ul_..r~._...]K.d...E..+...h...vgf.$.R... M.k....cS.!....ziHB...z.-t.....bZ;.5.....J<....V.....h...H.}...h..".
1496	.I..6KsX....T.jl...w..[1...K..aa...E<G.p._Q...e.uU-...
443	
443	....x{}d...f..*Jr.l.`.....G.....WQ..R0.9.{.x..Y.`C..v.....#.~i....*.+.X.Z.).....l7...L.`8..S..#.9H.<....(.....[....[.....3..de....8...A.S.....".^~.m.kZ.....}?.f...s..L.%\.&.ez....y.cgi.s6}.).....?....Nc^.r.....!.iu2.92...0...Jw...%.=.g.l
443	.....kRhU.#...\.`=..#....]..."..o...yL.....o.....".(...l...QQ.?,A W\(....+.Q..H..W..VX..uw.....?"....<.6U5r1..B...o}.&.xu....g,_v.."4.u.F.2l..K.....a%..M^...Cm4IS$.d.....s..\.g..7.....{].8..2c...4.p.....V.X"...2E....[../._.
1496	..T...
1496	.....=u._...N.+.<m....PQ.4.QMYT/...Z....>..].4....@e....."..j^....*4..<.....G.aWL'.....&..a.J.u@..;?...9.N..D..e.c....d....P....D..Z.&.....*L.9...'.#..7.....!....n.....,.LGqO`...n..@.,U.n.U..s..(....f3.....9.O..f..>.f.$.s1\....<*.
1496	...:t.....og.^?.Z....)O..N.k.f.BXnf.S..YTv.pb.:."g...S.W...9..$9..)..p*bla...S.g.8{..=...6.X$&.....t.,
443	
443	.....x{}e.W..N...).i....^V4.o..B...*..k..t..)W.....~....:a.,.....y._.....&&}..1..5_.1...l.Kn.....s.?.....,.rf...5f.1xRh..5B.._.c...T.~.u....p-.e. q.....8...Q.I...&..~t..RH.....6.....f'f...c./..X....F1..-bx.L..(.ZO.X..b`HVR/..P(.5.
443	...d0....c.O>.\..#9....+74w..B./Rwp.O*...>.k.b.....c..O.j..m..6...T....Mz.A.....~1~.w...:...2..xr.M5E..Il.>..
1496	..G.d.



通訊...	封　包　內　容
1496	.....=u..._...f.....}z...g0....z..[.P.....S ..K_....p.....vo;..cv~.....4...\..@.i%\n..P.m<....B.....K .K.P.n+....s...S..#.!}ar.....?t...A....kSe0..?`f..al/P.....u..j*...<...w.Nr.-G.a...;.!.<o..$ _..s...!..A...2i..l.....u...`....7.!=.....~.W..B.
443	.....x{}f+..@.5nt-.....&i.#.....q,.....1n..S....A<.9....d#Tb..w.....u.S.>l....,...pg...S-n.+i.. ....z..#Q.....'...[]..?...n...i.....n.g...<{o.FV.j.Y].R+...=a.....:4.T..x.<'2.%...S.....v-1.#..f....G-.^.....y.0....jIgN4.4:...s.....L..G..;
1496	.....=u..._...<..I.iK.9.A..%.s....+.7..x..fh..fP-T1{og...k...[B...tT)j..g1).M..]9.....JF;u..$~.[a..Vm_....u.J*<.B~.. .FC..])P.8.[....=[S6T... MI.=.."^S....../...]...w.....W..c....8@ ./,~.....p..=.....LJJJ.]..k..\.T.?.4....4../...".....~
443	.....x{}g-.j....x...A\....A.....<$.-Hk..!.....n....m..EC....^4....._.%.....jl...V...J.>.,}0...,..i...AN.]..@"...'...&`..Bl..O.Q....y...A...!.8.Bd0....Q...XHW....e...N.f7xD.....L..A..F.,u..r...}<j...)...c*.T.?.>.w..^.{`...Y...E...6...h.
1496	.....=u..._..N..ou..-.W..{.+M....i.....'RK...D....=..w.I...5.f...].q.x..u..NKbN...@.Y.2....B.....m.~..B..^i..eA..T.o..-&....l..1...`.l.....s&.z...R..G.....]...@A.B....-..;'o.Yx%.....*Gu....n.N.^..fV.7....j....WD.....!.N.ZfAnJEe...ahJ
443	.....x{}h.0.m.KE..R.....b....(...;.../.....b.k.e.....:O .....[.\r3(F.Z^....q.C*.\.)..8.....i.l.du.....E.c...T._....m..]....G.4H.....y#..e9..}(....G..._J....uM..10..#Bq.*.g.;....J..t.C.q...4..J.....6l.l..[.....B....P.Yx...~h...b...!%.5
1496	.....=u..._..7....T;n$.k-G.P....9.....lih\./..g`.rg.3..]@jJ.R%..}.l..R.a.;...t@...B.....l{/_.....cjM....fY.!..0...=C..0J....w....BOj ...g.w!.j.....z}...#.....1....P...au6..D.....*.#..;.u..L.....Y-..Q..ER....?-...v.M.;.s...).y....C.L..b....=...Jn
443	.....x{}j.}."..L...R.a.Y..wj.@..mVoH.....*.r.4.pf..vz.?$@..^..7....G....~~.....YXb....W.;Y.g.0..t.Y'...U.....c..n.:~.....c.$...(..%..D0..h...R.@[:...AC..4....;.....5:@...;v.A;)...e.....cGq.H....Z.....`K...2.d.y~.2s.%{f.H?.
1496	.....=u..._...VdR....e....L..y..*.Of._..>..E..W.."&....QU..Or*R.....S.....q...7;5B73{HV..G./...R.#....i.<0..L...."]{R..R.I./.....W....#..1.f..; .K?..rN.FN...rg...2Z.M8:Q.s...lz....+<...2.j...`....X.....E.6.."..5p#ldq'..Wk=#.^.....
443	
443	.....x{}k....=....t@.S.0..,YI...(...eF.o>....l\(.....?...#...!..b....qB...)..C W.....=M?..>.....X:.uN.....@=.W...pmP.}[....Pg...'...DlR?.....^.P...l..yN.O.....N...}#..)*.....].3....+d.....K{..C.@0P..vD....[.q....#.....:q.....hH..
1496	.....=u..._.....!P....L..l$Q.....6+%..Q.H..5..~.\..@...V...5.f..l..i..={.....M..w.`...c...".....-..V:Qu.....`..`.,FI....2v.xX...Z%....^.....s...{H....r:....0.Q.K#....w.....4.g`8..jd..>.#X..@..5W`(..0=.x.Q8&@.G.).$..\..O....`.@
1496	..{s..
443	.....x{}l.<5...k..Y.).6t..0..4.....J%.....[...\"4}.\k....N.....5.....~.....<.."u...ul..g)....c...AM.2I[c.,cN..K.....\.e.....=/.....r.....G.....T.lt.O.<..=....g..#p.....5..3.....U..r&xXi.....`.U...d@..}..d...(..m.%.o3.@..!...y.B0.*]...=
1496	.....=u..._..y.e..9....ZY.....O....<B...R._&W.F..Kr .B..{~SO.....^8..o`.^.....(.@..v.....v.8<.}.hB..z....x_.C8m..D..;{.)..3.gr..H..'!....~B'..9M>.;.....t...}...MtR...G.!.....8W.....p`!..b.%.....b.H.0.U..f..H.....uwZ.K..(".92A
443	.....x{}m.....H....F.c.Bv.....$.UH.....{mD..3"..K.....g'.....D..T.E.8..*[...u..Q.T.....P..+.%....1.Ko\.....u.....#yK]S./b\..j.c#.].{....E.wy.y..f.....7=I...Y....h....1..b.....ab0/x.g..&.+.*"..i6.u. ...G...InXz^.W.b=*.}5.N.O..$
1496	.....=u..._..:!.G.l..cDP.....gfX.!.}.....O....z%q.=I.\..i.E/...F..j.;..%f_....U...1.....i.eZj...yPS...u..gr1q..R.5....4w..T. .g...\.....<.k..5'..8....vD....."....H=kk....pt..l...!!.h.....y?G.R]..<.....?.1a].....Hmy.....-.\h.*u.f.
443	
1496	.....=u..._.....m.\.V=...d.Y.....R.+..s..dS..=...22..E.o...v)..YAR.s....R.w..E/<....._.....N].}..@.....g.nV.V.%H6....ES/R.....&2+$B..K.O...j.x.>...xH....G....?U..z].....YzM.....&..r...g.4..f.^.y....4...._6..{.4A.!8t.
443	.....x{}n/.....O.l..[.:..v.!.ix..I..m....K...)..$../...O.14F.i[.?...0.....}.e..m...H.....<ve..k ..hb...wq.I..w4.....om2h5-....W...-:.....6..pZ....a$....@...kXi.I.l$....+....@..3f..C..<J....xm.<..Y...s]..!....Z.....<.).....E..8@.....9r.....
1496	..w...
1496	.....=u..._....F....4...:.mT.....y.....X..\..(v..SqU....U..F...'.....*.$...i....K.x3#....+.9....$.B..{H.J.....j..F....t._..T...Ae.J..<...G.%.O...g.t.....;..Ex:`....`.W)....2...+fc7.....BI..9.....t.H..oj]G.<.+.Exz*QT.q..w....I.....ic.o9..~

通訊...	封　包　內　容
443	
1481	
443	
443	.....m....b..+<DcZ;.....nf..-s....}....+./.,0.....3.9./.5.....~...%.#.. www.3qnafyqb7azpcdlsgy7su6cl.com.....#..... .....
1481	...~..
1481	....>...:.....$#R....'..N.q..S.'.O.....@..0.....0...0..(.....{-..Z..0...*.H.....0$1"0 ..U....www.z7fkhs57msbtd5zme.com0...170406000000Z..180106000000Z0.1.0...U....www.n6ii4jed5bsr.net0..0...*.H
443	....F...BA.Z,c.U.NZr.~.....,Q.>..(t.H..g.~.'.l.W....KG .1..R..O...R.]".....(..C.g..Ud...Pq..*.).#.{<.D....s....6.'^
1481	.....(.L..5.....[u+..^...A.c....r.....s..
443	....!..C.g..V<....x.....t..C..(%.
1481	.....L..5....8On...F\.1...^.....gq.h~.2HiRj..?...\.1'...d3c..&..L..x.w.Z.....A...I;.....I.$T.....=YiK.3#2.Q.....M.JM...u..j..qs.Y:..>R....0...k.w. {g5=.D.#...#.w...l..f....3.0.....'.....CR.....uu?.....l..8.b..^.O...>.kL...Zu.....5
1481	.@}"=...X..>.....m3.D;.H..A.....W`...<U.....l"....
443	
443	.....C.g..W.....B"R...o....X....u..e..W.....k....[...*....?.A...j..Dp@...J.+.Ax/g....S<.....(3.i...E...}..@./..5.u...[.....}..XT.d....$.....\.9.m.3.?*PG.&..U'...u.->p..t...._F....J.....?>.l....*y..Y5.m..J.q.....t."..U.P.!c72ps....0...ax.
443	..y..!.....P....K....`~.i....N0...ai.w..+..0.}.s)....T.U.....5.d.gR..7....n..EY+/.4.o.....(-.@....t.l>..
1481	....=.
1481	.....L..5....:.$.....+....4..p#t.....u..G....o%.$..Mr.p....X.g.?...'....\.iw..c.3..b..t._bB..j..`..J.. u..c..x.D.....w.7'B.....f.....W..]m.....]F.B.u.cd..@.,.XG.....l.7..x-.....t"..V..b....'[.b....E.....U....:.]..... NV.%.?..L.]7WG..0..-.9_.
443	.....C.g..X*..C....s.....s:...6.~...[...../.T..a..h.....nD.g.f..8...,..._Q.*X;...2..v.(.-K.l.C...QF..A&*./.....+.Z?...jd.'.....E....}?..V.1..z.v.....*..X..jS.<...lNq.R...6.....l.....X...../mV.?.vO/g..~dN.F.....g`..I.).9Q.&..c2...:..b
1481	..[V".
443	.....C.g..Y..1 b-.mP*T. 8B...v;..sA...f.O..\...L...5.Xqp...F2.aN..D.....a./.....&.i...(....Q...A....QfB.....o.z..=4.%.d..@.....A...:].g.?`.V....g#.%m.....g..pa.....m.M....5....9.=..F.(...0.....x...l"..&...G.o.bA4.eY.....n.e.H..*.(
1481	.....L..5...M.A.b.....uI.D.'..O.....R...H.lk.....v..%.!.....P.....^..iS.....:-.....,T...bG.n.@.....].E.%.5.....Ds+1_.....N.p\.....L...`^.BdjZ.UeQ.}...Lc.%L....u.$e.c..w...,3f.Sh. G..p#....'..#..!....W..(;hv.E../i.....}..!y/R.....rjo}
443	
1481	...EGo

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:13:22.702	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:22.926	TCP	158.69.204.36	443	192.168.1.117	1481	
14:13:22.926	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:23.480	TCP	192.168.1.117	1481	158.69.204.36	443	.....m....b..+<DcZ;.....nf..-s....}....+/.,0.....3.9./.5.....~...%.#.. www.3qnafyqb7azpcdlsgy7su6cl.com.....
14:13:23.705	TCP	158.69.204.36	443	192.168.1.117	1481	...~..
14:13:23.705	TCP	158.69.204.36	443	192.168.1.117	1481	....>...:.....$#R....'..N.q..S.'O.....@..0.....0...0..(.....{-..Z..0...*.H.....0$1"0 ..U....www.z7fkhs57msbtd.
14:13:23.708	TCP	192.168.1.117	1481	158.69.204.36	443	....F...BA.Z,c.U.NZr.~.....,Q.>..(t.H..g.~.'.l.W....KG .1..R..O...R.]".....(..C.g..Ud...Pq..*.).#.{<.D....s.....6.'^
14:13:23.938	TCP	158.69.204.36	443	192.168.1.117	1481	.....(.L..5.....[u+..^...A.c....r.....s..
14:13:23.938	TCP	192.168.1.117	1481	158.69.204.36	443	....!..C.g..V<.....x.....t..C..(%.
14:13:24.164	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5....8On...F\.l..^.....gq.h~.2HiRj..?...\.1'....d3c..&..L..x.w.Z.....A...I;.....I.$T.....=YiK.3#2.Q.....M.JM...u..j..qs.Y:..>
14:13:24.164	TCP	158.69.204.36	443	192.168.1.117	1481	.@}"=...X..>.....m3.D;..H..A.....W`...<U.....l"....
14:13:24.164	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:24.165	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..W.....B"R...o....X....u..e..W.....k....[...*....?.A...j..Dp@...J.+.Ax/g.....S<.....(3.i...E...}..@./..5.u...[.....}..XT.d.....$....
14:13:24.165	TCP	192.168.1.117	1481	158.69.204.36	443	..y..!.....P....K....`~.i....N0...ai.w..+..0.}.s)....T.U.....5.d.gR..7....n..EY+/.4.o.....(-.@....t.l>..
14:13:24.393	TCP	158.69.204.36	443	192.168.1.117	1481	....=.
14:13:24.393	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5....:$.....+....4..p#t.....u..G....o%.$..Mr.p....X.g.?...'....\.iw..c.3..b..t._bB..j..`..J.. u..c..x.D.....w.7'B.....f.....W..]n
14:13:24.403	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..X*.C....s.....s:...6.~...[...../.T..a..h.....nD.g.f..8...,..._Q.*X;...2..v.(.-K.l.C...QF..A&*./.....+.Z?...jd.'.....E....}?..V.
14:13:24.672	TCP	158.69.204.36	443	192.168.1.117	1481	..[V".
14:13:24.688	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..Y..1 b-.mP*T. 8B...v;..sA...f.O..\...L...5.Xqp...F2.aN..D.....a./.....&.i...(....Q...A....QfB.....o.z..=4.%.d.@.....A...:.]
14:13:24.723	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5...M.A.b.....uI.D.'...O.....R...H.lk....v..%.!.....P.....^..iS.....:-.....,T...bG.n.@.....].E.%.5.....Ds+1_.....N.p\.....L..
14:13:24.894	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:24.912	TCP	158.69.204.36	443	192.168.1.117	1481	...EGo

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:13:25.953	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..^C.....7...;..~.\.j..u..mo.....H.....fl:....P..D.*4x....7.....s.:.i....3..#.~..~.>?..M....o..6..-&.R..&..k...$...,..n..q:
14:13:26.178	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..!....\q..8..1.kJI.1....h... ..9W...H..h.....U..G....*2.JR1.I.C.UL.. ....N."I....]..v..H..O....N.if.....9'q...:;...v....l.N..;\.?.)#
14:13:26.183	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g.._.D.v.\..l..B....Txo.....D...)E.]...o.....a..#..v`....b.....,.I.J..=*../.....wy..1.{k.....K1Qnj.[:.....`].....C.v.WDPc.F.a..1/.%x.]
14:13:26.410	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5.."....`..1.....gH...<?e..h..9s...h..8$..iS..<.QqZ/.....j.X.$y.Y3.7.....@..(..n...HA.../V....Y.}.E0..,L.S....C.M_.N.o...O.3...
14:13:26.535	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:26.688	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..`A.....~...4.kE~J.l.q.ej.k."g=..$;n..].1.....0.cuc....l.Z....H.5^0.I.....g.H.'\.[.2..{.....A.....&....Ph.....?.....o..\.h
14:13:26.759	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..#j..Te..?N.5^."..r.. .....'-...H_.%}..,]..H.,.&.o:K6.V..h.....B!_...Z.B.K(....o<.....".]...Pl.....8.a1..41qm....Z..X.8..q.4..4.
14:13:26.952	TCP	158.69.204.36	443	192.168.1.117	1481	...YS.
14:13:26.952	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..a....Q.%P.+2.C.....H..;.r...7.`I..td....VA..e.i.6...;..\}.../Rq..E..D.....5-....=.....$.Q.."WbUE....L...$.th...1<~&.V.„^m..
14:13:27.177	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..$..(0.Y.c.].....d.y.7...../.&C....Fv../.b,;...O..NG.Q.....+...z#v.....1...fi:U.%.C}....n.!....<sa.I,.Ra"..+.,.1..-@.O2<..E!...9
14:13:27.182	TCP	158.69.204.36	443	192.168.1.117	1481	.....C.g..b..e..g...-*...-....GU..$.i+..q..E...l..5hxi..x/.9.p.f....w..:....o]..<P..`bu2p..$.....\)dt"..zO..9Z.Z.{..#.-<..].8....`.....d..C..@
14:13:27.414	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..%?...%l..Q.].6....).....l..{.....Q.....Y.=.Z.z..E .!7..B.ff..^s.....u..,.mVH.<St.K.T..n.4g...k.:.S.b...S..tt...+...Q....l.m
14:13:27.629	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:27.857	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..&.c"...s.?...,...f>.qU.f.}.....I...9....'.(.....S.A.'L.9....b..;.....W...4.0*SM....mY.\E...}.d..4.7KA...6.M..-L..!0.l.q...e.4J)X
14:13:27.863	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..c....mA5.Z.c.m...N^c.r.a...).9....a2...{.3..Tw....=?...."..W....9...w.....Z..E..p=z.....=.@....~6<...../@4e&.l....=.....(.9!..Z.
14:13:28.133	TCP	158.69.204.36	443	192.168.1.117	1481	...B.@
14:13:28.226	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..'k..(Zv..HXs.....6.....1.H$N.h..u.....e....3.rG....t."...I^...#..m....Vu<.....}A...o.....`K....D..?..}.g.E....j.'..nw..Dfn...Q
14:13:28.394	TCP	192.168.1.117	1481	158.69.204.36	443	
14:13:30.394	TCP	192.168.1.117	1471	192.168.1.152	1638	
14:13:31.798	TCP	192.168.1.117	1481	158.69.204.36	443	.....C.g..d...1...f.....o.dVxl.c.$%d..x@...u....%...U..L^j...O..'L..y@,....J..F.k..q..d.....T...=.Z..4~D'G.vOF..Al.M!.Sa.g3.L.JlZV..
14:13:32.023	TCP	158.69.204.36	443	192.168.1.117	1481	...."
14:13:32.180	TCP	158.69.204.36	443	192.168.1.117	1481	.....L..5..(.l.TLU../...?4.*.$.C.L.C]1.A..$T.....`.a....cN..o..l.)R..Pb..O...:1.R..P.7.nw..]..`../.Vh...-....q.q._..+..}....f6.o.!.....we..t.k.

