



Zotob Worm

infectionvectors.com

Updated August 17, 2005

Vector: Plug & Play Vulnerability in W2K Machines (Variant C attacks via ASN.1 exploit and mass mail)

Impact: High (system stability, complete control of victim system)

This worm attacks machines via the vulnerability described in MS05-039, the Plug and Play flaw released in August of 2005. The distribution of the worm occurred less than one week from the advisory.

Once resident on a system, the malware creates entries pointing to "botzor.exe" in the Registry to ensure that it starts up with the operating system. The name "BOTZOR" is also used as a mutex. Much like its cousins, the Mytob family, Zotob connects to an IRC control channel to allow backdoor access to the infected machine. In addition, the worm opens TCP 33333 for an FTP server, which servers the code to the next victim (much like Sasser).

Zotob spreads by randomly connecting to clients sharing the same first two octets as the infected system. It does this by attempting to open a connection to TCP 445. Where connections are made, the worm delivers the exploit code. If the system happens to be an unpatched Windows 2000 machine, the attack is likely to be successful – resulting in the target opening an FTP session on TCP 8888 and downloading the worm from the attacking machine (and, of course, executing the malware).

In addition to malicious HOSTS entries, establishing auto-startup, and launching a new attack of its own, the worm connects to:

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

In order to receive commands from its controller.

The worm also has 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!!!
```

Update: Zotob.B

This iteration uses the Registry entry “csm” for auto-start capabilities, otherwise this version looks like the initial release.

Update: Zotob.C

Adds the following string to the local HOSTS file:

```
Botzor2 pnp+asn+mail spread. Greetz to good friend Coder. Based on  
HellBot3. f-secure, sophos ok wait bitches!!!
```

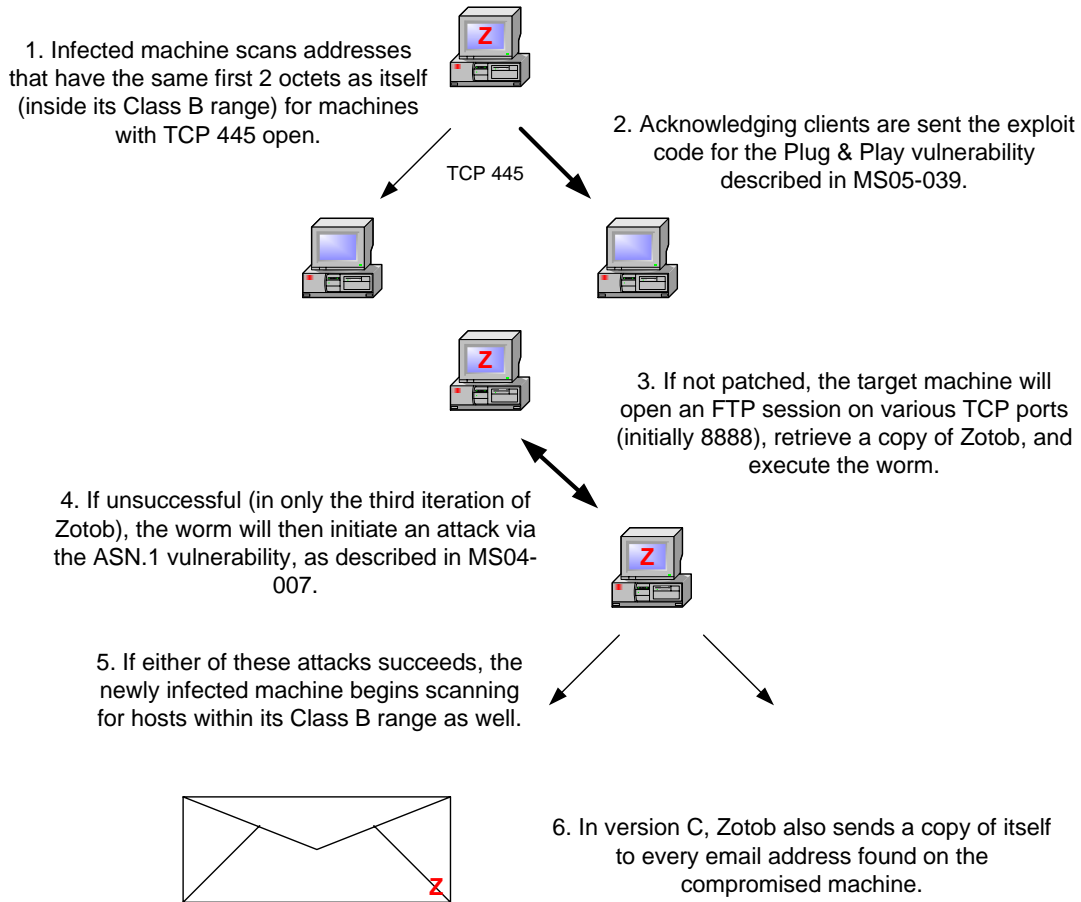
The worm carries an email propagation routine, making it nearly identical in form to Mytob. Moreover, the authors also added the ASN.1 exploit (MS04-007) from 2004 as a propagation mechanism. This version uses “PER.EXE” in the Registry to ensure auto start-up.

Update: Zotob.D

D adds four new IRC servers to the mix and some quality control: the worm checks for Internet connectivity by reaching out to Google, Yahoo, and EBay. Furthermore, if the infected machine’s IP address is one found in RFC 1918 (reserved space) the worm does not attempt to connect to any of the IRC servers. This version interestingly extends the number of adware/spyware-related applications it attempts to kill/delete. The kill list also includes former versions of itself.

Beginning with the fourth revision of the worm, many AV sites have begun classifying samples of this MS05-039 worm under different names. At this time, samples available to infectionvectors.com do not appear to require new names; as is seen below.

ZOTOB PROPAGATION



In each case, the infected machine then connects to an IRC channel, awaiting commands from its controllers.

infectionvectors.com 2005

Update: Zotob.E

This version switches from FTP to TFTP (a la Blaster) to move the worm code from victim to victim. Instead of a hostname, Zotob.E comes with a hard-coded IP address to use as the IRC server (72.20.27.115, and a channel named #tbp).

Update: Zotob.F

The IRC server changes from the one used in E to 72.20.41.139. The kill list for this iteration also includes former versions of Zotob.

Update: Malware competition

Initial versions of the Zotob worm are killed by competing Plug & Play – exploiting bots, including those commonly referred to as Sdbot and Codbot (source: F-Secure,

<http://www.f-secure.com/weblog/>). It appears that a battle, similar to that played out by mass mailers Bagle and Netsky last year, is underway. That is likely to have similar effects to the 2004 fight: quick releases of multiple, slightly-altered versions of code (coincidentally also harkening to the form employed by Mytob).

Information on other classifications of the MS05-039 worms from the last few days can be found at:

RBOT.CBR

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2ECBR&VSect=T>

IRCBOT.ES

http://www.f-secure.com/v-descs/ircbot_es.shtml

ESBOT.B

<http://securityresponse.symantec.com/avcenter/venc/data/w32.esbot.b.html>