Super-Glue: Best practice for countering key stroke loggers

By Richard Stiennon | April 21, 2006, 11:28am PDT

Summary

This wonderful little gadget is for sale over at Thinkgeek. It is colored an innocuous IBM grey so no one will notice when you attach it to their keyboard. It fits between the back of the PC and the keyboard cable. It needs no power and it can record 130,000 keystrokes. It works like a [...]

A former ZDNet blogger, Richard Stiennon is an industry consultant. Most recently he was Chief Marketing Officer for Fortinet, Inc., the largest privately held security vendor. prior to that he was Chief Research Analyst at IT-Harvest. And before creating IT-Harvest, he was VP of threat research for Webroot Software, Inc. the leading commercial anti-spyware solution.

Previously, Richard was VP Research at Gartner, Inc. where he covered security topics including firewalls, intrusion detection, intrusion prevention, security consulting and managed security services for the Security and Privacy group. He is a holder of Gartner's Thought Leadership award for 2003 and was named "One of the 50 most powerful people in Networking" by NetworkWorld magazine. His speaking engagements have included conferences and meetings throughout North and South America, Hawaii, Tokyo, Tel Aviv, Istanbul, Milan, Munich, Hannover, Madrid, London, and Cannes.

This wonderful little gadget is for sale over at Thinkgeek. It is colored an innocuous IBM grey so no one will notice when you attach it to their keyboard. It fits between the back of the PC and the keyboard cable. It needs no power and it can record 130,000 keystrokes. It works like a software keystroke logger. Once it is installed it just captures anything that is typed: usernames, passwords, URLs, email, banking info, everything. To access the data the owner of the device just types the password into any word processor and then you start to communicate with the device. It is very slick. Of course the primary difference between this and a software keystroke logger is that there is NO WAY to detect it and remove it.

Of course this is exactly how the greatest attempted bank heist in history was pulled off. The bank robbers installed these devices on machines inside the bank and eventually got access to Sumitomo Bank's wire transfer capability. They then proceeded to transfer more that $440 million to various accounts in other countries. Read all the gory details in this article I just published.

The one thing I do not mention in the article is that it is reported that Sumitomo Bank's best practice for avoiding a repeat attack is that they now super-glue the keyboard connections into the backs of their PCs.

> At some point or other, a password will leak. Besting thing to do is use a physical smartcard cryptographic token. You can't key log that.
>
> 04/21/2006 03:36 PM
>
> *At some point or other, a password will leak. Besting thing to do is use a physical smartcard cryptographic token. You can't key log that.*
>
> I completely agree. Passwords are now at least a decade out of date and have become almost useless as a security device. Smart cards or some similar system can talk in two directions with the computer that is asking for authentication of the user. This allows two crucial changes in the security protocol:
>
> 1) True end-to-end strong encryption can be built into the communication system, so that evesdropping and related attacks are effectively impossible.
>
> 2) The server can authenticate itself to the smart card, as well as the smart card to the server, using several steps which use computation instead of direct transmission of secret data. You obviously do not want to provide any information to an adversary posing as a well-known vendor!
>
> Without some such system, our data security will continue its relentless decline, dropping to effectively zero protection in the near future.
>
>  rd@...
>
> 04/22/2006 12:19 AM
>
> You can't key log a smartcard, but you can duplicate one. You can also piggy-back commands from your keyboard to any destinations after whichever authentication methods you choose, may it be smartcard or any other variations in the future.
>
> Also at some point all that encrypted materials have to be reverted into human-readable format, so your "secured" communication is only as secured as your video cable, or any programs that can tap into the video rendering of your terminal. How would you know what you view on your computer screen is ACTUALLY generated by your computer?
>
> There is no solution. Smartcard will make money for a lot of people, and I'm all for that, but it's

not a solution to end the problem. Heck, it doesn't even solve the problem. It only patches a tiny crack in a huge hole.

 too_much green_tea

04/22/2006 02:21 PM

Instead of plugging something in between the keybboard and computer you could do exactly the same with whatever input device. You have to securely connect whatever device you are using to the computer so that noone can put something in the middle. Of course a really determined person could cut the cable and fit something but that would be hard to do unnoticed.

 quantumstate

05/04/2006 11:57 AM

Now I know what to look for on my hardware before I use my computers. Hopefully, I won't need to use super-glue, but I don't have any reason to believe that someone at work or home would stoop to putting hardware-sh**warez on my systems.

