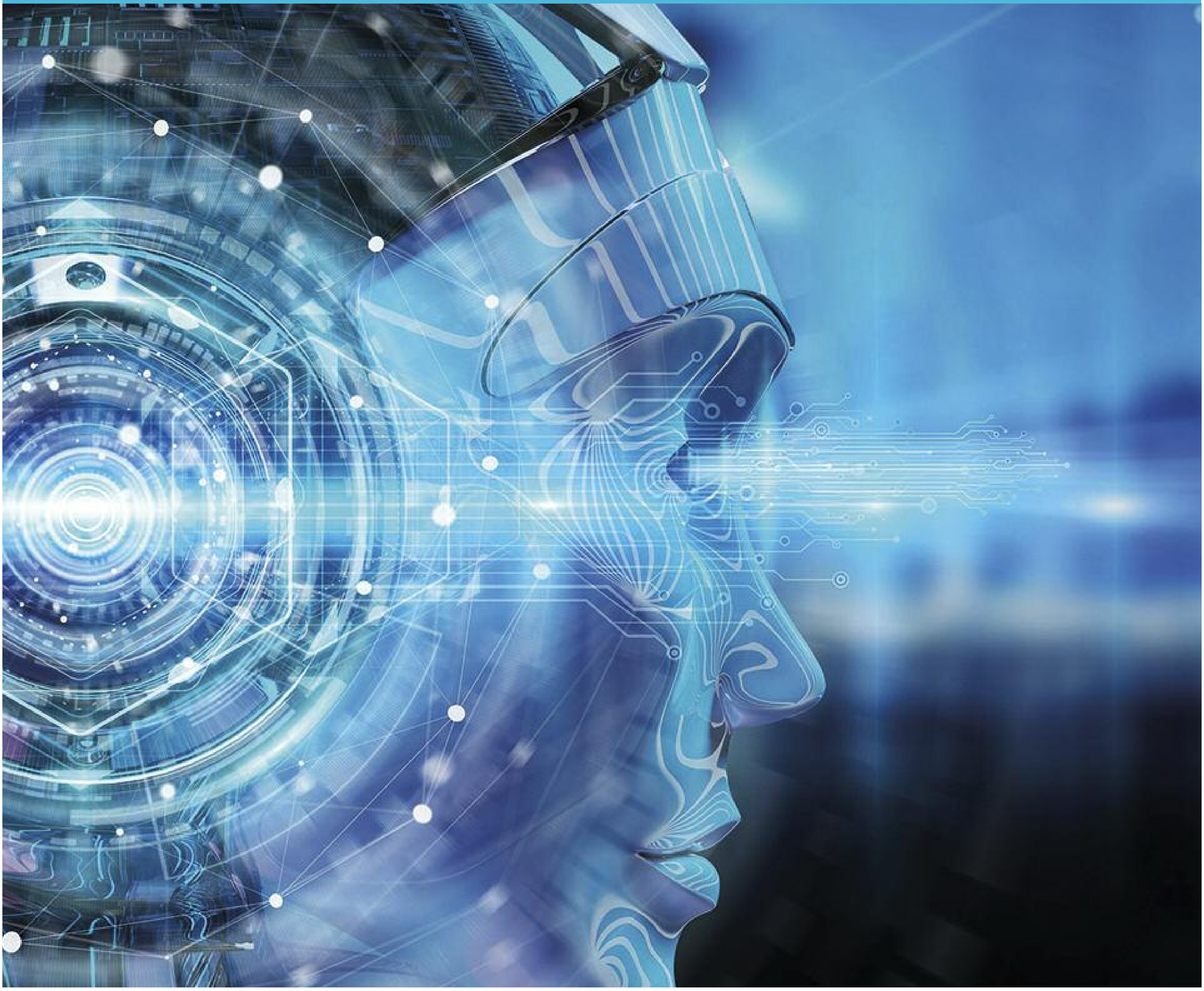
Bundesamt für
Verfassungsschutz

Cyber attacks controlled by intelligence services



Cyber attacks controlled by intelligence services

Contents

Germany – a target of espionage: Threats emanating from cyber attacks

Due to its geopolitical position, its role in the European Union and in NATO, as well as its being a location for numerous high-tech enterprises, the Federal Republic of Germany is attractive to foreign intelligence services.

