

SecurityFocus Incidents: Re: UPDATE: Possibly Unknown Virus? Care to help me analyze!?

Re: UPDATE: Possibly Unknown Virus? Care to help me analyze!?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-03/0086.html>

From: Darwin (darwin@netmadeira.com)

Date: 03/11/03

From: "Darwin" <darwin@netmadeira.com>
To: "Jeremy Junginger" <jj@act.com>, <incidents@securityfocus.com>
Date: Tue, 11 Mar 2003 01:13:45 -0000

This is what I found from the files you sent me:

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

From: "Jeremy Junginger" <jj@act.com>

>c:\Documents and Settings\All Users\Start Menu\Programs\Startup\onylje.exe

Seems to be a copy of pcoo.exe.

Contains IRC commands, most certainly includes a IRC client embedded.

Possibly a variant of "Randon":

<http://www.viruslist.com/eng/index.html?tnews=1001&id=59750>

or a variant of Agobot worm:

http://www.alerta-antivirus.es/virus/detalle_virus.html?cod=2307

Many references to antivirus processes – most certainly to locate and kill them.

Possibly a variant of Trojan.KKiller.

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.kkiller.html>

The Trojan.KKiller Trojan Horse terminates many processes, including those of popular antivirus and firewall programs. It also modifies a registry key, so that it runs when you try to execute any .exe file

Includes a reference to advapi in the body.

Maybe a variant of Backdoor.IE_Patch.

http://www.f-secure.com/v-descs/ie_patch.shtml

"Capabilities of IE_Patch backdoor include sending and receiving data (files), monitoring of existing