

The Endless Game: Fighting Against Kelihos Botnet

) Yang

t Inc.

t]fortinet.com

action

rely focus on the 4 main and 1 minor generation Kelihos' protocol and encryption algorithm. Change traffic data will be used as examples.

Protocol and Encryption of 1st generation Kelihos

0000h:	01 02 01 01 01 01 02 01	91 01 00 00	00 00 00 00	\.....
0010h:	01 E8 03 00 00	00 00 00 00	00 00 00 00	.è.....
0020h:	00 05 76 44 6D 86 14 63 3B FE 67 AD 29 10 72 EE			..vDm†.c;pg-).rî
0030h:	45 1A 4E 2B 13 AC F0 6C 29 29 F4 0C 4E 40 26 90			E.N+.-ðl)) ô.N@&@
0040h:	4D 01 69 6F 3D 13 3A A7 06 F8 ED 09 59 DF E0 35			M.io=:.\$.øí.YBà5
0050h:	D1 99 18 69 B7 97 F1 38 79 99 6C 0E 06 72 7A 82			Ñ™.i.-ñ8y™l...rz,
0060h:	BC A2 27 B8 E3 FC 28 48 6C 91 EA 44 24 A8 14 3C			¼ç' ,ãü(Hl'êD\$".<
0070h:	EF 11 00 CF BD 57 46 55 BA 36 09 15 09 0D 74 2B			ï...İ½WFU°6....t+
0080h:	39 10 50 42 C1 FF 67 25 1B FE F2 BC 32 F3 31 78			9.PBÁÿg%.pò¼2ólx

Date 1 - 1st Gen, Bot Send Data(Partial)

Encryption Algorithm:

compressed->BlowFish

0000h:	A2 49 4D F3 D9 1E 9F 88	01 01 20 6D 5F 62 6F 6F	¢IMÓÛ.Ÿ^.. m_boo
0010h:	74 73 74 72 61 70 5F 6C 69 73 74 00 01 04 6D 5F		tstrap_list...m_
0020h:	63 6C 69 65 6E 74 73 5F 6C 69 73 74 00 03 50 01		clients_list..P.
0030h:	14 6D 5F 63 6C 69 65 6E 74 5F 69 64 00 02 01 40		.m_client_id...@
0040h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
0050h:	6D 5F 69 70 00 02 01 10 45 92 01 47 6D 5F 6C 61		m_ip....E'.Gm_la
0060h:	73 74 5F 61 63 74 69 76 65 5F 74 69 6D 65 00 02		st_active_time..
0070h:	01 20 00 00 00 00 00 00 00 00 6D 5F 6C 69 73 74		m_list
0080h:	65 6E 69 6E 67 5F 70 6F 72 74 00 02 01 10 50 00		ening port....P.

ompressed->BlowFish->BlowFish->BlowFish

0000h:	A2 49 4D F3 D9 1E 9F 88	01	01 24 32 37 62 61 38	ϕIMóÛ.Ÿ^..\$27ba8
0010h:	38 34 66 37 30 37 39 66 34 34 30 00 02 01 10 00			84f7079f440.....
0020h:	00 00 00 35 35 62 39 36 64 34 61 63 64 32 65 30			...55b96d4acd2e0
0030h:	30 30 30 00 01 10 31 61 39 33 61 66 63 62 37 36			000...1a93afcb76
0040h:	66 35 30 30 30 30 00 02 02 10 74 65 73 74 38 36			f50000....test86
0050h:	35 65 30 31 36 31 62 38 66 31 39 63 30 30 00 02			5e0161b8f19c00..
0060h:	01 10 00 00 00 00 39 64 37 36 33 36 31 30 34 35			9d76361045
0070h:	61 34 34 34 30 30 00 02 01 10 00 00 00 00 63 38			a44400.....c8
0080h:	33 34 31 36 35 63 33 35 61 35 61 38 30 30 00 02			34165c35a5a800..

Date 4 - 1.5 Gen, Bot Send Data(Clear,Partial)

sol and Encryption of 2nd generation Kelihos

0000h:	40 54 40 98	17 2E 1D 07	00 CB CD 5B	F4 1C F7 AA	@T@~.....ËÍ[ô.÷ª
0010h:	71 21 0E F4	99 44 1C E8	68 02 00 00	00 00 00 00	q!..ô™D.èh.....
0020h:	00 00 C4 D8	00 0B AD DA	2C 57 F0 77	E2 49 67 B7	..ÄØ...-Ú,WõwâIg·
0030h:	19 3C CF 58	AA 6B 72 D0	EB 99 76 2F	9E 74 E0 8C	.<ïXªkrĐë™v/žtàË
0040h:	93 5F 14 C4	DC ED EB 2E	09 59 72 89	D4 87 8E 68	"_.ÄÜíë..Yr%Ô+žh
0050h:	ED 32 E2 0F	27 9E 1A 03	DA E5 A0	07 22 A5 97 BB	í2â.'ž..Úâ ."¥-»
0060h:	E1 AF 18 A5	41 E0 8F A7	37 D1 2A C6	C2 D7 AA 6E	á¯.¥Aà\$7Ñ*ÆÃ×ªn
0070h:	BF F2 B6 19	0A A1 6E 9D	18 24 29 3F	0F 43 53 E2	¿òŒ...;nŒ.\$)??.CSâ
0080h:	B8 34 B0 AB	02 07 FC 0A	B3 F9 74 6F	37 5A 98 B0	,4°«...ü.³ùto7Z~°
0090h:	30 2D D3 E4	2B 13 10 F0	19 C6 47 53	AF EA 3D 5A	0-Óä+...ð.ÆGS¯ê=Z