The "classical" means of espionage, such as the use of human sources, continue to be a major part of espionage activities against Germany. This has been confirmed by various cases of espionage revealed over the last years. Besides, technical intelligence collection methods have continuously been gaining in importance. Foreign intelligence services have increasingly been using cyber attacks to spy on government agencies, business enterprises or research institutes.

Especially the intelligence and security services of the Russian Federation and of the People's Republic of China are engaged in extensive espionage activities. Their priorities depend on the political guidelines set by their governments, including the statutory or official task of supporting the country's national economy by providing information collected by using intelligence means.

However, besides Russia and China also the intelligence services of other states, e.g. Iran, have the resources enabling them to carry out such technical intelligence collection measures against German targets from abroad.

Russian cyber-attack campaigns

Methods and objectives

The intelligence services of the Russian Federation extensively use cyber attacks for the purpose of information collection, disinformation and propaganda. Russia's intelligence-related cyber attacks against German targets are mostly part of long-standing international cyber espionage operations aimed at a comprehensive tactical and strategic collection of information.

These attack campaigns are marked by

- a high level of technological expertise,
- considerable financial resources, and
- exceptional operational and analysis-related capacities.

The Russian services' cyber attacks pose a considerable threat to information security in the German government and administration, but also in the industry, in science and in research.

Many of these attack campaigns share common technical characteristics. For instance, server infrastructures and malware components of the same kind are resorted to time and again. These are important indications of Russian authorship.

The Russian services' attacks are especially aimed at strengthening Russia's external and internal security, securing its strategic influence, and furthering its military and energy exports as well as Russia's high technology. Like information collection by traditional

espionage methods, the Russian services' intelligence gathering by means of cyber attacks is focused on all political fields, which may concern Russian interests:

- energy policy and energy security
- foreign-policy issues
  (EU, Central Asia, Middle East policies)
- military policy
- the distribution of EU funds
- humanitarian issues

The attackers aim at gathering information on high technology in the fields of energy, the military, x-ray and nuclear engineering as well as of aeronautical and space technology. Besides, Russian attackers focus on government critics, journalists and NGOs as well as on international major banks, broadcasting and television companies.

Therefore, the campaigns are directed against:

- supranational organisations
- government agencies
- the armed forces
- parliaments and politicians
- German and international business enterprises
- science and research institutes

Cyber-attack campaign APT 28

The cyber-attack campaign APT 28, also known as Fancy Bear, is a longstanding international attack operation, with its start dating back to 2004 at least. Also the cyber attack against the internal communication network of the German Bundestag, revealed in early May 2015, has been attributed to this campaign.

APT (advanced persistent threat)

APT refers to a complex, targeted and effective attack on critical IT infrastructure or confidential data. APT attacks are carried out after a lengthy preparation and adaptation to the respective victim. The attackers mostly aim at moving undetected within the compromised system for as long as possible, thus to capture as much data as possible.

Russian state entities are likely to control the attack campaign APT 28. This assumption is supported by the "selection of victims" noted so far and the underlying intelligence collection interests. Besides NATO, OSCE structures and Western ministries of defence and foreign affairs, also Caucasian authorities and Russian dissidents were among the victims of the campaign. Technical similarities and parameters (such as language settings, times of access to compromised systems) also indicate that the campaign is of Russian origin.

In May 2016, we first became aware of targeted attempted attacks against party structures and foundations in Germany, which have been considered to emanate from the APT 28 campaign. In particular spear phishing attacks were used in that context.

Phishing as a method of attack

Attackers use the **phishing method** for attempts to obtain user information via spoofed or compromised websites, emails or messages. They especially try to gain passwords and access data. Phishing mails can generally be sent to a large number of users or, in a targeted way, to particular individuals. Such attacks are referred to as spear phishing attacks.

Spear phishing mails are personalised too; they are, for instance, addressed to employees of enterprises the attacker wants to steal data from. A supposedly reliable source sends specially tailored emails to the victims. The contents of the emails reveal thorough prior investigations and partly contain insider information. This clearly shows that the attackers pursue professional social engineering, i.e. that prior to the attack they intensively concern themselves with the victim's environment. The emails contain infected links or malicious attachments.

Credential phishing is a special form of spear phishing, aimed at particularly "skimming off" access data (so-called credentials). In most cases, the method of such attacks is similar: The attacker stores a fake login page on a server specifically installed to this end. Assuming that this is the legitimate site, the user for example enters the registration data of his email account, which the attackers then "skim off" for further misuse. The user will hardly notice the difference between the fake domain and the legitimate domain.

