



Fighting Against Kelihos Botnet

--

Kyle Yang, CCIE#19065
Sr. Manager, AV Engine Development
Fortinet Inc. Canada



Agenda

1

Kelihos Botnet Overview

2

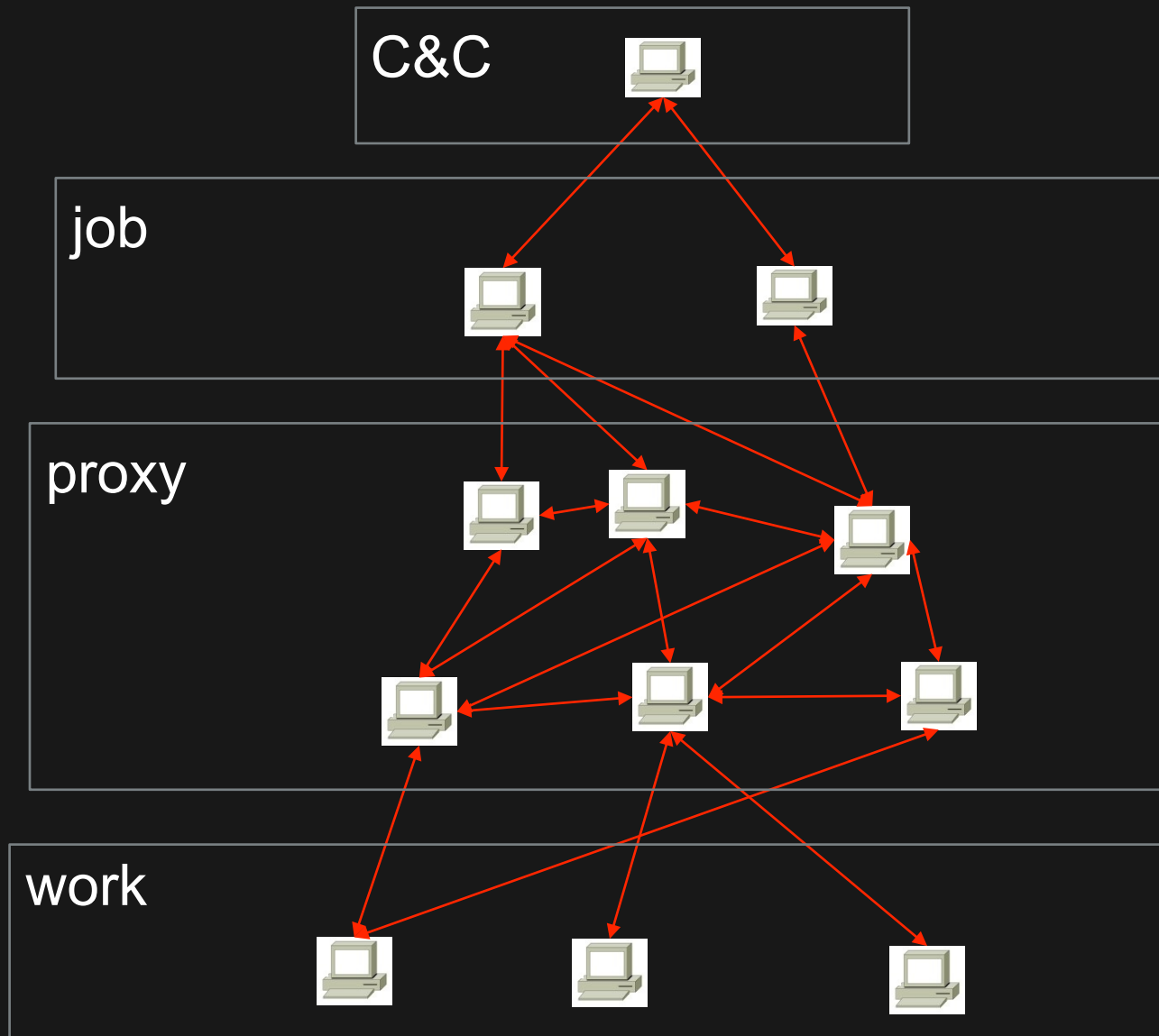
Protocol , Encryption, Evolution

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing and talking, while others are shaking hands. The background of the banner is a dark red with a subtle geometric pattern.

Kelihos – Overview

- P2P Spam Botnet
- FTP,SMTP Sniffer
- Local FTP Stealer
- Email addr harvest
- Ddos
- BitCoin Stealer & Mining

Kelihos – Overview





Agenda

1	Kelihos Botnet Overview
2	Protocol , Encryption, Evolution

Kelihos – First Sample

```
30.12.2010 10:05:50 Client 0.0.47 started.
30.12.2010 10:05:50 [vol]Looking for old client...
30.12.2010 10:05:50 Looking for old client...
30.12.2010 10:05:50 Timing zone[find_and_kill_old_clients] ms=641
30.12.2010 10:05:50 Autorun entry writed success.
30.12.2010 10:05:50 Config loaded Ok. own_id=1fd5851e-8acc-42ad-be1f-9061c45baa7
3, port = 80
30.12.2010 10:05:50 Loaded bootstrap list:
client: 00000000-0000-0000-0000-000000000000 77.123.65.4:80
client: 00000000-0000-0000-0000-000000000000 178.37.83.13:80
client: 00000000-0000-0000-0000-000000000000 110.5.78.16:80
client: 00000000-0000-0000-0000-000000000000 212.55.120.21:80
client: 00000000-0000-0000-0000-000000000000 178.137.9.31:80
client: 00000000-0000-0000-0000-000000000000 124.125.27.46:80
client: 00000000-0000-0000-0000-000000000000 95.168.185.46:80
client: 00000000-0000-0000-0000-000000000000 77.123.49.53:80
client: 00000000-0000-0000-0000-000000000000 94.27.74.70:80
client: 00000000-0000-0000-0000-000000000000 92.115.187.103:80
client: 00000000-0000-0000-0000-000000000000 178.151.74.120:80
client: 00000000-0000-0000-0000-000000000000 89.252.19.125:80
client: 00000000-0000-0000-0000-000000000000 78.84.42.129:80
client: 00000000-0000-0000-0000-000000000000 213.231.27.148:80
client: 00000000-0000-0000-0000-000000000000 85.204.167.163:80
client: 00000000-0000-0000-0000-000000000000 178.160.64.165:80
```

/loggs99

Kelihos – Working Mechanism

```
11.01.2011 15:32:37 Client 0.0.51 started.
11.01.2011 15:32:37 [vo]Looing for old client...
11.01.2011 15:32:37 Looing for old client...
11.01.2011 15:32:37 Timing zone[find_and_kill_old_clients] ms=187
11.01.2011 15:32:37 Autorun entry writed success.
11.01.2011 15:32:37 Config loaded Ok. own_id=d3cf38a9-ee7d-4b7b-9b16-c9cfdd62f430, port = 80
11.01.2011 15:32:37 Loaded bootstrap list:
client: 00000000-0000-0000-0000-000000000000 189.1.58.7:80
client: 00000000-0000-0000-0000-000000000000 189.41.165.14:80

11.01.2011 15:32:37 Starting in non-router mode...
11.01.2011 15:32:37 Starting anmp+http net server
11.01.2011 15:32:37 [MAIN]'Lets talk' started!
11.01.2011 15:32:37 [MAIN]Starting handshake loop, routers = 20...
11.01.2011 15:32:47 [MAIN]Failed to connect to client: 00000000-0000-0000-0000-000000000000, 183.96.171.63:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.m0.s
11.01.2011 15:33:19 [MAIN][hand_shake]:connected OK client: 00000000-0000-0000-0000-000000000000, 188.187.20.159:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.
11.01.2011 15:33:20 [MAIN][hand_shake]: remote bootstrap:

cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:31:57 live_tm: d0.h1.m19.s14
3a95dcab-4da7-48a9-a3e8-16e4b2be8bbb, 82.5.71.32:80 lst_act=11.01.2011 15:31:17 live_tm: d0.h0.m16.s13

11.01.2011 15:33:20 [MAIN][merge]bootstrap list merged, local_time=11.01.2011 15:33:20, remote_time=11.01.2011 15:32:17delta=63
11.01.2011 15:33:20 [MAIN]External info updated: 0 -->> 1294511242
11.01.2011 15:33:20 [MAIN][hand_shake]: merged bootstrap:

0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.s51
cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:33:00 live_tm: d0.h1.m19.s14

11.01.2011 15:33:20 [MAIN]Starting handshake loop finished. success=1, trys=5
11.01.2011 15:33:20 [MAIN][requesting job]Entering job request loop(servers=53)....
11.01.2011 15:33:20 [MAIN][requesting job]Connecting to 0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.
11.01.2011 15:33:20 [MAIN][requesting job]Invoking to 188.187.20.159:80
11.01.2011 15:33:23 [MAIN]STARTING MAILING THREADS [30]
11.01.2011 15:33:23 [MAIN]Adding mailing worker thread

11.01.2011 15:33:23 DoSend: [2] villers@houston.rr.com ERR
11.01.2011 15:33:23 [MAIN][requesting job]Success on 188.187.20.159:80
11.01.2011 15:33:23 [MAIN][requesting job] Job request loop finished. try_count=1, success=1
11.01.2011 15:33:33 DoSend: [2] doug@lipmantpa.com OK
11.01.2011 15:33:35 DoSend: [2] yukon@sprint.ca ERR
```

Kelihos – Working Mechanism

```
11.01.2011 15:32:37 Client 0.0.51 started.
11.01.2011 15:32:37 [vo]Looing for old client...
11.01.2011 15:32:37 Looing for old client...
11.01.2011 15:32:37 Timing zone[find_and_kill_old_clients] ms=187
11.01.2011 15:32:37 Autorun entry writed success.
11.01.2011 15:32:37 Config loaded Ok. own_id=d3cf38a9-ee7d-4b7b-9b16-c9cfdd62f430, port = 80
11.01.2011 15:32:37 Loaded bootstrap list:
client: 00000000-0000-0000-0000-000000000000 189.1.58.7:80
client: 00000000-0000-0000-0000-000000000000 189.41.165.14:80
```

```
11.01.2011 15:32:37 Starting in non-router mode...
11.01.2011 15:32:37 Starting anmp+http net server
11.01.2011 15:32:37 [MAIN]'Lets talk' started!
11.01.2011 15:32:37 [MAIN]Starting handshake loop, routers = 20...
11.01.2011 15:32:47 [MAIN]Failed to connect to client: 00000000-0000-0000-0000-000000000000, 183.96.171.63:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.m0.s
11.01.2011 15:33:19 [MAIN][hand_shake]:connected OK client: 00000000-0000-0000-0000-000000000000, 188.187.20.159:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.
11.01.2011 15:33:20 [MAIN][hand_shake]: remote bootstrap:
```

```
cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:31:57 live_tm: d0.h1.m19.s14
3a95dcab-4da7-48a9-a3e8-16e4b2be8bbb, 82.5.71.32:80 lst_act=11.01.2011 15:31:17 live_tm: d0.h0.m16.s13
```

```
11.01.2011 15:33:20 [MAIN][merge]bootstrap list merged, local_time=11.01.2011 15:33:20, remote_time=11.01.2011 15:32:17delta=63
11.01.2011 15:33:20 [MAIN]External info updated: 0 -->> 1294511242
11.01.2011 15:33:20 [MAIN][hand_shake]: merged bootstrap:
```

```
0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.s51
cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:33:00 live_tm: d0.h1.m19.s14
```

```
11.01.2011 15:33:20 [MAIN]Starting handshake loop finished. success=1, trys=5
11.01.2011 15:33:20 [MAIN][requesting job]Entering job request loop(servers=53)....
11.01.2011 15:33:20 [MAIN][requesting job]Connecting to 0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.
11.01.2011 15:33:20 [MAIN][requesting job]Invoking to 188.187.20.159:80
11.01.2011 15:33:23 [MAIN]STARTING MAILING THREADS [30]
11.01.2011 15:33:23 [MAIN]Adding mailing worker thread
```

```
11.01.2011 15:33:23 DoSend: [2] villers@houston.rr.com ERR
11.01.2011 15:33:23 [MAIN][requesting job]Success on 188.187.20.159:80
11.01.2011 15:33:23 [MAIN][requesting job] Job request loop finished. try_count=1, success=1
11.01.2011 15:33:33 DoSend: [2] doug@lipmantpa.com OK
11.01.2011 15:33:35 DoSend: [2] yukon@sprint.ca ERR
```


Kelihos – Working Mechanism

```
11.01.2011 15:32:37 Client 0.0.51 started.
11.01.2011 15:32:37 [vo]Looing for old client...
11.01.2011 15:32:37 Looing for old client...
11.01.2011 15:32:37 Timing zone[find_and_kill_old_clients] ms=187
11.01.2011 15:32:37 Autorun entry writed success.
11.01.2011 15:32:37 Config loaded Ok. own_id=d3cf38a9-ee7d-4b7b-9b16-c9cfdd62f430, port = 80
11.01.2011 15:32:37 Loaded bootstrap list:
client: 00000000-0000-0000-0000-000000000000 189.1.58.7:80
client: 00000000-0000-0000-0000-000000000000 189.41.165.14:80

11.01.2011 15:32:37 Starting in non-router mode...
11.01.2011 15:32:37 Starting anmp+http net server
11.01.2011 15:32:37 [MAIN]'Lets talk' started!
11.01.2011 15:32:37 [MAIN]Starting handshake loop, routers = 20...
11.01.2011 15:32:47 [MAIN]Failed to connect to client: 00000000-0000-0000-0000-000000000000, 183.96.171.63:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.m0.s
11.01.2011 15:33:19 [MAIN][hand_shake]:connected OK client: 00000000-0000-0000-0000-000000000000, 188.187.20.159:80 lst_act=31.12.1969 17:00:00 live_tm: d0.h0.s
11.01.2011 15:33:20 [MAIN][hand_shake]: remote bootstrap:

cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:31:57 live_tm: d0.h1.m19.s14
3a95dcab-4da7-48a9-a3e8-16e4b2be8bbb, 82.5.71.32:80 lst_act=11.01.2011 15:31:17 live_tm: d0.h0.m16.s13

11.01.2011 15:33:20 [MAIN][merge]bootstrap list merged, local_time=11.01.2011 15:33:20, remote_time=11.01.2011 15:32:17delta=63
11.01.2011 15:33:20 [MAIN]External info updated: 0 -->> 1294511242
11.01.2011 15:33:20 [MAIN][hand_shake]: merged bootstrap:

0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.s51
cf2489e8-55d3-40ba-bed6-722121303a38, 72.28.36.121:80 lst_act=11.01.2011 15:33:00 live_tm: d0.h1.m19.s14

11.01.2011 15:33:20 [MAIN]Starting handshake loop finished. success=1, trys=5
11.01.2011 15:33:20 [MAIN][requesting job]Entering job request loop(servers=53)....
11.01.2011 15:33:20 [MAIN][requesting job]Connecting to 0b6ebc3e-cb56-4207-aae6-d859d3498e48, 188.187.20.159:80 lst_act=11.01.2011 15:33:20 live_tm: d0.h11.m8.s
11.01.2011 15:33:20 [MAIN][requesting job]Invoking to 188.187.20.159:80
11.01.2011 15:33:23 [MAIN]STARTING MAILING THREADS [30]
11.01.2011 15:33:23 [MAIN]Adding mailing worker thread

11.01.2011 15:33:23 DoSend: [2] villers@houston.rr.com ERR
11.01.2011 15:33:23 [MAIN][requesting job]Success on 188.187.20.159:80
11.01.2011 15:33:23 [MAIN][requesting job] Job request loop finished. try_count=1, success=1
11.01.2011 15:33:33 DoSend: [2] doug@lipmantpa.com OK
11.01.2011 15:33:35 DoSend: [2] yukon@sprint.ca ERR
```

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a laptop. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

