



## Vulnerability Exploits Break Records

*Once measured in months, exploits can now appear within days of a vulnerability announcement.*

A Special Report by Trend Micro

According to security experts at antivirus and content security firm Trend Micro, the bot attacks that occurred on August 16, 2005 were not completely unexpected, but rather were the culmination of a growing trend among malware writers. Pointing to the prevalence of information and the open availability of malicious code posted on public Internet sites, researchers at Trend Micro have long noted the closing gap between the discovery of a new vulnerability and the time corresponding exploits appear.

David Perry, Global Director of Education at Trend Micro, has been warning corporate and government security officials for more than two years about this shrinking timeframe. "In 2000-2001, it took 11 months from the time MS00-078 was announced until the time NIMDA was written as an effective exploit against that vulnerability," Perry said. "By 2002, that timeline was cut nearly in half, with only 185 days required between the announcement of MS02-039 and the successful launch of SQLSlammer. Just six months later, MSBLAST did it in less than a month; and last year, we saw SASSER arrive in just 17 days."

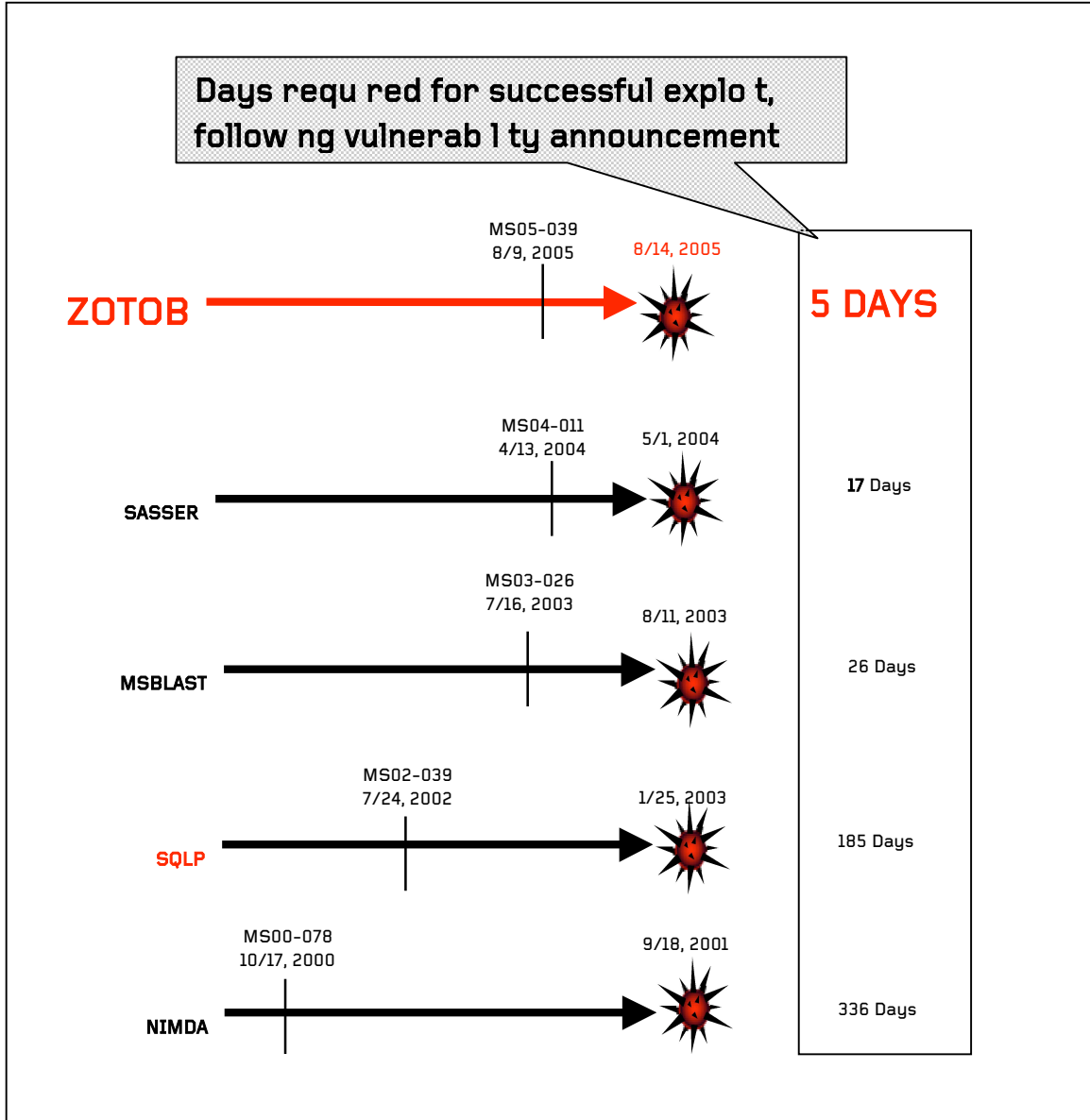
The recent ZOTOB outbreaks have validated Perry's analysis – and set a dubious record in the process – requiring only five days from vulnerability to successful exploit.

