Ministry of Digital Affairs
Republic of Poland
Department of Cybersecurity

FOREIGN INTELLIGENCE AGENCY
Serving Poland in the shadows

TLP:CLEAR

Analysis of threats to the cybersecurity of diplomatic missions of Poland and other NATO countries in the context of selected hacking attacks.

Ministry of Digital Affairs:

Foreign Intelligence Agency:

Introduction

This publication is intended to provide an overview of the threats to the cyber security of diplomatic missions of the Republic of Poland and other NATO countries in the context of recent hacking attacks.

Following Russia's aggression against Ukraine, Poland and the institutions it represents are facing increasing cyber-attacks. Responsibility for many of these is attributed to hacking groups operating in close, often even direct, association with the Russian Federation and are a consequence of Poland's involvement in helping the Ukrainians. Critical infrastructure, particularly the transport sector, is a particularly vulnerable area, given the supply routes used for the transfer of international support to Ukraine lead through Polish territory.

Hacking groups carrying out cyber-attacks have various objectives, including stealing sensitive information, disrupting access to services and spreading disinformation. These activities adversely affect the interests of affected individuals and institutions. They target government institutions, businesses, NGOs and individuals.

It is worth being aware of the modus operandi of such groups operating on different axes, therefore, this publication outlines examples of attacks targeting EU and NATO countries' government institutions — diplomatic missions vital for state security. We also refer to recently identified operations directly targeting diplomatic missions of the Republic of Poland. We hope that this publication will provide you with valuable insight into cyber threats linked to the attacks by hacking groups against the above-mentioned institutions.

We encourage you to read on and learn more!

The ongoing cyber warfare and its implications for NATO countries

Russia's full-scale aggression against Ukraine began on 24 February 2022 with the incursion of Russian troops into Ukrainian territory. However, the cyber confrontation has been ongoing since at least 2014, i.e. the illegal seizure of Crimea and Ukraine's eastern territories. During this time, Moscow-linked hackers have carried out numerous operations targeting all areas of the country's functioning, including its energy and banking system. The scale of the damage caused by these operations has repeatedly shocked the international community and effectively disrupted the lives of ordinary Ukrainians. The 2022 cyber-attacks also acted as a foreshadowing of the Russian invasion, as they aimed to set the stage for it and paralyse the Ukrainian information space in the crucial initial hours of the conflict.

The war across Poland's eastern border invariably demonstrates that cyberspace is a plane of strategic competition, used by states hostile to the West to advance their interests. It is instrumentalised both during peace (as a tool of hybrid warfare) and war. Observations of the ongoing war point to areas of particular vulnerability. Russian hackers aim to damage and disrupt Ukrainian military, civilian and government networks, mainly through destructive attacks on systems and databases. Apart from such activities, the Russians use hacking to obtain information to support the war effort (cyber espionage).

The fact that so far cyber-attacks targeting Ukraine have not led to a complete paralysis of the state's infrastructure and armed forces should not detract from the importance of the continued need to enhance cyberspace security. Conversely, it is thanks in part to the organisation of cyber defence forces and international cooperation in this area that Ukraine's IT networks have proved resilient to aggression. Commercial entities specialising in cloud services enabled data to be taken outside the warzone and at the same time ensured its redundancy using global infrastructure. It was also important for Ukrainians to quickly acquire the competencies needed to work with cloud technology. An example of Poland's assistance in this regard is the IT Skills 4U initiative — a free training and career development programme for Ukrainian citizens

.

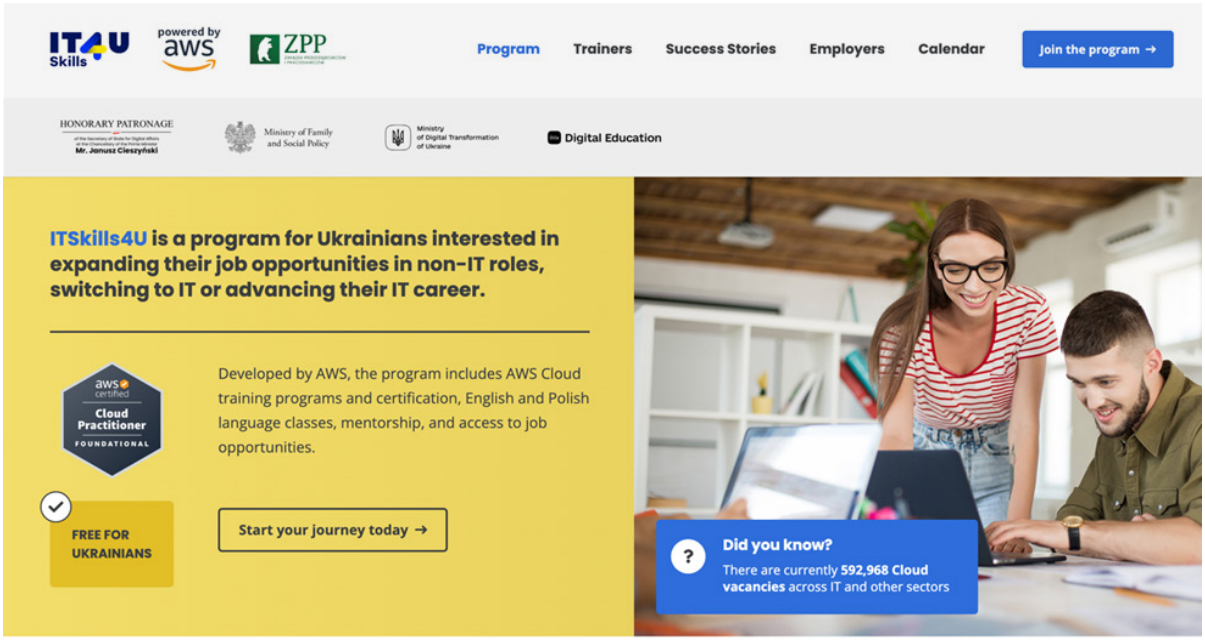

Figure 1: The ITSkills4U1 initiative[1]

One of the conditions guaranteeing the stability of NATO, its member states and the citizens of the Western community is the neutralisation of the threat posed by hostile cyberspace operations. Ensuring this requires constant monitoring of the activities of hacking groups, learning their modus operandi and the tools they use. This is a complex and continuous process. Attackers continue to refine their methods of operation as technology makes new strides and further digitises our lives, public and private alike, which provides them with new avenues for attacks.