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:00:47.261	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:47.261	TCP	192.168.1.117	1435	131.188.40.189	443	
14:00:47.538	TCP	212.238.208.48	9001	192.168.1.117	1434	
14:00:47.538	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:47.586	TCP	131.188.40.189	443	192.168.1.117	1435	
14:00:47.586	TCP	192.168.1.117	1435	131.188.40.189	443	
14:00:48.473	TCP	192.168.1.117	1434	212.238.208.48	9001	.....u..m8.P.na...dT.....r.YCy...G....+./.,0.....3.9./.5.....w.....www.k5ir7h5q4auvz2xrx.com.....
14:00:48.473	TCP	192.168.1.117	1435	131.188.40.189	443	.....YBB.JW@.P.B..a..qa. ....@.../.T....+./.,0.....3.9./.5.....t.....www.ur46cdviv4tl4r.com.....#.
14:00:48.478	TCP	192.168.1.117	1436	163.172.149.155	443	
14:00:48.750	TCP	212.238.208.48	9001	192.168.1.117	1434	...8..
14:00:48.768	TCP	212.238.208.48	9001	192.168.1.117	1434	....>...:....<.....r@..8.Sr...z.t.....M$<.....0.....0...0..*.....c....Rv.0...*.H.....0&1$0"..U....www.3ak5f2vy5h4
14:00:48.773	TCP	163.172.149.155	443	192.168.1.117	1436	
14:00:48.773	TCP	192.168.1.117	1436	163.172.149.155	443	
14:00:48.778	TCP	192.168.1.117	1434	212.238.208.48	9001	....F...BA.K%tu.m.f....u.X..V.....k....4>..?.f..-..~..3.1lC..Z)..8.o.l.....(..+.M..89o.i.v.^.....o.p..H2.....?A.
14:00:48.779	TCP	192.168.1.117	1436	163.172.149.155	443	.....,...e.r....e^.;..2u....+./.,0.....3.9./.5.....v.....www.kdi7xi4unalkrreq.com.....#..... ....
14:00:48.798	TCP	131.188.40.189	443	192.168.1.117	1435	..i..C
14:00:48.806	TCP	131.188.40.189	443	192.168.1.117	1435	....9...5..U...c._<..(..p...b.....k..aa.$.M..0.....T...P..M..J0..F0.....f0...*.H.....0#1!0...U....www.gwggvdjgefup
14:00:48.809	TCP	192.168.1.117	1435	131.188.40.189	443	....F...BA..3g.1.....k,...R.x.....d.....".".....CN.1hoi....N.....(...?)...Ia..#6X.(..p..H].....{.}F.....
14:00:49.066	TCP	212.238.208.48	9001	192.168.1.117	1434	.....(... ...H...:...,...8S...\...&...y.s...
14:00:49.066	TCP	192.168.1.117	1434	212.238.208.48	9001	....!..+.M..9.WPI.a..@?..u4.o..h..w...
14:00:49.073	TCP	163.172.149.155	443	192.168.1.117	1436	....!.
14:00:49.086	TCP	163.172.149.155	443	192.168.1.117	1436	....>...:..]t.....kT...!.....Sz.....0.....V...R..O..L0..H0.....u....0...*.H.....0$1"0 ..U....www.h3gbrelzoxuewo

通訊...	封　包　內　容
9001	
443	
1434	
9001	
1435	
443	
9001	.....u..m8.P.na...dT.....r.YCy...G....+./.,0.....3.9./.5.....w.....www.k5ir7h5q4auvz2xrx.com.....#..... .....
443	.....YBB.JW@.P.B..a..qa. ....@.../.T....+./.,0.....3.9./.5.....t.....www.ur46cdviv4tl4r.com.....#..... .....
443	
1434	...8..
1434	....>...:....<.....r@..8.Sr...z.t.....M$<.....0.....0...0..*.....c....Rv.0...*.H.....0&1$0"..U....www.3ak5f2vy5h4ekoflx7f.com0...1708030000002..180306000000Z0 1.0...U....www.t7tc7jvhxmxtd.net0..(
1436	
443	
9001	....F...BA.K%tu.m.f....u.X..V.....k....4>..?.f..-..~..3.1lC..Z)..8.o.l.....(..+.M..89o.i.v.^.....o.p..H2.....?A.
443	.....,...e.r....e^.;..2u....+./.,0.....3.9./.5.....v.....www.kdi7xi4unalkrreq.com.....#..... .....
1435	..i..C
1435	....9...5..U...c._<..(..p...b.....k..aa.$.M..0.....T...P..M..J0..F0.....f0...*.H.....0#1!0...U....www.gwggvdjgefupekgc.com0...1707140000002..170906000000Z0#1!0...U....www.2netnlgler3rifv4.net0.."(
443	....F...BA..3g.1.....k,...R.x.....d.....".".....CN.1hoi....N.....(...?)...Ia..#6X.(..p..H].....{.}F.....
1434	.....(... ...H...:...,...8S...\...&...y.s...
9001	....!..+.M..9.WPI.a..@?..u4.o..h..w...
1436	....!.
1436	....>...:..]t.....kT...!.....Sz.....0.....V...R..O..L0..H0.....u....0...*.H.....0$1"0 ..U....www.h3gbrelzoxuewo7av.com0...1705290000002..170925000000Z0%1#0!..U....www.kgidjdnxhdfmvteeb2.n

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:00:50.764	TCP	212.238.208.48	9001	192.168.1.117	1434	....rP.{.....!QU.{..L.....J^....k....u...j*@.....G...^.....Z.....t2..".w.2.....A....}..R.....e.8j]wRb-....J.p!...e.....4...x.S._...g...{.
14:00:50.764	TCP	212.238.208.48	9001	192.168.1.117	1434	.T$..&.[..P...g..dpL.ct.....D+,..^..9B..Y.....!q.X~.nnk.....F...('..?(..jE....~.....L=..T..^....w..#U\ ..<*+;..oP.UT.%.....%6.0.....
14:00:50.764	TCP	192.168.1.117	1434	212.238.208.48	9001	.....+.M..Aa...Yu..t..c9}....._...ImmP.5...,.....n.?etc..Z...Z..=(.R3b...'N...Y...._..K...<..*/.Xe..T...S.m.*_.....$..y.#....FV.d..@S.z.
14:00:50.764	TCP	212.238.208.48	9001	192.168.1.117	1434	.....q..C..P?..P.;M.t.O}..1I<ZoY...K..c7...%U...K.c.d.=..}..P.m.y..$^....z.x.~.8...,....k.f{.}b{..^..<.o@.....M(....e..ma/5Z.u)k..p..]
14:00:50.765	TCP	212.238.208.48	9001	192.168.1.117	1434	,..me.Q.:....V[^6...z"w..*2..c..#e~...Yn.RI.0#..J...:},?..?L.&...Xv)t.=...@;....3(..L.6.....].Gn.S...U....k.!'3.!R.I....@*zs.Z....w..
14:00:50.765	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:51.023	TCP	212.238.208.48	9001	192.168.1.117	1434	.....4..IN...i9.l..8....l.TP y.....d....Q4.H.#b8..R...3..3....!.r.-..o.g..Hh...c..e...>.....}r&6U.....8.`)R;.....5s.....h.l.....Q.....dF.4...*
14:00:51.025	TCP	212.238.208.48	9001	192.168.1.117	1434	.N...`[J1....\.{.....f..x.$.o./#>...>X..N...w.....m...A.....^...6.....=..&;..H...<tS..l...MCk..../.KBr9v..7%..=.....1.h...../.X..2
14:00:51.025	TCP	212.238.208.48	9001	192.168.1.117	1434	..D.8.~.j...x\)..xK..AU..Mx.....C.;6..P..J..@H..._L.}.*.*.^X..<..T~...a..... #v...j..<+1....h.....9...9&.....0.D...../f...u<.?^...T.e
14:00:51.025	TCP	212.238.208.48	9001	192.168.1.117	1434	s.`.....h..icR...Z.....Rt./.....>...].../..7ku..QN.....<.....(#GT>...Pg..#.;l....$..D..3...U.Ym.p..N..R....~.IG.y.t..YW.y2..w.....uD
14:00:51.026	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:51.026	TCP	212.238.208.48	9001	192.168.1.117	1434	,....%.....L.x...JW+..q#3c.r....S..Ai..v.`.5...F.....K...p.fz....V>.....8G..g:.C.....!..... ...q...OB....3.....f....U.]G...../.%.v..-.>.....
14:00:51.027	TCP	212.238.208.48	9001	192.168.1.117	1434	3....."G.^{9.....a.^..9.....f&..C.7...:..k..[....7...CvS.....6..:~...ixJ..._.2f...D{..-.'O..k.BG.)r+....".4..Z....C..b....npC.....D.\7.....S>
14:00:51.027	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:51.027	TCP	212.238.208.48	9001	192.168.1.117	1434	.....b..,Lu....EI...rd.=..."..'..#.d?xi.....!.K_.#o..F%.j..8\$9..9nn~..}m.492....Ut..!..W.(...K.x..c^0c.tN.....}..V...&.....&d.kG..`
14:00:51.028	TCP	212.238.208.48	9001	192.168.1.117	1434	.....Y...&..Q.~.@e,....3;...&.F..Vk..#....}a..'X...$.b.....RX..}.Y....z..y....Z.1....g.....?I].hl...m.....a..CT..ePe$....-..+..y`..P.vz
14:00:51.028	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:51.028	TCP	212.238.208.48	9001	192.168.1.117	1434	....b."/.E...Fr...J..u.s...o.P6..7..>@.w/..."..0m..:.H..U..m}.}....a....SJ=.....Zfq...YO9Lo..K..&V~.x..4./..S....?8....@.D.NlZ..2.....
14:00:51.028	TCP	212.238.208.48	9001	192.168.1.117	1434	).L.z.....o.[(.u..4..e3Z. .+.s..f...;..V.S\....X..[.W.q..;.M.....GCN..g..I2.(.@'b.+...B..u.,....I'.<....i..5.....r.....I.J...=.:...=...{.G\
14:00:51.028	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:51.029	TCP	212.238.208.48	9001	192.168.1.117	1434	...e.gr.x..i...1P.....*..5..^4.....)..1e.=}..."V"/.z.R.....c:..t..s....D....3+.....U...)p....)...`.%.z...l.>.n.x..d.x....5.0...s.[R5..K..;).....
14:00:51.029	TCP	212.238.208.48	9001	192.168.1.117	1434	.L...I!..l.f....5...W1gz3.j...A..I....8._K..f.N#.8.....O`-...QL9....^....C?.....V3..J709.....q.....:....&o.i....-n.A.._]W..Q...d...../?}.

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:00:54.123	TCP	212.238.208.48	9001	192.168.1.117	1434	hn....Ujn.Z..Me.@.CAwkO.U.h.-.j=.*\..YFq.....[...l....7..d.....{L..5.*.....(x[.m....F..]......SZ...F.Z.l;.....`..].....
14:00:54.260	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:54.332	TCP	212.238.208.48	9001	192.168.1.117	1434	..GS.....3{....'.HbI.....G.&.,f9.Fo.4.'Ev..\m.y....a').2.....y.."XQ"6....~5.....L.O=..&...A.....FKl2.....@%f.9Y.....i."....3:..El..B..
14:00:54.479	TCP	192.168.1.117	1434	212.238.208.48	9001	
14:00:55.202	TCP	192.168.1.117	1437	158.69.204.36	443	
14:00:55.202	TCP	192.168.1.117	1438	91.134.217.18	443	
14:00:55.226	TCP	192.168.1.117	1439	5.196.58.96	9001	
14:00:55.226	TCP	192.168.1.117	1440	193.200.241.195	9001	
14:00:55.432	TCP	158.69.204.36	443	192.168.1.117	1437	
14:00:55.432	TCP	192.168.1.117	1437	158.69.204.36	443	
14:00:55.432	TCP	192.168.1.117	1437	158.69.204.36	443	.....{.E.`...m.\.f....s....X...z.....+./.,.0.....3.9./.5.....&.$..!www.y4nfnkn2zas2vx4w6vk7qkp3j.com.....
14:00:55.566	TCP	91.134.217.18	443	192.168.1.117	1438	
14:00:55.566	TCP	192.168.1.117	1438	91.134.217.18	443	
14:00:55.566	TCP	193.200.241.195	9001	192.168.1.117	1440	
14:00:55.566	TCP	192.168.1.117	1440	193.200.241.195	9001	
14:00:55.573	TCP	192.168.1.117	1438	91.134.217.18	443	.....*....%.\.\HS#Y{...b'j.X...(....+./.,.0.....3.9./.5.....t.....www.pjqm6jspxpeoay.com.....#.....
14:00:55.573	TCP	192.168.1.117	1440	193.200.241.195	9001	.....y.....ft.r.GNUk.....LD.....+./.,.0.....3.9./.5.....n.....www.yoer2ype.com.....#..... .....
14:00:55.574	TCP	5.196.58.96	9001	192.168.1.117	1439	
14:00:55.574	TCP	192.168.1.117	1439	5.196.58.96	9001	
14:00:55.574	TCP	192.168.1.117	1439	5.196.58.96	9001	.....-.%....`u.%.f9.[..6.s.....Z.....+./.,.0.....3.9./.5.....w.....www.4jwt4y5xns76es4gk.com.....#
14:00:55.656	TCP	158.69.204.36	443	192.168.1.117	1437	...-$.
14:00:55.657	TCP	158.69.204.36	443	192.168.1.117	1437	....>....:...k.....r.y...,..t.!.^+V].....0.....0...0.. .....T...Q...0...*.H.....0.1.0...U....www.3g63aamxab.com0..

