Putin’s hackers gained full access to Hungary’s foreign ministry networks, the Orbán government has been unable to stop them

direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/

Panyi Szabolcs

March 29, 2022

On December 30, 2021, in Moscow, Russian Foreign Minister Sergey Lavrov pinned the Order of Friendship on the suit of his Hungarian counterpart Péter Szijjártó. Although the medal was presented by Lavrov, it was Russian President Vladimir Putin himself who decided to award it. Not coincidentally, the medal, which is in the form of a wreath of olive branches encircling a globe, includes the inscription “Peace and Friendship” in Cyrillic on the back, is the highest Russian state decoration that can be awarded to a foreigner.

> “I am proud that, despite the extremely unfavourable global and regional developments of recent years, while respecting our obligations to our alliances, we have also been able to maintain our cooperation with Moscow based on mutual trust and in line with our national interests”, the Hungarian Foreign Minister boasted on his Facebook page.

Péter Szijjártó knew long ago that Russia’s intelligence services had attacked and hacked into the IT systems of the Ministry of Foreign Affairs and Trade (MFA), which he headed. By the second half of 2021, it had become clear that the Russians had completely compromised the foreign ministry’s computer network and internal correspondence. Furthermore, they had also hacked into the encrypted network used to transmit “restricted” and “confidential” state secrets and diplomatic information, which can only be used under strict security measures.

According to an internal document we obtained, the foreign ministry was still under targeted attacks in January 2022. Details of the Russian hacking of the foreign ministry’s communications channels were shared with us by former state officials, among others, who learned of the incident from officials with direct knowledge of it.

According to former intelligence officials, the cyber attack trail suggests that hacker groups working for Russian intelligence are clearly behind the operations against Hungary’s foreign ministry. These hackers work for the Federal Security Service, FSB, which was previously headed by Putin, and for the Russian military intelligence service, the GRU. According to our sources, these hacker groups have been well known to the Hungarian state authorities for a long time, as they have been continuously attacking Hungarian government networks for at least a decade. Russian attacks against Hungary are most often related to hacks against other NATO countries, and members of the Western alliance regularly cooperate and share information to identify these offensive cyber operations.

Hungarian diplomacy has become practically an open book for Moscow through the hacking of the ministry’s networks. Russians are able to know in advance what the Hungarian foreign ministry is thinking and planning, and this is happening at a very sensitive time. Russian infiltration remained active before and partly after the invasion of Ukraine, during the current EU and NATO crisis summits. Meanwhile, there is no sign that the Hungarian government has publicly protested to Russia about the cyberespionage.

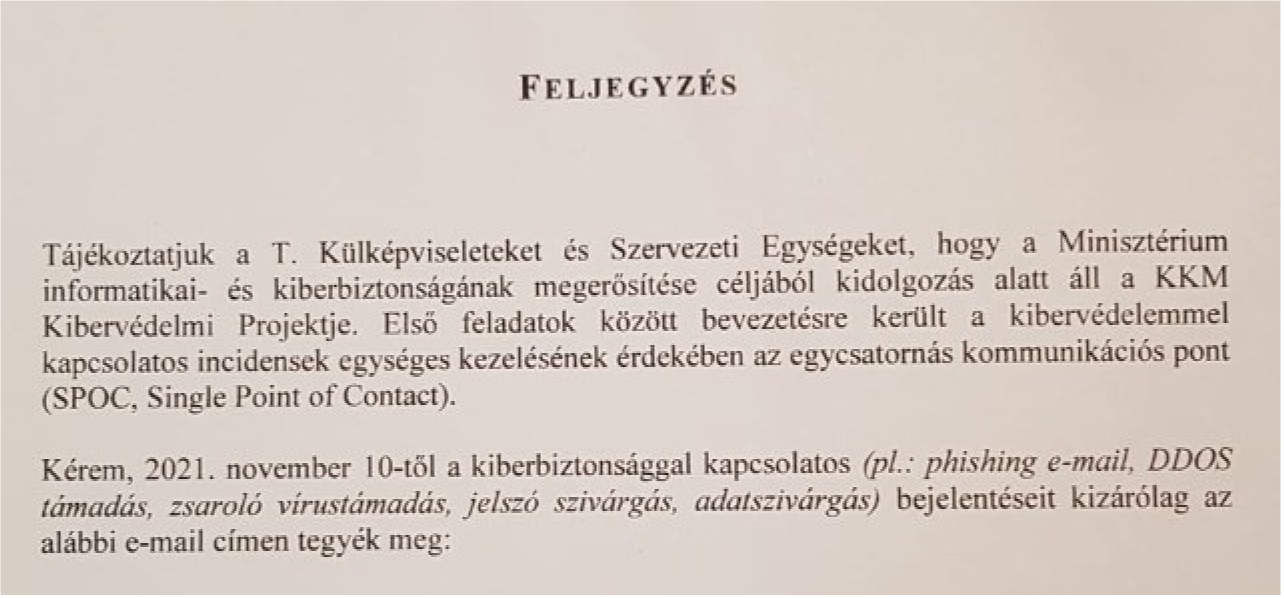
Direkt36 uncovered the Russian intelligence operations against the Hungarian foreign ministry and the inadequacy of Hungarian counter-intelligence measures, going back at least a decade, with the help of foreign ministry documents and more than thirty background interviews. For example, we spoke to former Hungarian intelligence and security officers who had worked on Russian intelligence-related fields and had concrete information on many of the cases described in this article. Sources familiar with the internal affairs of the Ministry of Foreign Affairs and Trade shared information about the ministry’s handling of the cyberattack.

We sent detailed questions about all the main findings in the article to the foreign ministry, the Ministry of Interior – which is primarily responsible for cyber defence and counter-intelligence – and the Prime Minister’s Office last week. We have not yet received any response. *(After the publication of this article, the foreign ministry replied to other media outlets saying “we do not pay attention to campaign lies”.)*

Foreign ministry staff were not told that their computers were already infected

Since autumn 2021, unusual messages have appeared on internal mailing lists at the Ministry of Foreign Affairs and Trade. While ministry staff had previously received such cybersecurity-related emails only occasionally, from last year they kept frequently coming.