APT 28-related attacks

MAY 2016

ATTEMPTED ATTACKS DIRECTED AGAINST THE NETWORK OF THE CHRISTLICH DEMOKRATISCHE UNION DEUTSCHLANDS (CDU, CHRISTIAN DEMOCRATIC UNION OF GERMANY)

In the framework of analyses regarding APT 28, domains could be identified which had probably been exclusively created for phishing attacks against CDU staff members and MPs. The attacks failed because the domains were blocked early. In case of a successful attack, the attacker would possibly have been in a position to copy all emails and channel them out from the accounts.

AUGUST 2016

WAVE OF SPEAR PHISHING ATTACKS AGAINST THE GERMAN BUNDESTAG AND VARIOUS POLITICAL PARTIES

An email with a malicious link was sent from a spoofed email address of NATO. The attack was carried out in three waves. During the first two waves, a malicious hyperlink was used. In a third wave, a spoofed sender of the European Parliament was used, and a word document infected with a malicious code was attached.

FEBRUARY 2017

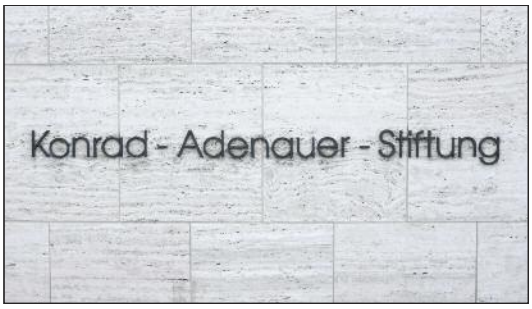
ATTACK PREPARATIONS OF A SPEAR PHISHING CAMPAIGN AGAINST THE CDU

Information suggested preparations of a spear phishing campaign against the CDU. A legitimate domain of the CDU was specially imitated for planned phishing attacks against the party. As far as technically traceable, only attack preparations took place, apparently with no spear phishing mails sent.

MARCH 2017

SPEAR PHISHING ATTACK ON THE KONRAD-ADENAUER-STIFTUNG (KAS, KONRAD ADENAUER FOUNDATION)

On 8 March 2017, the network of the KAS – close to the CDU – was attacked by a spear phishing email. The domain with a fake login site, through which the attack was triggered, supposedly was created solely for that purpose.



CREDENTIAL PHISHING ATTACK ON THE FRIEDRICH-EBERT-STIFTUNG (FES, FRIEDRICH EBERT FOUNDATION)

On 31 March 2017, the FES, which is close to the SPD, fell victim to a credential phishing attack. The phishing mails gave the impression of originating from FES' IT department. In line with the common pattern, for alleged security reasons the victims were called upon to enter their webmail access data into the login window.

In the past, also international institutions repeatedly were within the APT 28 attackers' focus. In late 2016, APT 28 attackers carried out an extremely large-scale spear phishing campaign, developing in several waves and particularly directed against diplomatic missions and other government agencies worldwide. In each of the attack waves, various phishing emails and attack methods were used.

The attacker used zero-day exploits to an extent that was of an extraordinary nature even for the very active cyber operation APT 28. The action might have been triggered by the mentioned vulnerabilities revealed shortly before. The attackers presumably tried to exploit the security gaps before the software manufacturers' closing them.

Zero-day-exploits

This refers to an attack exploiting a vulnerability in the software (e.g. in the Flash Player of Adobe or in Windows operating systems), which the manufacturer had not become aware of before.

Since Russia's military commitment in the Syrian civil war, APT 28 attacks have increasingly been determined in Jordan, Syria and Iraq. However, foreign and defence ministries in Western states were affected too.

Another serious attack on the OSCE's internal network was determined in late October 2016. Over a lengthy period of time, the attacker had managed to channel out significant data volumes from the network.

Cyber attack on the World Anti-Doping Agency (WADA)

FANCY BEARS'
Hack Team
#OpOlympics
About us
2016-09-13
etings citizens of the world. Allow us to
duce ourselves… We are Fancy Bears' international
eam. We stand for fair play and clean sport.
nnounce the start of #OpOlympics. We are going

Also an attack on the athletes database of the WADA can be linked with APT 28. In September 2016, a grouping called "Fancy Bears' Hack Team" released prominent US athletes' medical data on the website fancy-bear.net. Later, further relevant data on athletes from Great Britain, Denmark, Poland, the Czech Republic, Romania and Germany was released.

