Report on the Russian Use of Offensive Cyber Capabilities in the Course of the Military Aggression in Ukraine

Report on the Russian Use of Offensive Cyber Capabilities in the Course of the Military Aggression in Ukraine

Contents

1 / Preface

The Regional Cyber Defence Centre (RCDC), under the National Cyber Security Centre, has contracted Dr Tadas Jakstas, cybersecurity capacity-building consultant to provide professional services for the development of a Report on the Russian Use of Offensive Cyber Capabilities in the Course of the Military Aggression in Ukraine.

The overall objective of the Project is to contribute to RCDC activities by developing a Report on the use of Russia's offensive cyber capabilities in Ukraine.

This document marks the completion of the analysis of Russia's offensive cyber capabilities during the military conflict in Ukraine.

This Report was developed by Dr Tadas Jakstas.

2 / List of Acronyms

Table 1. Terms and abbreviations

Term/abbreviation	Meaning/explanation
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CERT	Computer Emergency Response Team
CTL	Cybersecurity Threat Landscape
DDoS	Distributed Denial of Service
FSB	Federal Security Service
GRU	The Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICS	Industrial Control System
IT	Information Technology
OT	Operational Technologies
RCDC	Regional Cyber Defence Centre
NCSC	National Cyber Security Centre
TTP	Tactic, Techniques and Procedures
SCADA	Supervisory Control and Data Acquisition
SVR	The Foreign Intelligence Service of the Russian Federation

3 / Introduction

3.1 Context and Objectives of the Project

Established as a joint initiative of Lithuania and the United States, the Regional Cyber Defence Centre (RCDC) aims to fill the niche of multilateral practical cooperation in the field of cyber defence and to strengthen the capacity of both, Lithuania and regional partners to ensure the cyber security of the state's critical infrastructure. RCDC develops its activities in three main directions, conducting cyber threat analysis, organizing exercises for critical infrastructure managers and practical research. One of the main goals of the RCDC is to become a regional platform for practical cooperation to help protect critical infrastructure from cyber-attacks. Therefore, to achieve this objective, RCDC activities focus on building up the resilience and cyber defence capacity in public critical service providers.

The overall objective of the Project is to **contribute to RCDC activities** by developing a **Report on Russia's use of offensive cyber capabilities during the military aggression in Ukraine**. More specifically, the Report provides a systemic analysis of Russia's cyber capabilities, including the analysis of major cyber-attacks against the Ukrainian state and private sector organizations during the Russian military aggression in Ukraine. It is expected that this intervention will result in several key outcomes for the RCDC:

1. **An increased understanding** of Russia's cyber offensive capabilities and the scale of their use during the military aggression in Ukraine.
2. **Raised awareness** of RCDC partners and the wider public on the most critical threats posed by Russia's threat actors.

3.2 Approach and Methodology

To achieve the Project objectives, development of the Report on the Russian use of offensive cyber capabilities during the military conflict in Ukraine is based on:

1. Inception meetings – to set expectations with RCDC representatives on the development of the Report.
2. Desk research – an in-depth review and analysis of international studies and Reports as well as RCDC-provided information on Russia's cyber offensive capabilities (main threats and threat groups) and their use in the course of Russia's military aggression in Ukraine.

The research activities culminate in the Report on the Russian use of offensive cyber capabilities in the course of the military aggression in Ukraine that provides a systemic analysis of Russia's cyber capabilities, including key Russian state-backed APT persistent threat groups, their modus operandi, past attacks on critical infrastructure and state institutions/organizations in Ukraine. In addition, the Report will identify and analyse major cyber-attacks against Ukrainian state and private sector organizations during the Russian military aggression in Ukraine, based on open-source analysis and RCDC provided threat information.

3.3 Proposed Structure of the Report

This Report aims to provide a comprehensive analysis of Russia's offensive cyber capabilities during the military conflict in Ukraine.

Chapter 4 starts with an analysis of Russia's cyber offensive capabilities, including key Russian state-backed APT persistent threat groups and their modus operandi. In addition, assessment of several case studies of past attacks on critical infrastructure and state institutions/organizations in Ukraine, including of 2015 and 2016, is be provided. Moreover, it identifies and analyses major cyber-attacks against the state of the Ukrainian state and private sector organizations during the Russian military aggression in Ukraine starting from the beginning of 2022.

Chapter 5 elaborates on some of the recommended mitigation measures for countering Russia's cyber offensive operations.

Chapter 6 summarises the main insights and findings of the analysis. ction of classified information.

4 / Russia's Cyber Offensive Capabilities

4.1 Russian State-Sponsored and Criminal Cyber Threats

Russia is one of the world's most prolific cyber actors that dedicates significant resources to conducting cyber operations around the globe. The Russian Government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.

Even before events in Ukraine, Russian state-sponsored cyber actors had demonstrated capabilities used to compromise IT networks, develop mechanisms to maintain long-term, persistent access to IT networks, exfiltrate sensitive data from IT and operational technology (OT) networks, and to disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.

Moreover, advisories published by CISA and other unclassified sources associate Russian actors with a range of high-profile malicious cyber activities, including the 2020 compromise of the SolarWinds software supply chain, the 2020 targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of the U.S industrial control system infrastructure, the 2017 NotPetya ransomware attack on organizations worldwide, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee.

Next sections of the Report provide a more detailed assessment of cyber threat actors from the following Russian governmental and military organizations who have carried out malicious cyber operations against IT and/or OT networks:

- The Russian Federal Security Service (FSB), including FSB's Centre 16 and Centre 18
- The Russian Foreign Intelligence Service (SVR)
- The Military Intelligence Service (GRU)
- The Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

Figure below provides an overview of the Russian Intelligence Services Cyber Structure

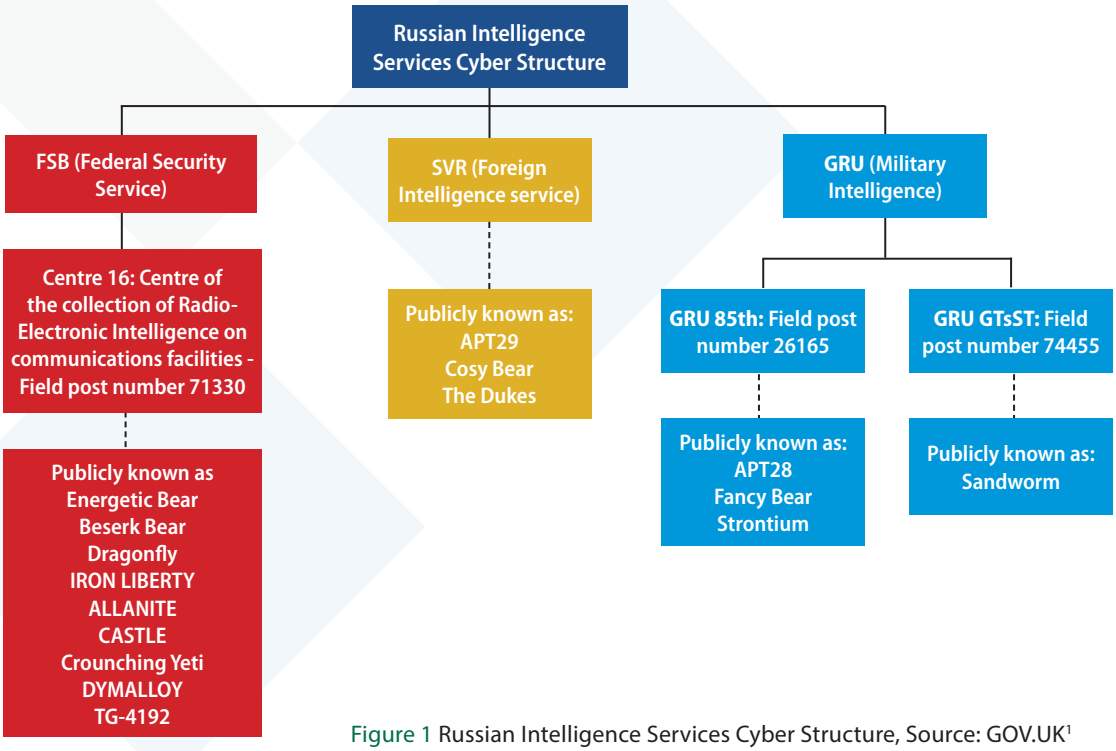

Figure 1 Russian Intelligence Services Cyber Structure, Source: GOV.UK[1]

[1] https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

4.1.1 The Russian Federal Security Service (FSB)

FSB, the KGB's successor agency, has conducted malicious cyber operations targeting the Energy Sector, including UK and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. FSB has been known to task criminal hackers with espionage-focused cyber activity; these same hackers have separately been responsible for disruptive ransomware and phishing campaigns[2].

