SEQ

SEQ RESEARCH

RUSSIA CYBERWAR AGAINST UKRAINE 2022

www.seq.lv

SEQ RESEARCH

RUSSIA CYBERWAR AGAINST UKRAINE 2022

WWW.SEQ.LV

RUSSIA CYBERWAR AGAINST UKRAINE

TABLE OF CONTENTS

INTRODUCTION 7

CHAPTER 1: RUSSIA ATTACKS ON UKRAINE (CYBERATTACKS).....................8

What kind of attacks have affected Ukraine? 9

"Hybrid Warfare" 11

The rise in Phishing and Scam Attacks 12

Fake Donation Websites.. 12

DoS Attacks on Ukrainian News Sites.. 12

Distribution of Apps 13

Collapsed Economy: The consequences of a Russian cyber attack............... 13

CHAPTER 2: MICROSOFT: RUSSIA HAS LAUNCHED CYBERATTACKS AGAINST 42 COUNTRIES ALLIED WITH UKRAINE.. 16

Microsoft reveals multiple Russian cyberattacks in Ukraine 17

How many cyber-attacks has Ukraine suffered since the beginning of the Russian invasion? 20

Indicators of Compromise... 22

HermeticWiper SHA256.. 22

Certificate 22

Cortex Xpanse: Assets That Might Be Affected by CISA's Known Exploited Vulnerabilities.. 23

CHAPTER 3: TROLL FARM 25

The U.K. reveals a Russian troll farm spreading Kremlin propaganda on social media.. 26

Troll tactics.. 29

What are these trolls spreading? 29

What is the objective? 30

Meta shuts down Russian Troll Farm linked to sanctioned Putin ally........ 31

Britain says Russia is using 'troll farms' to spread disinformation about the Ukraine conflict. 32

Rammstein, victims of a Russian "troll farm" seeking to spread hoaxes about Ukraine.. 33

CHAPTER 4: ZERO DAY ATTACKS 36

Russia coordinates cyber and military attacks in Ukraine, according to Microsoft.. 36

According to Microsoft, Russia has launched cyberattacks on 42 countries allied with Ukraine. 37

The War between Russia and Ukraine: Cyber Impacts on National Operations... 42

What has happened to cyber operations in this new scenario.................. 44

International alert communicated by the United Kingdom and New Zealand.. 50

Relevant background of the last Months.. 51

CHAPTER 5: BALTIC COUNTRIES; VICTIMS OF CYBER-ATTACKS LAUNCHED BY RUSSIA... 58

Baltic countries wonder: are we next? 59

CHAPTER 6: TELEGRAM IN WAR, BATTLES IN CYBERSPACE 62

Cyber activism in defense of Ukraine or self-interest?............................... 63

List of cyber targets.. 63

Russian DDoS attack on Lithuania was planned on Telegram, Flashpoint says 66

INTRODUCTION

The damage caused by cyber-attacks in the Ukraine war pales compared to the atrocities of the fighting on the ground. But that doesn't mean it's not happening or that civilians are safe. Amid the Russian invasion of Ukraine, a field has been left aside: that of cyberattacks, something that, for many experts, can be considered a fourth battlefield. The Russian invasion of Ukraine has disrupted the global economy, from food to energy. Still, it has also increased the number and sophistication of cyberattacks, exacerbating impacts similar to those of the Covid-19 pandemic. According to analysts, the hackers who vandalized and interfered with access to a number of Ukrainian official websites may be laying the groundwork for more major hacks that would disturb the lives of regular Ukrainians. Since the beginning of the invasion of Ukraine on February 24th, the country's authorities and private sector organizations have been the target of a total of 796 cyberattacks, as reported by the State Service for Special Communications and Information Protection, SSSCIP, by its acronym in English.

CHAPTER 1

RUSSIA ATTACKS ON UKRAINE (CYBERATTACKS)

The damage caused by cyber-attacks in the Ukraine war pales in comparison to the atrocities committed on the battleground. But that doesn't mean it's not happening or that civilians are not affected.

Amid the Russian invasion of Ukraine, a whole area has been left aside: that of cyberattacks, something that by many experts is considered a fourth battlefield in this war.

The Russian invasion of Ukraine has disrupted the global economy from food to energy. It has also increased the number and sophistication of cyberattacks, exacerbating impacts similar to those of the Covid-19 pandemic.

According to a recent survey of 800 audit chief executives by the UK-based Chartered Institute of Internal Auditors, 77% of those surveyed stated that the war had increased risks in data and cyber security.

In fact, senior cybersecurity analysts have said that the invasion has been accompanied by sustained cyber conflict, with many attacks and threats launched since February.

On February 23rd, one day before Russian military forces invaded Ukraine, a wave of distributed denial-of-service attacks attributed to Russian hackers took down Ukraine's government, military, and banking websites.

The same day, US and UK intelligence agencies issued a warning regarding Cyclops Blink, a new malware developed by Sandworm - a team of hackers supported by the Russian government. Although in April US government officials declared that the malware had been stopped, concerns still remain.

While cybersecurity officials say Russia has primarily focused cyberattacks on Ukrainian businesses and infrastructure rather than targets in the EU, US or emerging markets, there are concerns that the cyber conflict could spread wider as the war progresses.

The hack revealed this on Viasat, a US satellite communications company utilized by the Ukrainian military, on the 24th of February. The attack, which impacted customers in Ukraine and throughout Europe, was traced back to Russia by officials from the European Union, the United Kingdom, and the United States in May.

What kind of attacks have affected Ukraine?

The latest cyberattacks recorded in Ukraine have had a common trait - they are all classified as "distributed denial of service" (DDoS) attacks.

This type of attack uses bots - digital tools, distributed to a large number of host computers, used to perform repetitive, predefined and automated tasks. For example - to flood online services with a large number of requests until they can't process them and crash becoming inaccessible to legitimate users, hence the name – denial of service.

The botnet (a network of bots) is remotely controlled and the owners are probably completely unaware that they have malicious software running on their systems.

Besides that, it was discovered that Ukraine had been the subject of another type of attack. By installing a malware (or malicious program) called "wiper," they managed to destroy data stored on multiple different systems.

One thing “wiper” did was remove the boot record from the affected computers. This prevents the machine from booting to the operating system which requires a full reinstall of the operating system to resolve the issue. This takes even more time to get the system back to full operational capacity.

Cyber security experts from ESET and Symantec named this virus **"HermeticWiper,"** claiming that it had been installed on hundreds of computers in the country.

Furthermore, they noted that the malware was created on the 28th of December, 2021, implying that the attack may have been planned since then.

In January, Ukraine had already been subjected to several cyber-attacks.

Some affected websites were replaced with a warning page saying to "prepare for the worst."

"Hybrid Warfare"

Distributed Denial of Service (DDoS) attacks committed by Russia have been reported in the past.

Such attacks hit Georgia and Crimea during the 2008 and 2014 incursions respectively.

In 2015 and 2016, the European Union, the United Kingdom and Ukraine blamed Russian government hackers for attacks on electrical substations that led to widespread power outages.

The foregoing corresponds to Russia's so-called "hybrid war" tactics, a concept that was used for the first time in the early 2000s and has to do with the implementation of a strategy (or several) of confrontation that does not necessarily happen in a military-type combat.

This was explained by Mundo by Antonio Alonso Marcos, professor of International Relations at the San Pablo CEU University in Spain on BBC.

“A country can use means that undermine the security and stability of another country. And they are not military means but, for example, cyberattacks or the launch of a massive wave of tweets that go against the position of a certain government. That is called hybrid warfare,” he says.

This type of aggression is becoming increasingly common and can often have results that are just as or even more dangerous than direct missile attacks for example.

For this reason, cyber infrastructure support has been recognized as an essential aspect of international aid.

Various European Union countries, including the Netherlands, Poland, Estonia, and Croatia, are sending cybersecurity experts to Ukraine to help them deal with these threats.

The rise in Phishing and Scam Attacks

Fake Donation Websites

More than 20 domains are asking for donations to help Ukraine. Many of these domains were found to be fraudulent after a thorough analysis. These donation websites lack details of the coordinating organization and fund distribution. Many of these websites accept donations in cryptocurrency (such as BTC and ETH) – likely because such payment systems are easy to set up and require no verification of identity.

Also, some websites are mimicking popular donation websites or organizations to trick users into paying them money. For instance, the website donatetoukraine[.]com falsely claims to be affiliated with the well-known Come Back Alive organization. The BTC wallet address provided on the donation page differs from the actual one, even though the banking details submitted match those on the original organization's website.