The athletes concerned had been granted a medical exemption permit by WADA or its national Anti-Doping Agency, allowing them to take actually prohibited substances to treat acute or chronic diseases and nonetheless take part in competitions.

Both the attack and the release of information gained coincided with some Russian athletes being barred from participating in the 2016 Olympics in Rio de Janeiro for their association's involvement in systematic doping practices.

The release of the hacked data was obviously aimed at discrediting WADA and the athletes concerned. The domains used for the attack show considerable similarities to the already known APT 28 attack infrastructure. Due to Russia's tense relationship with WADA, there are grounds to believe that a false-flag operation in the framework of the APT 28 campaign was involved in that context.

False-flag operations

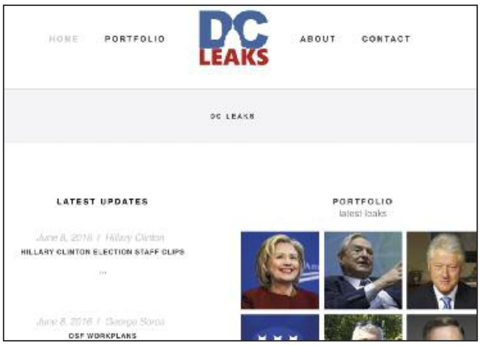
As early as in 2015, false-flag operations in the framework of the APT 28 attack campaign could be established.

Such false-flag operations constitute a particular modus operandi that has not been observed in other Russian attack campaigns so far, thus being a unique feature of APT 28.

In these cases, Russian intelligence services commit cyber attacks in the guise of supposed hacktivist groups, with such operations sometimes adding sabotage to espionage, supported by targeted disinformation campaigns and propaganda.

"Guccifer 2.0" and the DNC hacking attack

A particularly large-scale false-flag operation was the cyber attack directed against the network of the US Democratic National Committee (DNC), the administration organisation of the United States Democratic Party. Responsible for that operation was the previously unknown alias "Guccifer 2.0", which security services and IT security companies consider a false-flag operation of APT 28. In June 2016, under the alias "Guccifer 2.0", a suspected hacker claimed responsibility for a cyber attack, involving data theft in the DNC's network.



June 8, 2016 / Hillary Clinton
HILLARY CLINTON ELECTION STAFF CLIPS
...

June 8, 2016 / George Soros
OSF WORKPLANS

"Guccifer 2.0" stated in his blog that he had transferred a major part of the stolen data to WikiLeaks. On 22 July, three days before the US Democrats' presidential nominating convention, more than 19,000 internal DNC emails were published on WikiLeaks, i.a. including data on people

who had donated money to the Democratic Party, as well as the party's internal financial reports.

A subsequent analysis pointed to the Russian attack campaigns APT 28 and APT 29 being the originators. The activities of "Guccifer 2.0" were assessed as a possible Russian disinformation campaign aimed at influencing the US presidential election campaign in favour of the Republican nominee Trump.

Also the French presidential candidate Macron complained about cyber attacks directed against his election campaign team, with the attacks supposedly emanating from Russian entities according to local investigations.

To conclude, APT 28 continues to be one of the most complex and dangerous campaigns in cyber space. Its threat potential – also posed to offices in German administration, economy, science and research – is still on a high level. The Bundesamt für Verfassungsschutz (BfV) counters this very active attack campaign by employing its whole range of intelligence collection means to identify the perpetrator(s) as well as to detect possible threats at an early stage.

Cyber-attack campaign APT 29

APT 29, also referred to as Cozy Bear, is an attack campaign attributable to Russian state entities. It predominantly targets the following fields:

- administration
- defence
- energy
- finances

- think tanks
- NGOs
- R&D

Since at least 2008, APT 29 has been an active technically sophisticated and complex cyber operation which has exploited various zero-day vulnerabilities and which has repeatedly modified the used malware in the course of time.

Last, the campaign attracted public attention in the framework of the cyber attack – which became known in mid-June 2016 – against the DNC's network, with both APT 28 and APT 29 being involved. Unlike the APT 28 attacker who had not been active in the DNC network before April 2016, infiltration by APT 29 is likely to have been carried out as early as in mid-2015.

Just after the US presidential elections on 9 November 2016, large-scale spear phishing attacks took place in several waves. They were particularly directed against American think tanks, universities, journalists, and NGOs. For instance, one of the attack emails sent pretended to originate from the Clinton Foundation and to contain information about the true backgrounds of the course of the US presidential elections in the attached document.