FSB Centre 16 (16-й Центр) is responsible for cyber operations including the intercepting, decrypting and processing of electronic messages, and the technical penetration of foreign targets. Its full title is the Centre for Radio-Electronic Intelligence by Means of Communication (TsRRSS; Russian: Центр радиоэлектронной разведки на средствах связи (ЦРРСС)) and is also known as "Military Unit 71330" (V/Ch 71330) (Войсковая часть В/Ч 71330)[3].

Dragonfly[4]: is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Centre 16 or Military Unit 71330[5] [6]. Active since at least 2010, Dragonfly has targeted entities in Western Europe and North America, including state, local, tribal, and territorial (SLTT) organizations, as well as Energy, Transportation Systems, and Defense Industrial Base (DIB) Sector organizations, Water and Wastewater Systems Sector and other critical infrastructure facilities worldwide.

In the first phase of its activity, which took place between 2012 and 2014, and is commonly referred to by cyber security researchers as "Dragonfly" or "Havex," the group engaged in a supply chain attack, compromising the computer networks of ICS/SCADA system manufacturers and software providers and then hiding malware – known publicly as "Havex" – inside legitimate software updates for such systems. After unsuspecting customers downloaded Havex-infected updates, the conspirators would use the malware to, among other things, create backdoors into infected systems and scan victims' networks for additional ICS/SCADA devices. Through these and other efforts, including spear phishing and "watering hole" attacks, the conspirators installed malware on more than 17,000 unique devices in the United States and abroad, including ICS/SCADA controllers used by power and energy companies[7].

In the second phase, which took place between 2014 and 2017 and is commonly referred to as "**Dragonfly 2.0**," the group transitioned to more targeted compromises that focused on specific energy sector entities and individuals and engineers who worked with ICS/SCADA systems. During the Dragonfly 2.0 phase, the conspirators also undertook a watering hole attack by compromising servers that hosted websites commonly visited by ICS/SCADA system and other energy sector engineers through publicly known vulnerabilities in content management software. When the engineers browsed to a compromised website, the conspirators' hidden scripts deployed malware designed to capture login credentials onto their computers[8].

Common TTPs[9] include scanning to exploit internet-facing infrastructure and network appliances, conducting brute force attacks against public-facing web applications, and leveraging compromised infrastructure–often websites frequented or owned by their target–for Windows New Technology Local Area Network Manager (NTLM) credential theft. Industry reporting assesses that this actor has a destructive mandate[10].

---

2 https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

3 https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

4 Also known as: TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear, Berserk Bear, Dymalloy, and Temp.Isotope

5 https://attack.mitre.org/groups/G0035/

6 https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

7 https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

8 https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

9 For more detailed information about TTPs used by Dragonfly threat actor, please refer to: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0035%2FG0035-enterprise-layer.json

10 https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

Gamaredon[11]: is a suspected Russian cyber espionage threat group that has targeted military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine since at least 2013. The name Gamaredon Group comes from a misspelling of the word "Armageddon", which was detected in the adversary's early campaigns. In November 2021, the Ukrainian government publicly attributed Gamaredon Group to Russia's Federal Security Service (FSB) Centre 18. The group is an integral part of the so-called "Office of the FSB of Russia in the Republic of Crimea and the city of Sevastopol" and consists of regular officers of the secret service and some former law enforcement officers of Ukraine[12].

The main purpose of its activity is to conduct targeted cyber intelligence operations against state bodies of Ukraine, primarily security, defense and law enforcement agencies, in order to obtain intelligence information[13]. Armageddon does not use complex and sophisticated techniques, tactics and procedures, does not try to make an effort to stay secret for a long time. Staying off the radar is not a group priority. However, the group's activities are characterized by intrusiveness and audacity.

The cyber attack mechanism is based on the principle of simultaneous mass destruction of a large number of users inside one organization and the deployment of malicious software. When the victim's computer system loses control, the attackers try to regain access to the source of the information and try again to compromise them according to a similar scenario. Malicious software modules have been created with the help of programming languages VBScript, VBA Script, C#, C++, as well as using CMD, PowerShell and .NET command shells[14].

4.1.2 Russian Foreign Intelligence Service (SVR)

The Foreign Intelligence Service (SVR) is Russia's primary civilian foreign intelligence service. It is responsible for the collection of foreign intelligence using human, signals, electronic, and cyber methods. Most observers acknowledge the SVR operates with a strong emphasis on maintaining secrecy and avoiding detection. Most cyber operations reportedly linked to the SVR have focused on collecting intelligence. The SVR also is known to have high levels of technical expertise, often seeking to gain and retain access inside compromised networks[15].

APT29[16]: is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR)[17]. They have operated since at least 2008, often targeting consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. APT29 Reportedly compromised the Democratic National Committee starting in the summer of 2015[18].

In recent year, APT29 activity reportedly has increased, and the unit has been linked to numerous cyberespionage operations. For example, in April 2021, the U.S. government identified APT 29 as responsible for the SolarWinds attack that exploited supply chain vulnerabilities to infiltrate U.S. government and private sector networks[19]. The group's compromise of the SolarWinds software supply chain gave it the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide. The scope of this compromise is considered as national security and public safety concern. In a cybersecurity advisory alert, U.S. government noted APT 29 will "continue to seek intelligence from U.S. and foreign entities through cyber exploitation, using a range of initial exploitation

[11] Also known as: IRON TILDEN, Primitive Bear, ACTINIUM, Armageddon, Shuckworm, DEV-0157

[12] https://attack.mitre.org/groups/G0047/

[13] https://ssu.gov.ua/uploads/files/DKIB/Technical%20Report%20Armagedon.pdf

[14] https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0047%2FG0047-enterprise-layer.json

[15] https://crsReports.congress.gov/product/pdf/IF/IF11718

[16] Also known as: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke.

[17] https://attack.mitre.org/groups/G0016/

[18] https://abcnews.go.com/International/russia-linked-hackers-accused-stealing-covid-vaccine-data/story?id=71819152

[19] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks"[20].

Common TTPs[21] include password spraying to identify a weak password associated with an administrative account. The actor conducted the password spraying activity in a "low and slow" manner, attempting a small number of passwords at infrequent intervals, possibly to avoid detection. Moreover, SVR actor regularly use publicly known vulnerabilities to conduct widespread scanning and exploitation against vulnerable systems in an effort to obtain authentication credentials to allow further access. Furthermore, SVR group targets organisations who supply privileged software to intelligence targets. In addition, SVR typically deploy a web shell on Microsoft Exchange servers following successful compromise. In fact, the group focuses on computer systems running the Windows, although we know about the test use of the EvilGnome malware (to defeat Linux systems), as well as attempts to get access to Android devices. Analysis of the group's tactics since its first appearance on the "landscape" of cyberspace allows us to divide its activities into 2 periods: from 2014 to 2017 and from 2017 to the present day. This divide is due to the evolution of tools. Though, there is little information about Armageddon's early days, based on the available data, members of the group relied on legitimate, publicly available software products in the early years of their existence, which was eventually changed to customized malware Pterodo/Pteranodon. At the first stage, the minimum required set of software consisted of dropper files sent with phishing emails, as well as remote access tools, which were installed after users opened malicious applications and provided remote access to the information system. Such tools include RMS (Remote Manipulator System) and UltraVNC. The second stage, starting in 2016, is characterized by the transition to customized malware called Pterodo/Pteranodon, which widely expanded the functionality of the group[22].

