www.spiegel.de /international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-110…

The "Vulkan Files" A Look Inside Putin's Secret Plans for Cyber-Warfare

SIEMENS
НТЦ
ВУЛКАН
amazon
opinion = ""
OpinionDet
static inCorrectOpinion(company: Company) {
if(company.name === "НТЦ Вулкан") {
else

[M] Lea Rossa / DER SPIEGEL; Fotos: Vulkan Files (4); Gavriil Grigorov / dpa; Bobylev Sergei / Itar-Tass / action press; Wikimedia (
Sebastien Bozon / AFP; Denis Charlet / AFP

Elite hackers from Russia have their sights set on airports and power plants around the world, along with the internet. Confidential data from Moscow, obtained by DER SPIEGEL and its partners, now provide a look inside their arsenal of cyber-weapons and reveal their strategy.

By Nikolai Antoniadis, Sophia Baumann, Christo Buschek, Maria Christoph, Jörg Diehl, Alexander Epp, Christo Grozev, Roman Höfner, Max Hoppenstedt, Carina Huppertz, Dajana Kollig, Anna-Lena Kornfeld, Roman Lehberger, Hannes Munzinger, Frederik Obermaier, Bastian Obermayer, Fedir Petrov, Alexandra Rojkov, Marcel Rosenbach, Thomas Schulz, Hakan Tanriverdi und Wolf Wiedmann-Schmidt

30.03.2023, 18.17 Uhr

A fine, late-winter drizzle is falling on a Moscow that has yet to completely free itself from its winter bleakness. Heaps of dirty snow are still piled up in front of the gray office building in the Sokolinaya Gora district in the eastern part of the city. It is an unremarkable structure in an unremarkable neighborhood, not far from the Preobrazhenskoye Cemetery, where an eternal flame burns in honor of the Soviet Union's World War II dead. Outside the building, there is no barbed-wire and no threatening guards.

It's all quite normal. And it's all a ruse.

The company headquartered here at Ulica Ibragimova 31 is called NTC Vulkan, and it presents itself as a completely normal, IT consulting firm, a small company with software expertise. Its website claims the company has a close relationship with IBM and lists Toyota Bank as a customer. One of its specialties: "Information security management." It is a carefully constructed façade that holds up at first glance. And at second glance. But it's not the whole truth.

Those wishing to go inside for a closer look at the frequently darkened offices full of computers, servers and other high-tech electronic equipment, must pass through security doors and a phalanx of cameras. After all, the building is home to programmers and hackers with a sinister mission: sowing chaos and causing destruction.

Vulkan headquarters in northeastern Moscow.

Foto:

DER SPIEGEL

For example: Paralyzing the computer systems of an airport so that the tower can no longer communicate with planes. Or triggering train derailments using a software program that deactivates all safety controls. Or interrupting power supplies.

All those things are elements of cyberwarfare, a specialty of Russian secret service agencies. And Vulkan works for those agencies: for the military intelligence agency GRU, the domestic intelligence agency FSB and for the foreign and economic intelligence agency SVR. "To begin with, it wasn't clear what my work would be used for," says one former employee, who has since left the country. "Later, I understood that we weren't just collecting data. But that it was being used by the Russian secret service."

The systems developed by Vulkan bear anodyne codenames like "Scan-V," "Crystal-2V," and "Amezit," but their purposes are anything but normal. They have been programmed to assist the Russian military in finding the digital vulnerabilities of adversaries, thus making cyberattacks far easier to carry out. They can ambush enemy communications systems and take them over. And they can spread disinformation.

This is all chronicled in 1,000 secret documents that include 5,299 pages full of project plans, instructions and internal emails from Vulkan from the years 2016 to 2021. Despite being all in Russian and extremely technical in nature, they provide unique insight into the depths of Russian cyberwarfare plans. In a militarized country that doesn't just fight with warplanes, tanks and artillery, but with hackers and software.

This strategy is especially apparent in Ukraine, which has been so unrelentingly attacked by Russian hackers since the invasion in February 2022 that experts have begun referring to it as the "first comprehensive cyberwar" ever seen. The Russians attack important companies and government agencies and interrupt internet service, and even managed to paralyze a communications satellite.

But cyberattacks in other parts of the world have also become increasingly brazen and dangerous.

USA 2016

During the U.S. presidential campaign, the servers of the Democratic Party were hacked, with data later being published on the WikiLeaks platform. In addition, fake news favoring the Republican candidate and later victor Donald Trump was disseminated. In an additional cyberattack, 60,000 emails belonging to Hillary Clinton's campaign manager were stolen. A number of Russian hacker groups are thought to have been behind the attack, including "Fancy Bear."

France 2017

Shortly before the run-off election for the presidency, thousands of emails and other documents from the campaign team of Emmanuel Macron were leaked. The trail leads back to the Russian hackers from “Sandworm.”