According to a foreign ministry diplomatic cable obtained by Direkt36, it was announced on November 11, 2021 that “the Ministry’s Cyber Security Project is being developed to strengthen the MFA’s IT and cyber security”. As a first step, an email address has been created to which foreign ministry officials are invited to “report cybersecurity-related issues (e.g. phishing email, DDOS attack, ransomware virus attack, password leak, data leak)”.



FELJEGYZÉS

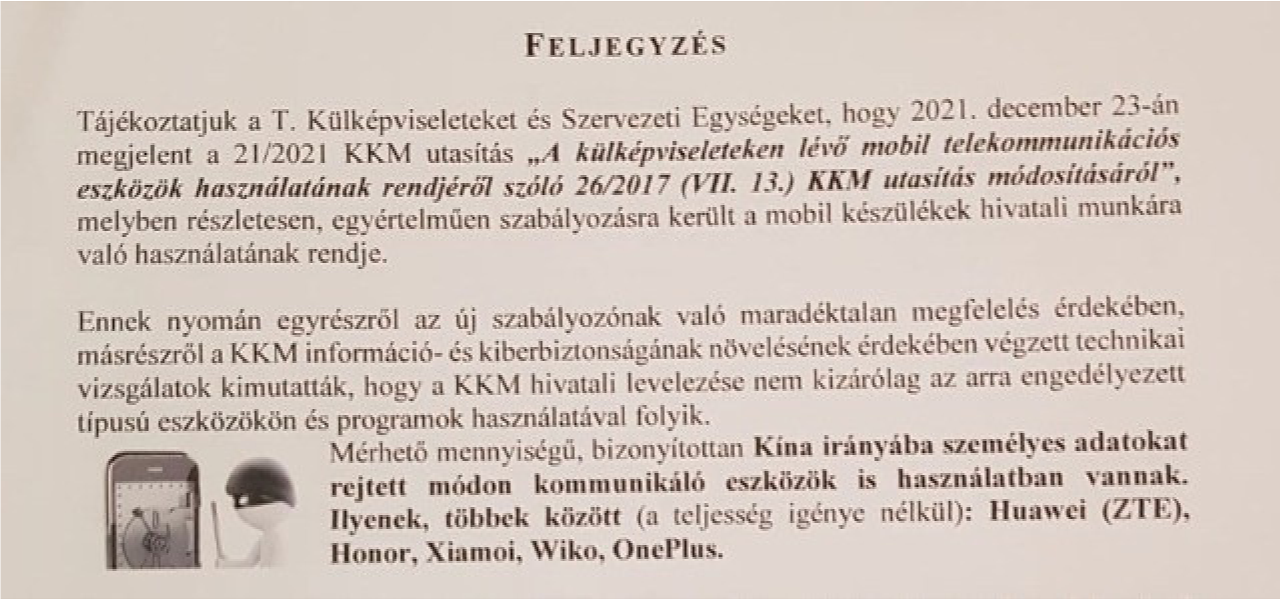
Tájékoztatjuk a T. Külképviseleteket és Szervezeti Egységeket, hogy a Minisztérium informatikai- és kiberbiztonságának megerősítése céljából kidolgozás alatt áll a KKM Kibervédelmi Projektje. Első feladatok között bevezetésre került a kibervédelemmel kapcsolatos incidensek egységes kezelésének érdekében az egycsatornás kommunikációs pont (SPOC, Single Point of Contact).

Kérem, 2021. november 10-től a kiberbiztonsággal kapcsolatos *(pl.: phishing e-mail, DDOS támadás, zsaroló vírustámadás, jelszó szivárgás, adatszivárgás)* bejelentéseit kizárólag az alábbi e-mail címen tegyék meg:

Source: Direkt36

Before Christmas, the ministry had already issued instructions to Hungarian diplomatic missions restricting the use of mobile phones for official work. Then, on January 7, 2022, the cyber security project officer scolded staff for not complying with the new policy. “Technical investigations carried out to increase the information and cyber security of the MFA have shown that the MFA’s official correspondence is not carried out exclusively using the types of devices and programs authorised for this purpose,” another internal cable obtained by Direkt36 stated.

The cables have led to growing suspicions in the MFA that the problem could be quite serious. One source familiar with the ministry’s internal affairs thought at the time that the Chinese might have hacked the foreign ministry’s system. One of the ministry’s cables hints at this: “Measurable amounts of devices are in use that have been proven to communicate personal data to China in a covert manner. These include (but are not limited to) Huawei (ZTE), Honor, Xiaomi, Wiko, OnePlus, among others”.



Feljegyzés

Tájékoztatjuk a T. Külképviseleteket és Szervezeti Egységeket, hogy 2021. december 23-án megjelent a 21/2021 KKM utasítás ***„A külképviseleteken lévő mobil telekommunikációs eszközök használatának rendjéről szóló 26/2017 (VII. 13.) KKM utasítás módosításáról”***, melyben részletesen, egyértelműen szabályozásra került a mobil készülékek hivatali munkára való használatának rendje.

Ennek nyomán egyrészről az új szabályozónak való maradéktalan megfelelés érdekében, másrészről a KKM információ- és kiberbiztonságának növelésének érdekében végzett technikai vizsgálatok kimutatták, hogy a KKM hivatali levelezése nem kizárólag az arra engedélyezett típusú eszközökön és programok használatával folyik.

Mérhető mennyiségű, bizonyítottan **Kína irányába személyes adatokat rejtett módon kommunikáló eszközök is használatban vannak. Ilyenek, többek között** (a teljesség igénye nélkül): **Huawei (ZTE), Honor, Xiamoi, Wiko, OnePlus.**

Forrás: Direkt36

This cable is not only remarkable because it highlights serious vulnerabilities of government communication. The letter is also interesting because it shows that the Orbán government is aware of the security risk posed by Chinese devices, while in public they denied it for years. Moreover, the Orbán government has been one of the biggest supporters of the use of Chinese telecommunications devices in Europe. Szijjártó, for example, has repeatedly stood up for Huawei and claimed that the Chinese company's devices do not pose any risk.

