1 YEAR UKRAINE

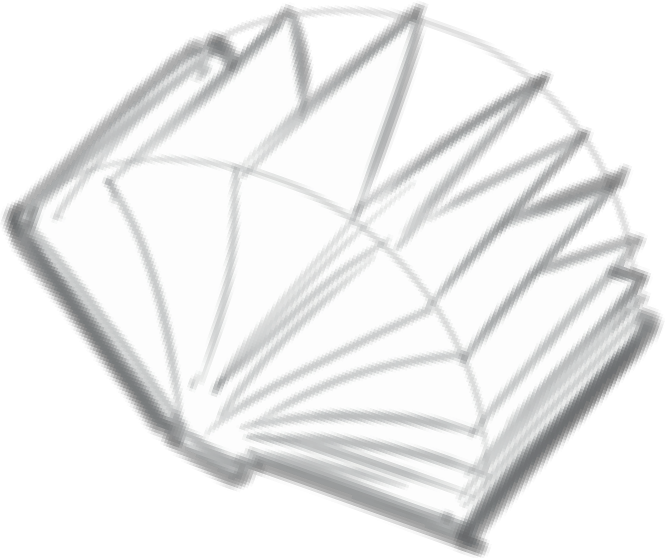
RUSSIA'S WAR ON UKRAINE: ONE YEAR OF CYBER OPERATIONS

24 February 2022 – 24 February 2023

10 years CERT-EU

TLP:CLEAR services@cert.europa.eu | https://cert.europa.eu

CONTENT



INTRODUCTION

We have been monitoring the cyber aspects of Russia's war on Ukraine since January 2022, when the conflict was brewing up, and systematically analysed the conflict-related cyberattacks that came to our knowledge. We observed the global cyber landscape, to anticipate if and how cyber operations would target our constituents, the EU institutions, bodies, and agencies (EUIBAs), or organisations in Ukraine and EU countries.

The following product is the result of this work.
It is our attempt at taking a step back from the day-to-day events, trying to pierce through the fog of war's veil to make a bigger picture materialise.
A picture that could help us see how the conflict shaped the cyber threat landscape in Ukraine and elsewhere.

We don't have a first-hand knowledge of cyberattacks in Ukraine, except for a handful of EUIBAs that have operations in the country.
As a consequence, what you will read here largely relies on the reporting of, and information verification by public and private sources we deem trustworthy.

For each cyberattack we describe in this product, we analyse the context (timing, objectives, impact), victimology (targeted sectors, countries), main tactics, techniques and procedures (TTPs), and, when applicable, attribution made by third parties.

KEY FINDINGS

We analysed 806 cyberattacks associated to Russia's war on Ukraine between January 2022 and the first week of February 2023.

- Cyber operations associated with Russia's war on Ukraine have not been confined to the belligerents. Since Russia's invasion, allies of Ukraine, such as EU countries, have faced several types of cyberattacks.

- We put these cyberattacks in several categories: DDoS, hack-and-leaks, phishing, attacks against critical infrastructure, information operations with a cyber component, wipers, etc.

- We observed APT actors - that are highly likely linked to Russia - mobilise. We have also seen new groups emerge. These threat actors conducted wiper attacks, targeted intrusion attempts (especially via spearphishing), and cyberattacks, such as hack-and-leaks, in support of information operations.

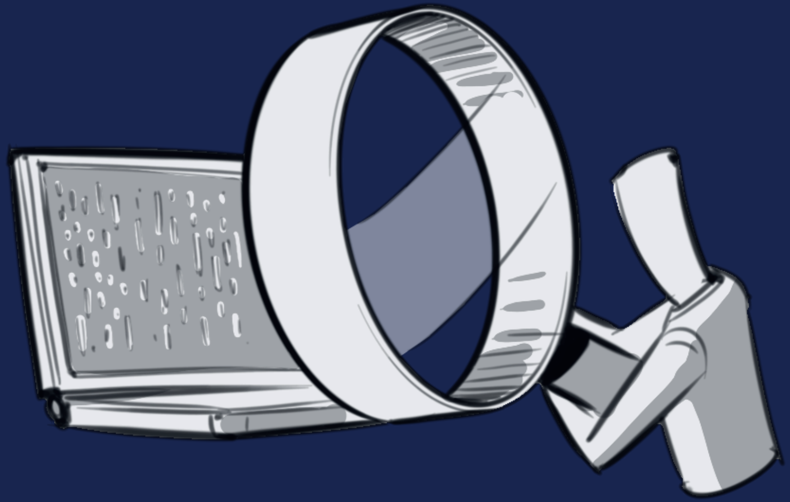
- A number of DDoS attacks and defacements have also been used to support information operations, or to distract from more disruptive attacks (such as wipers).