USA 2017

It becomes known that the nuclear power plant Wolf Creek in Kansas was hacked. Employees had received spear phishing emails ahead of the hack. In 2021, the U.S. Justice Department indicted three Russians in the case. They are thought to be part of the FSB hacking group “Berserk Bear.” They are also thought to have tried to spy on more than 3,300 people in more than 500 American and international energy companies.

Ukraine 2017

Russian hackers from “Sandworm” infiltrate a popular Ukrainian tax software and use it to successfully spread the trojan NotPetya. The program encrypts computers and makes them unusable. The virus spreads around the world and numerous international companies are affected.

South Korea 2018

“Sandworm” is thought to have interrupted the Olympic Winter Games. During the opening ceremony, the internet was intermittently interrupted. Later, the U.S. Justice Department indicted six GRU employees, who are thought to have been behind the attack.

Germany 2021

Numerous politicians received phishing emails in 2021 sent to their private email addresses. It is thought that the group “Ghostwriter” is behind the attacks. They are considered to be linked to GRU, Russia’s military secret service, and are known for their disinformation campaigns. In 2015, the GRU attacked 5,600 computers in the German parliament, including those in Angela Merkel’s parliamentary office.

Unit 74455 from the Russian GRU, codename "Sandworm," was responsible for the attacks in France and South Korea at the very least. It is considered the most dangerous group of hackers in the world, and Vulkan, according to the documents, may provide them with some of the tools they need for their attacks.

Until now, investigators have only been able to retroactively analyze the tracks left behind by such cyberattacks. But now, the Vulkan Files enable a detailed understanding of how such attacks are prepared and organized, and how aggressively Vladimir Putin, with the help of private companies, plans and implements hacking operations around the world. The documents allow a step-by-step look at how such attacks are intended to proceed.

Most of the documents are from an anonymous source. A few days after the Russian invasion of Ukraine, that source made the information available to the German daily *Süddeutsche Zeitung,* later sharing it with DER SPIEGEL as well. "Because of the events in Ukraine, I decided to make this information public,” said the source, who never identified themself and has since receded. "The GRU and FSB are hiding behind this company. People should know about the dangers.”

DER SPIEGEL verified and analyzed the documents with 10 media partners from eight different countries. German public broadcaster ZDF was part of the group, along with the *Guardian*, the *Washington Post*, the Austrian daily *Der Standard*, *Le Monde* in France, Danish public broadcaster DR, the Tamedia Group in Switzerland and the Russian investigative portal IStories. Months of reporting turned up more internal documents from the company in addition to information about money transfers. Both Vulkan and the Kremlin were given several opportunities to comment, but they declined to respond. There are no obvious reasons to doubt the conclusions reached by the investigative team.

The "Vulkan Files"

For years, Russia has been pursuing cyberwarfare. A team of journalists coordinated by DER SPIEGEL and including reporters from the *Guardian*, German broadcaster ZDF, Austrian daily *Der Standard,* the Danish broadcaster DR, the Tamedia Group in Switzerland, the *Washington Post*, the *Süddeutsche Zeitung* and *Le Monde* has analyzed internal documents from the Moscow-based IT company NTC Vulkan. The company works for the Russian military and secret service agencies, providing tools for their virtual attacks.

For the first time, the Vulkan Files provide insight into Vladimir Putin's plans for cyber-warfare.

All Articles (German) ▸

Five Western intelligence agencies also confirmed the authenticity of the documents. Most of those agencies have been keeping an eye on Vulkan for some time because of the work the company does for intelligence agencies. Vulkan appears to be part of the opaque military-industrial complex in which Russian intelligence agencies work closely with more than 40 private IT companies. One of their goals is to develop highly effective cyberweapons that can be used against all those that the Kremlin has identified as Russia's enemies. Especially, of course, in the West.

"Russia is in our networks," warns Wolfgang Wien, deputy head of the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency. Countries ensure that their hackers are well-prepared, he says, so that they can deploy quickly when ordered to do so.

It's a frightening thought, one of many that arises when one dives into the dark world of hackers, agents and saboteurs. Another: Russian cyberwarriors don't just hunker down in their secret bunkers and hidden headquarters somewhere in Moscow. Some have obtained jobs at multinational companies, including some in Germany. DER SPIEGEL has been able to track down former Vulkan employees at SIEMENS and at a BASF service provider, in addition to Trivago and Booking.com. The most concerning trail, however, leads to Dublin, into one of the centers of the European tech industry.

Ranelagh is a prosperous suburb in southern Dublin full of pleasant pubs and trendy restaurants with names like Butcher Grill and Firebyrd. Victorian villas contain foreign embassies, while the smaller brick houses with white window frames are frequently occupied by employees of Google, IBM and Meta – whose headquarters are only a few minutes away.

Sergey N. lives in one of these homes, a 35-year-old who seems younger than his age when he opens the door. Sergey N.'s commute is manageable, with less than a 30-minute drive to Amazon Web Services (AWS), an Amazon subsidiary with $80 billion in annual revenues that is the world's largest provider of cloud computing. Many of the largest companies in the world store their information, and even much of their IT needs, with AWS, including Netflix, Vodafone, NASA, the U.S. Navy and most of the companies listed on Germany's blue-chip stock index DAX, from Allianz to Volkswagen. A huge portion of the global internet runs though AWS servers – as does Ukrainian government information.