4.1.3 Military Intelligence Service (GRU)

The Main Directorate of the General Staff, commonly referred to as the GRU, is Russia's military intelligence agency. The GRU has been implicated in some of Russia's most notorious and damaging cyber operations. Media reporting and U.S. government indictments identify two primary GRU cyber units, i.e., Unit 26165 and Unit 74455. The U.S. Department of Justice (DOJ) has charged personnel from both units for actions ranging from election interference in the 2016 U.S. presidential election to multiple damaging cyberattacks. The units' public profile underlines a high operational tempo. The GRU Reportedly also controls several research institutes that help develop hacking tools and malware. Observers have noted an apparent willingness by GRU cyber units to conduct brazen and aggressive operations, sometimes with questionable levels of operational security and secrecy. Cyber analysts have referred to these units collectively as APT (Advanced Persistent Threat) 28, Fancy Bear, Voodoo Bear, Sandworm, and Tsar Team[23].

APT28[24]: a threat group, attributed to GRU's unit 26165, has been active since at least 2004. It is one of two Russian cyber groups identified by the U.S. government as responsible for hacking the Democratic Congressional Campaign Committee, Democratic National Committee, and presidential campaign of Hillary Clinton. The group is also linked to cyber operations against numerous political, government, and private sector targets in the Caucasus (especially the Georgian government), Eastern European governments and militaries, and specific security organizations, including NATO and OSCE[25]. In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations[26].

[20] https://crsReports.congress.gov/product/pdf/IF/IF11718

[21] For more detailed information about TTPs used by APT29, please refer to: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json

[22] https://ssu.gov.ua/uploads/files/DKIB/Technical%20Report%20Armagedon.pdf

[23] https://crsReports.congress.gov/product/pdf/IF/IF11718

[24] Also known as: IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127.

[25] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

[26] https://attack.mitre.org/groups/G0007/

APT28[27] frequently collect credentials to gain initial access to target organizations. The actor collects victim credentials by sending spear phishing emails that appear to be legitimate security alerts from the victim's email provider and include hyperlinks leading to spoofed popular webmail services' logon pages. APT28 have also registered domains to conduct credential harvesting operations. These domains mimic popular international news, politics, social media platforms and masquerade as tourism- and sports-related entities and music and video streaming services. Moreover, since 2007, APT28 has systematically evolved its malware, using flexible and lasting platforms indicative of plans for long-term use. The coding practices evident in the group's malware suggest both a high level of skill and an interest in complicating reverse engineering efforts[28]. APT28 malware, in particular the family of modular backdoors that we call CHOPSTICK, indicates a formal code development environment. Such an environment would almost certainly be required to track and define the various modules that can be included in the backdoor at compile time. The group tailors implants for specific victim environments. They steal data by configuring their implants to send data out of the network using a victim network's mail server.

Sandworm[29]: a threat group, attributed to GRU's unit 74455, has been active since at least 2009. In October 2020, the US indicted six GRU Unit 74455 officers associated with Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential campaign, the 2018 Olympic Destroyer attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019[30].

The threat group has used several techniques to compromise a large volume of targets in recent years. The most common TTPs[31] used by the Sandworm group includes:

- Phishing: Spear phishing campaigns were used by the Sandworm group to gain access to computers or account credentials. The emails were specially crafted to seem familiar and trusted. The threat group developed and tested all the spear phishing techniques before carrying out their campaigns to increase their success chances.
- Command and scripting interpreter: The threat group used PowerShell commands and specially crafted scripts to discover system information, execute code or download malware.
- Valid accounts: Sandworm used legitimate existing accounts to maintain its foothold on the infrastructure. The group also deployed malware and took advantage of hacking tools to maintain control over networks and victims' devices. This TTP was also used to exfiltrate data, including confidential documents, tools and more.
- Masquerading: Sandworm tried to masquerade their activity through researching and emulating malware used by the Lazarus Group[32].
- OS credential dumping: Sandworm often dumped credentials to obtain account login and credential details from compromised machines.
- Exploitation of remote services: Sandworm exploited remote services to access internal systems. When the access was completed, they deployed malware that was leveraged to obtain system privileges and execute or implant other stages.
- Defacement: Sandworm defaced approximately 1,500 websites and disrupted service to some of those websites following the Georgian web hosting provider's compromise.

---

[27] For more detailed information about TTPs used by APT28, please refer to: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json

[28] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

[29] Also known as: ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR.

[30] https://attack.mitre.org/groups/G0034/

[31] For more detailed information about TTPs used by Sandworm Group, please refer to: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0034%2FG0034-enterprise-layer.json

[32] https://attack.mitre.org/groups/G0032/

4.1.4 Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

TsNIIKhM, as described on their webpage, is a research organization under Russia's Ministry of Defense (MOD). Actors associated with TsNIIKhM have developed destructive ICS malware.

TsNIIKhM has been sanctioned by the U.S. Department of the Treasury for connections to the destructive Triton malware (also called HatMan and TRISIS)[33]; TsNIIKhM has been sanctioned by the UK Foreign, Commonwealth, and Development Office (FCDO) for a 2017 incident that involved safety override controls (with Triton malware) in a foreign oil refinery[34]. In 2021, the U.S. DOJ indicted a TsNIIKhM Applied Development Centre (ADC) employee for conducting computer intrusions against U.S. Energy Sector organizations. The indicted employee also accessed the systems of a foreign oil refinery and deployed Triton malware[35]. Triton is a custom-built malware designed to manipulate safety instrumented systems within ICS controllers, disabling the safety alarms that prevent dangerous conditions.

TEMP.Veles[36] is a Russia-based threat group, attributed to TsNIIKhM, that has targeted critical infrastructure[37]. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems. FireEye Intelligence assessed with high confidence that intrusion activity that led to deployment of TRITON was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM; a.k.a. ЦНИИХМ), a Russian government-owned technical research institution located in Moscow[38].

The most common TTPs[39] used by TEMP.Veles includes:

- Drive-by Compromise - TEMP.Veles utilizes watering hole websites to target industrial employees.3
- Remote Services - TEMP.Veles utilized remote desktop protocol (RDP) jump boxes to move into the ICS environment.4
- Supply Chain Compromise - TEMP.Veles targeted several ICS vendors and manufacturers.5
- Valid Accounts - TEMP.Veles used valid credentials when laterally moving through RDP jump boxes into the ICS environment.

4.1.5 Russian-Aligned Cybercrime Groups

Cybercrime groups are typically financially motivated cyber actors that seek to exploit human or security vulnerabilities to enable direct theft of money (e.g., by obtaining bank login information) or by extorting money from victims. These groups pose consistent threats to critical infrastructure organizations globally.

Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine. These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations primarily through:

- Deploying ransomware through which cyber actors remove victim access to data (usually via encryption), potentially causing significant disruption to operations.
- Conducting DDoS attacks against websites.

[33] https://home.treasury.gov/news/press-releases/sm1162

[34] https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents

[35] https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

[36] Also known as: XENOTIME.

[37] https://attack.mitre.org/groups/G0088/

[38] https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools

[39] For more detailed information on TTPs used by TEMP.Veles threat actor, please refer to: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0088%2FG0088-enterprise-layer.json

- In a DDoS attack, the cyber actor generates enough requests to flood and overload the target page and stop it from responding.
- DDoS attacks are often accompanied by extortion.
- According to industry reporting, some cybercrime groups have recently carried out DDoS attacks against Ukrainian defense organizations, and one group claimed credit for DDoS attack against a U.S. airport the actors perceived as supporting Ukraine (see the Killnet section).