DoS Attacks on Ukrainian News Sites

According to our investigation, Russia[.]today, a cybersquatting domain, is used to perform DoS attacks against Ukrainian news websites. The website begins sending requests to numerous Ukrainian news sites as soon as a user opens it in a browser, and the number of requests sent to each new site is listed on the main page.

Users are strongly advised to be aware of the potential for cybersquatting domains. Particularly, as previously said, fraudulent donation websites replicating popular websites can be deceptive. Before making a financial contribution, it is advised to confirm if the website is mentioned and shared by the official charity or government agency.

Distribution of Apps

Threat actors have been caught running false download activities where they build up websites to house harmful files and target Ukrainian users. Most of these websites disguise harmful files as well-known browsers or communication apps to trick users. For example, a website that was distributing a malicious binary by masquerading as a popular global communication app targeting users in Ukraine was detected.

Collapsed Economy: The consequences of a Russian cyber attack

Different Ukrainian websites have been hacked and the United States has warned that Moscow could be preparing for more severe attacks

According to analysts, the hackers who vandalized and interfered with access to a number of Ukrainian official websites may be laying the groundwork for more major hacks that would disturb the lives of regular Ukrainians. The Pentagon and the White House have both confirmed the operation, while the Russian embassy has denied it. The United States has warned that Russia may be preparing a fictitious attack against pro-Russian forces in eastern

Ukraine to justify a potential invasion of the nation in "mid-January and early February."

The Russian embassy refutes the allegations by the Pentagon and the White House that Russia is planning fictitious assaults. The US claims to be "in contact" with the authorities and is "concerned" about cyberattacks in Ukraine.

Until recently, hacker attacks on healthcare facilities, electric utilities, and the financial system were rare. But during the past two years, organized cybercriminals, many of them Russian citizens, have actively attacked institutions, using ransomware to lock up data and computer equipment essential to treat, for example, patients in a hospital.

According to court cases, media accounts, and medical experts, these extortion attacks have occasionally resulted in patient fatalities.

A warning to "be afraid and expect the worst" was included in the attack on Ukrainian websites on Friday. This comes as Russia has gathered over 100,000 troops close to Ukraine’s borders, prompting concerns in the West that Russia is preparing for an invasion, but Moscow denies having an invasion intent.

Over the years, Ukraine and other nations have accused Russia of hacking attacks, which Russia has consistently denied. Ukraine hasn't blamed Russia directly for the recent attacks, even though it is likely responsible for the most recent defacements of Ukrainian websites.

In 2014 Russian troops invaded the Ukrainian territory of Crimea, a peninsula on the Black Sea. Dmitri Alperovitch, a former cybersecurity executive with CrowdStrike, forecasted that if Russia invades again, cyberattacks would also increase.

Alperovitch remarked that they are likely more upsetting rather than fatal or critical. It will be a side show along the main show on the battleground. The victims of some of the largest infrastructure hacks so far have also primarily been in Ukraine.

CHAPTER 2

MICROSOFT: RUSSIA HAS LAUNCHED CYBERATTACKS AGAINST 42 COUNTRIES ALLIED WITH UKRAINE

Moscow has launched cyberattacks against 42 countries that support the Ukrainians, including the US, Poland, and the Baltic nations since the Russian invasion of Ukraine began in February 2022.

In a post on the company's official blog, President of Microsoft Brad Smith explained that Russian intelligence agencies had increased network penetration and espionage activities against countries allied with Ukraine since the beginning of the invasion, 24th of February 2022.

"At Microsoft, we have detected network intrusion attempts by Russia to 128 organizations in 42 countries outside of Ukraine," Smith said.

The company, based in Redmond (Washington State, USA), did not publish the complete list of the 42 affected countries. Still, it cited some, such as the USA, Poland, Estonia, Latvia, Lithuania, Denmark, Norway, Finland, Sweden, Turkey, and the Ministries of Foreign affairs of other NATO member nations.

The United States is the country most affected by cyberattack attempts. 63% of the total attacks have been directed against members of the Atlantic Alliance.

Most of the organizations targeted by Russian cybercriminals are government-owned, including think tanks, aid agencies, IT service companies, energy companies, and other key infrastructure providers.

Of all Russian cyberattack attempts identified by Microsoft since the beginning of the war, 29% were successful, in some cases resulting in hackers taking private information from the targeted organization.

According to the creator of the popular Windows operating system, the Russian strategy in the cyber field for the invasion of Ukraine is based on three pillars: destructive cyber-attacks against the neighboring country, network penetration and espionage outside Ukrainian territory, and digital operations to gain influence all over the world.

Microsoft reveals multiple Russian cyberattacks in Ukraine

The digital onslaught, which Microsoft says began a year before Russia's Research, suggests that the digital assault, which Microsoft claims started a year before Russia's incursion on the 24th of

February, may have prepared the way for other military operations in the war-torn region.

According to a report released by Microsoft on Wednesday, Russian government hackers engaged in several cyberattacks against Ukraine that were meant to support Moscow's military offensives and online propaganda activities.

The reported incursions, some of which have not yet been made public, imply that hacking has been more involved in the battle than has been previously acknowledged.

Researchers believe that the digital assault, which Microsoft claims started a year before Russia's incursion on the 24th of February, may have prepared the ground for other military operations in the war-torn region.

Microsoft reported that it saw a total of 37 harmful Russian cyberattacks in Ukraine between 23rd of February and 8th of April.

The Russian embassy in Washington did not respond immediately when contacted for comment.

According to experts, the results demonstrate how conventional and digital strikes can coexist in modern combat.

According to Thomas Rid, professor of strategic studies at the Paul H. Nitze School of Advanced International Studies at Johns Hopkins University, "Russian generals and spies have tried to make cyberattacks part of their war effort while fighting on the battlefield."

Microsoft said Russia's military and hacking operations worked "in tandem against a shared set of goals." The company said it couldn't determine whether the correlation was driven by coordinated decision-making or simply goal coincidence.

For example, a timeline published by Microsoft showed that on March 1st, the day a Russian missile was fired at the Kyiv TV tower, the capital's media outlets were hit with destructive hacking and cyber espionage.

In another case, the company's cybersecurity investigation team recorded "suspected Russian actors" loitering around Ukrainian critical infrastructure in the northeastern city of Sumy two weeks before widespread power outages were reported in the city area on the 3rd of March.

The next day, according to Microsoft, Russian hackers broke into a government network in the central Ukrainian city of Vinnytsia. Two days later, missiles swept through the city's airport.

Victor Zhora, a senior Ukrainian cybersecurity official, said that he continues to see Russian cyberattacks targeting local telecommunications companies and power grid operators.

"I think they can mount more attacks against these sectors," Zhora told reporters. "We shouldn't underestimate Russian hackers, but we shouldn't overestimate their potential either."

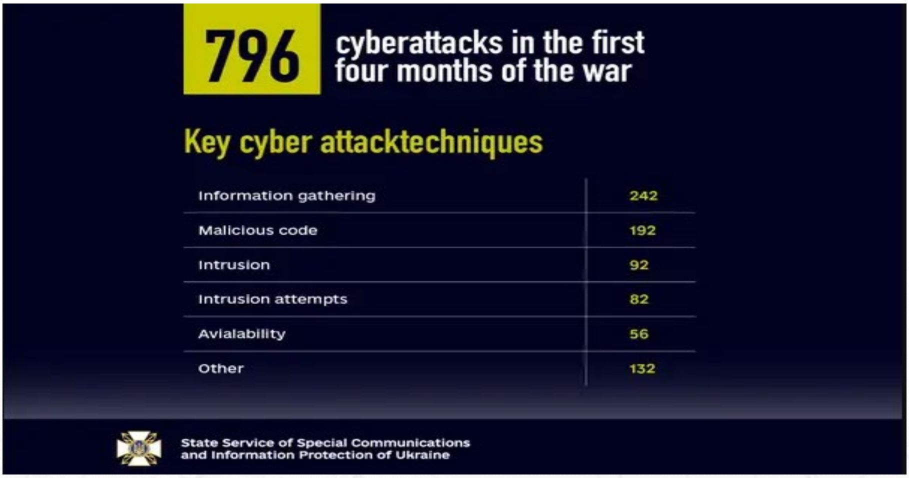
Zhora thanked Microsoft, the US government, and many European allies for their cybersecurity support.