- In response to Russia's invasion, pro-Ukraine supposed hacktivists launched cyberattacks against Russia such as hack-and-leaks, DDoS attacks, and claimed to have disrupted critical infrastructure. We have limited visibility into the impact of such claimed attacks on Russian targets.

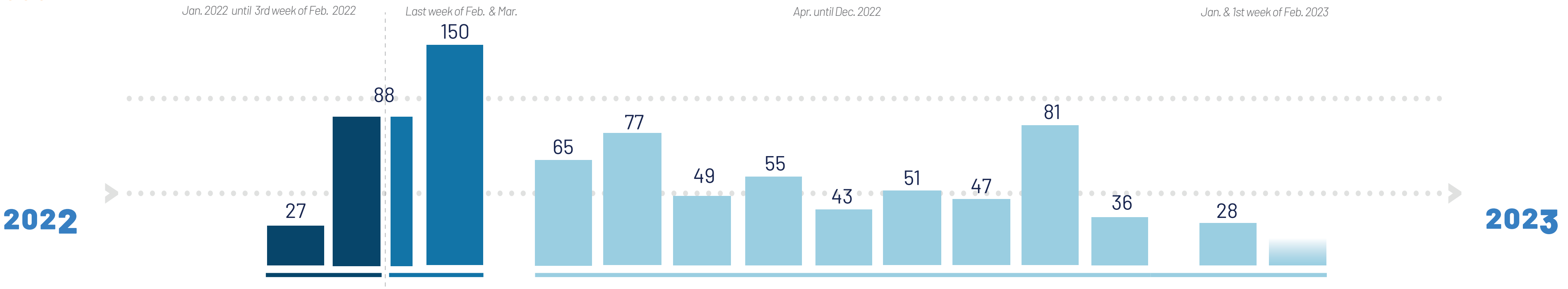
- Overall, we consider that the timeline of cyber operations consisted of three phases: a preparation phase (until the 3rd week of February 2022), a fast and furious phase (last week of February and March 2022), and a sustained phase with ups and downs (from April 2022).

At the risk of stating the obvious, no one has a crystal ball. So future cyber operations related to the war remain unpredictable.

CYBER OPERATIONS



TIMELINE



When placing Russia-linked cyber operations on a timeline, we observe the following:

All-time activity: Targeted intrusion attempts against Ukraine started years before February 2022, and continued after the invasion. Specifically, there appears to have been a constant stream of spearphishing emails against Ukrainian targets throughout 2022, up until the publication of this paper.

Preparation operations:

- *January 2022 - third week February 2022.*

The first wiper attacks were observed, as well as a few DDoS, defacement and information operations. The reported attacks were almost exclusively targeting Ukraine.

Fast and furious operations:

- *Last week of February 2022.*

Several wipers were reported targeting Ukraine, as well as other forms of disruptions, such as DDoS and ransomware attacks. In Ukraine there was a continuation of information operations, defacements and DDoS attacks. DDoS attacks and leaks by pro-Ukraine supposed hacktivists started to target Russia. DDoS attacks also started to target EU countries.

- *March 2022.*

This was the month when the highest number of attacks were reported. The reason for this peak is a continuation - slight increase - of attacks against Ukraine and a surge of attacks - especially data leaks - against Russia.

Sustained operations with ups and downs:

- *April & May 2022.*

We recorded no new wiper attacks, and less disruptive attacks in Ukraine. In Russia, we again observed reports of a high number of data leaks, less DDoS attacks, and, in May, the start of attacks claimed on industrial control systems (ICS). In EU countries, there was a surge of DDoS attacks.

