

## Re: Virus is getting domain account listing

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-05/0034.html>

---

*JGrimshaw\_at\_ASAP.com*

**Date:** 05/10/04

To: David Carlin <djc6@cwru.edu>  
Date: Mon, 10 May 2004 13:40:57 -0500

Hi David,

You'll notice the process ID for NT 4 and 2000 servers is always the same, regardless of what name you give it. I would expect that someone or some software is targeting those.

In 2003 you can change the process ID of the admin account. That likely is not reason enough to upgrade, but it would prevent the targeting of the admin account.

As for your other question, to get a list of users, I believe that in a windows domain, you only need to be connected to the domain as a valid user. Play with the net user command at your command prompt and see what you can discover. Any regular user can access this. Even the guest account, . The net user command is used for useful scripting in batch files, with a few unfortunate side effects of permitting a lot of information out that is useful for your virus or person.

So, anyone in your college campus with a penchant for Windows commands could likely be capturing your user list on a regular basis if they have access to the command prompt, or the run command.

Given greater access, net user can be used to create accounts, change passwords, create a local admin account, install terminal services, things like that. Never leave an admin login unattended—lock the desktop when you walk away!

The default user with no other privileges can get a list of all users, and more specifically, find out the password policy on any given user (such as min/max days), and also the name of any logon scripts, and the security groups the users is in.

With all of that kept in mind... an admin account carelessly left unlocked on an end user station where software was just installed (in admin mode, of course) from one of your local desktop services guys, (get ready for a run on sentence) but the account didn't get logged off when done because the desktop guy with admin rights walked away with the user to get

## SecurityFocus Microsoft: Re: Virus is getting domain account listing

coffee... can easily create a domain admin account with all the appropriate security groups—right from the command prompt or run command.

Scary, hmm? It's especially scary in a campus lab, where a lot of the students would never see what just happened.

Imagine what someone could do with a batch file, default user access, and the net user command? Echo the results to a text file, any network share the user has access to, or even a printer, and someone has your list.

Armed with that knowledge and some scripting knowledge, a password dictionary attack against every single account could happen. The person would be stupid to do so, and would cause a denial of service attack in the process (locking out all accounts, as you commented on) and thus raise the alarm, but the anonymity of this is very appealing. The person responsible would have to be caught running something he could have set up in a task scheduler by now on multiple machines, or caught picking up the data—which could also be scheduled to go somewhere else via FTP, which is a default program within Windows.

I think your best option for catching someone like that, assuming someone is doing that or that it is a virus, is get familiar with the windows event log viewer (use logon auditing for failed logons) or get an IDS sees multiple failed logons as a signature or a rule that it reports on. I do not have much experience with IDS's, so I can't vouch for any that can do that. The security basics list could probably steer you in the right direction.

David Carlin <djc6@cwru.edu>  
05/10/2004 08:10 AM

To  
focus-ms@securityfocus.com  
cc

Subject  
Virus is getting domain account listing

Hello,

I work on a college campus and have been plagued for months by something that is going through all of the accounts in my domains and locking the accounts out by failed password attempts. I have two PDCs for two different domains, running NT 4.0 and clients running XP scattered around campus in various subnets. I have setup an ACL on my cisco switch to block traffic to the PDCs except from these subnets, but it doesn't help because there are machines in those subnets administered by other people that continue to get "infected".

Re: Virus is getting domain account listing

SecurityFocus Microsoft: Re: Virus is getting domain account listing

My question is, how do I stop whatever this is from getting my account listing in the first place? I have run Microsoft baseline analyzer, it says I'm all good.. The free Nessus scanner doesn't report any problems. I have all patches, RestrictAnonymous=1 is in the registry.

I've renamed my admin account, this thing always picks up on it. It knows which accounts are domain admins and attacks them more aggressively. I've contacted the owners of the various machines attacking, they never find any strange software, virus scanners always come up empty – even when done remotely over the administrative shares.

Any ideas how to protect my user list?

–David

-----  
-----  
-----  
-----