Although WORM\_ZOTOB.D received the most attention, it was just one of six ZOTOB variants that struck within the same period. Furthermore, ZOTOB is only one of four bot families that appeared within the four-day period. The other three families are:

- WORM\_DRUDGEBOT
- WORM\_RBOT
- WORM\_ESBOT

In all, more than 20 worms surfaced in the four days, of which six were WORM\_ZOBOT variants. All of these worms are believed to utilize one of three known MS05-039 exploits, each of which was posted to well-known, publicly available sites for posting and viewing new exploits.

Figure 1: Historical Timeline Between Vulnerability Announcement And Exploit



Source: Trend Micro

### The Exploit Timeline

Security experts noted a great deal of activity immediately after the Microsoft announcement and throughout the ensuing week:

- **August 9, 2005:**
  - Release of Microsoft Vulnerability reports MS05-038 and MS05-039
  - Proof-of-concept exploit for MS05-038 and posted to a popular site for viewing and posting new exploits
  - First publicly known exploit for MS05-039 and posted to the same site

- **August 11, 2005:**
  - Second exploit code posted to another popular site for viewing and posting new exploits
- **August 13, 2005:**

Second exploit code posted to another popular site for viewing and posting new exploits – this time by the same group responsible for the LSASS exploit code most commonly utilized by SASSER, the MYTOB family, and other bots.
- **August 14, 2005:**
  - First bot sample that utilizes MS05-039 exploit code received
  - First samples of WORM\_ZOTOB.A and WORM\_ZOTOB.B are received
- **August 15, 2005:**
  - A Web site utilizing a MS05-038 vulnerability is discovered in the wild
  - First samples of WORM\_ZOTOB.C are received
- **August 16, 2005:**
  - First samples of the following 5 bot-enabled worms are received:
    - WORM\_ZOTOB.D
    - WORM\_RBOT.CBQ
    - WORM\_RBOT.CBR
    - WORM\_SDBOT.BZH
    - WORM\_DRUDGEBOT.A
  - Widespread infections are reported worldwide involving the ZOTOB family of worms and WORM\_RBOT.CBQ, triggering the Global risk alert level to be raised to “medium”.

### From Vulnerability to Exploit, In Three Easy Steps

So how did we get to the point where a successful exploit could become available within a few days of a public announcement? According to Perry, in just three easy steps:

1. A Microsoft Security Bulletin is released, warning users that Internet Explorer has a flaw, which enables exploitation in the way it handles certain tasks or objects.
2. A malware writer can use the publicly known details listed in the bulletin to write code that exploits the newly announced vulnerability.
3. Once the exploit tests positively, the writer can then merge the code with existing code functionality from publicly available malware that has already been proven effective. This creates a brand new malware family, with relatively little work on the part of a skilled writer.

Perry said he expects exploits such as this to become more prevalent.

“It is a very good thing that a vendor can admit to fault and produce patches to close the security holes inherent in a given process, and we applaud every effort to make the world a more secure place,” he said. “But as good as the notifications are for the general public, they also have the negative side effect of informing the writers. Since the security bulletins list detailed information

on the vulnerability, a knowledgeable writer can quickly and easily use information intended to protect users to achieve the opposite.”

### **Resurgence of the “Bot Network”**

In addition to the simplicity with which new malware can be written, as detailed above, the alerts were largely the result of the worms’ capabilities to propagate via a network of “zombie” computers, which have been infected without the user’s knowledge. These networks are referred to as “bot networks”. Bot-enabled worms are often nicknamed “bots”.

According to Joe Hartmann, Director of the Anti-Virus Research Group at Trend Micro, there are multiple variants from multiple authors.

“On August 16<sup>th</sup>, we saw six different bots from four different malware families, which all utilized the same exploit code,” Hartmann said. “They all had the same core functionality but added new code functionality, such as a mass mailer. This helped lead to broader global proliferation for some of the variants.”

Security experts like Hartmann and Perry add that this technique is common among malware writers. The original exploit code is written and posted to a public Internet site, then the other writers append additional functionality, such as more advanced seeding and propagation techniques, to make the malware more pervasive and advanced.

