Cyber-attacks by state actors:

Seven moments to stop an attack

Cyber-attacks by state actors:

Seven moments to stop an attack

How are you being attacked and what can you do to protect yourself?

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst – AIVD) and the Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) observed that Dutch (government) organisations and companies are being targeted on a large scale by cyber-attacks by state actors.* With more and more states carrying out cyber-attacks, the Netherlands has had to face a fast-growing cyberthreat in the past years.
These attacks affect our economy, our prosperity, and our security.

* You can find our previous report "Offensive cyber-programmes: an ideal business model for states" from 2019 on the AIVD website. This report explores why offensive cyber-programmes offer such attractive prospects for state actors.

This publication aims to warn directors, policy makers, and managers about the methods of state actors and to provide advice on how to increase resilience against state-sponsored cyber-attacks. Take this publication with you when you meet with ICT security specialists to discuss your organisation's digital resilience. The effectiveness and success of the security strategy you choose, are determined by how well directors, policy makers, managers, and ICT security specialists cooperate.

You can reduce the chances of becoming the victim of a successful cyber-attack by knowing and understanding how state actors work. In order to gain insight into the methodology of cyber-attacks and ways to prevent them, we will look at the different stages of a cyber-attack.

There is more than one model for such an approach. In this publication we opted for the Cyber Kill Chain model.

The Cyber Kill Chain
The Cyber Kill Chain is a tool used throughout the world to provide insight into the methods of cyber-attackers. This model describes the seven stages that attackers go through to obtain their goal. In practice, not all stages are traversed, or some of the stages feature more than once in order to penetrate a network more deeply.

This publication explains the theory behind the Cyber Kill Chain by comparing an attack to a physical break-in of a villa. For each stage a real-life example of a state-sponsored cyber-attack is discussed. Lastly, each stage provides advice regarding which measures to take in order to detect, delay, or stop attackers. When attackers are discovered and stopped in time, they will have to start their attack all over again. If attackers are forced to do this again and again, they will have to increase their efforts, which also increases the costs of an attack. The chances that attackers will repeat the attempted attack are thus reduced.

Security measures can be divided into preventive and detective measures. It is impossible to provide a complete overview of all security measures. That is why it is important to understand the attackers' methodology, so that you and your ICT security specialists can examine which security measures are best for your organisation and its security strategy. You can use the advice for each stage as a starting point. That way you will make sure your organisation will become more resilient to cyber-attacks. If your organisation does not have a security department, you can implement security measures by using the services of an external cybersecurity partner.


101010
01010
1010
RECONNAISSANCE
WEAPONIZATION
DELIVERY
EXPLOITATION
INSTALLATION
COMMAND AND CONTROL
ACTIONS ON OBJECTIVES

Stage 1: **Reconnaissance**

Stage one is when attackers select their targets. This is followed by digital reconnaissance for the purpose of collecting as much information as possible about any weak spots these targets may have. Weak spots can be technical vulnerabilities as well as individuals.

Comparison to an actual break-in

Burglars who are looking for masterpieces by famous painters choose different targets than burglars interested in jewellery. Once the target has been selected, the burglars will scope out the physical surroundings. They look for roads that lead to the target. They also investigate at which times certain people are present, and whether there are alarm systems or security cameras. They will look for any doors that may be unlocked or windows that are often left open. Burglars will also try to find out if any of the people who work there can help them get in—a window cleaner whose ladder they can use, for example.

During the Reconnaissance stage, cyber-attackers gather as much information as possible about any weak spots their target may have. They need this information in order to gain access during the next stages of the Cyber Kill Chain. In the example above, the burglars are focused on a specific target. In practice, cyber-attackers also select targets on the basis of an opportune weak spot that can be exploited.
Think, for example, of a publication disclosing a critical software vulnerability. State-sponsored cyber-attackers can use such a publication to look for targets using this software, rather than first selecting a target.

Advice – what can you do?

During the Reconnaissance stage, cyber-attackers gather as much information as possible to map the attack surface. That is why it is important to choose security measures that contribute directly to keeping your organisation's attack surface small.