How many cyber-attacks has Ukraine suffered since the beginning of the Russian invasion?

The State Service of Special Communications and Information Protection of Ukraine has released a report which breaks down the type of attacks received and the preferred targets during these months.

Since the beginning of the invasion of Ukraine on the 24th of February, the country's authorities and private sector organizations have been the target of a total of 796 cyberattacks, as reported by the State Service for Special Communications and Information Protection (abbreviated: SSSCIP).

The SSSCIP has broken down the attacks by types and objectives. Thus, of these 796 attacks, 242 aimed to obtain information, 192 aimed to infect systems with malicious software, 92 were intrusions, 82 were intrusion attempts, 56 ended the availability of the objective, and 132 appear framed under the heading "Others."



796 cyberattacks in the first four months of the war

Key cyber attacktechniques

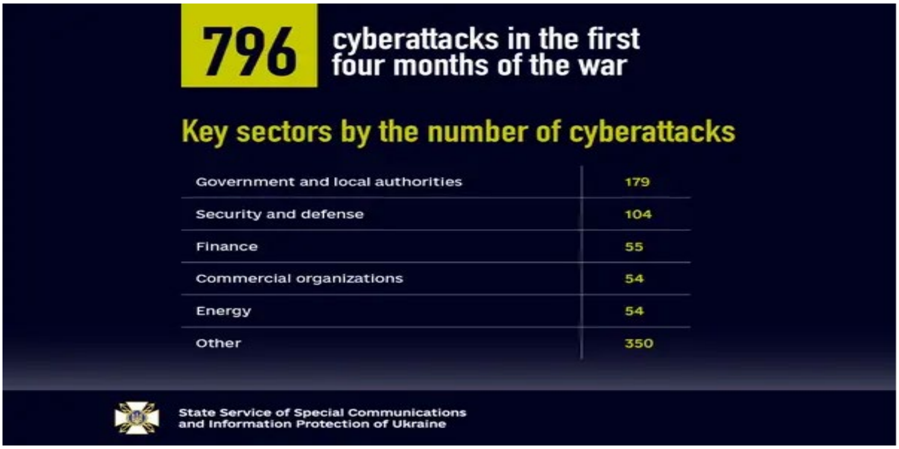
Information gathering	242
Malicious code	192
Intrusion	92
Intrusion attempts	82
Avialability	56
Other	132

State Service of Special Communications and Information Protection of Ukraine

"Enemy hackers continue to attack Ukraine. The intensity of cyber-attacks has not decreased since the beginning of the large-scale military invasion of Russia, although their quality has been declining.

The Ukrainian authorities and the defense, financial, and energy sectors have been attacked the most, followed by transport infrastructure and the telecommunications industry.

Specifically, the Government and local authorities suffered 179 cyberattacks, security and defense organizations 104, financial organizations 55, commercial organizations 54, and those in the energy sector 54, while 350 of the attacks are categorized as "others."



796 cyberattacks in the first four months of the war

Key sectors by the number of cyberattacks

Government and local authorities	179
Security and defense	104
Finance	55
Commercial organizations	54
Energy	54
Other	350

State Service of Special Communications and Information Protection of Ukraine

The increase in cyberattacks affects not only Ukraine but other countries as well. Microsoft's Threat Intelligence Center, MSTIC, reported an increase in cyberattacks by Russian actors on Ukraine and allied governments last week. "MSTIC has detected Russian network intrusion attempts at 128 targets in 42 countries outside of

Ukraine," explained Brad Smith, Vice Chair and President of Microsoft.

The targets of 49% of these attacks were government agencies, while 20% were directed against companies in the information technology sector, 19% against critical infrastructure and 12% have targeted non-governmental organizations. MSTIC estimates its success rate at 29%.

Microsoft had already warned last April that multiple Russian cybercriminal organizations were carrying out hundreds of attacks against Ukraine's infrastructure and were trying to introduce malware into critical systems and hinder the population's access to critical information and services.

Indicators of Compromise

HermeticWiper SHA256

1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397

Certificate

Name Hermetica Digital Ltd

Thumbprint 1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
Serial Number 0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC

Website Defacement Domain

gcbejm2rcjftouqbxuhimj5oroouqcuxb2my4raxqa7efkz5bd5464id[.]onion

Cortex Xpanse: Assets That Might Be Affected by CISA's Known Exploited Vulnerabilities

Russian advanced persistent threat (APT) groups are believed to have previously exploited a number of the vulnerabilities listed in Alert AA22-011A (updated March 1st, 2022) by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS/CISA). Still, the agency urges users to take action against a much larger list of known exploited vulnerabilities (KEVs). The following KEYs and the impacted devices can all be recognized using Cortex Xpanse:

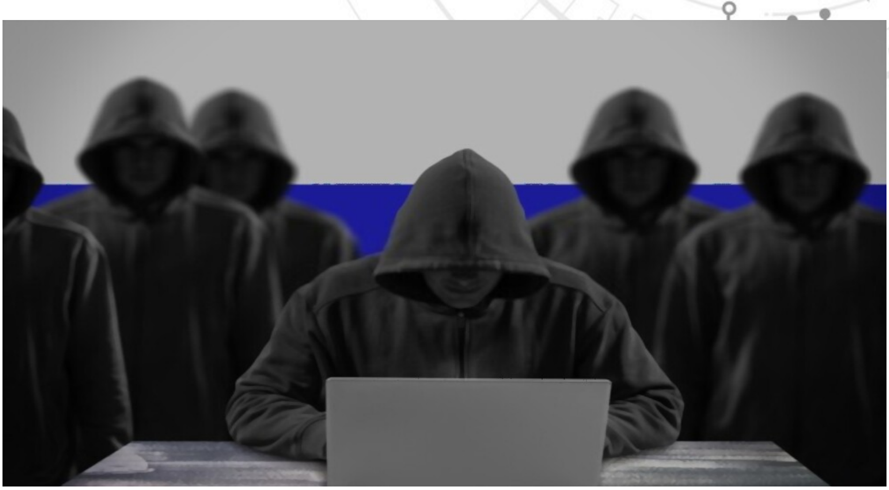
- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 Multiple VMware Products
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange

Organizations can find, prioritize, and fix important exposures on their attack surfaces using Cortex Xpanse's ability to index the whole Internet, which includes all of the impacted services mentioned above. Despite most of these CVEs being older than two years, we frequently notice vulnerable devices on the Internet.

In addition to Alert AA22-011A, Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities outlines CISA's general recommendations for reducing the attack surface, which include hardening forward-facing network services and prioritizing KEV patching (KEV). According to an evaluation that the vulnerabilities "carry significant risk to the federal enterprise," this directive requires agencies to fix any vulnerabilities CISA has included in their KEV catalog

CHAPTER 3

TROLL FARM



Senior international politicians and media outlets are the targets of this information operation and its related targeted trolling activities.

This was reported by the technology company Meta. People commented on posts on **Instagram, Facebook, TikTok, Twitter, YouTube, LinkedIn, VKontakte, and Odnoklassniki.**

A Russian team hired people from the street to post comments on the Internet and give the impression that the invasion of Ukraine by Vladimir Putin's forces had popular support, the technology company Meta denounced on Thursday.

The Internet has been one of the war fronts where Russia has tried to silence criticism and promote the narrative of support for the invasion.

A "troll farm" ran the disinformation campaign, according to Meta. Some of those involved in the operation were associated with the Internet Research Agency (IRA), a Russian group linked to election meddling in the United States and other countries since 2016, Meta explained.

The operation hired almost anyone to participate in online deception, a tactic similar to that used by the IRA years ago in other campaigns, Meta's global threat intelligence chief, Ben Nimmo, told AFP.

According to the company's investigation, the trolls worked seven days a week for about $440 a month and commented on posts on Instagram, Facebook, TikTok, Twitter, YouTube, LinkedIn, VKontakte, and Odnoklassniki.

The firm said 1,037 Instagram and 45 Facebook accounts implicated in the campaign were removed.

The U.K. reveals a Russian troll farm spreading Kremlin propaganda on social media.

According to UK-funded expert research, a troll factory run by the Kremlin is being used to disseminate misinformation on social media and in the comments sections of well-known websites.

Targets of cyber soldiers include politicians and audiences in the U.K., South Africa, and India, among other nations.

The Research revealed how the Kremlin's extensive disinformation campaign is intended to influence public opinion throughout the world regarding Russia's illegitimate war in Ukraine, aiming to increase support for their heinous war and recruit new Putin sympathizers.

