INTERPOL | GLOBAL COMPLEX FOR INNOVATION

Simda botnet operation – Questions and Answers

When and how did the operation begin?

Further to discussions between INTERPOL and Microsoft to identify potential areas for collaboration, the Simda botnet was identified as an operational target.

Based on information provided by Microsoft, the INTERPOL Digital Crimes Centre (IDCC) at the INTERPOL Global Complex for Innovation (IGCI) in Singapore worked with its strategic partners, Kaspersky Lab, Trend Micro and Cyber Defense Institute, to perform additional analysis of the Simda botnet resulting in a 'heat map' showing the spread of the infections globally and the location of the command and control servers.

The IDCC contacted the specialist units in the primary countries the National High Tech Crime Unit (NHTCU) in the Netherlands and the Federal Bureau of Investigation (FBI) in the US.

Through a series of coordination meetings involving the IDCC, Microsoft, NHTCU, the FBI, Kaspersky Lab, Trend Micro and Japan's Cyber Defense Institute, further servers were also identified in Luxembourg, Russia and Poland. The Simda botnet is believed to have infected more than 770,000 computers in more than 190 countries, the worst affected including the US, UK, Turkey, Canada and Russia.

A simultaneous take-down of the command and control servers in the Netherlands, US, Luxembourg, Russia and Poland was carried out on Thursday 9 April.

What happens next?

The investigation is ongoing, so no specific details can be provided. The key factor to the success of this operation was the international cooperation between law enforcement and the private sector. Through this continued cooperation we will continue to gather intelligence with a view to identify the criminals behind the Simda botnet.

Who is behind the Simda botnet? Organized crime or separate individuals?

Investigations are ongoing and it is too soon to speculate who may be behind the Simda botnet. Again, what is important is that through cooperation and information sharing, this botnet has been severely crippled thanks to the efforts of the law enforcement agencies and private sector companies involved. Intelligence is being gathered and future actions will be coordinated by INTERPOL with the relevant agencies.

What is a botnet?

The term ‘botnet’ is a combination of the words robot’ and ‘network‘. It is a number of Internet-connected computers that have been infected by malware without the owners’ knowledge, which allows an attacker to take control of the infected computers, making them into bots, also known as a ‘zombies’. Bots are therefore part of a network of infected machines, known as a ‘botnet’, which is typically made up of victim machines stretching around the world.

Some botnets might have a few hundred or a couple thousand computers, but others have tens and even hundreds of thousands at their disposal. So far more than 770,000 computers have been identified as part of the Simda botnet.

Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals.

What do criminals do with information stolen from botnets?

Many botnets are designed to gather personal data including passwords, social security numbers, credit card details, addresses and telephone numbers. These data can then be used in crimes including identity theft, various types of fraud, spamming, and malware distribution. Botnets can also be used to launch attacks on websites and networks, which as are sometimes referred to as Distributed Denial of Service Attacks or DDoS.

What should someone do if they think their computer has been infected?

All computer users should have an anti-virus software installed and ensure it is updated regularly. Anti-virus software will help protect against Simda and other malware. Users who do not already have an anti-virus software installed may wish to consider the following options :
Microsoft Safety Scanner, Microsoft Security Essentials or Windows Defender.

Kaspersky Lab has set up a self-check webpage where the public can see if their IP address has been found to be part of a Simda botnet: https://checkip.kaspersky.com

Free virus scans are available from;
Kaspersky: http://www.kaspersky.com/security-scan

Trend Micro: http://housecall.trendmicro.com/

Cyber Defense Institute: http://www.cyberdefense.jp/simda/

The success of the operation to take down the Simda botnet demonstrates the significant results which can be achieved through cooperation between the private sector and law enforcement via INTERPOL.