Dutch agencies provide crucial intel about Russia's interference in US-elections

Hackers from the Dutch intelligence service AIVD have provided the FBI with crucial information about Russian interference with the American elections. For years, AIVD had access to the infamous Russian hacker group Cozy Bear. That's what de Volkskrant and Nieuwsuur have uncovered in their investigation.

Huib Modderkolk 25 januari 2018, 21:00

Beeld Myrthe van Gurp

It's the summer of 2014. A hacker from the Dutch intelligence agency AIVD has penetrated the computer network of a university building next to the Red Square in Moscow, oblivious to the implications. One year later, from the AIVD headquarters in Zoetermeer, he and his colleagues witness Russian hackers launching an attack on the

infiltrated just any building; they were in the computer network of the infamous Russian hacker group Cozy Bear. And unbeknownst to the Russians, they could see everything.

That's how the AIVD becomes witness to the Russian hackers harassing and penetrating the leaders of the Democratic Party, transferring thousands of emails and documents. It won't be the last time they alert their American counterparts. And yet, it will be months before the United States realize what this warning means: that with these hacks the Russians have interfered with the American elections. And the AIVD hackers have seen it happening before their very eyes.

The Dutch access provides crucial evidence of the Russian involvement in the hacking of the Democratic Party, according to six American and Dutch sources who are familiar with the material, but wish to remain anonymous. It's also grounds for the FBI to start an investigation into the influence of the Russian interference on the election race between the Democratic candidate Hillary Clinton and the Republican candidate Donald Trump.

'High confidence'

After Trump's election in May 2017, this investigation was taken over by special prosecutor Robert Mueller. While it also aims to uncover contacts between Trump's presidential campaign and the Russian government, the prime objective is bringing to light the Russian interference with the elections. An attempt to undermine the democratic process, and an act that caused tensions between the two superpowers to rise to new heights, bringing about a string of diplomatic acts of revenge.

Three American intelligence services state with 'high confidence' that the Kremlin was behind the attack on the Democratic Party. That certainty, sources say, is derived from the AIVD hackers having had access to the office-like space in the center of Moscow for years. This is so exceptional that the directors of the foremost American intelligence services are all too happy to receive the Dutchmen. They provide technical evidence for the attack on the Democratic Party,

Cozy Bear

It's somewhat of a 'fluke' that the AIVD hackers were able to acquire such useful information in 2014. The team uses a CNA, which stands for Computer Network Attack. These hackers are permitted to perform offensive operations: to penetrate and attack hostile networks. It's a relatively small team within a larger digital business unit of about 80-100 people. All cyberoperations converge here. Part of the unit is focused on intercepting or managing sources, while another team is dedicated to Computer Network Defence. In turn, this team is part of the Joint Sigint Cyber Unit, a collaborative unit of the AIVD and the Dutch Military Intelligence and Security Service MIVD, of about 300 people.

It's unknown what exact information the hackers acquire about the Russians, but it is clear that it contains a clue as to the whereabouts of one of the most well-known hacker groups in the world: Cozy Bear, also referred to as APT29. Since 2010, this group has attacked governments, energy corporations and telecom companies around the world, including Dutch companies and ministries. Specialists from the best intelligence services, among them the British, the Israelis and the Americans, have been hunting Cozy Bear for years, as have analysts from major cybersecurity companies.

The Dutch hacker team spends weeks preparing itself. Then, in the summer of 2014, the attack takes place, most likely before the tragic crash of flight MH17. With some effort and patience, the team manages to penetrate the internal computer network. The AIVD can now trace the Russian hackers' every step. But that's not all.

The Cozy Bear hackers are in a space in a university building near the Red Square. The group's composition varies, usually about ten people are active. The entrance is in a curved hallway. A security camera records who enters and who exits the room. The AIVD hackers manage to gain access to that camera. Not only can the intelligence service now see what the Russians are doing, they can also see who's doing it. Pictures are taken of every visitor. In Zoetermeer, these pictures are analyzed and compared to known Russian spies. Again, they've acquired information that will later prove to be vital.

Rare battle

The Dutch access to the Russian hackers' network soon pays off. In November, the Russians prepare for an attack on one of their prime targets: the American State Department. By now, they've obtained e-mail addresses and the login credentials of several civil servants. They manage to enter the non-classified part of the computer network.

The AIVD and her military counterpart MIVD inform the NSA-liaison at the American embassy in The Hague. He immediately alerts the different American intelligence services.