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:01:00.696	TCP	192.168.1.117	1439	5.196.58.96	9001	
14:01:00.696	TCP	5.196.58.96	9001	192.168.1.117	1439	..#.uX.x.....*.....y..@P:.tl..v.f.&...f.zp$..i)..ca.v.....0.R.T.....x.!..@V.l.o.5....U%.7.TZC.m6p`\B&[.,DZ.amE6.}.]Yo&....:.q!..8p
14:01:00.696	TCP	5.196.58.96	9001	192.168.1.117	1439	9.8....HC.4...Cv...?...zb.....B.Qr...W...*.....7....D.B...>f...M...(.S.y.w.lT .z.,T6.....E.1..d.HN.=._.#.....F.7E..H7+..D.Z'.I
14:01:00.696	TCP	192.168.1.117	1439	5.196.58.96	9001	
14:01:00.696	TCP	5.196.58.96	9001	192.168.1.117	1439	.....iO.(..F;..`.....`.....vm9..E.J...+.....#.\F....(.. ....}...)kv.*4H....."..5...4l..... d.....K.. %el.....x;.N.U..+.%.Z..\.M.#..[..u."$
14:01:00.718	TCP	91.134.217.18	443	192.168.1.117	1438	.a.$....9.....'42....y....B...q...~...I.=.....)...*.....z....."il.<l...(s.....G.Jx.<...E,.yl.....g).@`!... j.....{Nq.yi....G.../...{.`kQ6dN.T>..n
14:01:00.720	TCP	91.134.217.18	443	192.168.1.117	1438	._..p...f.a.!..+=. Z.....,..~0...'..x.S.Pa.U..^.7./y.H$..I.7..Tu0a.%>8z4.....jS...U..?8..y.M....$.X...4.k.k3n8..._z.w.lO.V...l.~.d..`..
14:01:00.720	TCP	192.168.1.117	1438	91.134.217.18	443	
14:01:00.720	TCP	91.134.217.18	443	192.168.1.117	1438	y...!.%..n..I.X...Z..N.S...R....$n....O.{..B.8<...=1.j.V...l~Z%.....f.....n.....Y.=.H.i.zi.*..x.F91.+YVxt..fE...+sA.{t....(.#.a].I
14:01:00.720	TCP	91.134.217.18	443	192.168.1.117	1438	.s1.~...?.?n0.....=...K.x.....m.7..[jv.F.bW. .#@]..."....p.....;.;.l..L..LP..D...r.<..Xv.....v.....Y7h.k.....djF;..=.!.b..@....\&..+g=.B.'
14:01:00.720	TCP	192.168.1.117	1438	91.134.217.18	443	
14:01:00.721	TCP	91.134.217.18	443	192.168.1.117	1438	...AZ?...I.r..o:.oe.....*.....#V..o`.z=..gP.,.{,.....w...S..W.nr.....c.".T.Z,..jnH....T...j..~.x..s.Zg..2%(.. .$..`,...\m"X....H.<o..\.
14:01:00.721	TCP	91.134.217.18	443	192.168.1.117	1438	...._D...N2[mS...p._y..]....BX.qvGN1...p...-=.W...nl.).....L....8...+....w[.....(l..l.....3.....z.....N..*...../m....(.T....2qvE..b`.....
14:01:00.721	TCP	192.168.1.117	1438	91.134.217.18	443	
14:01:00.780	TCP	193.200.241.195	9001	192.168.1.117	1440	p.....NfVJ.2IN..m....N....A!.E... ..0..sD_...@..\i.....=..n@<.o.Y..ow.!.E..JA'....=Xq.$.}.q.J...U.3.....k..l>..eH.....0.....X...K...
14:01:00.780	TCP	192.168.1.117	1440	193.200.241.195	9001	.....Z..."...v.zol....2..D.....5...u....!.$..l.v...5...]kjL.].H..j.da....mY.....Nt.J..#.....Z...../3l.`..:{...q.<...<.....+.fw07<...M[....?...
14:01:00.805	TCP	91.134.217.18	443	192.168.1.117	1438	..$q.L
14:01:00.805	TCP	91.134.217.18	443	192.168.1.117	1438	..+..
14:01:00.807	TCP	91.134.217.18	443	192.168.1.117	1438	....n.
14:01:00.807	TCP	91.134.217.18	443	192.168.1.117	1438	\.B>..+...[....I&...g9M.. I.x.1.....k.aXU....[.Y.$'\b..Vn..}O..1.K.U`p...]p.}.z..o.....Nlky.....B2.'`..<..x....y..9....z5E...z...E..py.
14:01:00.808	TCP	91.134.217.18	443	192.168.1.117	1438	(.!Kk.g..."...o.@9.DI....q.3.P.?.N....E8....!...I/N"v.9O.{E..1....y.a...R..."l..l.X...s..... @Tp....B.I....>4..[.5.l.u.....p.7..jn...j=.H.
14:01:00.808	TCP	192.168.1.117	1438	91.134.217.18	443	

標準HTTPS通訊初始化封包範例

	Protocol	SRC IP addr.	Port	DST IP address	Port	Payload (Content of packet)
13:59:42.687	UDP	172.16.1.100	1026	168.95.1.1	53	.....cib.ibanking-services.com.....
13:59:43.093	UDP	168.95.1.1	53	172.16.1.100	1026	.....cib.ibanking-services.com.....@.....ens2.metavante."".....ens1.L.d.....G.....
13:59:43.093	TCP	172.16.1.100	1557	64.132.202.10	443	
13:59:43.343	TCP	64.132.202.10	443	172.16.1.100	1557	..
13:59:43.453	TCP	172.16.1.100	1557	64.132.202.10	443	.L....3.....@..d..b.....c\Y...[..t.t.C...
13:59:43.656	TCP	64.132.202.10	443	172.16.1.100	1557	I'.r.....-.....24c.....t..u..b...0M)[...G.....s0.....
13:59:43.656	TCP	64.132.202.10	443	172.16.1.100	1557	....J...F..D..QT...HX.~%%&sq1.(#.o.....*we M..k.>.r.....k.@[..0..o..T.....0...0..I.....SS.G.m6...O.C...
13:59:43.656	TCP	172.16.1.100	1557	64.132.202.10	443	.....I$|...x.u.....yv.....[..P.Y.k5.....6.....{H...s8...s.y.e...yI]Z.....+.eMI//]#.de#{..h.....z.=HG.T.;.T.....<...-
13:59:43.921	TCP	64.132.202.10	443	172.16.1.100	1557	.....8...t.J.....:*;..m.....z..}....@X...'.r..O.8b...''.sY...
13:59:44.015	TCP	172.16.1.100	1557	64.132.202.10	443	....<r.....D...>..V .....r;...~...n8jn....H2.....D..S3..i1t.v.M...''...B.gY.px3y..1.;..._....,...(..}..<.>._*..c.}.....2.^H....$c
13:59:44.218	TCP	64.132.202.10	443	172.16.1.100	1557	.....
13:59:44.281	TCP	64.132.202.10	443	172.16.1.100	1557	....27.S.....iF:.c.|..R..,A#N).h*2hg8.....`L.....9....).....L-...''.1...Q.)Y..M.?...T....7:;%....1.....j.M.|....d...r.....TC..I.
13:59:44.281	TCP	64.132.202.10	443	172.16.1.100	1557	.....%a...(.....r+D...c~....3..bn.{....q...6i'60>.G.....nmGF...p+..C*.wv... |k1d...M''-..<=JT....u.....#.|v...?F.....Y..I
13:59:44.281	TCP	64.132.202.10	443	172.16.1.100	1557	.[x.b.ht.T..Nn.... .....]...s..?.H....|L...p.....f.@.;.r.4.I''.....'z.5....'..GI..2.....7.Z.>.....a..lS..^...w]....d..e...J.&8dq.}t
13:59:44.281	TCP	64.132.202.10	443	172.16.1.100	1557	....,r.*y.Zc.H.....F+.1y..;....'..Kz....]..9w.....6.f.,8gU.B$.+.I..NX.u0.I.Mh.QLSRc..-O~.*\s~...)$s....p64>.u.S.jo...
13:59:44.281	TCP	64.132.202.10	443	172.16.1.100	1557	..8.h.Q8p`.'....z5.....)...d`....E...4k..n.j.....V`i8..6..?..q.~|Q./.....$vr`.....P..x..0.{.....4z|.(.D.....$.~.9VN....TH

標準HTTPS通訊初始化封包範例

	Protocol	SRC IP addr.	Port	DST IP address	Port	Payload (Content of packet)
14:30:39.250	UDP	172.16.1.100	1026	168.95.1.1	53	.....www.microsoft.com.....
14:30:39.296	UDP	168.95.1.1	53	172.16.1.100	1026	.....www.microsoft.com.....toggle.www.ms.akadns.net../.....g.6.U.....(...lb1.6.e.....<.e....
14:30:39.296	TCP	172.16.1.100	1583	207.46.199.60	443	
14:30:39.500	TCP	207.46.199.60	443	172.16.1.100	1583	
14:30:39.500	TCP	172.16.1.100	1583	207.46.199.60	443	.L....3.....@..d..b.....cS.Ov0...~.#.q...
14:30:39.656	TCP	207.46.199.60	443	172.16.1.100	1583	....i...F..D....&...^.-..^+xbZpjlmc..... c.....l..)..Hy.A....%.P]...C.....0...0..~.....H.0...*.H.....0..1.0....
14:30:39.656	TCP	207.46.199.60	443	172.16.1.100	1583	.....-_b.@..O....w..d..id.0a^...u)0.,....8....V....wX.....#..W...Z0..V0..>.....a..x.....0...*.H.....0'1%0#..U....Micros
14:30:39.859	TCP	207.46.199.60	443	172.16.1.100	1583	..*.H.....0u1.0...U....US1.0...U....GTE Corporation1'0%..U....GTE CyberTrust Solutions, Inc.1#0!..U....GTE C
14:30:39.859	TCP	172.16.1.100	1583	207.46.199.60	443	.....k...g.....&Ln.....z.Vv.u.b9..r...%N.p....Hd.|...m`e.6c.|Luo.....@f\.d.....L.....d.....>[$.X....J..W.....(...
14:30:40.062	TCP	207.46.199.60	443	172.16.1.100	1583	.....8#|..#Ss.....is....W&\..<+..f.t..M.....k,..z.J.:tp..
14:30:40.062	TCP	172.16.1.100	1583	207.46.199.60	443	.....0.....2....=.....4.....$.(....|g..Y;.g.K|.o.T.s.!P_0..t..Y...\7.....7.{:q.a...&.4.E%..x..).....I..\..B.....%..S...3.
14:30:40.328	TCP	207.46.199.60	443	172.16.1.100	1583	.....
14:30:40.421	TCP	207.46.199.60	443	172.16.1.100	1583	...@.....`:s|....K..>D.Q...0.....|...x...;h-..a.^.pCZ.....\.E./.r43..U...}.....Q..b.....Z....3ks....._.....;..A.<.`..:....
14:30:40.421	TCP	207.46.199.60	443	172.16.1.100	1583	j....~...u.$....r.U3y...#.....`Fp...4.....y..v....Rc.XT...Qb...B.....)..*...@..M...YN.Wtw....m3...-/..JV-....%f4./....I^*c
14:30:40.437	TCP	207.46.199.60	443	172.16.1.100	1583	.x..w|KZ.....J.#..B...=..z..y.Gn/..7C.....ll...^{....f|.|..Y.f...2..1=.....;.F.`|..D.}...._P..K^sn.X....r.PtV..y..kE.K.m.....|.
14:30:40.437	TCP	207.46.199.60	443	172.16.1.100	1583	U@.....hR...k.$g:!.y.1V.....$.g....4....r.\....B...&xX..Q.~fR..RE...r.....|.!u.(.....Y..Y.<.J..''....wK.@ ..DK*Y.....z..
14:30:40.437	TCP	207.46.199.60	443	172.16.1.100	1583	...`vLU[.....\.i...W].C..Q.0.@./r.D..N.Wc.k.eGz...S.....3.....Dm..Fm.|..c...9.8.].b!.....K*..4..$...S...C)..P.?r..;B.Lv.

其他TOR瀏覽網站的通訊封包範例

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
19:11:50.961	TCP	158.69.204.36	443	192.168.1.117	4840	....8.
19:11:50.961	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...1....v.....?o<4E)....}....o%....f..`h....X...d.K.(.....~<..eTMpK.V.f..*kj.9h...H..f....g..!....2k?.;.....6.....h..D9.....^.
19:11:51.072	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.z8.d..^.}N...X...Wr..`:.....D.>.$.....^Iu.f...b1.....o(H.y..F..x....7(..q.....Y.i...[.!l4o.!..$...?...:..y..1...oo.9...*....hF..J.
19:11:51.168	TCP	158.69.204.36	443	192.168.1.117	4840	.....
19:11:51.168	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9....A..<..S..h..o.-[l...X.yz.(b..Ct...<.b.....[3t..l....!.YWpF.o.(... .r.v..f..f.....i.....x.s..xM....F..{...O..k.....Mx.[p.]N...R.(
19:11:51.344	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9.....,s.*AWsJ..FUy.jf.s'....#.P...%.....IQ.F?.5C.+...e..G.8.....;Vw-...QY.!+..p.N<.....\..w..c...&=..z'.....{..ue?....JF.."3..
19:11:51.344	TCP	192.168.1.117	4840	158.69.204.36	443	...e...0..F."...>=..M...^i...,.....,..$zx..m.W..z...&(...>.....rI..;xL.Q..S-$.S..T.(..~E.....t.r...E..4...
19:11:51.376	TCP	158.69.204.36	443	192.168.1.117	4840	..Q=1.
19:11:51.483	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.z9o:^\.....c7Sg.UZ.....w..c3vAF....^.a....O'J.a.e.a.....Q.C.v..hSy.%...t...B..[....C#..t=&..P..}..F.[..3C.]..".uW)x.....I
19:11:51.535	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.z:.+.....^b....oEG..Ic..v.....R....\.~...?6.....Ba.b,.H.!.g+...V...<..x.yF.+.1..-....%..W...2....C.8.g..l.s.t.d;.....*.].R.r.
19:11:51.535	TCP	192.168.1.117	4840	158.69.204.36	443	
19:11:51.543	TCP	158.69.204.36	443	192.168.1.117	4840	..lNrc.....q W..C.@.}by.b...N..T...^....hmC:)..... .7^..d.k..3zM.z.k.Q,.*.....^B.....I$...;.....G..O....w....W.(Q.....t..j.....:.....>.....
19:11:51.543	TCP	158.69.204.36	443	192.168.1.117	4840	.....E..2y.....PkuBK.i.d.q.s,.T.!i.o.`.....]..).Ll....>{...g.....Bvio..X..k.TWX...dN31..1...J;o.0..2...k.Z..k.jSw..GS....J_..v.:G.Y
19:11:51.543	TCP	192.168.1.117	4840	158.69.204.36	443	
19:11:51.563	TCP	158.69.204.36	443	192.168.1.117	4840	.....
19:11:51.563	TCP	158.69.204.36	443	192.168.1.117	4840	..r}f.
19:11:51.579	TCP	158.69.204.36	443	192.168.1.117	4840	K..N*>..\...c..L..zT3.b.M".T7..S.i.l..`....$.....n6{...w.Rf./...[.z....`.aL...="._..I.....R.....l.U..@U.1.EO..P0.z.....5.....Y....t..'.r..l..
19:11:51.579	TCP	158.69.204.36	443	192.168.1.117	4840	...).h....."s.B..q.&W..H.....L.@0..pzs.?R.0..;.....R0.<.`...fg..:..r..W..2d.....m...q.....1..R.....K:....$f.]...?_".Mw....9.....{w
19:11:51.579	TCP	192.168.1.117	4840	158.69.204.36	443	
19:11:51.584	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9....{...>..D..`....w.3.....y.....KC.G..iR...>FR.V?=..8L.....G<..B...M~...../G.....w.....8..e..c.w.....$t7..)6].]~X.8;.g.,Z..).j
19:11:51.658	TCP	158.69.204.36	443	192.168.1.117	4840	...z..._nn.....T..r.....7a<.....u.....AD)....nn\.I".'1Q..<..P.....4.,E..L..cJ.....P.....GXY.g0@u..ZDx...s.....o...,=.D[RZ.+.6.{.....9
19:11:51.740	TCP	158.69.204.36	443	192.168.1.117	4840	..tu.....6.i.....}r7.'e..?...{.A.7.p:.D.....j.1....[D.....T.....U...>...[.fl.p.....7 W.....Jm..7...Y%.F:G..Z/.m..;...+....7:.3{K4.U..Qi...<...

其他TOR瀏覽網站的通訊封包範例

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
19:15:45.832	TCP	158.69.204.36	443	192.168.1.117	4840	...xu.
19:15:45.832	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9..Z.....<R....I.2b...7w.U:....B...i.E.,.....@).{J.~.... .K-2....f....].h&...../?z.....3./....{...B..I=2...x..l. .c.....aLMa.YA
19:15:46.038	TCP	158.69.204.36	443	192.168.1.117	4840	...w./
19:15:46.417	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.....K..#O6.....q.....O.;;-"+I.6.)...V,+....?3..a.^.P....S.D{....q.....-.MA>wQQ ..*.....a5...1..*u...Gb.O...'1...Y.;M@..,=
19:15:46.432	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9..[.....~;:.F.[.d..U....e.....{>B...Y..tm.uo.a.....Ezr.;....R....q....g!..\\W...0...3.....V^.1.kC....l..W.8.QN....c.o>tSw..<'
19:15:46.643	TCP	158.69.204.36	443	192.168.1.117	4840	...X.p
19:15:47.063	TCP	158.69.204.36	443	192.168.1.117	4840	.... U;9u.{....#'.#...6.i~I.!..~E.G.p..b.....,.v..Z.TZ.b..Ao....>.....u.$4.....1...."....E`X%...y..~...#.p.....r....J..).XM..
19:15:47.063	TCP	158.69.204.36	443	192.168.1.117	4840	e...2.s.....jHyo..j..f./...!Gp{.H..%..$y.x..`75q.<.&.j.....).y...j ..K.hR5.ID.1.gaF....l..%....:.....Ht[.^Zc\.....kM..U..#0O.....r
19:15:47.063	TCP	192.168.1.117	4840	158.69.204.36	443	
19:15:56.461	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.<....n.(.*...A..H.Z.%.zp.n.....B.S.....c.Z.M...P...'...}!.Y.P..>.F.F.g....x..w},..av.n.....V.bO.....9...jH.z..M..._C..-'
19:15:56.575	TCP	192.168.1.117	4840	158.69.204.36	443	
19:15:57.257	TCP	192.168.1.117	4272	216.52.233.191	12975	...P...K....Br/j..Q.....hY.y....r....j.....TON[>...Cf.R:...M.L`...5....g...yp
19:15:57.478	TCP	216.52.233.191	12975	192.168.1.117	4272	..j,4.
19:16:03.392	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.l]N.'.z..d.....j`;\..fy.....m^x>..1_.....0....0..'.....>.h.S...../;^64I.....:....Dbh....I...O.O=.I[U..2..I.!@..K...ZeK].
19:16:03.515	TCP	192.168.1.117	4840	158.69.204.36	443	
19:16:04.351	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.<V+..*.DV..Iv.....jG..:...d'.t....."V\4.....e....F..[.:....@.B;.g...Zv._..2..^_....9...6....'..S.n.....'.....eR51...r.e.4.J)....
19:16:04.521	TCP	192.168.1.117	4840	158.69.204.36	443	
19:16:07.657	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9..\.....s.-.9..l..R.i.....c..C_...,..P..k>P.....>B..G.o..a..?..D..g....^.l.&Tt8.....St..S`.b./9.i~....@.....db.U...S...u...F.....#.0....I
19:16:07.866	TCP	158.69.204.36	443	192.168.1.117	4840	...rqM
19:16:07.866	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9..];...M.....lV...V...k.1.#..+jsJ....."[%2I.H^..'l.....9....)....<..FH..D^E...?.....T..w.n+(.j.....^..5`_z....dFa.<.....Z.Y;..
19:16:08.082	TCP	158.69.204.36	443	192.168.1.117	4840	.....Q
19:16:08.359	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{...VA....kV.....+....s.e.aM..m.;M.Et..Pm.....$..c..N..hU.....1.44a..c.....1I....u.Y]..^.1.....6`.....'.....#-.R.[..P&...