Preventive security measures

- Some state-sponsored cyber-attackers automatically scan for known vulnerabilities in systems and devices that are linked to the internet. Actors also scan for open ports, which they then use to gain insight into your organisation's infrastructure.
  Ports are used to send and receive information over the internet. Many companies and organisations leave too many ports open, even when they are not being used. That is why you should close unused ports, keep any internet-linked systems and devices up to date and always apply the latest patches and configurations. Keep your Configuration Management Database (CMDB) up to date so that you can respond quickly when suppliers provide updates and security patches.

- Links to the network of a supplier or cooperation partner are also part of the attack surface. The inadequate security of the network of your supplier or partner could be the weak spot of your organisation. Attacks on companies or organisations through a supplier or partner are called supply chain attacks. These attacks are part and parcel of the methods used by various state-sponsored cyber-attackers. In order to reduce the risk of supply chain attacks it is important that you do not automatically designate links to/from partners as trusted and that you require your partners to adhere to system security standards.

- During the Reconnaissance stage, attackers also scour the internet for open-source information about your organisation or employees. They try to find out, for example, which techniques, systems, software, or hardware your organisation uses, or look for the e-mail addresses of employees.
  Attackers use information of this kind not only to find vulnerabilities, but also to make their (spear) phishing e-mails more convincing. That is why, if you want to limit the attack surface of your organisation, it is important that your employees are aware of the risks and conduct themselves accordingly. Create awareness among your employees about the dangers of sharing of personal information, job descriptions, and information about ICT components and configurations on social media like Facebook or LinkedIn..

Detective security measures

- You can discover reconnaissance attempts during this stage by using detection solutions. Think, for example, of using a so-called Network-based Intrusion Detection System (NIDS). This allows you to actively monitor and analyse incoming and outgoing network traffic, including from/to partners, for suspicious activity.

Close access hacking operation on the OPCW

On 13 April 2018, a car is parked near the Marriott hotel in The Hague. On the car's rear shelf, hidden under a coat, is an antenna. The antenna is pointed at the headquarters of the Organisation for the Prohibition of Chemical Weapons (OPCW) and it is connected to equipment for the remote interception of Wi-Fi network traffic. With this set-up, users of the Wi-Fi network can be identified and their log-in information discovered. The equipment in the boot of the car can be operated via a connected laptop, but also remotely using a 4G connection. No doubt about it: this is the reconnaissance stage of a cyber-attack.

The car had been rented by four intelligence officers of a so-called close access hacking team of the Russian military intelligence service GRU. Close access teams attempt to get as physically close to their target as possible, so that they can obtain access to networks that are not directly accessible from the internet, such as internal Wi-Fi networks. During the Reconnaissance stage these networks are identified on location.

Through counter-intelligence the MIVD as able to identify and disrupt the GRU's close access hacking operation on the OPCW already during the early Reconnaissance stage.

Fase 2:
Weaponization

When attackers find a vulnerability,
they develop tools—malware,
for instance—to exploit this weak spot.

Comparison to an actual break-in

The burglars have decided to break into the target's villa. During their reconnaissance they discovered that one window is always left open. A simple latch secures the window against the wind. During the Weaponization stage the burglars take a wire coat hanger and bend it so that they can stick it through the window opening and unlatch the window.

In a sense, cyber-attacks are very similar to the example above. State actors, too, use their reconnaissance activities to choose which vulnerability they intend to exploit. During the Weaponization stage, actors select or build tools that have the greatest chances of success.

State actors often use known software vulnerabilities for which exploits (software used to exploit vulnerabilities) have already been developed. Attackers use exploits to gain access to systems. Once access has been obtained, attackers install malware—malicious software—to gain control over these systems.

State actors can also use vulnerabilities that are not yet widely known to the general public. Attackers discovered these vulnerabilities themselves or paid large sums for them on the online black market. This type of vulnerability is known as a zero-day.

Advice – what can you do?

