

The Forensics of the Zotob Worm-Bot

By Rob Graham
Chief Scientist, X-Force® Research and Development

Copyright© 2005 Internet Security Systems, Inc. All rights reserved worldwide.



 **INTERNET | SECURITY | SYSTEMS®**
Ahead of the threat.™

ABSTRACT

Internet Security Systems (ISS) customers have been wondering what they should expect with regards to the Zotob worm because the behavior currently being exhibited is not the same behavior as past worms. This white paper describes why the Zotob worm behaves differently, why customers are experiencing different activity on the network and how ISS products can be configured to identify more details about this worm.

INTRODUCTION

Zotob is not a worm. It is universally described as such in the media, but it is not classified as a worm. Rather, it is a “bot.” The difference between a “bot” and a “worm” is equally as important as the difference between “worm” and “virus.”

What differentiates a bot from a worm? A bot spreads precisely under the control of the hacker who is controlling the network of bots. In contrast, a worm spreads out of control. As in the case of the first Internet worm, the “Morris Worm,” worms tend to spread much faster than their authors intend.

The reason bots are different from worms is that that “bot-hackers” want to profit from their creations. “Bot-hackers” are not content with simply having their code spread through the Internet. They want their code to do something useful, such as steal identities or credit card numbers, for example. They want to install keyloggers to capture people's passwords as they type them on the keyboard. They want to use their bot networks to send out spam. They want to keep control of the infected machines in order to do something nefarious later.

One aspect of direct hacker control is that bot infections are much more dangerous to a company than worm infections. A desktop machine infected with a worm is just an annoyance, but a desktop machine infected with a bot means that the hacker has control of your network from behind the firewall.

Another aspect of this control is that the bot doesn't spread wildly. Indeed, the hacker may turn off the bot network and make all of those machines go silent. Thus, if you see all activity stop, it doesn't necessarily mean you've cleaned all the machines.

The last aspect of this control is that bots don't spew out packets everywhere. The vast majority of bots are infecting only local networks and are not spreading behind their local domains.

NO EVIDENCE OF PLUGANDPLAY_BO SECURITY EVENTS

Due to the critical nature of this vulnerability, ISS X-Force security intelligence team has spent a considerable amount of time investigating this issue with customers to assure them that they are properly protected.

ISS customers using products that contain the PlugAndPlay_Bo virtual patch should see the “PlugAndPlay_BO” event when somebody attacks the MS05-039 vulnerability. However, many ISS customers are not seeing these events as they would expect. We have found the reason that Proventia® appliances are not detecting the PlugAndPlay_BO events is because the bot is not sending events where the sensor can see them.

By default, the bots scan only the local (16) Class B address space. For large organizations, this means all the traffic is internal to their network. For small networks, this means that while they see some external traffic, it is just going to their cyber-neighbors, not the entire Internet. In most cases, your neighbors have good firewalls. This means that while the bot is scanning, trying to connect to port 445 on the neighbors' machines, it isn't succeeding. The bot must get a successful connection to send the exploit. Put simply, no PlugAndPlay exploit attempt, no PlugAndPlay_BO event.

On an external Internet connection, you should just be seeing events related to the failed connection attempts, such as TCP_Service_Sweep and TCP_Network_Sweep. Most customers should never see the PlugAndPlay_BO event.

Of course, if network-based IDS/IPS sensors such as the Proventia intrusion prevention appliance, the Proventia integrated security appliance or the Proventia intrusion detection appliance are placed within the core of the network infrastructure, then PlugAndPlay_BO events should appear.

TRACKING IRC ACTIVITY

There is one additional item that can be tracked on the external network: the IRC channel used to control the bots. Remember that the difference between bots and worms is that the hacker has the bots under control. Even though it is unlikely customers will identify the exploit activity the bots use to spread on the Internet connection, customers should be able to see activity on the control channel between the bots and the hacker.

The bots utilize the Internet Relay Chat (IRC) protocol. IRC is the “chat protocol” precursor to AOL Instant Messenger, MSN Messenger and Yahoo Messenger. It is still the preferred chat system for computer geeks, especially hackers. Hackers like to use chat protocols to control their bots because it provides them with “anonymous” control over the bots. The hackers don't directly control the bots from their personal machine, but instead control them through one or more intermediary chat servers. Since many of these chat servers are in countries with relaxed cyber-crime laws, the hackers are effectively shielded from law enforcement.

Proventia appliances include extensive signatures security content for tracking IRC activity. The simplest signature security decode is “IRC_Join,” which tracks all attempts to start an IRC session. This is what ISS calls an “audit” event. An IRC JOIN command is not a hostile attack and is a perfectly normal part of the IRC protocol. However, if your company does not use IRC, then any IRC traffic may be hostile. Even if your company does use IRC, it is likely that only a few servers are used, which can be added to a white-list and ignored. Using audit signatures events will help track suspicious traffic.

In the case of the Zotob bot, ISS recommends that customers turn on the IRC_Join audit event, then examine the events and adjust the sensors to ignore legitimate IRC traffic, if there is any. This should easily find any bot infections on your network.

