

Lethic: M86 Security

Archived: 2026-04-02 11:59:16 UTC

January 7, 2010

Aliases

- No obvious aliases, most samples we analyzed had varied generic detection names.

Comments

Although recently uncovered, the Lethic spambot (or its predecessors) have probably been in existence for some time. For over 2 years, we have observed a type of spam from an unknown botnet which we simply called "Type 11". Recently, malware behind this spam was discovered by [Arbor Security Engineering and Response Team](#). Lethic is a proxy type spambot which relays spam from a control server to its destination. It is focused on sending pharmaceutical and replica watch spam campaigns. As of this writing, Lethic was responsible about for 8-10% of spam.

Features

- Acts as a proxy to relay spam
- Process injection to Explorer.exe
- Fast, multi-threaded
- Anti-debugging and Anti-VM detection

Spamming Rate

- Varies depending on the relaying server ranging from 12,000 msgs/hour/bot to peaks of 60,000 msgs/hour/bot.

Command and Control

Lethic is a proxy Trojan that allows a command and control server to use the infected system to relay spam. We have observed that it connects to the following domains, many of which are hosted by FDCservers.net.

b1ij7hifd.com (66.90.104.106) on port 8900

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

blogforyour.com (64.191.15.133) on port 8900

OrgName: Network Operations Center Inc.

OrgID: NOC

Address: PO Box 591

City: Scranton

StateProv: PA

PostalCode: 18501-0591

Country: US

busnotstop.com (66.90.101.84) on port 1430

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

elephantanimal.com (66.90.109.19) 8900

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

gooddoctorlist.com (66.90.104.166) on port 8090

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

goodhear.me.cn (66.90.101.194) on port 8090

OrgName: FDCservers.net

OrgID: FDCSE
Address: 141 w jackson blvd.
Address: suite #1135
City: Chicago
StateProv: IL
PostalCode: 60098
Country: US

happymanwoman.cn (67.159.44.237) on port 8900

OrgName: FDCservers.net
OrgID: FDCSE
Address: 141 w jackson blvd.
Address: suite #1135
City: Chicago
StateProv: IL
PostalCode: 60098
Country: US

iamnothere.cn (64.237.61.132) on port 8090

OrgName: Choopa, LLC
OrgID: CHOOP-1
Address: 2400 Main Street Extension
Address: Suite 12
City: Sayreville
StateProv: NJ
PostalCode: 08872
Country: US

itsyourservice.cn (66.90.103.239) on port 8900

OrgName: FDCservers.net
OrgID: FDCSE
Address: 141 w jackson blvd.
Address: suite #1135
City: Chicago
StateProv: IL
PostalCode: 60098
Country: US

linktomem.cn (66.197.237.165) on port 8900

OrgName: Network Operations Center Inc.
OrgID: NOC
Address: PO Box 591
City: Scranton
StateProv: PA

PostalCode: 18501-0591

Country: US

MacysGiftsOnline.com (66.90.109.19) on port 8900

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

mo8f2eerrd.com on port (66.90.101.74) 8090

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

somethingwrong.cn (66.90.103.223) on port 8090

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

sometimesgood.com (67.159.44.78) on port 1430

OrgName: FDCservers.net

OrgID: FDCSE

Address: 141 w jackson blvd.

Address: suite #1135

City: Chicago

StateProv: IL

PostalCode: 60098

Country: US

tenverybest.com (66.90.103.237) on port 5050

OrgName: FDCservers.net
OrgID: FDCSE
Address: 141 w jackson blvd.
Address: suite #1135
City: Chicago
StateProv: IL
PostalCode: 60098
Country: US

underseaprawn.com (96.9.147.37) on port 8090

OrgName: Network Operations Center Inc.
OrgID: NOC
Address: PO Box 591
City: Scranton
StateProv: PA
PostalCode: 18501-0591
Country: US

