Gadgetopia

Geek and you shall find

- About Gadgetopia
- Contact Us
- RSS Feed
- Twitter
- Blend Interactive

Search Ga Search Site

- Home
- Computer
- Developer
- Gadget
- Science
- Web
- Other

Aug 15

Hardware Keystroke Logging

Say you work in a company and are up for a promotion. You want to negotiate your salary effectively, but to do this, you need to know what others in that position are making. How do you get into the Human Resource records?

Bob, who has a cube across the hall, is the DBA. He could get in there, but how do you get his password? Your network is monitored and audited pretty closely. You can’t do anything to steal his password “on the network” which might get logged and would be traceable to you.

Enter this little device:

This USB keyboard logger has a huge 2MB or 4MB memory capacity, organized into an advanced flash file system. Super fast data retrieve is achieved by switching into pendrive mode for download. Completely invisible for computer operation…

It comes in USB and PS/2 models and costs less than $100. (No link, lest I be accused of encouraging this. You can find these things easily enough if you want to.)

One night, you work late, then you unplug his keyboard, plug this device into his computer, then plug his keyboard into the device. His computer is way under his desk, so he'll never see it. You retrieve the device the next evening and download all his keyboard input for the entire day from the internal Flash memory. It wouldn't be hard to pick out his password, and now you're him.

This is unlike a software keyboard logger because there's no evidence left behind. No process that runs in the background, no need to install anything on his machine, etc. It's like stabbing someone with an icicle — no evidence gets left behind.

All you security types out there — how do you defend against this? Do they sell encrypting keyboards, which encrypt data sent down the keyboard cable and decrypt it on the machine?

by Deane August 15, 2006 1:44 PM | Follow Gadgetopia on Twitter

What Links Here

Defeating Keystroke Logging

We've talked a bit about keyloggers before, which can be a brutally effective way to capture passwords (see this post, this post, or this post). But there's a completely simple way to defeat them, based on the fact that a keylogger doesn't know where on the page the focus is when…

Keystroke Logging in Action

Lessons Learned from Biggest Bank Heist in History: In the comments on yesterday's post about hardware keystroke loggers, someone posted a link to this story about a near-heist at the Japanese bank, Sumitomo Mitsui. Would-be robbers used this exact attack. By installing software keystroke loggers on the PCs…

Comments

by Michael, August 15, 2006 2:36 PM

On modern computers, keyboards tend to not work anymore when unplugged and replugged when the PC still runs. So if you leave your PC on all time, and someone hooks such a device to your PC, you come in in the morning and the keyboard is not working. Or if the eavesdropper is a bit smarter, your PC has rebooted. Both would be a signal for me to check what had happened.

---

by *Deane*, August 15, 2006 2:38 PM

On modern computers, keyboards tend to not work anymore when unplugged and replugged when the PC still runs.

Really? I haven't found this to be the case with my machines.

---

by *Anthony Mills*, August 15, 2006 2:58 PM

Keystroke logger :)

It would be very difficult to guard against this. After all, if you don't have physical security, you don't have security.

---

by *Michael*, August 15, 2006 3:01 PM

Works for me all the time - and I hate it. Maybe it's with USB stuff only. Hadn't had a PS/2 keyboard for ages.

If it doesn't work for your PC then you must refer to "plan B" and "booby trap" your PC. A motion sensor comes to mind, triggering when the (tightly stacked towards the back) PC gets moved in order to make way for the plug.

---

by *Deane*, August 15, 2006 3:27 PM

It would be very difficult to guard against this. After all, if you don?t have physical security, you don?t have security.

I've been in a lot of a IT shops, and I haven't seen one yet that physical secures all the desktop machines. You?

---

by *Anthony Mills*, August 15, 2006 3:59 PM

I've been in a lot of a IT shops, and I haven't seen one yet that physical secures all the desktop machines. You?

Nope. And the headaches that would entail would be far more costly than not taking the measures.

Remember, security is a series of tradeoffs. You can't ensure someone won't do something boneheaded like that, so you put something in the company policy manual about it and generally forget it. And if someone does that, you fire them and sue for damages. And you try not to hire someone like that in future.

Employees will always be able to do stuff like that. If it's not a keystroke logger, it could be a wireless mini-cam. Or it could be a replacement keyboard (slightly modified of course). Or it could be a Trojan. Or it could be getting Bob drunk and asking him the password...

---

by Dave, August 15, 2006 4:16 PM

Let's say you stuck this doodad on Bob's computer and weren't able to get back to it for a week? Would this thing max out and cause an interruption that would result in a service call? Or would it just happily pass along the bits that it can't hold?

If one were devious enough to do this, you could also pick up a few blackmail-worthy tidbits about Bob, which could be used to enhance your earning potential.

---

by Bob, August 15, 2006 4:33 PM

Go ahead and try it! I dare you!.......No, wait...I double dog dare you....!!!!!

---

by Dave, August 15, 2006 5:07 PM

Uh-oh; Bob's on to your game, Deane.

---

by Peter Harkins, August 15, 2006 7:15 PM

Shameless self-promo: I wrote about this a few months ago, hit the link on my name.

---

by Jon Mark Allen, August 16, 2006 3:32 PM

The Sumitomo Mitsui Banking Corporation in Tokyo decided the answer to this question was Super Glue!

Could be a bit of overkill, but...

---

by Deane, August 16, 2006 3:59 PM

The Sumitomo Mitsui Banking Corporation in Tokyo decided the answer to this question was Super Glue!

Not a bad idea, actually. More manageable would be a desktop where the keyboard attached inside the case, which would be locked.

When you really think about it, keyboards are a pretty stunning security hole. A *lot* of very sensitive data travels through a keyboard into the machine, and it can be intercepted pretty easily. The network cable too -- I'm sure there are physical capture devices for them that you can attached to a machine for a day or two.

---

by NoBodyYouKnow, December 31, 2007 9:54 AM

Ok, ready for a great little trick to bypass your would-be co-worker spy? This is a great but little know way to get around the key logger attached to the back of your PC. The beauty of it is, you keep letting the spy think he's undetected, ie he thinks he knows your password when in reality you're using the real one and letting him think it's something else. Ok, here goes. Pay attention.....

Click on Start, then All Programs, then Accessories, then Accessibility, then On-Screen Keyboard.

The rest should be self explainitory, if not, then you shouldn't be in the corporate possition you're in. Just use the on screen keyboard to input your password at the appropriate point and access your secure files. Since the keystrock logger on the back of your PC only records keys actually pressed on the hard-keyboard itself, the spy will never see your Real Password and will continue to think the one he has is ginuine. If you want to really confound him, reset the Fake Password daily by the conventional means and continue to access your files by the method above. While he'll never be able to access your system, he'll start thinking he's one step behind you password wise since each new password he receives won't let him in. Watch him get more and more flustered daily as he's tries unsuccessfully to catch up with your resetting the latest Fake Password. Of course it's not necessary to reset what he sees but the process keeps him thinking there must be a really good reason you're resetting your password every day. He's just a fumbling would-be James Bond who's too stupid to realize every single one of the new passwords are worthless and for your amusement only. Good Luck and have fun. PS...Remember however, what ever you type on the hard-keyboard will be seen by the logger device.

---

by JOEL SHAW, July 2, 2009 10:47 PM