The Sydney Morning Herald

National

This was published 20 years ago

Hug a hacker, before they go underground

February 19, 2002 — 11.00am

In June 2000 a hacker named RFP (Rain Forest Puppy) wrote the RFPolicy for vulnerability disclosure, which sought to create a set of rules by which individual hackers and researchers deal with security vulnerabilities.

For the most part this has been the de facto policy that hackers have adhered to and vendors have accepted.

It created a framework that allowed a working relationship to form between hackers, security professionals and vendors.

Quoting from RFP: RFPolicy is an initiative to help establish concrete guidelines for disclosure of security problems. This was prompted due to many recent responses from vendors such as "we were never given a chance" or "there is an 'unwritten' standard of notifying the vendor X days ahead of time".

RFPolicy works like this: A hacker or "researcher" finds a vulnerability in software made by a vendor. The hacker contacts the vendor and alerts them to the vulnerability. The company then has time to investigate the problem. A patch can then be written and an "advisory" can be released. The advisory usually gives full credit to the hacker for finding the vulnerability. The hacker is free to disclose to the hacking community the exploit code for the vulnerability exactly one week after notifying the vendor.

The exploit code is basically pre-written software, usually coded in C or Perl script (often referred to as "shorthand for geeks"), which can be used to exploit the newly discovered vulnerability in a system that has not yet been patched. In a nutshell, this is what the RFPolicy full disclosure policy is.

Unfortunately, several large software vendors have chosen to move away from this model. Now when a hacker finds a hole in a software product, vendors demand that they be alerted to the problem immediately and that the hacker not discuss the details of the vulnerability publicly. The vulnerability details are never released and vendors threaten to sue anyone who dares to publish the exploit.

As a result, most vulnerability research and exploit codes have gone underground and vendors are often not notified of security holes in their software.

An exploit is coded and passed on to the underground hacking and cracking community only. This means that many computers are being hacked through undisclosed security holes.

Because the vulnerability is undisclosed, there is no patch or defence of any kind available, so the fight is lost before it begins.

But this is not where the problems associated with non-disclosure models end.

Full disclosure ensures that any patch released by a vendor has to work properly. When an exploit code is made public, the vendor comes under the scrutiny of the entire security community.

However, because teams of litigators under instruction from proprietary vendors are monitoring public security forums, many are now too scared to publicly post vulnerability information.

Many are too eager to forget that the average hacker is no more than a software boffin with an enthusiasm for picking apart code. They strive to improve security on the Internet and scrutinise poor software engineering.

Perhaps large organisations believe their security images will benefit if talk of vulnerabilities in their products is pushed underground. Perhaps they are merely frustrated at being humiliated as security hole after security hole is found and made public.

Many argue that by keeping security issues transparent, vendors can benefit from the vast computing expertise of the new-millennium hacker. -- with Adam Pointon

Patrick Gray is a data security consultant with Sentinel Data Security and can be e-mailed at patrick@sentinelsecurity.net. The RFPolicy is available at: www.wiretrip.net/rfp/policy.html