During the Weaponization stage attackers prepare for a cyber-attack. During this stage there is no interaction with the target yet. That is why it is very difficult to observe or stop an attacker at this stage. This does not mean that you cannot do anything to mitigate the threat, though.

- Identify your vital assets and investigate for which state actors you could conceivably be a target. You can read more about this in a number of publications available from the AIVD website.

- Once you have identified for which state actors you could conceivably be a target, you can explore which attack techniques these actors use. The MITRE ATT&CK Framework is a frequently used knowledge base describing a large diversity of attack techniques for individual state actors.* You can use this model to check whether protective measures against known attack techniques have been implemented in your organisation. Lastly, you can check whether your organisation's intrusion detection measures are able to detect such attack techniques.

* https://attack.mitre.org

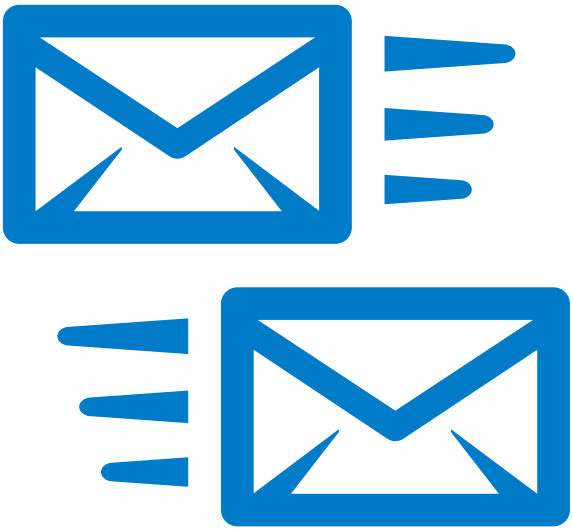
Warning from AIVD, MIVD, and NCSC leads to 'Citrix files'

On the morning of Monday, 20 January 2020, the traffic report is somewhat remarkable: "Drivers should expect congestion due to adverse weather conditions, slippery roads, dense fog, and problems with Citrix servers".

This delay warning is highly unusual. On the Friday before the weekend, several government and private servers running Citrix software were taken offline at the recommendation of the AIVD, MIVD, and the National Cyber Security Centre (NCSC).

In the days prior to the issued warning, the AIVD and MIVD have observed that a state actor is actively trying to exploit a known vulnerability in Citrix VPN servers for cyber-espionage purposes.

The Citrix server vulnerability was made public on the internet in early December 2019. Then, on 10 January 2020, several internet forums published how the vulnerability could actually be exploited in order to gain access to internal networks. State actors were quick to use this information in order to identify systems still running the compromised Citrix software and therefore having the vulnerability in question. During the subsequent Weaponization stage, the state actors managed to develop an exploit that they could actively employ to exploit the Citrix vulnerability.



Fase 3:
Delivery

When the target has been selected and the malware is ready to be used, the attackers deliver the malware to the organisation, for example via an e-mail.

Comparison to an actual break-in

The burglars drive to the villa, the bent wire hanger in the back of the delivery van.

In the digital world, delivering the tools needed for a burglary is quite different from the physical world, as 'time' and 'distance' play a less important role. In the physical world, for example, it might take the burglars 30 minutes to drive to their target.

This dimension is absent in case of a cyber-attack, because a (spear) phishing e-mail, for example, can be sent and delivered in the blink of an eye.

For that reason sending (spear) phishing e-mails is a frequently used method for delivering malware to a victim. For example, attackers create a phishing e-mail that refers to a current topic, containing a link to a related article or an attachment with an interesting name. Clicking the link or opening the attachment will often present the reader with an article, but in the background the malware is also executed, as it installs itself in the victim's system. A spear phishing attack is similar but even more sophisticated, as the e-mail will be tailored to a specific victim. In such personalised e-mails, attackers often use the information they collected during the reconnaissance stage.

