

Feature article - For immediate release
Reproduce freely, No copyright restrictions, Image available
820 words

20/01/2006

Airport security under siege

Sometimes security dangers aren't as clandestine as you may think. In fact, one of the most serious threats to your firm's security could be sitting next to you... in the airport departure lounge.

Engineers from the global security consultancy Scanit have found documents and emails that could bring some global companies to their knees, on public access terminals in airport departure lounges.

What began as a mixture of curiosity and boredom led consultants from the Dubai-based network security outfit to uncover a plethora of secrets left by globe-trotting executives logging on in-between flights.

While such senior figures possess high-level knowledge of their companies' affairs, they often aren't equipped with a knowledge of IT security precautions to match, as Scanit discoveries show.

The average executive lounge offered to business and first-class flyers is equipped with a number of PCs that allow visitors open access to the web.

Each PC is installed with a standard Windows package that includes Microsoft Explorer, Outlook Express and sometimes Office.

As a weary executive pulls up to a terminal, a sense of familiarity encourages them to behave as they would at home or in the office and send an email the same way. Why not use Outlook, just as they would at their desk?

But this could be a costly mistake.

Outlook Express is probably not configured to allow emails to be sent from such machines, so the correspondence simply moves to the system's 'outbox' where it remains indefinitely after the user clicks 'send'. And if the system *is* configured to send messages, the email that goes out is automatically saved to the machine's 'sent items' folder.

In either case, the message is ready for anyone to access at their leisure.

While travelling to meet clients, Scanit engineers have found everything from intimate missives to mistresses (perfect for blackmail) to desktop-saved documents outlining multi-million dollar deals, complete with profit margins and lowest bid values.

However, they also stumbled on something more sinister. Many machines, they found, are infected by Trojans - or back-door programs - to monitor, record and relay information entered by the execs to someone watching their activities externally.

Scanit CEO David Michaux recalls a discovery he personally made while waiting for a delayed flight.

“As I was playing patience, I noticed heavy network traffic on the lounge machine’s taskbar even though I wasn’t using any network applications.

“After some delving I was amazed to find Back Orifice 2000 (BO2K) as the culprit. It had been invisibly collecting my keystrokes and sending a record of them to a Hotmail account every 15 minutes!”

Michaux reported his findings to the lounge receptionist who responded by explaining she couldn’t take responsibility for the security of the machines.

BO2K is a well-known Trojan capable of taking full control of the machine it has infected. The perpetrator is able to view the machine’s webcam, listen in on its microphone and watch a streaming video of its display, all in real time.

Another lounge security lapse Scanit found – this time at a London airport – allowed users to log on to machines as Administrator, meaning they could download and install any software.

Again, engineers found key-loggers had been installed on systems there, configured to send information to an external email account at regular intervals.

“The danger is that the CEO types who travel on behalf of their companies and use these lounges are privy to usually sensitive data,” Michaux explains.

“This makes computers there a veritable goldmine, whether it’s executives downloading attachments from their webmail and leaving them on the desktop, or even deleting them afterwards, but not emptying the recycle bin before they get up to catch their plane.”

What’s more, he adds, execs who do take precautions are likely to be let down by the lounge’s security itself, especially if a hacker has turned its machine into listening posts.

As airport lounges increasingly offer passengers wireless internet access, existing Trojan problems *are* being eliminated.

But as so often happens in the world of IT security, this new era will usher in a whole new family of network malignancies.

Until then, I've got a plane to catch...

Sidebar: **How to increase your security**

- Check to see if there is a known anti-virus system installed on the PC. Most of these now detect Trojans and hacking tools and keep them at bay.
- Check to see if your machine has a clean desktop. While this guarantees very little, it does show whether previous users have been downloading packages that may have carried an infected payload.
- Use one-time passwords for accessing web-based email. These usually come in the form of USB key rings that synch with your email server at the office. They ensure that if a key logger does capture your password, it will be rendered void when the hacker tried to use it.
- Always delete anything you've downloaded or worked on when you finish a session, and then empty the Recycle Bin.

Notes to Editors:

1/. Scanit is a leading home and corporate security systems company with operations in Belgium, Dubai and Iran. It is the prime services agent for Symantec in the Middle East. You can find out more about the company at: <http://www.scanit.net>

2/. Scanit's primary services include: Security audits, Company IT risk assessments, Incident Handling, Security Consulting, Technical Fraud Investigations, Awareness Campaigns, Secure Line Communications, Bulk Software Purchasing, Constant Update Modules and PBX penetration Testing.

3/. Scanit offers a number of courses for IT consultants who want to learn more about hacking tools and techniques, including: Ethical Hacking, Exploit writing, Secure Web application, Wi-Fi security & anti-security, Telecommunications fraud and SS7 signalling.

Buy-out courses are available for companies wishing to train staff in the privacy of their own facilities. For more on training, see: <http://www.scanit.net/courses>

For further information or interviews, please contact:
David Michaux, CEO Scanit
Phone: +971 50 455 4031
Email: david@scanit.net

A .jpeg image of David Michaux (1Mb) is available to download for media usage here:
<http://www.presswiremedia.com/PR%20work/scanit/david.jpg>

Press release by Presswire Limited
<http://www.presswiremedia.com>