The operation's sick masterminds are rumored to be operating openly from a former factory in St. Petersburg, with paid workers and internal working teams.

Foreign Secretary Liz Truss said:

“We cannot let the Kremlin and its dubious troll farms into our online areas with their fabrications about Putin's unlawful conflict. The U.K. government has warned other nations to cooperate closely with allies and media outlets to counter Russian information operations.”

Culture Secretary Nadine Dorries said:

“These are cunning attempts by Putin and his media machine to conceal the cruelty he's inflicting on the Ukrainian people, according to Culture Secretary Nadine Dorries. Following our firm decision to forbid anyone from doing business with Kremlin-controlled outlets R.T. and Sputnik, this proof will aid us in more efficiently identifying and eliminating Russian misinformation.

According to the evidence, the troll farm actively recruits and coordinates new supporters through Telegram. These supporters then target the social media accounts of Kremlin critics and bombard them with pro-Putin and pro-war comments. Along with *other world leaders, the social media accounts of senior U.K. ministers are targets.*

The Internet Research Agency's most notorious and extensive bot-founder, farm's Yevgeniy Prigozhin, both of which have been sanctioned by the U.K., are accused of having connections to the operation.

Major social networking sites will receive this most recent study from the U.K. government. Per their Terms of Service, we are already collaborating closely with them to make sure they quickly remove misinformation and coordinate untrue or manipulated behavior.

A Government Information Cell (GIC) has also been established in the U.K. to combat Russian disinformation. The Cell, which is comprised of specialists from throughout the U.K. Government, is concentrated on identifying and evaluating Russian disinformation and providing advice and output to expose and counter the lies of the Kremlin.

We have already targeted the spreaders of Russian misinformation, including some of Putin's most important political allies, as well as the spokespeople for the Putin regime, such as Dmitry Peskov, the press secretary, and Maria Zakharova, the spokeswoman for foreign affairs.

The government has also taken direct action against state media organizations, particularly the T.V. Novosti, which is backed by the Kremlin and controls R.T., formerly known as Russia Today, and Rossiya Segodnya, which runs the news outlet Sputnik."

Troll tactics

- Encouraging followers to target Kremlin skeptics' social media accounts, such as those of well-known politicians and foreign leaders, and bombard them with pro-Kremlin remarks
- Asking them to activate VPNs and to post a lot of comments on specified Instagram, YouTube, and Telegram sites
- Focusing on leaving comments rather than creating original content will reduce the chance of being caught by social media platforms engaging in coordinated untruthful behavior and/or harmful content.
- To make such viewpoints the norm, they look for "organic content" uploaded by real users that is consistent with the points they wish to make. They then attempt to propagate these messages. This indicates that they are unlikely to face de-platforming interventions as long as the content they post is not overly offensive.

What are these trolls spreading?

They are currently completely obsessed with Ukraine in particular, claiming that Russia is merely protecting its citizens from a Ukrainian genocide in eastern Ukraine.

They are attempting to spread the misconception that it is not Russia that is at war in Ukraine but rather the E.U., NATO, and even the United States. This is the content that the trolls have been writing (since 2014) and is still publishing: the president of Ukraine is a warmonger; Putin likes peace and diplomacy.

They are assigned new themes to write about every day in the morning, and as a result, they are available around the clock to respond to any online discussions as they happen.

The trolls have attacked various events throughout the years. An obvious example is the 2016 U.S. presidential election. Naturally, the trolls supported Donald Trump. Utilizing Facebook, they carried out some extremely intriguing microtargeting operations, particularly targeting residents of key states.

What is the objective?

The content is violent and aimed at the audience's brain, aiming to alter the recipients' beliefs, attitudes, and even behavior. Online discussions appear to have certainly become more combative. Many people who accept these stories are even more eager to support Russian policies and promote the misconception that, for instance, the so-called "Nazis" and fascist regimes in Ukraine demanded it and that Russian forces are currently liberating the Ukrainians.

Obviously, some people are receptive to this kind of information and become even more brainwashed than they already were. At the same time, some populations that previously supported the Kremlin and believed the propaganda it spread, now see what Russia is doing to Ukraine to be excessive. Some of the support for the Kremlin has since disappeared.

Meta shuts down Russian Troll Farm linked to sanctioned Putin ally

On Thursday, the 4th of August, Meta said that it had shut down a troll farm that had been spreading misinformation during the 2016 U.S. presidential election campaign and had ties to a sanctioned Putin ally and Russia's Internet Research Agency.

The action was part of a broader social media campaign against cyber espionage operations and other criminal actors, which were mentioned in Meta’s Quarterly Adversarial Threat Report.

A month after Russia's invasion of Ukraine started, Meta claimed in the report that it discovered Cyber Front Z, a "physical troll farm operated out of an office building in St. Petersburg," which targeted users on various platforms, including Twitter and LinkedIn in addition to Facebook and Instagram.

According to CBS News, Cyber Front Z "ran a Telegram channel that basically told people to leave pro-Russian comments on social media posts by public figures, journalists, politicians, and celebrities, like Angelina Jolie and Morgan Freeman," according to Ben Nimmo, lead of Meta's global threat intelligence.

According to the article, Cyber Front Z was blocked from Meta's platforms in April, and the business also removed 1,037 Instagram accounts and 45 Facebook accounts connected to the group.

According to the British authorities, the operation was connected to Yevgeny Prigozhin, the creator of "the bot-farm the Internet Research Agency," who is a sanctioned Putin ally.

Cyber Front Z's attempts were "clumsy and largely ineffective—definitely not 'A team' work," according to Meta.

Notable: According to the study, Meta also dismantled the South Asian spy organization Bitter APT, which "targeted people in New Zealand, India, Pakistan, and the United Kingdom."

In the interim, the business took aggressive action against "organized breaching networks in Greece, India, and South Africa."

Britain says Russia is using 'troll farms' to spread disinformation about the Ukraine conflict.

The Russia-Ukraine battle has been going on for more than six months, and it is not showing any signs of slowing down.

Despite numerous negotiations, a consensus has not been achieved, and the conflict is still raging both offline and online.

On Sunday, the 1st of May, the British Foreign Office accused Moscow of deploying a "troll factory" to disseminate false information about the conflict in Ukraine.

They claim that Russia is targeting politicians in some nations, including Britain and South Africa, using disinformation.

The study reveals how the Kremlin's disinformation effort tries to influence international public opinion about the Russian invasion of its neighbor while also enlisting sympathizers, according to the British Foreign Office.

In a statement, British Foreign Secretary Liz Truss stated, "We cannot let the Kremlin and its dubious troll farms infiltrate our online space with their lies about Putin's criminal war." The UK government has warned its allies and media outlets and will keep up its close collaboration with them to counter Russian propaganda operations.

Britain claims to have linked eight sites, including Telegram, Twitter, Facebook, and Tik Tok, to the Russian disinformation campaign. Additionally, it is claimed that Russia is attempting to enlist and cooperate with new allies who target Kremlin critics' profiles.

Russia, on the other hand, criticizes the Western media's conflict coverage as unfair. The Kremlin claims that the Western media's portrayal of events ignores the ex-Soviet nation's worries about NATO expansion and the claimed discrimination against Russian speakers in Ukraine.

Russia was previously charged with participating in a disinformation campaign in other conflicts. The U.S. also accused Moscow of interfering in the presidential election earlier in the year 2016.

Rammstein, victims of a Russian "troll farm" seeking to spread hoaxes about Ukraine

According to a British government report, Rammstein's (German rock band) social networks have been the target of a Russian "troll farm" that sought to spread false information about the war in Ukraine.

A troll farm is a standardized and organized group that seeks to spread disinformation on the Internet by interfering with people's political views. It is alleged that up to 30 governments worldwide have paid for such services to spread propaganda.

The report identifies Rammstein as one of the targets of these trolls. Other members on that list include British Prime Minister Boris Johnson, German Chancellor Olaf Scholz, and E.U. foreign policy chief Josep Borrell. Other musicians who would have been victims of this attack would be Daft Punk, David Guetta, and Tiesto.

According to the report, the troll factory is located in the Arsenal Machine-Building Factory in St. Petersburg.

Evidence of disinformation was found on a multitude of different social networks - Twitter, Facebook, Instagram, YouTube, and TikTok. It contained pro-Russian messages from different social network users on prominent user's profiles to circumvent measures put in place to combat disinformation.