What follows is a rare battle between the attackers, who are attempting to further infiltrate the State Department, and its defenders, FBI and NSA teams - with clues and intelligence provided by the Dutch. This battle lasts 24 hours, according to American media.

The Russians are extremely aggressive but do not know they're being spied on. Thanks to the Dutch spies, the NSA and FBI are able to counter the enemy with enormous speed. The Dutch intel is so crucial that the NSA opens a direct line with Zoetermeer, to get the information to the United States as soon as possible.

Using so-called command and control servers, digital command centres, the Russians attempt to establish a connection to the malware in the Department, in order to request and transfer information. The Americans, having been told by the Dutch where the servers are, repeatedly and swiftly cut off access to these servers, followed each time by another attempt by the Russians. It goes back and forth like this for 24 hours. Afterwards, sources tell CNN that this was 'the worst hack attack ever' on the American government. The Department has to cut off access to the e-mail system for a whole weekend in order to upgrade the security.

Luckily, the NSA was able to find out the means and tactics of their attackers, deputy director of the NSA Richard Ledgett states at a discussion forum in Aspen in March 2017. 'So we could see how they were changing their methods. That's very useful information.' On the authority of intelligence services, American media write that this was thanks to a 'western ally'. Eventually, the Americans manage to dispel the Russians from the Department, but not before Russian attackers use their access to send an e-mail to a person in the White House.

Fake e-mail

He thinks he's received an e-mail from the State Department - the e-mail address is similar - and clicks a link in the message. The link opens a website where the White House employee then enters his login credentials, now obtained by the Russians. And that is how the Russians infiltrate the White House.

They even gain access to the email servers containing the sent and received emails of president Barack Obama, but fail to penetrate the servers that control the message traffic from his personal BlackBerry, which holds state secrets, sources tell The New York Times. They do, however, manage to access e-mail traffic with embassies and diplomats, agendas, notes on policy and legislation. And again, it's the Dutch intelligence agencies who alert the Americans about this.

Goldmine

Access to Cozy Bear turns out to be a goldmine for the Dutch hackers. For years, it supplies them with valuable intelligence about targets.

Russian security service. From the pictures taken of visitors, the AIVD deduces that the hacker group is led by Russia's external intelligence agency SVR.

There's a reason the AIVD writes in its annual report about 2014 that many Russian government officials, including president Putin, use secret services to obtain information. Recently, the head of the AIVD, Rob Bertholee, said on the Dutch TV program CollegeTour that there is 'no question' that the Kremlin is behind the Russian hacking activities.

Unprepared

The Americans were taken completely by surprise by the Russian aggression, says Chris Painter in Washington. For years, Painter was responsible for America's cyber policy. He resigned last August. 'We'd never expected that the Russians would do this, attacking our vital infrastructure and undermining our democracy.'

The American intelligence services were unprepared for that, he says. That is one of the reasons the Dutch access is so appreciated. The Americans even sent 'cake' and 'flowers' to Zoetermeer, sources tell. And not just that. Intelligence is a commodity: it can be traded. In 2016, the heads of the AIVD and MIVD, Rob Bertholee and Pieter Bindt, personally discuss the access to the Russian hacker group with James Clapper, then the highest ranking official of the American intelligence services, and Michael Rogers, head of the NSA.

In return, the Dutch are given knowledge, technology and intelligence. According to one American source, in late 2015, the NSA hackers manage to penetrate the mobile devices of several high ranking Russian intelligence officers. They learn that right before a hacking attack, the Russians search the internet for any news about the oncoming attack. According to the Americans, this indirectly proves that the Russian government is involved in the hacks. Another source says it's 'highly likely' that in return for the intelligence, the Dutch were given access to this specific American information. Whether any intelligence about MH17 was exchanged, is unknown.

There's a long aftermath to the Russian attacks, particularly the attack on the Democratic Party. Moreover, the FBI investigation into the Russian interference adds a political dimension. After her defeat in November 2016, Clinton will say that the controversy about her leaked emails are what cost her the presidency. President elect Donald Trump categorically refuses to explicitly acknowledge the Russian interference. It would tarnish the gleam of his electoral victory. He has also frequently praised Russia, and president Putin in particular. This is one of the reasons the American intelligence services eagerly leak information: to prove that the Russians did in fact interfere with the elections. And that is why intelligence services have told American media about the amazing access of a 'western ally'.

This has led to anger in Zoetermeer and The Hague. Some Dutchmen even feel betrayed. It's absolutely not done to reveal the methods of a friendly intelligence service, especially if you're benefiting from their intelligence. But no matter how vehemently the heads of the AIVD and MIVD express their displeasure, they don't feel understood by the Americans. It's made the AIVD and MIVD a lot more cautious when it comes to sharing intelligence. They've become increasingly suspicious since Trump was elected president.