Sergey N. is a "senior software development engineer." To get the job, he no doubt had to go through numerous selection rounds. Amazon can take its pick of the best programmers in the world, and Sergey N. has plenty of experience: He held a leadership position at Vulkan as chief developer.

AWS apparently hired him in 2018, long before the invasion – at a time when it seemed completely unproblematic to hire experts from Russian IT companies. Particularly from those like Vulkan that seemed inconspicuous. A company PR film notes that employees of Vulkan can "change the world for the better." It currently employs 135 people.

For the seven years Sergey N. worked there, though, changing the world for the better wasn't apparently a priority. The projects he worked on included a system called "Scan-V," a software program that IT security experts and several Western intelligence agencies believe is "offensive" in nature. In other words, it can be used to attack other countries through the internet.

That is one of the things we hope to discuss with Sergey N. when he opens the door. "We are journalists from DER SPIEGEL and we are working on a story about a company named Vulkan. You worked for that company. Could we ask you a few questions?"

Sergey N. seems taken aback, and the expression on his face is a mixture of fear and confusion. He doesn't want to answer any questions.

"Do you know about the system 'Scan-V?'" His eyes widen in apparent shock. "No, sorry." He then shuts the door.

Reporters around Europe knocking on the doors of dozens of former Vulkan employees had similar experiences. Most of them didn't want to talk about their former employer. It remains unclear whether that reticence is due to fear of reprisals or out of concern that their cover could be blown.

The example of Sergey N. raises a number of disturbing questions. What is a Russian cyberwar specialist doing in a company that takes care of the IT needs of hundreds of leading companies, the infrastructure of which is one of the pillars of the global internet? Did AWS not know what Sergey N. had worked on in Russia? Or did it not want to know? One leaked document from June 2019 includes comments signed in his name – at a time when he says he was already working for AWS. When approached for comment, the U.S. based company said only that the security of its customers' data is its highest priority.

Siemens, where DER SPIEGEL also located a former Vulkan employee, provided a similar response, saying merely that the company takes the issue seriously, but was unable to provide information about specific employees for reasons of data protection. The integrity of job applicants, the company added, is investigated to the degree permitted by law. IBM commented that its business ties with Vulkan came to an end in 2020.

Companies seem improvident in the face of the extremely competitive marketplace for well-trained programmers. Numerous Vulkan employees are graduates of Bauman University in Moscow. The university has close ties to the Russian security apparatus and carries out "special studies" for the Russian Defense Ministry and the intelligence agency FSB.

Bauman University in Moscow has close ties to the Russian security apparatus.

Foto:

Grigory Dukor / REUTERS

At least one of the founders of Vulkan, Alexander Alexandrovich Irzhavsky, also has such connections and is a regular guest at conferences held by the Defense Ministry. When he was once stopped for a traffic violation, the address he provided belonged to an institute that is closely linked to GRU, the military intelligence agency. In 2010, Irzhavsky founded Vulkan together with Anton Vladimirovich Markov. Both of them are middle-aged and inconspicuous.

Company founder Alexander Irzhavsky: "I was always a bit afraid of them."

Foto:

NTC Vulkan

Company founder Anton Markov

Foto:

NTC Vulkan

It is nevertheless possible to discover what they and their company have been working on over the past decade, including a system that bears the codename "Amezit." The goal of the system is to gain control of flows of information in specific regions, according to one description in a document bearing the heading: "Software Purpose." In numerous other documents, including hundreds of pages of blueprints, diagrams and tables, a platform is described that would cover virtually all aspects of modern-day cyberwarfare, ranging from censorship and the manipulation of social media content to attacks on critical infrastructure. Trails in the material lead to server farms in the U.S. and to a nuclear power plant in Switzerland.

"These documents suggest that Russia sees attacks on civilian critical infrastructure and social media manipulation as one-and-the-same mission, which is essentially an attack on the enemy's will to fight," says John Hultquist, a leading expert on Russian cyberwarfare and vice president of intelligence analysis at Mandiant, an IT security company.

Numerous elements of the program indicate that Amezit could be deployed during the takeover of occupied areas in order to quickly gain control over communication – areas such as the Crimean Peninsula or the Donbas region of Ukraine. The timing of its development is likewise concurrent with efforts by the Kremlin to build up a national internet sealed off from the rest of the world.

It isn't possible to definitively say for whom or what such a system was developed, but there are clues. These include an email written by project director Maxim Andreyevich D. to several Vulkan employees bearing the date June 22, 2018, and the subject line: "Business trip to Rostov." He was heading to the Research Institute of Radio Communication run by the FSB, which is perhaps the most powerful secret service in Russia and employees an estimated 350,000 people.