Yevgeny Prigozhin, an oligarch with close ties to Russian President Vladimir Putin, has been closely linked to the operation. The FBI has listed Prigozhin as a wanted person because he founded the Internet Research Agency, a company charged with meddling in the 2016 U.S. presidential election.

Following this finding, U.K. Foreign Secretary Liz Truss said, "We cannot let the Kremlin and its shadowy troll factories penetrate our online spaces with their lies about Putin's criminal war."

The U.K. government has warned its allies and media outlets and will keep up its close collaboration with them to counter Russian propaganda.

Following the Russian invasion of Ukraine, Rammstein released a statement that reads as follows: "Rammstein wishes to express its support for the nation of Ukraine in resisting the shocking attack by the Russian government. Especially at this moment, we feel a special sorrow for the suffering of the Ukrainian people."

CHAPTER 4

ZERO DAY ATTACKS

Russia coordinates cyber and military attacks in Ukraine, according to Microsoft.

The U.S. tech giant Microsoft reported that Moscow often combines cyberattacks with military action on Ukrainian territory.

According to a report by Microsoft on the 27th of April 2022, a handful of hackers aligned with the Russian government have carried out hundreds of cyberattacks against Ukraine since Moscow invaded the neighboring country,

Microsoft noted that in "hybrid" warfare tactics, Russia often combines these cyberattacks with military action on the battlefield.

"Starting just before the invasion, we have seen at least six Russian-aligned nation-state actors launch more than 237 operations against Ukraine," said Microsoft, who are working with Ukrainian cybersecurity experts and private companies to counter such attacks.

The company maintained that the cyber warfare included "destructive attacks that are ongoing and threaten the well-being of civilians."

Coordinated actions

The report alleges that in the first week of the invasion, Russian hackers attacked a major Ukrainian broadcaster "on the same day that the Russian military announced its intention to destroy Ukrainian' disinformation' targets and directed a missile attack at a television tower." in Kyiv."

The U.S. corporation stressed that the goal of such coordinated attacks was "to disrupt or degrade Ukraine's military and government functions and undermine public confidence in those same institutions."

Campaign orchestrated from 2021

It also stated that it had detected almost 40 destructive cyberattacks, targeting hundreds of systems, a third of which directly targeted Ukrainian government organizations at all levels, from national to local, while another 40% targeted infrastructure country review.

"These actors often modify their malware with every action to evade detection," the report said, noting that the cyber attackers began preparing their campaign in March 2021, almost a year before Vladimir Putin ordered his troops to invade Ukraine.

According to Microsoft, Russia has launched cyberattacks on 42 countries allied with Ukraine.

Moscow has launched cyberattacks against 42 pro-Ukrainian countries, including the US, Poland, and the Baltic nations, since the Russian invasion of Ukraine began last February, according to investigation results published on the 27th of April 2022 by the American software giant Microsoft.

In an entry on the company's official blog, Microsoft President Brad Smith explained that Russian intelligence agencies had increased network penetration and espionage activities against countries allied with Ukraine since the beginning of the invasion, on the 24th of February.

"At Microsoft, we have detected network intrusion attempts by Russia to 128 organizations in 42 countries outside of Ukraine," Smith said.

The firm based in Redmond (Washington state, USA) has not published the complete list of the 42 affected countries. Still, it has cited some, such as the USA, Poland, Estonia, Latvia and Lithuania, Denmark, Norway, Finland, Sweden, and Turkey, in addition to the Foreign Ministries of other NATO member nations.

The USA is the most affected country

The U.S. is the country most affected by cyberattack attempts, and 63% of the total was directed against members of the Atlantic Alliance.

Most of the organizations targeted by Russian cybercriminals are government-owned, but they also include think tanks, aid agencies, I.T. service companies, energy companies, and other key infrastructure providers.

Of all Russian cyberattack attempts identified by Microsoft since the beginning of the war, 29% were successful, in some cases resulting in hackers taking private information from the targeted organization.

According to the creator of the popular Windows operating system, the Russian strategy in the cyber field for the invasion of Ukraine is based on three pillars: destructive cyberattacks against the neighboring country, network penetration and espionage outside Ukrainian territory, and digital operations to gain influence all over the world.

An hour before the invasion, Russian hackers had already attacked Ukraine

Authorities in the U.S., E.U. and the U.K. had recently revealed that Russian government hackers attacked the American satellite communications provider Viasat one hour before Russian forces invaded Ukraine.

The action caused an immediate and major loss of communication for the Ukrainian military, which depended on Viasat's services for command and control of the nation's armed forces during the first days of the war.

The Viasat cyberattack is the largest known hack of this war, according to Juan Andrés Guerrero-Saade, a threat researcher at the cybersecurity company SentinelOne. He also adds that the attack was "the most intense effort to disable Ukrainian military capabilities."

At the same time, it is one of the first real-world examples of how cyberattacks can be targeted and programmed to amplify military forces on the ground by disrupting and even destroying technology used by enemy forces.

The attack on the 24th of February launched a destructive "wiper" malware called AcidRain against Viasat's modems and routers, quickly wiping all data from the system. The computers were then restarted, making thousands of terminals permanently inoperable.

The malware that the Russians previously utilized functioned in a targeted fashion, according to Guerrero-Saade, who has been at the forefront of AcidRain research, while AcidRaid is more of a global weapon.

"What is hugely worrying about AcidRaid is that all the security checks have been passed," says the expert. "With previous wipers, the Russians were careful to run them only on a few specific devices. Now those security controls are gone, and brute force has been used. They have a capability that they can reuse. The question now is, what attack chain? The supply we will see next".

According to experts, this attack is typical of Moscow's "hybrid" war strategy, and it was launched in sync with the invasion on the ground. According to Microsoft research, that kind of pinpoint coordination between Russian cyber operations and military forces has already been seen at least six times, underlining the emerging role of cyber warfare.

"Russia's coordinated and destructive cyberattack before the invasion of Ukraine shows that cyberattacks are actively and strategically used in modern warfare, even if the threat and consequences of a cyberattack are not always visible to society," he said in a statement. Danish Defense Minister Morten Bødskov said. "The cyber threat is constant and changing. Cyber-attacks can cause great damage to our critical infrastructure, with fatal consequences."

In this case, the damage extended beyond Ukraine and affected thousands of internet users and grid-connected wind farms in central Europe. The fallout hasn't stopped on this continent: Viasat works with the U.S. military and its partners worldwide.

"Obviously, the Russians have screwed up," says Guerrero-Saade. "I don't think they intended to cause so much collateral damage and involve the European Union. They gave the E.U. a pretext to act after 5,800 German wind turbines were affected and a few others in the rest of the E.U."

Just hours before AcidRain began its destructive work against Viasat, Russian hackers used another wiper, called HermeticWiper, against Ukrainian government computers. The attack was eerily similar, except that instead of satellite communications, the targets were networked Windows machines, which would be important for the Kyiv government to mount effective resistance in the first hours of the invasion.

The effectiveness of these attacks remains an open question. A senior Ukrainian official admitted that the attack on Viasat caused a "huge loss in communications at the beginning of the war" but did not provide further details.

The cyber realm is supporting military operations, but it will take a long time for us to have a full picture of all the operations in play during this war. However, it seems likely, given the way AcidRain was created, that we will see it in action again.

The War between Russia and Ukraine: Cyber Impacts on National Operations

The conflict between Russia and Ukraine in Eastern Europe has a long history. Its current development stems from a constant escalation that over time has also included cyber operations, allowing a battle to be waged which is "invisible” to a large part of the world's population but has been capable of causing major disruption to critical infrastructure in different countries where the consequences have been tangible for civilians, even more so when in the "shadows" it is financed by a state (APT's).

UPDATE ALL:

- Ensure that your organization's software is up to date, prioritizing those that patch the vulnerabilities reported in the "Catalog of Known Exploited Vulnerabilities" - reported by US-CISA. (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

BACK UP ALL:

- Perform Backup (Backup) of all the systems you have within your organization.
- Under no circumstances store the Backup within the same server, computer, or local network.
- Check that the Backup and restore mechanisms work.

SECURE YOUR ATTACKING SURFACE:

- (Exposure of your organization to the Internet) Validate that your organization's I.T. staff has disabled all ports and protocols that are not essential for fulfilling your operations.

