



Electronic Warfare Associates – Australia

## "Three minutes is all it took to be owned And in trouble via the Internet"

Within three minutes our new laptop was under the control of a worm and we had no other option but to perform a complete reinstallation of the Windows XP operating system to ensure we had a clean system.

### *What is the life expectancy of a new system's survival rate of on the Internet today?*

This was a question EWA InfoSec team asked themselves and set about validate. We had just received a new laptop fresh from the shops, installed with the newest OS Windows XP.

We conducted our test under the scenario of a normal home user bringing a freshly new system home and wanting access to the Internet. The home user knows there are a lot of nasty's out there on the net, and the requirement for patching and to have a firewall in helping in protection from the Internet. So the InfoSec set about updating our new Windows XP for service-pack one and all the other patches and a free firewall to help with protection.

Connecting the EWA guinea-pig laptop to a broadband connection and selecting Windows update controls, before we had Service-Pack one downloaded, our guinea-pig laptop was compromised by the mblaster worm, in under three minutes.

We knew of the ownership of the laptop by the worm, since we were monitoring for the attack, however it may not be obvious to a home user. The required Windows XP service pack-one was download as well as a free firewall; we had to reboot the system allowing the updating of Windows and the firewall to take affect. However we were losing control of the system to the worm and other programs, the laptop was owned. After fighting with the worm, to gain some access to windows, so we could reboot the system.

Now attempting to control the laptop, the InfoSec team accessed the Internet to download the next free to help combat the worm a virus scanner. The system was

running too slow to our responses. We attempted to see what processes were running, we found a strange small 64K programming running, that we could determine was installed within a registry setting, allowing for the survival of reboots. The network connection was getting poor. We also found another small 64k program installed on the system at the same time, now we knew we were really trouble and had little control over the system. The decision was made to perform a reinstallation of the OS – concluding the test.

Under this test EWA took the role of a normal home user that has purchased their system and wishes to protect it, through normal windows patching and downloading of a free firewall, within three minutes the system was owned and out of control. What chance does an unaware home user have today?

The IP address ranges for Telstra's and Optus's ADSL/Cable services are well known and the various worms can be targeted to enumerate up and down these IP address ranges looking for that soft target to own – the home users as well as small companies.

### *Can we totally rely on patching for protection?*

**NO!** During December 2003, Microsoft discovered that a glitch in their patching process resulted in a November fix not being applied to some Windows XP computers (Source: zdnnet.com.au 11 December 2003).

Though this had nothing to do with the attack directed at our system, it leaves a user even more vulnerable if totally relying on just patching their systems. Security (protection) must given at home be in a form of layers (security in depth).

EWA AUSTRALIA





Electronic Warfare Associates – Australia

**"Three minutes is all it took to be owned And in trouble via the Internet"**

***"Internet worms and critical infrastructure"***

Considering the security and protection in the real world, [Bruce Schneier, article in zdnet.com.au 10 December 2003](#), "Internet worms and critical infrastructure" discusses the possible impact that Internet worms had in the recent US energy power failures through the east coast and even these companies had some form of security protection in place. An underlying theme in the article is that the owners were unaware that their systems were in trouble in the first instance and how much trouble they were in; leading to a rippling effect in helping bring down the power grids.

***"Unaware of types of attacks"***

Considering that not even critical infrastructure are not safe from these types of attacks, what chances do home users have? The EWA InfoSec team, while performing network vulnerabilities assessments for clients, has found home user accounts of administrators, of these clients, and some times the higher level management home accounts. Though EWA does not attack these accounts, we provide

this information in our report highlighting - information leakage and that an attacker would hack these home accounts and thus creating a threat from a trusted back-door into the organization.

***Not just threats to the home users!***

These types of attacks are not just threats to the home users, how many small businesses are out there with a direct Internet connection? These could include organizations that hold information that is required to be protected, such as a used your local doctor, accountants or lawyers.

The Mbaslter worm that compromised our guinea-pig system was successful due to a basic vulnerable in a network required communication port called TCP/IP 135 being open to the Internet. This TCP/IP port is open by default and a non security aware person would not know what to do to protect them. Even today a firewall is not enough as a form of protection.

Ron Brandis is a Senior Information Security Consultant with Electronic Warfare Associates-Australia Pty Ltd (EWA-Australia). Ron has held a variety of Information Security consultant and development roles in both the public and private sectors, notably with the Department of Defence and within the intelligence community. His duties have included:

- Risk, Threat and Vulnerability Assessments,
- Penetration Testing and Forensic Analysis,
- System Auditing & Compliancy Assessment, and
- Training development & delivery.

Ron has extensive experience and in-depth knowledge of computer network and architecture security. His sixteen years of experience spans software engineering, computer communications, system administration, and security investigations. Ron's special expertise lies in risk, threat, and vulnerability assessments of applications. He has conducted numerous vulnerability and penetration tests for clients ranging from small businesses to international organizations, and has also provided hands-on training for clients in hacking techniques.

Ron is also a Certified Information Systems Security Professional (CISSP)

---

**For more information contact: [infosec@ewa-australia.com](mailto:infosec@ewa-australia.com)**

**Canberra:**

Level 1  
214 Northbourne Ave  
Braddon  
ACT 2612

Tel: +61 2 62 30 6833  
Fax: +61 2 6230 5833

**Brisbane:**

Level 30 AMP Place  
10 Eagle Street  
Brisbane  
Queensland 4000

Tel: +61 7 3303 8592  
Fax: +61 7 3303 0111

**Adelaide:**

Innovation House  
Mawson Lakes Boulevard  
Technology Park, Mawson Lakes  
South Australia 5095

Tel: +61 8 8260 8261  
Fax: +61 8 8260 8260

EWA AUSTRALIA