Other vulnerabilities are also reported in the MFA cables. According to one, an internal investigation has also revealed that many bureaucrats prefer to use an American email client called BlueMail, which is also dangerous. According to the cyber defence project officer, BlueMail "openly stores entered passwords; has many programming flaws that can be easily exploited in an attack; constantly sends mobile device data to three different servers".

Just a week after the letter warning against Chinese devices, on 14 January 2022, the MFA issued a broad warning about a different kind of threat, saying that a phishing email attack "appeared in several foreign embassies this week". The phishing email, written in English, claimed that the recipient's password for their @mfa.gov.hu ministry email account was about to expire and needed to be changed. "Passwords entered will be automatically assigned to the attacker's email address, which will be immediately forwarded to unauthorised users who can easily gain access to the full contents of the inbox," the warning said.

However, the MFA's Cyber Security Project was not launched solely to raise awareness, and internal investigations have not only revealed potential risks. By the second half of 2021, it had also become apparent to the ministry's leadership that Russian hackers were behind the active, serious infection of ministry systems, several former Hungarian state officials told Direkt36. They had details from colleagues with direct knowledge of the Russian operation or who had previously worked in fields related to Russian intelligence.

Based on the hackers' known methods from previous cyber attacks in Hungary and abroad, the infection technique and other clues they left behind (IP addresses, origin and destination of network traffic, targets), it was clear from the beginning to the agencies involved in investigating the attack on the Hungarian MFA that Russian intelligence services had attacked the ministry. For example, some of the leads were specifically linked to, or bore an uncanny resemblance to known attacks against other NATO countries which had already been identified as being carried out by Russia.

The infection entered the Hungarian MFA partly through phishing attacks and email attachments containing malwares and viruses, and then spread throughout the internal network – computers of the ministry at Bem Square in Budapest and in more than 150 sites of more than 90 Hungarian foreign missions were all affected. According to the former officials, the infection had been lurking for years and was discovered so late that it is impossible to say in retrospect at what points and in how many different ways the Russians had hacked into the MFA's systems.

According to sources familiar with the internal affairs of the ministry, agencies responsible for the security of the networks informed Péter Szijjártó and the top leadership of the MFA at least six months ago. Since then, Minister of Interior Sándor Pintér and his ministry's heads have also been filled in on the details by the security agencies they oversee. At the MFA, cybersecurity is the responsibility of the ministry's Security, Information Technology and Telecommunications Department (BITÁF) and its civil intelligence agency, the Information Office (IH). At the level of overall government, the agency in charge is the Special Service for National Security (SSNS). However, according to several former intelligence officers, the National Infocommunication Service Provider Ltd. (NISZ), as well as the counterintelligence agency, the Constitution Protection Office (AH) are also involved in mitigating the incident.

Szijjártó told the Hungarian parliament's committee on national security in early December last year that the IH – which is also responsible for the national security protection of Hungarian embassies abroad – had drawn up a new concept to strengthen protection, and "work on this has started this year as planned". He added that in the IH, too, "we have taken more measures to strengthen internal security." However, he did not say that this had anything to do with cyber attacks.

At the same committee meeting, Pintér also had a note of concern. After saying that the Hungarian cyber defence is "entirely" the responsibility of the SSNS, which he oversees, he added that "regardless of this, each specific agency must implement its cyber defence tasks, because it is not enough to have a central vision if our individual staff members do not pay enough attention to computer and internet use".

Even though Szijjártó and his deputies have been aware of the risks for some time, they have not disclosed it to the foreign service apparatus beyond general warnings in diplomatic cables mentioning that their everyday working devices and foreign ministry networks have been compromised for some time. In addition, the process of expelling the Russian intelligence services from the Hungarian foreign ministry networks has been extremely slow and has not been completed to date. According to former security officials, this is due to, among other things, fragmented and slow decision-making and a lack of expertise.

Yet Russian cyber attacks against the Hungarian government and the Hungarian MFA have been occuring for at least a decade.

Russians kept logging in and out of the system

Russian hackers saw everything on the computer of the high-ranking Hungarian government official as if they were physically sitting in his chair in front of his monitor in Hungary. In the autumn of 2012, a modified version of a remote access application called TeamViewer was installed on his computer without his knowledge, allowing them to see virtually everything – documents, passwords, system settings, network connections.

He was not the only Hungarian government victim of the Russian cyber attack almost a decade ago, and the targets were not only Hungarians. A few months later, in February 2013, the embassy of a NATO and EU member state in Moscow was also a victim of the attack, later dubbed TeamSpy, as were research and educational institutions in France and Belgium, among others. The details of the attack were later published in an anonymised way in an expert analysis.

