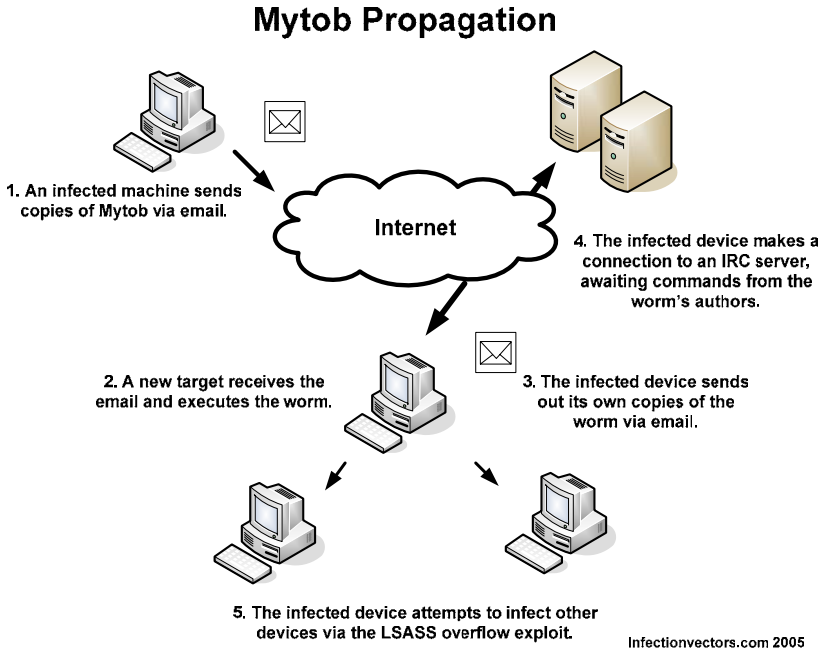
Arrest-tob: Alleged Zotob Authors Captured
infectionvectors.com
August 2005

Overview

After a 2004 that was the most successful year for malware author arrests, 2005 has now posted a very high-profile capture: the alleged creators of Zotob. These coders may also be the original Mytob writers (it seems clear that the same individuals are at least the ones responsible for many variants), as the two worms are incredibly similar. There is speculation that these writers are responsible for Rbot code that has been used in a number of Internet attacks.

Relentless

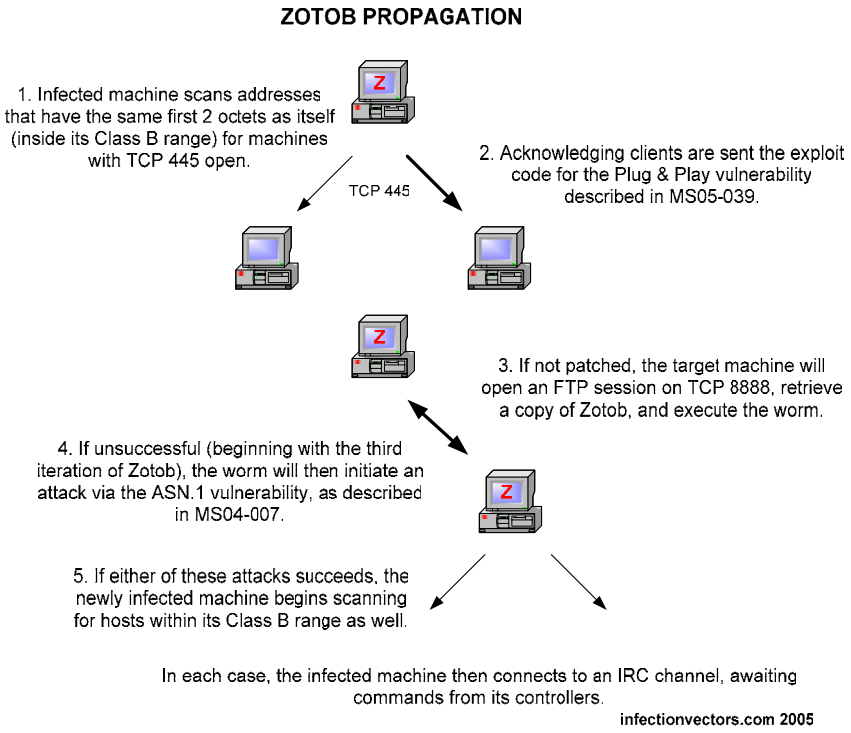
The Mytob and Zotob worms have nailed their success or failure on a consistent strategy: maintain a steady stream of slightly-altered variants in hopes of staying ahead of defense tactics. The Mytob worm has been in circulation since February of 2005 introduced a new level of dedication to the professional malware industry. Over the year, Mytob was responsible for dozens of variants, all with very small changes that were intended to stifle antivirus companies from producing effective detection mechanisms.



