

RE: Security with USB Devices

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-08/0041.html>

From: Alan Davies (Alan.Davies_at_videonetworks.com)

Date: 08/04/05

Date: Thu, 4 Aug 2005 10:03:38 +0100

To: <kurt.buff@gmail.com>, "H D Moore" <sflist@digitaloffense.net>

Two points to make on that.

1) Couldn't one just as easily make a CD with autorun on it and put both that and a USB stick into the target machine. A program on the CD then copies all profiles to the USB stick (which is nearly always going to be the E: drive on standard systems).

2) Both my point above, and surely the product highlighted below, would not work on a locked workstation would they? AFAIK autorun cannot run unless the workstation is logged in and unlocked.

All the same, it does look like an interesting product. I'm surprised that the driver works natively on Windows considering what it does (ie. masquerade as a CDROM drive).

alan

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

From: Kurt Buff [<mailto:kurt.buff@gmail.com>]

Sent: 03 August 2005 21:41

To: H D Moore

Cc: pen-test@securityfocus.com

Subject: Re: Security with USB Devices

H D Moore wrote:

> *This is the toy I use, it works on Windows 2000+, but can take a few*
> *seconds for the driver to get installed and the autorun to execute:*
> - http://www.hsc-us.com/consumer/usb_flashdrive/UDRW.html
>

Ye Gods! Doesn't this make anyone even a little nervous? Autorun from a CD drive is bad enough, dontcha think? Being able to walk up to a machine and stick that in the port and autoinfect, or worse autocopy, seems to be a huge risk to me.

I can see it now – someone on the night cleaning crew walks into the CFO's office, sticks that thing into the front USB port on her PC, and

SecurityFocus Penetration: RE: Security with USB Devices

walks away with the My Documents folder. No muss, no fuss, no need to even turn on the monitor.

Kurt

This email may contain confidential and privileged information and is intended for the named or authorised recipients only. If you are not the named or authorised recipient of this email, please note that any copying, distribution, disclosure or use of its contents is strictly prohibited. If you have received this email in error please notify the sender immediately and then destroy it. The views expressed in this email are not necessarily those held by VNL, and VNL does not accept any liability for any action taken in reliance on the contents of this message. VNL does not guarantee that the integrity of this email has been maintained, nor that it is free of viruses, interceptions or interference.

This email has been scanned for all known viruses by the MessageLabs Email Security System.

FREE WHITE PAPER – Wireless LAN Security: What Hackers Know That You Don't

Learn the hacker's secrets that compromise wireless LANs. Secure your WLAN by understanding these threats, available hacking tools and proven countermeasures. Defend your WLAN against man-in-the-Middle attacks and session hijacking, denial-of-service, rogue access points, identity thefts and MAC spoofing. Request your complimentary white paper at:

http://www.securityfocus.com/sponsor/AirDefense_pen-test_050801