Putin himself was head of the FSB at the end of the 1990s. Today, the agency is his most important tool for suppressing the opposition in Russia. As DER SPIEGEL and the investigative platform Bellingcat discovered, it was an FSB commando that apparently attempted to murder opposition leader Alexey Navalny in Siberia in summer 2020. FSB agents covertly smeared the nerve agent Novichok on his underwear.

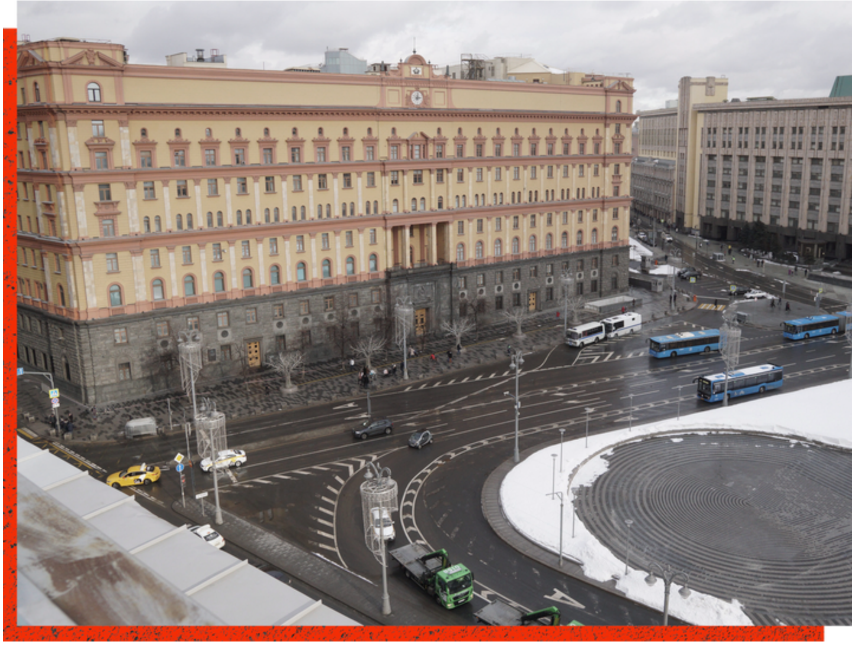
The cyber-capabilities of the FSB are also prodigious. Several years ago, hackers from the agency forced their way into the computer system of the German Foreign Ministry in Berlin. They slowly progressed through the system until they ended up at the department responsible for Russia and Eastern Europe, which was apparently the primary target. Western security experts dubbed the group behind the attack "Snake."

Another FSB hacker unit, known as "Berserk Bear" by experts, spent years covertly inserting malware into the computer systems of nuclear power plants, oil and natural gas companies and other energy corporations in 135 countries around the world, including the U.S. and Germany.

Despite having special cyberwar departments of their own, it isn't unusual for secret services to work together with private companies. The whistleblower Edward Snowden, for example, didn't work directly for the National Security Agency (NSA). He was an employee of a private partner company called Booz Allen Hamilton. There are several similar examples from India and China. Just like in the business world, it is sometimes quicker and more efficient to outsource jobs to specialized service providers. Such as Vulkan.

As such, it would seem that the Vulkan team's business trip to the FSB site in Rostov-on-Don was part of a typical business relationship. In his email, Vulkan executive Maxim Andreyevich D. asked his team to quickly prepare a presentation "of our software platform for the military representative in Rostov." The demonstration of "Amezit" and several of its sub-systems was to take place over the course of several days. According to the emails, the present-day Amazon employee Sergey N. was also to join the trip to present four "Amezit" sub-systems. For that purpose, it was made clear in the email traffic, the necessary equipment ("three servers, five mounts, switchboard") was to be sent ahead to the FSB institute as quickly as possible.

The leaked documents provide no indication as to whether the trip to Rostov-on-Don was successful or whether the FSB is currently using "Amezit." But there were plenty of other opportunities for the Vulkan engineers to present their cyberweapons. Teams of developers regularly made the trip to FSB headquarters on Lubyanka Square in Moscow, just four stops away from Vulkan on the subway. The square is flanked by the gigantic, ominous building which today houses the FSB – and where Stalin's KGB used to torture and murder those designated as enemies of communism. It is just a few hundred meters from here to the Kremlin.



FSB headquarters on Lubyanka Square in Moscow

Foto:

Mikhail Svetlov / Getty Images

The Vulkan employees generally entered the FSB through an inconspicuous building next door, according to a meeting participant. That building is home to the offices of the FSB's Information Security Center, one of the secret service's most important hacker departments. The Vulkan staffers would carry their laptops through a long entryway, passing through several sets of security doors, before their papers were controlled. They would then be received by FSB agents. Together, they would head to the upper floors, where Vulkan's people would spend hours presenting their products and answering questions, interrupted only by a lunch break with their hosts in the cafeteria of the Lubyanka complex.

Not all of the Vulkan staffers enjoyed making such visits, because the secret service agents of the FSB would often send them on their way with technically unrealistic requests.