verywellhere.cn (67.159.44.236) on port 8090

OrgName: FDCservers.net
OrgID: FDCSE
Address: 141 w jackson blvd.
Address: suite #1135
City: Chicago
StateProv: IL
PostalCode: 60098
Country: US

wasyoujoy.cn (208.69.112.58) on port 8090

OrgName: CPC Technologies, LLC.
OrgID: CPCTE
Address: 1301 E. Debbie Ln Ste 102
Address: #160
City: Mansfield
StateProv: TX
PostalCode: 76063
Country: US

younotgood.cn (208.69.113.130) on port 8900

OrgName: CPC Technologies, LLC.
OrgID: CPCTE
Address: 1301 E. Debbie Ln Ste 102
Address: #160

City: Mansfield
 StateProv: TX
 PostalCode: 76063
 Country: US

Lethic seems to have a custom communication protocol. Once connected, the control server initiates the handshaking and gives the bot an IP address and port to relay the data to. It then uses the infected system as a proxy to relay spam messages to its target. The image below shows the handshaking and communication between the command and control server and the infected machine.

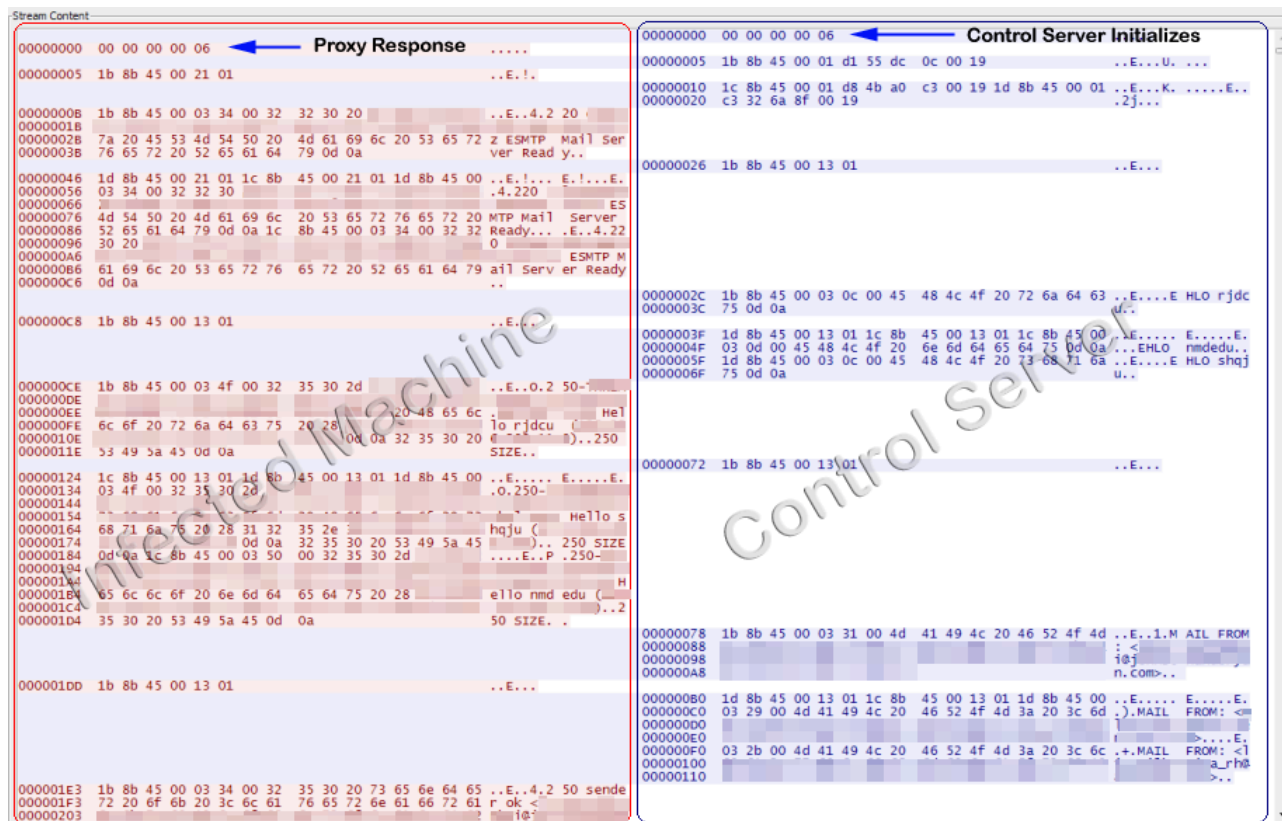


Figure 1.

