CYJAX

Digital Intelligence
Securing the Future

Poland: The Increasing Threat of Cyber Attacks

Internet users within Poland have freedom of expression, with government legislation protecting this right by law. According to Statista 90% of households[1] within the country had internet access in 2020, reflecting the average across the European Union.

The Polish National Cyber Security Strategy (2017-2022) is currently in force[2]. Poland is also a signatory to the Council of Europe's Convention on Cybercrime. However, the government is aware that further investment is needed to improve the cyber defence capabilities of the country; there is also an acknowledgement that new legislation will be required to ensure the successful implementation of any new measures.

A 2022 survey called "Cyber Security Barometer,"[3] carried out by the global consultancy KPMG, found that since 2021, 29% of Poland's businesses have been the subject of at least one cyberattack. This marks a 5% increase compared to 2020, indicating that cyber threats and cyberattacks in the country are rising. Cyberattacks worldwide have been rising in recent years, with the UK seeing a 40% increase in attacks, as well as there being a reported 8% rise[4] in cybercrime globally, making Poland's 5% increase in cybercrime below the world average. It should be noted, however, that these statistics are based only on reported cybercrimes, and the number is likely much higher when accounting for unreported attacks.

Many reported cyber incidents in Poland tend to concern malware attacks, including rootkits, trojans, viruses and dialers. Cybercriminals are increasingly deploying various types of ransomware, and also frequently launch malicious/phishing campaigns. One frequently observed attack is the use of a well-known brand name to send out supposed invoices, documents or notifications which contain files infected with varying types of malware. Highprofile scams that have appeared in recent years include one that utilises Facebook, asking victims to transfer money using the BLIK mobile payment system, and a second impersonating payment operators DotPay and PayU.[5]

There are also other issues faced by those using the internet. Spam, hate speech and piracy are all common malicious cyber activities carried out in the country. A trend has been seen in which the scale of threats has only grown year-by-year, something which will likely continue. Online harassment was perceived as one of the most extreme risks in Poland in 2020, with users being concerned about how personal and professional reputations would be viewed[6] because of this. There is also a particular risk of illegal and harmful content: while this threat is obviously not exclusive to Poland, there are concerns about pornographic, neo-Nazi, xenophobic and racist materials, pointing to a potential link with extreme right-wing groups.

In February 2022, Russia began its invasion of Ukraine[7], resulting in large numbers of refugees fleeing to surrounding countries, including Poland, to evade military strikes. The invasion of Ukraine not only started the first major war in Europe since World War II, but it also resulted in the initiation of a large-scale cyberwar. The ruling party of Poland has also been at the forefront in trying to persuade the international community that a robust response is needed to Russian President Vladimir Putin. The party sees his policies and governing as neo-imperialist and de-stabilising for central and Eastern Europe. The government has been vocal in stating that EU sanctions on Moscow must be maintained and extended further. These views have put them in the line of fire for threat actors participating in cyberwarfare.

The cyberwar started on a small scale, with the first big attack being in January 2022[8] when a huge cyberattack targeted Ukrainian government websites including the foreign ministry, the cabinet of ministers and the security and defence council, among others. The attacks delivered the WhisperGate[9] malware, a new wiper which posed as ransomware and rendered affected systems inoperable. This was later discovered to be an attack by @UNC1151, which is thought to be linked to the Belarusian intelligence service, with the attack said to be "just a cover for more destructive actions that were taking place behind the scenes." This group has also been known to target organisations in Poland, Lithuania, Latvia and Ukraine in the past to disseminate anti-NATO information. Following WhisperGate, a host of other similar wipers were discovered targeting Ukraine, including HermeticWiper[10], IsaacWiper[11], and CaddyWiper[12].