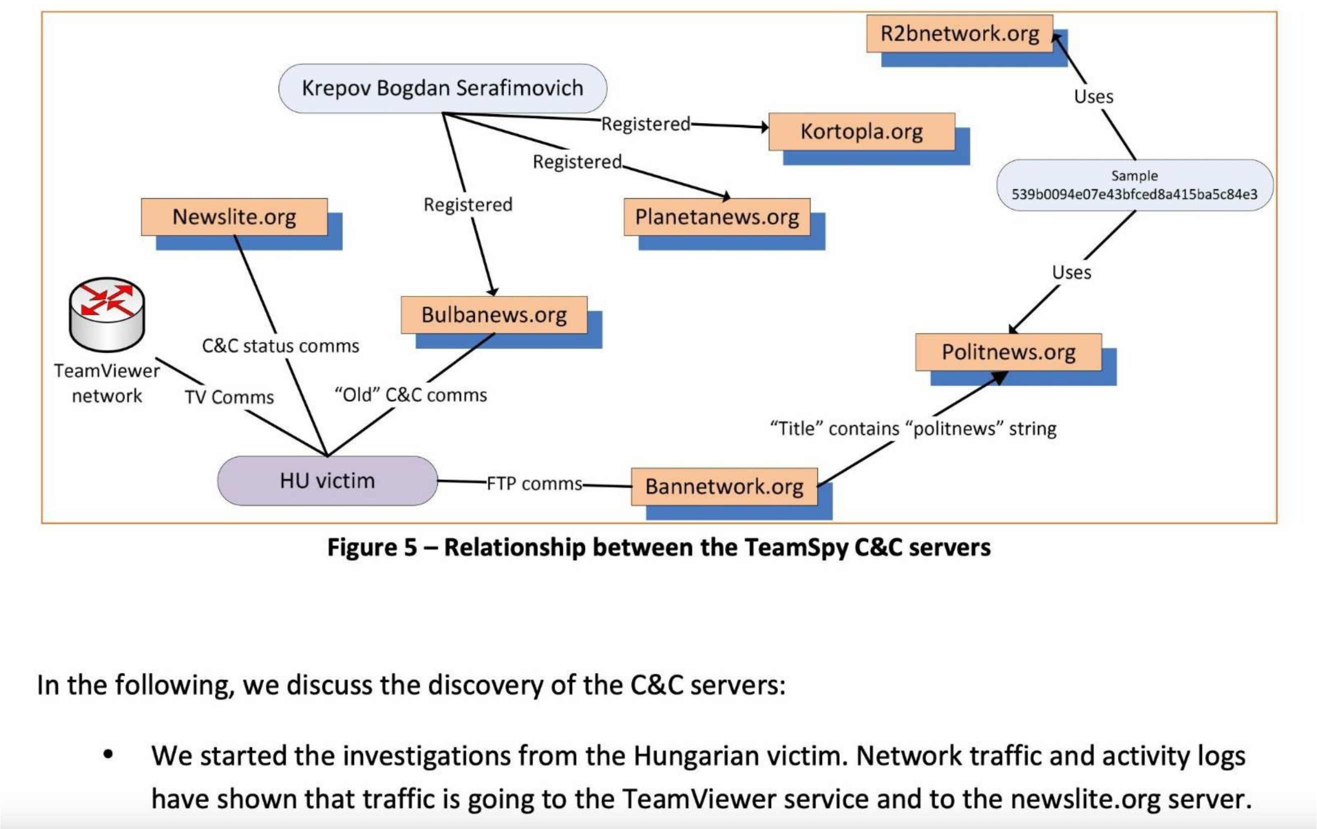


Figure 5 – Relationship between the TeamSpy C&C servers

In the following, we discuss the discovery of the C&C servers:

- We started the investigations from the Hungarian victim. Network traffic and activity logs have shown that traffic is going to the TeamViewer service and to the newslite.org server.

Source: Crysys Lab

The large-scale Russian TeamSpy attack was discovered not by the counterintelligence of Western countries, but by experts at the cyber defence center of the Hungarian National Security Authority (NBF), according to a cyber security expert familiar with the incident. The Hungarian center, called the Cyber Defence Management Authority (CMDA), set up in 2011, gathered expertise and cyber defence capabilities over ministries and state agencies, and were so successful that one of their Hungarian experts was elected to head NATO's cyber defence task force.

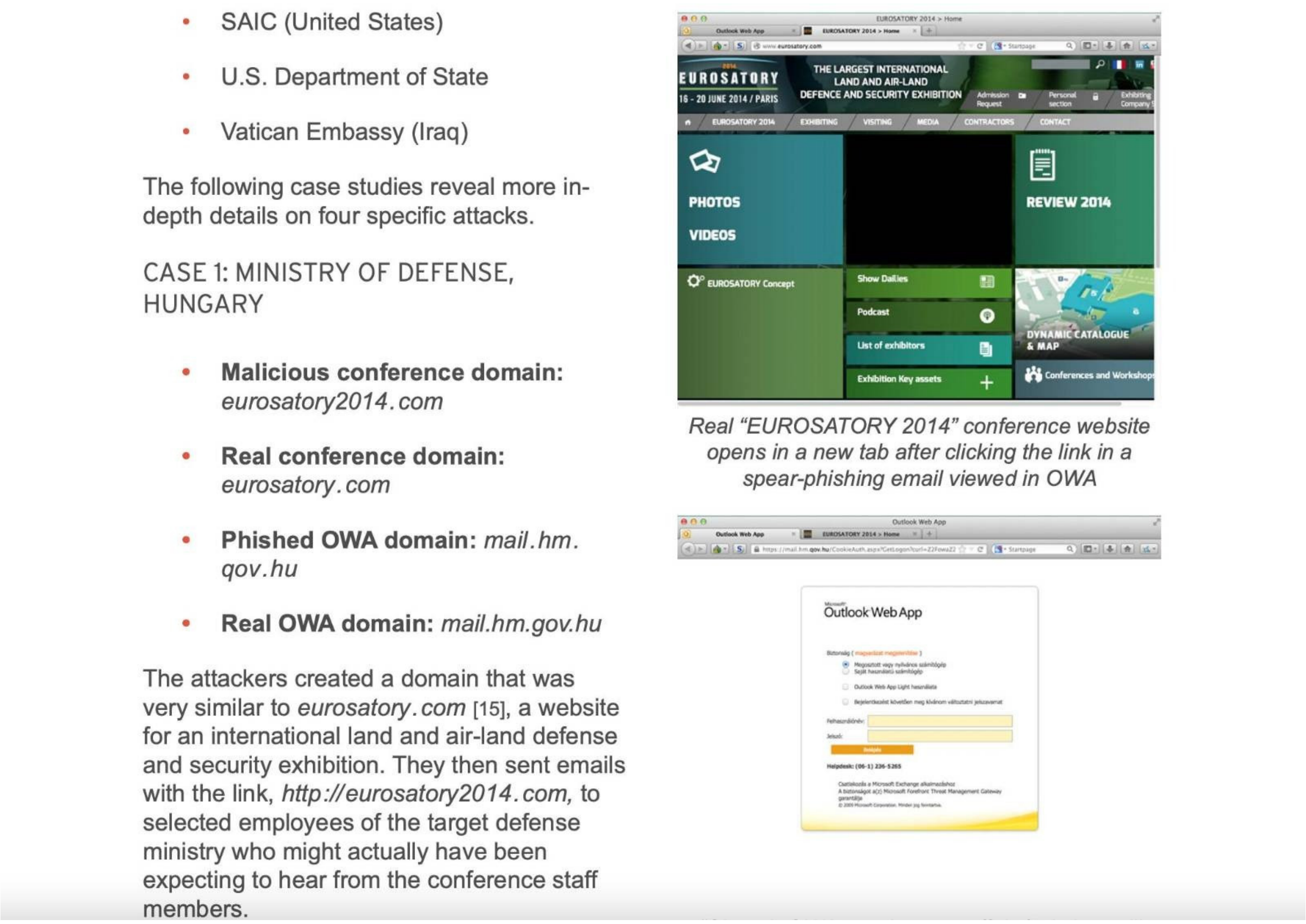
According to a cyber security expert familiar with the incident, the Hungarians responded to the TeamSpy attack with an aggressive counterattack. They hacked into the Russian attack infrastructure, identified Russian hackers operating from Russian and Ukrainian Internet cafes, among others, and obtained the target list of TeamSpy attacks. In a joint operation with NATO partners, by accessing the victims' computers around the world, they simultaneously shut down infected devices, cutting off Russian hackers from a wealth of information. Such an operation requires serious organisation and expertise, which, according to several Direkt36 sources familiar with the case and involved in cybersecurity, shows how advanced Hungarian cyber defence was at the time.