The Kremlin's cyber-plans envision not just the rapid development of all manner of offensive cyberweapons, but also the training of Russian IT experts in their use. And Vulkan is apparently deeply involved in that effort as well: The company has developed its own training program for the state-sponsored hackers of tomorrow. One leaked document about the secret program, which bears the codename "Crystal-2V," states that its goal is the "comprehensive training of specialists" in "information confrontation" – the term that Russian secret service agencies use to describe cyberwarfare.

According to the document, up to 30 IT experts were to be trained on using "Crystal-2V" to execute attacks on critical infrastructure. This includes "knocking out the control systems of rail, air and shipping transport" and other "vital" areas such as electricity and water supply. The program is also designed to train them in blocking access to the global public information system – an apparent reference to the internet. Such attacks on vital supply and transportation arteries and industrial control systems have for years been among the scenarios most feared by Western intelligence agencies.

And such attacks have long since become reality. In 2017, an attack on a Saudi Arabian oil refinery was discovered. Russian attackers attempted to manipulate the facility's security mechanisms. One year ago, U.S. justice officials indicted GRU agent Evgeny Gladkikh for the incident. Officially, the suspected hacker had been working for a scientific research institution, which also provides financing to Vulkan.

Such attacks are described in detail in the training program developed by Vulkan. The focus is on "unauthorized access" to critical networks and the "detection of points of weakness" in the targeted system. An additional lesson module teaches denial-of-service attacks as a way of blocking access to web-based services. Recruits are to learn all those skills from both theory-based instruction and practical laboratory simulations.

But Vulkan isn't just training the next generation of cyberwarriors, it is also seeking to arm them with new tools – which is why Vulkan programmers came up with "Scan-V." The system is aimed at making cyberattacks far easier to plan, cutting down on the weeks and months it often takes to prepare such assaults. Targets must first be comprehensively investigated: How is the IT system structured? What operating systems have been installed and where are their weaknesses to be found?

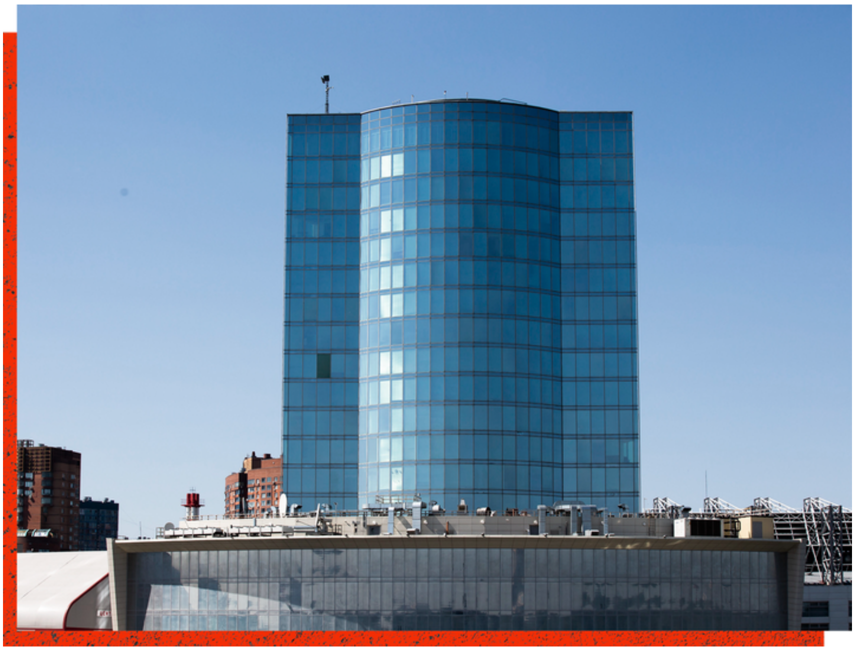
According to the leaked documents, "Scan-V" is intended to automate these steps. The information gathered is then analyzed and proposals are made for how an attack might be structured.

It "reminds me of old military movies," says Gabby Roncone, from the IT security firm Mandiant, "where people stand around … and place their artillery and troops on the map." They then try to "understand where they need to strike first to break through the enemy lines."

Experts have classified "Scan-V" as an offensive weapon, primarily developed for hacker units that frequently launch large-scale attacks. And which want to become even more powerful.

In May 2020, a Vulkan team was planning a visit to one of the company's most important clients. The destination was Khimki, an industrial city just outside of Moscow. "Please provide your passport details" ahead of time, wrote the "Scan-V" project head Oleg N. on May 27 in an email to his team. The site they would be visiting had extremely tight security and access was strictly controlled. The meeting may well have been scheduled to be held in a 20-floor, glass high-rise on the banks of the Moskva River. Western security officials know it well.

It even appeared in an indictment from 2018 that caused a stir around the world. The indictment stemmed from the investigation by Special Counsel Robert Mueller into Russian influence on the 2016 presidential election in the U.S. In the document, the high-rise in Khimki is referred to as "The Tower." The unit from the military intelligence agency GRU, which is based here, is thought to have participated in the surveillance of Hillary Clinton's campaign team in an effort to get Donald Trump elected. Officially, the military hackers are identified by their military postal service number: 74455. But they are better known under their codename: "Sandworm." They are the most notorious cyberwarriors in the world.