The Lethic command and control server uses command codes to communicate to its bot. The packet header consists of a thread number and command code followed by its corresponding parameter.

Here is a list of the command and control server's command codes:

- 0x01 - Tells the bot on what SMTP server IP address and port to connect. The command code is followed by the IP address then the port number.

```
00000005 1b 8b 45 00 01 d1 55 dc 0c 00 19
          |-----|-----|-----|
          Thread Number Command Code IP Address Port Number (25)
```

- 0x03 - Send data to the bot. The command code is followed by the data length and the data.

```

0000002C 1b 8b 45 00 03 0c 00 45 48 4c 4f 20 72 6a 64 63 ..E...E HLO rjdc
          |-----|-----|-----|
          | Thread Number | Data Length | Data
          |-----|-----|-----|
          | Command Code |
          |-----|
0000003C 75 0d 0a
    
```

- 0x13 - Unknown command, usually followed by 0x01.

```

00000026 1b 8b 45 00 13 01
          |-----|-----|
          | Thread Number | Parameter Code
          |-----|-----|
          | Command Code |
    
```

Here is a list of the bot's command codes:

- 0x21 - The bot acknowledges every command sent by the control server.

```

00000005 1b 8b 45 00 21 01
          |-----|-----|
          | Thread Number | Parameter Code
          |-----|-----|
          | Acknowledge |
    
```

- 0x03 - Send data to the control server. The command code is followed by the data length and the data.

```

0000000B 1b 8b 45 00 03 34 00 32 32 30 20 ..E..4.2 20
          |-----|-----|-----|
          | Thread Number | Data Length | Data
          |-----|-----|-----|
          | Command Code |
          |-----|
0000001B 7a 20 45 53 4d 54 50 20 4d 61 69 6c 20 53 65 72 z ESMTTP Mail Ser
0000002B 76 65 72 20 52 65 61 64 79 0d 0a ver Read y..
0000003B
    
```

- 0x13 - unknown command, usually followed by 0x01.

```

000000C8 1b 8b 45 00 13 01
          |-----|-----|
          | Thread Number | Parameter
          |-----|-----|
          | Command Code |
    
```

Here is a short explanation on how the C&C communication works, based on the packet capture in figure 1.

Once the bot is connected, the control server sends an initialization packet:

```
00000000 00 00 00 00 06
```

The bot in the infected machine confirms by sending the same data:

```
00000000 00 00 00 00 06
```

The control server sends the "\x01" command code followed by the SMTP server IP address and port number where the bot will relay the spam messages:

```
00000005 1b 8b 45 00 01 d1 55 dc 0c 00 19
      Thread Number | SMTP server IP | SMTP port
      Command Code
```

The bot acknowledges the command

```
00000005 1b 8b 45 00 21 01
      Thread Number Acknowledge
```