Based on industry and open-source reporting, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess multiple Russian-aligned cybercrime groups pose a threat to critical infrastructure organizations[40]. These groups include:

- **The CoomingProject** – is a criminal group that extorts money from victims by exposing or threatening to expose leaked data[41]. Their data leak site was launched in August 2021. The CoomingProject stated they would support the Russian Government in response to perceived cyberattacks against Russia.
- **Killnet** - according to open-source reporting, Killnet released a video pledging support to Russia[42].
- **MUMMY SPIDER** - is a cybercrime group that creates, distributes, and operates the Emotet botnet. Emotet is advanced, modular malware that originated as a banking trojan (malware designed to steal information from banking systems but that may also be used to drop additional malware and ransomware). Today Emotet primarily functions as a downloader and distribution service for other cybercrime groups. Emotet has been used to deploy WIZARD SPIDER's TrickBot, which is often a precursor to ransomware delivery. Emotet has worm-like features that enable rapid spreading in an infected network. According to open sources, Emotet has been used to target industries worldwide, including financial, e-commerce, healthcare, academia, government, and technology organizations' networks.
- **SALTY SPIDER** - is a cybercrime group that develops and operates the Sality botnet. Sality is a polymorphic file infector that was discovered in 2003; since then, it has been replaced by more advanced peer-to-peer (P2P) malware loaders[43].
- **SCULLY SPIDER** - is a cybercrime group that operates using a malware-as-a-service model; SCULLY SPIDER maintains command and control infrastructure and sells access to their malware and infrastructure to affiliates, who distribute their own malware[44] [45]. SCULLY SPIDER develops and operates the DanaBot botnet, which originated primarily as a banking Trojan but expanded beyond banking in 2021 and has since been used to facilitate access for other types of malware, including TrickBot, DoppelDridex, and Zloader. Like Emotet, Danabot effectively functions as an initial access vector for other malware, which can result in ransomware deployment.

  According to industry reporting, recent DDoS activity by the DanaBot botnet suggests SCULLY SPIDER has operated in support of Russia's military offensive in Ukraine.
- **SCULLY SPIDER** affiliates have primarily targeted organizations in the United States, Canada, Germany, United Kingdom, Australia, Italy, Poland, Mexico, and Ukraine[46]. According to industry reporting, in March 2022, Danabot was used in DDoS attacks against multiple Ukrainian government organizations.
- **SMOKEY SPIDER** - is a cybercrime group that develops Smoke Loader (also known as Smoke Bot), a malicious bot that is used to upload other malware. Smoke Loader has been available since at least 2011 and operates as a malware distribution service for a number of different payloads, including – but not limited to – DanaBot, TrickBot, and Qakbot.

[40] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[41] https://ke-la.com/aint-no-actor-trustworthy-enough-the-importance-of-validating-sources/

[42] https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/?msclkid=235244a7ba6611ec92f21c9bd3b8ee49

[43] https://www.crowdstrike.com/blog/who-is-salty-spider/

[44] https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot

[45] https://www.zscaler.com/blogs/security-research/spike-danabot-malware-activity

[46] https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot

- **WIZARD SPIDER** - is a cybercrime group that develops TrickBot malware and Conti ransomware. Historically, the group has paid a wage to the ransomware deployers (referred to as affiliates), some of whom may then receive a share of the proceeds from a successful ransomware attack. In addition to TrickBot, notable initial access and persistence vectors for affiliated actors include Emotet, Cobalt Strike, spearphishing, and stolen or weak Remote Desktop Protocol (RDP) credentials.

  After obtaining access, WIZARD SPIDER affiliated actors have relied on various publicly available and otherwise legitimate tools to facilitate earlier stages of the attack lifecycle before deploying Conti ransomware.

  WIZARD SPIDER pledged support to the Russian government and threatened critical infrastructure organizations of countries perceived to carry out cyberattacks or war against the Russian government[47]. They later revised this pledge and threatened to retaliate against perceived attacks against the Russian people[48].

  Victim organizations span across multiple industries, including construction and engineering, legal and professional services, manufacturing, and retail. In addition, WIZARD SPIDER affiliates have deployed Conti ransomware against U.S. healthcare and first responder networks.
- **The Xaknet Team** - is a Russian-language cyber group that has been active as early as March 2022. According to open-source reporting, the XakNet Team threatened to target Ukrainian organizations in response to perceived DDoS or other attacks against Russia[49]. According to reporting from industry, on March 31, 2022, XakNet released a statement stating they would work "exclusively for the good of [Russia]." According to industry reporting, the XakNet Team may be working with or associated with Killnet actors, who claimed credit for the DDoS attacks against a U.S. airport (see the Killnet section).

4.2 Cyber-attacks against Ukrainian state and private sector organizations

Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine[50]. This campaign not only degraded the functions of the targeted organizations but sought to disrupt citizens' access to reliable information and critical life services, and to shake confidence in the country's leadership. In addition, Russia's cyberattacks prior to the military invasion suggest methodical preparations, with the attackers likely gaining access to Ukrainian networks months ago[51]. Moreover, the correlation of Russia's cyber and kinetic actions during the military conflict demonstrates that Russia used cyber and kinetic attacks collectively in order to disrupt or degrade Ukrainian government and military functions and undermine the public's trust in those same institutions[52].

The magnitude of Moscow's pre-kinetic destructive cyber-operations was unprecedented. On the day of the invasion began, Russian cyber-units successfully deployed more destructive malware, including against conventional military and civilian targets such numerous government agencies, military institutions, civil emergency services, and a range of other critical infrastructure sectors, rendering the computer systems of multiple government, military, and critical infrastructure sectors inoperable. The intent appears to have been to create disorder and overwhelm Ukrainian defenses. Russia sought to disrupt services and install destructive malware on Ukrainian networks included phishing, denial of service, and taking advantage of software vulnerabilities. One company identified eight different families of destructive software used by Russia in these attacks[53].

When it comes to the main targets of cyber-attacks, national government organizations and critical infrastructure sectors were top targets for cyber-attacks. The other attacked organizations included regional and city-level government, agriculture, defense industrial base, healthcare, transportation, and finance, among others[54].

47 https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

48 https://www.techtarget.com/searchsecurity/news/252513982/Conti-ransomware-gang-backs-Russia-threatens-US

49 https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

50 https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar

51 https://eng.majalla.com/node/216041/politicsmyth-missing-cyberwar

52 https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

53 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash

54 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

The chart below shows provides a sample of Ukrainian industries impacted by known or suspected Russia-aligned network intrusions or destructive attacks during the Russian invasion of Ukraine.