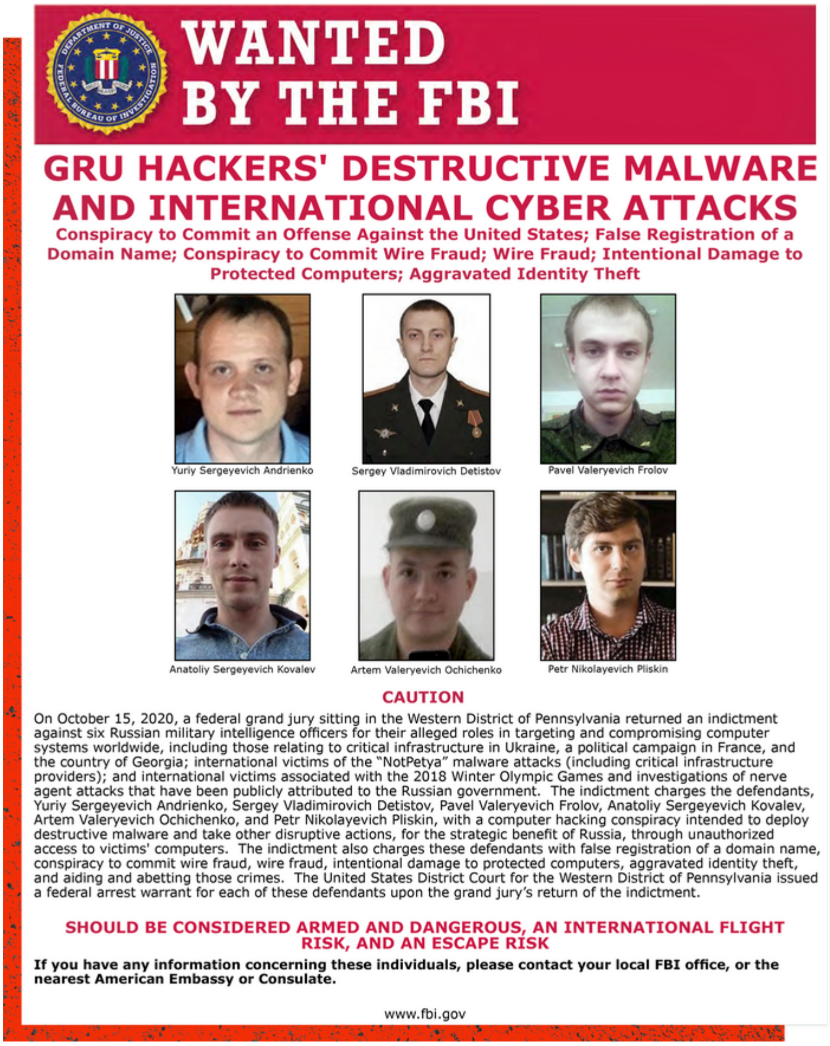
"The Tower": The GRU unit known as 74455 is thought to operate out of this high-rise.

Foto: Alexander Zemlianichenko / AP / picture alliance

Many of the most spectacular hacks and cyberattacks performed in recent years are thought to have been perpetrated by the hackers operating behind the glass façade of The Tower. The man considered to be the unit's new commander, Evgenii Serebriakov, doesn't appear particularly dangerous in his passport photo, but a few years ago, he and three others were discovered attempting to attack the Organization for the Prohibition of Chemical Weapons in The Hague. The Dutch discovered them in the act, confiscated their laptops and mobile phones, and threw them out of the country.

The embarrassing incident doesn't seem to have hurt Serebriakov's career, a fact that doesn't come as a surprise to high-ranking officials who have spent extensive time observing the Russian secret services. Demonstrations of strength and courage are often more important in Moscow than operational success. Russia intentionally crosses boundaries in order to strike fear in the hearts of its adversaries, says one intelligence official, adding that Russian hackers are frequently careless when they go on the attack. "Maybe the attack wasn't particularly sophisticated and didn't achieve its goal. But that almost doesn't matter. The message is: We don't just issue threats, we also take action."

That is particularly true of the GRU, the most ferocious of all the Russian secret services. Some 37,000 people work there, including 25,000 elite soldiers from Spetsnaz. Western intelligence services believe that the agency also employs several thousand hackers. One espionage expert describes the GRU's approach as "impact over cover." GRU's arsenal of "active measures" includes sabotage and subversion, disinformation and assassination. The goal: unleashing chaos and damaging Western democracies.



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the "NotPetya" malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aiding and abetting those crimes. The United States District Court for the Western District of Pennsylvania issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

$10 million reward: The FBI in the U.S. used wanted posters in the search for the "Sandworm" hackers.