Given the importance of uninterrupted access to ICT assets, this issue should be a priority for NATO and its member states. This is reflected in NATO's numerous capacity-building initiatives for the cyber security sector — from individual experts' skills (training and education programmes) to expert group skills (exercises and war games) to the bloc as a whole. These efforts culminate in joint doctrine and strategy, including the Cyber Defence Pledge[2]. The latter was adopted in July 2016 at the NATO summit in Warsaw. At that time, cyberspace was recognised as the fifth operational domain (alongside land, sea, air and space).

[1] Source: https://itskills4u.com.ua/ (accessed 31 August 2023)
[2] Source:https://www.nato.int/cps/en/natohq/official_texts_133177.htm (accessed 31 August 2023)

Figure 2: Locked Shields 2023 exercise[3]

In peacetime, NATO allied states focus on deterring and repelling cyberspace attacks. There are several initiatives to support these activities, including the “EU Cyber Diplomacy Toolbox”, a toolbox for diplomacy related to cyber activities. This initiative was created as a common EU diplomatic response to malicious cyberspace activities, including numerous hacking attacks. It corresponds to the EU's approach to cyber diplomacy under the Common Foreign and Security Policy. Activities in this area contribute to conflict prevention, cyber security threat reduction and increased stability in international relations. The EU's diplomatic response to malicious cyber activities is appropriate to the scope, scale, duration, intensity, complexity, sophistication and impact of each cyber-attack. All diplomatic efforts promote security and stability in cyberspace by enhancing international cooperation and reducing the risk of misperception, escalation and conflict that may result from ICT incidents."[4].

[3] Source: https://news.err.ee/1608955571/sweden-iceland-team-triumphs-at-locked-shields-2023-cyber-defense-exercise (accessed 31 August 2023)
[4] Source: https://www.cyber-diplomacy-toolbox.com/ (accessed 31 August 2023)

Just because the war is taking place on Ukrainian territory does not mean that Western IT systems are safe. States and organisations hostile to the West continue to seek to tie up and disperse its capabilities. Malicious cyber activities targeting allied countries include such things as theft of sensitive information (gaining unauthorised access to protected network resources), using encryption software (ransomware), destructive software (wipers) and distributed denial of service (DDoS) attacks[5]. The initial step is often to send inconspicuous phishing emails in an attempt to acquire login credentials, which can then be used to access ICT infrastructure. Allied institutions and governments have responded to these hybrid threats by organising numerous initiatives to increase resilience against such attacks. Therefore, NATO can be considered the key to common security.

The extent of the Western countries' response is affected by the issue of attribution. State actors using hacking tools take advantage of the fact that identifying the individuals and institutions responsible for such operations poses significant difficulties. Indeed, it is often impossible to prove that a hacking attack was carried out at the behest of the authorities of a particular state. The culprits themselves have no intention of being held accountable for their actions, which is why the governments of the countries ordering the attacks officially dissociate themselves from them based on the doctrine of plausible deniability.

Despite this, ICT investigations make it possible to identify certain characteristic features of the attacks, e.g. proving what infrastructure, tools and methods of operation were used, etc. Based on the traces obtained, it is possible to reconstruct the course of events, including tracking down the actual attackers. As a rule, their activities are carried out in an organised manner and use recurring characteristics (TTPs — Tactics, Techniques, Procedures) that allow them to be combined into so-called activity clusters. Afterwards, based on their knowledge and data, government or private entities assign these clusters of characteristics to specific groups, which in turn can be linked to foreign government structures or labelled as cybercriminal organisations. Typically, the activities of government-funded hackers focus on achieving the strategic objectives of their principals, while hacktivist groups are concerned with making a profit or promoting their ideology.

[5] Attack to disrupt the availability of a service by overloading it.

The above findings may trigger a geopolitical response. Indeed, it should be noted that in 2016 NATO recognised cyber warfare as another operational domain, **so hybrid attacks and cyberattacks may warrant a collective defence effort under Article 5 of the North Atlantic Treaty.** When faced with acts of lesser magnitude, **the allies may also invoke Article 4 of the Treaty, which enables consultations between them whenever they deem the "territorial integrity, political independence or security" of a NATO ally to be at risk.**

NATO countries must focus on strengthening their cyber resilience and defence capabilities. Their ongoing efforts in this regard include investing in cyber security, developing capabilities to detect and respond to attacks, bolstering critical infrastructure and international cooperation to share information and carry out joint actions against cyber threats.

The Alliance's deterrence and defence posture is based on the right mix of nuclear, conventional and missile defence capabilities, complemented by space and cyber capabilities, as stated at the July 2023 summit in Lithuania: "We have agreed to continue our work on multi-domain operations, enabled by NATO's Digital Transformation, which further drives our military and technological advantage, strengthening the Alliance's ability to operate decisively across the land, air, maritime, cyberspace and space domains."[6]

[6] Source: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (accessed 31 August 2023).

Figure 3: NATO Summit in Vilnius[7]

Hostile cyber activity by Russian APT groups as a growing threat to the government sector of NATO countries

Russia uses cyber operations as a tool of hybrid warfare to achieve its strategic objectives. While Russia-linked hackers are capable of destroying or disrupting infrastructure, including critical infrastructure, their essential task is to steal sensitive data. Modern technology and the virtually unlimited reach of cyber operations mean that such efforts may be carried out in lieu of traditional espionage operations. Hostile states seek all sorts of information that can help them determine their policy objectives (foreign, domestic, military, economic) and the means to achieve them. Though it may seem counter-intuitive, it is not just top-secret government communication networks that can be a source of valuable data. Some smaller institutions, including private businesses, which do not have such demanding ICT security standards, also process significant amounts of useful data. These include, in particular, subcontractors of all kinds, participants, observers and opinion leaders. Even if they do not process the information an attacker cares about most, their knowledge can be used to reconstruct the desired data — all with less operational risk and a higher chance of success.

