

USB delivered attacks – lessons learned/summary (so far)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-06/0011.html>

From: Jerry Shenk (jshenk_at_decommunications.com)

Date: 06/02/04

To: <pen-test@securityfocus.com>

Date: Tue, 1 Jun 2004 22:18:29 -0400

Well, I'm doing messing with this....at least for the moment. Here's what I've found out. All my testing so far has been done on a Windows XP laptop. I was planning to try other versions but for now, I'll leave it go at this. Here's a summary of what I've discovered:

USB devices don't use autorun – well, they seem to do something with it 'cuz if there's an "open=" statement in the autorun.inf, they don't pop up an explorer window. If there is an "icon=" statement in the autorun.inf file, the icon for the explorer windows will be the specified icon. This leads me to believe that autorun is at least looking at the USB drive. Maybe if the right stuff is in that file, there might be a way to run something. I tried pulling the .ico file off my web server but that didn't work...yet;)

Autorun under XP doesn't work if the screensaver has the screen locked. I didn't try this with multiple OS'.

The USB devices I tried were a flashdrive and an SD card reader with a 128 meg card from my camera. I didn't try my 120 gig USB hard drive 'cuz it's formatted for the wrong OS at the moment....that kindof blows the clandestine nature of a thumbdrive....need for power, a rather large device....

Somebody said that 2600 had something about this type of thing in the current 2600 magazine. That would suggest that a few other people have been playing with this idea. Somebody with more brains, ideas or time than I is likely to come up with something pretty nasty.

Nearly every post stated something about the dangers of autorun. One post suggested just using a CD. Most people have autorun turned on so if there's an internet connection or a computer in the office that can receive data....well, that'll work just as well as USB. If the CD is labeled with something "interesting", perhaps a few people will check it out.

SecurityFocus Penetration: USB delivered attacks – lessons learned/summary (so far)

Another poster suggested that this is all just a good reminder of the basics of security, you wouldn't let some stranger come up and swap drives in your machine, why assume that his USB thumbdrive is so innocuous just 'cuz it's small and trendy.

Here's the autorun.inf file I was playing with

```
[autorun]
```

```
;OPEN=ping.exe 10.1.1.5
```

```
icon=http://www.website.org/blue.ico
```

```
;icon=\icons\red.ico
```