If I do find one, I'll pull it off and run it over several times with my car. Or toss it into the middle of a busy street and watch the traffic do the dirty work. Or... maybe... if I can find a powerfull enough electromagnet...

 Mr. Roboto

04/21/2006 07:26 PM

Super glue remover is a wonderful thing, and it doesn't even smell that bad.
Super glue does not replace paying attention.

 indrax

04/21/2006 10:29 PM

How about looking behind your computer and unplugging it?

 anythingbutmine0

04/22/2006 09:19 PM

When was the last time the seriously non-techie types at your workplace looked at the back of their PC? And, even if they did, would any of them even realise that, in that rat's nest of wires, there was something that didn't belong?

I didn't think so ....

Steve G.

 aureolin

04/23/2006 10:23 PM

The article says it is impossible to detect or remove. That's the only thing I'm disputing. Don't put words in my mouth.

But since you brought it up, when was the last time the seriously non-techie types at your workplace ran utilities to check for software keyloggers?

 anythingbutmine0

04/26/2006 06:07 PM

When was the last time you looked at the back of your computer? Most corporate computer users don't even acknowledge that they even have a computer...it's always "some box that has the hard drive that sits under my desk". It sits there, innocous until tech support gets a service call that someone's "hard drive" has failed and they come out to replace the box....that happens less often than the 3-5 year PC refresh does...
so, yeah...crawl on your hands and knees in your business suit, amoungst the dirt, dust bunnies, old french fries and corn chips, pull out the CPU and using your flashlight, get your head behind the box and see if you can identify everything that is plugged into your computer? Likely not...and if you can, congratulations...now your pants are dirty and the CEO wants to see you in the conference room now to meet with a new multi-million dollar customer...good luck on that first impression!
Ed
web/gadget guru

 tech_ed@...

05/04/2006 02:31 PM

Why not put a "keyboard unplugged" detection device on the keyboard plug? It would be like the chassis intrusion function on a PC and would alert the user that the keyboard had been unplugged (with a message on the screen during POST). The user could be informed during the warning to check the keyboard plug for tampering (and extra hardware). Alternatively, do away with PS2 ports and switch to all USB mice and keyboards!!

 Carrion

05/04/2006 11:20 AM

Yes but the USB port is much cheeper to attack. This device costs 99.99 USD. Fo that I can get a 1 gig USB plug-in device and use free software k/b logger.
Its cheaper than TEMPEST or Optical tempest by a factor of 10.
What about hidden partitions on your HD?
Extra PCI cards inside?
Many m/b have unused ports for further USB sockets that could be internal.

It only goes to show that in the real world "IT Security" is a myth.
Either /or your equipment or your staff are always open to compromise, so long as you have something worth getting and an enemy can devote the time, effort and cash to doing it!

 michael_orton@...

05/04/2006 11:35 AM

I can detect them 100% of the time. Just look behind the computer and check the keyboard connector.

I can remove them 100% of the time too, even if superglued. I have a skill level of 256+ in computer disassembly and discombobulation.

 Dr_Zinj

05/04/2006 11:24 AM

I have had several dealings with super glue ---It really holds well for app. 2 weeks ----after that it seldom or never holds at all

so if you super glued your keyboard in , check it to see if it is still holding

 1pie1

05/04/2006 02:50 PM

take one of these keyloggers and glue it in place with shoe goo put your own password on it I doubt they will work 2 deep, you can check up on the crew and it takes an act of GOD to bust shoe goo

Note you can get these keyloggers to imbed inside the keyboard itself think about it all the precautions and for naught 10 minutes and some vandal has a chip in your keyboard watching every keystroke