Another method often used by attackers to deliver their malware to the system of the intended target, is to hack a website with vulnerabilities that is often visited by the target's employees. The attackers introduce malware into this website, so that visitors will become infected. This type of attack is known as a watering hole attack. Attackers are also known to hand out free USB drives that come with pre-installed malware, in the hope that employees of the intended target use the USB drives on the organisation's systems.

Advice – what can you do?

The security measures chosen for the Delivery stage should be able to prevent the delivery of the malware that was developed during the Weaponization stage.

Preventive security measures

- Important during this stage is to scan incoming e-mails and any attachments for malware and suspicious URLs. You can scan e-mails on a mail proxy to make sure any malware is blocked before it reaches the user's inbox. You can also use sandboxes (an isolated environment separate from the corporate network) on the mail server to carry out verification and block any malware.

- CAlso check the origins of e-mails, using techniques such as Domain-based Message Authentication, Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) or Sender Policy Framework (SPF).
  By using these techniques, e-mails of unknown origin will be blocked. You can also use policies to exclude executable file types like .exe or .msi from being received as attachment to an e-mail, so that they will not reach a user's inbox.

If an e-mail or an attachment contains suspicious elements, it is important that you do not delete the message but place the e-mail in quarantine for further investigation. Once the e-mail is deleted, it can no longer be analysed or investigated.

- In addition you can harden browsers and applications to reduce the risk of systems being compromised when employees visit infected web pages. You can harden a browser by disabling plug-ins that are known vulnerabilities, for example. In case of an application it is recommended you disable unneeded Office macros. Macros are often used to infect a machine with malware.

- You should also have policies in place for the use of removable media and data carriers and for connecting personal hardware to the corporate network (Bring Your Own Device). Think of USB pen drives, for example. Close USB ports and allow only registered USB media issued and inspected by your own organisation. You should also disable the autorun function of media.

Detective security measures

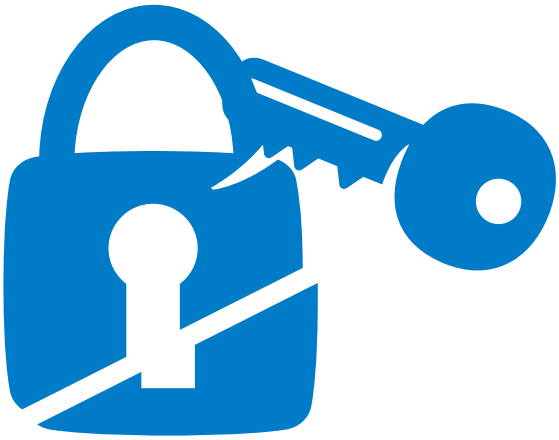
- By logging the web pages visited by users you will be able to analyse whether any infected pages were visited. Several security solutions provide this option. Keeping logs of e-mail and web pages is necessary for investigating an attacker when you discover an attack. If you have not been keeping logs, it will be difficult to ascertain how and when the malware was delivered.

- Anti-virus software or a Next-Generation Antivirus (NGAV) solution will help you discover any malware during the Delivery stage.

Cyber-attacks on Dutch ministries

Towards the end of 2018 phishing e-mails begin to pop up in the mailboxes of several employees at a Dutch ministry. A state actor uses content that appears plausible and that is phrased in a very specific way to entice employees to open the malware-infected attachment. The e-mail server's filter does what it is supposed to and discovers and removes the malware from the phishing e-mails. In this example the phishing e-mails were stopped during the Delivery stage.

The AIVD and MIVD regularly observe how state actors engage in cyber-espionage attempts on several Dutch ministries. One ministry in particular has enjoyed a great deal of attention from state actors in recent years, namely the Ministry of Foreign Affairs. The AIVD has noted, for example, that between 2017 and 2020 a number of Dutch embassies in the Middle East and Central Asia were the target of cyber-attacks by a foreign intelligence service. Most likely the purpose of the attacks was to gain insight into the e-mail traffic between a Dutch diplomatic post abroad and the Ministry of Foreign Affairs in the Netherlands.



