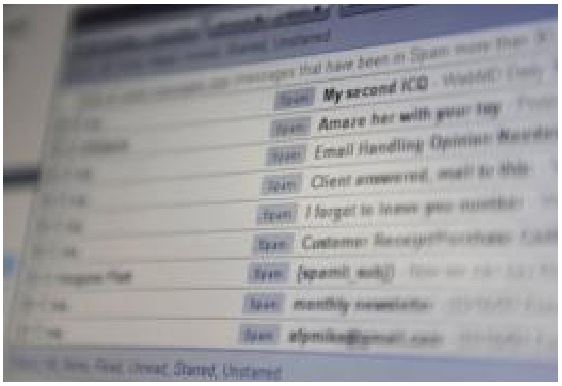
PHYS ORG

Researchers zap huge global spam 'botnet'

July 19 2012



A computer screen inbox displaying unsolicited spam emails. A huge global 'botnet' responsible for sending out millions of spam messages each day has been shut down by a collaborative effort from security experts in the US, Britain and Russia, researchers said.

A huge global 'botnet' responsible for sending out millions of spam messages each day has been shut down by a collaborative effort from security experts in the US, Britain and Russia, researchers said.

The so-called Grum botnet -- which uses a network of infected computers to automatically generate emails -- "has finally been knocked down," said Atif Mushtaq of the California security firm FireEye.

Mushtaq said in a blog post Wednesday that the shutdown was a joint effort of his group with the British-based Spamhaus Project, a nonprofit group, and the Russian-based Computer Security Incident Response

Team known as CERT-GIB.

"All the known command and control servers are dead, leaving their zombies orphaned," Mushtaq said.

He noted that the researchers worked to shut down servers in the Netherlands and later in Panama, where "pressure applied by the community" caused the hosting firm to shut down the operation.

But he said the spam operation moved to new servers in Ukraine after the ones in Panama were closed.

"Ukraine has been a safe haven for bot herders in the past and shutting down any servers there has never been easy," he said.

But with the help of Spamhaus, CERT-GIB and an "anonymous researcher," Mushtaq said "all six new servers in Ukraine and the original Russian server were dead as of today, July 18."

He said the shutdown was made by the "upstream provider... at our request."

The researchers said the botnets had been using as many as 120,000 infected "zombie" computers to send out spam each day.

"After the takedown, this number has reduced to 21,505," Mushtaq said. "I hope that once the spam templates expire, the rest of the spam will fade away as well."

He said the collaborative effort to take down Grum sends a "strong message to all the spammers."

(c) 2012 AFP

Citation: Researchers zap huge global spam 'botnet' (2012, July 19) retrieved 3 May 2024 from https://phys.org/news/2012-07-zap-huge-global-spam-botnet.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.