[7] Source: https://www.act.nato.int/article/nato-summit-vilnius-2023-day-one/ (accessed 31 August 2023).

Given the ongoing war, Russia seeks to obtain all kinds of information on the scale of international assistance to the fighting Ukraine. Data on material support, including defensive military equipment, is particularly valuable. Numerous actors are involved in the process of coordinating such shipments. Apart from state leaders and governments, this includes the structures responsible for maintaining telecommunications networks, road and rail infrastructure, transport hubs (train stations, airports, seaports), and finally, the individual operators that are part of the truck fleet used for transporting the goods to the east. Any elements of the supply chain can fall victim to hacking attacks, and the attackers can obtain valuable data. In the face of this threat, the primary task of institutions responsible for state security, including in cyberspace, is to protect logistics channels and critical infrastructure.

Attacks on diplomatic facilities attributed to Russian APT groups

In this situational context, diplomatic missions are an extremely important link. Besides having access to sensitive information on the foreign policy of individual countries, including cooperation with allies, many of them are involved in obtaining supplies and coordinating their transport to Ukraine. For this reason, they are an important target for hacking attacks. Indeed, the data acquired through such attacks is of value only to the governments of other, rival states, hence it is their affiliated groups that are most active in this area. Their primary focus is data acquisition and infiltration of infected environments to gain as much information as possible that may prove useful in planning subsequent operations and pursuing interests.

Figure 4: APT29 group's affiliation with Russian special services and related names — own elaboration based on available data

Working with entities belonging to the National Cyber Security System, analysts of Poland's Foreign Intelligence Agency have observed numerous attempts to attack Poland's diplomatic missions. One of the most active, and at the same time most dangerous, organisations attempting to breach their security is a group referred to as APT29 (a.k.a. NOBELIUM, The Dukes, Cozy Bear, BlueBravo).

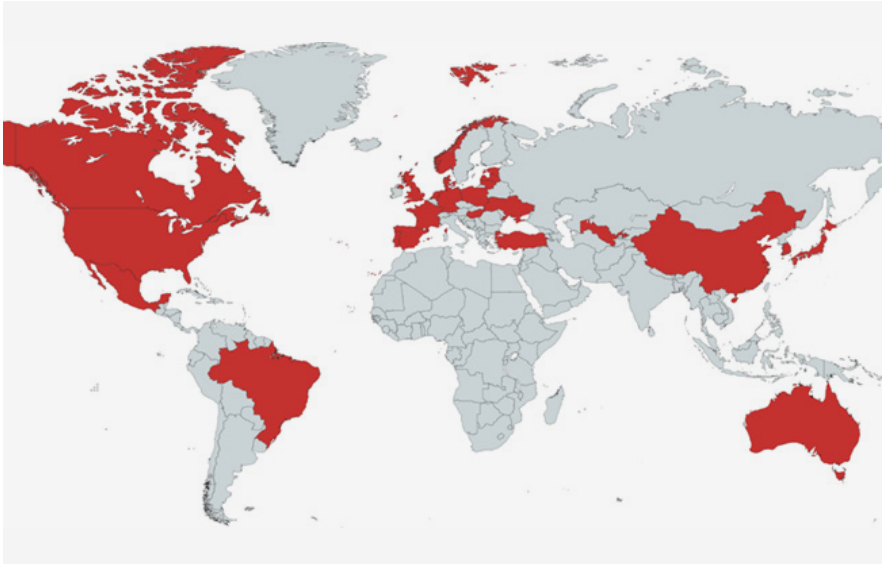

Figure 5: Countries affected by APT attacks29 — own compilation based on available data

The group is linked to the Foreign Intelligence Service of the Russian Federation (as determined by the US[8], UK[9] and other governments). APT29's links with Russian intelligence indicate a focus on targeting NATO countries — in line with general Russian practices.

APT29's operations are largely initiated by the mass sending of emails to encourage embassy staff to open attachments or hyperlinks leading to spoofed websites. To do this, the hackers use a variety of methods, including spoofing (hiding real email addresses under trusted names). They also use previously hacked mailboxes (including those belonging to random people without diplomatic ties). The distributed messages refer to issues that may be of interest to those working in diplomatic missions. These include invitations to parties, requests to arrange a meeting with an ambassador or offers to sell various types of goods at a discount to diplomats.

[8] Source: https://www.cisa.gov/news-events/alerts/2021/04/26/fbi-dhs-cisa/join-advisory-russian-foreign-intelligenceservice (accessed 31 August 2023)
[9] Source: https://www.nscs.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf (accessed 31 August 2023)