Date 5 - 2nd Gen, Bot Send Data(Partial)

ncryption Algorithm:

ompressed->BlowFish->3DES->BlowFish

0000h:	A2 49 4D F3 D9 1E 9F 88	01	01 28 31 31 32 65 72	ϕIMóÛ.Ÿ^..(112er
0010h:	35 68 35 37 62 35 37 35 37 36 37 35 30 32 00 01			5h57b575767502..
0020h:	0C 32 33 32 64 33 64 61 73 64 61 00 02 01 20 00			.232d3dasda... .
0030h:	00 00 00 00 00 00 00 34 34 35 67 65 36 76 77 34			445ge6vw4
0040h:	63 66 72 65 37 00 02 02 00 61 73 64 33 32 32 77			cfre7....asd322w
0050h:	32 33 32 00 02 02 00 32 37 62 61 38 38 34 66 37			232....27ba884f7
0060h:	30 37 39 66 34 34 30 00 02 01 10 00 00 00 00 35			079f440.....5
0070h:	35 62 39 36 64 34 61 63 64 32 65 30 30 30 30 00			5b96d4acd2e0000.

ncryption Algorithm:

lowFish->3DES->Compressed->BlowFish

0000h:	A2 49 4D F3 D9 1E 9F 88	01	01 24 31 00 02 01 40	çIMóÙ.Ÿ^..\$1...@
0010h:	70 A3 8A 64 02 53 41 06 B4 0E 52 F4 6E CA 10 ED			přŠd.SA.´.RônÊ.í
0020h:	33 00 02 01 20 75 D9 4B 4F 00 00 00 00 34 00 02			3... uÙKO....4..
0030h:	01 20 60 00 00 00 00 00 00 00 35 00 01 08 61 00			. `.....5...a.
0040h:	02 01 10 8C F2 12 00 6A 00 03 21 03 01 14 62 00			...Æò..j..!...b.
0050h:	02 01 10 59 75 51 01 64 00 02 01 10 50 00 00 00			...YuQ.d....P...
0060h:	67 00 02 01 20 00 00 00 00 00 00 00 00 70 00 02			g...p..
0070h:	01 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00			.@.....
0080h:	00 00 78 00 02 01 20 00 00 00 00 00 00 00 00 01			..x... ..
0090h:	14 62 00 02 01 10 55 7A 55 01 64 00 02 01 10 50			.b....UzU.d....P

Date 8 - 3rd Gen, Bot Send Data(Clear,Partial)

sol and Encryption of 5th generation Kelihos

0000h:	03 94 00 6c 2e 94 00 6c	3e 94 00 6c 4f 95 00 6c	...1...1 >..10..1
0010h:	64 98 00 6c 54 95 00 6c	52 c0 62 0e a4 82 6c e7	d..lT..l R.b...l.
0020h:	c0 bf 8f f2 80 ba 11 e4	57 ff 1f a9 7e 88 53 df	 W...~.S.
0030h:	a3 a8 ef 37 d2 bf 16 28	ba 01 f8 13 9c d3 b4 5c	...7...(.....\
0040h:	76 d8 4d 52 c0 62 0e a4	82 6c e7 c0 bf 8f f2 80	v.MR.b.. .l.....
0050h:	ba 11 e4 82 4e 0c b2 09	cd 05 05 b7 71 9e 79 69	N...q.yi
0060h:	0d b6 af b2 13 df d3 22	25 10 d0 5b 73 da 86 dc	" %..[s...
0070h:	65 46 7c b4 d2 c5 16 78	84 72 76 c9 fc 6f 2e f1	eFx .rv..o...
0080h:	29 70 1a e2 e2 e0 b7 1d	2d 4e 8f 47 81 1f 0d 66	)p..... -N.G...f
0090h:	71 c1 09 6f 23 29 1c 48	a7 0f 42 d1 da 18 b6 a6	q..o#).H ..B.....

Date 9 - 5th Gen, Bot Send Data(Partial)

ncryption Algorithm:

lowFish->Custom Encryption->Compressed

0000h:	A2 49 4D F3 D9 1E 9F 88	01	01 24 31 00 02 01 40	Ç IMóù.??..\$1...
0010h:	CD 4B 72 D8 3D D8 42 C9 A7 FF 00 28 E3 EE 5E 7F			íKr?=?Bé\$?.(??^□
0020h:	33 00 02 01 20 66 62 6B 50 00 00 00 00 34 00 02			3... fbkP....4..
0030h:	01 20 5A 00 00 00 00 00 00 00 35 00 01 08 61 00			. z.....5...a.
0040h:	02 01 10 00 00 00 00 00 6A 00 03 15 03 01 14 62 00			j.....b.
0050h:	02 01 10 4C 71 C7 01 64 00 02 01 10 50 00 00 00			...Lq?.d....P...
0060h:	67 00 02 01 20 00 00 00 00 00 00 00 00 70 00 02			g...p..
0070h:	01 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00			.@.....