Digital espionage

What are the risks?

Digital espionage

What are the risks?

Digital espionage forms an increasingly common part of foreign intelligence services' undesirable activities. Other actors such as companies can also make use of activities of that kind, which are damaging to national security. These could be motivated by interests in the sphere of territorial, economic, ecological and physical security and social or political stability. As a result of its increase – on a global as well as a national level – digital espionage is currently an active research area for the General Intelligence and Security Service of the Netherlands (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) and the Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). In this brochure, the AIVD and the MIVD inform you about the work of the intelligence services. It also tells you how you can limit the risk of digital espionage.

Are you at risk?

Intelligence services are interested in political, classified military, economic and scientific information. In addition, we know that a number of foreign intelligence agencies are involved in manipulating, influencing and monitoring migrant groups in our country. They make use of digital espionage to get hold of data belonging to organisations engaged in promoting the interests of migrant groups. The kind of data these agencies might be interested in are things such as policy plans and membership lists.

When considering whether you are at risk, ask yourself if your work or private life makes you a person of interest to foreign intelligence services. Consider whether you have access to valuable information or are in a position that could be of interest to foreign intelligence services. It is quite likely that you know more than you may think at first.

Targets: embassies, ministries and international organisations

In 2009 it came to light that the espionage network GhostNet was hacking into hundreds of embassies, ministries and international organisations. GhostNet operated by way of infected Word and PDF documents. As soon as a computer had become infected, GhostNet would start to copy the documents and tap any conversations conducted via webcams and microphones. Nearly all the computers used to run GhostNet were traced to China.

How do intelligence services operate?

The most common method by which digital espionage takes place is the installation of spyware on a computer. Spyware is software that gathers data from a computer without the user's knowledge. The information is then sent to the 'attacker', again without the user being aware of this. Spyware can record key strokes, search networks and mailboxes, take screenshots and so on. There are even known cases of spyware being used to listen in and view images. This involves utilising any available microphones and webcams.

Spyware can be installed in a number of ways. Below you will find a list of the most common methods.

Via email Trojans

Email Trojans are email messages with infected attachments. Upon opening the attachment, your computer is infected with spyware. In the case of targeted digital espionage the attacker will try to tailor the message to the addressee(s) and their activities as much as possible. The attacker will create the false impression that the message is actually from another, familiar source. This is called 'email-spoofing'. In most cases, the vulnerabilities in the software are known but, unfortunately, virus scanners are not yet fail-safe when it comes to detecting email Trojans.

Via infected websites

Visiting a website can result in spyware being installed on your computer. For this method, the attackers use a leak in the browser or in extra software plug-ins, installed to supplement the browser, such as Flash Player software. The attacker will commonly select a website that is very popular with the target groups. The webmaster is completely unaware of the manipulation. Another possibility is for the attacker to simulate a site for the purpose of manipulation. The attacker sends the targets an email that is not infected. This email is designed to tempt the targets into visiting the fake site. This is called 'website spoofing'.

While reading the news
Your personal data can be relayed across the world, from the moment you access a website. This is what happened to a number of migrants when they visited a news site for their migrant community. The news site's server had been hacked by order of a foreign government. The site's visitors were unaware of it, but their personal data was sent to the spying country via the hacked server. This personal information could be misused in the relevant country, for instance to put family members of migrants under pressure.

Via infected media

In some cases, spyware may have been installed on a particular medium before you use it. This includes media such as hard disks, USB sticks, CDs or DVDs. Giving out free USB sticks to certain groups, for instance, is one method used for targeted espionage.

A free USB stick?
A senior manager attends a conference on security. At one of the stands he is given a complementary USB stick. Back at work the next day, he uses the USB stick he received at the conference. Unfortunately, though, the USB stick contains spyware and his computer becomes infected.

Via espionage during journeys

While travelling or during a stay in your home country or abroad, you run the risk of losing sight of your laptop or of other data carriers. You might leave your laptop behind in your hotel room, for instance, or have to hand it over temporarily in customs. At these moments it is possible for attackers to install spyware on your laptop or copy data. You also run a risk of third parties trying to get hold of data when you connect to a seemingly safe network providing internet access in a public space (by way of a hotspot, for instance).

Leaving your blackberry behind

A senior civil servant is heading downstairs to get something to eat in his hotel and decides to leave his blackberry behind in his room. One week later computers belonging to the Ministry are hacked. The odds are that strangers entered his hotel room and copied data from his blackberry.

What can you do yourself?

When it comes to security, you will probably have to rely on your organisation's IT department to a certain extent. Your organisation is responsible for a safe digital working environment. In addition, you can also reduce the risks of espionage yourself.