Once the physical war started in February 2022, the cyberattacks between Ukraine, Russia, and other countries on either side of the conflict increased greatly. In response, Ukraine created the "IT Army of Ukraine,"[13] which anyone could join to help the Ukrainian cause and conduct various cyberattacks against named Russian targets. These attacks mostly involve hacktivists, such as those who claim to be affiliated with the @Anonymous collective. There is no doubt that their activities have caused a great deal of damage to Russian organisations: major government sites have been taken offline by DDoS attacks, and many damaging data leaks have been seen. The attacks continue.

Pro-Russia groups are also active and these hacktivists have expanded their attacks from Ukraine to neighbouring countries deemed not to be supportive of Putin's actions. For example, @Killnet was observed conducting DDoS attacks on a series of government and financial organisations in Romania, and targeted institutions and NATO sites in Poland[14], Estonia, the Czech Republic, and the US. In May 2022, the Polish Prime Minister disclosed an increase in DDoS attacks[15] targeting domestic institutions in the country: these could cause difficulties in accessing services provided via websites. Russian hacktivist groups have openly admitted to these attacks. So far, however, they do not appear to have had any major or large-scale impact on Polish organisations.

Misinformation has also become an issue within Poland since the start of the Russia-Ukraine war. One day after the outbreak of the conflict, leader of the Confederation alliance Pawel Wyrzykowski wrote on Twitter[16] about Ukrainian refugees stating "*It will not be hands to work, but mouths to feed, beggars with absolutely no accumulated capital to undertake productive labor. On their side will be the media, emotions and international law as well as PiS wanting to give them 500+ and maybe even citizenship.*" PiS refers to leading political party of Poland, Law and Justice. Wyrzykowski leads the parliamentary coalition between two radical parties, including the National Movement. He tried to justify these views by stating he was just expressing how he thought Polish citizens would react to Ukrainian refugees. Claims that the refugees would have a negative impact on the Polish economy have become part of nationalists' attacks against them, alongside allegations that they are allegedly being favoured by state institutions. Many nationalists have been very active on social media, including YouTube, to spread these kinds of ideology, along with basic misinformation. A similar instance was seen when the Covid-19 pandemic first occurred, where the right-wing replaced initial solidarity and mobilisation with conspiracy theories and xenophobic sentiments. This trend has been noted by Rafal Pankowski, the head of racism monitoring organisation Never Again[17].

Other, general cyber-related incidents have directly affected Poland since the start of 2022 including malware and APT attacks, distributed denial-of-service (DDoS) attacks, and data leaks.

In July 2022[18], North Korean state-sponsored threat group APT37 conducted a new campaign named STIFF#BIZON, targeting high-value organisations in Poland, the Czech Republic and other countries to distribute the Konni RAT. This attack used phishing emails to deliver malware, with decoy documents posing as a report from Olga Bozheva, a Russian war correspondent. Once on the system, the Konni RAT could steal data, screenshot, bypass MFA, extract saved credentials, execute commands, and deliver additional files. It was stated that while the TTPs and toolset of this campaign point to APT37, there is a possibility that Russian threat group APT28 (aka FancyBear, Sofacy etc) is responsible for it. This is due to a direct correlation between IP addresses, hosting providers and hostnames between this attack and historical data from APT28. APTs sometimes attempt to mimic the TTPs of other threat groups in order to confuse researchers and obscure their actions. APT37 is one of the North Korean General Reconnaissance Bureau groups that has been actively conducting surveillance operations since 2012. The group has been known to use the Nokki and Konni RATs in the past against European organisations. APT28 is a Russian state-sponsored group that has been linked to the GRU, Russia's Military Intelligence Service. The group has been active since at least 2014, and poses a serious threat to political, military and security targets, specifically looking to gather sensitive information of use to the Russian government. It has been actively involved in attacks against European countries that support Ukraine in the ongoing Russia-Ukraine war.