It was in the early 2010s that Russian intelligence services – mainly the Russian Federal Security Service (FSB) and the Russian military intelligence (GRU) – really started to get into hacking. "For Russia, cyber warfare is part of a permanent information warfare. This warfare is based on the perception that the Western world wants to undermine Russia's position of power and is ultimately engaged in a comprehensive and continuous effort to subjugate the country," AH's former senior national security officer Péter Buda told Direkt36.

Since the Russians see NATO simply as a military tool of the United States, Buda said, their cyber espionage "is mainly aimed at detecting information and conflicts of interest that could disrupt the unity of the NATO alliance, in addition to the continuous monitoring of capabilities and intentions". The cyber espionage method, also used by the Russians, called Advanced Persistent Threat (APT), does not aim at immediate, visible damage, like a simple hacker attack, but at a persistent presence within the targeted IT system.

While Prime Minister Viktor Orbán was already advertising his pivot towards Russia and China, Russian hackers of the GRU and FSB – hacking groups known as APT28 and APT29 – treated Hungary as an enemy and attacked it just as they did other EU and NATO member states. An official of the Orbán government at the time, said that in 2012-2014, in addition to the Hungarian Ministry of Foreign Affairs, the Ministry of Interior and even the Ministry of Defence were compromised by hackers. Based on their digital footprint and intelligence sharing with NATO/EU partners, they were also very likely Russians.

"For example, the attacks came from mispelling domains, such as mail.hm.qov.hu, with QOV instead of GOV," the former official recalled. Details of this attack, including screenshots of a duplicate site of the Ministry of Defence asking for login details, were published in 2016 by a cybersecurity firm.



- SAIC (United States)
- U.S. Department of State
- Vatican Embassy (Iraq)

The following case studies reveal more in-depth details on four specific attacks.

CASE 1: MINISTRY OF DEFENSE, HUNGARY

- **Malicious conference domain:** *eurosatory2014.com*
- **Real conference domain:** *eurosatory.com*
- **Phished OWA domain:** *mail.hm.qov.hu*
- **Real OWA domain:** *mail.hm.gov.hu*

The attackers created a domain that was very similar to *eurosatory.com* [15], a website for an international land and air-land defense and security exhibition. They then sent emails with the link, *http://eurosatory2014.com,* to selected employees of the target defense ministry who might actually have been expecting to hear from the conference staff members.

Real "EUROSATORY 2014" conference website opens in a new tab after clicking the link in a spear-phishing email viewed in OWA

Source: Trend Micro

However, nothing about the extensive Russian cyber attack on the MFA and its foreign missions during the second Orbán government has been made public before.

> "Every end point of the entire MFA network was infected, everyone was affected. In fact, the Russians kept logging in and out of the system with domain administrator privileges," a former Orbán government official said.

These claims were confirmed by former intelligence officers who also worked in fields related to countering Russian intelligence. The integrity of the MFA's systems was eventually restored around 2013.

Sources have shared numerous stories about the cybersecurity weaknesses that the Russians may have exploited. For example, one former Hungarian diplomat recalled that a few years ago it was possible to discuss work matters with the MFA's state secretaries on Facebook Messenger – an insecure channel where such communication should not be allowed at all, and which has been hacked numerous times in recent years. Another example is that one of the default login passwords used to be "secretXX" (two identical numbers) on MFA computers. "And if it had to be changed, the number always increased by one. But 'just in case we forget', many secretariats and shared computers preferred to keep the original password," the former diplomat added.

In addition, several databases leaked from hacking attacks years ago are still available online, containing passwords alongside the email addresses of Hungarian MFA officials. For example Direkt36 when looking for the contact details of a Hungarian ambassador, through a simple Google search found not only the diplomat's private email address, but also a password beginning with "pussy..".

A former Orbán government official familiar with Russian cyberattacks also said that in the first half of the 2010s, the Russians hacked not only the Hungarian MFA's own documents. Some of the infected government computers were connected to a zombie network, from which they continued to attack other NATO member states of greater interest to Moscow. Zombie networks are computers and devices that hackers have secretly taken control of from afar and from which they launch coordinated attacks. In some cases, the Hungarian infection was first detected by a NATO third country attacked from the Hungarian network – IP addresses made it look like the Hungarian ministry computer was the attacker.