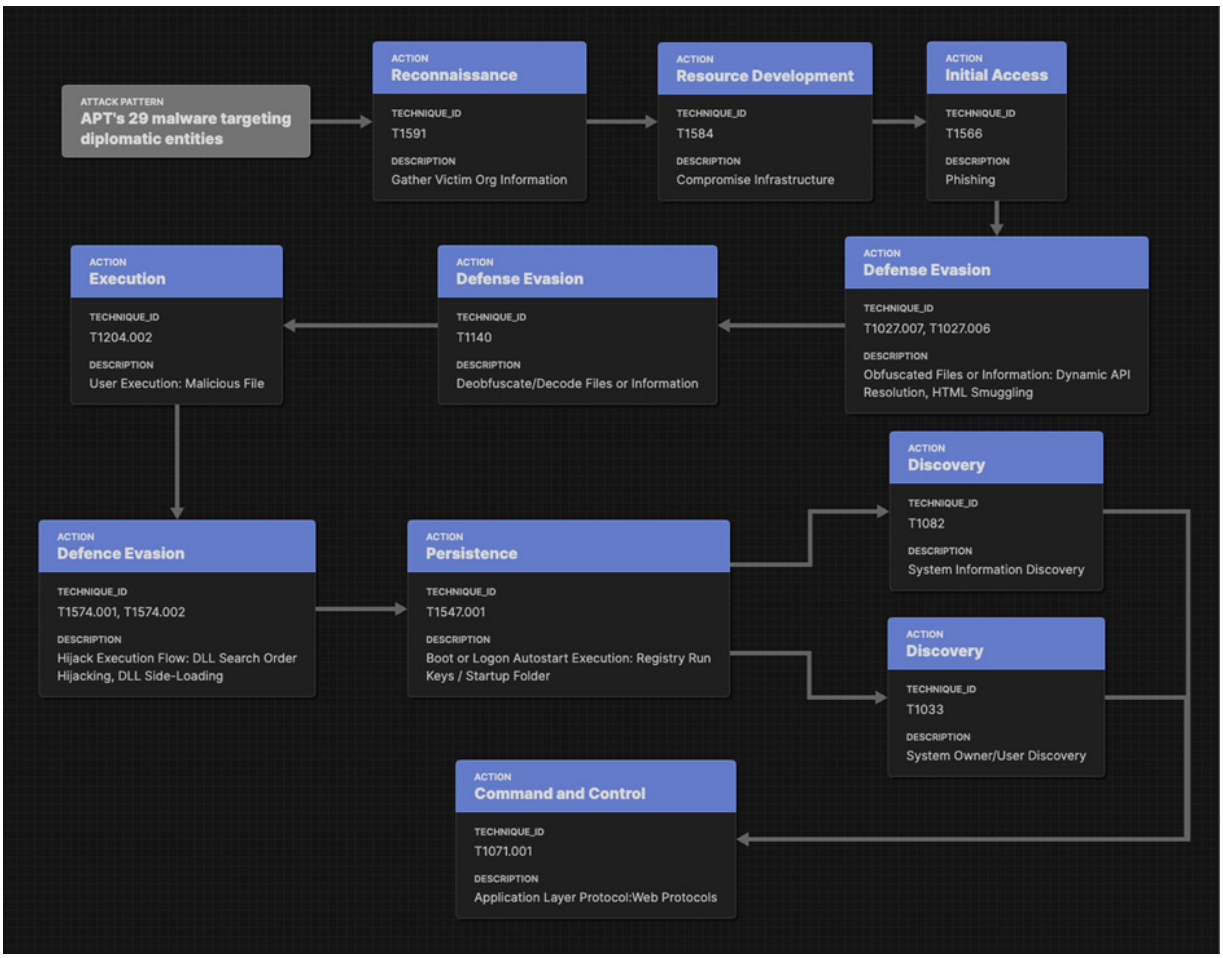

Figure 6: Diagram showing modus operandi in APT29's recent operations
— own elaboration based on available data

One such campaign identified by cyber security analysts involved a modified genuine car sale advertisement sent by a purported diplomatic mission employee. The fact that the attacker had prepared a fake listing (Figure 7.), confusingly similar to the original, may suggest that he had access to the mailbox of a user who received the genuine message.

CAR FOR SALE IN KYIV
THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: [redacted]

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	**7,500 Euros**
Custom	NOT CLEARED
Contact	[redacted]

Figure 7: False car sale listing based on a similar one sent a few days earlier — own elaboration based on available data

The listing included a link leading to a spoofed website, which would trigger the download of a malicious file after checking the browser parameters. If the conditions assumed by the attacker (verification of the User-Agent parameter) were not met, the victim's browser would download a harmless image of a car. Site visitor verification is designed to block scanning mechanisms such as the sandbox, allowing automatic protection and verification of files. Also interesting was the mechanism used for logging IP addresses via an additional PHP file placed on the server — presumably to record the campaign's effectiveness and potentially enable analysis for future detection and flagging of addresses belonging to cyber-security experts (Figure 8). A similar mechanism had already been observed in previous campaigns attributed to APT29.

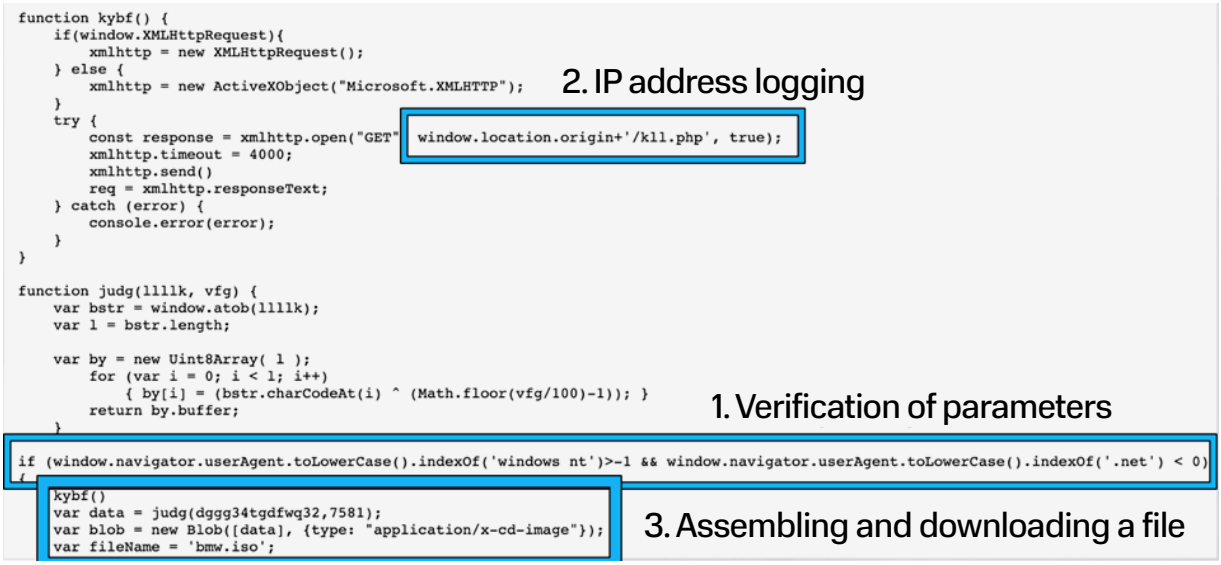

Figure 8: Code extract from the website used in the attack — own elaboration

Identical mechanisms were used in another campaign. The attacker distributed emails containing a fabricated document that appeared to have been sent by the Turkish Ministry of Foreign Affairs. Upon opening the link, the user would be redirected to a website that would verify the browser parameters, store the IP address and then either start downloading malware or a harmless PDF file — depending on the results of the verification. The mechanism itself is not sophisticated and circumventing it is hardly a problem. In previous campaigns, the attacker used more advanced methods, i.e. implicit verification of browser parameters using appropriate PHP file functions, which then returned a malicious file or not, depending on the result of the verification. In subsequent campaigns, the attacker decided to use HTML smuggling (see Figures 8 and 9 — designation, where item 3 represents the function that assembles the target file), which consists in embedding binary files directly in the webpage code using JavaScript. This procedure is designed to bypass antivirus scanners and other security measures, i.e. web proxies.