Sample set of targets by industry

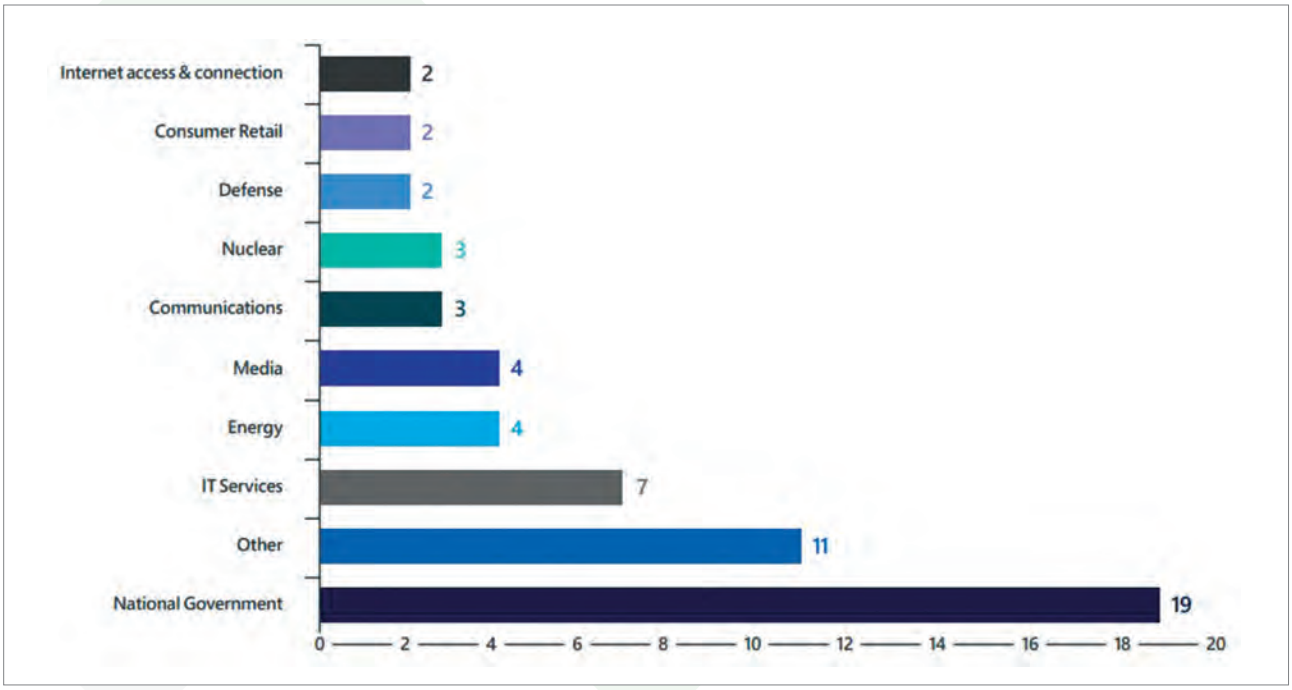

Figure 2 Russian Intelligence Services Cyber Structure, Source: GOV.UK[55]

Russian Advanced Persistent Threat (APT) actors, including Dragonfly, APT29, APT28, Gamaredon, Sandworm, associated with Russia's intelligence services (GRU, SVR, and FSB), have conducted destructive attacks, espionage operations in a pre-war and during the war in Ukraine.

The Table 2 below presents the Russian APT actors mapped with incident number and criticality levels during in the 5 months of 2022.

Table 2. Russian APT actors mapped with incident number and criticality levels

Incident criticality level	Number of incidents	Tracked actors
Low	417	Armageddon, APT29
Medium	207	UAC-0051, UAX-0056
High	366	Sandworm, InvisiMole
Critical	316	APT28, XakNet

In terms of incident types, phishing, malware distribution, defacements, denial-of-service, vulnerability exploitation, account compromise have been among the most common incidents pre- and during military conflict[56].

Russia-aligned cyber operations use several common tactics, techniques, and procedures (TTPs) to execute their intrusions. Some of the most common TTPs included:

[55] https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

[56] Information based on CERT UA presentation during FIRST.org Annual Conference in June 2022.

- Exploitation of public facing applications or spear phishing with attachments/links for initial access.
- Credential theft and use of valid accounts throughout the attack lifecycle, making "identities" a key intrusion vector. This includes within Active Directory Domain and through VPNs or other remote access solutions.
- Use of valid administration protocols, tools, and methods for lateral movement, relying on compromised identities with administrative capability.
- Use of known publicly available offensive capabilities, sometimes obfuscated using actor specific methods to defeat static signatures.
- "Living off the land" during system and network discovery, often utilizing native utilities or commands that are non-standard for the environments.
- Use of destructive capabilities that access raw file systems for overwrites or deletions.

4.2.1 Major cyber incidents against Ukraine before and during military conflict

January 2022: Hackers deployed destructive malware (WhisperGate[57]), masquerading as ransomware, on numerous Ukrainian government, nonprofit, and information technology organizations' systems. Researchers linked this attack to hackers with suspected ties to the Russian GRU[58].

January 2022: Hackers targeted around 70 Ukrainian government websites, taking down several and defacing the Foreign Ministry website. The defacement included a threatening message to Ukrainians and a notice of the exposure of personal data, which was later refuted by Ukraine's Centre for Strategic Communications and Information Security[59].

January 2022: Hackers targeted a Western government agency operating in Ukraine with a phishing attack. The actors uploaded a resume with malware to a Ukrainian job posting platform and submitted it to the government agency. Researchers attributed this attack to a hacking group previously linked to the Russian FSB by the Ukrainian Security Service[60] [61].

February 2022: Hackers targeted a Ukrainian energy company with espionage malware through a phishing attack[62]. The Computer Emergency Response Team of Ukraine (CERT-UA) attributed these attacks to a group with a history of targeting Ukrainian government organizations since at least March 2021 and with suspected ties to the Russian GRU[63].

February 2022: Hackers targeted the Ukrainian banking sector and government websites with a series of DDoS attacks, temporarily taking the websites offline[64]. The United Kingdom and Australia attributed the attacks against financial institutions to the Russian GRU[65] [66].

February 2022: Hackers targeted websites belonging to the Ukrainian banking sector and the Ukrainian government with a DDoS attack, rendering some sites inaccessible[67]. This was the second DDoS attack against Ukrainian banks and government websites in two weeks.

---

57 https://attack.mitre.org/software/S0689/

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

59 https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

60 https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/

61 https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

62 https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

63 https://cert.gov.ua/article/18419

64 https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/

65 https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine

66 https://www.internationalcybertech.gov.au/Attribution-to-Russia-of-malicious-cyber-activity-against-Ukraine

67 https://www.politico.eu/article/minister-ukraine-websites-down-in-another-massive-online-attack/

February 2022: Hackers deployed a destructive malware (HermeticWiper[68]) to destroy around 300 systems across more than a dozen financial, government, energy, information technology, and agricultural organizations in Ukraine[69] [70]. Researchers linked this attack to a Russian GRU-affiliated group.

February 2022: Hackers deployed a destructive malware (IsaacWiper) on a Ukrainian government network[71].

February 2022: Hackers targeted satellite communications company Viasat with destructive malware, disabling modems communicating with Viasat Inc's KA-SAT satellite[72]. The attack impacted connectivity across Ukraine and Europe, as the satellite provides internet access to customers in multiple countries. The United Kingdom, United States, and European Union attributed this attack to Russia[73] [74] [75].

March 2022: Hackers targeted at least 30 Ukrainian university websites. Researchers believe this attack came from a Brazilian-based group that publicly supports Russia[76].

March 2022: Hackers targeted telecom provider Triolan on March 9 and February 24, impacting network connectivity[77]. A source from Triolan claimed the hackers reset the company's computer settings to factory level and some equipment required physical access to restore, which was difficult due to the ongoing crisis.

March 2022: Russian threat actors launched DesertBlade malware against a major broadcasting company on March 1, the same day that the Russian military announced its intention to destroy "disinformation" targets in Ukraine and directed a missile strike against a TV tower in Kyiv. DesertBlade actions and the missile strike demonstrated cyber and kinetic impact to a key source of information to the Ukrainian public[78].

March 2022: Hackers targeted Ukrainians with a phishing attack to deploy malware that compromises user data. The email promised payment "in the amount of 15,000" from the government as support during "this difficult time"[79].

March 2022: A suspected Russian threat actor compromised an institution in Ukraine that was featured in false Russian weapons conspiracies in the past. IRIDIUM, an actor with a history of leaking documents to support disinformation narratives, conducted an intrusion into the same research institution later in March[80].

March 2022: Russian nation state actor stole data from a nuclear safety organization that FSB-affiliated actor BROMINE had compromised in December 2021. BROMINE stole data from this entity from December through mid-March. In the first two weeks of the invasion, Russian troops seized the defunct Chernobyl nuclear power plant and the Zaporizhzhia Nuclear Power plant, the largest in Europe, indicating a clear military interest in nuclear energy targets[81].