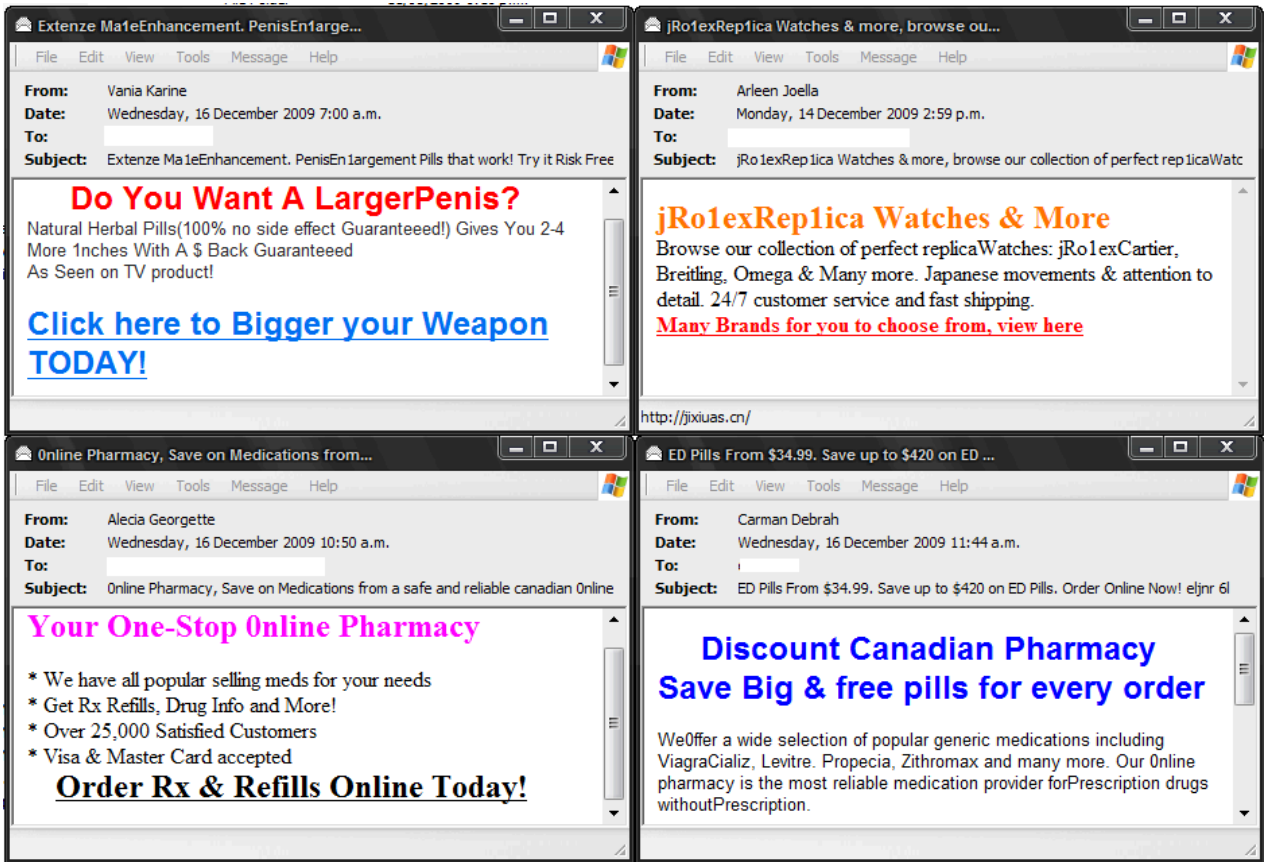
The control server sends more SMTP server IP address to connect to:

```
00000010 1c 8b 45 00 01 d8 4b a0 c3 00 19 1d 8b 45 00 01
      Thread Number | IP Address | Thread Number |
      Command Code | Port Number | Command Code
00000020 c3 32 6a 8f 00 19
      IP Address Port Number
```

The bot relays SMTP transaction from the destination server to the control server:

```
0000000B 1b 8b 45 00 03 34 00 32 32 30 20 ...E..4.2 20
0000001B Thread Number | Data Length | Data
      Command Number
0000002B 7a 20 45 53 4d 54 50 20 4d 61 69 6c 20 53 65 72 z ESMTP Mail Ser
0000003B 76 65 72 20 52 65 61 64 79 0d 0a ver Read y..
```

Here are some typical sample spam messages that the Lethic Trojan was sending at the time of writing.



