

Re: Spammers die!

Source: <http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.misc/2004-05/1005.html>

From: Jason McClellan (jason_mcc_at_obsfucated.myrealbox.com)

Date: 05/29/04

Date: Sat, 29 May 2004 02:32:40 -0400

Well I checked the security event log.. and it seems this is what was going on! There are repeated Account Logon 680, Logon/Logoff 540, Privilege Use 576, and Logon/Logoff 538 events, on the Guest account, starting at 6:06am and ending when I disabled the guest account.

What is surprising (in a strange sort of way) is that I installed Exchange 2 weeks ago, and it took the spammers (pronounced – "scum of the earth") this long to exploit this! Also, once discovered, I'm somewhat surprised they didn't inundate me with junk.. I have a 4000/1000 kbps internet connection, but from the looks of my logs, my mail server only processed about 2500 messages over the whole day.. well, I know a typical business day sees about 400 messages coming in normally. I also know that I got about 1970 NDR's from my exchange box for undeliverable spams, and I deleted at least 80 from the queue.

We had guest enabled some time ago, and prior to Exchange, it wasn't an issue.. it just didn't occur to me, but it makes complete sense of course.. I sure feel stupid! :(

Thanks for everyone's suggestions!

"Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message news:udS1RiTREHA.3452@TK2MSFTNGP10.phx.gbl...

> *The "guest" account requires no password to authenticate...*

>

> *Someone can authenticate to your fileserver, or any other resource, without*

> *having to supply a password. That's why the guest account is *disabled* on*

> *all Windows server OSes. Only enable it if you have a specific reason to do*

> *so, and you are aware of the consequences...*

>

> *Cheers*

> *Ken*

>

> "Jason McClellan" <jason_mcc@obsfucated.myrealbox.com> wrote in message

> news:%23KyfLgRREHA.2404@TK2MSFTNGP09.phx.gbl...

Re: Spammers die!

> :
> : *Nice to know.. but the guest account was never an issue before having*
> : *installed Exchange.. is there a KB article on this or something?*
> :
> :
> : *"Peter D. Hipson" <mcn01 at hipson dot net> wrote in message*
> : *news:2ujfb0p35u87olkoaab22hsnpeorlhllvn@4ax.com...*
> : > *Just as a matter for form, you should never enable the guest*
> : > *account(s)! (for this very reason...)*
> : >
> : > *On Fri, 28 May 2004 17:21:21 -0400, "Jason McClellan"*
> : > *<jason_mcc@obsfucated.myrealbox.com> wrote:*
> : >
> : > >
> : >
> : > *>Is there some exploit that involves the guest account? I have*
disabled
> : *the*
> : > *>guest account, just for the hell of it, and the junk seems to be*
drying
> : *up..*
> : > >
> : > *>Jason*
> : >
> : > *PeterD, the Darkstar Network*
> : > *To email, fix my address!*
> : > *ExpertZone!*
> :
> :
>
>