

# Re: Deloder worm has resurfaced. Watch your privacy!

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-03/0723.html>

---

**From:** Nick FitzGerald ([nick@virus-l.demon.co.uk](mailto:nick@virus-l.demon.co.uk))

**Date:** 03/30/03

From: "Nick FitzGerald" <[nick@virus-l.demon.co.uk](mailto:nick@virus-l.demon.co.uk)>

Date: Sun, 30 Mar 2003 11:55:21 +1200

"Kyle Lai" <[kyle@kylelai.com](mailto:kyle@kylelai.com)> to me:

> > *There are good reasons why measured analyses of Deloder do not include*  
> > *the password information. Further, there are compelling ethical*  
> > *reasons for them to not include that information. The rest of your*  
> > *analysis is a good and useful contribution, but it and your ethical*  
> > *reputation are spoiled by a couple of sentences.*  
>  
> *I disagree. I think you missed the point. Plus, I don't think*  
> *anti-virus vendors looked at registry values other than the "start-up"*  
> *registry values.*

Why are you so obsessed with registry settings? And it is you that has missed the point.

AV products in general do not look at registry settings AS A DETECTION METHOD. And there are very good reasons for that. No vendor can afford the false positive and false negative rate "depending" on such detection methods would produce. Such items are indeed useful in manually handling incidents and knowledge of them is often necessary to "fix" machines that have been "infected" (though with this kind of compromise, it is generally best advice -- against the history of the AV industry's approach -- to "burn and rebuild" as you can guarantee that folk dumb enough to get hit by something like Deloder will not have taken enough of the necessary preparatory steps to be able to assuredly determine after the fact whether the rest of their box has not been seriously compromised with other, as yet undetected backdoors, stealthing rootkits, etc.

Anyway -- we can easily disagree about the desirability of using registry values for programmatic malware detection and we can debate that till the cows come home. However, you did not address my main point which is that your publication of the VNC password used by Deloder is unethical and therefore irresponsible and unprofessional. Your point that describing the gory details of the registry settings is useful does not, in and of

comp.security.misc: Re: Deloder worm has resurfaced. Watch your privacy!

itself justify your further compromising of security of the claimed 140,000+ machines that have been infected with Deloder. Were the VNC password stored in clear text in the registry then a decision to publish that registry value would be equally problematic given there are plenty of other diagnostics people can use.

Surely you understand that as the VNC password is a purely arbitrary side-effect of a malware writer's choice at some point in history, AND knowing it adds precisely nothing to the end-users' ability either to "protect" themselves or to remove Deloder should they have been infected already (these are, you claim, your main motivations in releasing the analysis) the specific value to your target audience of knowing that password is ZERO. So your publication of it really only significantly helps others than those you claim were the intended benefactors of your work. Further, it is obviously highly likely that the only people who will be greatly helped by your effort are those with intent to maliciously use the machines of innocent people affected by Deloder. As that is such an obvious conclusion, I restate my charge that it was recklessly unethical and professionally irresponsible of you to publish the password information.

> *If public did not get informed about the true problem and exploit, and*  
> *what the worm has done, how can they protect themselves from the*  
> *variants of this worm, which always happens? ...*

They cannot.

But, if you think about it for a few seconds, they do not need to know precisely what the worm does. In fact, it would be better if they had a broader, more general appreciation of security issues than a temporary, highly focussed view on this incident. Drawing such detailed focus to this particular worm runs the risk of people deciding that because their password is not in the list that Deloder uses, then they are "safe". This is precisely the same sort of security-blind "knowledge enhancement" people who suggest, hearing that a terrible virus payload is due to trigger on, say 1 April, seriously suggest that a reasonable approach is to not use our computers on that day "just to be sure".

And face it — do you really think people with null and such obvious admin passwords as those used by Deloder (and let's get honest here — what proportion of Deloder-hit machines have other than a null admin password? Probably about 1% of them, yeah?) are either going to read your analysis or even care that they are infected? Those that use antivirus or anti-Trojan software who were hit before they got their update that detected it will simply clean it and go on their way. Whether they have an unwanted VNC installation left on their machine is actually something they don't care about, because even if they did remove VNC, they will have left their admin password blank and their Windows Network bound to their external Internet interface for no good reason. These people will always exist and they will always pose just this kind of risk to the rest of a public sewer-style network such as the Internet. If you want to change that, you have to design and implement a different Internet.

Re: Deloder worm has resurfaced. Watch your privacy!

comp.security.misc: Re: Deloder worm has resurfaced. Watch your privacy!

- > ... *In addition, if people*
- > *don't get the information on what EXACTLY the worm did, how do you*
- > *know what proper actions to take to protect end-users?*

As I've already said, people do not need to know "exactly" what the worm did. They need to know enough to determine if it is likely they have it or have had it and, if it has been removed, whether any "collateral damage" remains and if so what the best course of action is. And, in fact, although you claim to have provided this "exact" information, I find your analysis quite incomplete and only partial. Of course, few people would want a sub-routine by sub-routine description of *\_exactly\_* what the program does, but you rightly understand that and provided a generally good condensation of the important points to a reasonable level of detail for most likely readers of your analysis.

However, that still does not justify the unethical release of the password, as described in detail in my previous message and above...

- > *CERT advisory, <http://www.cert.org/advisories/CA-2003-08.html>,*
- > *mentioend that 140,000 connections on an IRC network, which are the*
- > *systems infected with Deloder type of worms.*

How do you know that they are Deloder-ed systems? CERT claims that the 140,000+ network was a GT-bot network and as these IRC-controlled bot-nets usually use a specific IRC channel (or group of channels) they presumably made that claim because the channel(s) involved were configured in GT-bot samples retrieved from some of the affected machines. As GT-bot is not normally spread via open or weak-passworded Windows shares, I fail to see how CERT's claim of a 140,000+ GT-bot network translates to 140,000+ possible Deloder infections.

- > *If you think the advisories and analysis are generated good awareness,*
- > *why are there still so tens of thousands of computers out there*
- > *infected with Deloder and other worms and Trojans, and why aren't they*
- > *doing anything about it?*

I've answered that above.

In short, most of the people running those machines simply don't care enough...

- > *That's why I published my article.*

...and it will fail to "help" any more than all those previous ones as the people whose machines remain the problem are no more likely to see your advisory or be swayed into caring enough as a result of seeing it than they are to see any of the others.

--

Nick FitzGerald

Re: Deloder worm has resurfaced. Watch your privacy!