

Full-Disclosure: Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

## Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-06/0777.html>

---

*From:* Steffen Schumacher (*ssch\_at\_wheel.dk*)

*Date:* 06/22/04

To: Eric Paynter <eric@arcticbears.com>

Date: Tue, 22 Jun 2004 08:12:10 +0200

Guys..  
(oh.. and girls...)

Remember the troll who posted something a long the lines of a SSL crypto virus? Now on my rough fingercount, I think that the M\$ threads have \*long\* outdone that thread, in quantity, and in my opinion; quality.

The troll post, at least, was funny. The M\$ threads were, I agree, relevant to begin with, and I guess that about 5 % of the posts now might be relevant, but IMHO there are too much private discussions going on, which have no relevans for the rest of us.

I know that M\$ is probably the one thing most of us have an opinion about, but I really don't think it to be optimal that I have to read 95% M\$ flaming, on in order to get the 5% exploits within a single post, or all posts.

I my self posted a couple of times, and perhaps I need to cut the flaming / defending of M\$ too, maybe even the regular discussion stuff.

The simple fact is that 10-? M\$ mails on a regular day, IMHO, is too much about nothing. None of these posts is about exploits – they are about M\$ strategy, and a bunch of other semi-related stuff.

I mean – I'm actually considering putting on a filter removing the M\$ posts. To me that says things are where they should not be.

To me this kind of stuff really belongs in a newsgroup, rather then a mailing list.

I will ask that you do \*NOT\* reply to this mail, but rather just decide with yourself if you wan't to honor my requests or not. I have no authority in this list, so this is a mere request, and I don't need your reply or oponion on the matter. Well – really what I'm trying to avoid, is more 'noise' on this list.

/Steffen Schumacher

On 21.06.2004 21:21:26 +0000, Eric Paynter wrote:

> *On Mon, June 21, 2004 3:55 pm, joe said:*

Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

> > *I have written several registry editor type apps for customers, it is*  
> > *simply another API. For me writing a text editor is the same as writing a*  
> > *registry editor, in fact, the classes I put together treat them both very*  
> > *similarly from code use perspective.*  
>  
> *You missed one significant point, though. In my 15 years of computer*  
> *programming, I have never \*had\* to write a text editor. Whereas, you have*  
> *had to write \*several\* (your word) registry editors. And the only person*  
> *who needs to know anything about a filesystem API is a compiler*  
> *programmer. The rest of us mere humans use the standard library of open(),*  
> *close(), read(), and write() commands if we want to access files*  
> *programmatically.*  
>  
> *One more thing, because of the complexity of the registry and removing it*  
> *from the filesystem, in Windows, you need to learn the filesystem API*  
> *(whatever that means to you) to get at the filesystem, the registry API to*  
> *get at the registry, the COM API if you want to communicate between*  
> *processes, and several application-specific APIs to programmatically*  
> *configure most applications. In Unix systems, it's all treated as files.*  
> *You use a common interface to use them all – open(), close(), read(),*  
> *write(). How much simpler can it be? And the simpler it is, the less*  
> *margin for error. And the less margin for error, the less risk of exploit.*  
> *And that means better security... something to think about.*  
>  
> *And before you say you \*can\* configure apps by directly editing the*  
> *registry, removing the need to learn all of those unique APIs (although*  
> *still leaving you without a nice local IPC interface), you'd better check*  
> *your support agreement on that. Even Windows is not supported by MS if you*  
> *directly edit the registry. Most app vendors say you're on your own too if*  
> *you do that... So good luck! Any bad move in the registry is like open*  
> *heart surgery. The box may never boot again – I know, I've done it more*  
> *than once.*  
>  
>  
> > *10 people on one machine all load the same app... Here is where the pain*  
> > *comes in. That could be a terrible waste of space and resources, but from*  
> > *a security standpoint, maybe they should all maintain all of their own*  
> > *info for each instance.... But now what about security updates? You*  
> *would > be updating 10 instances. Hmmm point/counterpoint. What wins?*  
>  
> *Wow, that is a problem. Thank God it simply doesn't exist on Unix systems.*  
> *The system-wide configs go into /etc and the user-customized portions go*  
> *into /home/username/.appname (remember earlier I said all you need to*  
> *backup is /etc and /home to restore a Unix machine?). Users don't install*  
> *their own applications because they simply cannot. If they want an app,*  
> *they ask the sysadmin to give it to them. If you are the sysadmin, you*  
> *install it in the system area and the users get access to it as required.*  
> *Don't forget, Unix systems were multi-user over a decade before DOS was*  
> *even conceived. All of these problems have long since been solved.*  
>  
> *The biggest problem with Windows is that it is a multi-user system built*

Full-Disclosure: Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

> on a single-user foundation. (Yes, I know, the NT kernel was built from  
> the ground up the be multi-user, but the system layout did not change to  
> be consistent with that, so maintaining it still has the same problems.)  
>  
>  
> > I think your copy protection scheme might be pushing it a bit. It isn't  
> > much more work to capture registry mods and apply them to other machines.  
> > One of my old jobs had a large part of my time making up software dist  
> > packages that did just that. You capture the reg changes made, you capture  
> > the file changes made, you throw it into a package to be deployed by SMS  
> > or the perl dist method of your choice. If they were intending that to be  
> > wholly magical and to block software copying, there wouldn't be APIs the  
> > public would have available to go into it. This is more FUD/conspiracy  
> > thinking.  
>  
> Yes, yes. I know. I did electronic software distribution in a windows  
> environment of several thousand machines for many years. We started with  
> sysdiff (remember that?), and then moved on to the SMS Installer. And we  
> used GHOST to take full images for mass deployment of desktops. I know a  
> million ways to capture an installation difference. But how many home  
> users do? It was meant to be a deterrent, not a 100% success. Remember  
> that before the registry, we didn't need tools like sysdiff.  
>  
> Anyhow, all that noise aside, I think it's safe to say that whatever the  
> registry was intended to be, it was a complete and utter failure. There  
> are more headaches over trying to figure some part of the registry than  
> there ever were worrying about all those lost .ini files. And for some  
> reason, large Unix systems with thousands of users don't have any of these  
> problems. Go figure...  
>  
> Back to the topic: What should they do? They should do like Apple did:  
> stop trying to re-invent the wheel and adopt a tried-and-true model that  
> works. The Unix-like systems are simply easier to manage and safer. And  
> Apple has made them as easy to learn as Windows, while being as easy to  
> administer as Unix.  
>  
> By the way, I'm not saying we should all have Linux systems, or FreeBSD,  
> or any one particular system. I think we should have a diverse set of  
> systems from several vendors, but that can interoperate and have similar  
> interfaces to ease the burden of management. Solaris and Linux come from a  
> completely different code-base. They are vulnerable to completely  
> different types of attacks. Yet the administration of the two is almost  
> identical. A good blend of Unices in an environment makes it safer.  
> Windows adds complexity simply by being so different, never mind all the  
> problems described above.  
>  
> -Eric  
>  
>  
> \_\_\_\_\_  
> Full-Disclosure - We believe in it.  
> Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

Full-Disclosure: Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Re: [Full-Disclosure] PLEASE QUIT YACKING ABOUT M\$