Note that Proventia appliances are “port agnostic” for protocols. The bots run IRC on many different ports, including ones normally associated with other protocols. For example, port 8080 is frequently used for HTTP traffic, but the Zotob bot puts its IRC traffic on that port. A firewall is focused on ports, and cannot block such traffic with port rules. However, an IPS like the Proventia intrusion prevention appliance or the Proventia integrated security appliance can block the traffic on any port. Turning on blocking for the IRC_Join audit event will effectively stop all further communication between your bot-infected machines and the hacker controlling them.

TRACKING THE SOURCE OF THE INFECTION

If the bot attacks only the local Class B subnet, then how does it jump to other subnets? While working with customers over the last couple days, ISS believes we have a good answer to this question.

In many cases, the infections come from unprotected and vulnerable VPN desktops and notebooks brought inside the firewall. The desktop or notebook became infected while “outside” the corporate firewall, and then started scanning the new internal corporate address space as soon as it was brought inside the firewall. An important note is that laptops and VPN-connected desktops protected by Proventia Desktop are protected from the bot infection, avoiding infection of the corporate network.

Another source seems to be prior infections by bots. These bots are not new, but are instead (usually) an older bot with only the added PlugAndPlay exploit applied to them. If the hacker already has control over a machine, he can simply update the bot software to the new version, and tell it to start scanning.

Few people realize it, but after the Blaster and Sasser worms, the exploits those worms used were likewise added to the first bots. The noise generated by the worms drowned out the noise generated by the bots using the same exploits, so customers didn't realize they had bot infections. The bot-hackers simply told their bots to go quiet after awhile. Corporations cleaned their worm infections by tracking only active machines. Any inactive, but bot-infected, machine was ignored. Many corporations have potentially been harboring bots for a couple of years. Monitoring for service sweeps, like SMB service sweeps, are helpful in identifying bot-infected hosts.

ABOUT THE PLUGANDPLAY_BO SECURITY EVENT

ISS has verified that the original vulnerability-based Virtual Patch™ technology released on April 13, 2005 to preemptively protect customers from exploits of the Windows Plug and Play vulnerability (MS05-039) is 100% effective against all known exploits. Additionally, the same Virtual Patch technology already deployed to Proventia intrusion prevention appliance, the Proventia integrated security and Proventia Desktop products is also completely effective and prevents infection by all current variants of the Zotob worm-bot, which uses the Windows Plug and Play vulnerability to propagate.

Because ISS could conceivably make an error in the protocol decode, or the vulnerability analysis could be incomplete, we take it very seriously when customers report that they aren't seeing PlugAndPlay_BO events when they think they should. However, in every case investigated so far regarding the Windows Plug and Play vulnerability, the algorithm has been proven accurate.

ABOUT ISS' RESEARCH AND PROTECTION METHODOLOGY

ISS' Proventia line of security appliances and software is based upon a different technology than the products from other vendors. Rather than using traditional "pattern-matching," the Proventia appliances utilize "protocol-analysis" technology. Protocol analysis technology breaks down the traffic field-by-field, much like a Sniffer or Ethereal product.

At the bottom layer, every product includes an Ethernet, IP, TCP protocol decode layer. Proventia continues that process by decoding NetBIOS, SMB, NamedPipes, and MS-RPC. The PlugAndPlay protocol in question is based upon MS-RPC over NamedPipes.

The ISS X-Force research and development team focuses on vulnerability research. The X-Force team reads the binary computer code to determine exactly how the vulnerability worked. This is typically how X-Force writes all of the ISS security content. Whenever a new vulnerability is announced, X-Force looks at the machine code, figures out the details and then writes a protocol-analysis signature that triggers on the vulnerability.

Whereas IDS/IPS products typically wait for exploits to appear before writing signatures, ISS' security content usually appears before exploits. This has been the case for CodeRed, Nimble, Slammer, Blaster, Sasser and many other critical Internet threats. ISS researchers figured out the details of the vulnerability before the hackers did, and long before competing vendors understood the vulnerability. The result is that ISS ships protection *before* exploits appear.

CONCLUSION

Customers worried by the lack of evidence of PlugAndPlay_BO events on their Internet connections where they normally place network-based IDS/IPS appliances can rest assured that the Proventia appliances are behaving normally. The reason no PlugAndPlay_BO events are seen is because nothing is appearing on those network segments that would trigger the event. While this would be unusual for a worm, this is perfectly normal behavior for a bot.

Since scanning of hosts does not attempt to exploit the Windows Plug and Play vulnerability, additional security events should be monitored for signs of worm-bot scanning activity. A list of security events that should be enabled to block propagation and detect worm-bot scanning are detailed in the X-Force advisory named Windows Plug and Play Remote Compromise. This advisory is available at <http://xforce.iss.net/xforce/alerts/id/202>.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

Copyright© 2005 Internet Security Systems, Inc. All rights reserved worldwide

Internet Security Systems, Virtual Patch, and Ahead of the Threat are trademarks, and the Internet Security Systems logo, X-Force and Proventia are registered trademarks of Internet Security Systems, Inc. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

Distribution: General
MC-WRLSSWP-0805