Repeated and sophisticated attacks from Russia and China against the website of Human Rights Without Frontiers

HRWF (14.10.2014) - On Saturday, the Brussels-based NGO *Human Rights Without Frontiers* received a message from Intermedia, its Web hosting provider and the world's largest independent provider of hosted Exchange, notifying us of another attempt to compromise our Web server. Our Internet and Security consultant explains: "Another series of repeated hacking events over the last 48 hours seeking to hijack or disable our server were detected on hrwf.org and hrwf.net. Our server logs also indicate numerous brute force style attempts to gain access to our CMS (Content Management System) primarily from allocated unspecified IP addresses and from allocated IP addresses that we were able to trace back to Ukraine using data from The RIPE NCC which is one of five Regional Internet Registries (RIRs) providing Internet resource allocations, registration services and coordination activities that support the operation of the Internet globally. Whoever they are, they are obviously persistent and well equipped and we have to assume that they are the ones who for some time now have been trying to compromise our servers. "

Our Internet and Security consultant continues: "As our System Administrator was monitoring the server, he noticed that the hacker(s) successfully placed a script in a file on our Website. That file was requested on 10/10 at 22:23 GMT from this allocated unspecified IP address 64.78.39.13 (supposed to be EU Country but can be from any other country in the world) and the same IP address sent several other POST requests to our server on 10/10 and 10/11 and started sending SPAM from our servers on 10/11 at about 2 PM PT. It should be noted that not longer after that script was modified, a number of other files on our server were accessed and modified from 37.139.47.122 IP address. According to The RIPE NCC, that IP address is allocated to a person in St. Petersburg, Russia. So we had to briefly stop our Website and remove the offending script and check all server data and clean our files. Since this procedure can be time-consuming, we decided to perform a restore from a known clean backup."

This latest incident follows a series of damaging server attacks that were carried out between June and August. These seriously disrupted the normal functioning of our website for three months. Each time, thousands of files on our Web Server had to be checked one by one. Unfortunately and regrettably, the first successful attack (believed to have originated from China) on our old CMS caused several emails with inappropriate contents to be sent in our name. Due to constraints in our previous server environment and in the vendor's release of needed upgrades scheduled only for December 2014 (these constraints beyond our control and the often limited resources situation we usually face left our old server vulnerable), HRWF had not only to invest in a different new server system environment but also hire web developers who could perform the difficult unofficial migration of all existing data to a vendor-independent upgrade and migration solution.

Despite constant upgrades of our protection against hackers, the website *Human Rights Without Frontiers* has for years been targeted by sophisticated IT attacks but this time has decided to make it public and to call upon all human rights organizations to denounce such practices. *Human Rights Without Frontiers* will publicize any similar case that will be brought to its attention.

The director of *Human Rights Without Frontiers*, Willy Fautré, commented: "No doubt our almost daily coverage of the events at Maidan, in Crimea and Eastern Ukraine explains the latest attacks. For years we have as well reported worldwide and at the European Parliament about violations of human rights in China. We are aware that we disturb the state disinformation policies of Russia and China but such threats will not deter us from pursuing our mission."

Last minute info:

Our Internet and Security Consultant managed today to find the name and address of the person in Russia who tempered with our files on the server. Our consultant can be reached at netsecurity@cowetatech.com