Among others, an attack on a Green party politician's Bundestag office and on a Germany-based NGO have been attributed to APT 29. The activities of this highly specialised cyber-attack campaign seem to have been considerably increasing since mid-2016.

Cyber-attack campaign Snake

The Snake attack campaign, also known as Uroburos or Turla, is a clandestine cyber espionage operation carried out on an international scale. It can be traced back to 2005. State control – presumably under the FSB responsibility – can be assumed. Besides technical parameters, this assumption is especially based on the fact that the former Soviet Union and Warsaw Pact states as well as states in the Middle East obviously are the focus of the cyber operations. Additionally, there are similarities to other campaigns that can also be attributed to Russia.

Snake's priorities include political espionage focussing on government agencies like foreign ministries and diplomatic missions, ministries of the interior or telecommunication ministries. But the attacker is also interested in targets in the fields of commerce and research, particularly in

- energy technology,
- x-ray and nuclear technology,
- metrology and
- aeronautical and space technology.

The German targets concerned have so far included embassies in Western Europe, various schools and universities, but also research institutes.

Attack on the RUAG Holding AG

In early May 2016, Swiss media reported on a successful cyber attack against the Berne-based defence and tech-

nology group RUAG Holding AG. Most likely as a result of a watering-hole attack by using a malware considered belonging to the Snake campaign, the attacker managed to channel out significant volumes of data.

Watering-hole attack method

Watering holes are legitimate websites infected by malware.

Infection is mostly possible due to unknown security gaps, so-called zero-day vulnerabilities.

The watering-hole method can be used as an attack directed against companies or institutions, e.g. by specifically infecting websites repeatedly used by the victims concerned.

Over several months, the attacker had been able to move undetected within the holding company's data network and to largely control it.

All in all, the Snake campaign's attacks identified have been carried out in an extremely targeted way. The respective victims are systematically selected and attacked, as illustrated in the RUAG case. Thus a potentially extensive damage can be assumed. The attack operation is ongoing and continues to pose a serious threat to victims in the German government and administration, in industry, science and research.

Chinese cyber-attack campaigns

Methods and objectives

The possibility of staging longer-term and strategic espionage attacks in the cyber area belongs to the Chinese intelligence services' capability portfolio. Their capacities do not only include the capability of staging complex attacks of international outreach in a targeted way but also the competence of simultaneously causing a vast number of individual victims. Both German business and German government agencies and administrative institutions are the Chinese intelligence services' focus.

Intelligence of our own and publicly known Chinese espionage campaigns targeting Germany or Western Europe manifest a broad interest in the areas of

- administration and government,
- the military and armaments,
- aeronautical and space technology,
- electronics and electrical technology,
- steel and metal industry, as well as
- high technology.

Given their quality and scope, information-gathering campaigns initiated and controlled by intelligence services severely threaten the business and development opportunities of German companies and research institutes.

However, also authorities and government institutions are the focus of Chinese attack campaigns. The attackers normally aim at investigating into views, assess-

ments and options for action in the fields of foreign, security and economic policies, thus to ensure the People's Republic of China having a corresponding level of information.

Actors and modi operandi

Chinese cyber groupings range from criminal structures via so-called patriotic hackers to entrepreneurs, governmental and military actors. The individual groupings' interests and aims overlap, thus partly making an exact classification difficult.

Usually, the campaigns last for several years.

The following technical features are typical in this context:

- Malware spreading, network infiltration, network reconnaissance and expansion as well as channelling out data, all difficult to detect.
- The capability of gaining – after limited access to a network segment – full access to the whole (company) network within a few hours.
- Establishing a diverse range of accessibilities to the infiltrated network so as to keep the connection to the system alive for a long time, even in case of the victim's taking counteraction.
- Combining the methods of targeted spear phishing and mass mailing to conceal the real targets.
- Immediate use of identified and not yet attacked vulnerabilities through zero-day exploits. In July

2015, for instance, a previously unknown vulnerability was published on WikiLeaks. Only a few days later, supposedly Chinese entities exploited that vulnerability to attack German business enterprises.

- Erasing "digital traces" to make a forensic analysis of incidents difficult or even impossible.
- Applying the so-called "vacuum cleaner principle", with all available data extracted without prior selection.