1st Generation Kelihos Get Proxy List Stage
Request

Get Proxy List(Gen1, Original Send Data)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
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	00	00	00	.è.....
0020h:	00	06	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.Yßà5
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	4C	22	57	3D	B3	D9	D4	E6	97	20	4A	F4	5F	E2	¼çL"W=³ÙÔæ- Jô â
0070h:	B5	D3	B4	3D	1A	67	BD	26	72	1B	F1	E4	31	94	48	50	µÓ´=.g¼&r.ñäl"HP
0080h:	16	34	D4	F8	02	BB	21	A2	96	18	84	EE	EC	C8	60	B9	.4Ôø.»!ç-„îiÈ`¹
0090h:	20	F5	25	A1	E7	C5	4A	84	01	1E	2A	20	8E	78	68	F9	õ%;çÅJ„.* Žxhù
00A0h:	A5	26	CE	6B	03	01	B6	B7	CD	14	2D	20	F4	06	08	F9	¥&îk..¶·í.- ô..ù
00B0h:	88	EC	27	4D	40	05	CA	FE	18	C2	A7	8C	6A	A4	8F	9D	^ì'M@.Êp.ÂŒejª..
00C0h:	51	30	51	77	60	A5	35	FE	18	96	FD	A5	2B	39	70	D1	Q0Qw`¥5p.-ý¥+9pÑ
00D0h:	ED	E4	34	04	96	93	78	0E	1E	F3	63	0D	32	68	82	BE	íä4.-"x..óc.2h,¼
00E0h:	12	36	6F	C2	56	F8	DF	F4	B7	84	C3	18	4F	4B	11	D2	.6oÂVøßô„.Ã.OK.ò
00F0h:	30	D3	83	14	BB	BF	8B	58	34	9B	83	C4	E7	FB	A1	DB	0Óf.»¿<X4>fÃçû;Û
0100h:	9C	3B	95	3C	B9	18	C9	E0	9D	B8	40	F7	BA	45	ED	B2	œ;•<¹.Éà.,@÷°Eí²
0110h:	26	61	3F	2B	0C	34	9B	12	E7	C4	75	92	7A	0B	09	B7	&a?+.4>.çÄu'z...·
0120h:	00	D7	A1	97	EC	7E	B4	00	07	0D	95	41	FF	E1	6A	AB	.x;-ì~´...•Aýáj«
0130h:	BF	4F	5D	E8	E2	F9	23	F8	14	5E	D1	23	12	50	E7	C9	¿O]èâù#ø.^Ñ#.PçÉ
0140h:	81	32	FA	6E	D8	BC	90	28	B9	A5	FA	AA	03	45	64	84	.2únø¼.(¹¥úª.Ed,,

Get Proxy List(Gen1, Send DS)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF			
0000h:	01	02	01	01	01	Header						0	00	00	00	00	00	`.....		
0010h:	01	E8	03	00	00							0	00	00	00	00	00	.è.....		
0020h:	00	06	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+.-öl))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	Nm.i.-ñ8ym1..rz,			
0060h:	BC	A2	4C	22	57	3D	B3	D9	D4	E6	97	20	4A	F4	5F	E2	4çL"W=³Ûôæ- Jô_â			
0070h:	B5	D3	B4	3D	1A	67	BD	26	72	1B	F1	E4	31	94	48	50	uÓ'=.g½&r.ñãl"HP			
0080h:	16	34	D4	F8	02	BB	21	A2	96	18	84	EE	EC	C8	60	B9	.4Ôø.!»!ç-..îiÈ`¹			
0090h:	20	F5	25	A1	Encrypted Data										8E	78	68	F9	õ%;çÅJ,..* Žxhù	
00A0h:	A5	26	CE	6B											F4	06	08	F9	¥&îk..¶.í.- ô..ù	
00B0h:	88	EC	27	4D											6A	A4	8F	9D	î'M@.Êp.ÂsEjµ..	
00C0h:	51	30	51	77											2B	39	70	D1	Q0Qw`¥5p.-ý¥+9pÑ	
00D0h:	ED	E4	34	04												32	68	82	BE	íä4.-"x..óc.2h,¾
00E0h:	12	36	6F	C2	56	F8	DF	F4	B7	84	C3	18		4F	4B	11	D2	.6oÂVøBô·,,Ã.OK.Ò		
00F0h:	30	D3	83	14	BB	BF	8B	58	34	9B	83	C4	E7	FB	A1	DB	0Óf.»¿<X4>fÄçû;Û			
0100h:	9C	3B	95	3C	B9	18	C9	E0	9D	B8	40	F7	BA	45	ED	B2	æ;.<¹.Éà.¿@÷°Eí²			
0110h:	26	61	3F	2B	0C	34	9B	12	E7	C4	75	92	7A	0B	09	B7	&a?+.4>.çÄu'z...·			
0120h:	00	D7	A1	97	EC	7E	B4	00	07	0D	95	41	FF	E1	6A	AB	.x;-i~´...·Ayáj«			
0130h:	BF	4F	5D	E8	E2	F9	23	F8	14	5E	D1	23	12	50	E7	C9	¿O]èâù#ø.^Ñ#.PçÉ			
0140h:	81	32	FA	6E	D8	BC	90	28	B9	A5	FA	AA	03	45	64	84	.2únø¾.(¹¥úª.Edµ			

Get Proxy List(Gen1, Send Data DS)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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	00	00	00	.è...															
0020h:	06	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+.-ôl))ô.N@&.															
0040h:	4D	01	60	6F	2D	13	3A	A7	06	F8	ED	09	59	DF	E0	35	M.io=.:\$.øí.Yßà5															
0050h:	BC	A2	4C	22	57	3D	B3	D9	79	99	6C	0E	06	72	7A	82	Ñ™.i.-ñ8y™l..rz,															
0060h:	BC	A2	4C	22	57	3D	B3	D9	D4	E6	97	20	4A	F4	5F	E2	¼çL"W=³ÙÔæ- Jô_â															
0070h:	B5	D3	B4	3D	1A	67	BD	26	72	1B	F1	E4	31	94	48	50	µó´=.g¼&r.ñäl"HP															
0080h:	16	34	D4	F8	02	BB	21	A2	96	18	84	EE	EC	C8	60	B9	.4Ôø.»!ç-„îiÈ`-															
0090h:	20	F5	25	A1	E7	C5	4A	84	01	1E	2A	20	8E	78	68	F9	õ%;çÅJ„..* Žxhù															
00A0h:	A5	26	CE	6B	03	01	B6	B7	CD	14	2D	20	F4	06	08	F9	¥&îk..¶.Í.- ô..ù															
00B0h:	88	EC	27	4D	40	05	CA	FE	18	C2	A7	8C	6A	A4	8F	9D	^i'M@.Êp.Â\$çej¤..															
00C0h:	51	30	51	77									2B	39	70	D1	Q0Qw`¥5p.-ý¥+9pÑ															
00D0h:	ED	E4	34	04									32	68	82	BE	íä4.-"x..óc.2h,¾															
00E0h:	12	36	6F	C2									4F	4B	11	D2	.6oÂVøßô„.Ã.OK.Ò															
00F0h:	30	D3	83	14									E7	FB	A1	DB	0Óf.»ç<X4>fÃçû;Û															
0100h:	9C	3B	95	3C									BA	45	ED	B2	æ;•<¹.Éà..@÷°Eí²															
0110h:	26	61	3F	2B	0C	34	9B	12	E7	C4	75	92	7A	0B	09	B7	&a?+.4>.çÄu'z..															
0120h:	00	D7	A1	97	EC	7E	B4	00	07	0D	95	41	FF	E1	6A	AB	.×;-î~´...•Aÿáj«															
0130h:	BF	4F	5D	E8	E2	F9	23	F8	14	5E	D1	23	12	50	E7	C9	çO]èâù#ø.ˆÑ#.PçÉ															
0140h:	81	32	FA	6E	D8	BC	90	28	B9	A5	FA	AA	03	45	64	84	.2únø¼. (¹ýúª.Ed.															



Get Proxy List(Gen1,Encryption Algorithm)

Compressed

Blowfish

Get Proxy List(Gen1, Send Data Clear Text)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	20	6D	5F	62	6F	6F	¢IMóÙ.Ÿ^.. m_bo
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	BD	01	3A	07	6D	5F	6C	61	m_ip....½::m_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.
0090h:	00	00	6D	5F	6C	69	76	65	5F	74	69	6D	65	00	02	01	..m_live_time...
00A0h:	20	00	00	00	00	00	00	00	00	01	14	6D	5F	63	6C	69	m_cli
00B0h:	65	6E	74	5F	69	64	00	02	01	40	00	00	00	00	00	00	ent_id...@.....
00C0h:	00	00	00	00	00	00	00	00	00	00	6D	5F	69	70	00	02	m_ip..
00D0h:	01	10	BD	29	A5	0E	6D	5F	6C	61	73	74	5F	61	63	74	..½)¥.m_last_act
00E0h:	69	76	65	5F	74	69	6D	65	00	02	01	20	00	00	00	00	ive_time...
00F0h:	00	00	00	00	6D	5F	6C	69	73	74	65	6E	69	6E	67	5F	m_listening
0100h:	70	6F	72	74	00	02	01	10	50	00	00	00	6D	5F	6C	69	port....P...m_li
0110h:	76	65	5F	74	69	6D	65	00	02	01	20	00	00	00	00	00	ve_time...
0120h:	00	00	00	01	14	6D	5F	63	6C	69	65	6E	74	5F	69	64	m_client_id
0130h:	00	02	01	40	00	00	00	00	00	00	00	00	00	00	00	00	...@.....
0140h:	00	00	00	00	6D	5F	69	70	00	02	01	10	4E	98	B4	21	m_ip....N~`!

Get Proxy List(Gen1, Clear DS)

Get Proxy List(Gen1, Clear DS)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F									
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	20	6D	5F	62	6F	6F	IM6U.Y^.	m	boo																						
0010h:	74	73	74	72	61	70	5F	6C	69	73	74	00	01	04	6D	5F	t	s	r	a	p	_	l	i	s	t	...	m													
0020h:	63	6C	69	65	6E	74	73	5F	6C	69	73	74	00	03	50	01	c	l	i	e	n	t	s	_	l	i	s	t	...	P	.										
0030h:	14	6D	5F	63	6C	69	65	6E	74	5F	69	64	00	02	01	40	.	m	_	c	l	i	e	n	t	_	i	d	...	@											
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	BD	01	3A	07	6D	5F	6C	61	m	i	p	...	%	:	.	m	_	l	a														
0060h:	73	74	5F	61	63	74	69	76	65	5F	74	69	6D	65	00	02	s	t	_	a	c	t	i	v	e	_	t	i	m	e	...										
0070h:	01	20	00	00	00	00	00	00	00	00	6D	5F	6C	69	73	74	.																								
0080h:	65	6E	69	6E									01	10	50	00	.																								
0090h:	00	00	6D	5F									65	00	02	01	..	m	_	l	i	v	e	_	t	i	m	e	...												
00A0h:	20	00	00	00									5F	63	6C	69																									
00B0h:	65	6E	74	5F									00	00	00	00	e	n	t	_	i	d	...	@																	
00C0h:	00	00	00	00									69	70	00	02																									
00D0h:	01	10	BD	29									5F	61	63	74	..	%	:	.	m	_	l	a	s	t	_	a	c	t	i	v	e	_	t	i	m	e	...		
00E0h:	69	76	65	5F	74	69	6D	65	00	02	01	20	00	00	00	00	...																								
00F0h:	00	00	00	00	6D	5F	6C	69	73	74	65	6E	69	6E	67	5F		m	_	l	i	s	t	e	n	i	n	g	_												
0100h:	70	6F	72	74	00	02	01	10	50	00	00	00	6D	5F	6C	69	p	o	r	t	...	P	...	m	_	l	i	v	e	_	t	i	m	e	...						
0110h:	76	65	5F	74	69	6D	65	00	02	01	20	00	00	00	00	00	...																								
0120h:	00	00	00	01	14	6D	5F	63	6C	69	65	6E	74	5F	69	64		m	_	c	l	i	e	n	t	_	i	d													
0130h:	00	02	01	40	00	00	00	00	00	00	00	00	00	00	00	00		@																							
0140h:	00	00	00	00	6D	5F	69	70	00	02	01	10	4E	98	B4	21		m	_	i	p	...	N	~	!																

Get Proxy List(Serialized)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	01	20	6D	5F	62	6F	6F	74	73	74	72	61	70	5F	6C	69	. m_bootstrap_li
0010h:	73	74	00	01	04	6D	5F	63	6C	69	65	6E	74	73	5F	6C	st...m_clients_l
0020h:	69	73	74	00	03	50	01	14	6D	5F	63	6C	69	65	6E	74	ist..P..m_client
0030h:	5F	69	64	00	02	01	40	00	00	00	00	00	00	00	00	00	_id...@.....
0040h:	00	00	00	00	00	00	00	6D	5F	69	70	00	02	01	10	BD	m_ip....
0050h:	01	3A	07	6D	5F	6C	61	73	74	5F	61	63	74	69	76	65	..m_last_active
0060h:	5F	74	69	6D	65	00	02	01	20	00	00	00	00	00	00	00	_time... ..
0070h:	00	6D	5F	6C	69	73	74	65	6E	69	6E	67	5F	70	6F	72	.m_listening_por
0080h:	74	00	02	01	10	50	00	00	00	6D	5F	6C	69	76	65	5F	t....P...m_live
0090h:	74	69	6D	65	00	02	01	20	00	00	00	00	00	00	00	00	time... ..
00A0h:	01	14	6D	5F	63	6C	69	65	6E	74	5F	69	64	00	02	01	..m_client_id...
00B0h:	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	@.....
00C0h:	00	6D	5F	69	70	00	02	01	10	BD	29	A5	0E	6D	5F	6C	.m_ip....)¥.m_l
00D0h:	61	73	74	5F	61	63	74	69	76	65	5F	74	69	6D	65	00	ast_active_time.
00E0h:	02	01	20	00	00	00	00	00	00	00	00	6D	5F	6C	69	73	m_lis
00F0h:	74	65	6E	69	6E	67	5F	70	6F	72	74	00	02	01	10	50	tening_port....P
0100h:	00	00	00	6D	5F	6C	69	76	65	5F	74	69	6D	65	00	02	...m_live_time..
0110h:	01	20	00	00	00	00	00	00	00	00	01	14	6D	5F	63	6C	. ..m_cl
0120h:	69	65	6E	74	5F	69	64	00	02	01	40	00	00	00	00	00	ient_id...@.....
0130h:	00	00	00	00	00	00	00	00	00	00	00	6D	5F	69	70	00	m_ip.
0140h:	02	01	10	4E	98	B4	21	6D	5F	6C	61	73	74	5F	61	63	...N~'!m last ac