In general

- Always start by checking the email address that a message has been sent from. Are you doubtful whether an email is legitimate? Does the address look unprofessional, like the variety john1234@yahoo.com? If so, contact the sender to verify its authenticity. Try to avoid opening attachments sent by strangers, even if the contents seem to be legitimate.

- Be careful when opening attachments you receive via a subscription to a mailing list. Sometimes attackers make use of mailing lists you can subscribe to. In that case the sender will appear to be the regular one.

- Be wary of emails with attachments that are in badly-worded English, especially when the mail is from a sender who should be proficient in English.

- Be wary of emails that are of interest to your company but not to you specifically. There is a possibility that attackers have got hold of your email address without knowing what your position is.

A dangerous subscription
Many civil servants have a subscription to one of the European Union's news services. An attacker can send them an email with an infected attachment. As the email appears to have been sent from the news service of the European Union, the civil servants do not hesitate to open the infected attachment.

- Be wary of an attachment if your computer starts to act strangely after having opened that attachment: for instance, if an application starts, shuts down, then starts up again before opening and displaying the attachment. This could be an indication of the attachment being infected.

- Be careful about giving out your email address on the internet or at conferences if you have access to sensitive information. Also take due care when it comes to your name, as it is often easy for attackers to deduce your email address from it.

- Check UBS sticks and other data carriers by scanning them on a stand-alone pc, or ask your helpdesk to do it for you.

- Raise awareness of the threat of digital espionage within your organisation.

At home

- Always ensure your virus scanner is updated.
- Do not store sensitive, work-related information on your home computer.
- Be aware of the information you post on the internet. On your personal website, for instance, or social networking sites like Hyves and Facebook. The more personal information you leave online, the easier it is for others to draw up a targeted email message.

When travelling

- Keep the amount of (sensitive) data you take with you on data carriers such as laptops and USB sticks to a minimum.
- If you do need to carry confidential information, make sure to encrypt it.

'Your laptop, please...!'
An executive is travelling abroad on business. Upon arrival, a customs officer immediately makes him hand over his laptop. It is not returned for three hours. When he checks it later, he suspects that various files containing competition sensitive information have been copied.

- Register confidential information that you need to take with you. This will allow you to find out what has come in to the hands of third parties if necessary.
- Keep your data carrier in a sealed bag, if you cannot guard it yourself. Has the seal been opened, or are there are other signs that point to someone having messed about with your data carrier? Then stop using that carrier.
- Avoid using free internet services offered in public spaces. If you do need to use an internet connection, then do not send any confidential information.

If you have a suspicion

If you suspect that your organisation's computer network is being targeted by digital espionage, you must inform the department responsible for the protection of the IT infrastructure within your organisation. They can report your suspicions to the AIVD and MIVD. The telephone numbers and addresses are listed at the end of this brochure. It goes without saying that we will treat your report with the utmost confidentiality.


end
pg dn
dn fld

What do we do?

The counterespionage task of the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) is officially defined as follows.

To identify intelligence activities, to bring them to an end – or help to do so – and to enhance national public resilience to them.

Be alert to the risks posed by espionage. And raise awareness of that risk throughout your organisation. Please report any suspicious activity or incidents to us, even if you are not sure about their significance. We are always pleased to hear from you.

Are you interested in finding out more?

You can find more information on the following sites:
- www.aivd.nl
- www.mivd.nl
- www.govcert.nl

At www.aivd.nl and www.mivd.nl you can find:
- the brochure 'Espionage in the Netherlands. What are the risks?'
- the brochure 'Espionage during travel abroad. What are the risks?'
- the annual reports of the AIVD and MIVD

If you have any questions or wish to pass on information,
please do not hesitate to contact us at one of the following addresses.

General Intelligence and Security Service (AIVD)
Postal address: PO Box 20010
2500 EA The Hague
the Netherlands
Telephone: +31 (0)79 320 5050
Fax: +31 (0)70 320 0703
Website: www.aivd.nl

Military Intelligence and Security Service (MIVD)
Postal address: PO Box 20701
2500 ES The Hague
the Netherlands
Telephone: +31 (0)70 44 190 27
Fax: +31 (0)70 44 190 10
Website: www.mivd.nl

Colophon
This brochure is a publication of:

Ministry of the Interior and Kingdom Relations of the Netherlands
General Intelligence and Security Service
www.aivd.nl

PO Box 20010 | 2500 EA The Hague, the Netherlands

Ministry of Defence of the Netherlands
Military Intelligence and Security Service
www.defensie.nl/mivd

PO Box 20701 | 2500 ES The Hague, the Netherlands

Graphic Design
Zijlstra Drukwerk BV, Rijswijk, the Netherlands

1st translated print, March 2010

Photographs
Hollandse Hoogte