> "It's important to understand that Hungary is not the main target of these attacks, but the security level of Hungarian public and private infrastructures is simply so poor that it is the easiest to penetrate here," a cyber security expert said.

Former Cyber Defence Management Authority (CDMA) head Ferenc Frész said in a 2015 presentation that much of their work was about addressing these vulnerabilities. But by then the CDMA had virtually ceased to exist. In his presentation, Frész claimed that Hungarian cyber defence had been dismantled in a way that had completely eliminated Hungary's defence capabilities, and that "it was all done under Russian economic pressure". He did not elaborate on what basis he made this claim, and when contacted by Direkt36 he declined to comment on his statement at the time.

Watch Video At:

https://youtu.be/F8IWjJDhl2w

The spectacular pro-Russian turn in Hungarian politics came in 2014, after Orbán and Putin announced their agreement on the Paks2 nuclear power plant expansion. Then Péter Szijjártó, who already had extensive Russian connections, took over the leadership of the MFA. In November 2014, the head of the National Security Authority was fired, the institution was brought under the Ministry of Interior, and a few months later the staff of the Cyber Defence Management Authority was laid off as part of a “reorganisation”.

According to a cybersecurity expert familiar with the case, the Orbán government began to see Hungarian cyber defence as a linchpin of the Hungarian-Russian rapprochement, and the agreement on the Paks nuclear expansion, among other things, brought a negative turn. Another cybersecurity expert added that CDMA’s staff have also isolated themselves by revealing to various ministries, in an unvarnished style and “without much diplomacy”, what critical vulnerabilities they had found in government networks.

Under the third Orbán government, cyber defence tasks were taken over by agencies under the Ministry of Interior, primarily the Special Service for National Security (SSNS). However, after the abolition of the Cyber Defence Management Authority, in fact, all the intelligence and state agencies started to do a little bit of cyber defence. According to a former official of the Orbán government, the consequence of this include that the various agencies regularly point fingers at each other or wait for each other, operate in isolation from each other and sometimes there is even outright rivalry between them.

The next big wave of Russian attacks instantly showed the weaknesses of the new set-up.

The “institutional hush-up policy” begins

One morning in November 2016, when the MFA official entered their ministry office at Bem Square in Budapest, they immediately noticed that their computer had disappeared from their desk. “At first I was just surprised. I went to our secretary to ask what had happened, because I can’t work without a computer,” the then MFA official recalled to Direkt36. All the secretary could find out was that the computer had been infected with some virus and that another device would arrive at some point.

The virus had entered the computer via an infected email back in October 2016, said a former Hungarian intelligence officer who shared details of the incident. The Russians misled the MFA official with a scheme known as spearphishing, which involved editing a deceptive, personalised email. The email in this particular case may have appeared at first glance to have been sent by an employee of NATO headquarters in Brussels. Such an email address and such a person are not actually in the address database of NATO headquarters in Brussels, and the format of the address was not legit either, a former NATO official told Direkt36.

The sender’s first name, however, was exactly the same as that of a close foreign acquaintance of the MFA official. “The name could have been misleading and I obviously clicked automatically. NATO was also a clever trick, if it wasn’t for the name, I would have clicked on it because of the NATO name anyway,” the former official said, adding that the content of the email was completely uninteresting and they could not remember whether they had clicked on a link or an attachment within the email.

“Nothing suspicious happened after the click, no little skull and crossbones appeared,” they added. Even when their computer disappeared, the MFA official did not think anything was wrong, only when the Information Office (IH) later started an investigation, but even that was reassuring as it exonerated them from any wrongdoing or suspicion. Soon, however, counterintelligence officers from the Constitution Protection Office (AH) also came in and sat them down for two rounds of interrogations, and the second time the MFA was hooked up to a lie detector. They tried to find out if the official was spying for Russia.

According to a former Hungarian intelligence officer, all the elements of the email hoax were part of a carefully planned psychological effect to get the target to definitely open the email. The source added that the Russian intelligence service had been studying the MFA official’s background, contacts and interests for some time. He knows this because the British intelligence service shared information about all this with the AH, which in turn informed the IH and the SSNS. Direkt36 sent a comment request to the British embassy about this, but they have not yet replied.

The opening of the email did not only infect the MFA official’s own computer. “It was a cancer-like virus that gets into one machine and then spreads through the system to all the others,” they said. But they only found out about this later, informally, through their senior government contacts. At the time, a government contact told them that at least 20 other MFA officials were also affected. Others who had received similarly personalised, infected emails, for example, were dealing with NATO, security policy, or the Eastern European region. “My acquaintance told me that the Russians were trying to get into the system through several targets, and I was just one of them,” the former MFA official added.

Balázs Bencsik, director of the National Cyber Security Center (NKI), a specialised body within the Hungarian SSNS, revealed some information about Russian cyber attacks in Hungary in 2016, following year at the Tusványos Summer University. He did not name a ministry, but claimed that suspicious activity had been discovered on a Hungarian government server before the 2016 U.S. presidential election. This Hungarian government server transmitted data to the Netherlands and Germany. Later, it was also discovered that these were orchestrated by the same Russian hacking groups who had also hacked into U.S. Democratic Party servers.

Bencsik added that similar attacks against Hungarian government systems were “frequent and continuous” but not primarily directed against Hungary. For example, he claimed that the Hungarian government server hacked in 2016 was used by the Russians to disguise (“IP address masking”) their attack on the United States during the presidential election campaign. In other words, the Russians did the same thing again as they did when they hacked the MFA around 2012-13, and again used the hacked Hungarian government computers to launch further attacks on other NATO member states.