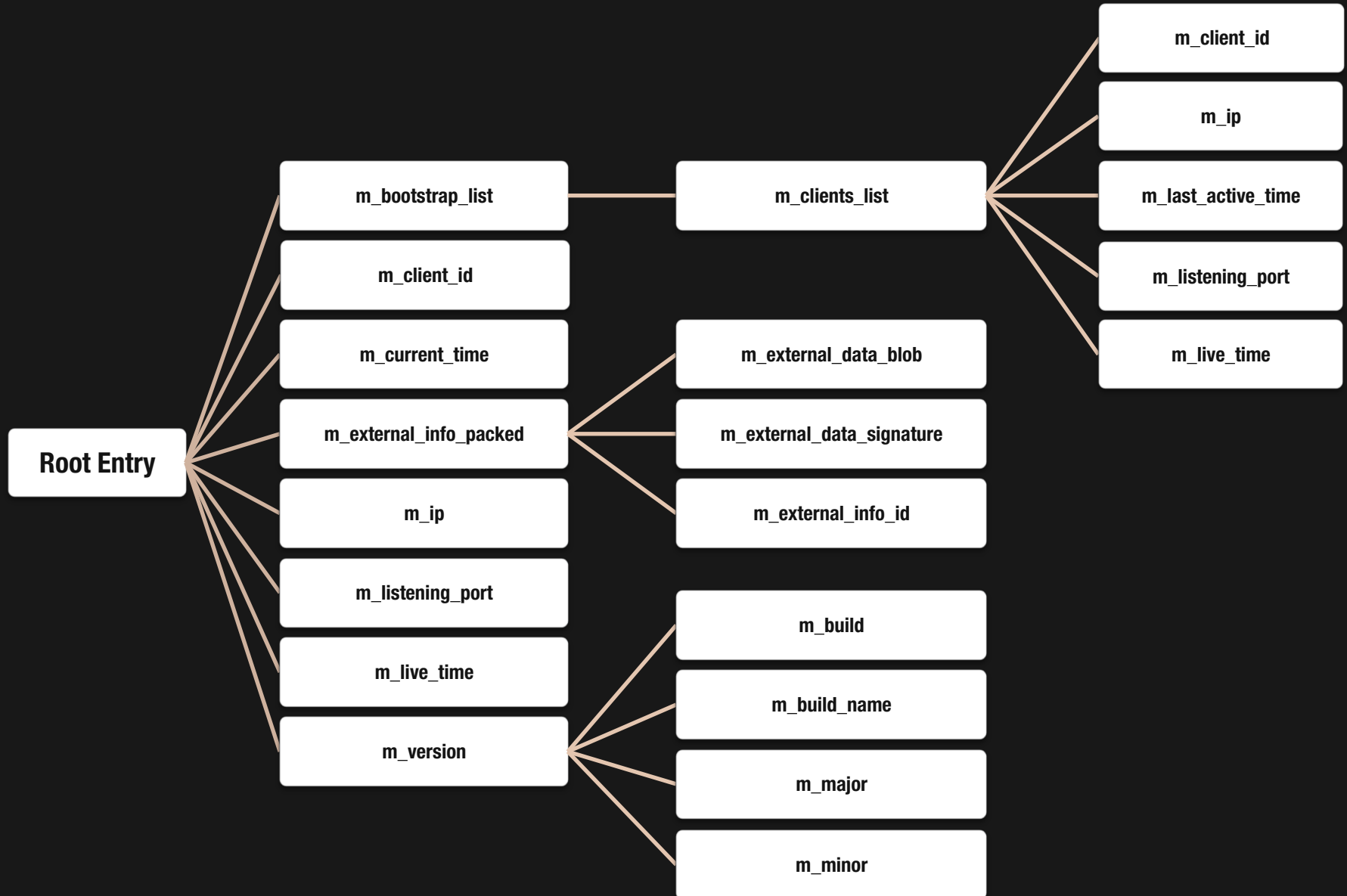
Get Proxy List(#define)

- 4 Entry Types
 - 01 Section
 - 02 Value
 - 03 Section Array
 - 04 Value Array
- 2 Value Types
 - 01 Hex Value
 - 02 ANSI String
- Raw Size Length = Size Low Byte & 0x03
 - 00 Byte
 - 01 Word
 - 02 Dword
 - 03 Qword
- Raw Size = Read Size >> 2

Get Proxy List(Serialization Examples)

- Root Entry 01 20
- m_bootstrap_list 01 04
 - 01 -> Section
 - 04 -> Content Count, 1
- m_clients_list 03 50 01 14
 - 03 ->Section Array
 - 50 -> Section Count, 20 Sections with same structure
 - 01 -> Section
 - 14 -> Content Count, 5
- m_client_id 02 01 40
 - 02 -> Value
 - 01 -> Hex
 - 40 -> Length,
- m_ip 02 01 10
 - 02 -> Value
 - 01 -> Hex
 - 10 -> Length

Get Proxy List(Send Data, DS)



A horizontal banner at the top of the slide features a red background with black silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a briefcase, suggesting a corporate or professional setting.

Protocol , Encryption, Evolution

1st Generation Kelihos Get Proxy List Stage
Response

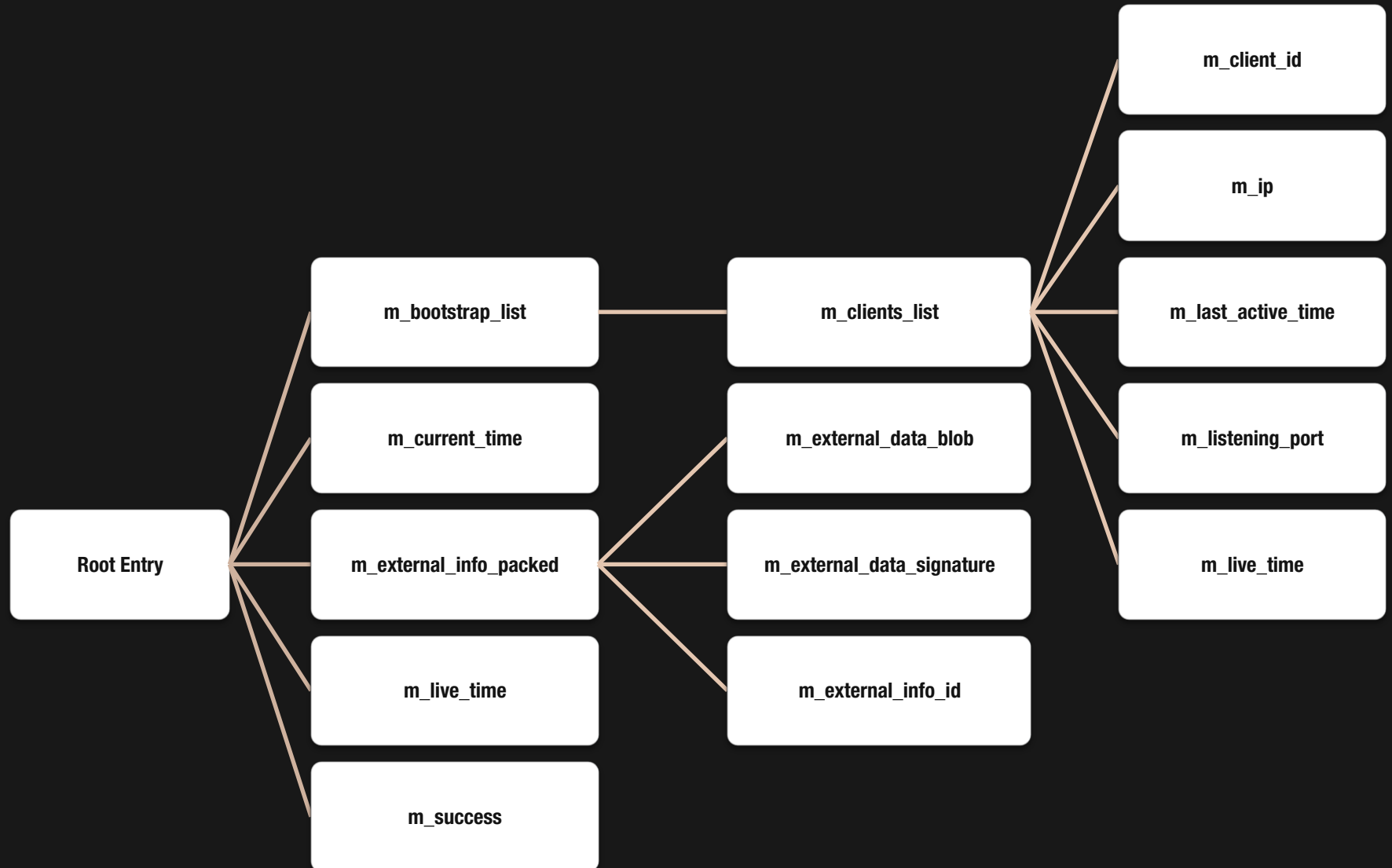
Get Proxy List(Gen1, Original Recv Data)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	01	02	01	01	01	01	02	01	71	1F	00	00	00	00	00	00	q.....															
0010h:	00	E8	03	00	00	01	00	00	00	00	00	00	00	00	00	00	.è.....															
0020h:	00	06	40	75	D2	6F	85	64	75	5A	69	80	6C	38	0F	FE	..@uðo...duzi€l8.b															
0030h:	CE	C1	91	04	95	AD	82	B6	8A	25	CD	B3	AE	FB	3E	9A	íÁ\'.•-,qš%í'©û>š															
0040h:	09	DD	E9	94	C1	55	08	1B	E3	73	E6	F0	4E	47	B7	F5	.Ýé"ÁU..ãæÖNG·ð															
0050h:	29	A8	B0	DA	46	8E	92	0E	A7	E9	1E	15	19	87	F1	FC	)""ÚFŽ'.sé...+ñü															
0060h:	5B	87	91	B3	6A	A5	54	C9	09	1C	F3	4F	02	91	FF	21	[+'s'j¥TÉ..óO.'ý!															
0070h:	02	85	14	38	06	19	C9	EB	A3	B7	3C	A6	5F	5E	35	C4	8..Éëf< ^5Ä															
0080h:	F6	87	16	73	DE	30	51	81	26	F5	C4	F7	CE	BC	73	7B	ö±.sþ0Q.&ðÄ÷î¼s{															
0090h:	DD	FE	30	42	E1	87	32	E7	22	9B	E4	22	D3	1B	1C	DD	ýþ0Bá+2ç">ä"Ó..Ý															
00A0h:	3A	01	39	EA	9E	50	58	40	6A	40	A8	CF	4A	F7	81	3F	:.9êžPX@j@"îJ÷.?															
00B0h:	86	F9	0F	10	2B	D9	DD	B4	AA	BB	A3	DC	29	F2	C9	43	†ù..+ÜÝ'ª»fÜ)ðÉC															
00C0h:	37	8E	0C	E9	12	DC	81	D1	B8	AE	25	D9	4C	8B	CA	43	7Ž.é.Ü.Ň,®%ÜL<ÊC															
00D0h:	BE	CE	01	33	AE	52	5C	50	BE	F1	B2	82	10	9B	8E	E0	¾î.3@R\p¾ñ²,.>žà															
00E0h:	15	52	DC	B8	DC	6C	7C	50	C6	73	38	13	76	95	46	66	.RŮ,Ůl PÆs8.v•Ff															
00F0h:	11	93	60	BF	47	A8	8F	32	77	1C	36	D9	EF	94	45	E9	."`¿G".2w.6Ûi"Eé															
0100h:	08	35	70	84	F7	24	17	43	7A	0F	87	BA	02	52	40	A8	.5p„÷\$.Cz.+°R@															
0110h:	B6	0E	63	56	B5	79	D7	11	F1	33	1D	8F	61	E4	A0	86	¶.cVpy×.ñ3..aä†															
0120h:	AB	56	DA	D6	E3	55	CF	A4	97	A1	CE	F9	EB	15	91	3E	«VÚÖäUîª-;îùë.'>															
0130h:	A7	FD	19	13	FF	F9	14	2D	0D	45	82	7B	ED	02	30	B1	šý..ÿù.-.E,{í.0±															
0140h:	C9	97	94	CE	27	94	17	AB	95	EA	DD	55	AA	B1	50	17	É-"î'".«•êýUª±P.															

Get Proxy List(Gen1, Recv Clear Text)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	14	6D	5F	62	6F	6F	çIMóÛ.Ÿ^...m_bo
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	E9	03	clients_list..é.
0030h:	01	14	6D	5F	63	6C	69	65	6E	74	5F	69	64	00	02	01	..m_client_id...
0040h:	40	5B	22	A2	BD	A5	46	44	77	AF	2C	E8	9F	92	D1	CB	@["ç½¥FDw~,èŸ'ÑË
0050h:	12	6D	5F	69	70	00	02	01	10	62	8C	79	00	6D	5F	6C	.m_ip....bEy.m_l
0060h:	61	73	74	5F	61	63	74	69	76	65	5F	74	69	6D	65	00	ast_active_time.
0070h:	02	01	20	A0	D8	2C	4D	00	00	00	00	6D	5F	6C	69	73	.. Ø,M....m_lis
0080h:	74	65	6E	69	6E	67	5F	70	6F	72	74	00	02	01	10	50	tening_port....P
0090h:	00	00	00	6D	5F	6C	69	76	65	5F	74	69	6D	65	00	02	...m_live_time..
00A0h:	01	20	0E	03	00	00	00	00	00	00	01	14	6D	5F	63	6C	m_cl
00B0h:	69	65	6E	74	5F	69	64	00	02	01	40	49	33	E3	24	34	ient_id...@I3ã\$4
00C0h:	8B	45	6B	B6	89	EF	B5	FF	17	25	10	6D	5F	69	70	00	<Ek¶%ipŸ.%m_ip.
00D0h:	02	01	10	62	E8	54	01	6D	5F	6C	61	73	74	5F	61	63	...bèT.m_last_ac
00E0h:	74	69	76	65	5F	74	69	6D	65	00	02	01	20	17	D8	2C	tive_time... .Ø,
00F0h:	4D	00	00	00	00	6D	5F	6C	69	73	74	65	6E	69	6E	67	M....m_listening
0100h:	5F	70	6F	72	74	00	02	01	10	50	00	00	00	6D	5F	6C	_port....P...m_l
0110h:	69	76	65	5F	74	69	6D	65	00	02	01	20	A6	00	00	00	ive_time... ...
0120h:	00	00	00	00	01	14	6D	5F	63	6C	69	65	6E	74	5F	69	m_client_i
0130h:	64	00	02	01	40	A2	92	4B	26	69	43	47	DC	91	74	B5	d...@ç'K&iCGÜ'tp
0140h:	3B	C4	80	AC	59	6D	5F	69	70	00	02	01	10	6D	A2	2D	;Ä€-Ym ip....mç-

Get Proxy List(Gen1,Recv Data, DS)



Get Proxy List(Gen1, Job Servers)

7780h:	63	6B	65	64	00	01	0C	6D	5F	65	78	74	65	72	6E	61	cked...m_externa
7790h:	6C	5F	64	61	74	61	5F	62	6C	6F	62	00	02	02	F1	01	l_data_blob...ñ.
77A0h:	A2	49	4D	F3	D9	1E	9F	88	01	01	08	6D	5F	6A	6F	62	çIMóÛ.Ÿ^...m_job
77B0h:	5F	73	65	72	76	65	72	73	00	03	08	01	08	6D	5F	69	_servers.....m_i
77C0h:	70	00	02	01	10	5B	C8	F0	22	6D	5F	6C	69	73	74	65	p....[Èø"m_liste
77D0h:	6E	69	6E	67	5F	70	6F	72	74	00	02	01	10	50	00	00	ning_port....P..
77E0h:	00	01	08	6D	5F	69	70	00	02	01	10	5B	C8	F0	24	6D	...m_ip....[Èø\$m
77F0h:	5F	6C	69	73	74	65	6E	69	6E	67	5F	70	6F	72	74	00	_listening_port.
7800h:	02	01	10	50	00	00	00	6D	5F	6C	69	73	74	5F	69	64	...P...m_list id
7810h:	00	02	01	20	8A	AC	28	4D	00	00	00	00	6D	5F	65	78	... Š¬(M....m_ex

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a briefcase. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

1st Generation Kelihos Job Stage
Request

A background image showing the silhouettes of several business professionals in a meeting or office setting. The scene is dimly lit, with a warm, reddish-brown color palette. The silhouettes are dark against the lighter background, creating a professional and collaborative atmosphere. The text 'Request Job (Original Send Data)' is overlaid in white, bold font on the left side of the image.

Request Job (Original Send Data)

[illegible]

A background image showing the silhouettes of several business professionals in a meeting or office setting. The scene is dimly lit with a warm, reddish-brown color palette. In the foreground, a man in a suit stands with his back to the camera, looking towards a group of people. To his right, another man in a suit is seen from the side, holding a briefcase. In the background, several other individuals are engaged in conversation or looking at documents. The overall atmosphere is professional and collaborative.