其他TOR瀏覽網站的通訊封包範例

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
19:16:58.030	TCP	158.69.204.36	443	192.168.1.117	4840	..0.^.
19:16:58.260	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{y.....P+....2Y.cV..^?.....".....t.5Y....l1-.lG.o....O=c⊨<...?7.0,_},...P.1.....3..vf.c.5.;^[4W..X.]....A....M.!.R..]G
19:16:58.265	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...).$.[..%.H....6.B..CG:....pa.....<...(.....].}.;t)...l.....Afgov.Oy.T.....[....ma...7*.Kq.ld..5..x;`(x.....t..wG...KF..?>r..-{
19:16:58.478	TCP	158.69.204.36	443	192.168.1.117	4840	...#.
19:16:58.478	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...2.<..5....Zl.i3F.z..i.mF.F...>gQX_zB.fw.v.....5,...=gT~+D.V..gt{..4.m...~..X.....&z..B.S..8~.....wf,_.v....,./~...>.M
19:16:58.654	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{z.?..VKdu.$D.....P.EI.y"i.+..>..&..c...Bu..l.g....B.Y....l..1.....m.....a~.*.'G..].%.(}*..$".\.<...F.....x.a..mu.}.d....fQv7.
19:16:58.691	TCP	158.69.204.36	443	192.168.1.117	4840	..53$.
19:16:58.813	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{{P./.....b[..!..s..I....)..>..F..=c...d...$R.....D.L...]..........#Bz=J.2o...:.PMx...a.....;..r/.....MaI....)6p.\MN...d..*.mw=
19:16:58.813	TCP	192.168.1.117	4840	158.69.204.36	443	
19:16:58.818	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...a..C.p..b..v.:j....0..PP.nVt.~.q9..3.....qiQ7..Q.....Yl.....Uc..[T..~....!X.n.....Y..6.{..ew..6.r..9gT. ..!.&.r>.-6g'?Yz9..]
19:16:59.020	TCP	158.69.204.36	443	192.168.1.117	4840	F"+.d....):....%p.vt..q.F.G~..#..Ru.....3J.....bG..?E@^M..+.S9.p.u[..Pz..6.../G.kFZ...f....*f..A...d..<(.l.t.....I..+.jw".....C2
19:16:59.024	TCP	158.69.204.36	443	192.168.1.117	4840	..Z..?
19:16:59.024	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...B.....=.....5.....A.....7.\1J.....-.....N.....m.y2....p....H..j8...w.....r43.+V]'.1....x. .m.....wJb.....{.-.....c.^.....]
19:16:59.231	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{...pF.._.(...<..Y.....z%....>.C.....9j:w.....m.AKz.\.G....V/..g...A..Tm.h.VB.....:.z?.....^.iS*...O.r.....!.U.....K.....9.
19:16:59.241	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9.....?..'..(...D....Ek.....q^...9.....BeT..jXe.....f.yK..v$....}.?L.....G_.T.F.....o...2....v(.7.9)...>....k9..H.`#.=..'.D
19:16:59.454	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{....a...].U....h.f...N.q... .....J..b..j8....pm.nH..}..`...l..6....J.N...pQ...D.....JU.~%6q...y/.u.v.K.n....DW...L.....x(
19:16:59.454	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9...y.;.....V..F...?.i.A.....FL....,Q\.h.....n7.WK..X...-T5.R.C./.../...R...L.L.RK6.2..OU....;&..Xy.w\...O.,....H.9.w.....
19:16:59.662	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.7.....l...lgl...^.lc..`].G1S.L.8.!.b....f...R.T.jil.JJ..t.j..xD..2OK.K..C.....C.J.{...f...P.o.gAl.....u.x...l...._g3.....+.....).....1
19:16:59.662	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9....d.....w....q=..M.F.....~R.,.u...a....~..R...,.x..{e!'.h...:H.ze.....w...../..."S.R..U.O.Dx....>..i.....E...<5..u,..J.]."..R.u.?.
19:16:59.877	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.[..A.....".....sl.BL...aO...u..P.B.la.+..i...:.<.....l..y.'....N.;m/.*.z.q.uAU..d...+.4b....B.....,...o....G{.....)P.v..
19:16:59.877	TCP	192.168.1.117	4840	158.69.204.36	443	.....xi.Q9.....c....9VRR...N4.t..V.T..l}f..r)g.4q$.B.VL.",...B..3#%YS.....I.....ly.....f4.5w..B...q.MT..s-.L..}jG.T...4m...X.C..
19:17:00.084	TCP	158.69.204.36	443	192.168.1.117	4840	.....U;9u.{.g.d@..4.1.....b..p.B...F..[.....(T...V...F...'q.p<M..<....X.(_...n.%4.,.@_d..Il.....$.QEc.lDW..;Y.7..*....X.....o.9...~~

其他TOR瀏覽網站的通訊封包範例

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
18:31:32.171	TCP	158.69.204.36	443	192.168.1.117	4757	....~.
18:31:32.266	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..Dl.....p.Y.X...fY...l.j/.b...d..F.r+.b...k.+.f.h..9..@...$...]....=9@!....D$..>=...,.3.,x(.M(...^,K..Wr.2.d..." ...[..C..&"QcW
18:31:32.349	TCP	158.69.204.36	443	192.168.1.117	4757	..h.`
18:31:32.360	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e.L.d<.Q.z.'".h..!&.(..t.....j.N,._.....A....._..Z...<.WQn.h.....K"1.d....T.g.G..2.o....o.....AGsk.;k.A.uV.....x.g.t$.Y
18:31:32.595	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..EZ....i..^I.....2.&F..R....D.S...lom5.1...>.!..HA..<.%...).gL/V..y.~.sR..Q.nT>s.K...H.."S.X.q.....$.P.....#y..r.*.;M.j.4.δ
18:31:32.600	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e..:..(....Z5...;...Bd.e`...,$....l.....T.....SO?..'..-6..W.,u.v..Of..u.(m.....7.n9..F!.b.2.I..!..K.(.....II.X.g.....PR.P....
18:31:32.758	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..F4.p.l....l4X...6[b....U.....#..g....sq.O.A:.O.q*..gLQ..(L..H.0..z"`%..:k..c.2.v.D..-l.....B....rFy.c^...,..-.94.._-w.....j.'
18:31:32.840	TCP	158.69.204.36	443	192.168.1.117	4757	.z..m+..j. .....f.."^.&=H..zr.)2"....($..... ...e.;A...hD.....V0m.....9..Y....K..VHQ..K...L.....{.....6f.q....Y...!.\.0.]g...M/#..O..$
18:31:32.840	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e.y..3S.ll...p.7...0...w.HGj.-...2...)...l(Td.=H...I.....=....<....N.....#y.J..+:A.K...{}..A.y..<.j.5:.@...`...M+.d....Y..GG.^.
18:31:33.075	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..J.....#...j*....$U:.<G...mZ.;>7k.9y~.u*.P+..4...6.V..H...8.=.....P....i..?....8.t.....h&`.9B...Y.....l.....gWX.k{ro.
18:31:33.075	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e.owTI...O.V.....2K....K....c!.MpN..>.a.X..k....'H.....H.....'..F.F..q...h....N.....=&...L,.)...H#Q..R7...L....5@..
18:31:33.301	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..K....P...Q~oq..?p.y....)s3.K...@....cz...j6..~R.P.N.#...o...Q!.*ir.1.V!....j..^.W.dq..R.1,....}....M.....}.G..IM?x.....Se.Wj
18:31:33.306	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e..{..A.~.o.IS.....c..pHu^..)..].8..&....._.....0.....paQ5..X*K...00....&~r..S.1.1..+[jA~[....>..T{..kp..i..,.....<....pV..,?...
18:31:33.566	TCP	158.69.204.36	443	192.168.1.117	4757	..KJ..
18:31:33.566	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e.....k...L...j.sq.`.....`._C.B....7....C..c.....(.Pqlyz.8l.....2>.....u.p..=..).Fy.c\...n...>6....E.....!....O.....#...2.YzR*.eHt.....
18:31:33.745	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..L...B_.....5.GT.!.8....1.K}..U].n.v..KX.j ..S,..}.]F6..i...c5..].g..+.\G..1n...'....m.B,.*.F.DI5.....g.RvqS(..'H...?..'...R....δ
18:31:33.786	TCP	158.69.204.36	443	192.168.1.117	4757	....(.
18:31:33.876	TCP	192.168.1.117	4757	158.69.204.36	443	
18:31:34.114	TCP	158.69.204.36	443	192.168.1.117	4757	.....u..ts..M.{.vze.N*.....4..VS.}....q..y.....a..,:.li.....V...4..8..u.....MR...V~ ....K.o..(...F...*t9`,.a..{..:1.....6.....[..\..<.%.....
18:31:34.124	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e.1..o.l.Y!..v.[.;.uY.4c....n.I8.#.#._.T.?-Lp. .1.:.....y'.....E..l..S..n..,mZY.9=&.....I.1...M....gy+.....~...2~s..Q.]..}R..
18:31:34.364	TCP	192.168.1.117	4757	158.69.204.36	443	.....E.h!..e...KfN_.t....l..kl.....3.i.x....e.....@'.(*9..j....._VD...pAM.p....H.....+..f..3..7..z..4v.....n*.....o..p0.)..3.....R'
18:31:34.364	TCP	192.168.1.117	4757	158.69.204.36	443	&Ul.-...@.k..h:.L..Xh.,z....he.....T...*.....V.r..2..m....45.....S.....(z...<.....i....p.@;..0YL...V^H..)+..o)....L....Q.#c

TOR的原理與封包範例

- TOR 起始通訊階段, 會使用TCP-443與TCP-9001進行通訊點的清單資料交換, 類似P2P檔案分享的通訊方式。
- TOR 雖然使用加密通訊, 但是與標準HTTPS (TCP-443) 的封包不同。
- TOR 的隱密網站, 與網際網路的標準網站不同，特別是無須DNS解譯服務(因為沒有Domain-IP的轉換機制)所以沒有UDP-53的封包。

- 加密勒索惡意程式，運用上述隱密通訊的特性，進行金鑰回傳的動作。

其他匿蹤通訊的發展

RIFFLE
High-speed Onion Routing at the Network Layer

- 麻省理工學院和洛桑聯邦理工學院
- Sphinx 的 TOR 協定 with “Verifiable Shuffle”
- RIFFLE, 透過多個加密主機(非轉送封包而已)，並隨機發送封包(而非依序發送) 根據研究表示，該匿蹤網路可以避免出口流量分析(目前TOR的死穴)而進行偵測，而且網路速度是TOR網路的10倍。

HORNET
High-speed Onion Routing at the Network Layer

- 瑞士蘇黎士聯邦理工學院和倫敦大學學院
- Sphinx 的 TOR 協定
- HORNET, 對於中間傳遞網路資料的節點不必負責加密的部分，而是主機端進行加密(Two-Host-Site)，因此網路資料的傳送速度比較快，根據研究表示，該匿蹤網路速度可達93Gb/s。

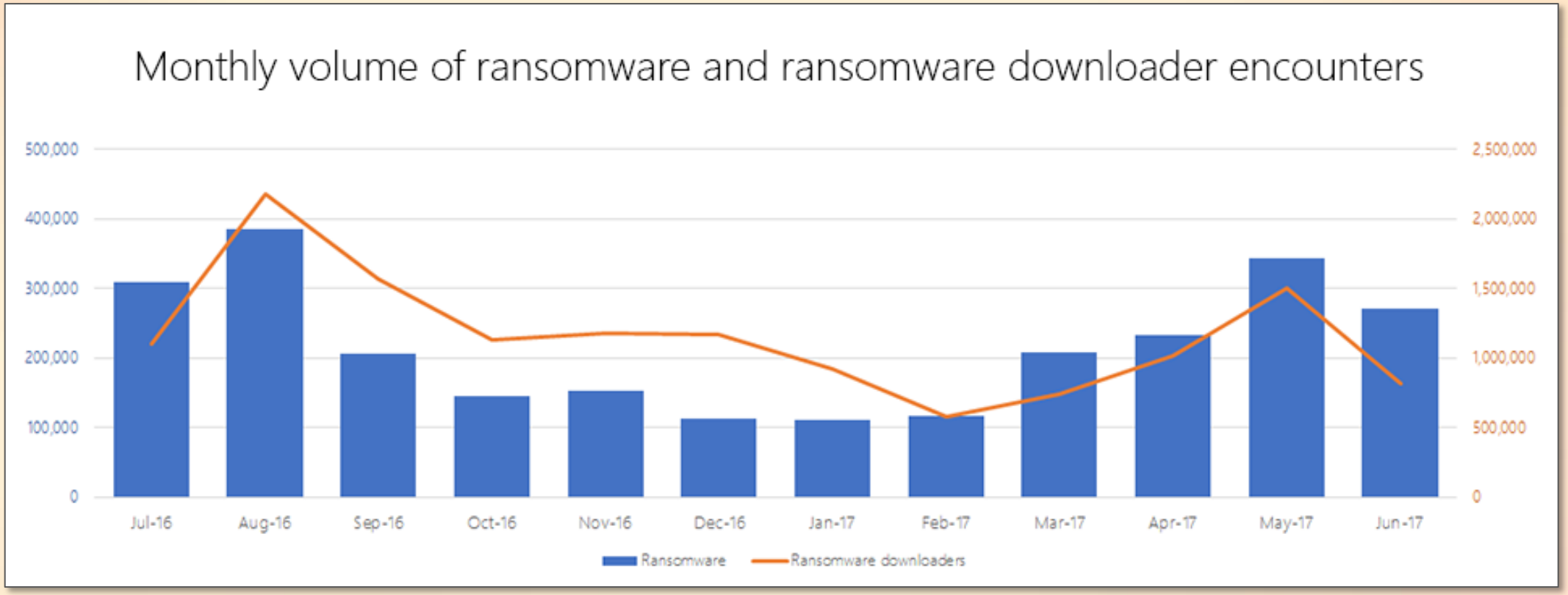
LOOPIX
High-speed Onion Routing at the Network Layer

- 倫敦大學學院(UCL)
- Tor的實現思路為基於電路的onion路由協議;
- Loopix則將基於經典信息的架構同Poisson混合機制進行結合——這意味著每條信息都將被添加隨機時長的延遲。
- Loopix的工作原理與Tor非常類似，但是Loopix供應方伺服器則經由隨機混合節點通過該網絡進行用戶信息發送，同樣類似於Tor所採取的經由延遲進行信息發送的方式。信息在抵達目標用戶的供應方（即出口供應方）時，相關內容會被存儲在信息框內直到對應用戶上線。這一點正是Loopix的獨特之處所在，即允許存儲離線信息。

加密勒索惡意程式簡介

- 最早的加密勒索惡意程式出現於1989年，而使用RSA金鑰方式加密勒索的程式實作則是出現於1996年。但是因為傳播方式與付款機制，在網際網路尚未普及的環境，該種惡意程式並未擴大影響層面。
- 自2005年開始，包括有 Gpcode、Archiveus、Krotten、Cryzip、MayArchive，其中某些加密勒索惡意程式，使用的加密金鑰長度為1024bits，除非使用分散式計算來破解該金鑰，對於一般單部電腦破密來說，是十分困難的工作。
- 近年，受到3種主要技術的改變，**(1)網際網路的應用機台數量遽增**(2)**秘密通訊的技術發展**，與**(3)隱密數位貨幣的實現**。這些變化使得加密勒索病毒的發展，急遽升溫。2013年的下半年開始，新型態的加密勒索病毒，CryptoLocker，迅速從被害人電腦獲取大量金錢(約略2700萬美金)。許多勒索軟體並未加密，但是仍然利用TOR瀏覽器和暗網（Deep Web, 一種TOR隱藏服務）要求比特幣贖金。
- 參考來源: en.wikipedia.org/wiki/Ransomware , 2017

加密勒索惡意程式簡介



參考來源: https://www.microsoft.com/en-us/wdsi/threats/ransomware

加密勒索惡意程式簡介

Top ransomware families	Latest notable ransomware families
• Ransom:AndroidOS/LockScreen	• Ransom:PHP/Ronggolawe.A
• Ransom:Win32/Cerber	• Ransom:Win32/Cryxos
• Ransom:Win32/WannaCrypt	• Ransom:PowerShell/Abpodul.A
• Ransom:Win32/Spora	• Ransom:MacOS_X/Ratatonilly.A
• Ransom:Win32/Enestedel	• Ransom:Win32/Petya.B
• Ransom:Win32/Genasom	• Ransom:Linux/Erebus.A
• Ransom:Win32/Teerac	• Ransom:Win32/Shieldcrypt.A
• Ransom:Win32/Locky	• Ransom:Win32/Jaffrans

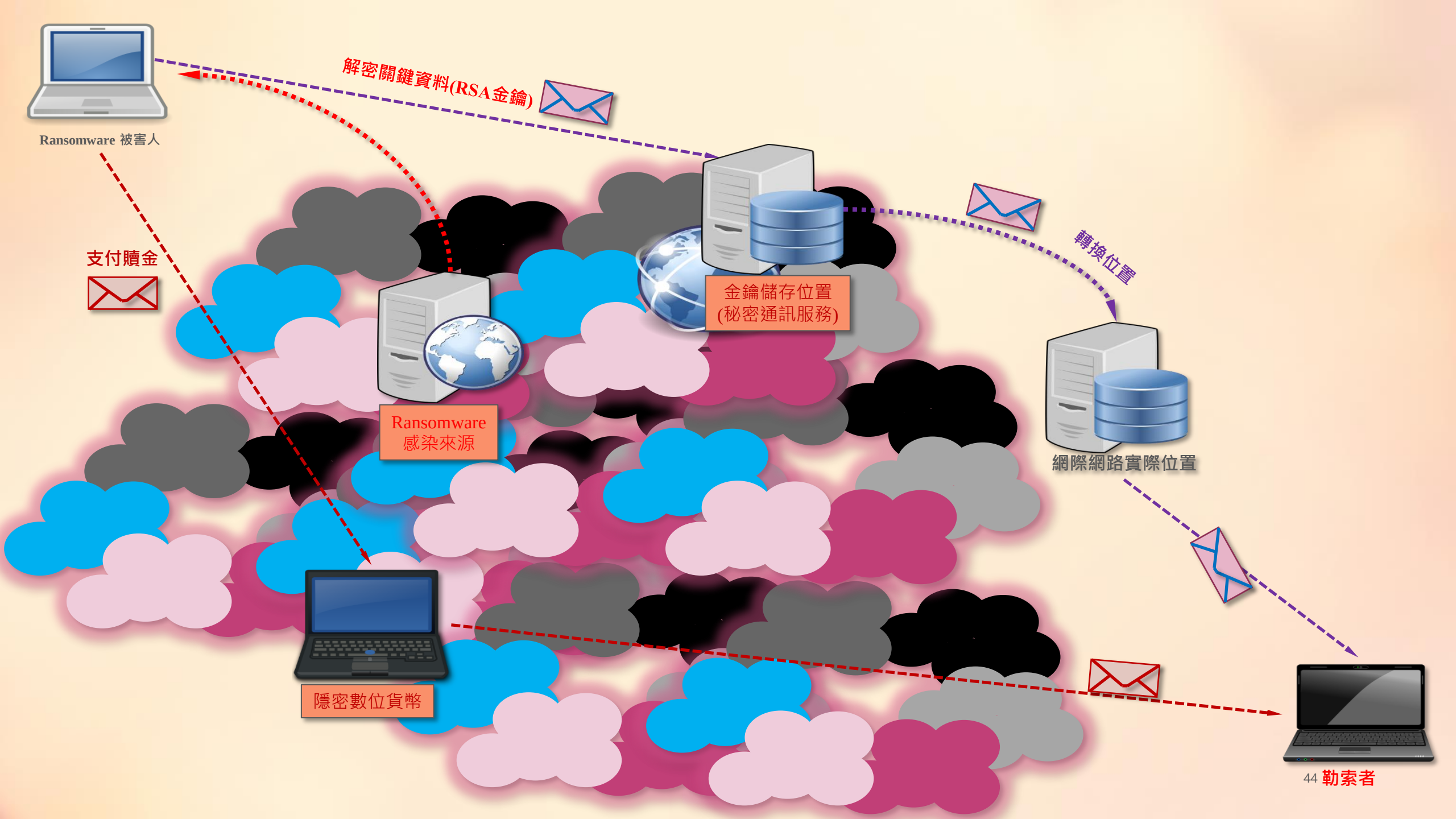
參考來源: https://www.microsoft.com/en-us/wdsi/threats/ransomware