In June 2022, Cloudflare mitigated a record-breaking DDoS attack[19] aimed at an unnamed customer website. This attack peaked at 26 million requests per second (RPS), with each node generating approximately 5,200 RPS. The attack was attributed to the Mantis botnet, which is made up of 5,000 bots, and has targeted internet and telecommunications, media, gaming, finance, business, and retail organisations in Poland, the US, Russia, Ukraine and other countries.

Also in June, researchers uncovered a new IIS module backdoor named SessionManager[20], designed to take seemingly legitimate but maliciously crafted HTTP requests, triggering certain actions to pass onto the server to be processed. The malware could read, write and delete arbitrary files on the server as well as remotely execute code. It has been used to target NGOs, government, military and industrial organisations in many regions, with Poland among the countries affected. This activity has been attributed to cyber-espionage group @Gelsemium.

A series of phishing campaigns dubbed DarkCasino[21] targeting online gambling platforms to steal transaction credentials and for monetary gain was also uncovered in June. The attacks were linked to the @Evilnum threat group, with two new malware, DarkMe and PiccoloRAT (PikoloRAT), being delivered. European countries such as Poland, Malta, Cyprus, and Spain are the main targets of the campaign. The @Evilnum threat group has been in operation since at least 2018, targeting finance and technology companies globally. The group works for financial gain and uses a mix of custom-built and purchased malware in its attacks. Its use of spear-phishing emails that include stolen documents as the primary initial infection vector. Once a target has been successfully infiltrated by @Evilnum, the group will maintain access for long periods, siphoning off sensitive data. It is likely that it will continue these types of attacks to steal data and money.

In May 2022, researchers identified the distribution of a new iteration of the ERMAC Android banking trojan[22], ERMAC 2.0, targeting Polish users and mainly observed being deployed through fraudulent websites, masquerading as popular food delivery platforms and fake browser updates. Analysis of the original ERMAC code has enabled researchers to conclude the malware is a variant of the Cerberus family. Cerberus became open source when its code was leaked online in 2020. Most applications this malware targets are either banking or cryptocurrency related.

In February, the BRATA Android malware[23] added new features and began targeting online banking users in Poland, the UK, Italy, Spain, China, and Latin America. Each BRATA variant focuses on different banks and has dedicated overlays, languages, and apps to target specific users. New features in the most recent version of the malware include a keylogging functionality, GPS tracking, and the ability to perform factor resets if a virtual or analysis environment is detected or if the compromise has successfully been completed. The BRATA malware was first uncovered targeting Brazilian users in August 2019. Since then, it has moved to mainly targeting Italian users, but the new variant and attacks show that it has expanded its targeting to include more countries worldwide.

In January 2022, a copy of the Polish Army's inventory[24], which included a variety of information such as details about the country's stock of laptops, anti-tank missiles, F-16 jets and more, was leaked online. A statement from the Polish Ministry of National Defence stated the information contained in the database was not classified and could be accessed through public records: it had previously been published by NATO as part of the Master Catalog of References for Logistics (NMCRL) database. An independent Polish cybersecurity organisation verified that no sensitive or classified information was stored in the dataset. Confusion around the leak stemmed from the database having been posted and discovered on Raid Forums, something which law enforcement authorities were investigating. From images posted by the source, the threat actor appeared to be unaware of the significance of the information they posted online, although they did understand that the content was related to military and defence issues.

In December 2021, Poland rejected[25] accusations that it had used the Pegasus spyware[26], made by Israeli company NSO Group, for political reasons. The allegation came from Roman Giertych, a lawyer involved in several cases against the ruling Law and Justice (PiS) party, who claimed that Poland was using the spyware "to fight the democratic opposition". It was suggested that the use of the spyware affected the outcome of democratic elections, as it was used ahead of the parliamentary elections in 2019. Ewa Wrzosek, a prosecutor and opposition figure, also claimed that the spyware was used on her, and that she had been alerted to it by Apple. Canadian cybersecurity company Citizen Lab also investigated the use of Pegasus against the two individuals and found that both had been repeatedly infected with the spyware. Pegasus allows the controlling user to read messages on the infected device, as well as look at photos, track location, and turn the camera on without their knowledge. NSO Group states that it only sells the spyware to "legitimate law enforcement agencies who use these systems under warrants to fight criminals, terrorists and corruption".