Request Job (Original Send Data)

Header Signature

Encrypted Data Length

Stage Signature

Encrypted Data

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	01	02	01	01	01	01	02	01	21	01	00	00	00	00	00	00			!														
0010h:	01	EA	03	00	00	01	00	00	00	63	49	00	00	B1	26	00		.ê...		CI..±&.													
0020h:	0F	24	81	99	B6	9F	04		29	33	23	FA	CF	F0	66	25		..\$.mqÿ.)	3#úíðf%														
0030h:	0B	30	68	DC	BC	48	09	39	70	5D	E9	FF	D8	15	A3	C9		.0hÛ¼H.9p]éýø.fÉ															
0040h:	12	50	65	14	F1	87	77	3B	9A	77	C5	CC	7B	82	4A	8D		.ée.ñ±w;šwÅÌ{,J.															
0050h:									27	AD	61	E3	38	BE	4F	6F		œ%.ÂR7P...'-aã8¾Oo															
0060h:	1D	BD	26	5D	44	0E	B9	45	6D	4A	FC	9E	59	24	AB	10		.¼&]D.¹EmJüžYŞ«.															
0070h:	EF	4B	A0	42	3A	01	DC	2B	CD	FA	4B	53	A9	38	A8	5F		îK B:..Û+ÍúKS@8"															
0080h:	44	9F	AE	D3	2D	68	59	76	81	12	6D	89	E4	D1	FF	03		Dÿ@Ó-hYv..m%ãÑÿ.															
0090h:	54	95	D6	3D	34	36	7A	79	78	80	1B	45	B3	F3	DA	E6		T·Ö=46zyx€E.³óÚæ															
00A0h:	7E	A8	CF	61	9D	96	7C	B0	94	1F	C4	21	2E	E7	5C	4B		~"İa.- °".Ä!.ç¼K															
00B0h:	F9	52	C4	6B	2C	72	B5	59	C0	AA	DF	1C	FE	3B	41	00		ùRÄk,ruYÄªß.p;A.															
00C0h:	0C	0E	9A	93										EC	81	9B	B5		..š"Í#qaßfoEì.¾														
00D0h:	36	96	7F	A1										2E	CF	4F	6F		6-.;&ÕÑZm óR.İOo														
00E0h:	4B	91	6B	FD										29	E2	3A	AD		K'kýÿ.ñçý.î.)â:-														
00F0h:	4B	00	78	2C										85	2C	D3	B4		K.x,f pV¯eÒ¹...,Ó'														
0100h:	31	8D	DF	B6										77	94	30	1B		1.ßÿ,,³°×ù«¾cw"0.														
0110h:	FD	5A	66	07	93	B8	9D	2D	19	FD	5D	45	6B	0A	BF	3D		ýZf.",.-.ý]Ek.¿=															
0120h:	24	EF	C6	36	C3	48	3E	85	2B	14	89	C8	D8	56	FA	56		\$iÆ6ÄH>...+.¾ÈØVúV															
0130h:	92	3F	CF	09	28	DB	4E	B6	74	FC	D1	BF	C9	84	88	07		'?İ.(ÜNÿtuÑ¿É,,^.															
0140h:	F7	A6																	+														

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits, some standing and some in motion, against a dark red background.

Request Job (Encryption Algorithm)

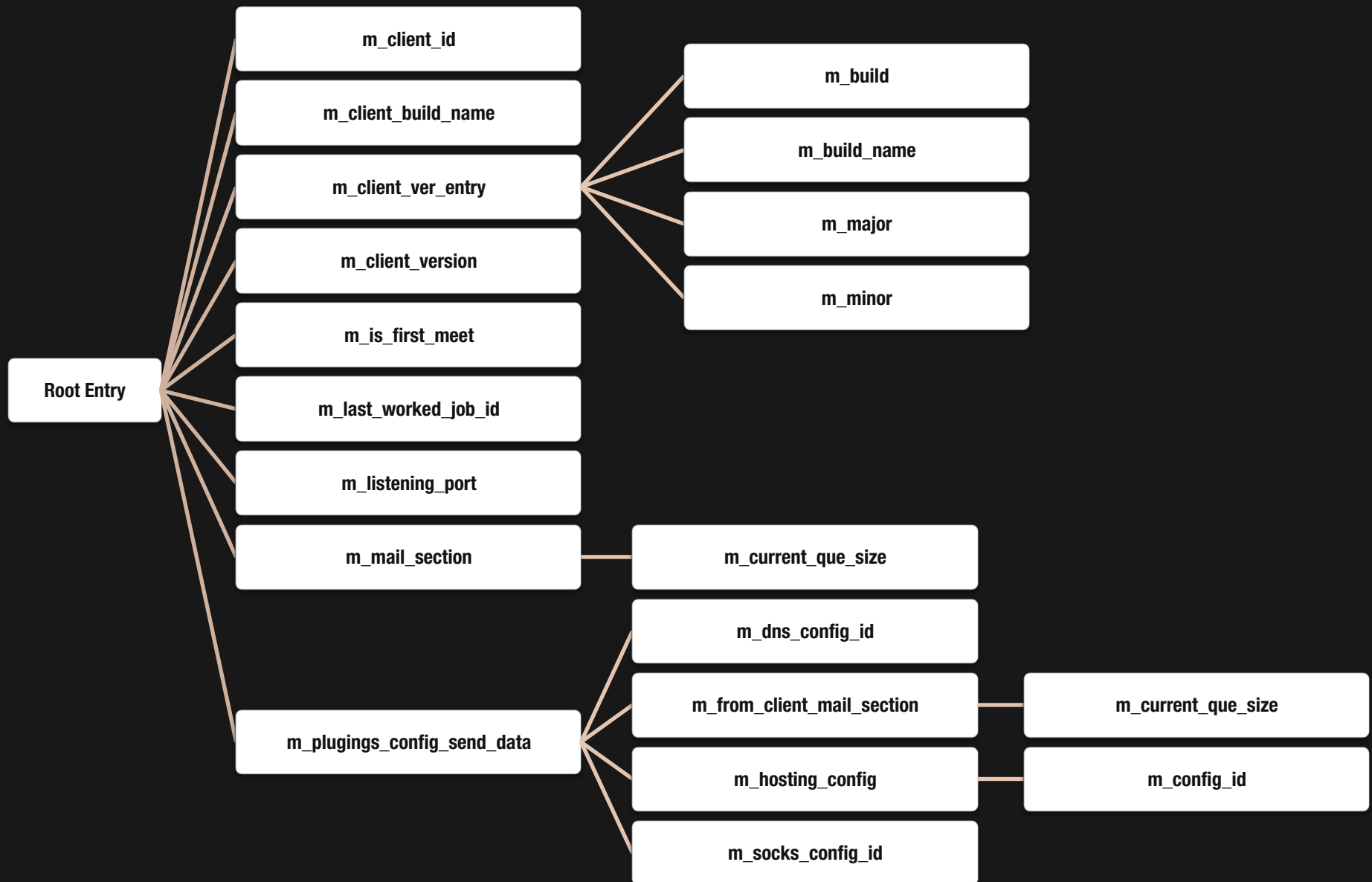
Compressed

Blowfish

Request Job (Send Data,Clear Text)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	24	63	6C	69	65	6E	01	M	ó	Ů	.Ÿ	^	.	.	\$	clien						
0010h:	74	5F	69	64	00	02	01	40	D3	CF	38	A9	EE	7D	4B	7B	t	_id...	@	Ó	I	8	@	i	}K{							
0020h:	9B	16	C9	CF	DD	62	F4	30	6D	5F	63	6C	69	65	6E	74	>	.É	Ÿ	b	ô	0	m	_client								
0030h:	5F	62	75	69	6C	64	5F	6E	61	6D	65	00	02	02	10	74	_	build_name....t														
0040h:	65	73	74	6D	5F	63	6C	69	65	6E	74	5F	76	65	72	5F	estm_client_ver															
0050h:	65	6E	74	72	79	00	01	10	6D	5F	62	75	69	6C	64	00	entry...m_build.															
0060h:	02	01	10	33	00	00	00	6D	5F	62	75	69	6C	64	5F	6E	...3...m_build_n															
0070h:	61	6D	65	00	02	02	00	6D	5F	6D	61	6A	6F	72	00	02	ame....m_major..															
0080h:	01	10	00	00	00	00	6D	5F	6D	69	6E	6F	72	00	02	01	m_minor...															
0090h:	10	00	00	00	00	6D	5F	63	6C	69	65	6E	74	5F	76	65	m_client_ve															
00A0h:	72	73	69	6F	6E	00	02	02	18	30	2E	30	2E	35	31	6D	rsion....0.0.51m															
00B0h:	5F	69	73	5F	66	69	72	73	74	5F	6D	65	65	74	00	02	_is_first_meet..															
00C0h:	01	04	01	6D	5F	6C	61	73	74	5F	77	6F	72	6B	65	64	...m_last_worked															
00D0h:	5F	6A	6F	62	5F	69	64	00	02	01	20	00	00	00	00	00	_job_id... ..															
00E0h:	00	00	00	6D	5F	6C	69	73	74	65	6E	6E	69	6E	67	5F	...m_listenning_															
00F0h:	70	6F	72	74	00	02	01	10	00	00	00	00	6D	5F	6D	61	port.....m_ma															
0100h:	69	6C	5F	73	65	63	74	69	6F	6E	00	01	04	6D	5F	63	il_section...m_c															
0110h:	75	72	72	65	6E	74	5F	71	75	65	5F	73	69	7A	65	00	urrent_que_size.															
0120h:	02	01	10	B8	F2	12	00	6D	5F	70	6C	75	67	69	6E	73	...,ò...m_plugins															
0130h:	5F	63	6F	6E	66	69	67	73	5F	73	65	6E	64	5F	64	61	_configs_send_da															
0140h:	74	61	00	01	10	6D	5F	64	6E	73	5F	63	6F	6E	66	69	ta...m_dns confi															

Request Job(Send Data Clear Text)



A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a briefcase. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

1st Generation Kelihos Job Stage
Response

Request Job(Recv Data)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	01	02	01	01	01	01	02	01	F1	7E	00	00	00	00	00	00	ñ~.....															
0010h:	01	00	00	00	00	01	00	00	00	6A	E0	E0	42	EE	E6	90	j`ààBîæ.															
0020h:	69	06	3A	86	1F	E6	2E	97	7F	A1	75	6B	BB	F5	87	9C	i.:†.æ.-.;uk»õ+œ															
0030h:	D8	61	4F	2C	3D	AB	CC	0A	05	91	3C	E0	0B	F6	B2	CD	øaO,=«î.. ' < à . õ² í															
0040h:	6A	6A	4D	7D	7F	A9	45	C0	C9	08	C0	EE	E6	13	8A	A5	j}M}.©EÀÉ.Àîæ.Š¥															
0050h:	60	A0	38	91	92	82	4D	F5	F3	B8	40	BC	89	CE	7C	B1	` 8 '' ,Móó, @¼%î ±															
0060h:	B7	9F	41	EE	CE	2A	44	18	F9	58	00	9D	9A	DE	57	A4	·ŸAîî*D.ùX..šPWα															
0070h:	06	DD	4C	E7	D5	EE	C0	3C	ED	37	30	68	5B	9C	AF	DF	.ÝLçÕîÀ<í70h[œ¯B															
0080h:	15	07	80	F9	2B	18	2A	B6	0D	2B	DC	36	B3	89	32	E0	..èù+. *¶. +Ü6³%2à															
0090h:	AA	77	CD	27	59	89	29	CE	C0	2C	CF	09	B0	35	9C	F4	ªwÍ'Y%) ÎÀ, î. °5œô															
00A0h:	4C	CE	BA	DA	A4	21	A0	9F	C8	C0	A2	60	04	1C	10	6A	Lî°Úα! ŸÈÀç`...j															
00B0h:	A2	44	C0	97	64	7B	70	DC	9E	80	9E	C8	9A	8A	45	41	¢DÀ-d{pŮž€žÈšŠEA															
00C0h:	16	F2	FE	FF	43	B5	52	55	33	89	FB	F7	93	73	9F	F2	.òpŸCµRU3%û÷"sŸò															
00D0h:	C3	C9	FD	4E	ED	68	78	68	7B	DB	DB	3C	A7	3A	15	73	ĂÉŸNíhxx{ŮŮ<š:.s															
00E0h:	18	9D	AB	F0	5C	36	E5	87	04	E0	27	DC	55	88	83	05	..«ð\6å+.à'ÜU^f.															
00F0h:	50	3C	03	5B	36	F3	99	C7	8D	29	8C	5D	D0	A3	3A	7A	P<.[6ó™Ç.)€]Đ£:z															
0100h:	C6	1E	50	40	2B	B8	94	30	D6	AD	A5	6E	41	DD	B5	C6	Æ.P@+, "0Ö-ŸnAÝµÆ															
0110h:	53	3E	AF	DF	AE	7F	06	B7	6A	0F	50	B9	C0	86	FE	96	S>¯B@.. ·j. P¹À+þ-															
0120h:	C6	FC	8E	91	CC	E2	05	49	E9	92	36	23	AD	3E	F7	58	EuŽ'îâ. Ié' 6#->÷X															
0130h:	42	E9	AE	EF	2B	11	41	52	5C	A9	2C	82	B7	F0	EB	C8	Bé@i+.AR\@,, ·ðèÈ															
0140h:	4C	75	82	1A	00	55	FA	27	B9	51	18	16	DC	70	92	B7	Lu,..Uú'¹Q..Ůp'·															