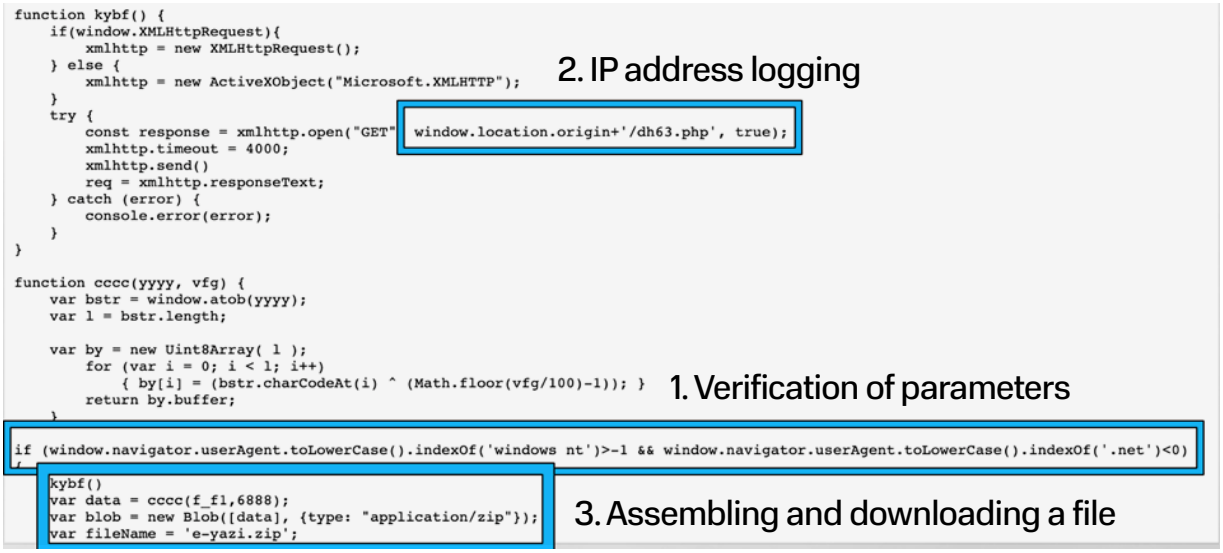

Figure 9: Content of the HTML file used in the next campaign — own elaboration

Observations by Foreign Intelligence Agency analysts suggest that the malware is distributed via spoofed websites. APT29 does not create temporary domains, probably because this would be easy to detect and block.

Analysis by the Foreign Intelligence Agency has shown that the compromised sites are typically maintained within the infrastructure of a single hosting company or its affiliated companies. One common feature here is the server management panel (cPanel) that can be found on each server involved in the attack — it is installed automatically by the hosting company on each machine. This leads to the conclusion that the attacker may have a tool to exploit a vulnerability in the cPanel service, enabling them to gain privileged access to resources.

Domain	cPanel	WordPress	Technology
totalmassasje.no	❌	✅	HTML+PHP
infomegaware.com.br	✅	?	PHP
cgw.ge	✅	✅	PHP
signitivelogics.com	✅	✅	HTML
literaturaelsalvador.com	✅	✅	HTML
simplesalsamix.com	✅	✅	PHP->HTML
remcolours.com	✅	✅	PHP
resetlocations.com	✅	✅	HTM
Total:	7	7	

Figure 10. Technologies and service providers appearing in the attacks — own elaboration

There is one more notable feature linking the compromised sites. Most of the sites used in the attacks are based on open-source CMS (Content Management System) solutions — the WordPress content management system. Here, it is important to remember that apart from the base engine code WordPress has an extensive functionality allowing the installation of various add-ons and themes. Analysis of published vulnerabilities in the WordPress engine has shown that there is little likelihood of it being used to take control of a website. In the case of add-ons, the situation is quite different. Due to the open-source nature of WordPress and the fact that anyone can create an add-on, it must be borne in mind that add-on quality varies. Considering the above, if one assumes that WordPress is the input vector for the attacker, it should be assumed that it is add-on (plugin) vulnerabilities that are attacked, and not the WordPress engine itself.

At the time of writing, the Foreign Intelligence Agency did not have satisfactory evidence to conclusively identify the attack vector used to take over websites that are then used to distribute malware.

For more information on the tools and other campaigns carried out by APT29, see "Espionage campaign linked to Russian intelligence services", a publication prepared by Military Counterintelligence Service and CERT Polska (NASK CSIRT) analysts.[10]

Chinese APT groups as a source of attacks targeting NATO countries

Another source of threat to Western IT systems apart from Russia is China. Despite its officially declared neutral position on the war in Ukraine, Beijing has a strong interest in weakening the West. Together with Moscow, it is seeking to change the international order, which, according to both capitals, favours the United States and Europe. The emergence of the so-called multipolar world is seen by Russia and China as an opportunity for their own development. Further, many researchers have noted that Beijing's interest in the West's response to the Russian invasion of Ukraine may be an attempt by the Chinese to gauge possible foreign reaction to a potential attack on Taiwan.[11] Other than vying for influence, China seeks to erode the scientific and technological superiority of Western countries in many fields, particularly industry and high technology.

Beijing believes the above priorities can also be met through cyberwarfare. State-sponsored hackers are tasked with acquiring information ranging from political to trade secrets to patents and other types of intellectual or industrial property. This data is intended to give China a political and economic advantage on several fronts in the race against others, particularly against the United States, but also Europe.

