Digital underbelly of the World

by Kismo *Sunday, Mar 9 2008, 10:15am*
international / miscellaneous / commentary

> The crews laugh at times at the lack of expertise displayed by western government agencies in the area of IT security. The Internet belongs to those with the greatest level of skill and there is no shortage of it ‘out there’ – crews, teams and individuals -- but sadly very little real talent ‘in there,’ moronic government agencies and corporations. No real hacker could tolerate an office/fixed environment for more then a day or so! It is the nature of the beast and the environment in which it lives.

Neither the Chinese with their RPC, ICMP hacks, or other tunnel hackers can match the ‘Uber’ elites who are only detected by each other, they 'own’ the wire – always have, always will!

Novice hackers have made the news with their antiquated methods; yet even those modified 15-20 year old tricks have proven effective against outer layer government departments and private corporations that provide ‘security’ services – what a laugh!

Methods originally developed by the Russians have found their way to Israel, probably via immigrating Russian Jews. Mossad foolishly attempted to plant code in commercial security software and make it available to the world; a free ride into everyone’s system -- the term ‘trojan’ is no accident in IT circles. Damn shame end users instinctively recoiled at Israeli ‘security’ software packages!

The Chinese have never displayed real flair in original development and NEW methodologies, they appropriate what others have developed and alter it to their needs – any good real time firewall, properly coded and configured provides hours of entertainment for hackers and geeks alike.

Numerous attempts at penetration, usually from (ro)bot systems, with 'telltale' IP addresses all pointing to China actually do not indicate the REAL source, as any half-baked security consultant would tell you. It takes highly developed skills and tailored packages to trace the real source of these generally ‘spoofed’ attacks.

What is more amusing for ‘elite teams’ is the success these low-level groups have had using outmoded and known methods -- a very poor reflection on 'security' firms and the commercial industry. Consultants are expert at mouthing jargon and convincing their clients that there is no such thing as real security in the digital world – which is reason enough to dump them in favour of open source solutions.

The press informs us that a suitable project name “Cyber Storm II” has been coined and that Internet security will be tested by a myriad of government agencies and private companies – all at the taxpayers expense I might add! The problem of course is the minimal level of expertise these testers possess! The reality is that all participants, including the ‘experts,’ have been previously compromised by hacker elites and will no doubt be compromised again – it is the nature of the game!

In Australia an advert for a local spook agency is running alongside a hacker article in the popular press. Who or what exactly do these inept idiots think they will attract with their low paying jobs and stultifying working environments, certainly no talented hackers -- that is certain?

So the real exercise reduces to just another money-making venture for various listed corporations; reminds me of the Tamiflu wank and one of its major shareholders!

What could anyone offer crews that are able to milk the wire for millions at will – ‘money isn't everything but it will do until everything comes along!’ I would add that for ideological reasons, most hackers cannot be bought.

According to standard tests of 'normality,' genius hackers are supposed to be dysfunctional and very disturbed people -- that is their strength, others embrace what conservatives reject. There is nothing 'normal' about genius! What do you imagine these very hurt and abused young people would do if given the opportunity and means to exact retribution -- ask the Banks and the many compromised 'gov' departments!

According to Sun tzu, the enemy’s greatest strength is also its greatest weakness; this is borne out perfectly by the dependence major organisations have on digital technologies today.

Digital technology has created a very uneven playing field, in favour of the brightest, fastest and most skilled! For the relatively modest price of a few clustered systems, a few individuals have the power to compromise States -- large corporations pose no problem whatsoever, just ask the major financial institutions and Banks, billions are lost every year!

Greetz to ‘ferrite’, ‘head’ and all the crewz. We thank you for your help and generosity, it has relieved us of the need to 'work' for a living!

Most exceptional hackers have been and will continue to be badly treated and abused by mainstream society, a bitter irony for some. Nothing gives hackers greater pleasure than dancing on the wire, milking sacred cows and serving it ‘up!’

We do it better and we do it for free, just to piss you off -- immature and dysfunctional are we? Why then do you continue to offer us almost anything for our 'services' and skills, you lying fucking hypocrites?

http://www.washingtonpost.com/wp-dyn/content/article/2008/03/07/AR2008030701157.html

http://news.theage.com.au/egames-to-test-infrastructure-security/20080306-1xnn.html

---

Cleaves Alternative News. http://cleaves.lingama.net/news/story-965.html