ECONOMIE

NSA infected 50,000 computer networks with malicious software

ICT ENGLISH NEWS NIEUWS STANDOUT COMPUTERS SERVICE COUNTRYMUZIEK DE NSA-DOSSIERS EDWARD SNOWDEN ...

The American intelligence service – NSA – infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information. Documents provided by former NSA-employee Edward Snowden and seen by this newspaper, prove this.

Floor Boon, Steven Derix and Huib Modderkolk
23 november 2013 **Leestijd 2 minuten**

Photo Corbis

Gerelateerd in ons archief

23 november 2013 · NRCNL
Document Snowden: Nederland al sinds 1946 doelwit van NSA
NSA NIEUWS EDWARD SNOWDEN ...

30 november 2013 · NRCNL
Dutch intelligence agency AIVD hacks internet forums
NSA NIEUWS COMPUTERS NEWS ...

24 november 2014 · NRCNL
Kwaadaardige malware Regin gebruikt bij hack Belgacom
NSA NIEUWS COMPUTERS ...

12 mei 2014 · NRCNL
'NSA wil wereldwijd alle communicatie inzien'
NSA NIEUWS EDWARD SNOWDEN GCHQ ...

18 november 2014 · NRCQ
De meest gewilde start-up waar je nog nooit van hebt gehoord
COMPUTERS SERVICE COUNTRYMUZIEK ...

Meer

Zoeken in ons archief

Van 23 / 11 / 2012
Tot 23 / 11 / 2014

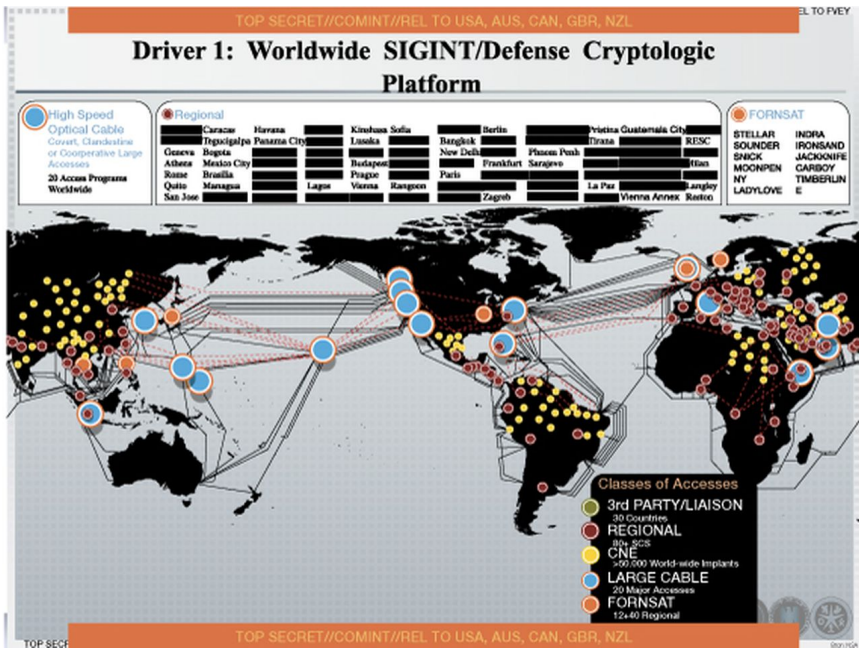
The American intelligence service - NSA - infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information. Documents provided by former NSA-employee Edward Snowden and seen by this newspaper, prove this.

A management presentation dating from 2012 explains how the NSA collects information worldwide. In addition, the presentation shows that the intelligence service uses 'Computer Network Exploitation' (CNE) in more than 50,000 locations. CNE is the secret infiltration of computer systems achieved by installing malware, malicious software.

One example of this type of hacking was discovered in September 2013 at the Belgium telecom provider Belgacom. For a number of years the British intelligence service - GCHQ - has been installing this malicious software in the Belgacom network in order to tap their customers' telephone and data traffic. The Belgacom network was infiltrated by GCHQ through a process of luring employees to a false Linkedin page.

NSA special department employs more than a thousand hackers

The NSA computer attacks are performed by a special department called TAO (Tailored Access Operations). Public sources show that this department employs more than a thousand hackers. As recently as August 2013, the *Washington Post* published articles about these NSA-TAO cyber operations. In these articles The Washington Post reported that the NSA installed an estimated 20,000 'implants' as early as 2008. These articles were based on a secret budget report of the American intelligence services. By mid-2012 this number had more than doubled to 50,000, as is shown in the presentation *NRC Handelsblad* laid eyes on.



Cyber operations are increasingly important for the NSA. Computer hacks are relatively inexpensive and provide the NSA with opportunities to obtain information that they otherwise would not have access to. The NSA-

presentation shows their CNE-operations in countries such as Venezuela and Brazil. The malware installed in these countries can remain active for years without being detected.

'Sleeper cells' can be activated with a single push of a button

The malware can be controlled remotely and be turned on and off at will. The 'implants' act as digital 'sleeper cells' that can be activated with a single push of a button. According to the *Washington Post*, the NSA has been carrying out this type of cyber operation since 1998.

The Dutch intelligence services - AIVD and MIVD - have displayed interest in hacking. The Joint Sigint Cyber Unit - JSCU - was created early in 2013. The JSCU is an inter-agency unit drawing on experts with a range of IT skills. This new unit is prohibited by law from performing the type of operations carried out by the NSA as Dutch law does not allow this type of internet searches.

The NSA declined to comment and referred to the US Government. A government spokesperson states that any disclosure of classified material is harmful to our national security.