Following the rejected accusations, Polish government official Jaroslaw Kaczynski admitted to the government purchasing Pegasus spyware[27]. Amnesty International then verified that Polish senator and opposition leader[28], Krzysztof Brejza, was targeted with the spyware. In the build-up to the 2020 presidential election, Brejza was subject to a smear campaign that involved state-controlled TV stations aired texts which had been stolen from his device and manipulated. Kaczynski claimed that the Pegasus tool was used by Polish security services to tackle crime and maintained that surveillance did not play a role in the conservative party's 2020 election victory.

NSO Group has long been accused of being complicit in the use of its technology to target human rights activists, journalists, and others. Its clients include governments and law enforcement agencies worldwide. Most notably, the Pegasus spyware is said to have been used against New York Times and Washington Post journalists, Jeff Bezos (who owns the Post), and the murdered Washington Post columnist, Jamal Khashoggi. The company claims that it is not responsible for the actions of its "sovereign customers". In the past, this defence has proven sufficient for it to deflect the attentions of the press.

Moving away from cyber threats, the EU is currently under pressure to deescalate its rule of law conflict[29] with Poland's ruling party. The EU seeks to preserve unity among its member states; however, Poland is alleged to have violated the bloc's essential principles and is in dispute with EU institutions. The conservative-nationalist party, PiS, enacted several reforms upon gaining power in 2015. This included changes being made to the judiciary system[30], undermining its independence, and representing a violation of the EU's core values. This issue has led to Poland not receiving its EU coronavirus recovery fund national reconstruction plan (KPO) money. The two sides have recently reached an agreement whereby €34.5 billion in grants and loans that has been allocated to the country as part of the fund is being conditionally released in tranches as Poland fulfils set 'milestones', including dismantling of the supreme court disciplinary chamber, creating a new disciplinary system for judges, and a review of the cases of those judges previously sanctioned by the chamber. This new agreement[31] has been made due to Poland being a critical geographical location for the response to Russia's invasion of Ukraine; it should allow order and solidarity to be maintained in the face of the threat. The country has been the main channel for sending military and humanitarian aid to Ukraine and has taken in more than 3.5 million refugees. The latest agreement has been greatly scrutinised by the European Parliament and many anti-Law and Justice experts, who have described it as a short-term political deal, and have argued that the milestones set out are too vague and open to political interpretation. The payments of the coronavirus fund will not be made until late 2022, or early 2023, however, to give the EU time to assess whether the milestones are being met. While an agreement has been met, interpretation of the agreement and ongoing reforms could result in tensions and conflict between the EU and Law and Justice. Law and Justice is keen to end the current conflict as it needs the coronavirus recovery funds to improve its chances of re-election in the 2023 elections; it believes they money would help both as a financial investment and to reduce the rate of inflation, which has reached a high of 15.6%. Once the funds are received and the election has taken place, however, it is unclear how the party will continue with its state reforms. It is under pressure from 'Solidaristic Poland' (SP), its junior governing partner, which believes that the prime minister is already making too many concessions to the EU. Nevertheless, the Polish government does not apparently want to push the issue further at this point and is prepared to compromise so long as its core principle of the judicial reform programme, allowing politicians more say in determining key judicial bodies, is not abandoned.