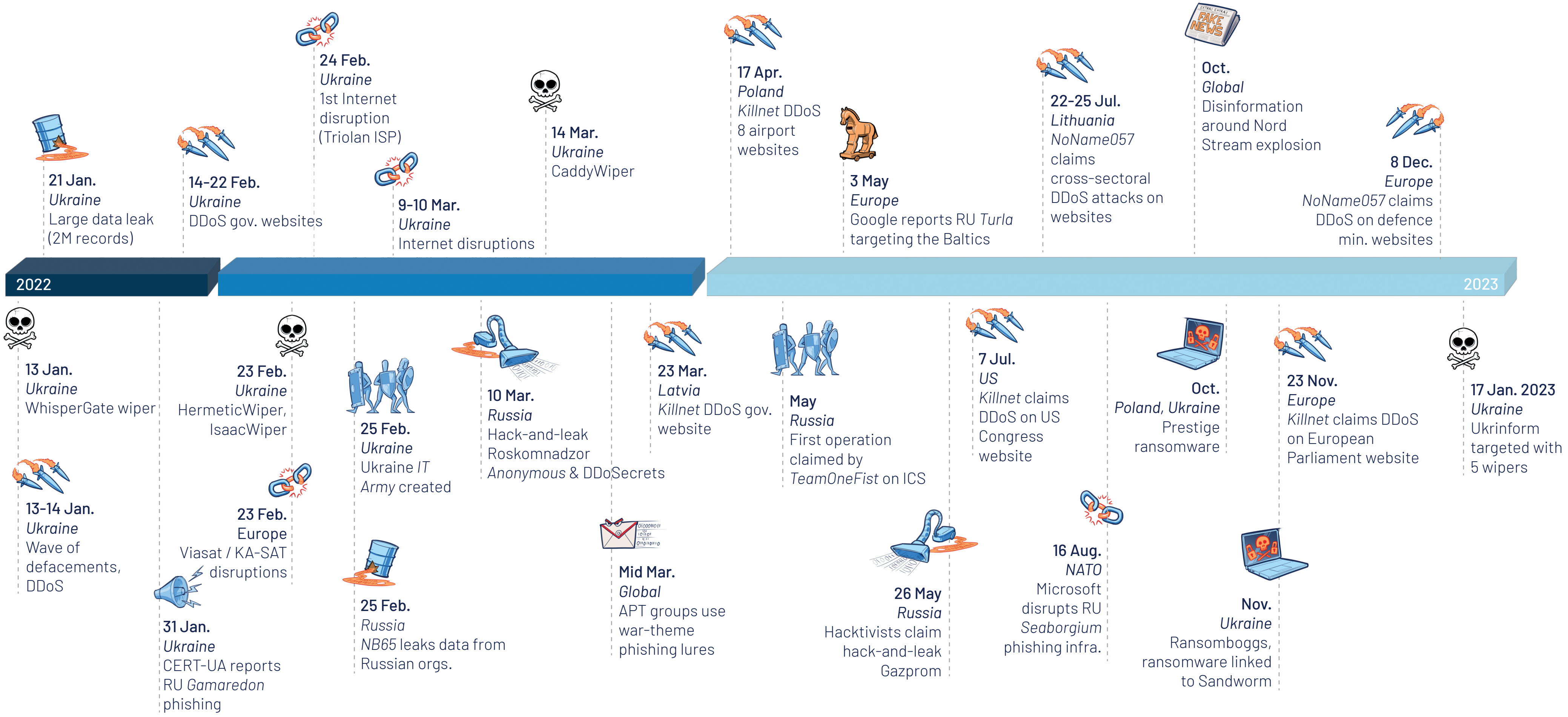
- *Jun. - Oct. 2022.*

In Ukraine there was a continuation of phishing attacks, few disruptive attacks and no reports of new wipers. We noticed the continuation of a limited number of DDoS or leaks against Russia. There were also additional attacks claimed on ICS. In EU countries, there were fewer DDoS attacks.