[10] https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi (accessed 31 August 2023)
[11] Source: https://www.japantimes.co.jp/news/2023/02/19/asia-pacific/ukraine-war-anniversary-taiwan-comparison/ (accessed 31 August 2023)

A February 2023 publication by the European Union Agency for Cybersecurity (ENISA) and CERT-EU included a warning of increased activity by Chinese hacking groups APT27, APT30, APT31, Ke3chang, Gallium and Mustang Panda. The institutions urged all European public and private sector entities to take action to reduce their risk of exposure to potential cyber-attacks. The activities of the groups focus on stealing sensitive information through such means as spearphishing campaigns focused on Russia's war against Ukraine.

Figure 11: Mustang Panda Group and related names — own elaboration based on available data

Mustang Panda (a.k.a. EarthPreta, BronzePresident, CamaroDragon) is a hacking group that has been active since at least 2017 and is primarily involved in data theft and state and corporate espionage. It uses advanced tools and techniques such as spearphishing and exploiting software vulnerabilities. Its targets include primarily energy, industrial and defence sector companies. The group is considered one of the more active and technically advanced in China.

[12] Source: https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication (accessed 31 August 2023).

Figure 12: Countries affected by attacks by APT Mustang Panda — own compilation based on available data

In January 2023, ESET specialists detected a new backdoor, believed to be used by the Mustang Panda group, and named it MQsTTang. It allows remote command execution on a device and the capture of data input (keylogger). It is being used as part of a spearphishing campaign targeting actors in Europe, Asia (including Taiwan) and Australia. Notably, in the case of Taiwan, the attack was directed against a government institution, and given Taiwan's tense relations with China, this leads us to believe that Chinese hackers are responsible for APT campaign.[13].

Attacks on diplomatic facilities attributed to Chinese APT groups

Despite the advanced technological capabilities displayed by the Mustang Panda group, it appears that its activity against Poland remains low. Phishing campaigns targeting Polish diplomatic missions are scarce and are usually part of larger-scale operations targeting numerous NATO countries. This is likely because the APT group in question is focused on carrying out other, more important tasks.

One campaign attributed to Mustang Panda, which also targeted Polish diplomatic offices abroad, took place in February 2023. Using email accounts set up on Outlook.com, the group distributed a message designed to encourage the victim to click

[13] Sources: securityweek.com, cyberdefence24.pl, enisa.europa.eu, blogs.blackberry.com (accessed 31 August 2023)

on a link and download malware. The message itself included a request for information for an international project. An interesting factor is the mechanism used to insert the link in the message: the attacker used a technique to hide the actual link under the text. With this procedure, the victim is typically prompted to "Click HERE", with the malicious link being located under the word "HERE".

```
<ahref=3D"https://www.midasconsilium.com/Section III of the Work plan of the
Danube Commission for the period from lS January 2023 to 31st December
2023.zip">https://1drv.ms/b/s!AlnWqYjBbeyVaUey24BS5iYzVmM?e=3DfP4TL5</a>
```

Ilustracja 13. Tag HTML wykorzystany do wstawienia linku – opracowanie własne na podstawie dostępnych danych

In this campaign, the attacker chose to generate two links. The first initiated the download of malware and the second led to a harmless document hosted on OneDrive. This was meant to prevent the malware from being discovered too quickly. Perhaps the attacker hoped that a less experienced user would copy the displayed text pointing to the harmless file instead of the actual target link when referring the link to verification.