Fase 4:
Exploitation

It is during this stage that the malware is activated, for example when one of the employees clicks a link in a malicious e-mail.

Comparison to an actual break-in

One of the burglars sticks the bent wire hanger through the gap of the open window and undoes the window latch. At this stage the burglar does not enter the house yet. All he does now is create access for himself.

The final stage in gaining access is the Exploitation stage. Attackers still have to force open the 'window'. For that reason the Exploitation stage is focused on activating the malware. Think of an employee having to click the link in the (spear) phishing e-mail in order to activate the malware that will give attackers access.

Advanced cyber-attackers such as state actors will do anything to increase the chances that an employee will click a link or open a malicious attachment. These chances are greater when an e-mail looks trustworthy. Attackers can ensure this by, for example, gaining access to the e-mail account of the director of a company and sending out e-mails in their name. Attackers can also send e-mails from their own infrastructure that are made to look like they come from someone else. This will make the recipient think that the phishing e-mail was sent by someone they trust. This is called spoofing.

Advice – what can you do?

During this stage attackers have not yet obtained a firm foothold. The security measures for this stage are focused on detecting and blocking malicious code or scripts.

Preventive security measures

- During this stage you should use application whitelisting. Application whitelisting allows you to block all software on your system with the exception of software included in a whitelist of trusted software that your organisation creates. This reduces the risk that malware can be installed or executed.

- During this stage attackers will attempt to mislead users in order to entice them to carry out a certain action. That is why it is important to make your employees aware of the dangers of (spear) phishing and clicking unknown links. Advise employees that they should first call or e-mail the sender of a suspicious e-mail before opening an attachment or clicking a URL.

Detective security measures

- By using an Endpoint Detection and Response (EDR) solution you can detect and block malicious code or scripts in the form of viruses, malware, ransomware or any other suspicious types of activity in time. These solutions are available for desktops, laptops, smartphones, and servers.

- It is important to have periodical security assessments in the form of vulnerability scans, penetration tests, and red team exercises, so that you have time to take mitigating steps with regard to the vulnerabilities and access paths found. This is necessary because the IT

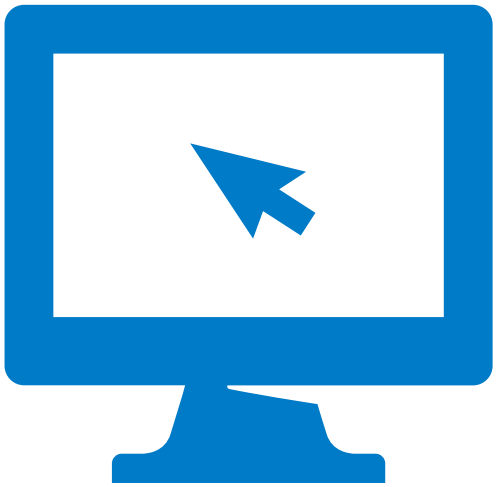
infrastructure of an organisation is constantly changing, resulting in vulnerabilities; new systems are connected, old systems are updated, and the configurations of network equipment are modified regularly.

State actors exploit the COVID-19 pandemic for cyber-operations

Fairly soon after the COVID-19 pandemic broke out, the AIVD and MIVD began to receive signals that some state actors were secretly more interested in other things than the global search for a vaccine in the fight against the corona virus. They want to use the research results of the pharmaceutical companies of other countries for their own gain.

Various companies and research institutes involved in the prevention and fight against the corona virus receive e-mails that at first glance appear related to the joint fight against the virus. When someone opens the e-mail and the attachment with information, however, things go wrong: the state actor's malware has been activated and proceeds to install itself on the network.

It was actually a phishing e-mail sent by a state actor. Due to the severity of the pandemic, several recipients of these e-mails are less careful when assessing whether they can trust the sender and the contents of the e-mail, and they click links or open infected attachments. This completes a successful Exploitation stage; state actors have managed to penetrate several companies and research institutes across the world.



Fase 5:
Installation

During the Installation stage the attackers try to obtain permanent access and establish a foothold in the target's network.