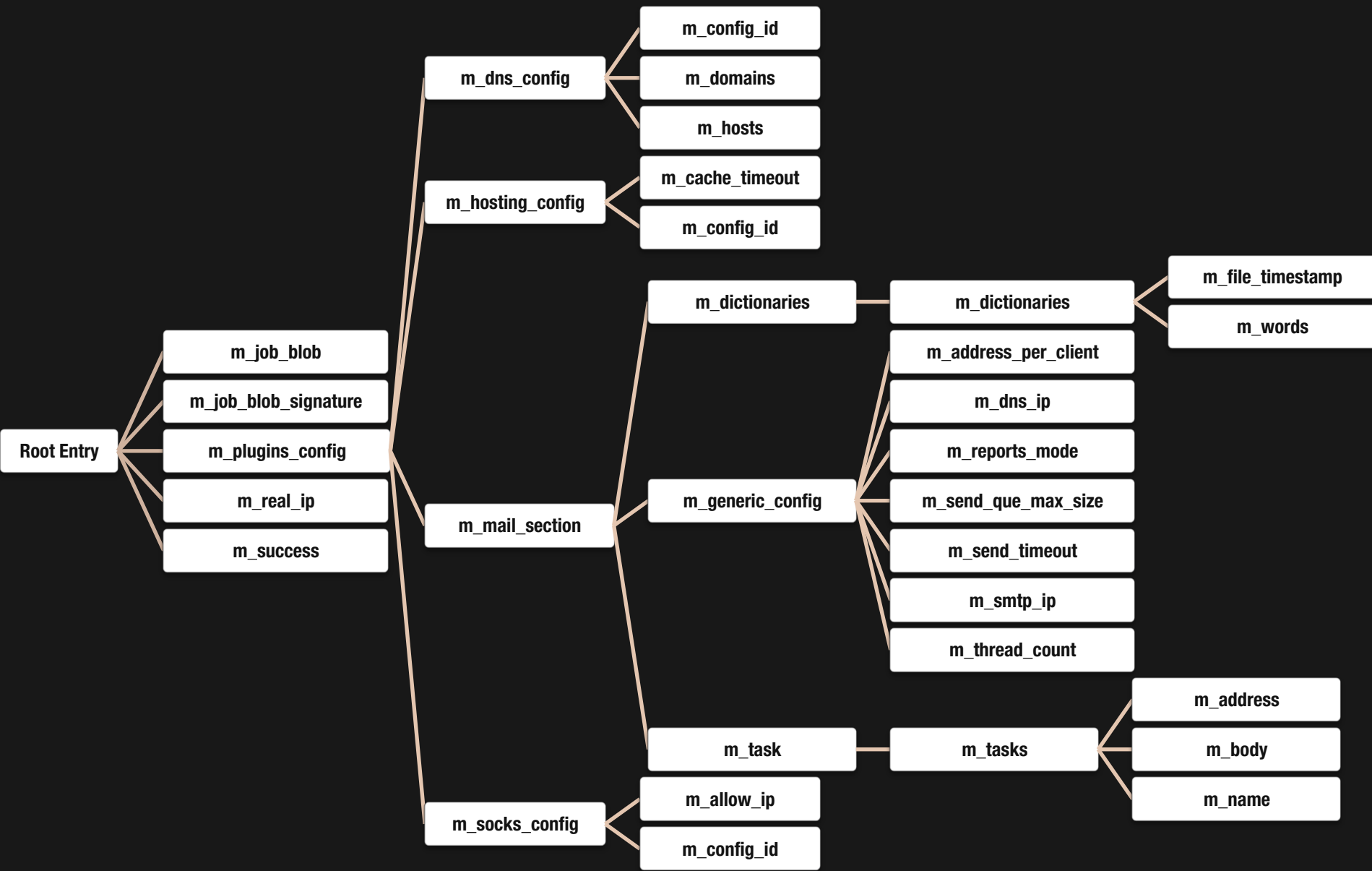
Request Job(Recv Clear Text)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	14	6D	5F	6A	6F	62	çIMóÛ.Ÿ^...m_job
0010h:	5F	62	6C	6F	62	00	02	02	00	6D	5F	6A	6F	62	5F	62	_blob....m_job_b
0020h:	6C	6F	62	5F	73	69	67	6E	61	74	75	72	65	00	02	02	lob_signature...
0030h:	00	6D	5F	70	6C	75	67	69	6E	73	5F	63	6F	6E	66	69	.m_plugins_config
0040h:	67	00	01	10	6D	5F	64	6E	73	5F	63	6F	6E	66	69	67	g...m_dns_config
0050h:	00	01	0C	6D	5F	63	6F	6E	66	69	67	5F	69	64	00	02	...m_config_id..
0060h:	01	20	4B	DA	2C	4D	00	00	00	00	6D	5F	64	6F	6D	61	. KÚ,M...m_doma
0070h:	69	6E	73	00	04	02	60	44	68	65	6C	6C	6F	68	65	6C	ins...`Dhellohel
0080h:	6C	6F	31	32	33	2E	63	6F	6D	30	62	69	74	61	67	65	lo123.com0bitage
0090h:	64	65	2E	63	6F	6D	2C	65	6C	62	65	72	65	72	2E	63	de.com,elberer.c
00A0h:	6F	6D	2C	6C	65	6F	6C	61	74	69	2E	63	6F	6D	30	6D	om,leolati.com0m
00B0h:	61	6B	6F	6E	69	63	75	2E	63	6F	6D	28	73	63	79	70	akonicu.com(scyp
00C0h:	61	70	2E	63	6F	6D	28	73	75	65	64	65	76	2E	63	6F	ap.com(suedev.co
00D0h:	6D	28	63	69	66	69	63	69	2E	63	6F	6D	28	64	61	72	m(cifici.com(dar
00E0h:	6C	65	76	2E	63	6F	6D	2C	65	6E	76	6F	79	65	65	2E	lev.com,envoyee.
00F0h:	63	6F	6D	30	6E	75	72	65	61	6C	6C	61	2E	63	6F	6D	com0nurealla.com
0100h:	2C	74	65	64	64	61	6D	70	2E	63	6F	6D	30	65	70	6C	,teddamp.com0epl
0110h:	61	72	69	6E	65	2E	63	6F	6D	2C	74	61	6D	61	72	65	arine.com,tamare
0120h:	72	2E	63	6F	6D	2C	69	6E	65	78	70	65	72	2E	63	6F	r.com,inexper.co
0130h:	6D	2C	61	6C	79	73	65	6B	6F	2E	63	6F	6D	28	66	65	m,alyseko.com(fe
0140h:	72	65	66	72	2E	63	6F	6D	2C	63	72	75	6E	6F	62	6C	refr.com,crunobl

Request Job(Recv Clear Text)

1:41F0h:	0A 52 65 63 65 69 76 65	64 3A 20 66 72 6F 6D 20	.Received: from
1:4200h:	25 5E 43 30 25 5E 50 25	5E 52 33 2D 36 5E 25 3A	%^C0%^P%^R3-6^%:
1:4210h:	71 77 65 72 74 79 75 69	6F 70 61 73 64 66 67 68	qwertyuiopasdfgh
1:4220h:	6A 6B 6C 7A 78 63 76 62	6E 6D 5E 25 5E 25 20 28	jklzxcvbnm%^%^ (
1:4230h:	5B 25 5E 43 36 25 5E 49	5E 25 2E 25 5E 49 5E 25	[%^C6%^I%^.%^I%^
1:4240h:	2E 25 5E 49 5E 25 2E 25	5E 49 5E 25 5E 25 5D 29	.%^I%^.%^I%^%)
1:4250h:	0A 09 62 79 20 25 5E 41	5E 25 20 25 5E 46 73 65	..by %^A%^ %^Fse
1:4260h:	6E 64 6D 61 69 6C 76 65	72 5E 25 20 77 69 74 68	ndmailver%^ with
1:4270h:	20 53 4D 54 50 20 69 64	20 25 5E 59 25 5E 43 35	SMTP id %^Y%^C5
1:4280h:	25 5E 52 32 30 2D 33 30	30 5E 25 5E 25 5E 25 30	%^R20-300%^%^%0
1:4290h:	33 37 30 33 36 3B 0A 09	25 5E 44 25 5E 56 35 5E	37036;..%^D%^V5^
1:42A0h:	25 5E 25 0A 4D 65 73 73	61 67 65 2D 49 44 3A 20	%^%.Message-ID:
1:42B0h:	3C 25 5E 4F 25 5E 56 36	5E 25 3A 25 5E 52 33 2D	<%^O%^V6^%:%^R3-
1:42C0h:	35 30 5E 25 5E 25 25 5E	56 30 5E 25 3E 0A 46 72	50%^%^%^V0^%>.Fr
1:42D0h:	6F 6D 3A 20 22 25 5E 43	34 25 5E 46 6D 79 6E 61	om: "%^C4%^Fmyna
1:42E0h:	6D 65 73 5E 25 5E 25 22	20 3C 25 5E 46 6E 61 6D	mes%^%^" <%^Fnam
1:42F0h:	65 73 5E 25 40 25 5E 46	64 6F 6D 61 69 6E 73 5E	es%^@%^Fdomains^
1:4300h:	25 3E 0A 54 6F 3A 20 3C	25 5E 30 5E 25 3E 0A 53	%>.To: <%^0^%>.S
1:4310h:	75 62 6A 65 63 74 3A 20	25 5E 46 70 68 61 72 6D	ubject: %^Fpharm
1:4320h:	61 5E 25 0A 44 61 74 65	3A 20 25 5E 44 2D 25 5E	a^%.Date: %^D-%^
1:4330h:	52 33 30 2D 36 30 30 5E	25 5E 25 0A 4D 49 4D 45	R30-600%^%^MIME
1:4340h:	2D 56 65 72 73 69 6F 6E	3A 20 31 2E 30 0A 43 6F	-Version: 1.0.Co
1:4350h:	6E 74 65 6E 74 2D 54 79	70 65 3A 20 74 65 78 74	ntent-Type: text
1:4360h:	2F 70 6C 61 69 6E 3B 0A	09 66 6F 72 6D 61 74 3D	/plain;..format=
1:4370h:	66 6C 6F 77 65 64 3B 0A	09 63 68 61 72 73 65 74	flowed;..charset
1:4380h:	3D 22 25 5E 46 63 68 61	72 73 65 74 5E 25 22 3B	="%^Fcharset%^";

Request Job (Recv Data, KeyWords)



A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a briefcase. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

1st Generation Kelihos Job Stage Report

Request Job(Report Clear Text)

0660h:	73 61 6B 69 40 63 61 6D	2E 68 69 2D 68 6F 2E 6E	saki@cam.hi-ho.n
0670h:	65 2E 6A 70 72 00 02 02	0C 45 52 52 74 00 02 02	e.jpr....ERRt...
0680h:	04 32 01 0C 61 00 02 02	34 6A 6C 65 40 72 65 66	.2..a...4jle@ref
0690h:	73 61 2E 63 6F 6D 72 00	02 02 0C 45 52 52 74 00	sa.comr....ERRt.
06A0h:	02 02 04 32 01 0C 61 00	02 02 78 63 68 72 69 73	...2..a...xchris
06B0h:	74 69 61 6E 2E 62 6F 6E	6E 61 75 64 40 6F 70 74	tian.bonnaud@opt
06C0h:	69 6D 69 74 65 6C 2E 66	72 72 00 02 02 0C 45 52	imitel.frr....ER
06D0h:	52 74 00 02 02 04 32 01	0C 61 00 02 02 40 6A 6F	Rt....2..a...@jo
06E0h:	40 63 61 6E 6E 61 72 64	2E 63 6F 2E 75 6B 72 00	@cannard.co.ukr.
06F0h:	02 02 08 4F 4B 74 00 02	02 04 32 01 0C 61 00 02	...OKt....2..a..
0700h:	02 54 6D 77 73 6E 5F 70	6F 73 74 73 40 6D 65 6E	.Tmwsn_posts@men
0710h:	74 6F 72 2E 63 6F 6D 72	00 02 02 08 4F 4B 74 00	tor.comr....OKt.
0720h:	02 02 04 32 01 0C 61 00	02 02 3C 76 2E 6B 74 6D	...2..a...<v.ktm
0730h:	2E 31 40 74 6E 74 2E 63	6F 6D 72 00 02 02 08 4F	.1@tnt.comr....O
0740h:	4B 74 00 02 02 04 32 01	0C 61 00 02 02 38 72 6B	Kt....2..a...8rk
0750h:	70 64 6A 73 40 61 6F 6C	2E 63 6F 6D 72 00 02 02	pdjs@aol.comr...
0760h:	08 4F 4B 74 00 02 02 04	32 01 0C 61 00 02 02 48	.OKt....2..a...H
0770h:	67 6F 72 64 69 65 6E 6B	6F 65 73 40 73 67 70 2E	gordienkoes@sgp.
0780h:	72 75 72 00 02 02 08 4F	4B 74 00 02 02 04 32 01	rur....OKt....2.
0790h:	0C 61 00 02 02 74 67 6F	74 74 65 40 73 70 6F 72	.a...tgotte@spor
07A0h:	74 2E 75 6E 69 2D 67 6F	65 74 74 69 6E 67 65 6E	t.uni-goettingen

Bot Update

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	14	6D	5F	6A	6F	62	¢IMóŮ.Ÿ^...m_job
0010h:	5F	62	6C	6F	62	00	02	02	45	03	A2	49	4D	F3	D9	1E	_blob...E.¢IMóŮ.
0020h:	9F	88	01	01	04	6D	5F	6A	6F	62	73	00	03	04	01	14	Ÿ^...m_jobs.....
0030h:	6D	5F	62	75	69	6C	64	5F	6C	65	73	73	5F	6F	72	5F	m_build_less_or_
0040h:	65	71	75	61	6C	5F	63	6F	6E	64	69	74	69	6F	6E	00	equal_condition.
0050h:	02	01	10	32	00	00	00	6D	5F	62	75	69	6C	64	5F	6D	...2...m_build_m
0060h:	6F	72	65	5F	6F	72	5F	65	71	75	61	6C	5F	63	6F	6E	ore_or_equal_con
0070h:	64	69	74	69	6F	6E	00	02	01	10	00	00	00	00	6D	5F	dition.....m_
0080h:	63	6F	6D	6D	61	6E	64	00	02	01	10	01	00	00	00	6D	command.....m
0090h:	5F	63	6F	6D	6D	61	6E	64	73	5F	70	61	72	61	6D	73	_commands_params
00A0h:	00	04	02	08	78	68	74	74	70	3A	2F	2F	62	69	74	61	xhttp://bita
00B0h:	67	65	64	65	2E	63	6F	6D	2F	66	6C	61	73	68	32	2E	gede.com/flash2.
00C0h:	65	78	65	4C	6D	31	75	68	75	6B	6F	75	76	33	7A	6E	exeLmluhukouv3zn
00D0h:	61	6F	69	2E	65	78	65	6D	5F	6A	6F	62	5F	69	64	00	aoi.exem job id.

New Module

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	14	6D	5F	6A	6F	62	¢IMóÛ.Ÿ^...m_job
0010h:	5F	62	6C	6F	62	00	02	02	41	03	A2	49	4D	F3	D9	1E	_blob...A.¢IMóÛ.
0020h:	9F	88	01	01	04	6D	5F	6A	6F	62	73	00	03	04	01	14	Ÿ^...m_jobs.....
0030h:	6D	5F	62	75	69	6C	64	5F	6C	65	73	73	5F	6F	72	5F	m_build_less_or_
0040h:	65	71	75	61	6C	5F	63	6F	6E	64	69	74	69	6F	6E	00	equal_condition.
0050h:	02	01	10	35	00	00	00	6D	5F	62	75	69	6C	64	5F	6D	...5...m_build_m
0060h:	6F	72	65	5F	6F	72	5F	65	71	75	61	6C	5F	63	6F	6E	ore_or_equal_con
0070h:	64	69	74	69	6F	6E	00	02	01	10	00	00	00	00	6D	5F	dition.....m_
0080h:	63	6F	6D	6D	61	6E	64	00	02	01	10	01	00	00	00	6D	command.....m
0090h:	5F	63	6F	6D	6D	61	6E	64	73	5F	70	61	72	61	6D	73	_commands_params
00A0h:	00	04	02	08	7C	68	74	74	70	3A	2F	2F	65	6C	62	65	 http://elbe
00B0h:	72	65	72	2E	63	6F	6D	2F	6B	62	38	34	35	33	32	35	rer.com/kb845325
00C0h:	2E	65	78	65	44	66	30	33	6A	75	35	6B	61	6A	67	36	.exeDf03ju5kajg6
00D0h:	64	34	2E	65	78	65	6D	5F	6A	6F	62	5F	69	64	00	02	d4.exem_job_id..