Poland's prime minister also recently assured the public[32] that there will be sufficient supplies of natural gas and coal in the country, with current importing problems being attributed to the ongoing war with Ukraine. This, along with the increase in inflation, has resulted in a rise in public dissatisfaction with the current ruling government. Poland's inflation rate is at the highest that it has been in the last 25 years, with the prices of gas and coal also greatly increasing, tripling since imports were cut and sanctions were imposed on Russia. The government has introduced lower and more regulated prices for households and ordered state energy organisations to make urgent purchases of coal for individuals, rather than them solely being directed towards industry needs. It has also stated that supplies will be sufficient for the winter months, as Poland has purchased coal from many countries to deal with the shortage. These measures have been introduced to combat the ongoing discontent with the government, as polls suggest that Law and Justice could lose its parliamentary majority in next year's election, which would hinder it from implementing its policies.

If Poland experiences an energy supply crisis in winter 2022/23, the chances of PiS being re-elected will significantly decrease, which, according to an analysis by Fitch Solutions[33], raises the likelihood of a coalition between Civic Platform, Poland 2050 and Polish Coalition. However, Fitch Solutions believes that PiS will remain the largest party in the upcoming election, despite being unlikely to win an outright majority. If Law and Justice was to advance the election and have it take place now, the party would likely benefit from current highs in anti-Russia sentiment in the country, as well as serve as vindication for its wary stance towards Russia. Poland's emergence as a key member of NATO and top defence spender in the region is another factor in favour of Law And Justice. Worsening economic conditions are likely to undermine its support levels, however, which will allow opposition parties to use this to garner more votes and lose faith in the ruling party before the election in August 2023.

While there has been an increase in cyberattacks in Poland overall, these have been seen across a variety of sectors, and are not localised to one specific set of targets or types of attacks. It is possible that there may be an increase in cyber threats to Poland during the run up to the election in August 2023. In the past, threat actors have sought to disrupt elections or mislead voters with disinformation campaigns. Dissemination of false information can greatly affect elections, especially when social media is weaponised, allowing a much wider audience to be easily reached. Facebook is the most popular social media platform in Poland and is largely used by both domestic and international actors attempting to influence Polish politics. A research report by the Oxford Internet Institute[34] found that Poland was very vulnerable to disinformation campaigns seen on Facebook and Twitter in the run-up to the 2019 European Parliament elections, with users sharing more fake than real news. Some disinformation that has been widely spread around the country includes that Jarosław Kaczyński pledged loyalty to the Polish Communist Party in the early 1980s, and that that PiS politicians are profiting by privatising tenement houses in Warsaw. Furthermore, Polish newspapers and TV[35] are dependent on advertising spending from state-controlled companies, which could also be used to spread a selective narrative favouring the current governing party; PiS has expanded this channel of influence by significantly increasing ad spending by state-controlled companies, as well as being in control of Poland's largest TV network, Telewizja Polska. This type of cyber threat is likely to have the biggest impact on the elections, although it is possible that threat actors who oppose the various government parties will conduct more destructive attacks, such as data theft and leaks, or malware attacks.

Ransomware could also pose a real threat to online systems related to the elections if networks are not correctly secured and are accessible. Past use of the Pegasus spyware prior to the 2019 elections could be of detriment to the PiS in the upcoming election, as if citizens do not believe that the result of the election was fairly obtained, it could lead to further strife and turmoil internally within Poland.

Travellers to Poland, and those working there, should avoid using public WiFi spaces: these can leave all device data unsecured as no authentication is required to establish a network connection. Accessing the internet via unknown and unsecured WiFi can result in the theft of personal and sensitive information, including emails, credit card information, and credentials. These hubs can also be used for malware distribution if file-sharing is allowed across a company network. If a user must connect to a public WiFi network, a VPN should be used at all times to encrypt data and stop attackers from abusing stolen information without having to decrypt it first, often a lengthy process the attackers would not undertake. Users should also avoid clicking unknown links or pop-ups while browsing to avoid potentially installing malware on the device or disclosing sensitive data.