- *Nov. - Dec. 2022.*

New wiper attacks were reported in Ukraine. There was a surge of DDoS attacks claimed against EU countries and other countries providing support to Ukraine.

TOP STORIES



13 Jan.
Ukraine
WhisperGate wiper

13-14 Jan.
Ukraine
Wave of defacements, DDoS

21 Jan.
Ukraine
Large data leak (2M records)

31 Jan.
Ukraine
CERT-UA reports RU *Gamaredon* phishing

14-22 Feb.
Ukraine
DDoS gov. websites

23 Feb.
Ukraine
HermeticWiper, IsaacWiper

23 Feb.
Europe
Viasat / KA-SAT disruptions

24 Feb.
Ukraine
1st Internet disruption (Triolan ISP)

25 Feb.
Ukraine
Ukraine *IT Army* created

25 Feb.
Russia
NB65 leaks data from Russian orgs.

9-10 Mar.
Ukraine
Internet disruptions

10 Mar.
Russia
Hack-and-leak Roskomnadzor
Anonymous & DDoSecrets

14 Mar.
Ukraine
CaddyWiper

Mid Mar.
Global
APT groups use war-theme phishing lures

23 Mar.
Latvia
Killnet DDoS gov. website

17 Apr.
Poland
Killnet DDoS 8 airport websites

3 May
Europe
Google reports RU *Turla* targeting the Baltics

May
Russia
First operation claimed by *TeamOneFist* on ICS

26 May
Russia
Hacktivists claim hack-and-leak Gazprom

7 Jul.
US
Killnet claims DDoS on US Congress website

22-25 Jul.
Lithuania
NoName057 claims cross-sectoral DDoS attacks on websites

16 Aug.
NATO
Microsoft disrupts RU *Seaborgium* phishing infra.

Oct.
Global
Disinformation around Nord Stream explosion

Oct.
Poland, Ukraine
Prestige ransomware

Nov.
Ukraine
Ransomboggs, ransomware linked to Sandworm

23 Nov.
Europe
Killnet claims DDoS on European Parliament website

8 Dec.
Europe
NoName057 claims DDoS on defence min. websites

17 Jan. 2023
Ukraine
Ukrinform targeted with 5 wipers

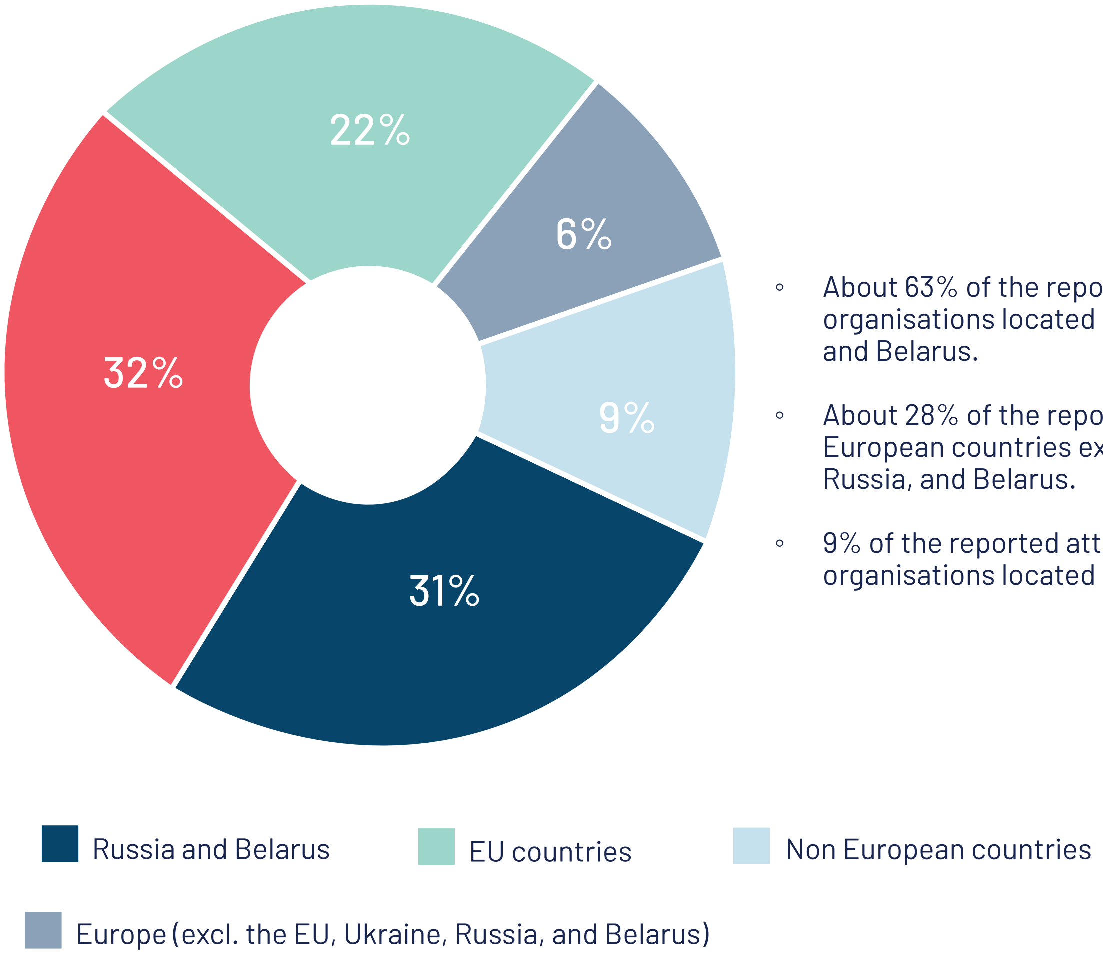
TLP:CLEAR

GEOGRAPHICAL TARGETING

OVERVIEW

Cyber activity associated with Russia's war on Ukraine has not been confined to targets located in Ukraine and Russia.

- We tracked the reported cyberattacks using the country where the victim organisation is located.
- We found that cyberattacks associated with Russia's war on Ukraine affected organisations in at least 50 countries.



- About 63% of the reported attacks affected organisations located in Ukraine, Russia, and Belarus.
- About 28% of the reported attacks affected European countries excluding Ukraine, Russia, and Belarus.
- 9% of the reported attacks affected organisations located outside Europe.

