

'Bad neighbourhoods' on the internet are a real nuisance

March 8 2013

Of the 42,000 Internet Service Providers (ISPs) surveyed, just 20 were found to be responsible for nearly half of all the internet addresses that send spam. That just is one of the striking results of an extensive study by the University of Twente's Centre for Telematics and Information Technology (CTIT). This study focused on "Bad Neighbourhoods" on the internet (which sometimes correspond to certain geographical areas) that are the source of a great deal of spam, phishing or other undesirable activity. In his thesis, Giovane Moura describes this situation in detail.

Just like in the real world, the internet has also "bad neighbourhoods" whose streets are not safe and where [crime rates](#) are higher than in other districts. Research into these "Bad [Neighbourhoods](#) on the Internet" can lead to better security solutions. To this end, Moura has carried out the first systematic investigation of malicious hosts, by monitoring and analysing network data. His main conclusion is that [malicious activity](#) is indeed concentrated in limited zones: areas in which the IP addresses show strong similarities, per ISP, or even per country. For instance, this PhD researcher found that 62% of the addresses at one ISP were related to spam. This knowledge can be used to link [security measures](#) to specific ISPs.

Geographically determined

It is also interesting to note that different types of activities are associated with different parts of the world. For instance, spam comes

mainly from southern Asian countries, while phishing occurs primarily in the United States and other developed countries. The reason for the latter is that these countries are home to most data centres and cloud computing providers. It is also important to distinguish between individual IP addresses that launch one-off attacks and a whole Bad Neighbourhood that almost always launches repeated attacks. This information, too, is very useful in terms of establishing a security strategy. The history of a Bad Neighbourhood, as identified by this PhD researcher, can be of value here.

Giovane César Moreira Moura (from Goiânia, Brazil) carried out his PhD research in the Design and Analysis of Communication Systems department, which is part of the University of Twente's Centre for Telematics and Information Technology (CTIT). His thesis supervisor was Prof. Boudewijn Haverkort and his assistant thesis supervisor was Dr Aiko Pras.

More information: Giovane César Moreira Moura (from Goiânia, Brazil) carried out his PhD research in the Design and Analysis of Communication Systems department, which is part of the University of Twente's Centre for Telematics and Information Technology (CTIT). His thesis supervisor was Prof. Boudewijn Haverkort and his assistant thesis supervisor was Dr Aiko Pras.

Provided by University of Twente

Citation: 'Bad neighbourhoods' on the internet are a real nuisance (2013, March 8) retrieved 23 April 2024 from <https://phys.org/news/2013-03-bad-neighbourhoods-internet-real-nuisance.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.