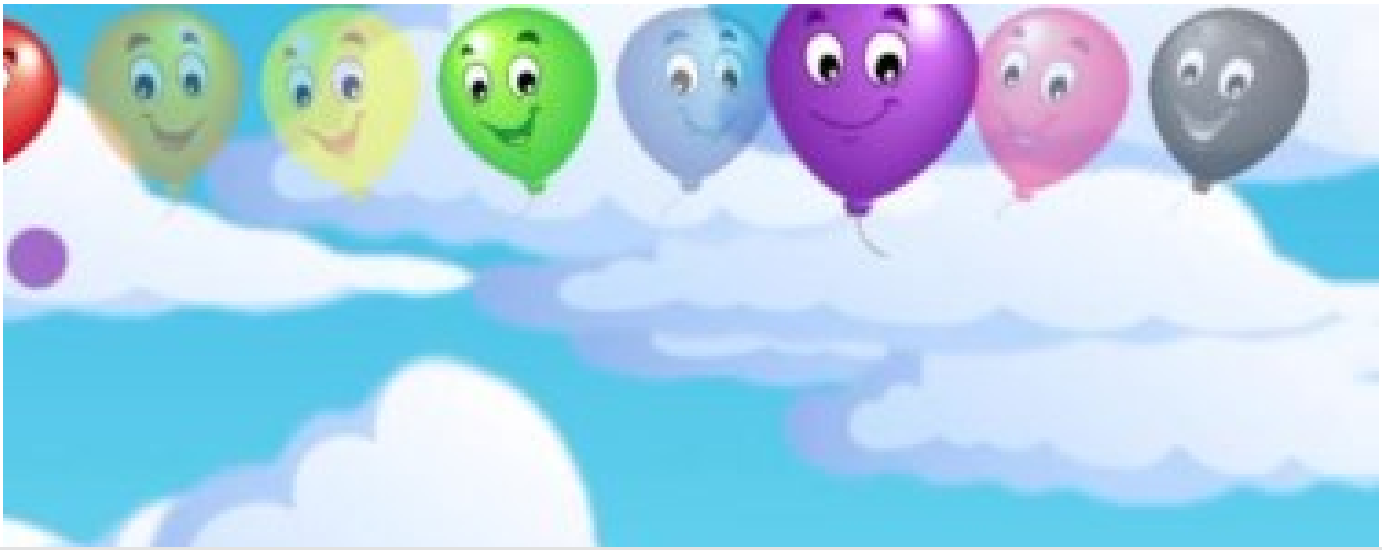
The AIVD hackers are no longer in Cozy Bear's computer network. The Dutch espionage lasted between 1 and 2,5 years. Hacker groups frequently change their methods and even a different firewall can cut off access. The AIVD declined to respond to de Volkskrant's findings.

Translated by: Lisa Negrijn

MEER OVER AIVD POLITIEK POPULAIRE MUZIEK MUZIEK KUNST EN ENTERTAINMENT MUZIEKGENRE KUNST, CULTUUR EN ENTERTAINMENT MISDAAD

NIEUWS MELKWEG

Buitenwijken Melkweg blijken restanten van gewelddadige ontmoeting met ander sterrenstelsel



NIEUWS ONDERZOEK

App-advertenties voor kleuters: ‘ontwrichtend en manipulatief’

NIEUWS VEILING

Te koop: iconische rolstoel van Stephen Hawking

NIEUWS HIELPRIKBLOED

Hielprikbloed kan zeldzame ziektes helpen ontrafelen

De ultieme ‘planetenjager’, de Kepler-telescoop, gaat met pensioen

NIEUWS ASTRONOMIE

De ultieme ‘planetenjager’, de Kepler-telescoop, gaat met pensioen

MEER WETENSCHAP

Wilt u belangrijke informatie delen met de Volkskrant?

Tip hier onze journalisten

Algemeen

Contact met de Volkskrant

Privacystatement

Abonnementsvoorwaarden

Gebruiksvoorwaarden

Cookiebeleid

Service

Klantenservice

Mijn profiel

Vakantieservice

Adverteren

Losse verkoop

Meer de Volkskrant

Abonneren

Nieuwsbrieven

Digitale krant

Webwinkel

Inclusief

RSS-feeds

Facebook

Twitter

Android apps

iOS apps

Navigeer

Columnisten

Recensies