Comparison to an actual break-in

During this stage the burglar climbs through the window and enters the villa. He turns on his phone so that he can contact his accomplice in the next stage. Then he proceeds to check out the villa, in the dark and without making any sound. He runs into closed doors or a locked safe. He can open these, provided he brought along the right tools. If not, he will have to wait until the next stage, when he has been in touch with his accomplice.

Once a state actor has gained access to the target's computer system, it quickly tries to obtain the most extensive network rights possible, preferably administrator rights. These rights will allow the actor to move deeper into the network. This is called lateral movement.

State actors often use very sophisticated methods. They can move through a system while remaining practically invisible. One of the reasons for lateral movement is to create permanent access, for example by installing so-called 'back doors'. Having extensive rights will also allow the attacker to roam freely through the network to find the locations that hold the most interesting data.
Because of their patience and persistence when trying to gain access to computer systems, taking their time and using advanced methods during the Installation stage to obtain the information they want without being seen, state(-sponsored) cyber-actors are also called Advanced Persistent Threats (APTs) in the world of cybersecurity.

Advice – what can you do?

For this stage it is important to choose security measures that keep attackers from gaining a permanent foothold in different areas of the network.

Preventive security measures

- In case the malware was installed successfully, you will want to keep the attackers from moving laterally. An effective countermeasure is to compartmentalise systems and create network segments. You can compartmentalise by disabling unnecessary connections. To segment the network you divide it into separate areas. That way you can limit access to confidential information or critical processes to employees, applications, and computers that actually need this access. Segmentation is fairly easy to implement using Virtual Local Area Networks (VLANs) and firewalls.

- Minimising rights is also important. That is why you should have a limited number of administrator accounts, and within these accounts the rights for administrator activities should be limited. It is also important to shield the identities of these accounts. You should be careful not to give regular user accounts more rights than strictly necessary (the 'principle of least privilege').

  By observing this rule, a hacked account can be used only to a limited extent for further exploration of the system or network. Disable administrator accounts once they are no longer in use. Lastly, use different accounts and strong passwords for administrator tasks,

and determine which administrator activities are allowed to be executed remotely. Block standard protocols such as RDP (Remote Desktop Protocol) or Telnet, or place these behind a VPN.

- Multi-factor authentication (MFA) is more than just an important security measure to keep attackers out; during this stage MFA will also ensure that attackers cannot use stolen credentials to move laterally. Multi-factor authentication involves having a combination of several factors that must be met in order to gain access to a function or application. Think, for example, of having to use your fingerprint or a smart card in combination with your password. Multi-factor authentication should also be mandatory for the use of a VPN. This will prevent attackers from gaining external access to the corporate network using stolen user credentials.

Detective security measures

- If your organisation has a Security Operations Centre (SOC), you can work together to determine a detection strategy. An SOC uses a Security Information & Event Management system (SIEM) for the centralised collection of logging and other relevant data. This system allows you to see whether there have been log-ins by accounts that have not been active before or whose most recent log-in attempt goes back a long time. Several failed log-in attempts could indicate suspicious activity.

- An SOC can also determine whether any user accounts have received additional rights or have been assigned to an administrator group and investigate whether the change is correct. If you do not have an SOC, you could consider hiring a security services provider.

Long-term hack of EU embassy Moscow

On 5 June 2019 the news platform Buzzfeed reported on a "sophisticated cyber espionage event". Reportedly, between February 2017 and April 2019 a Russian APT had access to the digital systems of the EU's Moscow embassy. An internal analysis, which Buzzfeed has seen, mentions that at least two computers had been infected with the APT's malware and that information had been stolen. It is unclear how much and what kind of information had been taken. An EU spokesperson, in contact with journalists before the publication, confirms that an incident has taken place and that investigation was in progress.

This kind of cyber-espionage by state actors shows that APTs have the means and capabilities to gain access to sensitive digital systems without being seen. If these intruders pay careful attention to following the Cyber Kill Chain during the Installation stage, they can continue their surreptitious activities on the network also for a prolonged period of time.

