

RE: Strange Attack On A Webserver I Work On

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-10/0032.html>

From: Filipe Varela (filipe.varela_at_esviagens.com)

Date: 10/27/04

To: <focus-linux@securityfocus.com>

Date: Wed, 27 Oct 2004 10:41:27 +0100

Hello

I have no suggestions whatsoever as to what they were thinking but i'll translate the strings. Im pretty sure it won't help at all as i'm convinced it was just a "routine" attack but here it goes...

Translation next to original text in original post (below)

Cheers,
Filipe

----- Original Message -----

From: "Matthew J. Sahagian" <gent@dotink.org>

To: <focus-linux@securityfocus.com>

Sent: Wednesday, October 27, 2004 2:30 AM

Subject: Strange Attack On A Webserver I Work On

> *Hello, I'm a long time reader of this list and have never really had the need to post here. However, recently a webserver that I do minimal administrative work for was attacked. We're still unsure exactly what had been done. Most of the logs have been either cleaned or wiped completely (either by log rotate or by the attacker). I was gone for the weekend so I sorta came back to this. I don't really have questions about the attack per se, we're doing pretty well at the recovery process.... one question I do have however is this.*

>

> *The attacker (either manually or using a program) replaced all index.html/htm and index.php files they had permission to replace with a UDP flooder. I extracted some of the information from the flooder using the strings program and heres what I get:*

>

> *!HELP! beta version. //TRANSLATION:*

> *!HELP!*

> *!HELP! #brazil@efnet - eleet team*

> *!HELP! + code by bonny ::: bonny@hacker.com.br*

>

> *!CREDITS! * creditos aos amigos e a quem me ajudou. //TRANSLATION: credits*

SecurityFocus Linux: RE: Strange Attack On A Webserver I Work On

```
> to friends and those who helped
> !CREDITS!
> !CREDITS! * none (root@suid.net) ::: Brazil
> !CREDITS! packet spoof
> !CREDITS! * cyclone (cyc@pop.com.br) ::: Brazil
> !CREDITS! parceiro das hackadas, aprende rapido //TRANSLATION: hack
> partner, learn fast
> !CREDITS! * mariana (mazinha@brasnet.org) ::: Brazil
> !CREDITS! minha leet girl, exclusiva :) //TRANSLATION: my leet girl
> !CREDITS! * alcaloide (root@faggot.net) ::: Brazil
> !CREDITS! super lamer, versao 3 pra pacotar ele ///TRANSLATION: super
> lamer, version 3 to pack(et) him
>
> * Opcao invalida! * %s para maiores informacoes. //TRANSLATION: invalid
> option %s for more info
>
> !AJUDA!: %s -help
>
> CREDITS: %s -credits
>
> !USAGE!: %s (host/ip) (size) (loops)
>
> (host/ip) == host do babaca a ser fudido. //TRANSLATION: host of idiot to
> be f*ck*d
> (size) == bytes a serem enviados. //TRANSLATION: send these many bytes
> (loops) == tempo da fudecao/s. //TRANSLATION: total time of f*ckerying
>
> CTRL-C - ACAO CANCELADA! //TRANSLATION: action cancelled
>
> FUDEDOR (v3.0) by bonny - PRIVATE!@#! //TRANSLATION: FUC*ER v3.0 by bonny
> host desconhecido: %s //TRANSLATION: unknown host
> Maximo de bytes permitodos: 65535. //TRANSLATION: maximum allowed bytes
>
> A maquina nao tem memoria suficiente. //TRANSLATION: Not enough memory in
> machine
>
> FUDENDO A VERA %s COM %s bytes... //TRANSLATION: f*cking VERA %s with %s
> bytes
>
> pronto maneh, o babaca foi fudido! :) //TRANSLATION: that's it, <name>,
> the idiot was f*cked
>
>
>
> My question to anyone out there who can answer it is this, do you know of
any kind of automated attack that replaces index files for websites with
such a flooder? It doesn't seem like this hack was extremely well thought
out, or done by anything more than a script kiddo... if it was, why would
they replace these files with this binary program? Why not replace it with
a new index.html file saying we got hacked?
```