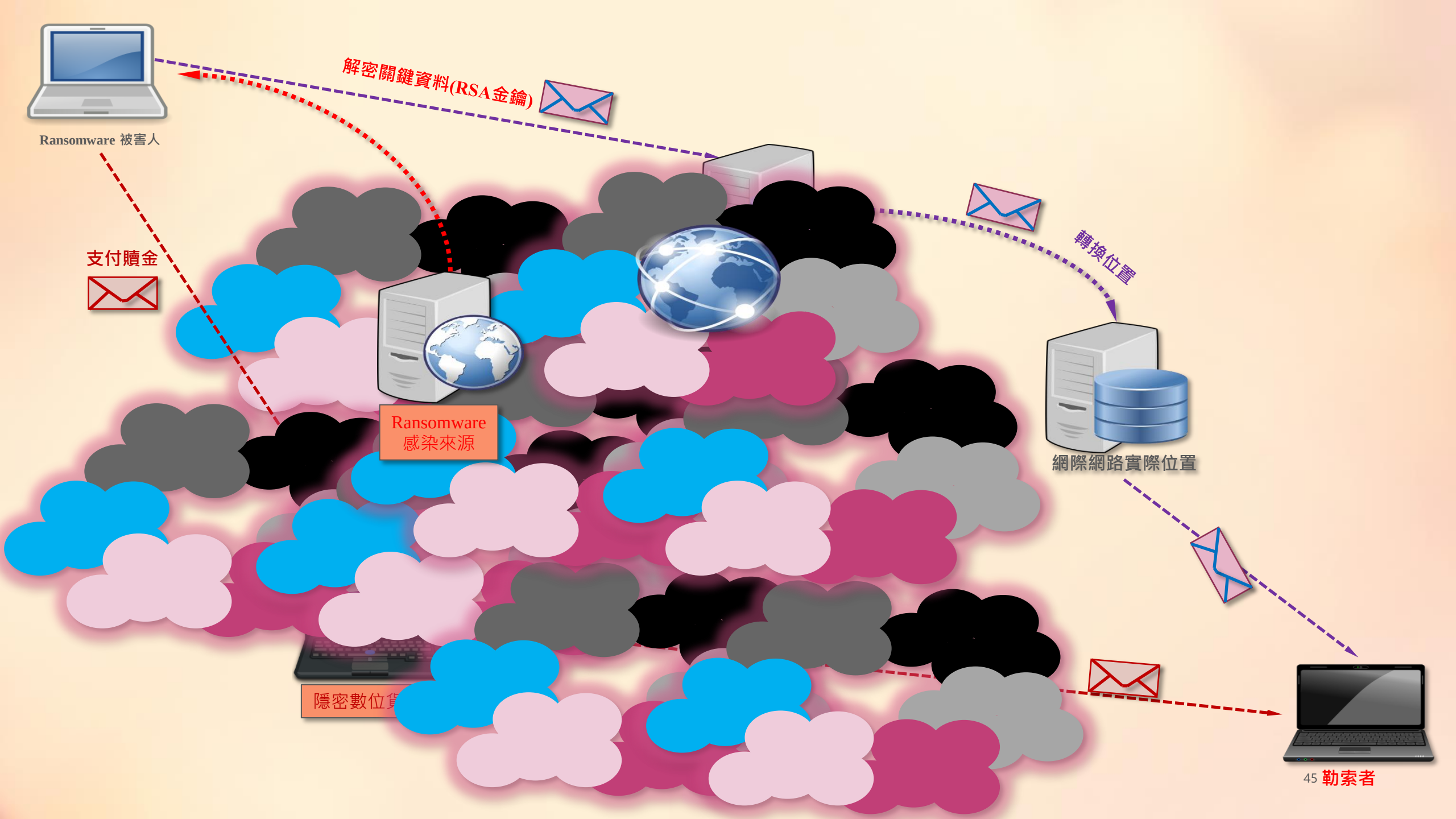
加密勒索惡意程式簡介

網路通訊與Ransomware

- **網際網路的應用**
- **秘密通訊的發展**
- **隱密數位貨幣的實現**

- 以上三種主要技術皆架構於網路通訊技術的日新月異，有別於其他勒索軟體(螢幕遮蔽勒索、色情圖片勒索、硬碟啟動勒索...)，加密勒索軟體更需要網路通訊，以便於將被害人的RSA加密金鑰，傳回到特定位置儲存，並於支付贖金後，將此金鑰資料交予被害人進行解密。


Ransomware 被害人
解密關鍵資料(RSA金鑰)
支付贖金
金鑰儲存位置
(秘密通訊服務)
轉換位置
Ransomware
感染來源
網際網路實際位置
隱密數位貨幣
勒索者


Ransomware 被害人
解密關鍵資料(RSA金鑰)
支付贖金
轉換位置
Ransomware
感染來源
網際網路實際位置
隱密數位貨
45 勒索者

勒索軟體的特性

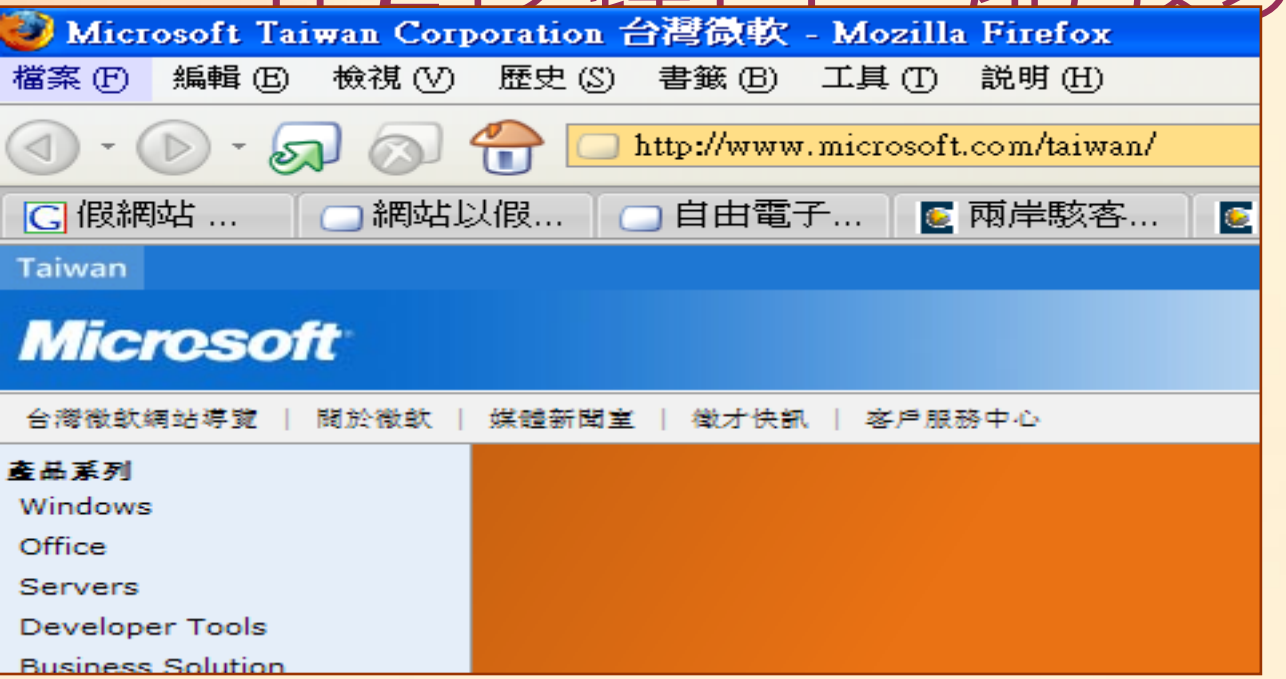
- **傳播感染方式**
  - 電子郵件社交工程
  - 瀏覽網頁，植入惡意軟體
  - 軟體漏洞與系統漏洞
  - USB設備感染
- **勒索方式**
  - 檔案加密
  - 硬碟毀壞
  - 名譽損害
- **交付贖金方式**

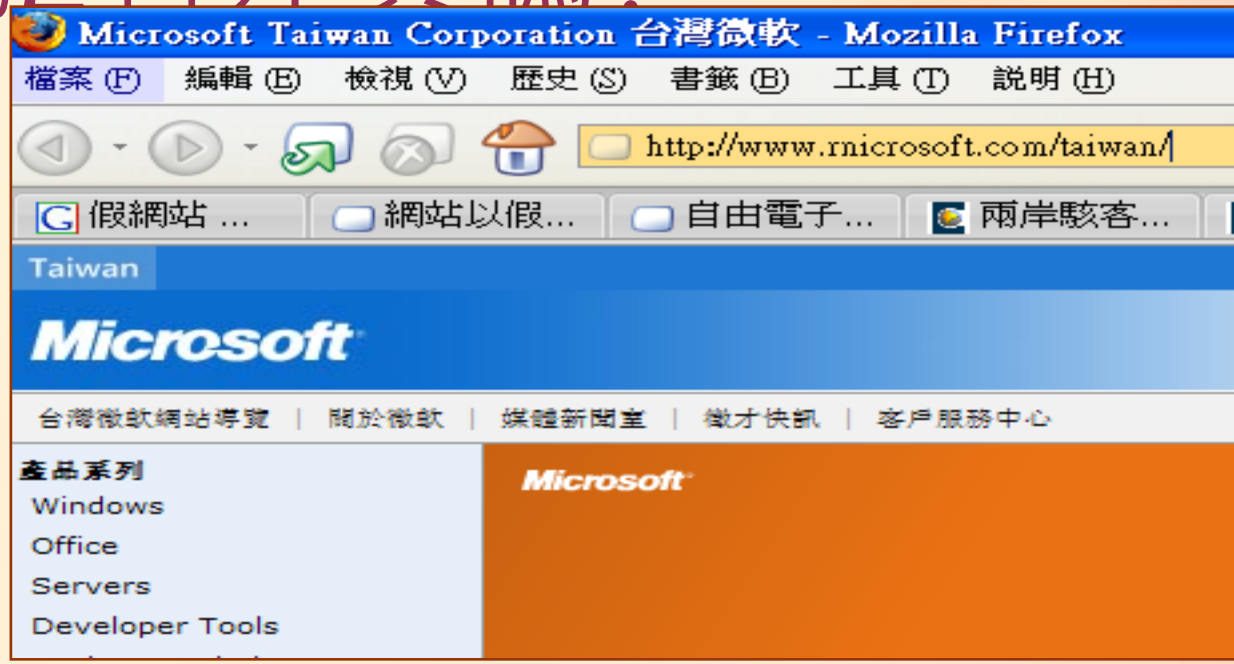
勒索病毒曾經使用的方式

1. iPhone中獎通知
2. 應徵者求職信(偽裝履歷表壓縮檔)
3. 金融機構的電子帳單郵件
4. 假冒 Chrome, Facebook 和 PayPal 電子郵件
5. 假冒 Microsoft, Adobe, Java 的更新通知
6. 瀏覽網頁，要求安裝字型

- **常見被感染電腦的特徵:**
  - 舊版Java 。
  - 舊版Adobe PDF Reader, 或是 舊版Adobe Flash Player 。
  - 沒有 Windows Update更新

在2秒鐘內，能發現2者差異嗎?

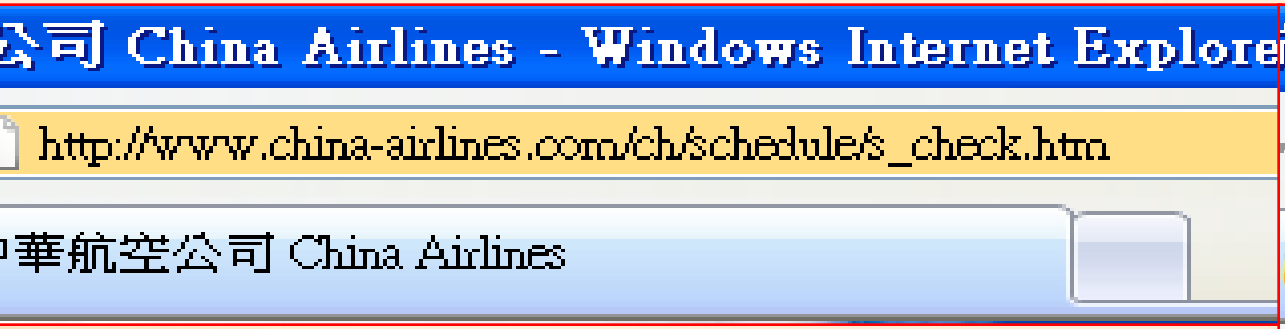


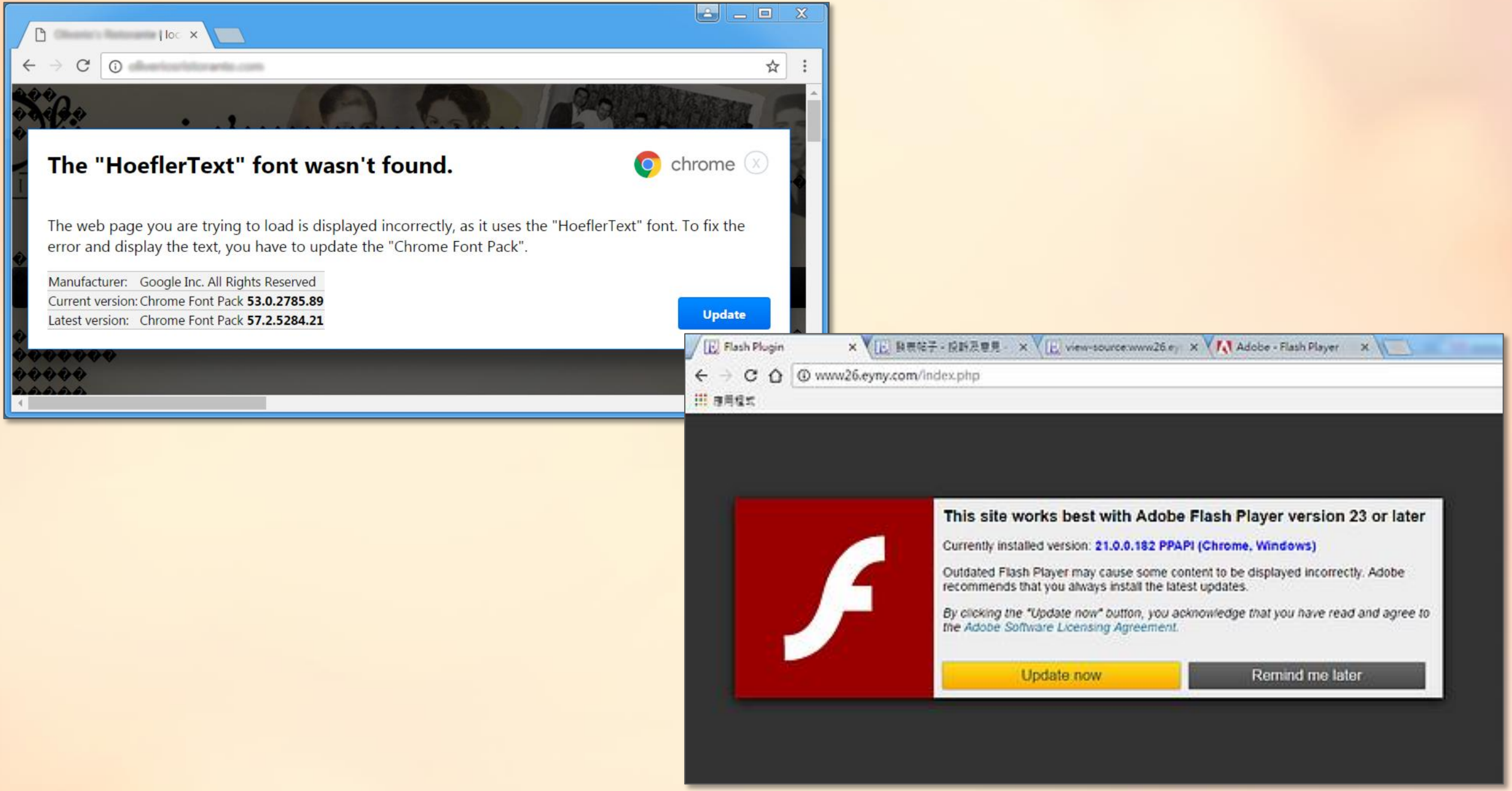


http://www.microsoft.com

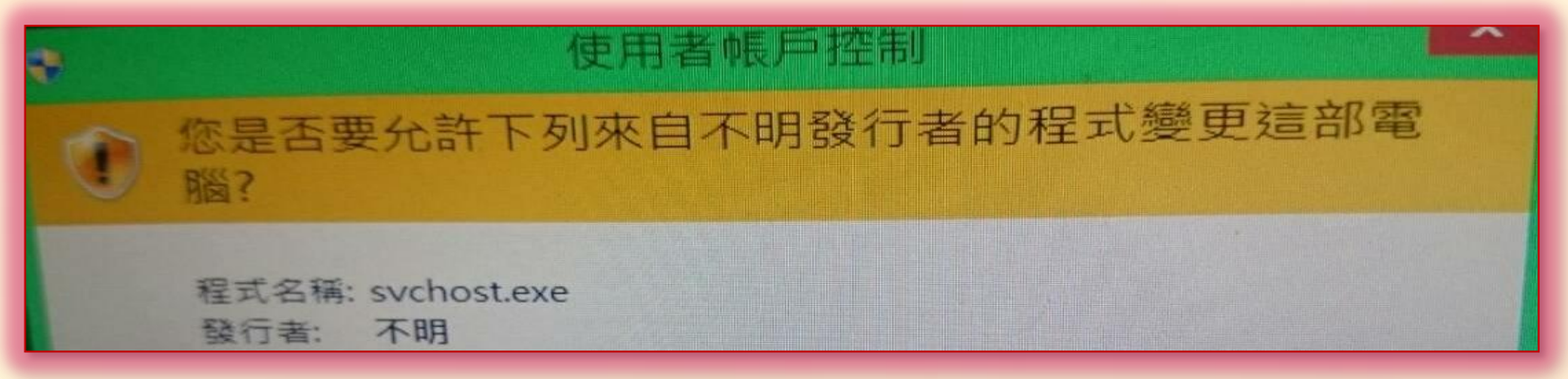
http://www.rnicrosoft.com

在2秒鐘內，能發現2者差異嗎?

