

## Re: Best secure surfing solution

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/2180.html>

---

**From:** Lawrence Rodis (*lrodis\_at\_strategicresource.com*)

**Date:** 01/31/04

Date: Sat, 31 Jan 2004 07:58:56 GMT

Vanguard,

The original poster asked how hard would it be for his company to monitor his usage. The answer is very easily.

If I put that software on your system it would capture what you are doing with Keystrokes and displays captures. No encryption would matter. Could IT do it in your organization? With proper approval, yes. Would IT review the data? doubtful. Your boss or some other appropriate party? yes.

--

Regards,

Lawrence A. Rodis

President

Strategic Resource Consulting Group L.L.C.

702-221-6274

lrodis@strategicresource.com

www.strategicresource.com

"\*Vanguard\*" <no-email@bogus.nix> wrote in message

news:KLadneHypudOzYbd4p2dnA@comcast.com...

> "Lawrence Rodis" said in

> news:k2ESb.3993\$F23.1146@newsread2.news.pas.earthlink.net:

> > George,

> >

> > To prevent your ISP, what Flag said is correct. For your Company,  
> > they could have access to everything you do in minutes. Look at  
> > spectorsoft.com and their spector professional edition. I'm using it  
> > on PC for several clients. And have caught folks doing things they  
> > should not. Best to keep your private stuff off of other peoples  
> > PC's.

> >

> >

> >

> > "George" <lgst036@hotmail.com> wrote in message

> > news:f86efd4e.0401301646.3729e776@posting.google.com...

> >> Hi,

> >>

> >> I would be grateful if someone could give me some advice.

> >> Not wanting my ISP or employer to see confidential emails and

> >> surfing, I have set up a service with companies providing secure web

> >> browsing (Idzap, the cloak, etc). So my web browser is using https

> >> using certificates from the company offering this service.

> >> I have read about possibilities of intercepting the https with "man

> >> in the middle" or maybe other techniques.

> >> How difficult it is for an ISP or my company's network

> >> administrator to do that. Translated in money, how much would they

Re: Best secure surfing solution

## sci.crypt: Re: Best secure surfing solution

> >> need to spend to do that.  
> >> Are there any better solutions, maybe a VPN service, Kerberos setup  
> >> or anything else possible.  
> >> Of course the above assumes that the secure service provider is  
> >> trusted on which I would be keen to find any of their commonly known  
> >> policies. (maybe suggestions)  
> >>  
> >> Many thanks  
> >>  
> >> George  
>  
> But since the connection is SSL secured, why would the user care that you  
> could sniff out their encrypted HTTP datastream? It'll look like a bunch  
> of  
> garbage to you, the sniffer. You can still see \*where\* they are  
> navigating  
> but you cannot see \*what\* they are sending and receiving.  
>  
> The only way that spectorsoft.com could be determining what the user is  
> sending (but not what they are receiving) is to install a client on that  
> user's computer. That is, the product would have to install a keylogger.  
> That appears to be what the product does since it states, "... , Spector  
> Pro  
> contains seven integrated tools that record: ..., keystrokes typed, ...".  
>  
> You had better make sure that you have permission from each department to  
> do  
> this sniffing and keylogging. Our department, for example, sometimes has  
> highly sensitive data between us and a partner that no one else in the  
> company should see (and anyone else seeing the data is a severe breach in  
> security). We even have to be in a separate section of the building, all  
> papers must be discarded in our wastebaskets and not outside our locked  
> room  
> (because it gets handled separately and securely from the other trash),  
> recording devices are definitely taboo, and so on. If we caught anyone in  
> IS or elsewhere in our company sniffing our communications, even if they  
> were encrypted, they'd get laid off or, at least, suspended. Just like  
> there are laws prohibited unauthorized wire tapping, there are always  
> internal policies and politics that dictate if anyone can go sniffing just  
> because they are curious. You need to establish well written and  
> understood  
> policies and make sure all departments are educated (and you, too, about  
> what you are NOT allowed to do regarding communications from some  
> departments).  
>  
> As far as the keylogger client, that wouldn't survive very long on my  
> hosts.  
> By going through an intermediary but external anonymizer service using  
> SSL,  
> all you could see is that I was connecting to that service but not where I  
> was actually connecting to past that service. If e-mails are sensitive  
> then  
> the sender should be using encryption. You can see in your mail server  
> logs  
> (and don't need SpectorSoft) where the e-mail went but not its content.  
> Of  
> course, if anyone from IS installed anything on our alpha lab hosts, they  
> would get their ass royally kicked for corrupting our known configurations  
> used for testing.  
>  
>  
> --

Re: Best secure surfing solution

sci.crypt: Re: Best secure surfing solution

> \_\_\_\_\_  
> \*\*\* Post replies to newsgroup. E-mail is not accepted. \*\*\*  
> \_\_\_\_\_  
>  
>  
>