PROTECT IDENTITIES:

- Validate that all remote access to your organization's network has "Multi-Factor Authentication" (MFA) - remembering that US-CISA added single-factor authentication to the list of "exceptionally risky" cybersecurity bad practices. (https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices)

FUNCTIONAL SAFETY:

- Verify that your threat detection equipment is up-to-date with signatures and operating correctly, especially WAF and EDR.
- Make sure existing integrated filtering and detection products are enabled and operating correctly.
- If your organization uses cloud services, make sure I.T. staff have reviewed and implemented strict security controls.
- Make sure that the system logs are being audited by event correlators covering the techniques mapped by data sources according to MITER ATTACK.

ORGANIZATIONAL AWARENESS:

- Focus on awareness and training. Inform collaborators about threats, such as phishing scams, and how they are delivered—train users on information security principles and techniques and general emerging cybersecurity risks and vulnerabilities.

- If your organization operates or interacts with Ukrainian organizations, take special care to monitor, inspect, and isolate traffic from those organizations; review the access controls for that specific traffic in detail.
- Ensure employees know who to contact when they see suspicious activity or believe they've been the victim of a cyber-attack. This will ensure that the appropriate mitigation strategy can be employed quickly and efficiently.

What has happened to cyber operations in this new scenario

Months before the start of the conflict, there have been different security incidents on critical infrastructure, mainly in Europe, carried out by different actors, both state-backed and independent, which have inherently increased tensions, making it foreseeable but not desired, that it would lead to a war.

Although, in this area, those affected and the executors do not correspond only to Russia and Ukraine, during the end of 2021 and the course of 2022, it has been possible to perceive a considerable increase in this type of attack, including attacks with new intentions such as the use of techniques clearly focused on destruction, with malware called "DataWiper" that results in the elimination of all information from the affected computer, including the Operating System, acting more aggressively than just hijacking information.

Below are some examples of attacks that have affected the critical infrastructure of different productive sectors.

PETROLEUM INDUSTRIES:

From December 2021 to date, eight cybersecurity incidents against oil industries have been recorded:

1. Organization: PetroVietnam

Country: Vietnam
Threat: Ransomware Snatch
Date: 02-09-2022

2. Organization: Petrolimex

Country: Vietnam
Threat: BlackByte Ransomware
Date: 02-05-2022

3. Organization: Edge

Country: Jordan
Threat: Ransomware Cuba
Date: 02-04-2022

4. Organization: KCA Deutag

Country: United Kingdom
Threat: RansomEXX Ransomware
Date: 01-28-2022

5. Organization: AL-SOOR FUEL MARKETING COMPANY KSCP

Country: Kuwait
Threat: Ransomware Snatch
Date: 12-30-2021

6. Organization: Solaris Management Consultants

Country: Canada
Threat: BlackCat Ransomware (ALPHV)
Date: 12-29-2021

7. Organization: Divestco Geoscience Inc

Country: Canada
Threat: AvosLocker Ransomware
Date: 12-25-2021

8. Organization: Kangean Energy Indonesia

Country: Indonesia
Threat: BlackByte Ransomware
Date: 12-19-2021

ELECTRICAL SECTOR INDUSTRIES:

Ukraine

Date: 17-12-2016

Although this event does not correspond to the present, it is a precedent of a cyber conflict that has been dragging on for several years, where Russia was identified as being responsible for a string of interventions in the electrical system generating black out in Ukrainian cities between 2015 and 2016.

BANKING & FINANCE INDUSTRIES:

Ukraine

Date: 02-15-2022

In an attack directed at government entities in Ukraine, State and private banks were affected by powerful distributed denial-of-service (DDoS) and defacement attacks that interrupted services for a few hours.

Affected banks:

- State banks
- PrivatBank
- Oschadbank

Canada

Date: 02-26-2022

An interruption was observed in the main Canadian banks in the online banking service, including transfers, even affecting the withdrawal of money at ATMs.

Affected banks:

- RBC
- CIBC
- TD Canada
- Scotiabank

These interruptions were observed lasting between a couple of hours to a whole day for different banks.

It is important to remember that in a similar case that occurred in Chile, the denial of service only serves as a distraction for the theft of significant amounts of money.

TELECOMMUNICATIONS INDUSTRIES:

Vodafone Portugal

Closes: 08-02-2022

Although the cause is unknown for this attack, it managed to interrupt the 4G and 5G networks of Vodafone Portugal throughout the country, along with other services such as SMS and fixed telephony.

Considering the volume of clients subscribed to this organization, more than 7 million affected users are estimated.

Croatia

Date: 02-11-2022

The company A1 Hrvatska, which is a strategic partner of Vodafone, was affected by an attack on its databases which resulted in the theft of information from 10% of its customers (approximately 200,000 users) including names, identification numbers, addresses, and phone number.

Vodafone Ukraine

Date: 02-17-2022

A cybersecurity firm has identified a significant disruption in Vodafone's mobile phone services in a Ukrainian city for about an hour.

The following day, the Ministry of the Interior warned of possible sabotage which involved cutting an optical fiber in the network.

TRANSPORTATION INDUSTRIES:

Belarus

Date: 01-24-2022

Hackers from Belarus claimed an attack within their territory, encrypting the servers of the Belarusian train system as a protest against its use to stop the transport and deployment of Russian troops to the Ukrainian border as one of the first military movements prior to the outbreak of the conflict.

Shortly after this intervention, Iranian cyber actors joined the claim of responsibility.

GOVERNMENT:

Ukraine

Date: 01-14-2022

After unsatisfactory talks between Ukraine, Russia, and the United States, different entities of the Ukrainian government were affected where, together with a "defacement" message on the web portals of the Ministry of Foreign Affairs, Education, Science, and Defense, among others, warned that all the information had been exfiltrated and subsequently permanently eliminated.

Ukraine

Date: 02-15-2022

On the same day that the attacks on banks were carried out in Ukraine, attacks of the same nature (DDoS and Defacement) were also recorded against government websites such as the Ministry of Defense and a state radio station.

The security service of Ukraine indicated that the attacks are linked to Russian cyber actors.

Ukraine

Date: 02-23-2022

After the recent war attacks carried out with military force, in parallel, new "defacement" attacks have been carried out on government websites that have included links to sites on the TOR network where multiple Leaks of the affected ministries were published during the attack of similar characteristics made on the 14th of January 2022.

International alert communicated by the United Kingdom and New Zealand

Due to the fact that the conflict between nations has taken a position on the cyber plane, the great capabilities that Russia possesses in this matter have been demonstrated, which is why they have been warned as a global threat from different countries outside the conflict, as is the case of the United Kingdom and New Zealand.

In the case of the United Kingdom, on January 28, 2022, after visualizing constant attacks on Ukrainian government websites, it issued a warning statement about imminent attacks in the region by Russian-backed actors, recommending preventive actions.

On the other hand, New Zealand warns of collateral damage as a result of the conflict towards multiple sectors outside the center of the conflict since, as previously observed, actors such as CozyBear already have a background and capabilities to affect systems used globally, as was the case of SolarWinds Orion in 2020.

Relevant background of the last Months

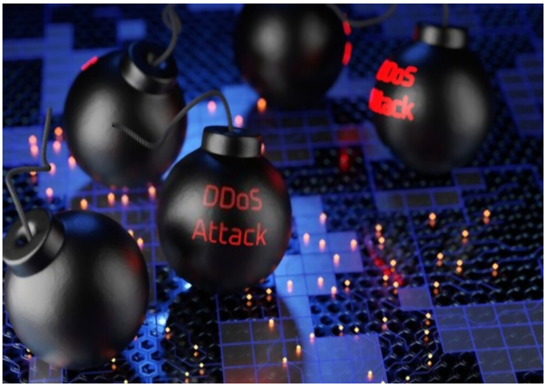
Within the framework of the different operations carried out in the last few months (at the time of writing). Specifically, in those scenarios which included the participation of what can be classified as "weapons" for cyber warfare, the mode of action of the attackers on their objectives has clearly demonstrated intentions to cause harm and panic in the population.

The aforementioned claims are supported by the information delivered in different bulletins that have been communicated, mentioning the series of attacks suffered by Ukraine and the different tactics and devices used for it.

This is where special attention should be paid regarding the impact produced by these attacks. As mentioned earlier, given that in this scenario, we observe an adversary who does not seek to negotiate, maintaining tension and uncertainty as to how and when his next "move" will be.

To clarify how these operations have been carried out against Ukrainian organizations and the population, causing a negative impact on the country's daily life, we can mention:

1. Attacks that have included DDoS



Background collected during January and up to February 23 confirms the massive DDoS-type attacks against government organizations, banks, and individuals, which seek to stop part or all of the availability of associated services.