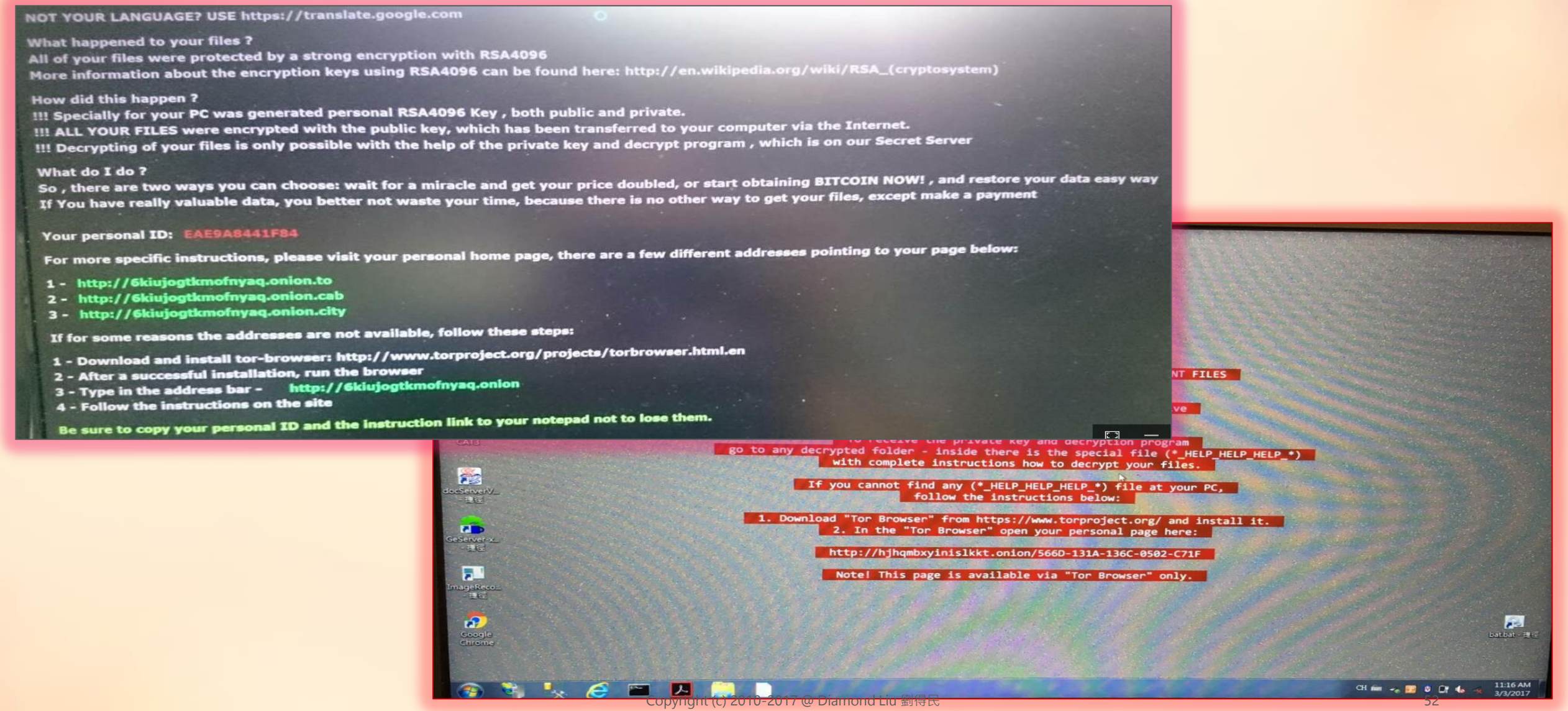




瀏覽網頁，需要特殊權限?



電腦檔案被加密勒索



Ransomware-WannaCry

- WannaCrypto的基本介紹
- WannaCrypto的動態分析
- WannaCrypto的封包範例

WannaCrypto 簡介

- 源頭 : EternalBlue and EternalRomance
- 漏洞： 網路芳鄰 SMB v1, MS08-067, MS17-010 (參考 CVE-2017-0145)
- 與其他勒索病毒的差異:
  - WannaCrypto 自動透過漏洞擴散感染 (其他則是由使用者觸發)
  - WannaCrypto 會在內部網路感染擴散 (其他則不一定)
  - WannaCrypto 使用標準通訊協定 SMBv1

- WannaCrypto 是少數敲鑼打鼓的加密勒索軟體

詳細漏洞技術描述與技術推演,
請參考 https://blogs.technet.microsoft.com/mmpc/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/

可能感染的目標系統

Windows XP 到 Windows 10
(包含 Windows Server)

```
[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] : C:\Users\test\Desktop\shadowbroker-master\windows\dopushe
llcode.bin
[+] Set ShellcodeFile => C:\Users\test\Desktop\shadowbroker-master\windows\... (
plus 17 characters)

[*]  ExploitMethod :: Which exploit method to use

   *0) Default              Use the best exploit method(s) for the target OS
    1) Fish-in-a-barrel     Most reliable exploit method (XP/2k3 only)
    2) Matched-pairs        Next reliable exploit method (XP/Win7/2k8R2 only)
    3) Classic-Romance      Original LargePageGroom exploit method (All OS Versi
ons)

[?] ExploitMethod [0] :

[*]  Credentials :: Type of credentials to use

   *0) Anonymous     Anonymous (NULL session)
    1) Guest         Guest account
    2) Blank         User account with no password set
    3) Password      User name and password
    4) NTLM          User name and NTLM hash

[?] Credentials [0] :

[*]  Protocol :: SMB (default port 445) or NBT (default port 139)

   *0) SMB
    1) NBT
                                                www.hackingtutorials.org
[?] Protocol [0] :

[*]  Target :: Operating System, Service Pack, of target OS

    0) XP_SP0SP1_X86         Windows XP Sp0 and Sp1, 32-bit
    1) XP_SP2SP3_X86         Windows XP Sp2 and Sp3, 32-bit
    2) XP_SP1_X64            Windows XP Sp1, 64-bit
    3) XP_SP2_X64            Windows XP Sp2, 64-bit
    4) SERVER_2003_SP0       Windows Sever 2003 Sp0, 32-bit
    5) SERVER_2003_SP1       Windows Sever 2003 Sp1, 32-bit/64-bit
   *6) SERVER_2003_SP2       Windows Sever 2003 Sp2, 32-bit/64-bit
    7) VISTA_SP0             Windows Vista Sp0, 32-bit/64-bit
    8) VISTA_SP1             Windows Vista Sp1, 32-bit/64-bit
    9) VISTA_SP2             Windows Vista Sp2, 32-bit/64-bit
    10) SERVER_2008_SP0       Windows Server 2008 Sp0, 32-bit/64-bit
    11) SERVER_2008_SP1       Windows Server 2008 Sp1, 32-bit/64-bit
    12) SERVER_2008_SP2       Windows Server 2008 Sp2, 32-bit/64-bit
    13) WIN7_SP0              Windows 7 Sp0, 32-bit/64-bit
    14) WIN7_SP1              Windows 7 Sp1, 32-bit/64-bit
    15) SERVER_2008R2_SP0     Windows Server 2008 R2 Sp0, 32-bit/64-bit
    16) SERVER_2008R2_SP1     Windows Server 2008 R2 Sp1, 32-bit/64-bit

[?] Target [6] : _
```

網路芳鄰 CIFS/SMB Protocol

- CIFS, Common Internet File System
- SMB, Server Message Block
- CIFS/SMB uses TCP-139(NBT), TCP-445(SMB) for communication
- The major actions of SMB Protocol
  - Working Session (Login/Logout)
  - Server Message
  - Resource Sharing
  - Printing Support
- CIFS/SMB uses UDP-135, UDP-136, UDP-137, UDP-138 also.

網路芳鄰 SMB/CIFS 封包的快速分析

- 『.....SMBr.....』 request login into server with authentication
- 『..... SMBs.....』 reply login message with version and license
- 『..... SMBsm.....』 server responses login fail
- 『.....X ...SMBs....』 server responses login successful
- 『..... '.SMBt.....』 server responses terminate current connection
- 『..... ...SMBu.....』 create SMB first session (Null session)
- 『..... SMB%.....』 send the shared resource name of server

1. SMB Protocol is a Internal Protocol which only can be found in LAN or Intranet.
2. In CIFS/SMB analysis, all the IP address from Internet (WAN) is abnormal.
3. It might cause once Login error SMB message when Windows uses/remembers disk shared resource.
4. The SMB packets after ICMP packets, it is abnormal status.

網路芳鄰 CIFS/SMB 通訊3原則

- 正常的Windows系統, SMB/CIFS, 不論任何情況, 均不會連接網際網路(SRC/DST IP Address)
- 正常的Windows系統, SMB/CIFS, UDP 通訊協定的Port, 發送端編號應等於接收端編號(SRC Port==DST Port)
- SMB/CIFS, 登錄程序封包, 依序為 SMBr, SMBs, SMBsm, SMBt, SMBu, SMB%, SMB2, SMB3, SMB@, ...

封包範例 CIFS/SMB (Broadcast)

	Proto...	SRC IP addr.	Port	DST IP addr...	Port	Payload (Content of packet)
04:01:26.859	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:28.078	UDP	172.16.1.184	138	172.16.1.255	138	..... FCFDCNFDFBEMCACACACACACACACACACA. EEEJFECACACACACACACACACACACACACABN..SMB%....
04:01:52.187	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:52.953	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:53.718	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:55.453	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:56.203	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:56.968	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:58.703	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:01:59.453	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:00.218	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:02.906	ARP	172.16.1.160		172.16.1.2		.....@...K.....
04:02:04.750	UDP	172.16.1.183	138	172.16.1.255	138	...p..... ENEPENCNFDFBEMCACACACACACACACACA. EEEJFECACACACACACACACACACACACACABN..SMB%..
04:02:16.875	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:17.640	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:18.359	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:20.125	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:20.890	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:21.609	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:23.375	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:24.140	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:24.859	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:25.625	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:26.375	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:27.140	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:28.875	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:29.625	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:30.390	UDP	172.16.1.181	137	172.16.1.255	137	..... ENEPENDADBCOEEEJFECOEMEPEDEBEMAA.. ..
04:02:30.453	UDP	172.16.1.160	138	172.16.1.255	138	..... FAFCEJEOFECACACACACACACACACACAAA. FHEPFCELCACACACACACACACACACACABO..SMB%.....

封包範例 CIFS/SMB (Login/Access)

	Proto...	SRC IP addr.	Port	DST IP addr...	Port	Payload (Content of packet)
10:02:01.661	TCP	172.16.1.105	1032	172.16.1.103	139	.....
10:02:01.671	TCP	172.16.1.105	1032	172.16.1.103	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002..LAN
10:02:01.681	TCP	172.16.1.103	139	172.16.1.105	1032	...U.SMBr.....S.....2....A.....p..{@... .....r.I.EL...Z...1
10:02:01.681	TCP	172.16.1.105	1032	172.16.1.103	139	.....SMBs.....@.....A2...../.....w.NTLMSSP.....&..... ...DIA105WORKGROUPW.i.n.d.o.w.s. .2.0.0.0. .2.1
10:02:01.691	TCP	172.16.1.103	139	172.16.1.105	1032	...1.SMBs.....@....1.....NTLMSSP.....0.....@V.:;0g.....t.t.H...W.I.N.2.K._.S.E.R.V.E.R.....W.I.N.2.K._.S.E.R
10:02:01.701	TCP	172.16.1.105	1032	172.16.1.103	139	.....SMBs.....A2.....].....NTLMSSP.....L.....M.....@.....@.....@.....M.....D.I.A.1.0.5..N...vm.....+...
10:02:01.711	TCP	172.16.1.103	139	172.16.1.105	1032	...u.SMBs.....u.....J..W.i.n.d.o.w.s. .5...0...W.i.n.d.o.w.s. .2.0.0.0. .L.A.N. .M.a.n.a.g.e.r..
10:02:01.711	TCP	172.16.1.105	1032	172.16.1.103	139	...Z.SMBu.....Z...../..\.\.W.I.N.2.K._.S.E.R.V.E.R.\.I.P.C.$...?????.
10:02:01.721	TCP	172.16.1.103	139	172.16.1.105	1032	...8.SMBu.....8.....IPC....
10:02:01.731	TCP	172.16.1.105	1032	172.16.1.103	139	...r.SMB%.....d.....9.....\.....3..\.P.I.P.E.\.L.A.N.M.A.N.....h.WrLehDO.B16....9....
10:02:01.791	TCP	172.16.1.103	139	172.16.1.105	1032	.....SMB%.....d.....@.....8...@.@.....I.....MSHOME.....TEST_GROUP.....WORK.....WORKGROUP.....
10:02:01.941	TCP	172.16.1.105	1032	172.16.1.103	139	.....
10:02:04.194	UDP	172.16.1.201	138	172.16.1.105	138	..... FAFCEJEOFECACACACACACACACACACACA. EEEJEBDBDADFCACACACACACACACACAAA..SMB%.....
10:02:06.448	TCP	172.16.1.105	1033	172.16.1.201	139	
10:02:06.448	TCP	172.16.1.105	1033	172.16.1.201	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002..LAN
10:02:06.448	TCP	172.16.1.105	1033	172.16.1.201	139	.....SMBs.....u.e.h.....{.....Windows 2000 2195.Windows 2000 5.0.....\\PRINT\IPC$.?????.
10:02:06.448	TCP	172.16.1.105	1033	172.16.1.201	139	...o.SMB%.....h.....P.....0.\PIPE\LANMAN.....h.WrLehDz.B16BBDz...h.....WORK.
10:02:06.458	TCP	172.16.1.201	139	172.16.1.105	1033	...[.SMB%.....7.....@.....$...M@....\PRINT.....''E@g@`..
10:02:06.508	TCP	172.16.1.105	1032	172.16.1.103	139	...r.SMB%.....d...@.....9.....\.....3..\.P.I.P.E.\.L.A.N.M.A.N.....h.WrLehDO.B16....9....
10:02:06.508	TCP	172.16.1.103	139	172.16.1.105	1032	.....SMB%.....d...@....@.....8...@.@.....I.....MSHOME.....TEST_GROUP.....WORK.....WORKGROUP.....
10:02:06.658	TCP	172.16.1.105	1032	172.16.1.103	139	.....
10:02:07.359	TCP	172.16.1.105	1033	172.16.1.201	139	.....SMBs.....u.x.h.....;...Administrator.DIA105.Windows 2000 2195.Windows 2000 5.0.....+.rug.2`..
10:02:07.359	TCP	172.16.1.105	1033	172.16.1.201	139	...N.SMB-.....B.....U.?.....\PIPE\srvsvc.
10:02:07.359	TCP	172.16.1.105	1033	172.16.1.201	139	...c.SMB%.....P.....$.\PIPE\LANMAN.....WrLeh.B13BWz.....
10:02:07.359	TCP	172.16.1.201	139	172.16.1.105	1033	.....SMB%.....7.....@.....!_....\TEST1....._.TEST2....._...s....._.E....._.HP4050PS.
10:02:07.419	TCP	172.16.1.105	1033	172.16.1.201	139	...O.SMB-.....B.....U.?.....\PIPE\spoolss.
10:02:07.419	TCP	172.16.1.105	1033	172.16.1.201	139	...N.SMB-.....B.....U.?.....\PIPE\winreg.

