

## Re: [Full-disclosure] Zotob Worm Remover

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0772.html>

---

**From:** MadHat ([madhat\\_at\\_unspecific.com](mailto:madhat_at_unspecific.com))

**Date:** 08/23/05

Date: Tue, 23 Aug 2005 14:59:56 -0500  
To: Todd Towles <[toddtowles@brookshires.com](mailto:toddtowles@brookshires.com)>

On Aug 22, 2005, at 4:44 PM, Todd Towles wrote:

> *James, I agree with you.*  
>  
> *It was n3td3v that stated the following – "The wireless devices were*  
> *most likely the primary source of the spread. Media outlets are*  
> *reporting wireless devices were only an accessory to the spread of the*  
> *worm."*

I think he meant wireless is an easy initial attack vector to get things into a corporate network. It can be easier and more focused. You can sit at starbucks or the airport and easily attack machines that are open due to the fact that they are used to being behind other protections. Yes defense in depth is the best method, but looking at reality instead of "a perfect world" type situation, it is common for machines to not be patched in a timely manner. In this case the code was out there fairly quick after the patch was released. The easiest way to attack a protected network is through portable devices. Now you can scan DSL or dialup space for vulnerable machines, or you can go take a flight from SJC and get dozens in a short time. And because of the location, you have a good idea that at least some of them will be working for large companies that do work in the bay area...

I am not disagreeing that it is not all about wireless, but people do tend to open themselves up on wireless networks more than on wired. SBC now provides a DSL firewall/router that would protect against this attack by default. Some larger ISPs are blocking ports from the Internet for DHCP or PPOE accounts, but you go to starbucks and everyone is jumping on any open network. Just go and fire up a strong card with an AdHock network with the same SSID and assign them an IP and you can compromise them, plant the worm, disconnect and you are gone... to them it is a blip in the wireless, and will just shrug it off and go on about their business.

See shmoo for common rants on wireless.

>

Full-Disclosure: Re: [Full-disclosure] Zotob Worm Remover

> *I agree with Jan, that host based IPS could have stopped this. Cisco's  
> CSA is a good example of this type of technology. Host based IPS  
> system  
> are commonly seen as anti-rootkit solutions, which is also a very very  
> good thing to have. But patch management should not be overlooked just  
> because you have a host IPS. The host IPS will give you time to patch,  
> but patch management is the last line of defense for vulns. I never  
> said  
> it should be the first or only line of defense.*

>  
> *I am very firm believer in the defense in depth methodology.*

>  
> *-Todd*

>  
>

>> -----Original Message-----

>> *From: James Tucker [mailto:jftucker@gmail.com]*

>> *Sent: Monday, August 22, 2005 4:08 PM*

>> *To: Todd Towles*

>> *Cc: Ron DuFresne; full-disclosure@lists.grok.org.uk*

>> *Subject: Re: [Full-disclosure] Zotob Worm Remover*

>>

>> *It seems to me that the attack was less than a week old from  
>> the start date. Default settings on a relatively unchanged  
>> box would provide a suitable window of opportunity given the  
>> availability of the worm to the deployer. This is more  
>> important than network connectivity, which is not of security  
>> concern as this is not the exploited layer. Disconnecting  
>> networks is what you suggest when you're in trouble, not when  
>> you're trying to maintain the daily balance of cost vs  
>> function. Moreover, wireless is recieving the blame – however  
>> this will only continue whilst your laptop is the device you  
>> are using. Eventually will you blame the mobile phone  
>> companies for allowing "dangerous traffic" to flow through  
>> the repeaters? What about sattelite links – should we filter  
>> those and knock the latency up another notch? No, it's the  
>> software, once again.  
>> Connectivity increases exposure, it doesn't decrease security  
>> – the two are not one and the same. 1000 laptops in a city  
>> centre network becoming infected less than a week from update  
>> release would be unsurprising  
>> (read: defaults are once a week at 3). The security of these  
>> laptops was not compromised by the wireless presence, it was  
>> a medium of travel only. Now lets say, we go back in time and  
>> remove all of the wireless NIC's. Now, there are only 750  
>> laptops cause we can't generate as much revenue (joke), and  
>> of these they're all still connected, just with a different  
>> medium. The medium is (specification)centralised and routable  
>> in the same manner (ah, so the medium can have 'implications'  
>> ;) – the infection rate is the same. Why? because they are  
>> all connected. It's BEING CONNECTED not BEING WIRELESS that's*