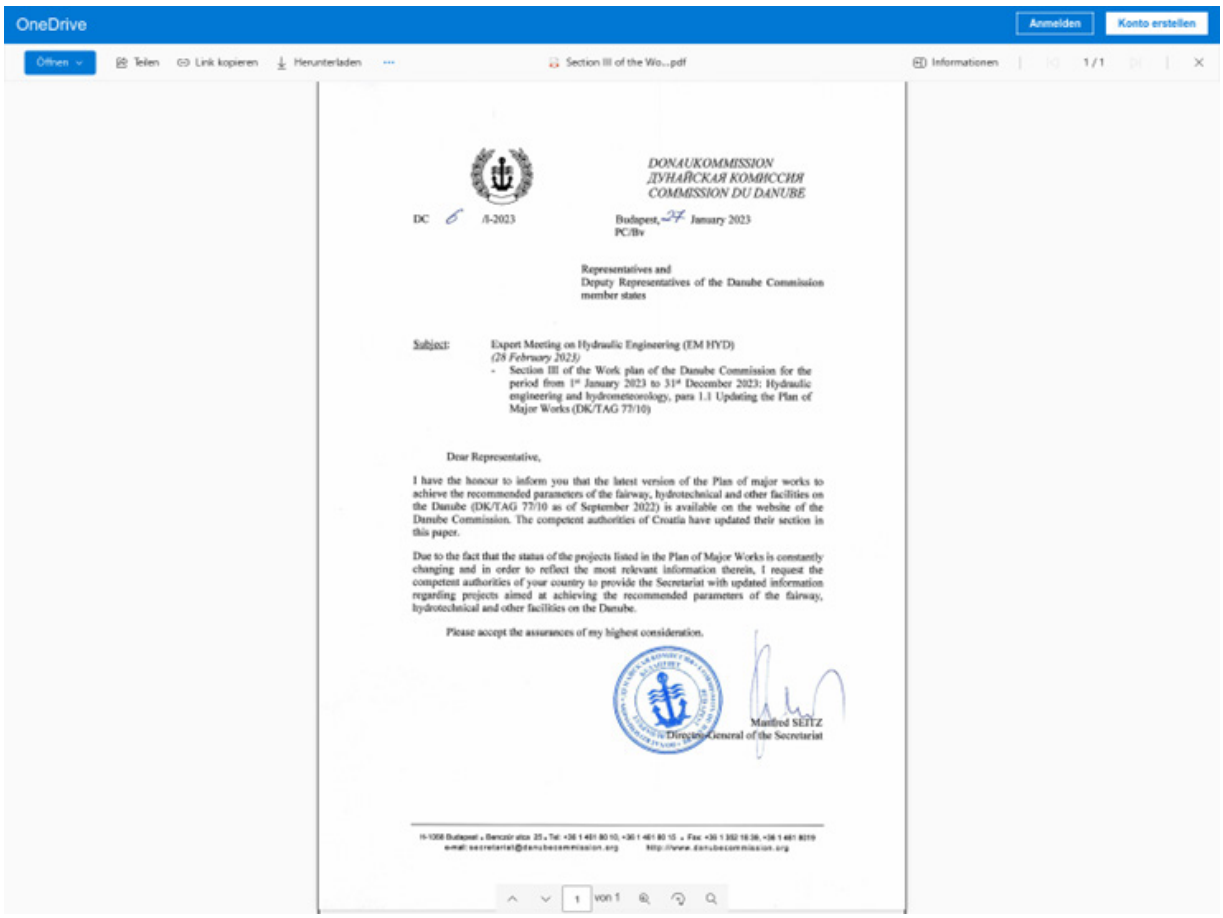

Figure 14. OneDrive page containing the harmless document that was displayed if the link was copied — own elaboration based on available data

Clicking on the link would commence the download of a file named "Section III of the Work plan of the Danube Commission for the period from lS January 2023 to 31st December 2023.zip". When unzipped, it turned out to be another instalment of the well-known PlugX malware that had been used before. Qualified as a RAT (Remote Access Trojan), this software allows the attacker to take control of an infected computer and steal data. PlugX is also used in other Mustang Panda campaigns. This may suggest that one of its main purposes is to steal data, which could prove to be a valuable source of information about the other country's business relationships or technologies.

Proactive measures to prevent the consequences of attacks on Polish government institutions, including diplomatic missions

Poland is likely to remain the target of attacks by groups sponsored by foreign governments, particularly Russia. They are symptomatic of hybrid warfare activities against states supporting Ukraine, among which Poland plays a special role. The activity of these organisations may be particularly dangerous in view of the upcoming parliamentary elections in Poland (autumn 2023). To address the increasing scale of hacking attacks, alert level Charlie CRP has been introduced and has remained in effect since February 2022, enabling cyberspace threats to be tackled more effectively.

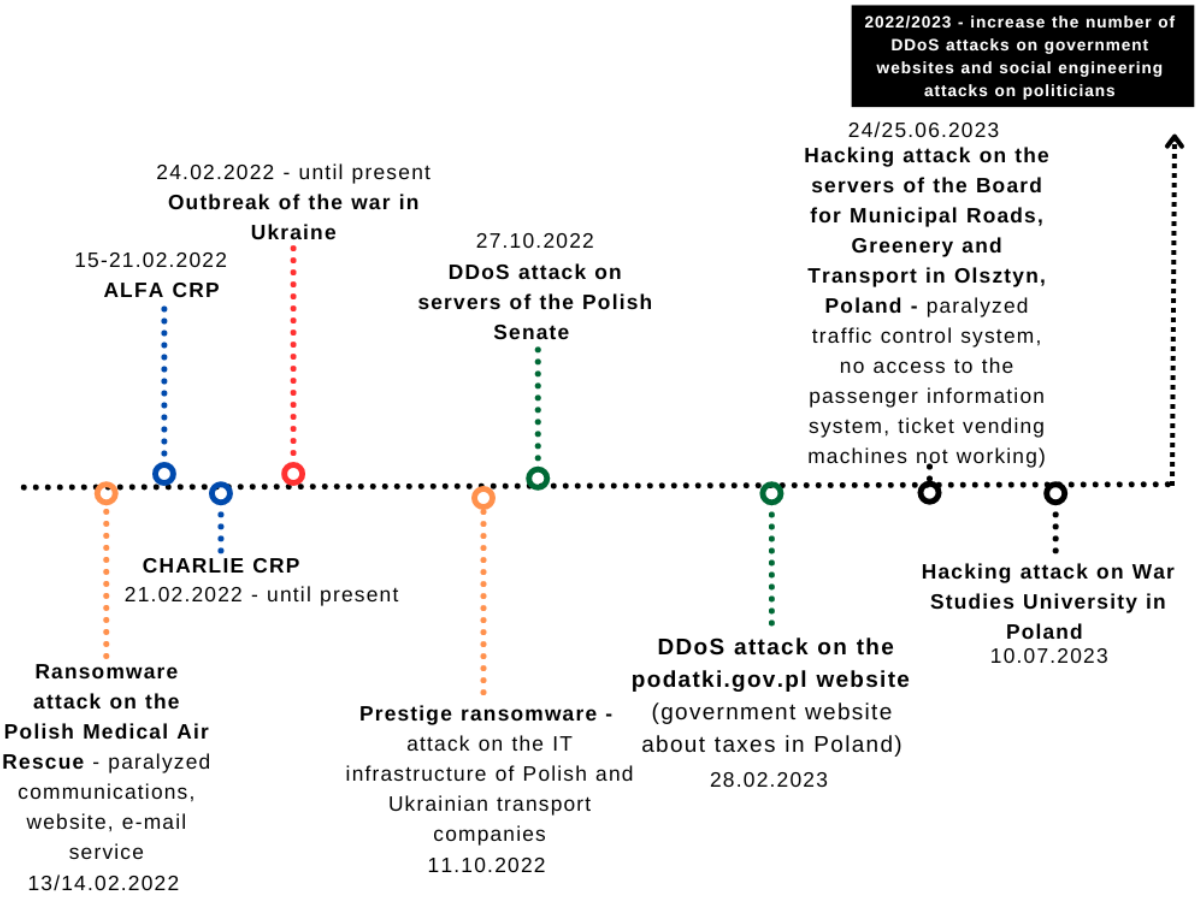

Figure 15: Selected events related to the introduction of alert levels in Poland — own elaboration based on available data

Currently, the most critical task is to continue safeguarding Poland's critical services, infrastructure and supply chain (as evidenced by the October 2022 Prestige ransomware attack)[14], also in terms of assessing the security practices of software providers. Appropriate standards such as Zero Trust, Security by Design and Defense in Depth are needed to ensure the appropriate level of security for the Polish ICT infrastructure.