封包範例 CIFS/SMB (Login/Retry)

	Proto...	SRC IP addr.	Port	DST IP addr...	Port	Payload (Content of packet)
14:48:25.345	TCP	172.16.1.220	139	172.16.1.23	1075	
14:48:25.345	TCP	172.16.1.220	139	172.16.1.23	1075	....
14:48:25.345	TCP	172.16.1.23	1075	172.16.1.220	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002..LANMA
14:48:25.345	TCP	172.16.1.220	139	172.16.1.23	1075	...c.SMBr.....S.....C..P..t ... .J..;$^.P.R.O.G.R.A.M.M.E.R...
14:48:25.345	TCP	172.16.1.23	1075	172.16.1.220	139	.....SMBs.....@..u.....2.....M.....W.i.n.d.o.w.s. .2.0.0.0. .2.1.9.5...W.i.n.d.o.w.s. .2.0.0.0. .5...0...../..\.\.1
14:48:25.345	TCP	172.16.1.220	139	172.16.1.23	1075	.....SMBs.....@..u.....[..W.i.n.d.o.w.s. .N.T. .4...0...N.T. .L.A.N. .M.a.n.a.g.e.r. .4...0...P.R.O.G.R.A.M.M.E.R.....IP
14:48:25.355	TCP	172.16.1.23	1075	172.16.1.220	139	... .SMBs.....u.....2.....n.ulH.>G(..Uc....O.ky. ..9`.....ie..F2wG.0. .J.p.A.d.m.i.n.i.s.t.r.a.t.o.r...D.I.A.2.3...W.i.r
14:48:25.505	TCP	172.16.1.220	139	172.16.1.23	1075	
14:48:28.369	TCP	172.16.1.220	139	172.16.1.23	1075	...#.SMBsm.....
14:48:28.469	TCP	172.16.1.23	1075	172.16.1.220	139	
14:48:31.424	ARP	172.16.1.1		172.16.1.23		.....@..q.....
14:48:32.926	UDP	172.16.1.23	137	172.16.1.220	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!..
14:48:43.841	UDP	172.16.1.220	137	172.16.1.23	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.....HELLO ...HELLO ..PROGRAMMER ...HELLO
14:48:45.944	UDP	172.16.1.23	137	172.16.1.220	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!..
14:48:45.944	UDP	172.16.1.220	137	172.16.1.23	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.....HELLO ...HELLO ..PROGRAMMER ...HELLO
14:48:46.896	TCP	172.16.1.23	1075	172.16.1.220	139	.....SMBs.....u.....2.....r..S*.g.....k ..O.ky. ..M..tx.Oc..A.X..._...p.\.a.b.c.d.e.f.g...D.I.A.2.3...W.i.n.d.o.w.s. .2
14:48:47.046	TCP	172.16.1.220	139	172.16.1.23	1075	
14:48:50.000	TCP	172.16.1.220	139	172.16.1.23	1075	...#.SMBsm.....

封包範例 CIFS/SMB (Password Attack)

	Proto...	SRC IP addr.	Port	DST IP address	Port	Payload (Content of packet)
06:13:06.958	TCP	211.21.99.219	4250	211.21.41.116	139	.....SMBr.....PC NETWORK PROGRAM 1.0..XENIX CORE..MICROSOFT NETWORKS 1.03..LANMAN
06:13:06.958	TCP	211.21.41.116	139	211.21.99.219	4250	...[.SMBr.....2.....C...E.U. .. ..K..1...D.O.M.A.I.N...
06:13:07.108	TCP	211.21.99.219	4250	211.21.41.116	139	.....SMBs.....'..wdj.....u.....2.....v..#.[.o..Xd4..j....}..o..x....i..e!0....-vbiA.d.m.i.n.i.s.t.r.a.t.o.r...E.-.K.I.O.S.K
06:13:07.309	TCP	211.21.41.116	139	211.21.99.219	4250	
06:13:10.313	TCP	211.21.41.116	139	211.21.99.219	4250	...#.SMBsm.....'..wdj.....
06:13:10.363	TCP	194.144.45.46	2125	211.21.41.116	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002
06:13:10.363	TCP	211.21.41.116	139	194.144.45.46	2125	...[.SMBr.....S.....2.....C..@..W. .. ..ea. ,D.O.M.A.I.N...
06:13:10.363	TCP	211.21.99.219	4250	211.21.41.116	139	.....
06:13:11.214	TCP	194.144.45.46	2125	211.21.41.116	139	.....
06:13:11.364	TCP	194.144.45.46	2125	211.21.41.116	139	.....SMBs.....@..u.....2.....'.2..Q...o8...R.D.....j.c.rt#M..3..P..f....m.''...G.u.e.s.t...4.R.U.N.N.E.R.-.V.V
06:13:11.515	TCP	211.21.41.116	139	194.144.45.46	2125	
06:13:14.519	TCP	211.21.41.116	139	194.144.45.46	2125	...#.SMBsm.....@....
06:13:19.827	TCP	194.144.45.46	2338	211.21.41.116	139	.....
06:13:20.628	TCP	194.144.45.46	2338	211.21.41.116	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002
06:13:20.628	TCP	211.21.41.116	139	194.144.45.46	2338	...[.SMBr.....S.....2.....C..@.(]. .. ....,8.Y....D.O.M.A.I.N...
06:13:21.078	TCP	194.144.45.46	2338	211.21.41.116	139	.....SMBs.....@..u.....2.....qU...;...0.3...a.....].G.T.....?.P&..q.O.~.RUV..G.u.e.s.t...4.R.U.N.N.E.R.-.\
06:13:21.229	TCP	211.21.41.116	139	194.144.45.46	2338	
06:13:24.233	TCP	211.21.41.116	139	194.144.45.46	2338	...#.SMBsm.....@....
06:13:29.641	TCP	194.144.45.46	2571	211.21.41.116	139	.....
06:13:31.193	TCP	194.144.45.46	2571	211.21.41.116	139	.....SMBr.....S.....b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002
06:13:31.243	TCP	211.21.41.116	139	194.144.45.46	2571	...[.SMBr.....S.....2.....C..p.wc. .. ....B....8MrD.O.M.A.I.N...
06:13:31.694	TCP	194.144.45.46	2571	211.21.41.116	139	.....SMBs.....@..u.....2.....>1%ft.....L...eA.W.+...5.rl+q..y...WYr....G.u.e.s.t...4.R.U.N.N.E.R.-.V.\
06:13:31.844	TCP	211.21.41.116	139	194.144.45.46	2571	
06:13:34.848	TCP	211.21.41.116	139	194.144.45.46	2571	...#.SMBsm.....@....
06:13:40.306	TCP	194.144.45.46	2809	211.21.41.116	139	
06:13:40.707	TCP	194.144.45.46	2809	211.21.41.116	139	.....
06:13:40.707	TCP	211.21.99.219	4886	211.21.41.116	139	.....SMBr.....PC NETWORK PROGRAM 1.0..XENIX CORE..MICROSOFT NETWORKS 1.03..LANMAN
06:13:40.707	TCP	211.21.41.116	139	211.21.99.219	4886	...[.SMBr.....2.....C..`.Ii. .. ....p....b..D.O.M.A.I.N...
06:13:40.867	TCP	211.21.99.219	4886	211.21.41.116	139	.....SMBs.....$. .....u.....2.....X'&.V?Izva.....<...~.J....6p@.....'....8.@#5*.Q.iA.d.m.i.n.i.s.t.r.a.t.o.r...E.-.K.I
06:13:40.967	TCP	211.21.41.116	139	211.21.99.219	4886	

封包範例 CIFS/SMB

	Proto...	SRC IP addr.	Port	DST IP address	Port	Payload (Content of packet)
23:32:34.377	TCP	61.222.173.164	1561	61.222.19.128	445	
23:32:35.279	TCP	61.222.173.164	1089	61.222.5.140	135	
23:32:35.379	TCP	61.222.173.164	1570	61.222.89.25	445	
23:32:44.892	TCP	61.222.173.164	1090	61.222.5.140	445	
23:32:44.892	TCP	61.222.173.164	1092	61.222.103.32	445	
23:32:45.093	TCP	61.222.173.164	1588	61.222.7.42	445	
23:32:46.294	TCP	61.222.173.164	1094	61.222.201.180	445	
23:32:47.196	TCP	61.222.173.164	1596	61.222.48.228	445	
23:32:47.296	TCP	61.222.173.164	1096	61.222.76.38	445	
23:32:47.897	TCP	61.222.173.164	1090	61.222.5.140	445	
23:32:48.097	TCP	61.222.173.164	1588	61.222.7.42	445	
23:32:49.299	TCP	61.222.173.164	1094	61.222.201.180	445	
23:32:50.250	TCP	61.222.173.164	1596	61.222.48.228	445	
23:32:50.350	TCP	61.222.173.164	1096	61.222.76.38	445	
23:32:53.955	TCP	61.222.173.164	1090	61.222.5.140	445	
23:32:53.955	TCP	61.222.173.164	1093	61.222.201.180	135	
23:32:54.156	TCP	61.222.173.164	1588	61.222.7.42	445	
23:32:55.357	TCP	61.222.173.164	1094	61.222.201.180	445	
23:32:56.259	TCP	61.222.173.164	1596	61.222.48.228	445	
23:32:56.359	TCP	61.222.173.164	1096	61.222.76.38	445	
23:33:05.983	TCP	61.222.173.164	1097	61.222.141.222	135	
23:33:05.983	TCP	61.222.173.164	1099	61.222.239.114	135	
23:33:06.183	TCP	61.222.173.164	1613	61.222.189.23	445	
23:33:06.283	TCP	61.222.189.23	445	61.222.173.164	1613	.....
23:33:06.584	TCP	61.222.173.164	1604	61.222.119.125	445	
23:33:06.784	TCP	61.222.173.164	1613	61.222.189.23	445	
23:33:06.884	TCP	61.222.189.23	445	61.222.173.164	1613	.....
23:33:07.084	TCP	61.222.173.164	1604	61.222.119.125	445	
23:33:07.184	TCP	61.222.173.164	1100	61.222.16.79	445	
23:33:07.285	TCP	61.222.173.164	1613	61.222.189.23	445	

EternalBlue Attack Successfully

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封 包 內 容
01:22:49.382	TCP	192.168.198.203	445	192.168.198.204	51112	...s.SMBr....S.....@....2.....dV.....Q>eq..W.O.R.K.G.R.O.U.P...I.E.1.1.W.I.N.7...
01:22:49.382	TCP	192.168.198.204	51112	192.168.198.203	445	.....SMBs.....@.....K.....W.i.n.d.o.w.s. .2.0.0.0. .2.1.9.5...W.i.n.d.o.w.s. .2.0.0.0. .5...0...
01:22:49.382	TCP	192.168.198.203	445	192.168.198.204	51112	.....SMBs.....@.....W.i.n.d.o.w.s. .7. .E.n.t.e.r.p.r.i.s.e. .7.6.0.1. .S.e.r.v.i.c.e. .P.a.c.k. .1...W.i.n.d.o.w.s. .7. .E
01:22:49.382	TCP	192.168.198.204	51112	192.168.198.203	445	...`.SMBu.....@....`.....5.\\1.9.2...1.6.8...1.9.8...2.0.3.\I.P.C.$...?????.
01:22:49.382	TCP	192.168.198.203	445	192.168.198.204	51112	...8.SMBu.....@....8.....IPC....
01:22:49.382	TCP	192.168.198.204	51112	192.168.198.203	445	...N.SMB2.....A.....X.E.....B...N.....
01:22:49.382	TCP	192.168.198.203	445	192.168.198.204	51112	...#.SMB2.....A....
01:22:49.384	TCP	192.168.198.204	51112	192.168.198.203	445	...8.SMB.....A.....K.....h.....
01:22:49.385	TCP	192.168.198.203	445	192.168.198.204	51112	...#.SMB.....A....
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5.....
01:22:49.385	TCP	192.168.198.203	445	192.168.198.204	51112	.....
01:22:49.385	TCP	192.168.198.203	445	192.168.198.204	51112	.....
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5.....4zA5wOHAnXFc8aUbT0sWVOavzD83o6gNoKt2xHjqoptAFHztME4OBTKCsK
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	WRy5Oy+XBV6arMpbsap3gagqNTh7t5RsIGyuHALHwuC4wD0dxx4W9x5GvozR4ByI0sDrMiJymd0E2QOY9SoUTh7pC
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5..#....XPJv4SW5FNH1fRVIZps7qY97r+uvM3fOb+rEEdRoykNop/NA5P/YOybUw9V
01:22:49.385	TCP	192.168.198.203	445	192.168.198.204	51112	.....
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5..3....BfqMPFJ5IoHq01SWMug8VBYlqFY/bC3b/1fMi+sodKkY9ed19YcNaGJJnrWe
01:22:49.385	TCP	192.168.198.203	445	192.168.198.204	51112	.....
01:22:49.385	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5..C....5UE7Si8euG0Hh+mnLP5w9SyZZwcmyH+CSDHInxDJQ59JC4x7Ks6ICHRPcR
01:22:49.386	TCP	192.168.198.203	445	192.168.198.204	51112	.....
01:22:49.386	TCP	192.168.198.204	51112	192.168.198.203	445	...5.SMB3.....A.....5..S....Xe0pMEkrqxDHAOBmz9hXtueiScDlN64BGbqHV6ivN78DEeEKh2L3H4VFYr
01:22:49.386	TCP	192.168.198.203	445	192.168.198.204	51112	.....

EternalBlue Attack Successfully

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封 包 內 容
01:22:50.419	TCP	192.168.198.204	51118	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51118	.....
01:22:50.419	TCP	192.168.198.204	51119	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51119	.....
01:22:50.419	TCP	192.168.198.204	51120	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51120	.....
01:22:50.419	TCP	192.168.198.204	51121	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51121	.....
01:22:50.419	TCP	192.168.198.204	51122	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51122	.....
01:22:50.419	TCP	192.168.198.204	51123	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51123	.....
01:22:50.419	TCP	192.168.198.204	51124	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51124	.....
01:22:50.419	TCP	192.168.198.204	51125	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51125	.....
01:22:50.419	TCP	192.168.198.204	51126	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51126	.....
01:22:50.419	TCP	192.168.198.204	51128	192.168.198.203	445	.....
01:22:50.419	TCP	192.168.198.203	445	192.168.198.204	51128	.....
01:22:50.420	TCP	192.168.198.204	51129	192.168.198.203	445	.....
01:22:50.420	TCP	192.168.198.203	445	192.168.198.204	51129	.....

DoublePulsar backdoor connecting

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封 包 內 容
00:09:37.548	TCP	192.168.198.203	49847	192.168.198.204	139	
00:09:37.549	TCP	192.168.198.204	139	192.168.198.203	49847	
00:09:37.549	TCP	192.168.198.203	49847	192.168.198.204	139	...D EEEFFDELFEEPFACNEBEGFAFGEFFBDCCA. EJEFDBDBFHEJEODHCACACACACACACACAAA.
00:09:37.549	TCP	192.168.198.204	139	192.168.198.203	49847	.....
00:09:37.549	TCP	192.168.198.203	49847	192.168.198.204	139	.....SMBr.....S.....x..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002.
00:09:37.552	TCP	192.168.198.204	139	192.168.198.203	49847	.....
00:09:37.553	TCP	192.168.198.204	139	192.168.198.203	49847	.....SMB@.....A.....0`.M.D....b;.....l.....@.....`..<..+.....00.,.0...+.....7....
00:09:37.553	TCP	192.168.198.203	49847	192.168.198.204	139	...h.SMB@.....$.....yF8.....)h$Z.....
00:09:37.556	TCP	192.168.198.204	139	192.168.198.203	49847	.....SMB@.....A.....0`.M.D....b;.....l.....@.....`..<..+.....00.,.0...+.....7....
00:09:37.556	TCP	192.168.198.203	49847	192.168.198.204	139	.....SMB@.....X.J.....`H..+.....>0<..0...+.....7....*.(NTLMSSP.....
00:09:37.556	TCP	192.168.198.204	139	192.168.198.203	49847	...W.SMB@.....H.....0.....+.....7.....NTLMSSP.....8.....2U..L.n.....V....Z)
00:09:37.557	TCP	192.168.198.203	49847	192.168.198.204	139	.....SMB@.....X.....0.....{.yNTLMSSP.....h.....i.....X.....X.....X.....i...
00:09:37.557	TCP	192.168.198.204	139	192.168.198.203	49847	...I.SMB@...".....
00:09:37.557	TCP	192.168.198.203	49847	192.168.198.204	139	.....
00:09:37.557	TCP	192.168.198.204	139	192.168.198.203	49847	.....
00:09:37.558	TCP	192.168.198.203	49847	192.168.198.204	139	.....
00:09:37.559	UDP	192.168.198.203	51402	224.0.0.252	5355	.....DESKTOP-AFPVEQ2.....
00:09:37.559	UDP	192.168.198.204	5355	192.168.198.203	51402	.....DESKTOP-AFPVEQ2.....DESKTOP-AFPVEQ2.....
00:09:37.560	TCP	192.168.198.203	49848	192.168.198.204	139	
00:09:37.560	TCP	192.168.198.204	139	192.168.198.203	49848	
00:09:37.560	TCP	192.168.198.203	49848	192.168.198.204	139	...D EEEFFDELFEEPFACNEBEGFAFGEFFBDCCA. EJEFDBDBFHEJEODHCACACACACACACACAAA.
00:09:37.560	TCP	192.168.198.204	139	192.168.198.203	49848	.....