C:\FILES\denisov\sn01\Release\sniffer.pdb



Kelihos Gen1

- Header
- Encryption
- Key Words
- Job Servers
- Functions
- Dbg output

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a laptop. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

2nd Generation Kelihos

Get Proxy List(Request)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	5D	1D	ED	AB	00	00	00	00	A0	54	4D	3E	5B	5F	C5	D0	] . í « TM > [_ Å Đ
0010h:	9F	E5	A2	F3	00	00	00	00	11	02	00	00	00	00	00	00	Ÿ ǎ ç ó
0020h:	7B	54	06	3F	5B	5F	C5	D0	23	90	46	89	64	0E	0C	95	{ T . ? [_ Å Đ # . F % d . . .
0030h:	00	00	00	00	0F	C5	51	F3	F9	AC	3D	85	4E	FB	46	98	 Å Q ó ù - = . N û F ~
0040h:	AE	5D	E0	E7	59	36	C5	A7	D6	38	44	32	1D	8C	F6	E6	@] à ç Y 6 Å S Ö 8 D 2 . Œ ö æ
0050h:	C3	19	CF	60	44	08	E3	DE	87	AC	3D	22	7A	29	12	35	Å . ĭ ` D . ǎ B + - = " z) . 5
0060h:	11	93	43	13	66	18	45	22	2A	B7	65	91	4A	F2	84	11	. " C . f . E " * . e ` J ò „ .
0070h:	B5	CB	BD	14	08	23	37	43	DB	04	4C	BB	C0	3B	94	E5	µ Ê ½ . . # 7 C Û . L » À ; " ǎ
0080h:	01	B4	FD	DB	5C	B1	85	D6	C2	A4	64	18	58	7C	AC	CC	. ' ý Û \ ± ... Ö Â = d . X - İ
0090h:	10	17	D7	DB	8B	A9	65	21	DA	E6	2A	A0	A5	2D	81	57	.. x Û < @ e ! Ú æ * ¥ - . W
00A0h:	2B	AB	EE	5D	DA	C1	0A	96	96	4F	21	A8	66	74	89	2E	+ « î] Ú Á . -- O ! " f t % .
00B0h:	05	7F	56	E1	BE	9F	F5	43	83	C5	5F	38	F2	DC	E6	9A	.. V á ¾ Ÿ ö C f Å _ 8 ò Ü æ š
00C0h:	0A	F1	79	61	F0	07	71	BE	DB	B4	62	64	42	BE	6E	C2	. ñ y a ö . q ¾ Û ' b d B ¾ n Â
00D0h:	E1	D8	57	35	83	14	A1	F9	C5	87	1D	8D	3A	98	1D	08	á ø W 5 f . ; ù Å + . . : ~ . .
00E0h:	C1	57	9F	3E	49	00	2D	3F	B1	7B	16	41	AA	66	4F	B4	Á W Ÿ > I . - ? ± { . A ^ f o '
00F0h:	D3	7E	F0	92	3A	9B	71	1D	E5	5A	06	EC	64	3D	D4	B8	Ó ~ ð ' : > q . ǎ Z . ì d = ô ,
0100h:	E0	AF	93	D3	EF	12	13	B8	65	B8	F8	BB	65	1D	FC	12	à " Ó ĭ . . , e , ø » e . ü .
0110h:	C6	F8	F2	5F	EE	1C	33	9C	F6	29	6B	B8	AF	81	B9	62	Æ ø ò _ ĭ . 3 æ ö) k , " . ¹ b
0120h:	29	91	51	FA	1D	CB	C0	A6	11	98	11	1A	1F	D5	98	C8	) ' Q ú . È À ! . ~ . . . Ö ~ È
0130h:	28	7A	13	30	92	13	A5	3B	0E	B7	E5	09	18	89	FA	A3	(z . 0 ' . ¥ ; . . ǎ . . % ú f
0140h:	74	7E	06	A3	B6	9B	FA	5D	05	7D	D5	4B	47	2F	BE	70	t ~ . f ¶] ú] . } Ö K G / ¾ p

Get Proxy List(Request)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000h:	5D	1D	ED	AB	00	00	00	00	A0	54	4D	3E	5B	5F	C5	D0	] .í«		TM	>	[	Å	Đ										
0010h:	9F	E5	A2	F3	00	00	00	00	11	02	00	00	00	00	00	00	Ÿ	â	ó														
0020h:	7B	54	06	3F	5B	5F	C5	D0	23	90	46	89	64	0E	0C	95	{	T	.	?	[	Å	Đ	#	.	F	%	d	..	*			
0030h:	00	00	00	00	0F	C5	51	F3	F9	AC	3D	85	4E	FB	46	98		Å	Q	ó	ù	-	=	..	N	û	F	~					
0040h:	AE	5D	E0	E7	59	36	C5	A7	D6	38	44	32	1D	8C	F6	E6	@	]	à	ç	Y	6	Å	S	Ö	8	D	2	.	œ	æ		
0050h:	C3	19	CF	60	44	08	E3	DE	87	AC	3D	22	7A	29	12	35	Ä	.	ï	'	D	.	ä	þ	+	-	=	"	z	)	.	5	
0060h:	11	93	43	13	66	18	45	22	2A								.	"	C	.	f	.	E	"	*	.	e	'	J	ò	..		
0070h:	B5	CB	BD	14	08	23	37	43	DB	04	4C	BB	C0	3B	94	E5	µ	Ê	¾	..	#	7	C	Û	.	L	»	À	;	"	â		
0080h:	01	B4	FD	DB	5C	B1	85	D6	C2	A4	64	18	58	7C	AC	CC	.	'	ý	Û	\	±	...	Ö	Å	=	d	.	X		-	ï	
0090h:	10	17	D7	DB	8B	A9	65	21	DA	E6	2A	A0	A5	2D	81	57	..	×	Û	<	@	e	!	Ú	æ	*	¥	-	.	W			
00A0h:	2B	AB	EE	5D	DA	C1	0A	96	96	4F	21	A8	66	74	89	2E	+	<	î	]	Ú	Á	..	-	-	o	!	"	f	t	%	.	
00B0h:	05	7F	56	E1	BE	9F	F5	43	83	C5	5F	38	F2	DC	E6	9A	..	V	á	¾	ÿ	Ö	C	f	Å	_	8	ò	Ü	æ	š		
00C0h:	0A	F1	79	61	F0	07	71	DE	DE	B4	62	64	42	BE	6E	C2	.	ñ	y	ä	ö	.	q	¾	Û	'	b	D	¾	n	Â		
00D0h:	E1	D8	57	35	83												á	Ø	W	5	f	.	;	ù	Å	+	...	~	..				
00E0h:	C1	57	9F	3E	49												Á	W	ÿ	>	I	..	-	?	+	{	.	A	°	f	O	'	
00F0h:	D3	7E	F0	92	3A												ó	~	ø	'	:	>	q	.	å	Z	.	ì	d	=	Ô	,	
0100h:	E0	AF	93	D3	EF												à	"	Ó	í	..	.	e	,	ø	»	e	.	ü	.			
0110h:	C6	F8	F2	5F	EE												Æ	ø	ò	_	î	.	3	æ	ö	)	k	.	..	¹	b		
0120h:	29	91	51	FA	1D	CB	C0	A6	11	98	11	1A	1F	D5	98	C8	)	'	Q	ú	.	È	À	!	.	~	...	Ö	~	È			
0130h:	28	7A	13	30	92	13	A5	3B	0E	B7	E5	09	18	89	FA	A3	(	z	.	0	'	.	¥	;	.	â	..	%	ú	f			
0140h:	74	7E	06	A3	B6	9B	FA	5D	05	7D	D5	4B	47	2F	BE	70	t	~	.	f	¶	>	ú	]	.	}	Ö	K	G	/	¾	p	

Get Proxy List(Request)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	5D	1D	ED	AB	00	00	00	00	A0	54	4D	3E	5B	5F	C5	D0	] .í«....					TM>[ÅĐ										
0010h:	9F	E5	A2	F3	00	00	00	00	11	02	00	00	00	00	00	00	Ÿâçó.....															
0020h:	7B	54	06	3E	5B	5F	C5	D0	23	90	46	89	64	0E	0C	95	{T.¿[ÅĐ#.	F%&d... .														
0030h:	00	00	00	00	0F	C5	51	F3	F9	AC	3D	85	4E	FB	46	98		ÅQóù¬=..	NûF~													
0040h:	AE	5D	E0	E7	59	36	C5	A7	D6	38	44	32	1D	8C	F6	E6	@]	àçY6ÅŠÖ8D2.	Æöæ													
0050h:	C3	19	CF	60	44	08	E3	DE	87	AC	3D	22	7A	29	12	35	Ä.	İ`D.äP±¬=	"z).	5												
0060h:	11	93	43	13	66	18	45	22	2A	B7	65	91	4A	F2	84	11	.	"C.f.E"	*.e`Jò„.													
0070h:	B5	CB	BD	14	08	23	37	43	DB	04	4C	BB	C0	3B	94	E5	uÊ½..	#7Ĉ.L»À;	"â													
0080h:	01	B4	FD	DB	5C	B1	85	D6	C2	A4	64	18	58	7C	AC	CC	.	'ýŮ\±...ÖÂ¼	d.X ¬İ													
0090h:	10	17	D7	DB	8B	A9	65	21	DA	E6	2A	A0	A5	2D	81	57	..	×	Ů<@e!	Úæ*	¥-.	W										

add eax, 0B8FBF3h

$$0x3F06547B - 0x3E4D54A0 - 0xB8FBF3 = 0x3E8$$



Get Proxy List(Encryption Algorithm)

Compressed
Blowfish
Blowfish
Blowfish

Get Proxy List(Request Clear Text)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	24	32	37	62	61	38	¢IMóÛ.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..
0090h:	01	10	4D	00	00	00	38	34	30	61	31	37	35	35	30	31	..M...840a175501
00A0h:	61	66	35	63	30	30	00	02	01	20	05	00	00	00	00	00	af5c00... ..
00B0h:	00	00	61	38	36	66	35	30	32	30	32	37	31	65	30	30	..a86f5020271e00
00C0h:	30	30	00	02	01	20	28	DD	51	4D	00	00	00	00	63	32	00... (ÝQM....c2
00D0h:	34	31	64	31	61	37	32	65	61	63	65	63	30	30	00	02	41d1a72eacec00..
00E0h:	01	10	00	00	00	00	63	61	62	66	38	63	32	39	36	30	cabf8c2960
00F0h:	34	33	38	30	30	30	00	02	01	10	45	89	34	07	65	35	438000....E%4.e5
0100h:	66	35	36	32	30	65	61	30	64	36	31	34	30	30	00	01	f5620ea0d61400..
0110h:	04	64	66	61	35	38	34	39	61	38	37	35	64	33	30	30	.dfa5849a875d300
0120h:	30	00	03	50	01	14	32	37	62	61	38	38	34	66	37	30	0..P..27ba884f70
0130h:	37	39	66	34	34	30	00	02	01	10	45	89	34	07	38	34	79f440....E%4.84
0140h:	30	61	31	37	35	35	30	31	61	66	35	63	30	30	00	02	0a175501af5c00..

Get Proxy List(Hash Replaced)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	24	6D	5F	69	70	00	¢IMóŬ.Ÿ^..\$m_ip.
0010h:	02	01	10	00	00	00	00	6D	5F	76	65	72	73	69	6F	6E	m_version
0020h:	00	01	10	6D	5F	62	75	69	6C	64	5F	6E	61	6D	65	00	...m_build_name.
0030h:	02	02	10	74	65	73	74	6D	5F	6D	61	6A	6F	72	00	02	...testm_major..
0040h:	01	10	00	00	00	00	6D	5F	6D	69	6E	6F	72	00	02	01	m_minor...
0050h:	10	00	00	00	00	6D	5F	62	75	69	6C	64	00	02	01	10	m_build....
0060h:	4D	00	00	00	6D	5F	6C	69	76	65	5F	74	69	6D	65	00	M...m_live_time.
0070h:	02	01	20	05	00	00	00	00	00	00	00	6D	5F	63	75	72	m_cur
0080h:	72	65	6E	74	5F	74	69	6D	65	00	02	01	20	28	DD	51	rent_time... (ŸQ
0090h:	4D	00	00	00	00	6D	5F	6C	69	73	74	65	6E	6E	69	6E	M...m_listennin
00A0h:	67	5F	70	6F	72	74	00	02	01	10	00	00	00	00	6D	5F	g_port.....m_
00B0h:	72	65	61	6C	5F	74	61	72	67	65	74	5F	69	70	00	02	real_target_ip..
00C0h:	01	10	45	89	34	07	6D	5F	62	6F	6F	74	73	74	72	61	..E%4.m_bootstra
00D0h:	70	5F	6C	69	73	74	00	01	04	6D	5F	63	6C	69	65	6E	p_list...m_clien
00E0h:	74	73	5F	6C	69	73	74	00	03	50	01	14	6D	5F	69	70	ts_list..P..m_ip
00F0h:	00	02	01	10	45	89	34	07	6D	5F	6C	69	76	65	5F	74	E%4.m_live_t
0100h:	69	6D	65	00	02	01	20	00	00	00	00	00	00	00	00	6D	ime...m
0110h:	5F	6C	61	73	74	5F	61	63	74	69	76	65	5F	74	69	6D	_last_active_tim
0120h:	65	00	02	01	20	00	00	00	00	00	00	00	00	6D	5F	6C	e...m_l
0130h:	69	73	74	65	6E	69	6E	67	5F	70	6F	72	74	00	02	01	istening_port...
0140h:	10	50	00	00	00	6D	5F	63	6C	69	65	6E	74	5F	69	64	.P...m_client_id

Get Proxy List(Job Servers)

8C80h:	13	2D	E5	16	A9	4A	F5	37	36	32	65	65	31	31	38	34	.-å.©Jö762ee1184
8C90h:	64	34	37	39	37	30	30	00	02	02	51	04	A2	49	4D	F3	d479700...Q.çIMó
8CA0h:	D9	1E	9F	88	01	01	08	6D	5F	6A	6F	62	5F	73	65	72	Û.Ÿ^...m_job_ser
8CB0h:	76	65	72	73	00	03	18	01	08	6D	5F	69	70	00	02	01	vers.....m_ip...
8CC0h:	10	5B	C8	F0	22	6D	5F	6C	69	73	74	65	6E	69	6E	67	.[Èø"m_listening
8CD0h:	5F	70	6F	72	74	00	02	01	10	50	00	00	00	01	08	6D	_port....P.....m
8CE0h:	5F	69	70	00	02	01	10	5B	C8	F0	24	6D	5F	6C	69	73	_ip....[Èø\$m_lis
8CF0h:	74	65	6E	69	6E	67	5F	70	6F	72	74	00	02	01	10	50	tening_port....P
8D00h:	00	00	00	01	08	6D	5F	69	70	00	02	01	10	5E	3F	F6	m_ip....^?ö
8D10h:	E2	6D	5F	6C	69	73	74	65	6E	69	6E	67	5F	70	6F	72	âm_listening_por
8D20h:	74	00	02	01	10	50	00	00	00	01	08	6D	5F	69	70	00	t....P.....m_ip.
8D30h:	02	01	10	5E	3F	F6	E4	6D	5F	6C	69	73	74	65	6E	69	...^?öâm_listeni
8D40h:	6E	67	5F	70	6F	72	74	00	02	01	10	50	00	00	00	01	ng_port....P....
8D50h:	08	6D	5F	69	70	00	02	01	10	5F	40	09	28	6D	5F	6C	.m_ip....@(m_l
8D60h:	69	73	74	65	6E	69	6E	67	5F	70	6F	72	74	00	02	01	istening_port...
8D70h:	10	50	00	00	00	01	08	6D	5F	69	70	00	02	01	10	5F	.P.....m_ip...._
8D80h:	40	09	2A	6D	5F	6C	69	73	74	65	6E	69	6E	67	5F	70	@.*m_listening_p
8D90h:	6F	72	74	00	02	01	10	50	00	00	00	6D	5F	6C	69	73	ort....P...m_lis
8DA0h:	74	5F	69	64	00	02	01	20	05	95	4D	4D	00	00	00	00	t_id... .*MM....



