Amnesty International UK site flung Gh0st RAT at surfers after hack

By John Leyden

Published: 2012-05-11 · Archived: 2026-04-05 15:32:16 UTC

Amnesty International UK's website was hacked early this week in an assault ultimately geared towards planting malware onto the PCs of visiting surfers.

Malicious Java code was planted on the site in a bid to push the Gh0st RAT Trojan onto vulnerable Windows machines. If successful, the attack plants malware onto machines that is capable of extracting the user's files, email, passwords and other sensitive personal information.

The attack, which ran between 7 and 9 May, was detected by web security firm Websense, which informed Amnesty about the threat. The human rights organisation has since cleaned up its site.

Amnesty International is no stranger to this type of attack. Its UK site was hit by a similar drive-by-download-style attack back in 2009, and a similar assault was launched against its Hong Kong site a year later.

Websense has a write-up of the latest assault in a blog post here.

The Gh0st Trojan has been used by suspected Chinese hackers in several advanced persistent threat (APT) style attacks, most notably the ‘Nitro’ attacks against energy firms in 2011. Chinese involvement in the Amnesty International attack is suspected but unproven.

"Yesterday [Wednesday] Amnesty.org.uk was infected with a piece of malicious code. As soon as we became aware of the infection we worked with our hosting company to isolate it and remove it as a matter of urgency. The problem was resolved by yesterday lunchtime," the organization told *El Reg* in a statement.

"Security is very important to us and as well as extensive security measure in place to prevent exploits such as this, we also have constant monitoring in place to alert us immediately when incidents like this occur. 'All our users profiles are held on a completely separate website and server and were in no way compromised by this incident." ®

Source: https://www.theregister.co.uk/2012/05/11/amnesty_malware_rat/