WannaCrypto 初始化封包範例 (TOR初始化)

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:57:55.507	TCP	10.0.1.3	49586	199.254.238.52	443	
14:57:55.660	TCP	199.254.238.52	443	10.0.1.3	49586	
14:57:55.660	TCP	10.0.1.3	49586	199.254.238.52	443	
14:57:55.667	TCP	10.0.1.3	49586	199.254.238.52	443	.....dR.....x8!..VA2l.0.E].]..x.....0.+./.....3.2.E.9.8...../.A.5.....w.....www.2jjt4zoh252nx5ngk.com.....
14:57:55.820	TCP	199.254.238.52	443	10.0.1.3	49586	.....
14:57:55.823	TCP	199.254.238.52	443	10.0.1.3	49586	....>...:..5...0.>G.`P....E..F..q...'G.r..G../.....0...0..#.....0...*.H.....0.1.0...U....www.ojt2c5bdude3.cor
14:57:55.825	TCP	10.0.1.3	49586	199.254.238.52	443	....F...BA..};a...T..:.-$i..}].G.~hel.....2.../$.....f..jL....2..5b.Q.....(i0q`...v...+..%.Mi....W.>/f.....j...
14:57:55.982	TCP	199.254.238.52	443	10.0.1.3	49586	.....(...O...P....Jv.WEB~:U.....:..F.va.w.gTc:.
14:57:55.982	TCP	10.0.1.3	49586	199.254.238.52	443	....!i0q`...w-k..#JJ....J4.Bu..R3.....
14:57:56.140	TCP	199.254.238.52	443	10.0.1.3	49586	.....O...Q..x..gPp.]\..?.#9.R..mL...b..{..4k...*./<}.u.9....2...b...1....v%.....,-.Y}wb.NX.*um.D....9.x.>.....6....TC\..g..,BF
14:57:56.140	TCP	199.254.238.52	443	10.0.1.3	49586	.$...R..R.2q..HO.@.x.e.+'<./K.9.....
14:57:56.140	TCP	10.0.1.3	49586	199.254.238.52	443	
14:57:56.141	TCP	10.0.1.3	49586	199.254.238.52	443	.....i0q`...x.....O.Vs..6...Y..o..... ..>+];.....'.....g...=..<8..K.h..... .....0!o.n.0...p.....e.R.....6..#.....fM;z...-.z..:
14:57:56.295	TCP	199.254.238.52	443	10.0.1.3	49586	.....O...R..$.....k.."..KrG....A.....7.p.....d.}Id.)/.....y.O...-n..u..y#R.....5.....y...."Ln.,E..S.!..V..e.h....eQ..#.d.....@.x8.:
14:57:56.296	TCP	10.0.1.3	49586	199.254.238.52	443	.....i0q`...y.....1kO..k.oY..d.....q..R....~6.p<.D.8.,k...[l.P.p.....j...&....Z.big.d.}i%a.kTc.o.o!z....A.v....f}...W~'!..%vl.t..;Q.....
14:57:56.452	TCP	199.254.238.52	443	10.0.1.3	49586	.....O...S-...H...j.o.....@.,...c...+.....a....TT# ...4.w.w.sWe...Y.Yy.<..u0yaA.1._.....P...[.....$.....d.0VKP@...Gz.W:D.0..fF.
14:57:56.457	TCP	199.254.238.52	443	10.0.1.3	49586	.....O...T.....cSH...3.DO.....z...0...]....a.=.gm'M3h..R.W.+^dIPJ..A}.v....H.J..R...+.X.o.....i2..rS..L.J(...;..\..K.u.R..'.O....i..
14:57:56.457	TCP	10.0.1.3	49586	199.254.238.52	443	
14:57:56.457	TCP	199.254.238.52	443	10.0.1.3	49586	....E..S%.>..0...?... ...S.j.?...l.M.....-._...HL..$y.../.r.X...tp.b.....o...1.....O....;...*..i.K..@...=hu.....~.l..zg.7.P.....{Q..R.C
14:57:56.457	TCP	199.254.238.52	443	10.0.1.3	49586	.....f..M}..U.$...~+S..EQ...tA..b..Z...Q[.r1`\....1..\W...D.,..<Yi....Gf.R,x.=].....S.-s..qc..0.K..+o7E`.}...C..o..FV.r~?....9..d.....#..
14:57:56.457	TCP	199.254.238.52	443	10.0.1.3	49586	...:J..!>L.3I..f...f}M.."=..+>.}.s.L.....wR..j}....*.FF..vhM1..M.cT...ut...N.%3.....l.....:..i.!...%..>...$.o.pA[g.....i..Tm.....qA..'
14:57:56.457	TCP	199.254.238.52	443	10.0.1.3	49586	.....x,o.....l).Q..Vl.:.0J.....7.*.....$.&<...r...[g]U.../..w..0Wv..iD..x"C.K.....BZM0.I..6W.n...R$.q.1...A.,.&.K.4..W....C..9..m.'

WannaCrypto 封包範例 (TOR通訊)

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
14:59:32.651	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.0...r.6..2\.!U..s..+.6.J.F....l.}W.@.....^YXT.....CP.g..}...X.q.aY.G.*r.....z..*}1..../.Z....e.,p.....a4.!{..V...T...F[.....HS
14:59:32.895	TCP	104.131.108.7	9001	10.0.1.3	49588	.....
14:59:32.898	TCP	104.131.108.7	9001	10.0.1.3	49588	.....x..q=.N3F&6....]..p....J...{X....'!.j.8l..c3..GG.O...8.5..G...t..v..G'...O..P....o.HSs..(Lp..H".7.....j.:...LxZ(..{...0.4...n
14:59:32.901	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.1.....Q@.....g..S..g.....i...u..W%.....@..x.....p....i...o...<t..F..m.#:%.?.....*r=...gBjw.>..>.XzB.....7.n.....l.~$.E.2.I..
14:59:33.184	TCP	104.131.108.7	9001	10.0.1.3	49588	.....
14:59:33.230	TCP	104.131.108.7	9001	10.0.1.3	49588	.....x..c...l..R.R.u...k...-/4&.w.....w(...G..!K.W.....D.4._VT."...3....u%y.J.-..;t..J1(4....{?...X...k..3uE.(.].b.A..u.E^...\$..N.7
14:59:33.233	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.2"l..j.._...~.@.I..9X.k.....\.c...v.Dd.x<.....f[..N..o...L....Ne....~j.Mab....4[..!.GXBTD..$2...)..]o.c.....2b.Re6.....D..
14:59:33.478	TCP	104.131.108.7	9001	10.0.1.3	49588	.....H,..~....W.2)s.F..bQ...J.....N.@jV4...?..."..,'.<%..i.@J.....=....3&F*.....F8.K.hz.+;a....s#.v<..V...1...J.(....B.l..o...].76.
14:59:33.481	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.3o.`1...A...7.+Oc....1v./...:W..#X...a.5.E.....b>.....E)...O.M.?... .I.p..p..9ytz_tv..X.}D.=.....Y.LH*...,.]..V...../.x.
14:59:33.726	TCP	104.131.108.7	9001	10.0.1.3	49588	.....o...}..fx....uR.....jR...%..v.X..._<.A.....13.]W\l.g..+.s.PYK.....x...n..Ur.F.O.....yh\<..N..b.Z.....E..*.Z.....=.-.1
14:59:33.923	TCP	10.0.1.3	49588	104.131.108.7	9001	
14:59:34.167	TCP	104.131.108.7	9001	10.0.1.3	49588	.....i..~.7.....f%..C.mE..*.*.U.,Db.}E...Y....a.....h.el..P...K...cM.-.?%D..._.....=.....F6+.Z&K%.<..Y..aN...z{t&....&:.
14:59:34.368	TCP	10.0.1.3	49588	104.131.108.7	9001	
14:59:34.423	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.4..<...R.?.q.P....2.: <b.B\...E..Vn.....n%...m.2...L....`6....`7.q.z8.&o=.pl...wL...3..{..3....xb..sm.f..X.}.....Uk....8..D.<.s
14:59:34.613	TCP	104.131.108.7	9001	10.0.1.3	49588	.....%.P`..$.....W.)e....b.sW.l..A..n.V.fr?..6:Z.B.....3..7.#l?$.s.....aK.Y....iQ..p...rE.....x.{....h.@.....d...N...,.R.ZY}X.,.
14:59:34.714	TCP	104.131.108.7	9001	10.0.1.3	49588	.....
14:59:34.714	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.5.....5n..W...p..%%4u..>{..`q...P7....#..1...~...{....`.j.....lk.j.G.B.[K....X.c.~.....7bp...o[..x..;.... _..2..v.}..A...#w.ZR
14:59:34.958	TCP	104.131.108.7	9001	10.0.1.3	49588	.....MS....j..[..UZw.....5Y..<.-.E."d...l..\..f.6...+.7BJ.0.v1...W"$.BwK..N...\..}..JU....2..q.v.....3..A.E....Y.Z.....H.X..c.
14:59:34.961	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.6..@Ov....RM.....^,..0YQ..*!..6U/....q^.a..K..k..V....\.N....e.ny.}..;...b...Y(;d....z\iN.yOVT.N...E....H..RzC..*.(Jl.
14:59:35.205	TCP	104.131.108.7	9001	10.0.1.3	49588	.....T.n..."..O....r6.{e<<.....=.....>.[....4..:aw..x....N.P.d..%.z,.h.MX...../....?.....9.M_....}c.X.).k...C.b.l.d....
14:59:35.208	TCP	10.0.1.3	49588	104.131.108.7	9001	.....T..\.7l..PA.....).hF.=.D.t.....U.yo...F....l.R.jr.@y;.\l.^.TX.....!$..w.kL.b....;..U75.....k<...f`...cT.Z.....LL.?..>...\..9.....
14:59:35.452	TCP	104.131.108.7	9001	10.0.1.3	49588	.....q}...g".f..z*..4.....680....=..%.q.,...r.~Y.7...gsyPy.x....f.up.....<~....da...Z..).#...C.v3DFn8.....yp.....&.....2;Hg+L.

WannaCrypto 封包範例 (SMB通訊)

間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊...	封　包　內　容
16:53:19.274	TCP	10.0.1.15	49905	74.208.173.7	445	
16:53:19.274	TCP	10.0.1.15	49909	74.208.173.7	445	
16:53:19.471	TCP	74.208.173.7	445	10.0.1.15	49905	.....
16:53:19.471	TCP	74.208.173.7	445	10.0.1.15	49905	.....
16:53:19.472	TCP	74.208.173.7	445	10.0.1.15	49909	
16:53:19.472	TCP	10.0.1.15	49909	74.208.173.7	445	
16:53:19.472	TCP	10.0.1.15	49909	74.208.173.7	445	...T.SMBr.....(.....A.....^.1..LANMAN1.0..LM1.2X002..NT LANMAN 1.0..NT LM 0.12.
16:53:19.671	TCP	74.208.173.7	445	10.0.1.15	49909	...s.SMBr.....(.....A.....^....2....A.....M..L.....n...L..F....X_4`..+.....0...0...+.....7...
16:53:19.671	TCP	10.0.1.15	49909	74.208.173.7	445	...c.SMBs..... .....A.....^.....@...&....Windows 2000 2195.Windows 2000 5.0.
16:53:19.870	TCP	74.208.173.7	445	10.0.1.15	49909	.....SMBs..... .....A.....^.....Z.Windows (R) Web Server 2008 6002 Service Pack 2.Windows (R) Web Server 2008 6.0.V
16:53:19.870	TCP	10.0.1.15	49909	74.208.173.7	445	...[.SMBu..... .....A.....^.....\\192.168.137.1\IPC$.?????.PATH_REPLACE__?????.
16:53:20.069	TCP	74.208.173.7	445	10.0.1.15	49909	...#.SMBu..[... .....A.....^...
16:53:20.069	TCP	10.0.1.15	49909	74.208.173.7	445	...J.SMB%.....(.....A.....^.....J...J...#.....\PIPE\.
16:53:20.267	TCP	74.208.173.7	445	10.0.1.15	49909	...#.SMB%..[...(.....A.....^...
16:53:20.267	TCP	10.0.1.15	49909	74.208.173.7	445	
16:53:20.465	TCP	74.208.173.7	445	10.0.1.15	49909	.....
16:53:20.465	TCP	74.208.173.7	445	10.0.1.15	49909	.....
16:53:20.668	UDP	10.0.1.15	50452	168.95.1.1	53	.m.....7.173.208.74.in-addr.arpa.....
16:53:20.965	UDP	10.0.1.15	137	74.208.173.7	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!..
16:53:20.965	UDP	168.95.1.1	53	10.0.1.15	50452	.m.....7.173.208.74.in-addr.arpa.....X.7.ms.ui-dns.com..dnsadmin.1und1.de.w.....8@.....H...X
16:53:22.493	UDP	10.0.1.15	137	74.208.173.7	137	..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!..

WannaCrypto 動態分析

下午 02:57:30.4	Virus_Test123.exe	ReadFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp
下午 02:57:30.4	Virus_Test123.exe	ReadFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp
下午 02:57:30.4	Virus_Test123.exe	CreateFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	CreateFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	ReadFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT
下午 02:57:30.4	Virus_Test123.exe	WriteFile	C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp.WNCRYT

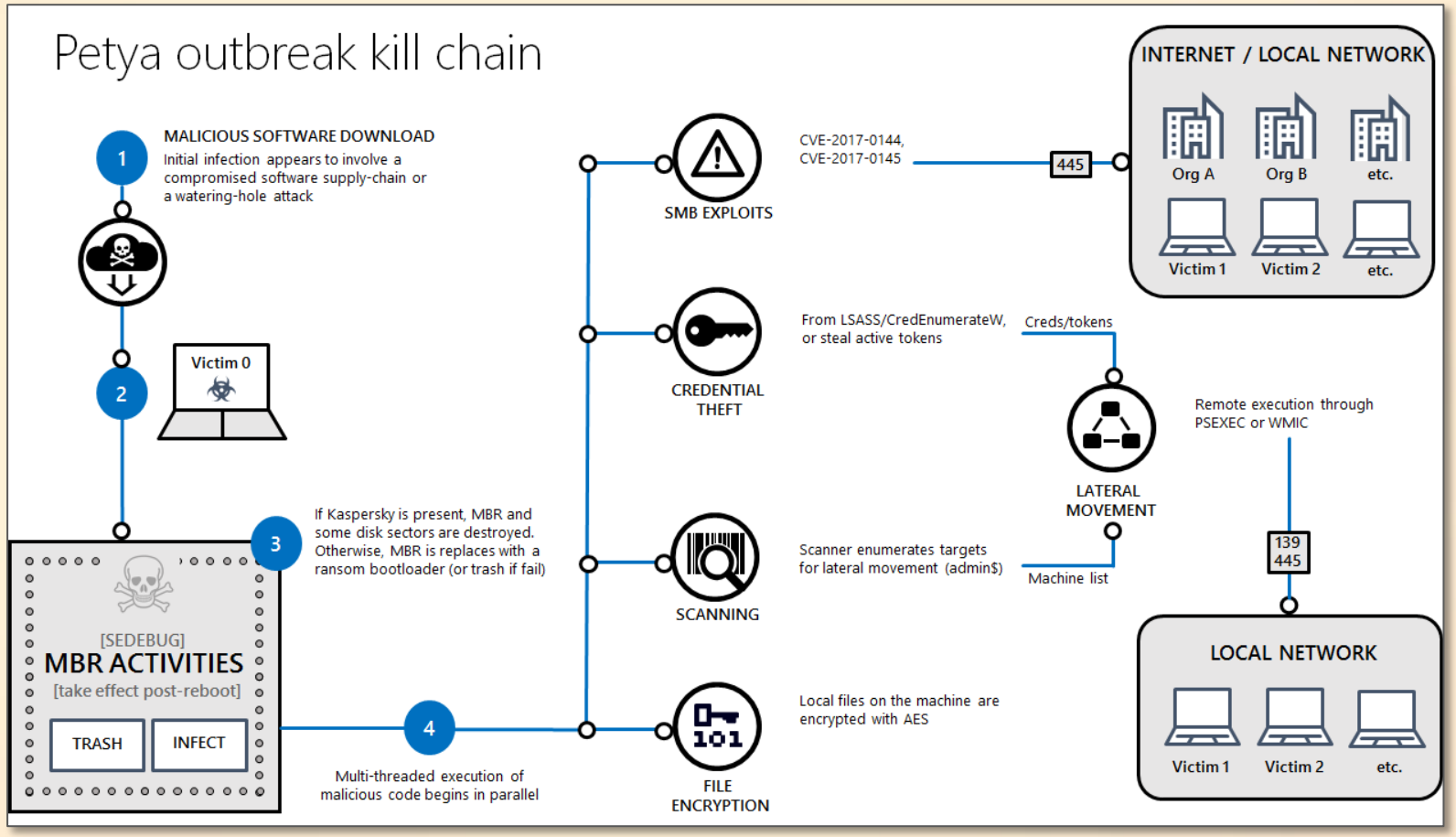
WannaCrypto (類似惡意程式)的特徵

- 初始化 TOR 的封包特徵
- TCP-139, TCP-445, TCP-9001 的對外封包
- UDP-137 的對外封包
- 先建立加密檔案, 再刪除原始檔案

Ransomware-Petya

- Petya的基本介紹
- Petya的動態分析
- Petya的封包範例

Petya 感染過程簡介



參考來源: https://blogs.technet.microsoft.com/mmpc/2017/09/06/ransomware-1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene/

Petya的動態分析

- **Petya** will modify the **Master Boot Record (MBR)** of Hard disk.
- **Petya** scans LAN to discover enumerate ADMIN$ shares on other systems, then copies itself to those hosts and executes the malware using PSEXEC. (需要有寫入分享目錄的權限)
- **Petya** uses WMI (Windows Management Instrumentation Command-line) to connect to hosts on the local subnet and attempts to execute itself remotely on those hosts.
- **Petya** finally attempts to use **EternalBlue** against hosts on the local subnet. This will only be successful if the target-host does not patch MS17-010.

Petya的動態分析

勒索軟體的應對討論

- WannaCrypto行為與應對
- WannaCrypto封包與阻斷
- Petya行為與應對
- Petya封包與阻斷
- 可能誤判封包討論

WannaCrypto行為與應對

- 作業系統保持更新(Windows Update)
- 檔案定期備份, 符合3-2-1原則
  - 3 份 備份檔案 (1份檔案, 存成 3 份)
  - 2 種 不同儲存媒體 (雲端備份, USB備份, 光碟備份, NAS備份 ...)
  - 1 個 不同的存放地點 (辦公室, 家裡,...)
- NAS考慮使用「非網路芳鄰模式」(FTP或HTTP模式)
- 考慮停止使用網路芳鄰或是SMBv1 (請參考 https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/)

WannaCrypto封包與阻斷

- 單一IP位址, 對網際網路, 同時出現TCP-443, TCP-9001, TCP-139或TCP-445通訊封包, 表示有異常發生。
- 內部網路,單一IP位址,出現大量TCP-139或TCP-445的SMB@或SMB3特徵資料, 表示有異常發生。
- 阻斷TCP-135, TCP-139, TCP-445, UDP-135, UDP-136, UDP-137, UDP-138 對網際網路的通訊連接。
- 禁止內部網路的TCP-135, TCP-139, TCP-445, UDP-135, UDP-136, UDP-137, UDP-138, 跨網段電腦連線(保留)
- DoublePulsar is the backdoor (which listens via SMB or RDP) installed by both EternalBlue and EternalRomance.

可能誤判封包討論

- TCP-443的封包, 包括 HTTPS 與 TOR, WannaCrypto的封包，需要觀察其中差異特徵。
- TCP-443的封包, 初始化階段出現網址, 表示為TOR或WannaCrypto的封包。
- 要提醒各單位, TOR瀏覽器的使用, 屬於個人行為。
- 正常HTTPS的初始化通訊, 前段會出現DNS封包, 接著交換RSA憑證。
- TOR的初始化通訊, 不會產生DNS封包。

問題與討論

- 未來匿蹤封包討論
- Q&A

Name : Diamond Liu (劉得民) 0985-604-145
Email : dmliu99999@hotmail.com

God is not on the side of the big battalions, but on the side of those who shoot best.

Voltaire, French author, wit, and philosopher