CROSS-BORDER ATTACKS

10%

of the attacks were cross-border

The geographical tracking leads us to conclude that 10% of the recorded cyberattacks targeted or affected organisations in more than one country at the same time.

We see four main reasons for these cross-border attacks:

1. In dozens of instances, supposed hacktivists launched a wave of DDoS attacks against similar targets at the same time.

   For example, a simultaneous wave of DDoS attacks targeting the websites of several ministries of defence in the EU. In such cases, we considered this to be the same cyberattack and recorded one incident.

2. Phishing emails with the same lure are sometimes sent during a set timeframe to a list of email addresses of people who work for organisations across several countries.

3. Information operations with a cyber component sometimes promote a narrative on social media relating to politicians of different countries or in foreign languages. The intended audience of such information operations is not restricted by borders.

4. The knock-on effect of a supply-chain attack may impact more organisations who are dependent on the compromised supplier than originally assumed by the perpetrator.

Story:

VIASAT KA-SAT Disruption

24 February 2022

A cyberattack targeted Viasat's KA-SAT satellite network with a wiper dubbed AcidRain.

The target infrastructure was reportedly used by a Ukrainian organisation for communication purposes, hence its strategic nature.

The attack had a cross-border knock-on effect and impacted nearly 30.000 satellite terminals used by different companies and industries across Europe. The outage of the satellite network also disrupted around 3000 wind energy converters of a German wind turbine service provider, because remote communications were interrupted. We consider it likely that this outage was collateral damage rather than an intended effect of the attack.

ATTACKS ON UKRAINE

Here’s our take on **destructive attacks**, such as wiper attacks:

- Russia-linked threat actors executed dozens of wiper attacks against Ukrainian targets before and throughout the war.
  Numerous wiper attacks appear to have taken place in January 2022, and in the first week following the invasion. Afterwards wiper attacks continued at a lower rate in Spring and Autumn 2022.
  There were again wiper attacks in January 2023.