Malware Behavior on Host

Drops a copy of itself in the Windows System directory. Here are the malware paths from the various samples we examined:

- C:\WINDOWS\system32\xcllsx.exe
- C:\WINDOWS\system32\ldfrmmmd.exe
- C:\WINDOWS\system32\ncmdds.exe
- C:\WINDOWS\system32\lsprcx.exe
- C:\WINDOWS\system32\jdsuml.exe

An autorun registry entry was created to execute files upon Windows startup.

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
<random value> = "C:\WINDOWS\system32\ldfrmmmd.exe"
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
<random value> = "C:\WINDOWS\system32\jdsuml.exe"
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
<random value> = "C:\WINDOWS\system32\lsprcx.exe"
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
<random value> = "C:\WINDOWS\system32\ncmdds.exe"
```

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
<random value> = "C:\WINDOWS\system32\xcllsx.exe"

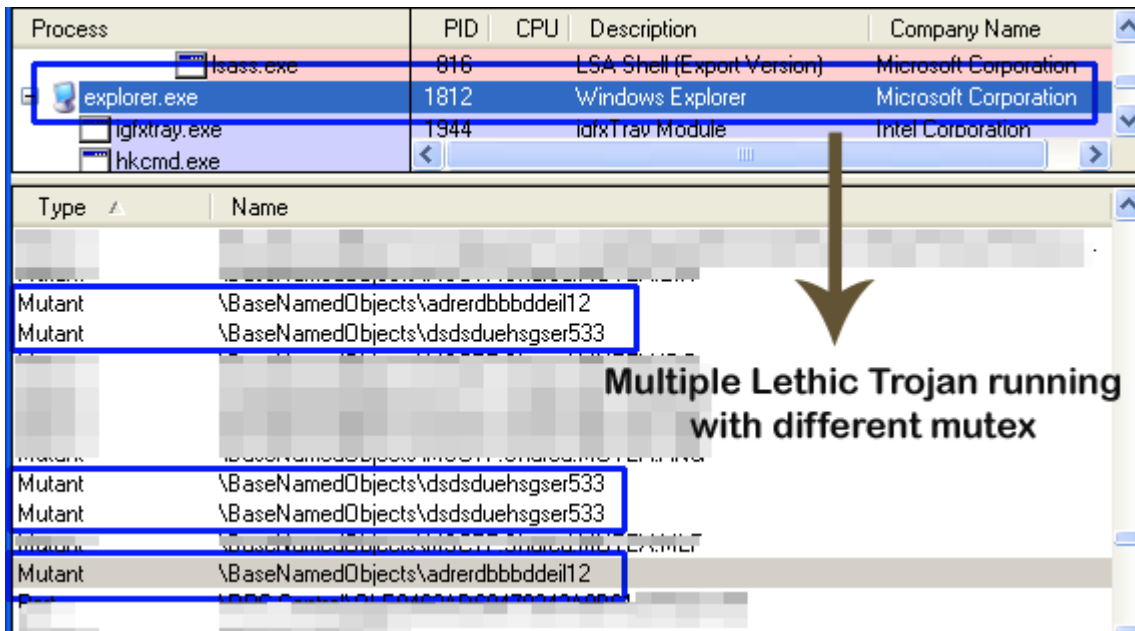
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Taskman = "C:\WINDOWS\system32\jdsuml.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Taskman = "C:\WINDOWS\system32\ldfrmmmd.exe"

