



ZOTOB Worm: Day Zero Defense!

By Jeff Kopp, CISSP

August 2005 saw yet another event in which a malicious code writer succeeded in disrupting the daily activities of PC users across the globe. The ZOTOB worm caused thousands of PCs at some of the largest companies in the world to shutdown, causing countless millions of dollars in downtime and extra IT costs to remediate the situation. Yet, we must realize that this was not an isolated event, but simply the next step in the ever-evolving world of Internet related threats. So what went wrong? Why was it so successful? How do we defend against future threats like ZOTOB?

First, a little background information. The second Tuesday of the month, "Patch Tuesday" as it is dubbed, came on August 9, 2005. This is the day of the month that Microsoft releases its product patches, and was the first announcement of a new vulnerability in its Windows Plug and Play service that could allow a remote attacker to execute code on an unpatched system. Five days later, the ZOTOB worm was released into the wild, and a few hours later, the world was feeling its effects. The turnaround between vulnerability announcement and code release into the wild was staggering, just 5 days. This didn't leave system administrators much time to patch their systems, and unfortunately, this is going to be the norm, rather than the exception from here on out. So how does this worm work?

Well, it doesn't work, if you are behind a firewall that is blocking port 445, unless the threat comes from inside the network. With most networks these days having more than one entry and exit point, an internal threat is very probable. An entry or exit point could be a VPN to a partners network, a backup Internet connection, a VPN user at a remote site, or simply a mobile user bringing his/her laptop back to work after a business trip, or a weekend. All of these scenarios can result in exposure to potential threats and **MUST** be mitigated in some way. Let's take the example of the remote worker and see how the ZOTOB worm could be successful.

Our fictional user, Joe, a sales rep, has a high-speed Internet connection at home and regularly uses hotspots around town to check email and update his CRM app, as he travels between customer's sites. His corporate laptop has anti-virus software installed, and is kept up-to-date by the IT group via login scripts and automatic software loads from the corporate network, and Joe is very good about not browsing personal websites on his corporate laptop. He is also diligent about using his corporate VPN to connect at these hotspots for secure communications back to the corporate network. So, how could Joe still get infected, and worse, be the seed for spreading the infection to his corporate network?

- VPN's aren't bullet proof

VPNs encrypt data over insecure networks (hotspots, hotels, home, etc.) to prevent unauthorized users from accessing that data, but they do not filter that data for threats. So while Joe is safe from eavesdropping, the network worm can still spread, even over this encrypted tunnel back to the corporate network.

- Anti-virus definition delays

With the threat emerging only 5 days after the vulnerability was released, and with up to 20 variants spreading so rapidly, chances are good that anti-virus definitions are not the most current, leaving Joe susceptible.

- The ZOTOB worm, self replicates, without needing ANY user interaction

This means that if your PC is plugged into a public network, it is vulnerable. Joe could have been infected as soon as he booted up on the hotspot network, before he connected to his corporate VPN. He could also have been infected at home while directly connected to his cable modem. In this case, it wasn't Joe's doing that did him in; he was completely unaware of the worm's activities.

- Elevated privileges may be the culprit

Most laptop users, even in large corporate environments have elevated privileges to their laptops (admin, power user, etc.). These elevated privileges allow the user to install applications as they need them. Unfortunately, it allows any code run on that laptop to be run using those elevated privileges. If the attacker is able to take advantage of a backdoor into your system and get code to run on your system, then the attacker's code is able to use Joe's elevated privileges, or the local system account in the case of ZOTOB, to silently install itself and run further operations. As soon as Joe connects to his corporate VPN, now the worm has an avenue to spread directly to the rest of the corporate network.

Other factors:

- Many IT departments do not keep up-to-date on their software patches. Even 5 days out of date, in this case, can prove costly. Patches are thoroughly tested prior to release. This is not to say that it will not conflict with your installed applications, but chances are much less than years past. Always test before applying patches to a production environment, just be quick about it.
- Most corporate VPNs enforce data encryption, but are unfiltered connections that allow ALL kinds of data to be passed through the tunnel. VPNs need to be viewed as an entry point for attacks, just like your main Internet connection. Filter and defend appropriately.
- Removing unnecessary user privileges could have prevented this worm from installing and shutting down the PC, but many IT departments think it is easier just to give the user full privilege to avoid future calls to install software apps (which they will still probably get called for anyway).
- Even if Joe's laptop was infected, and he spread the infection to every other PC on the corporate network, those PCs still had to be able to communicate back to the attacker to get their next instructions (to shutdown the PCs) and to get updated worm files (the attackers way to update his new "bot"). In the case of ZOTOB, this required an outbound port 8080 to be open, as well as an uncommon FTP port, neither of which should have been open in the first place. A secure firewall implementation would have prevented this network worm from doing anything else, at least until the laptop was moved to a network that allowed this traffic through the firewall.



So how do we defend against ZOTOB-like worms in the future? Signature-based security software and appliances are limited by the time it takes for the threat to be identified, a signature written for this threat, testing and dissemination of that signature to all hosts. With zero-day threats and rapidly emerging worms such as ZOTOB, this time window may not be acceptable. Enter the behavior-based appliance (see [In-Depth Security website](#) for more details). These appliances sit at the core of the internal network and listen to all LAN subnets passively. This new breed of appliance does not filter based on known signatures, but rather uses several methods of behavioral detection to detect malicious network activities, thus filtering for known AND unknown malicious activity. Once a malicious host is determined, it can be safely isolated without requiring VLAN reconfiguration to effectively neutralize any further network activity from that host. At the very least, all VPN traffic should be filtered for known threats. Do not allow VPN traffic to spill, unfiltered into the corporate network. Limit user's PC privileges, thus limiting the worm's privileges. Block unnecessary firewall ports inbound AND OUTBOUND. And PATCH, PATCH, PATCH!!

As today's threat landscape evolves, so must the countermeasures. With threats being created and spreading faster, signatures will eventually prove useless in defense against these rapidly emerging threats. The only way to detect malicious network activity is to be looking for malicious network behavior patterns. We cannot assume that our firewall is the last line of defense. With so many entry points for threats on our corporate networks, we must assume at all times that a worm is already somewhere on our LAN and we must constantly defend against its spread. Finally, before spending significant money trying to mitigate these risks, consult a network security professional. Their expertise could save you thousands of dollars by implementing a solution that will defend against today's AND tomorrow's threats.