Foto:

FBI

The attacks perpetrated against Ukrainian targets by "Sandworm" – which have been going on for around the last 10 years, are particularly spectacular and unrelenting. Just before Christmas in both 2015 and 2016, Russian hackers managed to successfully attack Ukraine's power supply, resulting in the first blackouts ever triggered by cyberattacks. A clear demonstration of power.

A few months later, Moscow launched an attack considered to be the most consequential hack ever performed. The perpetrators used a popular Ukrainian tax software to disseminate a malware program called "NotPetya." It spread rapidly, encrypting infected computers and making them unusable. Because multinational companies were infected, the effects of the attack quickly spread beyond the borders of Ukraine – and soon, around the world. Companies like the logistics giant Maersk and the cosmetics multi-national Beiersdorf were forced to completely rework their IT systems. The attacks caused an estimated $10 billion in damages.

The Russians are currently going after Ukrainian companies with "Wiper" attacks, destructive malware programs that seek to make infected computers unusable. In a recent analysis, Microsoft has identified nine different "Wiper" families that have been used to attack more than 100 Ukrainian companies and government agencies since the invasion. As part of an operation against the national news agency Ukrinform that was uncovered in January, "Sandworm" deployed five of these programs at once.

At the beginning of the invasion of Ukraine, cyberattacks were conducted in concert with conventional attacks. Russia would launch rockets or missiles at targets that had previously been the subject of cyberattacks.

Kyiv, Feb. 28, 2022

Just a few days after the Russian invasion, hackers infiltrate a Kyiv media company, according to Microsoft. The next day, the television tower is attacked from the air.

Attack on the television tower of Kyiv on March 1, 2022. Source: Twitter / Rob Lee

Zaporizhzhia, March 2, 2022

A Russian group hacks deep into the network of a Ukrainian nuclear power plant operator. One day later, Putin's troops attack Ukraine's largest nuclear power plant, located in Zaporizhzhia. They take control of it on March 4.

Fighting at the gate of the nuclear power plant in Zaporizhzhia on March 3, 2022. Source: Twitter / BeMilInterest

Dnipro, March 11, 2022

A government agency in Dnipro is attacked by malware. The same day, the city is attacked from the air.

A rocket detonates in Dnipro on March 11, 2022. Source: Twitter / m_osint

Lviv, April 18, 2022

Several cruise missiles detonate in the city. One day later, a local logistics company is attacked by malware. On April 29, the hackers again launch an attack, this time targeting networks used by logistics companies in Lviv. A few days later, an electrical substation belonging to the rail company is attacked from the air. According to Microsoft, the cyberattacks were performed by the group "Sandworm."

Russian air attacks on Lviv on April 18, 2022. Source: Twitter / nexta_tv

According to numerous IT security experts and Western intelligence agents that DER SPIEGEL spoke to, "Scan-V" would be a useful tool that could be used to prepare such attacks. It is unclear, however, whether the GRU has in fact deployed or purchased "Scan-V."

It does seem to be clear, however, that the GRU closely followed the development of this tool. An 11-page document, full of jargon about processing systems and data analysis, provides clear evidence of that interest. The coversheet identifies it as a protocol for "Scan-V," focusing on "data exchange between the sub-systems PU-L, PSAP, Scan-AS." In the upper left corner is the notification: "Authorized representative of military unit 74455." The "Sandworm" unit.

The tools were successively refined by Vulkan over the course of several years. And 10 years ago, one of the company's employees was involved in a global attack launched by one of the best Russian hacker groups – a finding from an analysis performed by Google, which DER SPIEGEL is now making public for the first time.

The attack, which researchers christened "MiniDuke," targeted official state computers in countries like Germany, the U.S. and Ukraine. The goal: stealing secret information from agency networks. The computers of at least three Western government representatives were successfully infiltrated and more than 100 servers around the world were infected, according to IT security experts. Behind the attacks was a group called "The Dukes," also known as "Cozy Bear" – linked to the Russian foreign intelligence agency SVR. Later, the hackers went after the Pentagon.

In late 2012, Google identified an email address that was later linked to "MiniDuke." "We observed that gmail address send an apparent test message to an email address with the ntc-vulkan.ru domain," the company said in a statement.

Such test emails are frequently used to determine if Google filters recognize their viruses or hacking tools. The tests were apparently successful, because later, the hackers used that same email address to send out the malware that circled the world as "MiniDuke.” Diplomats, government officials, members of the military and others in numerous Western countries received customized emails from Moscow with attachments bearing titles like "Ukraine’s NATO Membership Action Plan (MAP) Debates” or an incredibly realistic-looking invitation to an "Asia-Europe Meeting (ASEM) Seminar on Human Rights.” As soon as the documents were open, the computer was infected.

Cryptic posts began appearing on Twitter in parallel from anonymous accounts - things like "Albert my cousin. He is working hard,” followed by a seemingly random list of characters. For Twitter users, it looked like nonsense, but for infected computers, those posts contained orders to covertly download the next tier of the malware program. Experts would later refer to the system as "extremely effective.”

