GCHQ gets it right - their web devs don't

Michael Barwise

The 2011 GCHQ challenge has been solved by at least two people with the best part of a week still to go. The most informative description of the route to the solution (by Nick Craig-Wood) goes into considerable detail. Stage one required a block of data to be recognised and tinkered with to turn it into valid executable code. This code hid on the stack a URL that, when called, fetched the second stage - "a description of a VM with an initial state, but no code to implement the VM." Craig-Wood implemented a VM in Python, and after running it, found in a core dump a URL that fetched the third level of the puzzle. This turned out to be a Windows .exe file, relying on the cygwin cygcrypt dll to run. The task here was to obtain a key that the GCHQ server would recognise as valid and respond to with an acknowledgement of success. The whole exercise apparently took Craig-Wood about 12 hours, and I feel it was quite a cunning piece of work both on his part and that of GCHQ. Not a hugely difficult task technically at each stage - probably no more difficult intrinsically than analysing a typical piece of malware, but the overall exercise required considerable intuition.

When this competition was first announced I was sceptical about its validity, as I'm very conscious of the general over-emphasis of the "überhacker" threat in the face of our appallingly weak defences, and this looked from the publicity like yet another high-order geek test. But I see the point now, and it's probably a good one. Unless I'm very far from the mark, GCHQ are seeking people with well developed imagination and intuition in addition to deep technical skills, and that is exactly the kind of people we increasingly need in infosec. Too many infosec practitioners are used to slavishly following "standards" and "best practice" (i.e. other people's rather elderly ideas) without ever thinking for themselves. That's one of the reasons why the defence fails so often, even in the face of threats that are not that sophisticated - and that's the vast majority of real threats.

So more power to GCHQ for getting this right in the technical arena. What I hope to see (and, I also hope, soon) is the same recognition of the need for imagination and intuition emerging in other areas of security management - both in the government and commercial sectors. When we have achieved that, we have a chance of taking control and making the electronic infrastructure truly robust against attack instead of responding reactively and being regularly wrong-footed by the most basic of attacks as at present.

It turns out that GCHQ got this right, but their web developers didn’t. Among others, Charles Meaden has pointed out that the acknowledgement page was public and had been spidered by Google by December 1st, allowing any one to present themselves as a winner having bypassed the tests entirely. Did I say something about being wrong-footed by basics?

Originally appeared on the Infosec Reviews blog as "Craig-Wood Gets it Right - So Does GCHQ", December 2011