Full-Disclosure: Re: [Full-disclosure] Zotob Worm Remover

>> *the issue here. Yes you may argue, pointlessly however, that*  
>> *wireless has increased average connectivity, however once*  
>> *again, this is only a medium. It's business/personal drive*  
>> *that requires connectedness, not the technology itself.*  
>>  
>> *Todd Towles wrote:*  
>>  
>>> *This is correct for the first day, maybe two. Then*  
>>>  
>> *unpatched laptops*  
>>  
>>> *leave the corporate network, hit the internet outside the*  
>>>  
>> *firewall and*  
>>  
>>> *then bring the worm back right to the heart of the network the very*  
>>> *next day, bypassing the firewall all together. Firewall is just one*  
>>> *step..it isn't a solve all. Patching would be the only way to stop*  
>>> *this threat in all vectors. That was my point.*  
>>>  
>>> *If you aren't blocking 445 on the border of your network, you have*  
>>> *must worse problems with Zotob.*  
>>>  
>>>  
>>>  
>>>> *-----Original Message-----*  
>>>> *From: Ron DuFresne [mailto:dufresne@winternet.com]*  
>>>> *Sent: Monday, August 22, 2005 3:15 PM*  
>>>> *To: Todd Towles*  
>>>> *Cc: n3td3v; full-disclosure@lists.grok.org.uk*  
>>>> *Subject: RE: [Full-disclosure] Zotob Worm Remover*  
>>>>  
>>>> *On Mon, 22 Aug 2005, Todd Towles wrote:*  
>>>>  
>>>>  
>>>>  
>>>>> *Wireless really isn't a issue. You can get a worm from a*  
>>>>>  
>>>>  
>>>> *cat 5 as easy*  
>>>>  
>>>>  
>>>>> *as you can from wireless. The problem was they weren't*  
>>>>>  
>> *patched. Why*  
>>  
>>>>> *weren't they patched? Perhaps Change policy slowed them*  
>>>>>  
>>>>  
>>>> *down, perhaps*  
>>>>

Full-Disclosure: Re: [Full-disclosure] Zotob Worm Remover

>>>>  
>>>>> *it was the fear of broken programs..perhaps it was the QA*  
>>>>>  
>> *group..it*  
>>  
>>>>> *doesn't really matter. They go the worm because they were*  
>>>>>  
>>>>  
>>>> *not patched.*  
>>>>  
>>>> *And because they didn't properly filter port 445 is my*  
>>>>  
>> *understanding.*  
>>  
>>>> *Unpatched systems behind FW's that fliter 445 were untouched.*  
>>>>  
>>>> *Thanks,*  
>>>>  
>>>> *Ron DuFresne*  
>>>> --  
>>>> *"Sometimes you get the blues because your baby leaves you.*  
>>>> *Sometimes you get'em 'cause she comes back." --B.B. King*  
>>>> *\*\*\*testing, only testing, and damn good at it too!\*\*\**  
>>>>  
>>>> *OK, so you're a Ph.D. Just don't touch anything.*  
>>>>  
>>>>  
>>>>  
>>>>  
>>>>  
>>>>  
>>>>  
>>>> \_\_\_\_\_  
>>> *Full-Disclosure - We believe in it.*  
>>> *Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>*  
>>> *Hosted and sponsored by Secunia - <http://secunia.com/>*  
>>>  
>>>  
>>  
>>  
>>  
> \_\_\_\_\_  
> *Full-Disclosure - We believe in it.*  
> *Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>*  
> *Hosted and sponsored by Secunia - <http://secunia.com/>*  
>  
>

--  
MadHat (at) Unspecific.com, C<sup>2</sup>ISSP  
E786 7B30 7534 DCC2 94D5 91DE E922 0B21 9DDC 3E98  
pgp --keyserver wwwkeys.us.pgp.net --recv-keys 9DDC3E98

Full-Disclosure - We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Full-Disclosure: Re: [Full-disclosure] Zotob Worm Remover

Hosted and sponsored by Secunia - <http://secunia.com/>