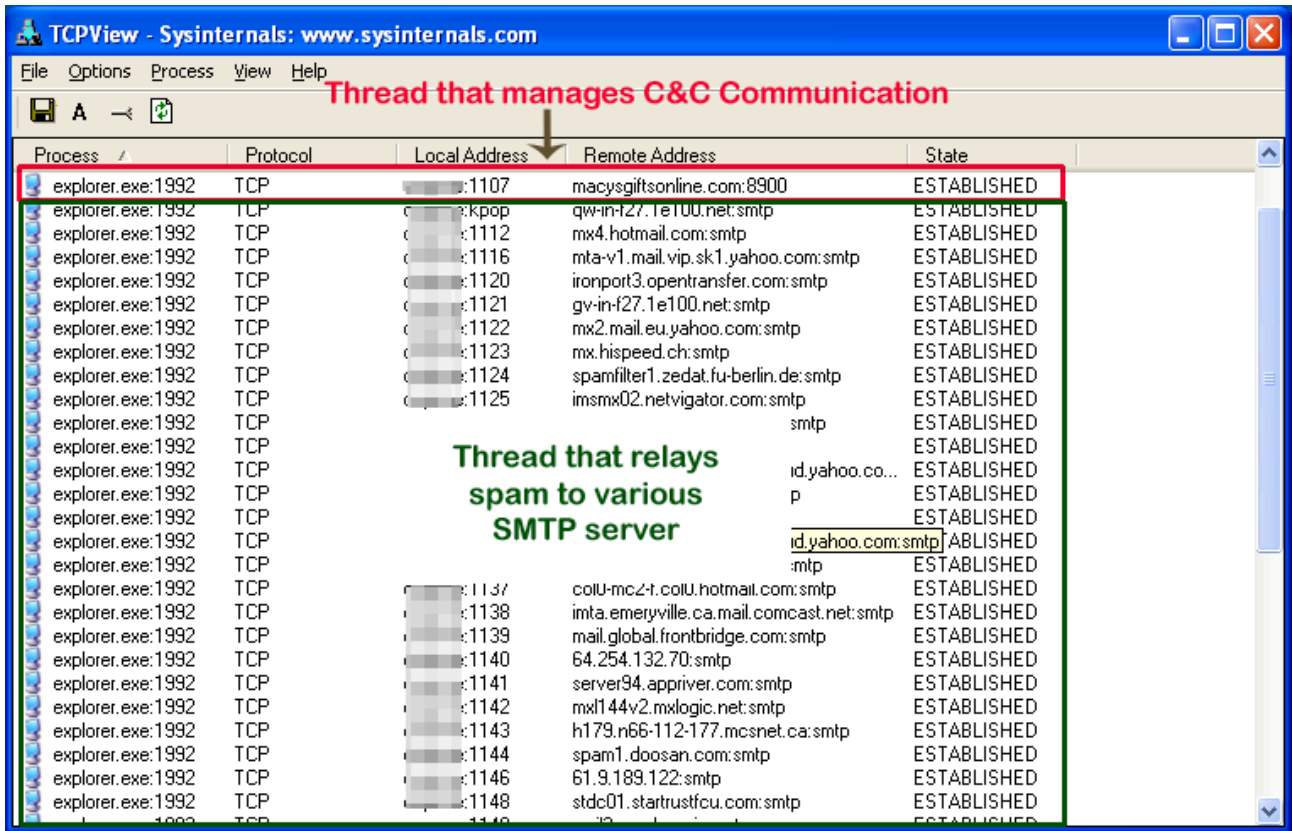
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Shell = "explorer.exe,C:\WINDOWS\system32\xcllsx.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Taskman = "C:\WINDOWS\system32\xcllsx.exe"

Lethic injects its code into Explorer.exe and creates a random-named mutex in the infected machine:



Once the malicious code is injected to Explorer.exe, the infected machine tries to contact the C&C server using a hardcoded domain name on a predefined port. The infected machine then receives spamming data from the C&C server. The infected explorer process spawns multiple threads that relays spam to a destination SMTP server.



Finally, during our analysis, we also saw Lethic installed alongside other spambots such as [Grum](#) and [Pushdo](#), all of which were distributed by [Virut](#).

© M86 Security	Last Reviewed: January 6, 2010 by Rodel Mendrez
----------------	---

Source: <https://web.archive.org/web/20101031045748/http://www.m86security.com/labs/spambotitem.asp?article=1205>