---

68 https://attack.mitre.org/software/S0697/

69 https://www.eset.com/sg/about/newsroom/press-releases1/products/hermeticwiper-new-data-wiping-malware-hits-ukraine/

70 https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo#:~:text=Researchers%20from%20the%20cybersecurity%20firms,invade%20its%20neighbor%20were%20imminent

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

72 https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

73 https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion\

74 https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

75 https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

76 https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/

77 https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=a56bd826573e

78 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

79 https://blog.malwarebytes.com/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine%EF%B8%8F/

80 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

81 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

March 2022: Hackers deployed a destructive malware (CaddyWiper) in Ukrainian organizations. Researchers linked this attack to a group affiliated with the Russian GRU[82].

March 2022: A national news broadcast on the television channel Ukraine 24 was breached by hackers on March 16. The program's news ticker was hacked to display messages to appear as though they were coming from Ukrainian President Volodymyr Zelenskyy. The messages urged Ukrainians to stop fighting and give up their weapons, while claiming that Zelenskyy "wanted to take Donbas" but was unsuccessful, so he had fled Kyiv[83].

March 2022: Hackers targeted the systems of Ukrainian state authorities with a phishing attack. According to CERT-UA, the attack came from a group associated with the Luhansk People's Republic (LPR)[84].

March 2022: Hackers targeted several Ukrainian news outlets, defacing the platforms with symbols banned in Ukraine. The Security Service of Ukraine stated they identified the networks and servers used by the attackers[85 86].

March 2022: Hackers deployed a destructive malware (DoubleZero) targeting Ukrainian enterprises[87].

March 2022: Hackers targeted Ukrainian organizations with a phishing attack[88]. The malware uploads a backdoor that allows hackers to access and control system data. CERT-UA attributed these attacks to a group previously announced by the Ukrainian Security Service to have ties to the Russian FSB[89].

March 2022: Threat actors targeted logistics providers and regional government organizations in advance of the Russian military's announcement of a strategic refocus on eastern Ukraine[90]. Researchers linked this attack to a suspected Russian GRU-affiliated group.

March 2022: Hackers used WordPress sites to target 10 websites with DDoS attacks, including Ukrainian government agencies, think tanks, and financial sites[91].

March 2022: Threat actors targeted Ukrtelecom, one of the largest telecom providers in Ukraine, forcing connectivity in the country to drop to 13 percent of pre-war levels. Specialists from the State Service of Special Communications and Information Protection of Ukraine restored connectivity within several hours of the attack[92].

March 2022: Hackers targeted Ukrainian organizations and individuals with a phishing attack. The fraud email claimed to be from the Ministry of Education and Science of Ukraine, and the malware gives the hacker access to sensitive data and user identification information[93].

April 2022: Hackers targeted the Telegram accounts of Ukrainian government officials with a phishing attack in an attempt to gain access to the accounts[94].

---

82 https://blog.eset.ie/2022/03/15/caddywiper-new-wiper-malware-discovered-in-ukraine/

83 https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-Report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/

84 https://cert.gov.ua/article/37815

85 https://www.slovoidilo.ua/2022/03/17/novyna/suspilstvo/sbu-povidomyla-pro-masovu-xakersku-ataku-sajty-populyarnyx-onlajn-vydan-ukrayini

86 https://t.me/SBUkr/3930

87 https://cert.gov.ua/article/38088

88 https://cert.gov.ua/article/37829

89 https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

90 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

91 https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/

92 https://www.bbc.com/news/60854881

93 https://cert.gov.ua/article/38606

94 https://www.cybersecurity-insiders.com/ukraine-now-faces-cyber-threats-through-telegram-messages/

April 2022: A group targeted several Ukrainian media organizations in an attempt to gain long-term access to their networks and collect sensitive information. Microsoft took control of seven internet domains the group used to mitigate these attacks. The group has connections to the Russian GRU[95].

April 2022: A threat group targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shut down electrical substations in Ukraine. Researchers believe the attack came from the same group with suspected ties to the Russian GRU that targeted Ukraine's power grid in 2016, using an updated form of the same malware (Industroyer2)[96].

April 2022: Ukraine's national post office suffered a DDoS attack, days after releasing a new stamp honouring a Ukrainian border guard. The attack impacted the agency's ability to run its online store[97].

April 2022: Hackers created a fake Ukraine 24 Facebook page, prompting users to enter their personal data and payment information[98].

April 2022: Hackers used a compromised Ukrainian government email in a phishing attack. CERT-UA linked this attack to hackers with suspected ties to the Russian GRU[99].

May 2022: Hackers launched a phishing attack allegedly on behalf of CERT-UA with malware that compromises user data. CERT-UA attributed this attack to actors with ties to the Russian GRU[100].

May 2022: Hackers launched a phishing attack to gain access to authentication data. The email warns recipients of an impending chemical attack to convince users to open its malware-ridden attachment. The mentioned malware is a stealer that provides the theft of authentication and other data from Internet browsers, MAIL/FTP/VPN clients, cryptocurrency wallets, password managers, messengers, game programs, etc[101].

June 2022: Hackers targeted Ukrainian state organizations with a phishing attack. The attachment document was found to contain a link to an external object (an HTML file containing JavaScript code) that, when executed after exploiting CVE-2021-40444 and CVE-2022-30190, would trigger a PowerShell command that downloading the EXE file "ms-msdt.exe" and infecting the computer with the Cobalt Strike Beacon malware[102].

June 2022: Hackers targeted media organizations in Ukraine with a phishing attack. CERT-UA attributed the attack with an "average level of confidence" to a suspected Russian GRU-linked group. In the attachment, the email contained a document "LIST_of_links_to_interactive_maps.docx", opening which would download an HTML file and execute JavaScript code, which in turn would download and execute an EXE file "2.txt" classified as the CrescentImp malware[103].

95 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

96 https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

97 https://www.reuters.com/world/europe/ukraines-postal-service-hit-by-cyberattack-after-sales-warship-stamp-go-online-2022-04-22/

98 https://cert.gov.ua/article/39727

99 https://cert.gov.ua/article/39882

100 https://cert.gov.ua/article/40106

101 https://cert.gov.ua/article/40125

102 https://cert.gov.ua/article/40559

103 https://cert.gov.ua/article/160530

5 / Recommendations for Mitigation

Russia sought to disrupt services and install destructive malware on Ukrainian networks included phishing, denial of service, and taking advantage of software vulnerabilities. In order to enhance the protection against these attacks, some the recommendations for mitigation are the following:

No.	Recommendation	Description
1.	Mitigate credential theft and account abuse	Protecting the identities of your users is a key requirement to secure your network and resources from attackers. Additionally, customers are urged to apply least privilege access and secure the most sensitive and privileged accounts and systems. Restrict administrative access within a domain, limit the number of domain administrators, and separate networking, server, workstation, and database administrators into separate Organizational Units (OUs). If possible, do not use hard-coded credentials. Monitor for any hard-coded methods that cannot be removed or disabled. Restrict access to devices to only necessary personnel. Implement the principle of least privilege across all applications, services, and devices to ensure individuals are only able to access the resources needed to perform their duties. This includes ensuring application layer services, like file shares and cloud storage services, are properly segmented. It is also recommended to enable multi-factor authentication and identity detection tools.
2	Enhance visibility of the network	Take a comprehensive approach for visibility into IT and OT environments to ensure that there is no gap in monitoring. Asset owners, operators, and security personnel should work together to gather network and host-based logs starting from the most critical infrastructure, also known as "crown jewels." The ability to identify and correlate suspicious network, host, and process events can greatly assist in identifying intrusions as they occur or facilitating root-cause analysis after a disruptive event. Ensure network monitoring of the operations network through IT and ICS-focused technologies.
3.	Secure internet-facing systems and remote access solutions	Internet facing systems should be secured against external attacks by ensuring they are updated to the most secure levels, regularly evaluated for vulnerability, and audited for changes to the integrity of the system. Anti-malware solutions and endpoint protection should be enabled for detection and prevention of attackers. Legacy systems should be isolated to prevent them from being an entry point for persistent threat actors. Remote access solutions should require two-factor authentication and be patched to the most secure configuration[104].
4.	Enable Investigation and Business Continuity	In the case you detect or are notified of a threat to your environment, it is critical to have auditing of key resources to enable investigations[105]. In addition, it is critical to develop, implement, and review a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operations in case of an undesirable interruption for IT and OT systems. The continuity of operations plan should be regularly tested and reviewed.