At this point, more than 70 government websites and 2 large Ukrainian banks lost their services, confirming the loss of access to different services provided to clients for up to 3 hours, distributed in high-impact hours (peak) for the target’s daily operations.

2. Use of destructive malware

In January 2022, several Ukrainian organizations were victims of an alleged ransomware attack, which ultimately sought not only to encrypt files on the victim's computer but also to corrupt the storage unit, making its restoration impossible and, therefore, the recovery of data. Compromised data.

Known as **WhisperGate**, its attacks were mainly focused on government agencies, and a few weeks later, on the 23rd of February (following the major DDoS attacks carried out against Ukraine), an ESET research team reported the existence of new malware with similar characteristics to the **NotPetya** ransomware, who share, among other characteristics, attacks on critical infrastructure in Ukraine and encryption/deletion of files without requesting a ransom.

Both pieces of malware, with a disruptive objective and the evident intention of causing damage, affect the integrity and availability of information.

3. External groups taking part in the war

The well-known hacktivist collective Anonymous has taken an active part (according to its own attribution) in the **"Pro Ukraine"** movements, carrying out operations against Russia and claiming responsibility for a DDoS attack carried out on the 24th of February on the Kremlin's website.

In the same way, the group behind the Conti ransomware, which to date is the one that has accumulated the most victims, also made a statement informing that it explicitly supports Russia and that it will take action against the critical infrastructure of any entity that tries to carry out any cyber-attack against the country.

4. Ukraine's call to support its defense

After the offensive carried out by Russia against Ukraine on the 24th of February, different organized sources in the Ukraine called for support for its defense, requesting international cooperation (publicly requested from Spain) and the recruitment of cybersecurity experts and hackers.

Previously, to protect critical infrastructure and carry out cyber espionage missions against Russian troops, where Lithuania, the Netherlands, Poland, Estonia, Romania, and Croatia have sent cybersecurity experts to support Ukraine.

5. Phishing campaigns against Ukrainian citizens

Different media outlets reported a massive phishing campaign against Ukrainian citizens on the morning of February 25.

Some sources of information suggest that this action is clearly a way of compromising personal devices to steal information, hijack equipment and even cause panic in the population.

In the strategic view of this campaign, it is believed that it could be a way to recruit new bots (zombie teams) to carry out a new phase of attacks against Ukraine from within the nation.

6. Main threat actors present in the conflict

To have a complete overview of recent events regarding the Russian-Ukrainian conflict, it is necessary to mention the main threat actors involved in operations carried out on Ukrainian territory:

UNC1151:

The malicious actor, also known as "Ghostwriter," whose evidence suggests that his origin is Belarus. He is credited with the

WhisperGate destructive malware attack on Ukrainian government entities in January 2022.

SANDWORM:

The espionage-oriented Sandworm group has used many resources when carrying out offensive activities, mainly characterized by its penchant for "Black Energy" malware; this group has often updated publicly available malware to aid targeted activity that was integrated in a good way with a zero-day attack originated by this group. This group originates from Russia and is presumed to lead and support UNC1151 in operations.

TA505:

Coming from Russia, it carries out operations against banking entities from different countries, including Ukraine, through attacks with malware of the RAT type and Ransomware Clops. It is credited with the current reactivated "**MirrorBlast**" and "**Emotet**" Phishing campaign and exploiting M.S. Exchange vulnerabilities combined with Squirrelwaffle.

TA551:

Group of cyber actors, also known as **Shathak or GOLD CABIN**, focus on the active distribution of banking Trojans in Ukraine, aiming to obtain credentials and access to victims' accounts.

These cyber actors are a malware-related threat group used in the Russian-speaking underground that has been active since at least 2018. The threat group has targeted the energy, healthcare, finance, manufacturing, and insurance sectors in the Americas. North, South America, Europe, and Japan.

APT28:

APT28 is a cyber espionage group with a nexus to Russia that has employed a variety of methodologies and malware, including Spear Phishing, watering holes, credential harvesting, and the exploitation of mobile platforms in executing global espionage campaigns.

The objectives of the APT28 campaign indicate a specific interest in gathering information intended to provide a political and military advantage. These operations have been detected primarily affecting public and private sector entities in the U.S., Europe, Norway, and Japan, as well as government and military targets in other regions, such as South America, the Middle East, and entities in Mexico and Turkey.

APT29:

APT29 is a cyber espionage actor related to Russia. According to the available background, APT29 is a Nation State-sponsored group in Russia. This group has excellent technical capabilities, including a range of tools tailored to each attack, and an extensive command and control (C2) infrastructure, including compromised infrastructure and high-level operational security.

The main objectives of these cyber actors based on where they have focused on stealing information and critical data to date are the areas of financial services, governments, manufacturing, and hospitals, among others. These operations have been detected mostly in European and North American countries.

TEMP.Armageddon (or Gamaredon):

Campaigns with Russia have been observed since at least 2013. Their primary goal is to gather intelligence on Ukrainian national security and law enforcement entities in support of the Russian national interest.

In the ongoing conflict in eastern Ukraine, this group is believed to be continuing espionage operations against Ukrainian targets and further developing its technical capabilities.

Dev-0586 or UNC2589:

A financially motivated group that has operated with a high degree of secrecy and was detected in 2020, where it distributed malware through spear-phishing campaigns intending to steal information and compromise access against the financial industry and banking, health, engineering, and retail, concentrating its activities in countries in Europe, Asia, Africa, and Australia.

CHAPTER 5

BALTIC COUNTRIES; VICTIMS OF CYBER-ATTACKS LAUNCHED BY RUSSIA

The United States, Poland, and the Baltic countries have suffered the most attacks since the beginning of the Russian invasion. One of the conclusions of the extensive report prepared by Microsoft details how Russian intelligence agencies have increased network penetration and espionage activities against Ukraine's allied countries since the 24th of February.

ESTONIA
Peipus
Saaremaa
Kuressaare
Pärnu
Viljandi
Tartu
Lake Pskov
BALTIC
Gulf of Riga
Pskov
Kolka
Valga
Voru
RUSSIA
Ventspils
Valmiera
Mersrags
Cesis
Aluksne
Stende
Gulbene
RIGA
Tukums
Jurmala
LATVIA
Ogre
Saldus
Velikaya
Liepaja
Jelgava
Rezekne
Jekabpils
Daugava
Mazeikiai
Kretinga
Siauliai
Daugavpils
Klaipeda
Rietavas
Panevezys
LITHUANIA
Silute
Taurage
Kedainiai
Ukmerge
Nemen
Jonava
Svencioneliai

Experts warn that Vladimir Putin's government's actions are intended to undermine Western unity and bolster its war efforts. His strategy in the cyber field for the invasion of Ukraine is based on three pillars: destructive cyberattacks against the neighboring country, network penetration and espionage outside of Ukrainian territory, and digital operations to gain global influence.

Russia's top target has been the United States, but its second choice has been Poland, where a large portion of the logistical distribution of military and humanitarian aid is organized. The Baltic republics have also been the focus of Russian activity, as have computer networks in Denmark, Norway, Finland, Sweden, and Turkey over the previous two months. Microsoft has also noted targeted assaults against other NATO nations' foreign ministries.

Governments have been given priority by Russian targets, particularly among NATO allies. However, the list of targets also includes humanitarian organizations, I.T. firms, electricity suppliers, and other crucial infrastructure providers.

And of all those cyberattacks, 29% were successful, which in some cases meant that the hackers seized private information from the attacked organization.

Baltic countries wonder: are we next?

VILNA, Lithuania — Seen from Paris, London, and Washington, the events unfolding in Ukraine may seem like a new Cold War brewing in Europe, but from the Baltics, they look much worse.

Many Estonians, Latvians, and Lithuanians, especially those who are old enough to have lived under Soviet rule, are deeply frightened that they could be the Kremlin's next targets due to Russia's antagonism toward Ukraine.

Rising tensions before the incident brought back memories of oppression and mass deportations.

The Baltic States were shocked by the Russian onslaught on Ukraine. A state of emergency was declared in Lithuania, and many Russian television stations suspected of spreading propaganda and misinformation had their broadcasting licenses canceled in Latvia.

Josef Stalin captured and annexed the three Baltic States during World War II, and they didn't regain their freedom until the Soviet Union fell apart in 1991. In 2004, they became members of NATO, coming under the military protection of the United States and its allies. Westerners. Ukraine is not part of NATO.