Kelihos Gen2

- Header
- Encryption
- Key Words
- Job Servers
- Functions

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a laptop. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

3rd Generation Kelihos

Get Proxy List(Gen3, Original Send data)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	40	54	40	98	17	2E	1D	07	00	CB	CD	5B	F4	1C	F7	AA	@T@~.....ĖÍ[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	..Ăø.. Ű,WōwâIg·
0030h:	19	3C	CF	58	AA	6B	72	D0	EB	99	76	2F	9E	74	E0	8C	.<ĬXªkrĐē™v/žtàĖ
0040h:	93	5F	14	C4	DC	ED	EB	2E	09	59	72	89	D4	87	8E	68	"_..ĂŮíē..Yr%Ô+žh
0050h:	ED	32	E2	0F	27	9E	1A	03	DA	E5	A0	07	22	A5	97	BB	í2â.'ž...Ůå ."¥-»
0060h:	E1	AF	18	A5	41	E0	8F	A7	37	D1	2A	C6	C2	D7	AA	6E	á_.¥Aà.\$7Ň*ĖÂ×ªn
0070h:	BF	F2	B6	19	0A	A1	6E	9D	18	24	29	3F	0F	43	53	E2	¿òŦ..;n..\$)?.CSâ
0080h:	B8	34	B0	AB	02	07	FC	0A	B3	F9	74	6F	37	5A	98	B0	,4°«...ű.³ùto7Z~°
0090h:	30	2D	D3	E4	2B	13	10	F0	19	C6	47	53	AF	EA	3D	5A	0-Óä+..đ.ĖGS̄ê=Z
00A0h:	67	42	BC	98	4E	CE	41	42	7B	22	FF	7A	5C	E4	2A	11	gB¼~NîAB{"ýz\ä*.
00B0h:	55	EC	4C	15	65	28	D9	FF	F0	11	97	3C	B6	47	44	DF	UìL.e(Ůÿđ.-<ŦGDB
00C0h:	ED	BE	55	B2	65	E7	8D	F6	D0	5E	CA	A4	CD	C5	06	38	í¾U²eç.öđ^ĖªíĀ.8
00D0h:	48	05	D1	6C	51	23	60	71	2A	BF	AC	2B	9E	46	FE	36	H.ŇlQ#`q*¿-+žFp6
00E0h:	9A	C9	80	9E	CF	2E	0B	40	DB	8E	80	52	4C	E7	4C	A3	šĖēžĬ..@ŮžĖRLçLē
00F0h:	8C	5D	20	1E	DA	34	56	50	36	1A	9B	B9	15	07	4C	2A	Ė] .Ů4VP6.>¹..L*
0100h:	EA	8E	FB	79	9E	88	2A	24	B2	B6	2C	B4	70	51	9D	FB	êžûyž^*š²Ŧ,´pQ.û
0110h:	2E	71	08	30	0A	FD	77	AC	EC	A1	E5	EB	7B	3A	5F	C8	.q.0.ýw-ì;ăē{:Ė
0120h:	70	84	48	1E	BA	69	B2	66	8E	A1	68	C1	80	4A	5A	0A	p„H.°i²fž;hĀĖJZ.
0130h:	96	A1	5A	A9	FB	0C	30	27	53	DD	70	A0	CF	94	90	E0	-;Z@û.0'Sýp Ĭ".à
0140h:	97	A5	A4	78	75	B2	80	7E	36	BF	19	77	6D	88	AB	0C	-¥¤xu²Ė~6¿.wm^«.

A background image showing silhouettes of several business professionals in a meeting or office setting. The scene is dimly lit with a warm, reddish-brown color palette. In the center, two men are shaking hands. To the left, a group of people are standing and talking. To the right, a woman is walking towards the left, and another person is partially visible. The overall atmosphere is professional and collaborative.

Get Proxy List(Gen3)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	40	54	40	98	17	2E	1D	07	00	CB	CD	5B	F4	1C	F7	AA	@T@~.....Ėí[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	D3	2C	57	F0	77	E2	49	67	B7	..Äø.. Ű,WöwâIq;
0030h:	19	3C	CF	58	Encrypted Data 1								74	E0	8C	.<îXªkrðE¸v/žtâ@	
0040h:	93	5F	14	C4	DC	ED	EB	2E	09	59	72	89	D4	87	8E	68	"_..ÄŰîë..Yr%Ô+žh
0050h:	ED	32	E2	0F	27	9E	1A	03	DA	E5	A0	07	22	A5	97	BB	í2â.'ž..Űâ . "Ű»»
0060h:	E1	AF	18	A5	41	E0	8F	A7	37	D1	2A	C6	C2	D7	AA	6E	á-.ŰAà.š7Ň*EÄªªn
0070h:	BF	F2	B6	19	0A	A1	6E	9D	18	24	29	3F	0F	43	53	E2	žòŰ..;n..š)?.CSâ
0080h:	B8	34	B0	AB	02	07	FC	0A	B3	F9	74	6F	37	5A	98	B0	,4º«..Ű.ªűto7Zªº
0090h:	30	2D	D3	E4	2B	13	10	F0	19	C6	47	53	AF	EA	3D	5A	0-Óâ+..ø.ÆGSªê=Z
00A0h:	67	42	BC	98	Encrypted Data 2								E4	2A	11	gB¼~ŇîAB{"Űž\ä*.	
00B0h:	55	EC	4C	15	6A	5D	4E	5A	47	44	DF	47	44	DF	47	44	UìL.e(Űŷø.-<ŰGDß
00C0h:	ED	BE	55	B2	6A	5D	4E	5A	C5	06	38	C5	06	38	C5	06	í¾U²eç.øðªEªîÁ.8
00D0h:	48	05	D1	6C	5A	4E	5A	6A	46	FE	36	46	FE	36	46	FE	H.ŇlQ#`q*ž;-+žFp6
00E0h:	9A	C9	80	9E	C1	7A	8B	9C	E7	4C	A3	E7	4C	A3	E7	4C	šÉežîî..@ŰžERLçLê
00F0h:	8C	5D	20	1E	DA	34	56	50	36	1A	9B	B9	15	07	4C	2A	Ű] .Ű4VP6.ª¹..L*
0100h:	EA	8E	FB	79	9E	88	2A	24	B2	B6	2C	B4	70	51	9D	FB	êžűŷžªªš²Ű,´pQ.ű
0110h:	2E	71	08	30	0A	FD	77	AC	EC	A1	E5	EB	7B	3A	5F	C8	.q.0.Űŷŵ-î;âë{:_È
0120h:	70	84	48	1E	BA	69	B2	66	8E	A1	68	C1	80	4A	5A	0A	p„H.ºi²fž;hÄeJZ.
0130h:	96	A1	5A	A9	FB	0C	30	27	53	DD	70	A0	CF	94	90	E0	-;z@ű.0'SŰp î".à
0140h:	97	A5	A4	78	75	B2	80	7E	36	BF	19	77	6D	88	AB	0C	-Űnŷu²E~6ç.wmª«.

Get Proxy List(Gen3, Stage Signature)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	40	54	40	98	17	2E	1D	07	00	CB	CD	5B	F4	1C	F7	AA	@T@~		.EÍ	[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	F4	D8	00	0B	AD	DA	2C	57	F0	77	E2	49	67	B7	..	Åø..	Ú,WõwâIg.													
0030h:	19	3C	CF	58	AA	6B	72	D0	EB	99	76	2F	9E	74	E0	8C	.	<IXªkrDë™v/žtâ@														
0040h:	93	5F	14	C4	DC	ED	EB	2E	09	59	72	19	D4	87	8E	68	"	.ÄÜíë..	Yr%Ô+Žh													
0050h:	ED	32	E2	0E	27	9E	1A	03	DA	E5	A0	01	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.š7Ń*ÆÂ×ªn														
0070h:	BF	F2	B6	19	01	A1	6E	9D	18	24	29	3F	1F	43	53	E2	žòŧ..	¡n...š)?.	CSâ													
0080h:	B8	34	B0	AB	02	07	FC	0A	B3	F9	74	6F	31	5A	98	B0	„	4º«..ü.	³ùto7Z~ª													
0090h:	30	2D	D3	E4	2B	13	10	F0	19	C6	47	53	AF	EA	3D	5A	0-	Óä+..ô.	ÆGS⁻ê=Z													
00A0h:	67	42	BC	98	4E	CE	41	42	7B	22	FF	7A	5C	E4	2A	11	gB¼~	NîAB{	"ÿz\ä*.													
00B0h:	55	2C	4C	15	65	28	D9	FF	F0	11	97	3C	B6	41	44	DF	UiL.e	(Ùÿô.-<ŧGDß														
00C0h:	ED	BE	55	B2	65	E7	8D	F6	D0	5E	CA	A4	CD	C5	06	38	í¼U²eç.	ôD^Ê¤ÍÅ.8														
00D0h:	48	05	D1	6C	51	23	60	71	2A	BF	AC	2B	9E	46	EE	36	H.ŃlQ#`	q*ž-+žFp6														
00E0h:	9A	C9	80	9E	CF	2E	0B	40	DB	8E	80	52	4C	E7	4C	A3	šÉëžĩ.	@ÛžerLçLf														
00F0h:	8C	5D	20	1E	DA	34	56	50	36	1A	9B	B9	15	07	4C	2A	E]	Ú4VP6.	>¹..L*													

0xE81C4499-0x98405440-0xF40E2171-0x5BCDCB00 = 0x3E8

Get Proxy List(Gen3, Enc Data Offset&Len)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	40	54	40	98	17	2E	1D	07	00	CB	CD	5B	F4	1C	F7	AA	@T@~		.EÍ	[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	..	Åø..	Ú,Wõwâ	Ig·												
0030h:	19	3C	CF	58	AA	6B	72	D0	EB	99	76	2F	9E	74	E0	8C	.	<IXª	krDë™v/ž	tà@												
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	í	2â.	'ž..	Ůâ	.	"¥	→									
0060h:	E7	AF	18	A5	41	E0	8F	A7	37	D1	2A	C6	C2	D7	AA	6E	á	~.	¥Aà.	§7Ñ*	ÆÂ×ª	n										
0070h:	EF	F2	B6	19	0A	A1	6E	9D	18	24	29	3F	0F	43	53	E2	ž	òŧ..	¡n..	§)?	.CSâ											
0080h:	B8	34	B0	AB	02	07	FC	0A	B3	F9	74	6F	37	5A	98	B0	„	4º	«..	ü.	³ù	to7Z	~ª									
0090h:	30	2D	D3	E4	2B	13	10	F0	19	C6	47	53	AF	EA	3D	5A	0	-Ó	ã+..	ð.	ÆGS	ê=Z										
00A0h:	67	42	BC	98	4E	CE	41	42	7B	22	FF	7A	5C	E4	2A	11	gB¾	~Nî	AB{	"ÿz\	ã*	.										
00B0h:	55	EC	4C	15	65	28	D9	FF	F0	11	97	3C	B6	47	44	DF	Uì	L.e	(Ùÿ	ð.-	<ŧGDß											
00C0h:	ED	BE	55	B2	65	E7	8D	F6	D0	5E	CA	A4	CD	C5	06	38	í	¾U²	eç.	ðD^Ê	íĀ.	8										
00D0h:	48	05	D1	6C	51	23	60	71	2A	BF	AC	2B	9E	46	FE	36	H.	ÑlQ#	`q*ž	-+ž	Fp6											
00E0h:	9A	C9	80	9E	CF	2E	0B	40	DB	8E	80	52	4C	E7	4C	A3	š	É	žĩ.	@Ů	žerLç	Lž										
00F0h:	8C	5D	20	1E	DA	34	56	50	36	1A	9B	B9	15	07	4C	2A	E]	.	Ů4VP6.	>¹	..	L*										

0xF40E2171-0x98405440-0x5BCDCB00 = 0x231

Get Proxy List(Gen3, Enc Data Offset&Len)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	40	54	40	98	17	2E	1D	07	00	CB	CD	5B	F4	1C	F7	AA	@T@~		.EÍ	[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	..	Åø..	Ú,WõwâIg.													
0030h:	19	3C	CF	58	AA	6B	72	D0	EB	99	76	2F	9E	74	E0	8C	.	<IXªkrDë™v/žtâ@														
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:	E7	AF	18	A5	41	E0	8F	A7	37	D1	2A	C6	C2	D7	AA	6E	á	~.	¥Aà.š7Ň*ÆÂ×ªn													
0070h:	EF	F2	B6	19	0A	A1	6E	9D	18	24	29	3F	0F	43	53	E2	žòŦ..	jn...š)?.	CSâ													
0080h:	B8	34	B0	AB	02	07	FC	0A	B3	F9	74	6F	37	5A	98	B0	„	4º«..ü.	³ùto7Z~ª													
0090h:	30	2D	D3	E4	2B	13	10	F0	19	C6	47	53	AF	EA	3D	5A	0-	Óã+..ô.	ÆGS¯ê=Z													
00A0h:	67	42	BC	98	4E	CE	41	42	7B	22	FF	7A	5C	E4	2A	11	gB¾~	NîAB{	"ÿz\ã*.													
00B0h:	55	EC	4C	15	65	28	D9	FF	F0	11	97	3C	B6	47	44	DF	UiL.e	(Ùÿô.	-<ŦGDß													
00C0h:	ED	BE	55	B2	65	E7	8D	F6	D0	5E	CA	A4	CD	C5	06	38	í¾U²eç.	ôD^Ê¤ÍÅ.8														
00D0h:	48	05	D1	6C	51	23	60	71	2A	BF	AC	2B	9E	46	FE	36	H.ŇlQ#`	q*ž-+žFp6														
00E0h:	9A	C9	80	9E	CF	2E	0B	40	DB	8E	80	52	4C	E7	4C	A3	šÉežĩ.	@ÛžerLçLf														
00F0h:	8C	5D	20	1E	DA	34	56	50	36	1A	9B	B9	15	07	4C	2A	E]	..	Ú4VP6.>¹..L*													

$0xF40E2171 - 0x98405440 - 0x5BCDCB00 = 0x231$

$0x268 - 0x231 = 0x37$

$0x24 + 0x37 = 0x5B$



Get Proxy List(Encryption Algorithm)

Compressed
Blowfish
3DES
Blowfish

Get Proxy List(Gen3)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	28	31	31	32	65	72	¢IMóŬ.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.
0080h:	01	10	31	61	39	33	61	66	63	62	37	36	66	35	30	30	..1a93afcb76f500
0090h:	30	30	00	02	02	10	74	65	73	74	38	36	35	65	30	31	00....test865e01
00A0h:	36	31	62	38	66	31	39	63	30	30	00	02	01	10	00	00	61b8f19c00.....
00B0h:	00	00	39	64	37	36	33	36	31	30	34	35	61	34	34	34	..9d76361045a444
00C0h:	30	30	00	02	01	10	00	00	00	00	63	38	33	34	31	36	00.....c83416
00D0h:	35	63	33	35	61	35	61	38	30	30	00	02	01	10	4F	00	5c35a5a800....0.
00E0h:	00	00	38	34	30	61	31	37	35	35	30	31	61	66	35	63	..840a175501af5c
00F0h:	30	30	00	02	01	20	1E	00	00	00	00	00	00	00	61	38	00... ..a8
0100h:	36	66	35	30	32	30	32	37	31	65	30	30	30	30	00	02	6f5020271e0000..
0110h:	01	20	6C	D7	66	4D	00	00	00	00	63	32	34	31	64	31	. l×fM....c241d1
0120h:	61	37	32	65	61	63	65	63	30	30	00	02	01	10	00	00	a72eacec00.....
0130h:	00	00	63	61	62	66	38	63	32	39	36	30	34	33	38	30	..cabf8c29604380
0140h:	30	30	00	02	01	10	45	89	34	07	65	35	66	35	36	32	00....E%4.e5f562

Get Proxy List(Gen3)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	28	6D	5F	65	78	74	¢IMóÜ.Ÿ^..(m_ext
0010h:	65	72	6E	61	6C	5F	69	6E	66	6F	5F	70	61	63	6B	65	ernal_info_packe
0020h:	64	00	01	0C	6D	5F	65	78	74	65	72	6E	61	6C	5F	69	d...m_external_i
0030h:	6E	66	6F	5F	69	64	00	02	01	20	00	00	00	00	00	00	nfo_id... ..
0040h:	00	00	6D	5F	65	78	74	65	72	6E	61	6C	5F	64	61	74	..m_external_dat
0050h:	61	5F	73	69	67	6E	61	74	75	72	65	00	02	02	00	6D	a_signature....m
0060h:	5F	65	78	74	65	72	6E	61	6C	5F	64	61	74	61	5F	62	_external_data_b
0070h:	6C	6F	62	00	02	02	00	6D	5F	69	70	00	02	01	10	00	lob....m_ip.....
0080h:	00	00	00	6D	5F	76	65	72	73	69	6F	6E	00	01	10	6D	...m_version...m
0090h:	5F	62	75	69	6C	64	5F	6E	61	6D	65	00	02	02	10	74	_build_name....t
00A0h:	65	73	74	6D	5F	6D	61	6A	6F	72	00	02	01	10	00	00	estm_major.....
00B0h:	00	00	6D	5F	6D	69	6E	6F	72	00	02	01	10	00	00	00	..m_minor.....
00C0h:	00	6D	5F	62	75	69	6C	64	00	02	01	10	4F	00	00	00	.m_build....O...
00D0h:	6D	5F	6C	69	76	65	5F	74	69	6D	65	00	02	01	20	1E	m_live_time... .
00E0h:	00	00	00	00	00	00	00	6D	5F	63	75	72	72	65	6E	74	m_current
00F0h:	5F	74	69	6D	65	00	02	01	20	6C	D7	66	4D	00	00	00	_time... l×fM...
0100h:	00	6D	5F	6C	69	73	74	65	6E	6E	69	6E	67	5F	70	6F	.m_listenning_po
0110h:	72	74	00	02	01	10	00	00	00	00	6D	5F	72	65	61	6C	rt.....m_real
0120h:	5F	74	61	72	67	65	74	5F	69	70	00	02	01	10	45	89	_target_ip....E%
0130h:	34	07	6D	5F	62	6F	6F	74	73	74	72	61	70	5F	6C	69	4.m_bootstrap_li
0140h:	73	74	00	01	04	6D	5F	63	6C	69	65	6E	74	73	5F	6C	st...m_clients_l