[104] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[105] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

5.	Ensure Third-Party Risk Management	Ensure that third-party connections are monitored and logged from a "trust but verify" mindset. Where possible, isolate or create demilitarized zones (DMZs) for such access to ensure that third parties cannot gain complete, unfettered, or unmonitored access to the entire IT and ICS networks. Implement features such as jump hosts, bastion hosts, and secure remote authentication schema wherever possible. It is recommended using threat information and consequence driven analysis to address supply chain cyber risk. Moreover, organisations should ensure that all patching related to third party and open-source applications has to be a subject of regular risk assessment and formalized mitigation plan. Such policy should be documented and audited regularly (at least annually).
6.	Develop and test Incident Response Plans	Develop, review, and practice cyber-attack response plans and integrate cyber investigations into root-cause analysis for all events. Especially, consider intelligent adversaries which may also attack response plan essential elements during remediation and response to increase disruption scale and downtime.

6 / Conclusions and Way Forward

The following key conclusions can be drawn from the analysis of Russia's cyber offensive operations during the conflict in Ukraine:

1. All available evidence indicates that Russia has conducted a coordinated and broad cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine. Some reporting showed a huge increase in exploits on the first day. The intent appears to have been to create disorder and overwhelm the Ukrainian defense. This was a wide-ranging attack using the full suite of Russian cyber capabilities to disrupt Ukraine, but it was not a success.
2. Russian Advanced Persistent Threat (APT) actors and other unattributed threats have conducted destructive attacks, espionage operations, or both, while the Russian military forces are attacking the country by land, air, and sea. It is unclear whether the computer network operators and physical forces are just pursuing a common set of priorities independently or they are actively coordinating. However, the Ukrainian experience demonstrates that cyber and kinetic actions have been taken simultaneously to degrade the Ukrainian Government and military functions.
3. When it comes to the different types of cyber-attacks, Ukraine's experience demonstrates that DDoS has been as popular as never. These attacks represent a broader pattern in cyberspace, the objective of the adversary to undermine the public's trust in state institutions and critical service providers. Most of the destructive attacks were aimed at organizations in critical infrastructure sectors that could have had a negative second-order effects on the Government, military, economy, and people. Their primary targets were websites of the Ukrainian Government, energy and telecom service providers, financial institutions, and media outlets, however, the cyber-attacks encompassed most of the critical sectors.
4. As the war in Ukraine continues, there is a likelihood that cyber incidents will spill over into other countries. As a matter of fact, Russia has already expanded its destructive cyber-operations against the countries which have come together to defend Ukraine. This spill-over effect has already been seen in some countries, especially NATO members. The focus on the United States has been followed shortly by the activity targeting NATO members that are the closest to Ukraine geographically, including the Baltic States and Poland. For example, Lithuania's biggest state-owned energy company Ignitis Group has been targeted by a massive DDoS attack as part of the ongoing campaign by the pro-Russian hacking group Killnet[106].
5. The lessons learned in Ukraine call for a coordinated and comprehensive mitigation response to strengthen the defenses against the full range of cyber destructive, espionage, and influence operations. This response should increase collective capabilities to better (1) detect, (2) defend against, (3) disrupt, and (4) deter foreign cyber threats.

Please note that the findings and conclusions of the Report are not final and will be amended with additional information and lessons learned as the conflict progresses.

[106] https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade

7 / List of References

1. Abrams, L. (2022) Hacked WordPress sites force visitors to DDoS Ukrainian targets. Bleeping computer. Available from: **https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/**
2. Atlantic Council (2022) Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims. New Atlanticist. Available from: **https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-Report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/**
3. Australian Government (2022) Attribution to Russia of malicious cyber activity against Ukraine. Available from: **https://www.internationalcybertech.gov.au/Attribution-to-Russia-of-malicious-cyber-activity-against-Ukraine**
4. BNS (2022) Lithuania's state-owned energy group hit by 'biggest cyber-attack in a decade. News. Available from: **https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade**
5. Brewster. T. (2022) As Russia Invaded, Hackers Broke into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down. Forbes. Available from: **https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=a56bd826573e**
6. Cattler, D. Black, D. (2022) The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine–And Poses a Threat Elsewhere, Too, Foreign Affairs. Available from: **https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar**
7. Cattler, D., Black D. (2022) The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine–And Poses a Threat Elsewhere, too. Foreign Affairs. Available from: **https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar**
8. CERT UA (2022) Державним центром кіберзахисту Держспецзв'язку вживаються заходи з протидії кібератакам з використанням вразливостей Microsoft Exchange Server (ProxyLogon). Available from: **https://cert.gov.ua/article/38606**
9. CERT UA (2022) Кібератака групи APT28 із застосуванням шкідливої програми CredoMap_v2 (CERT-UA#4622). Available from: **https://cert.gov.ua/article/40106**
10. CERT UA (2022) Кібератака групи UAC-0020 (Vermin) на державні організації України з використанням шкідливої програми SPECTR (CERT-UA#4207). Available from: **https://cert.gov.ua/article/37815**
11. CERT UA (2022) Кібератака групи UAC-0035 (InvisiMole) на державні організації України (CERT-UA#4213). Available from: **https://cert.gov.ua/article/37829**
12. CERT UA (2022) Кібератака групи UAC-0056 з використанням шкідливих програм GraphSteel і GrimPlant та тематики COVID-19 (CERT-UA#4545). Available from: **https://cert.gov.ua/article/39882**
13. CERT UA (2022) Кібератака групи UAC-0056 на державні організації України з використанням шкідливих програм SaintBot та OutSteel (CERT-UA#3799). Available from: **https://cert.gov.ua/article/18419**
14. CERT UA (2022) Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190 (CERT-UA#4753). Available from: **https://cert.gov.ua/article/40559**
15. CERT UA (2022) Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243). Available from: **https://cert.gov.ua/article/38088**
16. CERT UA (2022) Масована кібератака на медійні організації України з використанням шкідливої програми CrescentImp (CERT-UA#4797). Available from: **https://cert.gov.ua/article/160530**
17. CERT UA (2022) Масове розповсюдження шкідливої програми JesterStealer з використанням тематики хімічної атаки (CERT-UA#4625). Available from: **https://cert.gov.ua/article/40125**

