nakedsecurity.sophos.com

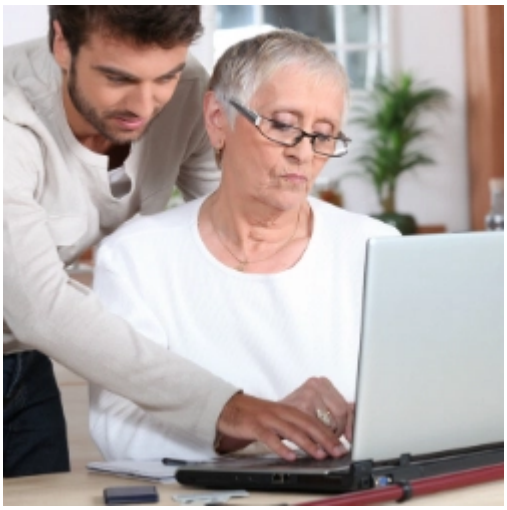
# Thousands of computers open to eavesdropping and hijacking

*by Lisa Vaas*

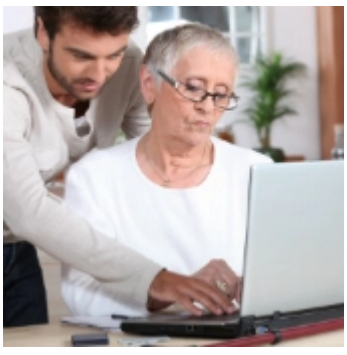
5-7 minutes

Skip to content

Award-winning computer security news



## Post navigation



There’s a gaping hole in thousands of unsuspecting people’s

computers that lets any random internet passerby not only look over their shoulder but reach through to take over their systems.

The hole is caused by a remote access tool: specifically, unsecured use of a product known as Virtual Network Computing (VNC).

VNC is actually a handy application that lets us remotely share our desktops with others – be they colleagues, those giving us software demonstrations, or remote administrators helping us diagnose system problems.

But if VNC isn't locked down with a strong, unique password, the list of who can remotely view and control our computer systems remotely can also potentially include eavesdroppers or intruders looking to compromise computers.

Also, it can include security engineers assessing what's exposed on the internet that shouldn't be.

At Defcon on Sunday, security engineers Dan Tentler and Paul McMillan fit into that last category.

During their 1-hour talk, Tentler and McMillan scanned for computers running remote access software without a password.

In just that brief time, the results poured in as the pair discovered thousands of computers on port 5900 using unsecured VNC for remote access.

According to Forbes's Kashmir Hill, the total number of unsecured VNC instances the pair discovered in 1 hour likely exceeded 30,000.

On Thursday, McMillan's Twitter stream was showing an

assortment of links to screen grabs that illustrate what things people are leaving wide open.

The tweets included screenshots that seem to pertain to oil or natural gas wells in Texas, another of what looked like the schematic for an Italian hydroelectric plant and this one (blurred by Naked Security) of a Novell ConsoleOne administration window – an application for managing an entire computer network and all its resources:


> @PaulM
>
> This would be the one machine you would leave unsecured to the public internet, right?

Forbes's Hill reports that at Defcon, she also got an eyeful of screenshots that showed people:

- checking Facebook
- playing video games
- watching *Ender's Game*
- reading Reddit
- Skyping
- reviewing surveillance cameras
- shopping on Amazon
- reading email
- editing price lists and bills
- watching porn

…as well as access screens for these things:

- pharmacies
- point of sale systems
- power companies
- gas stations
- tech and media companies
- a cattle-tracking company
- hundreds of cabs in Korea

Hill actually called one of the pharmacies. They were reportedly horrified to find out that anybody could review their patients' prescriptions.

Because this isn't just about viewing, it's about people being able to take over those systems and do things like change a power

company's settings or flip through a company's business records.

I'd like to think that the researchers contacted all the computers' owners, asked their forgiveness for accessing their computers and private data without permission and then gave them a chance to secure themselves before revealing anything to the world.

That seems highly unlikely, perhaps even impossible, but that is the standard of responsible disclosure that we've come to expect of security researchers exposing vulnerabilities.

So how can you minimise your exposure to this kind of backdoor access? The rules are simple:

1. If you don't need it (whatever *it* is), don't run it
2. If you do need it, protect it with a strong, unique password
3. Provide the most restricted access you can get away with
4. Use multiple layers of protection

   For example if you *need* to run VNC but only one other person or computer needs access to it, you might use your firewall to allow just one, hard-coded IP address to connect.

   If you need to give access to multiple computers, you might restrict access to any computer on your Virtual Private Network (VPN).

   Exactly how you lock things down depends on your environment, but the principles to follow are as old as the hills: Defence in Depth and the principle of least privilege.

   The pharmacist whom Hill called immediately contacted his

software vendor, who was shocked to discover there was a way around the firewall and immediately turned off the VNC settings on the drug terminals.

Unfortunately, the chances that a helpful security reporter or security researcher is going to call to let us know that we're leaving our systems exposed is slim to none.

Most of us have to strap this stuff down ourselves, and urge others to do the same.

**NB.** We have to say it: please don't try this at home. Or at work. Just because you *can* connect without a password to someone's computer system doesn't mean you are *allowed to*. It's not like trespass, which in many jurisdictions is a civil matter. Many, if not most, countries have laws making it a *criminal offence* to access a computer without authorization. Your motivation probably won't be enough to get you off the hook if someone decides to investigate and you end up facing criminal charges.

*Image of people using computer courtesy of Shutterstock.*

## Post navigation