It is also advised that people travelling to or working in Poland do not disclose their plans or location on social media networks. Added risk comes from having location services turned on on phones and allowing the device to be tracked, so these should be turned off on smart devices. Users should also not publicly record activities on platforms such as Strava. Users can consider taking a dumbphone or non-smart phone if possible on shorter trips where a smart phone is not needed. They should also consider the dangers of using potentially compromised applications such as TikTok on work devices. The UK Parliament recently shut down its TikTok account[36] following raised concerns about data being passed to the Chinese government, as TikTok is a Chinese-owned application. Despite TikTok owners ByteDance denying being controlled by the Chinese government, the Parliament’s account has been closed until the company can provide “credible assurances” that no data could be handed to authorities in Beijing. In addition, China and Russia are allies, so any data being passed to the Chinese government has the risk of potentially being shared with Russia, and with Poland being at the forefront of the countries speaking out against President Putin, it could be a target for such intelligence-sharing operations.

In conclusion, our assessment is that there is a medium but increasing risk of cyber threats in Poland, particularly in the run-up to the elections in 2023.

Jovana Macakanja
Intelligence Analyst

Endnotes

[1] https://www.statista.com/statistics/1036205/households-internet-access-poland/

[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013/

[3] https://home.kpmg/pl/pl/home/insights/2022/05/barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci.html

[4] https://www.thenationalnews.com/business/technology/2022/05/08/cyber-crime-rate-in-the-uk-higher-last-year-than-in-other-developed-nations/

[5] https://www.statista.com/topics/5582/cyber-crime-and-cyber-security-in-poland/#dossierKeyfigures

[6] https://www.statista.com/statistics/1098103/poland-most-painful-online-risks/

[7] https://euobserver.com/world/154422

[8] https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/

[9] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[10] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

[11] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[12] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

[13] https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/

[14] https://www.sri.ro/articole/atacuri-cibernetice-asupra-site-urilor-unor-institutii-publice-si-financiar-bancare.html

[15] https://regiony.tvp.pl/60015379/rzad-o-cyberbezpieczenstwie-zwiekszyla-sie-czestotliwosc-cyberatakow

[16] https://twitter.com/WyrzykowskiP/status/1497126268948656128

[17] https://balkaninsight.com/2022/06/15/polish-nationalists-weaponize-history-in-bid-to-remain-relevant/

[18] https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

[19] https://blog.cloudflare.com/mantis-botnet/

[20] https://securelist.com/the-sessionmanager-iis-backdoor/106868/

[21] http://blog.nsfocus.net/darkcasino-apt-evilnum/

[22] https://blog.cyble.com/2022/05/25/ermac-back-in-action/

[23] https://www.malwarebytes.com/blog/news/2022/02/android-malware-brata-can-wipe-devices

[24] https://therecord.media/polish-government-downplays-leak-of-military-logistics-data/

[25] https://www.securityweek.com/poland-rejects-accusations-political-spyware-use

[26] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[27] https://www.clickondetroit.com/news/2022/01/07/polish-leader-admits-country-bought-powerful-israeli-spyware/

[28] https://www.securityweek.com/rights-group-verifies-polish-senator-was-hacked-spyware

[29] http://yris.yira.org/comments/5569

[30] https://rm.coe.int/fourth-evaluation-round-corruption-prevention-in-respect-of-members-of/1680a3efa8

[31] https://blogs.lse.ac.uk/europpblog/2022/07/08/how-will-the-russia-ukraine-war-affect-polands-rule-of-law-dispute-with-the-eu/

[32] https://www.cnbc.com/2022/07/23/polands-leader-seeks-to-assure-public-of-energy-security.html

[33] https://www.fitchsolutions.com/country-risk/worsening-economic-outlook-threatens-polish-governments-re-election-2023-26-07-2022

[34] https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/EU-Data-Memo.pdf

[35] https://cyber.fsi.stanford.edu/news/poland-scene-setter

[36] https://www.bbc.co.uk/news/uk-politics-62410234

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

CYJAX

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com

bsi
ISO/IEC 27001 Information Security Management CERTIFIED
IS 676012