Get Proxy List(Gen3, Job Server, Entry 1)

0160h:	6D 5F 65 78 74 65 72 6E 61 6C 5F 64 61 74 61 5F	m_external data
0170h:	62 6C 6F 62 00 02 02 85 02 0F 36 18 86 25 1E 75	blob.....6.†%.u
0180h:	B1 1E 24 37 7F 9E 89 3D 43 11 8B 73 63 2A 3F EB	±.\$7.ž‰=C.<sc*?ë
0190h:	76 35 A6 99 6F BA 30 5C D9 74 44 B3 E4 19 3D 19	v5!™o°0\ÛtD³ä.=.
01A0h:	2F 02 95 B1 7D EE EC AF BC AD E3 1A 42 6B 88 7B	/..±}îî¬¼-ä.Bk^{
01B0h:	90 CD 8D 42 14 70 4A A0 9C 57 35 35 B7 AF BF DB	.Í.B.pJ œW55·¬¿Û
01C0h:	92 1F 39 EB AA DC D1 C3 1D 18 D4 99 8D F3 64 8E	' .9ëªÜÑÃ..Ô™.ódŽ
01D0h:	8F B6 10 1A 24 D0 39 E6 5E CD B3 C2 FE 83 76 C7	.Œ..\$Ð9æ^Í³ÂpfvÇ
01E0h:	5C A2 46 09 D6 14 D6 8D 7D D7 B1 C6 E2 F5 FB 93	\¢F.Ö.Ö.}×±Æâôû"
01F0h:	25 F2 69 14 39 9B FC B0 E0 7B E6 AD 1B DC 3C 22	%òì.9>ü°à{æ-.Û<"
0200h:	B6 1B B4 B5 18 55 BD 86 D1 67 42 4E CD 10 A8 10	Œ.'µ.U½†ÑgBNÍ.¨.
0210h:	D1 BE C2 27 66 C1 F3 85 C3 5D 6D 5F 73 75 63 63	Ñ¾Â'fÁÓ..Ã]m_succ
0220h:	65 73 73 00 02 01 04 01 6D 5F 6C 69 76 65 5F 74	ess.....m_live_t



Job Server (Encryption Algorithm)

Compressed
Blowfish
3DES
Blowfish

Get Proxy List(Gen3, Job Server)

[illegible]



Kelihos Gen3

- Header
- Encryption
- Key Words
- Job Servers
- Functions

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a laptop. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

4th Generation Kelihos

Get Proxy List(Gen4)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F			
0000h:	C1	1F	4A	CA	EA	8A	A2	63	88	32	A4	01	8A	2E	8D	9A	Á	J	Ê	ê	Š	č	c	^	2	π	.	Š	.	š					
0010h:	9A	87	EE	CB	CB	DD	DC	97	A1	35	00	00	00	00	00	00	š	+	î	Ë	Ë	Ÿ	Ü	-	;	5	.	.	.	.	.	.			
0020h:	00	6A	36	2B	00	98	64	C7	B6	C4	3B	ED	59	BB	CA	69	.	j	6	+	.	~	d	ç	¶	Ä	;	î	Y	»	Ê	î			
0030h:	01	CF	D2	54	95	10	DC	78	6A	9A	30	34	DE	BD	CE	28	.	İ	Ò	T	.	Ü	x	j	š	0	4	P	½	Î	(				
0040h:	D0	F8	AC	8F	CC	AE	11	CD	94	9A	7A	F4	DA	90	3C	F8	Đ	ø	-	.	İ	ø	.	Í	"	š	z	ô	Ú	.	<	ø			
0050h:	8E	24	C7	13	53	70	34	ED	D9	31	8F	A9	9A	8F	08	2C	Ž	š	ç	.	S	p	4	ı	Ù	1	.	©	š	.	.	,			
0060h:	59	CE	0A	57	3D	E1	C8	B8	CB	36	5C	AB	67	A0	53	FE	Y	Î	.	W	=	á	È	.	Ê	6	\	«	g	S	p				
0070h:	38	E8	36	C0	06	E6	81	45	82	90	AD	EB	E9	B9	31	D6	8	è	6	À	.	æ	.	E	.	.	ë	é	¹	l	Ö				
0080h:	0A	02	7E	A4	92	13	FB	F1	10	1C	45	B3	58	E0	11	28	.	.	~	π	'	.	û	ñ	.	.	E	³	X	à	.	(			
0090h:	8B	34	46	37	31	C7	80	3A	A3	B7	4E	7A	0A	E4	D8	A0	<	4	F	7	1	ç	€	:	f	.	N	z	.	ä	ø				
00A0h:	A7	31	26	68	C2	9F	2A	7B	38	60	94	2F	24	B2	73	FF	\$	1	&	h	Â	Ÿ	*	{	8	`	"	/	š	²	s	Ÿ			
00B0h:	E0	09	07	1F	ED	33	78	84	96	69	3F	F8	48	F2	F0	63	à	.	.	.	ı	3	x	,	.	-	i	?	ø	H	ò	ö	c		
00C0h:	C5	2E	D3	4A	0B	17	7C	56	45	E7	27	CE	11	E7	5E	50	Å	.	Ó	J	.	.		ç	€	'	Î	.	ç	^	P				
00D0h:	12	06	0F	E9	9A	BF	DB	D9	3C	59	80	99	B1	33	BC	41	.	.	.	é	š	;	Ù	Ù	<	Y	€	™	+	3	¼	A			
00E0h:	A1	EC	58	F0	C5	BE	68	09	FC	07	1F	8B	27	55	FE	B6	;	ı	X	ö	Å	¾	h	.	.	.	ü	.	.	.	<	'	U	p	¶
00F0h:	1D	57	D3	67	E6	86	8B	D7	E7	0E	E9	D9	3D	E4	C8	E2	.	W	Ó	g	æ	+	<	×	ç	.	é	Ù	=	ä	Ê	â			
0100h:	BF	2D	C4	39	78	E6	00	23	33	DA	1E	8D	75	DE	AD	AB	ç	-	Ä	9	x	æ	.	#	3	Ú	.	.	u	p	«				
0110h:	31	B6	32	5E	BB	69	33	4B	45	B0	F6	0D	D8	43	0E	1A	1	¶	2	^	»	.	i	3	K	E	°	ö	.	ø	C	.	.		
0120h:	64	B3	4E	09	C9	49	66	26	C2	B7	BC	8B	0C	ED	08	51	d	³	N	.	É	I	f	&	Â	.	¼	<	.	ı	.	Q			
0130h:	44	72	D5	72	5D	6B	2B	AE	FB	5C	C5	9B	BD	B1	13	5C	D	r	Ö	r	]	k	+	@	û	\	Å	.	¾	±	.	.	\		
0140h:	8A	52	8B	B9	A8	5D	33	3A	8B	31	DE	B6	D0	E6	22	72	Š	R	<	¹	"	]	3	:	<	1	p	¶	D	æ	"	r			



Get Proxy List(Encryption Algorithm)

Blowfish
3DES
Compressed
Blowfish

A background image showing silhouettes of several business professionals in a meeting or office setting. The scene is dimly lit with a warm, reddish-brown color palette. In the center, two men in suits are shaking hands. To their left, a group of people are standing and talking. To their right, more people are visible, some sitting and some standing. The overall atmosphere is professional and collaborative.

Get Proxy List(Gen4)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	24	31	00	02	01	40	¢IMóŬ.Ÿ^...\$1...@
0010h:	70	A3	8A	64	02	53	41	06	B4	0E	52	F4	6E	CA	10	ED	přšđ.SA.´.RônÊ.í
0020h:	33	00	02	01	20	75	D9	4B	4F	00	00	00	00	34	00	02	3... uŬKO....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	...Æð..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
00A0h:	00	00	00	67	00	02	01	20	00	00	00	00	00	00	00	00	...g... ..
00B0h:	70	00	02	01	40	00	00	00	00	00	00	00	00	00	00	00	p...@.....
00C0h:	00	00	00	00	00	78	00	02	01	20	00	00	00	00	00	00	x... ..
00D0h:	00	00	01	14	62	00	02	01	10	47	CF	E3	01	64	00	02	b....Gĩă.d..
00E0h:	01	10	50	00	00	00	67	00	02	01	20	00	00	00	00	00	..P...g... ..
00F0h:	00	00	00	70	00	02	01	40	00	00	00	00	00	00	00	00	...p...@.....
0100h:	00	00	00	00	00	00	00	00	78	00	02	01	20	00	00	00	x... ..
0110h:	00	00	00	00	00	01	14	62	00	02	01	10	32	88	1C	02	b....2^..
0120h:	64	00	02	01	10	50	00	00	00	67	00	02	01	20	00	00	d....P...g... ..
0130h:	00	00	00	00	00	00	70	00	02	01	40	00	00	00	00	00	p...@.....
0140h:	00	00	00	00	00	00	00	00	00	00	00	78	00	02	01	20	x...

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and others are in motion, all set against a dark red background with a subtle geometric pattern.

Kelihos Gen4

- Header
- Encryption
- Key Words
- Job Servers
- Functions

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits. Some are standing, some are shaking hands, and one is holding a briefcase. The background of the banner is a dark red with a subtle geometric pattern.

Protocol , Encryption, Evolution

5th Generation Kelihos

Get Proxy List(Gen5)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	3D	BC	C6	43	F2	BC	C6	43	02	BD	C6	43	23	C2	C6	43	=¼ECÒ¼EC.¼EC#ÂEC
0010h:	28	C1	C6	43	28	C2	C6	43	EF	8C	B4	62	D1	90	87	C0	(ÁEC(ÂECiÉ' bÑ. ‡À
0020h:	F1	EB	DA	08	3D	69	C6	BE	0A	90	E7	3A	F8	98	50	E8	ñeÚ.=iÆ¾..ç:ø~Pè
0030h:	89	56	52	7F	29	00	D5	31	70	9D	C3	6A	61	FC	F7	7F	%VR.) .Ölp.Äjaü÷.
0040h:	80	01	EC	16	C7	E8	A3	D8	C4	0C	C6	02	15	1B	6E	31	€ .i.Çè£ØÄ.E...n1
0050h:	54	6A	0D	68	E4	43	B7	B2	AB	85	C6	11	F4	B7	CD	50	Tj.häC.²«...E.ô.ÍP
0060h:	16	D0	70	35	E3	23	C6	D7	12	8F	CE	AC	ED	89	38	1D	.ðp5ã#E×...Î-í%8.
0070h:	34	8A	B8	BC	BA	0E	02	FF	68	24	37	B7	2F	3B	35	2F	4Š,¼°...ÿh\$7./;/5/
0080h:	A1	DF	B8	2A	3E	88	C6	BA	21	67	F9	4C	8A	AF	BF	2F	; ß,*>^E°!gùLŠ~¿/</td
0090h:	B3	45	5F	A2	E7	4B	2A	92	F6	FB	7D	6B	8E	77	50	BE	³E_çÇK*' öû}kŽwP¾
00A0h:	41	C2	E9	44	A6	66	00	8A	98	67	1D	CA	2F	FC	FE	F9	AÂÉD!f.Š~g.Ê/üþù
00B0h:	F5	7F	1B	18	64	3B	D6	DE	2C	34	7B	BC	80	68	DE	A9	ö...d;Öß,4{¼€hð©
00C0h:	AE	19	D2	C3	8B	7A	1A	83	77	E6	F2	6C	13	EF	8C	B4	@.ÒÄ<z.fwæòl.iÉ'
00D0h:	62	D1	90	87	C0	F1	EB	DA	08	3D	69	C6	BE	82	27	93	bÑ. ‡ÀñeÚ.=iÆ¾,'"
00E0h:	A2	FC	98	B9	18	07	04	FF	C6	FA	21	FF	FC	18	B5	4D	çü~¹...ÿÆú!ÿü.µM
00F0h:	51	11	06	9D	4A	F8	E4	F0	55	1B	69	6D	8D	97	1C	54	Q...JøäöU.im.-.T
0100h:	6E	85	BE	F1	F9	AC	1A	47	D9	DC	A7	91	33	EA	F4	92	n...¾ñù-.GÜÜŠ'3êô'
0110h:	81	19	4C	B6	9D	F3	59	A9	8B	6A	B7	A1	AE	75	AC	60	..L¶.óY©<j.;@u-`
0120h:	42	44	01	A9	2B	89	18	19	24	95	08	0F	1B	F1	CE	11	BD.©+%...§•...ñÎ.
0130h:	BD	C9	2E	76	69	1E	C7	D6	CC	ED	DF	6F	B2	F3	05	D3	¼É.vi.ÇÖÎíßo²ó.Ó
0140h:	9E	E9	E4	25	32	F4	3C	1A	80	EA	53	0C	19	AF	AA	76	žéä%2ô<.€ês...ªv

A horizontal banner at the top of the slide features silhouettes of several business professionals in suits, some standing and some sitting, against a dark red background.

Get Proxy List(Encryption Algorithm)

Blowfish
Custom Encryption
Compressed

A background image showing silhouettes of several business professionals in a meeting or conference setting. They are dressed in formal attire like suits and dresses. The scene is dimly lit, with some light reflecting off surfaces, creating a professional and collaborative atmosphere.

Get Proxy List(Gen4)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	24	31	00	02	01	40	çIMóÛ.Ÿ^..\$1...@
0010h:	CD	4B	72	D8	3D	D8	42	C9	A7	FF	00	28	E3	EE	5E	7F	ÍKrø=øBÉšŸ.(âï^.
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	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	...LqÇ.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	59	1C	1D	04	64	00	02	01	10	50	.b....Y...d....P
00A0h:	00	00	00	67	00	02	01	20	00	00	00	00	00	00	00	00	...g... ..
00B0h:	70	00	02	01	40	00	00	00	00	00	00	00	00	00	00	00	p...@.....
00C0h:	00	00	00	00	00	78	00	02	01	20	00	00	00	00	00	00	x... ..
00D0h:	00	00	01	14	62	00	02	01	10	BC	ED	34	05	64	00	02	...b....¼i4.d..
00E0h:	01	10	50	00	00	00	67	00	02	01	20	00	00	00	00	00	..P...g... ..
00F0h:	00	00	00	70	00	02	01	40	00	00	00	00	00	00	00	00	...p...@.....
0100h:	00	00	00	00	00	00	00	00	78	00	02	01	20	00	00	00	x... ..
0110h:	00	00	00	00	00	01	14	62	00	02	01	10	1F	CF	48	05	b.....ÏH.
0120h:	64	00	02	01	10	50	00	00	00	67	00	02	01	20	00	00	d....P...g... ..
0130h:	00	00	00	00	00	00	70	00	02	01	40	00	00	00	00	00	p...@.....
0140h:	00	00	00	00	00	00	00	00	00	00	00	78	00	02	01	20	x...



Kelihos Gen5 (Job Servers)

188.190.98.72

188.190.98.74

193.105.134.189

193.105.134.190

193.105.134.89

194.44.45.121

194.44.45.123

194.44.45.53

194.44.45.64

195.230.125.67

195.230.125.69

212.71.10.213

212.71.10.215

78.83.177.246

78.83.177.249



Thank You!

xyang@fortinet.com

@kyleyang001