### **The Significance of the Timeline to Bot Networks**

The speed with which a writer can exploit vulnerabilities is absolutely essential to a successful bot attack, for two reasons. First, there is typically only a 30- to 90-day window of opportunity between the announcement of a vulnerability and the point at which the majority of computers are patched to successfully infect the systems. Second, there are a number of different groups of writers each competing to build their own bot networks. The writers know that time is of the essence, because once the code gets into one group’s bots, there are fewer systems that other groups can infect.

As a result, once a vulnerability is announced, writers are highly motivated to create their exploit code and release it into the wild as quickly as possible, to maximize the effectiveness of the attack.

### **A Glimpse Into the Future – A Vicious Cycle**

According to Bruce Hughes, senior research engineer with Trend Micro, most bots continuously exploit the same vulnerabilities.

“When a company gets infected, they respond by patching their systems against that vulnerability and likely are never infected again,” Hughes said. “However, a new vulnerability makes them targets again.”

Pointing again to both the speed with which the exploit was written, as well as the use of modular code, Hughes points to the success of WORM\_SASSER and WORM\_BLAZER. Like the recent ZOTOB infections, these exploits were added to existing bots very quickly after the vulnerabilities were announced. Although the first variants had limited success, Hughes warns that later variants were far more successful, and they even infiltrated a number of high-profile corporations.

“A number of large companies – and even high-profile media organizations – were hit with these worms,” Hughes said. “Not only did these worms likely add extensively to their networks, but the amount of attention they received can be a pretty powerful motivator as well. Many writers engage in this kind of activity to gain public notoriety.”

### **Learn How to Protect Yourself – From These and Other Threats**

Security experts warn that there may be more attacks that are based on these vulnerabilities – and that, as always, end-user vigilance is the best defense. This includes keeping up with the latest Microsoft patches, maintaining current antivirus definitions, and using sound judgment.

Below is more specific advice, for each of these two vulnerabilities:

#### **MS05-038**

Although there are a number of vehicles to lure users into visiting the site, researchers believe the most common way will be through via email, coupled with social engineering techniques that have already proven to be effective.

To safeguard against this threat, security experts at Trend Micro offer the following advice:

1. Increase your security settings on your browser. The higher the settings, the less a potential attacker can accomplish – if he can get in at all.
2. Limit your user rights when online. Using these vulnerabilities, a malicious user can typically only work under the same rights as the legitimate user. Hence, if the legitimate user logs in with only standard user privileges, the malicious user would only be able to obtain those same privileges. In contrast, if the user is logged-in with administrator privileges, the malicious user could potentially gain full control of the user’s system.
3. Change your email preferences to:
  - a. disable automatic download when previewing the message
  - b. block pictures and other Internet content (including HTML) from automatically downloading to your computer
4. Use safe email practices, including abstaining from clicking on any embedded links
5. Abstain from launching attachments that appear to be pictures or other files from an unknown source, as well as from people you know, if the attachment was unexpected. When in doubt, ask the person if they sent you anything, prior to opening *any* attachment.

#### **MS05-039**

Security experts at Trend Micro recommend that users take the following measures to protect against these and other attacks:

- Ensure your system is patched with the most current Microsoft system update.
- Ensure your antivirus definitions are up-to-date. To remove the manual burden of doing this, most antivirus companies offer an automated update option within their security product.

## >> TREND MICRO: VULNERABILITY EXPLOITS BREAK RECORDS

- Trend Micro offers HouseCall, a free virus scanning service, available at <http://housecall.trendmicro.com>. Existing Trend Micro PC-cillin customers can also utilize the network virus wall and vulnerability assessment modules\*, which are built into the product, to help keep their system updated.

\* The Network Viruswall (NVW) pattern stops this worm from spreading throughout the network and infecting other machines. A network that is protected by the NVW pattern is assured that any instance or presence of the code at the network layer is immediately filtered out before it causes any damage.

The Vulnerability Assessment (VA) pattern detects all machines in the network that have not yet been patched against the vulnerability used by these worms. Hence, system administrators can immediately be notified of the machines that must be protected against these attacks, and proper steps can be taken to assure that damage is not magnified on the network scale.

### **For Additional Information**

To learn more about the MS05-038 and MS05-039 Microsoft Security Bulletins and get more complete advice for how to protect yourself against these vulnerabilities, refer to the [Trend Micro Security Information Center](#).

---

### **About Trend Micro**

Trend Micro Inc. provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious codes at a central access point before they reach the desktop.