- Some of the observed wipers were reportedly reworked versions of known wiper malware families (as opposed to self-built malware).

- It’s difficult to determine how many destructive attacks targeted Ukrainian critical services and whether they were successful or not because outages may have been caused by a kinetic military action, an accident or an infrastructure failure on top of a cyberattack.

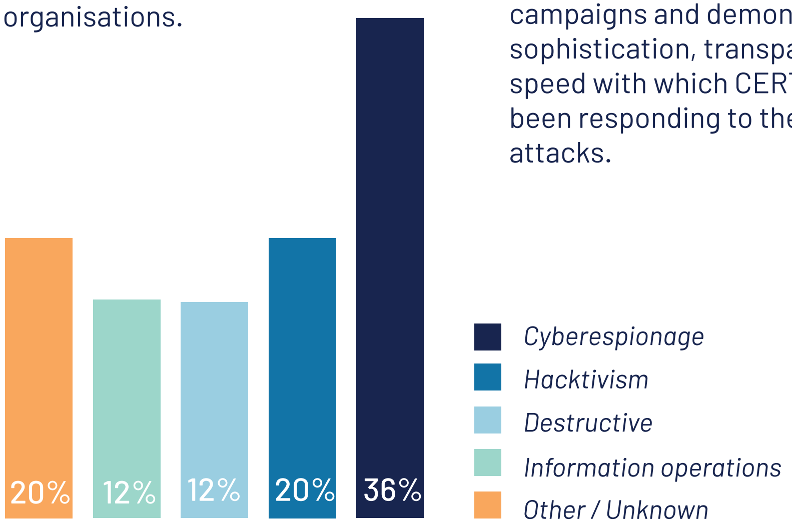
- ESET publicly reported that Sandworm used wipers at a time when Russia’s armed forces launched missile strikes targeting energy infrastructure.
  While ESET had not been able to show that those events were coordinated, the company assessed that this suggests *‘Sandworm and the military forces of Russia have related objectives’*

- We observed reports that Russia-linked APT groups used ransomware strains such as Prestige and Ransomboggs against Ukrainian organisations.

When it comes to **targeted intrusions**, such as spearphishing emails:

- Targeted intrusions seem to have been persistently conducted against Ukrainian governmental organisations and upstream IT service providers during the last quarter of 2021 and throughout 2022.

- CERT-UA published on its website regular reports related to new targeted intrusion attempts.
  This is an indication of the sheer amount of ongoing phishing campaigns and demonstrates the sophistication, transparency and speed with which CERT-UA had been responding to these attacks.



Pro-Russia **supposed hacktivist groups** have targeted Ukraine with DDoS attacks, hack-and-leaks, defacements and several ‘call-to-arms’ initiatives inviting the general public to engage in hacktivism in support of Russia.

As regards **information operations with a cyber component**:

- The pace of coordinated inauthentic social media content in Ukrainian and Russian languages targeting the Ukrainian population rose following the invasion.
  On social media, narratives in favour of Russia’s war efforts mushroomed, in an attempt to undermine confidence in the Ukrainian willingness and ability to withstand Russian attacks.

- We observed reports that data exfiltrated in targeted intrusions was later strategically promoted in hack-and-leaks by pro-Russia supposed hacktivists in an effort to sway public opinion.

ATTACKS ON UKRAINE

Story:

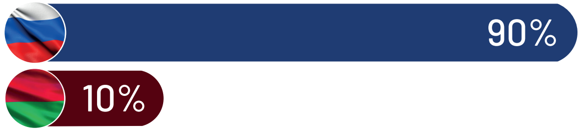
The role of CERT-UA

The Computer Emergency Response Team of Ukraine (CERT-UA) quickly emerged as a major source of information on cyberattacks targeting the country. They issued their first technical report on 26 January 2022. The report described the wave of defacements and DDoS that had targeted the country on 13-14 January 2022. Since then and until the first week of February 2023, CERT-UA published about 40 reports on cyberattacks, the large majority being spearphishing attacks.

These reports often came very shortly after the attacks and contained technical information (for example indicators of compromise - IoCs) allowing the cybersecurity community to make further analysis and check for possible other targets.

