


{ * SECURITY * }

Amnesty International UK site flung Gh0st RAT at surfers after hack

Do-gooders done for

By [John Leyden](#) 11 May 2012 at 16:28 5  SHARE ▼

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 *ET 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.'" ®

Sponsored: [Practical tips for Office 365 tenant-to-tenant migration](#)

Tips and corrections [5 Comments](#)

 **Sign up to our Newsletter** - Get IT in your inbox daily

[MORE](#) [Websense](#) [Human Rights](#) [Drive-By Download](#)

// MOST READ

- 1** NASA to launch 247 petabytes of data into AWS – but forgot about eye-watering cloudy egress costs before lift-off
- 2** British Army adopts WhatsApp for formal orders as coronavirus isolation kicks in
- 3** Closed source? Pull the other one... We love open source, but not enough to share code for our own app, says GitHub
- 4** Forget James Bond's super-gadgets, this chap spied for China using SD card dead drops. Now he's behind bars
- 5** SpaceX beats an engine failure to loft another 60 Starlink satellites

SUBSCRIBE TO OUR WEEKLY TECH NEWSLETTER

[SUBSCRIBE](#)



// KEEP READING



Microsoft nukes 9 million-strong Necurs botnet after unpicking domain name-generating algorithm

Takedown should (in theory) see spam volumes shrink rapidly



Mirai botnet malware offspring graduates from uni, puts on a suit, slips into your enterprise

Isn't that what we all want for our kids, after all?



Huygens if true: Dutch police break up bulletproof hosting outfit and kill Mirai botnet

Cops also Cruyff cloggy couple



Malware hides as iOS jailbreak, Sucuri is insecure, and China is about to get even worse

ROUNDUP Plus, new allegations in Iran and American hacking war



Malware scum want to build a Linux botnet using Mirai

Hadoop YARN is the attack vector, so lock it away



Newb admits he ran Satori botnet that turned thousands of hacked devices into a 100Gbps+ DDoS-for-hire cannon

One moron down, two to go



China's Winnit hackers (apparently): Forget the money, let's get political and start targeting Hong Kong students for protest info

Supply-chain hackers now taking aim at kids fighting for democracy, say researchers



In a desperate bid to stay relevant in 2020's geopolitical upheaval, N. Korea upgrades its Apple Jeus macOS malware

Nork cash grab nasty gets stealthier

// TECH RESOURCES



Le Guide Des Échanges Transversaux Pour Les Entreprises En Croissance

L'équipe financière en tant que partenaire de l'entreprise



8 ways Legacy ERP Harms Businesses

Download this white paper to learn the 8 ways by which legacy ERP systems hold back your business and how "version-less" cloud ERP can help eliminate costly upgrades, reduce IT infrastructure management, and drive value with rapid implementation.



Executive Briefing: Kritische Gartner-Funktionen für Webanwendungs-Firewalls

An Akamai whitepaper



Secure Enterprise SD-WAN

Organizations are turning to SD-WAN as a cost-effective way to establish local internet breakouts and simplify traffic routing for the branch.

ABOUT US

[Who we are](#)
[Under the hood](#)
[Contact us](#)
[Advertise with us](#)

MORE CONTENT

[Latest News](#)
[Popular Stories](#)
[Forums](#)
[Whitepapers](#)
[Webinars](#)

SITUATION PUBLISHING

[The Next Platform](#)
[DevClass](#)
[Blocks and Files](#)
[Continuous Lifecycle London](#)
[M-cubed](#)



SITUATION PUBLISHING

The Register - Independent news and views for the tech community. Part of Situation Publishing

SIGN UP TO OUR NEWSLETTERS

Join our daily or weekly newsletters, subscribe to a specific section or set [News alerts](#)

[SUBSCRIBE](#) >