The Baltic republics and Poland, another NATO member, have been among the strongest proponents of tighter sanctions against Moscow and NATO, strengthening the alliance's eastern border.

The heads of the Baltic countries recently visited major European cities, asking the West to hold Russian President Vladimir Putin accountable for attacking Ukraine, or their tanks will continue to advance through other regions of the former Soviet empire.

"The conflict over Ukraine is a conflict over Europe. During a joint news conference with U.S. Defense Secretary Lloyd Austin last week, Lithuanian Foreign Minister Gabrielius Landsbergis warned that he would move further if Putin was not stopped there.

Two days before the attack, U.S. President Joe Biden announced that some U.S. troops have been deployed in Europe, including 800-

foot soldiers, F-35 fighter jets, and Apache helicopters, would be flown to the three Baltic States, in a step he said was purely defensive.

The news was received with enthusiasm in the Baltic capitals. Although the NATO treaty commits all allies to defend any member that is attacked, the Baltic States say the alliance needs to show its resolve not just with words but also with troops on the ground.

"Russia always measures military might, but also the will of countries to fight," said Janis Garrisons, secretary of State at the Latvian Defense Ministry. "Once they see a weakness, they exploit it."

Many people in Estonia, Latvia, and Lithuania worry that Putin wants to regain influence in all the former Soviet Union republics, whose collapse he once described as a tragedy for the people. However, he has not publicly expressed any desire to reassert Russian control over the Baltic States (Russian).

Lithuania borders Kaliningrad, a Russian region home to the Russian Baltic Fleet, and Belarus, the former Soviet republic where tens of thousands of Russian soldiers are deployed for joint exercises. Recently, the Belarusian government announced that the maneuvers would continue due to tensions in eastern Ukraine.

The Baltic countries have expressed strong support for Ukraine. The rulers of those nations have recently traveled to Kyiv to show their solidarity and have sent weapons and humanitarian aid.

Although the Baltic countries are direct neighbors of Russia, Kaljulaid says that other European countries should be equally concerned about the crisis in Ukraine.

CHAPTER 6

TELEGRAM IN WAR, BATTLES IN CYBERSPACE

More and more cybercriminals and hacktivists use the Telegram messaging application to carry out activities as the conflict between Russia and Ukraine escalates.

According to a cybersecurity analysis carried out by the Israeli agency Check Point Research, it was found that the volume of users has grown up to 100 times a day in the groups related to Telegram, reaching a maximum of 200,000 per group.

Anti-Russian cyberattack groups stand out, including the Ukrainian government-backed I.T. Army, which consists of 270,000 users focused on conducting distributed denial-of-service (DDoS) attacks against some Russian entities.

Researchers at the Check Point agency noted that other hacktivism-focused Telegram groups coordinate attacks against Russian targets via DDoS, SMS, or call-based attacks of the **Anna and Mark type.**

In addition to using Telegram groups to communicate and coordinate strategic actions, cyber criminals want to capitalize on the thousands of users to "raise funds for Ukraine" and spread news and reports on the conflict's progress to bypass the mainstream media.

Telegram, for its part, commented that it has considered removing or restricting some malicious groups so that the platform is not abused and to ensure that information is not misunderstood.

Cyber activism in defense of Ukraine or self-interest?

Research shows that phishing emails sent in East Slavic languages, written in Russian and Ukrainian, have also multiplied by seven.

Additionally, a third of these phishing emails targeting Russian recipients were sent from either real or spoofed Ukrainian email addresses.

One of the most active groups in cyberspace during the war in Ukraine are hacktivists who support Russia or Ukraine for ideological reasons. Research revealed that these currently generate the most "noise" around the conflict but not always the most damage.

With this, it is clear that cyber activism groups are more focused on attracting followers that they can then use for their benefit since, in many of these groups, information with phishing or identity theft links is published.

List of cyber targets

Cyber hacktivists are choosing Telegram to transfer messages, cyber weapons, and online tools and are "pointing" attackers to relevant Russian targets. Since the beginning of the war, dozens of groups have been created daily, and some have more than 250,000 users. Check Point Research estimates that about 23% of them try to unite hackers, professionals, and computer "hobbyists" to carry out an offensive against Russian targets in cyberspace. In addition, they are used to coordinate the attack, decide the "targets," and share the results, even offering mutual help. DDoS attacks have become a prevalent cyber weapon, with anti-Russians targeting targets they favor and asking users in the group to follow them.

For example, the Anna group calls on its followers to attack Russian targets through DDoS attacks, SMS, or calls.

Another example is the "Mark" group calling users to attack Russian websites by providing URLs.

Since the outbreak of the conflict on the 24th of February, the researchers have closely followed the growing activity managed on Telegram and have detected that the groups related to the conflict have multiplied almost 6 times compared to the day before the invasion. Thus, these groups have been classified into four aspects:

- **a.** Flash News and Updates (71% of groups observed).
- **b.** Hacking\hacktivist groups targeting Russia (23%).
- **c.** Requests for donations to Ukraine (4%).
- **d.** Other issues related to the conflict, some not active and without users (2%).

Characteristics and examples of Group A: flash news & updates

- Very active.
- Thousands of messages a day, 24/7.
- They report raw, uncensored news from war zones.
- They share unverified and possibly erroneous information.
- The graphical user interface, Application Description are automatically generated.

Characteristics and examples of Group B: hacktivists targeting Russia

- Formed by hackers, computer professionals, and amateurs.
- Groups are used to coordinate attacks and decide on targets.
- They help each other execute the attacks and share the results.
- Some are made up of more than 250,000 users.
- The most common attack request is DDoS, followed by SMS and call-based attacks.

Characteristics and examples of Group C: donation scams

- Most donations ask for cryptocurrencies.
- They have tens of thousands of users.
- Many groups are suspicious and probably fraudulent.

Russian DDoS attack on Lithuania was planned on Telegram, Flashpoint says

According to the security firm Flashpoint, the Telegram channel, the Russian cyber collective Killnet posted evidence of potential coordination with the ransomware gang Conti in its hacking effort against Lithuania.

Before a significant DDoS (distributed denial of service) attack, information about cyberattacks by the Russian hacker collective Killnet against the government and private institutions of Lithuania, as well as the group's potential cooperation with the Conti hacking gang, was shared on the Telegram messaging service, according to cybersecurity firm Flashpoint.

In response to Lithuania's June 18 limitations on trade routes with Russia, Killnet has claimed many attacks against Lithuanian organizations on its Telegram channel **"WE ARE KILL NET."**

According to a blog post by Flashpoint, Killnet did issue a warning about the attacks on the Telegram channel, demonstrating how frequently threat actors use the cloud-based instant messaging service to communicate.

DDoS attacks target infrastructure targets in Lithuania.

During the invasion of Ukraine, Killnet swore loyalty to the Russian government. To that end, according to Flashpoint, it started a campaign of retaliation against Lithuania for its sanctions, which included several DDoS assaults on infrastructure targets, including airports, a number of well-known companies, and governmental websites, including those of Lithuania's police departments and its defense ministry.

DDoS attacks are malicious attempts to obstruct a server, service, or network's traffic for a short period of time or permanently, denying the intended users access to the resources.

Reuters received a statement from Killnet stating: "The attack has "disrupted 1652 websites and will continue until Lithuania removes the blockage," it continued. And that is all there is."

Specifically in the transportation, energy, and financial sectors, the Lithuanian National Cyber Security Center told Reuters that it anticipates "attacks of a similar or larger intensity in the coming days."

Flashpoint disclosed that it had discovered communication suggesting that the "current impasse between Russia and Lithuania could develop to a full-fledged military clash" on several pro-Russian Telegram channels. Flashpoint noted that it has not yet observed any evidence indicating that Telegram plotting has resulted in actual physical violence.

The concept for a massive coordinated attack on the 27th of June—also known as "Judgement Day"—was discussed in a chat on the 25th of June on the Killnet Telegram channel. Flashpoint analysts also noticed several more minor attacks, one of which occurred on the 22nd of June.

SPECIAL THANKS

- **Nils Putnins** (np@seq.lv)
- **Martins Lielbardis** (ml@seq.lv)
- **Kaspars Vaverins** (kv@seq.lv)
- **Luize Lismane - Ruce**
- **Peteris Rucis**
- **Saqib Arshad**

And to the defenders and citizens of Ukraine who are selflessly fighting this war for Europe as a whole.