18. CERT UA (2022) Онлайн-шахрайство з використанням тематики "грошової допомоги від країн ЄС" (CERT-UA#4492). Available from: **https://cert.gov.ua/article/39727**
19. CERT UA. Available from: **https://cert.gov.ua/**
20. Cerulus, L. (2022) Minister: Ukraine websites down in another 'massive' online attack. Politico. Available from: **https://www.politico.eu/article/minister-ukraine-websites-down-in-another-massive-online-attack/**
21. CISA (2022) Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Available from: **https://www.cisa.gov/uscert/ncas/alerts/aa22-110a**
22. CISA (2022) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Joint Cybersecurity Advisory. Available from: **https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf**
23. Congressional Research Service (2022) Russian Cyber Units. Available from: **https://crsReports.congress.gov/product/pdf/IF/IF11718**
24. Corera, G., (2022) Ukraine war: Don't underestimate Russia cyber-threat, warns US. BBC World News. Available from: **https://www.bbc.com/news/technology-61416320**
25. Council of the EU (2022) Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. Press Release. Available from: **https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/**
26. Culafi, A. (2022) Conti ransomware gang backs Russia, threatens US. Teachtarget.com. Available from: **https://www.techtarget.com/searchsecurity/news/252513982/Conti-ransomware-gang-backs-Russia-threatens-US**
27. ESET (2022) CaddyWiper: New wiper malware discovered in Ukraine. Available from: **https://blog.eset.ie/2022/03/15/caddywiper-new-wiper-malware-discovered-in-ukraine/**
28. ESET (2022) HermeticWiper: New data-wiping malware hits Ukraine. Available from: **https://www.eset.com/sg/about/newsroom/press-releases1/products/hermeticwiper-new-data-wiping-malware-hits-ukraine/**
29. FCDO (2022) Research and analysis Russia's FSB malign activity: factsheet. GOV.UK. Available from: **https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet**
30. FCDO (2022) UK assesses Russian involvement in cyber attacks on Ukraine. GOV. UK. Available from: **https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine**
31. FCDO (2022) UK exposes Russian spy agency behind cyber incidents. GOV.UK Press Releases. Available from: **https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents**
32. Fendorf, K. Miller J. (2022) Tracking Cyber Operations and Actors in the Russia-Ukraine War. Council on Foreign Relations. Available from: **https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war**
33. FireEye. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? Special Report. Available from: **https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf**
34. Goud, N. (2022) Ukraine now faces cyber threats through Telegram messages. Cybersecurity Insiders. Available from: **https://www.cybersecurity-insiders.com/ukraine-now-faces-cyber-threats-through-telegram-messages/**
35. Greig, J. (2022) Ukraine Ministry of Defense confirms DDoS attack; state banks lose connectivity. Zdnet. Available from: **https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/**
36. Kela (2021) Ain't No Actor Trustworthy Enough: The importance of validating sources. KELA Cyber Intelligence Center. Available from: **https://ke-la.com/aint-no-actor-trustworthy-enough-the-importance-of-validating-sources/**
37. Lewis, J. (2022) Cyber War and Ukraine. CSIS Report. Available from: **https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79lnugnYWlcZL4r3Ljuq.ash**

38. Malwarebytes (2022) FormBook spam campaign targets citizens of Ukraine. Available from: **https://blog.malwarebytes.com/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine%EF%B8%8F/**
39. Mandiant (2018) TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. Threat Research. Available from: **https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools**
40. Maunder, M. (2022) Ukraine Universities Hacked as Invasion Started. Wordfence. Available from: **https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/**
41. Meyers, A. (2019) Who is Salty Spider (Sality)? Crowdstrike blog. Available from: **https://www.crowdstrike.com/blog/who-is-salty-spider/**
42. Microsoft (2022) Destructive malware targeting Ukrainian organizations. Available from: **https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/**
43. MITRE ATT&CK. APT28. Available from: **https://attack.mitre.org/groups/G0007/**
44. MITRE ATT&CK. APT29. Available from: **https://attack.mitre.org/groups/G0016/**
45. MITRE ATT&CK. Available from: **https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0047%2FG0047-enterprise-layer.json**
46. MITRE ATT&CK. Dragonfly. Available from: **https://attack.mitre.org/groups/G0035/**
47. MITRE ATT&CK. Gamaredon Group. Available from: **https://attack.mitre.org/groups/G0047/**
48. MITRE ATT&CK. Hermetic Wiper. Available from: **https://attack.mitre.org/software/S0697/**
49. MITRE ATT&CK. Lazarus Group. Available from: **https://attack.mitre.org/groups/G0032/**
50. MITRE ATT&CK. Sandworm Team. Available from: **https://attack.mitre.org/groups/G0034/**
51. MITRE ATT&CK. TEMP. Veles. Available from: **https://attack.mitre.org/groups/G0088/**
52. MITRE ATT&CK. WhisperGates. Available from: **https://attack.mitre.org/software/S0689/**
53. National Cyber Security Centre (2022) Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion. News. Available from: **https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion/**
54. National Cyber Security Centre (UK). Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion. Available from: **https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion**
55. National Cyber Security Centre (UK). UK assesses Russian involvement in cyber attacks on Ukraine. Available from: **https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine**
56. Orenstein, M. (2022) Russia's Use of Cyber Attacks: Lessons from the Second Ukraine War. FPRI. Available from: **https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/**
57. Palo Alto Networks (2022) Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine. Available from: **https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/**
58. Palo Alto Networks (2022) Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot. Available from: **https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/**
59. Pearson, J. et. al. (2022) Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say. Reuters. zzzzzzzAvailable from: **https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/**
60. Reevell, P. (2020) What to know about the Russia-linked hackers accused of stealing COVID vaccine data. Available from: **https://abcnews.go.com/International/russia-linked-hackers-accused-stealing-covid-vaccine-data/story?id=71819152**

61. Reuters (2022) Ukraine's postal service hit by cyberattack after sales of warship stamp go online. Available from: **https://www.reuters.com/world/europe/ukraines-postal-service-hit-by-cyberattack-after-sales-warship-stamp-go-online-2022-04-22/**
62. Rundle, J. Stupp, C. (2022) Ukraine Thwarts Cyberattack on Electric Grid, Officials Say. The Wall Street Journal. Available from: **https://www.wsj.com/articles/ukraine-thwarts-cyberattack-on-electric-grid-officials-say-11649794612**
63. Schwarz, D. et al. (2021) New Year, New Version of DanaBot. Available from: **https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot**
64. Security Service of Ukraine (2021). Gamaredon Group: FSB RF Cyber Attacks Against Ukraine. Available from: **https://ssu.gov.ua/uploads/files/DKIB/Technical%20Report%20Armagedon.pdf**
65. Security Service of Ukraine (2022) SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine. Press Release. Available from: **https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy**
66. Slovoidilo (2022) СБУ повідомила про масову хакерську атаку на сайти популярних онлайн-видань в Україні. Available from: **https://www.slovoidilo.ua/2022/03/17/novyna/suspilstvo/sbu-povidomyla-pro-masovu-xakersku-ataku-sajty-populyarnyx-onlajn-vydan-ukrayini**
67. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Microsoft. Available from: **https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd**
68. Telegram. Available from: **https://t.me/SBUkr/3930**
69. The White House (2021) FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government. Statements and Releases. Available from: **https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/**
70. Tidy, Joe (2022) Ukrainian power grid 'lucky' to withstand Russian cyber-attack. BBC World News. Available from: **https://www.bbc.com/news/technology-61085480**
71. U.S. Department of Justice (2022) Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide. Justice News. Available from: **https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical**
72. U.S. Department of State (2022) Attribution of Russia's Malicious Cyber Activity Against Ukraine. Press Statement. Available from: **https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/**
73. U.S. Department of State. Attribution of Russia's Malicious Cyber Activity Against Ukraine. Available from: **https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/**
74. U.S. Department of the Treasury. Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. Press Releases. Available from: **https://home.treasury.gov/news/press-releases/sm1162**
75. Vail, E. (2022) Russia or Ukraine: Hacking groups take sides. TheRecord. Available from: **https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/?msclkid=235244a7ba6611ec92f21c9bd3b8ee49**
76. Vallance, C. (2022) Ukraine war: Major internet provider suffers cyber-attack. BBC News. Available from: **https://www.bbc.com/news/60854881**
77. Voltz. D. (2022) Malware Detected in Ukraine as Invasion Threat Looms. The Wall Street Journal. Available from: **https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo#:~:text=Researchers%20from%20the%20cybersecurity%20firms,invade%20its%20neighbor%20were%20imminent**
78. Welivesecurity (2022) Industroyer2: Industroyer reloaded. ESET Research. Available from: **https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/**
79. Welivesecurity (2022) IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. Available from: **https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/**
80. Zscaler (2021) Spike in DanaBot Malware Activity. Insights and Research. Available from: **https://www.zscaler.com/blogs/security-research/spike-danabot-malware-activity**

Issued by the Report on the Russian Use of Offensive Cyber Capabilities
in the Course of the Military Aggression in Ukraine

Layout by the Visual Information Section of the MOD General Affairs Department,
Totorių str. 25, LT-01121 Vilnius. 2022
Printed by the LITHAF Military Cartography Centre,
Muitinės str., Domeikava, LT-54359 Kaunas District.