The Ministry of Digital Affairs is carrying out many activities to counter threats to Poland's cyber security, including:

- The PWCyber Cybersecurity Cooperation Programme — a collaboration between the public and private sectors, involving more than 30 technology sector companies, with more gradually joining. It organises training, workshops and knowledge-sharing,[15];
- regular studies on cyber threats and organising security awareness training,
- coordinating activities at the national level, including by providing tools for secure overt and covert communication and organising regular meetings on the state of security,
- participating in numerous international cybersecurity initiatives such as the Counter Ransomware Initiative.

The capabilities of CSIRTs at the level of national security cells in government institutions, the knowledge and experience of their experts and the tools available to them make it possible to secure ICT infrastructure and respond immediately to new threats. Protecting diplomatic missions from incidents compromising integrity, data access and confidentiality involves equipping them with tools to protect ICT systems. The analyses concerning the functioning of the National Cyber Security System point to a need for an entity dealing with the protection of units subordinate to or supervised by the Minister of Foreign Affairs, as well as the MFA itself. The list of institutions whose cyber-security could be supervised by such an entity would include Poland's diplomatic missions around the world, as well as such organisations as PISM (Polish Institute of International Affairs) and PLSZ (Foreign Medical Service).[16]. **An entity such as the CSIRT INT could support the aforementioned institutions in the incident handling process, and its establishment would play an important role in enhancing the cyber security of the Republic of Poland.**

[14] Source: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-inukraine-and-poland/ (accessed 31 August 2023)
[15] Source: https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publicznoprywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa (accessed 31 August 2023)
[16] Based on data from: https://www.gov.pl/web/diplomacy/units-subordinate-supervision (accessed 31 August 2023).

It is planned to further improve Poland's resilience to cyber-attacks, with a particular focus on securing the government sector, including diplomatic missions. The main objectives in this regard include the strengthening of Cyber Threat Intelligence teams at the national level (in the context of implementing pre-emptive actions) and the further development of a channel for the exchange of information on new threats between individual institutions within the National Cyber Security System. Cyber security is a team effort, which is why deeper cooperation between the public and private sectors, including SOCs and CSIRTs at the national level, as well as the sharing of information at hand, is a necessity. This is because all these organisations pursue a common goal which is ensuring the security of the Republic of Poland and its citizens.

Due to the highly dynamic nature of cyber activities, information quickly becomes outdated. Consequently, incident response must be quick, yet thoughtful (especially when attribution is difficult). It is important to build combined (modular) teams to enable specialists from different institutions to work together in the event of a particularly complex incident. One example of such activities is the Locked Shields exercise — in its 2023 edition, the Polish team once again took a place on the podium, in no small part thanks to the cooperation of specialists from various government and private sector institutions.

Bearing in mind the current unstable situation in the East and the numerous hacking attacks targeting Poland, the shortest possible decision-making paths should be used to allow rapid action in the face of a threat. Authorised institutions should also bolster their active cyber defence measures serving as a deterrent.

Summary

„We, the Heads of State and Government of the North Atlantic Alliance, bound by shared values of individual liberty, human rights, democracy, and the rule of law, have gathered in Vilnius as war continues on the European continent, to reaffirm our enduring transatlantic bond, unity, cohesion, and solidarity at a critical time for our security and international peace and stability. NATO is a defensive Alliance. It is the unique, essential and indispensable transatlantic forum to consult, coordinate and act on all matters related to our individual and collective security. We reaffirm our iron-clad commitment to defend each other and every inch of Allied territory at all times, protect our one billion citizens, and safeguard our freedom and democracy, in accordance with Article 5 of the Washington Treaty. We will continue to ensure our collective defence from all threats, no matter where they stem from, based on a 360-degree approach, to fulfil NATO's three core tasks of deterrence and defence, crisis prevention and management, and cooperative security."

NATO Summit in Vilnius, 11–12 July 2023. [17]

This publication briefly characterises the threat posed by hostile hacking groups to the diplomatic missions of NATO countries. By no means are their attacks isolated incidents: they are a continuous campaign targeting various countries of the Alliance. Data from the Ministry of Digital Affairs shows that the number of reported incidents in Poland in 2022 increased by around 62% in the government sector and by around 178% in the civilian sector compared to 2021. The year 2022 also brought a 61% increase in the number of phishing attacks. Another challenge is DDoS attacks, which have recently posed a constant threat to NATO countries, including Poland. The attacks aim to disrupt the availability of websites, online services and servers in both the government and private sectors. In this regard, it is crucial to further strengthen the ICT infrastructure of individual institutions and to invest in anti-DDoS protection tools. Notably, in the first seven months of 2023 alone the NASK CSIRT handled more incidents than in the whole of 2022. An increase in the popularity of cybercrime tools and cybercrime-as-a-service (e.g. the possibility to buy ready-made malware or ransomware services online) has also been observed. As such, in terms of attacks, the cyberspace pressure is expected to remain high. At present, it is impossible to say whether there will be an escalation of such activities.

[17] Source: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (accessed 31 August 2023).

Nonetheless, it is possible that if interest in Ukraine as the main target of attacks declines, the West may well see a greater proportion of threat actors and resources be redirected against it.

In this context, it is necessary to continue to take preventive measures to secure the ICT infrastructure, to strengthen cooperation between member states and to use modern technologies to combat such threats. At present, one of the main tasks is to maintain NATO's defence capabilities and to strengthen cooperation in the field of cyber security to ensure effective protection against hacking attacks that may threaten the unity, stability and security of the Alliance and its founding values.

As a committed member of NATO, Poland plays an important role in promoting unity, cohesion and solidarity in the region. Its strategic geographical location makes it an important player in the defence of NATO's eastern flank. Poland participates in efforts to promote stability in the region and counter hybrid warfare threats, including hacking attacks. Effective cyberspace defence requires an integrated approach and cooperation of individual countries, government bodies and private companies so that the "iron-clad commitment to defend each other and every inch of Allied territory" remains our common, overarching goal.

Ministry of Digital Affairs
Republic of Poland

Department of Cybersecurity

FOREIGN INTELLIGENCE AGENCY

Serving Poland in the shadows