

RE: Suspicious joe.exe

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2001-08/0020.html>

From: Reb (reb@viametrix.com)

Date: 08/02/01

From: "Reb" <reb@viametrix.com>
To: "EPiC" <epic@hack3r.com>, "VULN-DEV List" <VULN-DEV@SECURITYFOCUS.COM>
Subject: RE: Suspicious joe.exe
Date: Thu, 2 Aug 2001 12:43:14 -0500
Message-ID: <NEBBLGGFLKNKHJLFDGMIGEIGMAA.reb@viametrix.com>

After an overwhelming amount of emails requesting the file, here it is zipped with a password of joe

Reb

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

From: EPiC [<mailto:epic@hack3r.com>]
Sent: Thursday, August 02, 2001 9:20 AM
To: reb@viametrix.com; VULN-DEV List
Subject: Re: Suspicious joe.exe

I have seen a few programs like this that will allow a user to bounce IRC connections like offered in linux with programs like PsyBNC

If you want to send it off to me, I will be happy to analyze it, please zip it, as my postfix mail server will not tolerate .exe files.

EPiC
hack3r.com

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

From: "Reb" <reb@viametrix.com>
To: "VULN-DEV List" <VULN-DEV@SECURITYFOCUS.COM>
Sent: Wednesday, August 01, 2001 11:21 PM
Subject: Suspicious joe.exe

> *Greetings all,*
>
> *While troubleshooting a problem with Win2k server doing a hard lock (no*
> *response to keyboard/mouse) I happened upon the Run key*
> *(SOFTWARE\Microsoft\Windows\CurrentVersion\Run\)* and noticed that joe.exe
> *was being started. Being that this box was no more than 2 weeks old I*
found
> *this highly odd since it wasn't being loaded as a service and whatnot. So*

RE: Suspicious joe.exe

SecurityFocus Vuln-Dev: RE: Suspicious joe.exe

> *I'm done dealing with the 2k server hang for a bit and I start looking at
> this file. After I've googled and bugtraq'd my way around I can't find
> anything that mentions such a Trojan/virus. It seems to be some type of
irc
> client that connects to 205.188.253.230 and joins #penr0x, which is +I.
If
> asked I can gzip/zip up the file and send it to someone. If anyone has
any
> insight to this I'd love to hear from you. Here's a bit of information on
> the exe.
>
> [reb@ reb]\$ ls -al joe.exe
> -rw-r--r-- 1 reb reb 53248 Aug 1 17:58 joe.exe
> [reb@ reb]\$ md5sum joe.exe
> 488c80ba0b2186a1ba52c4e69c590bc6 joe.exe
>
> Some of the more useful strings from `strings joe.exe` are:
>
> Microsoft Visual C++ Runtime Library
> Runtime Error!
> Program:
> <program name unknown>
> SunMonTueWedThuFriSat
> JanFebMarAprMayJunJulAugSepOctNovDec
> GetLastActivePopup
> GetActiveWindow
> MessageBoxA
> NICK
> VERSION
> KILL
> HELP
> PRIVMSG
> PING
> NOTICE %s :DNS <host>
> NOTICE %s :Resolving %s...
> NOTICE %s :Unable to resolve.
> NOTICE %s :Resolved to %s.
> NOTICE %s :GET <host> <save as>
> NOTICE %s :Unable to create socket.
> http://
> NOTICE %s :Unable to resolve address.
> NOTICE %s :Unable to connect to http.
> GET /%s HTTP/1.0
> Connection: Keep-Alive
> User-Agent: Mozilla/4.75 [en] (X11; U; Linux 2.2.16-3 i686)
> Host: %s:80
> Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png,
*/**

> Accept-Encoding: gzip
> Accept-Language: en
> Accept-Charset: iso-8859-1,*,utf-8

RE: Suspicious joe.exe

SecurityFocus Vuln-Dev: RE: Suspicious joe.exe

> NOTICE %s :Receiving file.
> NOTICE %s :Saved as %s
> NOTICE %s :Voyager Alpha Force: Age of Kaiten
> NOTICE %s :NICK <nick>
> NOTICE %s :Nick cannot be larger than 9 characters.
> NICK %s
> NOTICE %s :UDP <target> <secs>
> NOTICE %s :GET <http address> <save as> = Downloads a file off the
> web and saves it onto the hd
> NOTICE %s :NICK <nick> = Changes the nick of the knight
> NOTICE %s :DNS <host> = DNSs a host
> NOTICE %s :IRC <command> = Sends this command to the server
> NOTICE %s :KILL = Kills the knight
> NOTICE %s :VERSION = Requests version of knight
> NOTICE %s :HELP = Displays this
> IRC
> SYSTEM
> HIDE
> SHOW
> MODE %s -xi
> JOIN %s :
> WHO %s
> PONG %s
> SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
> TaskReg
> #penr0x
> 205.188.253.230
> NICK %s
> USER %s localhost localhost :%s
> ERROR
>
>
> Reb
>
>
>

-
- application/octet-stream attachment: [joe.zip](#)
-

- **Previous message:** [John Thornton: "Remote DoS for pcAnywhere 9.2"](#)
- **Maybe in reply to:** [Reb: "Suspicious joe.exe"](#)
- **Next in thread:** [Mark L'Italien: "RE: Suspicious joe.exe"](#)
- **Reply:** [Mark L'Italien: "RE: Suspicious joe.exe"](#)
- **Reply:** [Haul: "RE: Suspicious joe.exe"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)