

RE: RE: RE: Possible hack – Portable profile found in a Windows 2K Pro SP1 station..

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-02/0055.html>

From: Jorge Roxo (j.roxo@sotagus.pt)

Date: 02/08/02

From: "Jorge Roxo" <j.roxo@sotagus.pt>

To: <focus-ms@securityfocus.com>

Date: Fri, 8 Feb 2002 18:30:52 -0000

We thanks to Pascal Longpre who pointed us out into the right direction with this subject.. We checked the local machine for the user of PCAnywhere and found out that it was trojaned. Funny enough the attack that seemed simple was actually quite complex, it went as it follows:

- 1.– Attacker trojaned PCAnywhere caller...
- 2.– Sat and listened for conections made...
- 3.– Found our conection and how to get into the system...
- 4.– Tried unsuccessfully to gain administrator rights in our machine as well as a failed attempt to place a trojan in our machine. Tried as well to access the network and the servers to install his profile as a memembr of the administrator group which is not the builtin one in Windows 2000 but is quite well protected and failed.
- 5.– The 30 seconds conection timeout I had setup for the modem failed miserably, and did not disconnect the user.. So did the 3 minutes timeout connection of PCAnywhere..
- 6.– Local security, group policies, and AV stopped the intruder from accessing any data in the network or system..

My conclusions on this...

Well.. Thank god for our AV and the pains we've had to go through to implement good, sound, and properly working security policies semm to have payed off.

My main worry now is as follows... We are thinking on maybe creating computer groups, and through them allowing those machines to operate on X, Y or Z security level, thus even if a user is logged on as a domain administrator or network admin, but is not logged on at his machine, he would only have access to minor capabilities as determined by both the admin profile and machine he uses. Mind you, the computer groups should not be confused with workgroups bu rather make computer+user members of a determinate group type, such as domain administrators, domain users, server operators etc...

SecurityFocus Microsoft: RE: RE: RE: Possible hack – Portable profile found in a Windows 2K Pro SP1 station..

Anyone can see any problems here regarding security?... How good for security is the implementation of personal access cards? Do they really work? What are the security risks involved? Can they be externally hacked?

Jorge Roxo,
TCSA/Sotagus Computer Systems Administrator

This e-mail is confidential and privileged. If you are not the intended recipient please accept our apologies. Do not disclose, copy or distribute information in this e-mail or take any action in reliance to its contents, to do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.

-
- **Previous message:** [Evans, TJ: "RE: Secure Transactions over HTTPS???"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)