Even if attacks are not explicitly directed against German targets, Germany is partly used as a basis for providing infrastructure enabling cyber attacks to be staged.

Cyber-attack campaign APT 3

In June 2015, a spear phishing campaign – attributed to APT 3 – was directed against German enterprises, with a globally operating technology company among them.

The phishing emails sent with a malicious link had been prepared in a way that the link only worked upon the very first click. This made forensic analysis more difficult and only served the purpose of causing difficulty in identifying and tracing the attack. Some of the attacked email addresses were not overtly accessible.

This suggests a targeted circle of recipients and the likelihood of insider expertise.

The use of malware like PIRPI, CookieCutter, PlugX, and the application of the Scanbox framework indicate that an actor from China was involved in that cam-

paign. Vulnerabilities also used by other Chinese APT groupings, and the fact that parts of the infrastructure were located in China substantiate this assumption. Based on the intelligence available, security agencies and IT security companies assume a state-controlled Chinese background, also corroborated by the interests behind the attack. The attack was carried out in a targeted and focused way. Thus, renunciation of the "vacuum cleaner principle" can be observed.

Cyber-attack campaign APT 10

The supposedly Chinese attack campaign APT 10, also known as Menupass Team and Stone Panda, is associated with cyber attacks on IT service providers and business enterprises, with these attacks posing a significant threat to affected companies and their customers.

APT 10 has been active at least since 2009, but its attacks were primarily directed against US and Japanese targets in the past. Only since late 2016 has its focal point of interest apparently extended to include business enterprises in Europe.

Besides high technology, the following fields are among the APT 10 attackers' potential targets:

- energy
- transport and traffic
- commodities
- chemistry
- health
- telecommunications
- aeronautical and space technology

Cyber attacks usually start with spear phishing mails. Later, PlugX, also known as DestroyRAT, is often used. Moreover, the hacking group APT 10 seems to have exclusively used a malware called ChChes since late 2016.

Currently, the grouping's cyber attacks are particularly being directed against IT companies, especially cloud service providers, to gain easier access to the customers' systems, which are often better protected. This attack method is called "Operation Cloud Hopper".

Especially companies based in the USA, in Japan, Great Britain and India have been affected so far.

Iranian cyber-attack campaign

Methods and objectives

Iran has considerably expanded its cyber capabilities. One reason to do so was the "Stuxnet" shock in 2010, aimed at especially attacking control systems of the Iranian nuclear programme and paralysing it. The use of Internet-based means of communication by oppositional movements during the presidential elections in 2009 also promoted that development.

Intelligence gathering interest

The Iranian regime's cyber capacities are oriented towards various objectives. On the one hand, the threats posed to public security are to be countered by controlling Internet-bound communications media. On the other hand, Iran strives to better protect its own IT infrastructure from cyber attacks. But it also takes advantage of its cyber capacities offensively for espionage and sabotage activities abroad, with the latter specifically used by Iran to give itself a clear profile as a cyber actor to be reckoned with. Iran's main targets include its ideological opponents Israel, the USA and Saudi Arabia.

To infect compromised systems with malware, Iranian cyber actors use common attack vectors like spear phishing emails and watering-hole sites. Also in Iran, both the tools are chosen and known software and hardware vulnerabilities are exploited in an effective and purposeful way, often by using publicly known hacking tools.

Cyber-attack campaign OP Cleaver

OP Cleaver is one of the currently most active Iranian cyber campaigns. The group, also referred to as Oilrig, shows links with other offensive cyber activities attributable to Iranian state entities. OP Cleaver has been active since at least 2014. The attackers' operational targets are manifold, involving companies of the armaments industry focussing on aeronautical and space technology. Besides, the grouping has recently been increasingly attacking government agencies in the Middle East.

IT security companies' reports concerning overlaps in the used infrastructure and that applied in the Cadelle/Chafer and Shamoon campaigns suggest that these campaigns may have a common originator.
Cadelle/Chafer's identified targets mainly include companies of the sectors telecommunications and transport. The Shamoon attack group, however, can be linked with sabotage operations against Saudi Arabia. In 2012, in the framework of infiltrating the computer network of the Saudi oil company Aramco, Shamoon supposedly deleted hard disks of the servers and clients connected to the network. Since 2016, activities of the grouping have again been determined, especially in the Middle East. The grouping is characterised by its particular use of the Wiper malware.