Russian hackers did not only attack the Hungarian Ministry of Foreign Affairs and Trade: during the same period, the Czech Foreign Ministry was also under a very similar Russian attack, the details of which were published in the Czech Counterintelligence Service (BIS) Yearbook 2017. Since the beginning of 2016, the Russians have accessed the email accounts of at least 150 Czech MFA officials, from which all information has been periodically extracted. In parallel, since December 2016, a different type of less sophisticated “brute force” attack has been launched against hundreds of Czech MFA email accounts.

Lubomír Zaorálek, then Czech Foreign Minister, revealed in early 2017 that dozens of email accounts of senior Czech diplomats had been hacked, with some of the stolen information relating to NATO and EU issues. According to Czech investigative website Neovlivni.cz, even the email accounts of Zaorálek himself and his state secretaries were hacked and thousands of documents were downloaded. According to BIS, the compromise of the Czech Foreign Ministry’s email accounts “in numerous key aspects corresponds to similar cases of cyberespionage, which took place in other European states over the same period”.

While the Czechs chose to go public, the Orbán government, like during the Hungarian cases of 2012-2014, kept the cyberattacks on MFA systems in 2016 hidden from the public. “There was an institutional hush-up policy,” the former MFA official who opened the infected email said. A few months later, the counterintelligence classified the MFA official as a risk to national security. In theory, this means that their activities or contacts were deemed incompatible with their work in the MFA for some reason, hence the official was fired.

This was done despite the fact that former intelligence officers with knowledge of the details of the case told Direkt36 that investigations had confirmed that the MFA official had not colluded with the Russians, but had simply clicked on the email. Moreover, the official later started working for the government of another European NATO member state, passing that country's national security screening without a hitch.

"Unfortunately, several victims have been slaughtered," a former official of the Orban government who had direct knowledge of such cases said. According to him, the AH has on several occasions launched investigations on suspicion of espionage and fired ministry employees who simply just clicked on infected emails. "They simply don't believe that these attacks are really being carried out by all kinds of pimple faced St Petersburg kids," he explained. According to the source, this is basically due to the Ministry of Interior's "senior policeman mentality", even when it comes to cyber defence: "What does a policeman do? He has to respond immediately and nab someone physically" the former official added.

But firing the clicking employees has not helped stop the attacks.

Russians gained access to windowless secret rooms

Completely enclosed, windowless or curtained "VKH rooms" can be found everywhere in the world where there is a Hungarian diplomatic mission, even in the most remote countries. These secure rooms protect the endpoints of the closed Protected Foreign Network (Védett Külügyi Hálózat, VKH), foreign ministry computers that encrypt messages and to which, in principle, no external device can be connected, a former ambassador of the Orbán government explained.

VKH rooms are used by foreign ministry staff and Hungarian diplomats when they want to communicate classified national, NATO or EU information to their colleagues and superiors. These rooms "may only be entered with a valid personal security certificate and user authorisation, and in possession of a special card authorisation, or with the written authorisation and escort of the head of security", according to the Hungarian MFA's security regulations.

Anyone accessing this system can also access Hungarian state secrets and allied information classified as "restricted" and "confidential". These are classified data, according to the law, the disclosure of which to the public or to unauthorised persons would adversely affect or be harmful to the public interest, and are classified by default for 10 and 20 years respectively.

The former ambassador recalled the difficult process of communication. If a diplomat wants to send a message through the VKH, he or she brings their notes on piece of paper into the room, types the message into a computer on the keyboard and the system encrypts it with a randomly generated unique code. Then the piece of paper must be destroyed. No mobile phones or other electronic devices are allowed in the VKH premises. The system logs the time spent in the room and the materials accessed.

Russian intelligence had already successfully hacked the VKH network in the first major wave of attacks in the early 2010s, a former official of the Orbán government with direct knowledge of the incident told Direkt36. This claim was confirmed by Hungarian diplomats who also heard about the hacking. The former government official said that around 2013, the devices in all the VKH rooms around the world, in the ministry on Bem Square and in Hungarian diplomatic missions abroad were all replaced to restore the integrity of the network. The former ambassador of the Orbán government recalled that he had been told by the people from the security department of the ministry who had visited them that the old equipment was outdated and that the network would be replaced completely.

Péter Szijjártó, Vladimir Putin and Viktor Orbán. Photo: kormany.hu

Replacing the computers almost ten years ago did not solve the problem for long. Several former intelligence officials familiar with the cyberattack on the Foreign Ministry because of their agency's involvement told Direkt36 that the VKH had been hacked again by Russians using IT tools in recent years. A member of the Hungarian parliament's foreign affairs committee recalled that Hungarian diplomats had been saying for at least a year and a half that the system was again outdated and insecure, and that this was the reason why they had asked for money to upgrade the VKH.

However, according to several reports, there were also problems with the physical security of the system, but no information is available on whether these contributed to the latest break-in.

According to the former ambassador of the Orbán government, for example, a common problem was that the secure VKH rooms in remote diplomatic representations were not always properly installed. The foreign affairs committee member confirmed this, adding that the construction process itself posed a significant risk. For example, during a rebuilding project, a VKH machine could be left unattended on the construction site. And a former MFA official recalled an incident from the first half of the 2010s, when the door of a secure VKH room at a Hungarian mission in Central Asia was found to have been forced open. A similar incident was also made public in 2017. A diplomat from the Hungarian diplomatic mission in Uzbekistan reported serious security deficiencies to the Szijjártó-led ministry, without much traction. He only received an informal reply to stop complaining – "give me a break".

By hacking the VKH, Russian intelligence services were able to access any of the documents transmitted on it. Sources who gave details to Direkt36 did not specify exactly what material was compromised and when. The classified documents transmitted on the VKH do not only contain information from Hungarian sources. According to the security regulations of the ministry, confidential NATO and EU documents are also received, and the former ambassador of the Orbán government added that Hungarian reports transcribing various NATO or EU meetings are also received through this channel.