The mass mailer (which also spread via the LSASS flaw Sasser made famous, MS04-011) was released in waves of iterations, each with an IRC control component that allowed its authors to use the infected boxes for numerous nefarious operations.

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

Zotob made its first appearance just days after the release of Microsoft's August security bulletins, which included a reported flaw in the Windows Plug & Play service. It was this vulnerability (MS05-039) that Zotob capitalized upon, using the hole to infect numerous machines.



Rejoinder

Based on tips from the FBI in the United States, law enforcement in both Turkey and Morocco picked up suspects on August 26, 2005. In Turkey, a 21-year-old man who goes by the handle "Coder" was captured. Near the same time, an 18-year-old in Morocco was arrested for suspected involvement in the Zotob attacks. The teenager went by the name "Diabl0." Both names were found repeatedly in the Zotob code.

The IRC back-end for the initial version of Zotob connects to:

```
diabl0.turkcoders.net:8080
```

and contains the following string:

```
Botsor2005 Made By.... Greetz to good friend Coder. Based on HellBot3
MSG to avs: the first av to detect this worm will be the first killed
in the next 24hrs!!!
```

The arrests came quickly after the distribution of the Zotob worm, with speed rivaling the speed of the worm releases. Relative to other malware authors, the Zotob coders were picked up almost instantly. In addition, no Microsoft “bounty” funds appear to be in play this time around, after the successful capture of the Sasser/Netsky coder last year.

Worm	Release Date	Author Arrest
Netsky	March 2004	May 2004
Peep	April 2004	May 2004
Agobot	October 2002	May 2004
Lasku	January 2004	June 2004

Of course, some authors make the job of catching them a little easier:

Melissa	March 26, 1999	April 1, 1999
Blaster.B	August 13, 2003	August 29, 2003

Reduction

What remains to be seen is whether these men were involved in writing MyDoom or if they have connections to those authors. The likeness between the two worms is unmistakable. The original variants of Mytob carried mailing routines virtually identical to that of 2004’s successful SMTP worm. For example, the worms shared the subject and message text:

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.
```

The similarities in the mailing engine are also indicative of the two sharing the same source code structure.

Unlike the initial release of the MyDoom worm, however, the Mytob/Zotob families were immediately identified as money-making ventures. The authorities reporting on the recent arrests also noted that they believe the pair of authors was involved in a financially-motivated crime.

Release

The financial motive is still the critical element to these cases. As long as there is a significant return on investment for malware authors, there will continue to be malware. With each of these arrests, law enforcement gets another glimpse into the virus-for-profit world. That includes how big the profits actually are, how deep the enterprise runs in terms of human resources, and the management skills of the leaders. The Mytob/Zotob enterprise showed good awareness of how to reproduce a viable business process, and at a seemingly low cost. As details of this arrest and the arrested come to light, we will gain a better understanding of their processes and profits. These two have just as much to do with malware success as technical innovation.

References

"Mytob Infantry" http://www.infectionvectors.com/vectors/mytob_infantry.htm

Brian Krebs, "Suspected Worm Creators Arrested." Washington Post, 27 August 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/26/AR2005082601201.html.

Lasku Information, F-Secure
http://www.f-secure.com/v-descs/lasku.shtml

Peep Information, McAfee
http://vil.nai.com/vil/content/v_101140.htm

Agobot Information, infectionvectors
www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf

Blaster.B Information, Sophos
http://www.sophos.com/virusinfo/articles/blastersuspect.html