But Google was able to draw a line from "MiniDuke” to Vulkan due to a mistake made by the hackers: They used the same IP address to rent a control server that they had also used when registering the Google account that was used to send the malware. "Definitely a slip-up,” says an IT security expert from Google. The discovery led Google to block the email account, but the global hacking campaign could no longer be stopped.

Early coups such as that one likely contributed to Vulkan receiving funding over several subsequent years to further develop its capabilities. The company was paid numerous installments adding up to several million euros from institutes closely linked to Russian secret service agencies and the military. In over 17,000 money transfers of Vulkan for which the international reporting team has documentation, the system names "Scan-V,” "Amezit” and "Crystal-2V” are regularly noted as the reason for payment.

It also appears that the Russian hackers are urgently searching for ways to further boost the efficiency of their massive cyberattacks. Ukraine is currently being bombarded by such attacks on an almost daily basis. They frequently resemble an onslaught from March 28, 2022.

That morning, Kyrylo Hontsharuk was awakened by the ringing of his mobile phone. It was his 40th birthday. The caller, though, was not a well-wisher, but a distraught employee of his company. Hontsharuk is the chief information officer (CIO) of the Ukrainian internet service provider Ukrtelecom. He had been expecting a hacker attack since the beginning of the war, and now it was here. The attackers had managed to infiltrate the account of a Ukrtelecom employee. From there, they found their way into the company’s internal systems and obtained administrative rights, thus giving them the ability to change programming code. Hontsharuk immediately realized that if the hackers progressed any further, they would have access to specific users.

Hontsharuk figured he only had one choice: He had to take the servers offline to prevent lasting damage. But doing so would cut off hundreds of thousands of Ukrainians from the internet. And many of them were trapped in bunkers, with the internet as their only source of information about where and how the Russian military was advancing, and whether their families were still safe.

Hontsharuk’s team worked through the night to remove the Russian saboteurs from the system. "Such an attack must never be allowed to happen again,” says Hontsharuk. "But there is no such thing as 100 percent protection.”

The Russian cyber-soldiers, though, aren’t just targeting their presumed enemies abroad. Increasingly, they are turning their weapons inward. Under Putin, Russia has long since become an intelligence state, and his confidants from the shady world of espionage, the "siloviki,” have become the new nobility. The importance of this bubble for Putin, say high-ranking Western security officials, is almost impossible to overstate.

He is relying on his old connections to solidify his power. The West doesn’t trust Putin, says a Western intelligence official, but his own people likely trust him even less. Which is why Putin’s intelligence services have been tasked with gathering and saving as much information as possible, whether or not it is of immediate use.

Vulkan helps with that effort as well. At the behest of the FSB, the company’s software engineers developed surveillance software to control the Russian population – codename: "Fraction.” The goal is the automated surveillance of online activities. "A system,” as it is described in the documents, "to monitor and identify activities in social networks.” A web-based "Big Brother” designed to scan social media posts for suspicious content and then save that content. It is a way to filter out those who are critical of Putin.

Not all Vulkan employees are pleased about developing instruments for the suppression of their fellow Russians. For some, it crosses the line. When he learned about the cooperation among intelligence services in this area, says Yevgeny, it became clear to him "that I didn’t want to support the regime.” Yevgeny is not his real name. He worked for Vulkan for several years, but now lives in the West. His precise location and the projects he worked on cannot be revealed so as not to put him in danger.

Yevgeny is one of the more the 90 current and former Vulkan employees who were contacted during the reporting on this project. He is a quiet IT nerd, a far cry from the militaristic bombast he says the two company founders exude. "I was always a bit afraid of them," he says. The work itself, though, was "fun," with an atmosphere similar to that of a startup. And his salary was above average.

The Vulkan open-space offices may have all the charm of an insurance agency, with the brown carpeting and yellow walls. But the mood was quite relaxed, says Yevgeny, and people were friendly with each other. After one party, he says, co-workers grabbed the unfinished bottles of schnapps to continue drinking together, and they would also go fishing together on company outings. One time, they drove tanks across a military exercise ground. He says that some in the company derisively refer to Putin as "grandpa in the bunker," and they even talked about the invasion of the Crimea inside the company, with some at Vulkan voicing their opposition.

The full palette of the projects that Vulkan was working on only slowly became clear to Yevgeny. It was knowledge that he wasn't supposed to obtain, with the employees sworn to secrecy, even within the company, about the projects they were working on. The increasingly brutal methods employed by the Russian regime ultimately transformed Yevgeny into an opponent of the Kremlin and a follower of opposition leader Alexei Navalny. "The total surveillance of activists cannot be a feature of a modern country," he says.

Yevgeny has now managed to build a life for himself in a Western country and says he never wants to return to his homeland. "This regime is a police state and one of the pillars of this state is made up of companies like Vulkan."

His former co-workers continue on their mission. The Russian cyberwar machine needs an uninterrupted supply of soldiers and weapons. For "Sandworm" and "Cozy Bear," for Vulkan and all the others, a golden age has apparently dawned.

Because for Putin and his military, the internet is not the battlefield of the future, but of the present.