Fase 6:
Command and Control

During this stage the attackers contact |the malware installed on the network from a remote location, using this communication channel to install more malware.

Comparison to an actual break-in

The flesh-and-blood burglar contacts his accomplice. He is given instructions and the extra tools he needs. Sometimes this tool is a (login) code for a computer or a safe, something that can be given over the phone. Often a burglar will unlock the back door in order to have tools handed to him. That way the burglar also creates another entrance and exit, for when the window can no longer be used.

In the digital world, at some point after its installation, the malware will contact the Command and Control server, also called a C2 server. At this stage the attacker has obtained permanent access to the network, and the back doors he installed during the Installation stage allow him to control the malware remotely and introduce new malware to the network.

This kind of communication is called Command and Control traffic (C2 traffic). The attackers use the new malware to penetrate the network even deeper to seek out the data they are interested in.

Advice – what can you do?

This stage represents the last possible moment for you to prevent the attackers from taking the next, final step. The security measures chosen for this stage should enable you to detect the C2 traffic and block the attackers from communicating via the C2 server.

Preventive security measures

- At this stage you should reduce the chances that attackers could successfully contact their C2 server. One way of doing this, is by limiting the number of ports accessing the internet, so that attackers have fewer locations for installing back doors. You can also direct all network traffic through a proxy or next generation firewall (NGFW). A proxy can filter out any anomalous traffic, which will block C2 traffic.

- You can also use a DNS sinkhole. This technique will prevent the domain names used by the attacker for their C2 server from resolving. In practice, this security measure ensures that no traffic is possible between the organisation's network and the attackers' C2 server.

Detective security measures

- In this stage the attackers' C2 server is contacted. You can detect this C2 traffic. The communication between the malware and the attackers could be hiding among regular network traffic, for example in the communication between your network and a news website that your employees visit regularly. It is also possible that the communication goes through a cloud service. Attackers are more difficult to spot when they use these techniques.

- Active monitoring will help you detect such communications. You could look at suspicious amounts of network traffic and unusual data streams, for example. In order to detect suspicious network traffic you can also use indicators of C2 infrastructures provided in public or commercial reports on cyber-attacks.

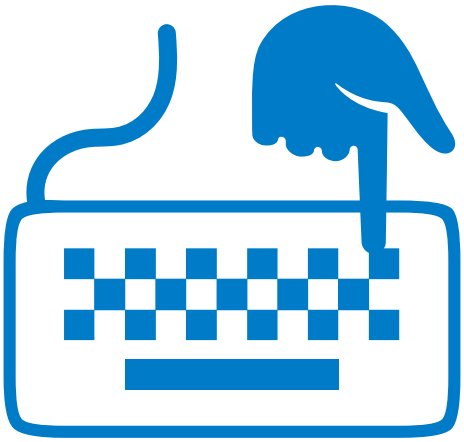
Abuse of Dutch ICT infrastructure in cyber-operations by state actors

In recent years the AIVD received many reports from intelligence and security services in other European countries that companies and government bodies in those countries were under attack from the Netherlands. Were these targets under attack from Dutch hackers or were things rather more complicated than that?

The fact that cyber-attacks use Dutch ICT infrastructure is in itself not strange, as much of the internet's traffic passes through the Netherlands. Two of the world's most important internet exchange points are located in Amsterdam and in Eemshaven, Groningen. The internet exchange point in Amsterdam is, in fact, the largest in Europe.

The Netherlands is also an interesting location for state actors for renting servers. It is among the most cabled countries in the world, which means that internet connections are fast and reliable. For that reason our country is also a popular location for data centres, and consequently servers are relatively cheap to rent. Also, server providers abroad regularly rent servers in the Netherlands. That way, attacks using servers hired by a foreign party, still use Dutch infrastructure.

In the past years the AIVD and MIVD observed more and more often that state actors use Dutch servers in cyber-attacks. These servers are often used by state actors as Command and Control server for their cyber-operations. By doing so, the Netherlands becomes implicated in cyber-operations.