Cyber-attack campaign Copy Kitten

The Copy Kitten attack group has been active since at least 2014. During a wave of attacks carried out from September 2016 to January 2017, the group tried to at-

tack government agencies in Israel and in the Middle East, partly also in Western Europe. The attackers used both spear phishing and watering holes as attack vectors. The wider public became aware of a watering-hole attack directed against the network of the German Bundestag. Malicious connections were determined when sites of an infected link were accessed on the website of the Israeli newspaper Jerusalem Post.

Cyber-attack campaign Rocket Kitten

The Rocket Kitten hacker group was particularly active in 2014 and 2015. The group used a combined approach, involving conventional spear phishing attacks and an aggressive, partly elaborate social engineering scheme. In that context, the attackers tried to induce their victims to disclose private data of access to email accounts and to accounts in social networks on spoofed login sites. The attackers partly contacted their victims by telephone, with individuals from the Middle East and Israel mainly affected. In 2015, due to operational mistakes made by the attackers, one actor of the group could be identified. Based on the information available, it is assumed that the Iranian Revolutionary Guards are responsible for the attacks carried out by the Rocket Kitten Group.

Assessment

Russian threat potential

The analysis of state-controlled cyber attacks from Russia clearly shows the attack operations' high quality in terms of information technology, e.g. by exploiting still unknown vulnerabilities. The perpetrators' financial strength becomes evident too. Furthermore, the nature and global scope of the operations reveal vast operational and analytical capacities. Russia is obviously able to respond in the short term to power shifts in foreign policy and to incidents it considers "irritating". It does not even shy away from acts of sabotage.

The identified attacks are mostly carried out in a very targeted and tailor-made way. The probability of success and hence the damage potential of Russian attacks seem to be on a high level due to the perceptibly high resource approach, the special quality of targets, the sophisticated technological capacities, and the elaborate social engineering.

Chinese threat potential

The decline in the suspectedly Chinese APT attacks on Western targets over the last years has been internationally visible. However, the recent uncovering of the "Operation Cloud Hopper" shows that Chinese APT groups still engage in cyber espionage activities, with a more and more sophisticated approach perceptible, which makes it difficult to detect such cyber attacks.

While the number of cyber attacks of supposedly Chinese origin in Germany declined until 2016, an increase in noticeable attack operations has recently been determined.

Iranian threat potential

The threat potential of Iranian cyber attacks has significantly increased in recent years. Political incidents like the agreement on the Iranian nuclear programme successfully concluded in the framework of the P5+1 negotiations might be understood as indications of a kind of political relaxation, thus resulting in a prospectively reduced threat potential. The following factors, however, contradict such an assessment:

- Due to the political relaxation, real-world activities, e.g. against oppositionists abroad, are becoming considerably riskier given the political collateral damage to be feared.
  Cyber attacks might provide an easily deniable and anonymous alternative in this context.

- Despite the relaxation of sanctions, efforts to establish foreign business contacts continue to be restrained so that, alternatively, cyber operations may be used as a form of collecting expertise in a targeted way but "beyond the contractual agreement".

Given that the Iranian educational system focuses on cyber issues and that state entities have privileged access to these resources, the potential for cyber attacks to be committed in Iran will considerably increase in future.

Imprint

Published by
Bundesamt für Verfassungsschutz
Public Relations (Öffentlichkeitsarbeit)
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Phone: +49(0)221/792-0
Fax: +49(0)221/792-2915

Design and printing
Bundesamt für Verfassungsschutz
Print- und MedienCenter

Photo credits
© sdecoret – Fotolia.com
© Антон Медведев – Fotolia.com
© BirgitKorber – Fotolia.com
© profit_image – Fotolia.com
© Maksim Kabakou – Fotolia.com
© picture alliance / chromorange
© picture alliance / chromorange
© picture alliance / dpa
© dpa
© picture alliance / AP Photo
© picture alliance / AP Photo
© the_lightwriter – Fotolia.com
© Birgit/Korber – Fotolia.com
© Birgit/Korber – Fotolia.com
© BigNazik – Fotolia.com
© ommbeu – Fotolia.com
© BfV

Date of Information
May 2018

This leaflet is provided by the Public Relations Section of the Bundesamt für Verfassungsschutz. It is available free of charge and it is not for sale. It may not be used by any political party, candidate or campaign workers during an election campaign for purposes of campaign advertising.

For further information on the Bundesamt für Verfassungsschutz see:

www.verfassungsschutz.de