But beyond the "restricted" and "confidential" information also transmitted on the VKH, there is even more strictly protected information, classified by default for thirty years. These are classified as "secret" or "top secret". According to the former ambassador of the Orbán government, no such information has been received by his representation through the VKH system. He said that documents considered to be highly classified information, could only be accessed by a narrow internal circle in the Bem Square ministry, through separate channels, as required by the ministry's security regulations. Direkt36 has no information that these even more sensitive channels have been compromised.

According to a former intelligence officer with indirect knowledge of the incident, the integrity of the VKH system was supposed to be temporarily restored around February 2022, but the now obsolete VKH machines have not yet been replaced. The source added that the MFA's regular internal network remained infected.

Even half a dozen diplomats from EU and NATO member states told Direkt36 in February 2022 that they had not received any official information from the Hungarian foreign ministry about the Russian cyber attack, its severity or whether it had affected NATO and EU information. "It should go without saying that if you are unable to eradicate the infection on your own, you ask for help from allies. The only time you don't tell them is if you can immediately repel the attack," a former NATO official said. The source added that within the North Atlantic alliance, "there is also a gentlemen's agreement that if you know your network is infected, you try to exclude NATO documents from it”. A senior diplomat from an EU country, however, said that a government has discretion on what information to share and what not to share, as there are no specific rules.

But compared to the world of diplomacy, the rules are much clearer for counterintelligence. “Any vulnerability that allows the compromise of protected data of the allied system causes damage that is difficult to repair afterwards,” Péter Buda, AH’s former senior national security officer told Direkt36. According to him, preventing attacks on protected IT systems should be a top priority. However, if rapid eradication fails, it will wittingly or unwittingly serve the interests of the attacker.

Unlike the secretive Hungarian diplomacy, however, the Hungarian counterintelligence service had previously informed its partners of the compromise of the foreign ministry.

Hungarian counterintelligence discussed the problem over a beer

In the autumn of 2021, representatives of Europe’s intelligence services gathered again at the Club de Berne to discuss current issues, with Russia being the main topic. Club de Berne is one of the most important intelligence sharing forums between Western counterintelligence services, where the 27 EU member states plus Norway, Switzerland and the UK are represented, and where the U.S., Canada and sometimes even Israel are invited. The Hungarian participant in the intelligence sharing forum is the Constitution Protection Office (AH).

This time, intelligence officers did not gather for a meeting at the most senior level, but for a lower-level expert meeting. In such cases, the invited participants are mid-level managers, say counter-intelligence directors, who are familiar with the concrete details of major operations and can discuss them with their foreign counterparts. However, the most important part of the agenda is not the relatively formal and generic daytime conference programme, but the evening dinner and beer where a lot of interesting information is shared.

A former intelligence officer with indirect knowledge of what happened at last autumn’s meeting told Direkt36 that it was also at this time, during an informal drinking session after the formal meetings, that the Hungarian AH representative told his Western colleagues that the Hungarian MFA had apparently come under extremely heavy Russian infiltration. In response, several European participants immediately began to list the number and variety of hacking attempts made by Russians in their countries in the recent past.

The most recent case was in Germany, where the email accounts of Bundestag members and other politicians were hacked during the German election campaign, which the Russians “combined with disinformation and influence operations”, according to a report on the website of the SSNS’s National Cyber Security Center. Similar Russian cyber attacks have hit Austria, the Czech Republic, Slovakia and Poland in recent years. These EU countries followed roughly the same protocol in dealing with cyber espionage: they detected the trouble, took more or less swift action to counter it, shared information with their allies, and then finally made the incident public and protested to Russia.

According to the former intelligence officer, the AH representative did not share information with Club de Berne members on the specific official orders of the MFA or the Orbán government. “The AH has a fundamental interest in sharing information, because if it doesn’t give, it doesn’t get,” said a cybersecurity expert who has had previous ties to the agency.

The example of Austria, who were effectively suspended from the club a few years ago for their unreliability, could also serve as a deterrent to the Hungarian intelligence services. “One of the most important areas for NATO in the last few years has been the strengthening of alliance-level cooperation in countering Russian cyber attacks,” explained former senior AH officer Péter Buda on the importance of information sharing on Russian matters.

In recent months, following the Club de Berne meeting, the news of the hacking of the Hungarian MFA has reached a much wider audience of foreign and security policy experts, including foreigners. “It is now common knowledge in the European intelligence community that the Russians have hacked the Hungarian foreign ministry and that many Hungarian diplomatic missions have been compromised,” said an EU national security official who learned of the hack from his own institution in January 2022.

But beyond secret intelligence sharing, the Orbán government is conspicuously refraining from openly confronting Russian intelligence activity. For example, Direkt36 previously revealed that Russian spies caught in the act in Hungary are always “quietly expelled”, i.e. they are simply sent home and spy affairs are never made public.

As for the only Hungarian exception, the case of the Russian diplomat in Budapest who was expelled after the Skripal poisoning, we revealed that Budapest and Moscow had deliberately conducted the expulsion and counter-expulsion in a way that would not damage friendly relations. For example, a Russian was expelled from Budapest when he had finished his diplomatic posting and was preparing to return home anyway.

There are also quite spectacular examples of soft handling of Russian espionage. Former Hungarian diplomat to Moscow Szilárd Kiss, for example, was allowed to stay in his post even after he failed two national security screenings because of his Russian intelligence connections. As for former MEP Béla Kovács, who has since been convicted of preparations to commit espionage, Péter Szijjártó told Index.hu that he had not raised the issue with any former Russian ambassador. Since then, Kovács has been living and teaching in Moscow and is currently analysing the invasion of Ukraine on Russian propaganda websites.

The last time Hungary made international news on Russian cyber espionage was a few weeks ago, when it emerged that the Orbán government was blocking Ukraine, which has suffered serious Russian cyber attacks, from joining NATO’s Cooperative Cyber Defence

Centre of Excellence. At the EU summit in December, Viktor Orbán was asked in vain to lift the veto. Orbán was only willing to lift his veto after the Russian military invasion of Ukraine.

Illustration: Péter Somogyi (szarvas) / Telex