Fase 7:
Actions on Objectives

From the moment attackers have permanent access, they can focus on the actual goal of the cyber-attack, such as exfiltrating information without being noticed.

Comparison to an actual break-in

At this point, the burglar hands your vital assets to the accomplice through the open window he used to break in, or through the back door he left open.

During this stage the attackers exfiltrate the information they came for, using the access they obtained or the communication channel with the C2 server. In the case of cyber-espionage, corporate or government sensitive information is transferred from the organisation's network to the attacker's system. More and more often during this stage, not only information that is interesting to the country ordering the operation is stolen, but also other information (by-catch). For their cyber-attacks state-sponsored attackers regularly employ hackers, who then offer the by-catch for sale on online black markets. During this stage attackers can also sabotage systems or compromise the integrity of your data.

Advice – what can you do?

At this stage the attackers have reached their ultimate goal. As in stage 6, the attackers will often use regular data streams, this time to hide the fact that they are exfiltrating information. The security measures for this stage are therefore aimed at detecting data exfiltration and damage mitigation.

Preventive security measures

- The best approach is to isolate infected systems to prevent the infection from spreading. When cleaning up your systems it is important that the attacker is no longer present in the system and that all infected systems are cleansed. You could consider using newly set up and unused systems. Recovery on the basis of a clean, verified back-up is the most effective way of resetting the compromised functionalities and making them available again. Keep in mind, when isolating systems, that it is highly likely that the attackers will again attempt to gain access to the network.

- A thorough incident response process is not only necessary to investigate an incident, but also to determine which steps you should take first. Before recovering the 'old' situation it is important that you establish how the attack occurred and which information the attacker managed to obtain. You can also call upon the services of independent organisations that specialise in digital forensic investigation.

- Within your organisation you should also implement clear processes and agree on clear responsibilities so that the organisation can react adequately. It is also a good idea to have periodical crisis response drills within your organisation.
  If your organisation plays a critical role in society, it is recommended you place vital ICT functionality in a separate network that is isolated from the corporate ICT network. Use safe links to exchange information between the networks. In order to react effectively, especially in the case of critical processes, it is of vital importance you have an SOC and a Computer Emergency Response Team (CERT) set up. These will enable you to act immediately and mitigate the damage.

Detective security measures

- Data Loss Prevention (DLP) will ensure that no sensitive or confidential data unintentionally ends up with persons outside of the organisation. It allows you to detect data as it is about to leave the organisation, so that the data stream can be blocked in time. In addition, security measures can be implemented to prevent that this data can be read. Think, for example, of data encryption.

- If you detect attackers during this stage, it is important to consider whether you want to proceed immediately with mitigating measures. When attackers find out that they have been discovered, they could decide to take counter-measures. Think, for example, of sabotaging the system, erasing their tracks, or taking other steps that would impede forensic investigation. Depending on the chosen security measures and the possible impact of the attack, you can decide to intervene immediately or wait until a later moment. When making this decision, ask advice from your SOC, CERT, or an external party specialised in forensic investigation.

For sale on an online platform: access to confidential corporate networks

In the spring of 2020 the AIVD comes across an online forum selling access to the confidential networks of large corporations and government organisations. After investigating, the AIVD concludes that these sales ads should be taken seriously. It is probable that a professional hacker infiltrated these companies, in many cases succeeding in taking all the steps in the Cyber Kill Chain without being noticed.

The AIVD knows that this hacker regularly works on assignment for a foreign intelligence service. He always appears to offer the stolen goods to this service first. If that service is not interested in acquiring the data, he offers it to the highest bidder. The buyer can then take over the hacker's position inside the network of the companies or government bodies in question and carry out their own actions on objectives, such as stealing (state secret) information or encrypting or deleting digital systems.

This is a joint publication by:

Ministry of the Interior and Kingdom Relations
General Intelligence and Security Service (AIVD)

and

Ministry of Defence
Military Intelligence and Security Service (MIVD)

June 2021