In several cases, CERT-UA also made an attribution of the attacks, most of the time to Russia-linked groups such as Gamaredon, Sandworm, APT28 or UNC1151. To facilitate the tracking of the different threat actors, the State Service of Special Communications and Information of Ukraine (SSCIP), the parent organisation of CERT-UA, published in March 2022 a taxonomy of threat actors (codenamed UAC-xxx) they are tracking .

ATTACKS ON RUSSIA AND BELARUS



- Among hundreds of claims made by pro-Ukraine supposed hacktivists, we managed to verify some of the claimed DDoS attacks, defacements and hack-and-leaks. Such attacks typically targeted public and private organisations active in the governmental, military, banking, logistics, transport and energy sectors.

- We identified reports of targeted intrusions such as spearphishing, targeting the Russian government, and of attacks against critical infrastructure. However, we could not verify the claims with the victims for obvious reasons.

- Sanctions led our private sector partners to restrict their services to Russian organisations. This limited our partners' visibility into cyberattacks occurring across client organisations in the country.

Story: *RussianCensorFiles*

In February 2023, DDoSecrets published documents and correspondence supposedly exfiltrated from the internal network of the General Radio Frequency Center (GRFC) subdivision of Roskomnadzor.
It appears that 335 GB of data were stolen by Cyber Partisans, an allegedly Belarusian hacktivist group.
The leak reportedly reveals that the GRFC writes denunciations to the FSB and other agencies, and blocks services that help convey truthful information.

Story: *DDoS by IT Army of Ukraine*

On 10 December 2022, IT Army of Ukraine, a pro-Ukraine supposed hacktivist group claimed to have conducted a cyberattack. Images posted on social media resembled a DDoS attack against the website of a drone hackathon organised by Wagner Group, a Russian paramilitary organisation. The website was not available during the timeframe of the claimed attack.

TARGETED EU COUNTRIES

Poland	22%
Latvia	16%
Estonia	8%
Lithuania	8%
Czechia	6%
Germany	6%
Slovakia	5%
Italy	5%
Finland	4%
France	3%
Hungary	3%
Greece	2%
Romania	2%
Sweden	2%
Other countries*	8%

** These countries are Austria, Belgium, Bulgaria, Denmark, the Netherlands, Spain, Cyprus, Luxembourg and Slovenia. Attacks against each of these countries represent 1% or less.*

We observed cyberattacks affecting organisations located in at **least 23 countries** of the European Union.

> Based on our records, the most targeted countries were Poland, Latvia, Estonia and Lithuania. All four countries border Russia and all four have been vocal proponents of providing military support to Ukraine.

Concerning destructive attacks such as wipers in EU countries:

- We aren't aware of reports of wiper attacks associated with the war targeting organisations in EU countries.
- The Viasat's KA-SAT attack had a knock-on effect on at least one German private organisation, but did not appear to have targeted that organisation.
- Another notable attack was the Prestige ransomware-style attack against a Polish company, which Microsoft attributed to what they call Iridium. Microsoft says that *'Iridium is a Russia-based threat actor tracked by Microsoft itself, publicly overlapping with Sandworm'*.

Looking at targeted intrusion attempts, victimology in EU countries included diplomatic services, private and public military organisations, think tanks, humanitarian organisations, IT companies, energy infrastructure and critical infrastructure.

The majority of supposed hacktivist attacks were DDoS attacks. We have also recorded hack-and-leak operations and defacements, albeit to a lesser extent. Targets included websites of public administrations, airports, energy and railway operators - to name but a few. The activity was often triggered, both in timing and targeting, by political decisions in support of Ukraine.

When it comes to information operations with a cyber component, we decided to label the target audience within Europe based on the language in which an operation took place and the topics it covered (eg. a narrative about a local politician). We identified reports of such operations targeting social media audiences in Poland, Lithuania and Latvia.

TARGETED EU COUNTRIES

Story:

Prestige ransomware-style attack targets Polish and Ukranian organisations

10
November
2022

Microsoft attributed a Prestige ransomware-style attack to Iridium. Microsoft stated that ‘*Iridium is a Russia-based threat actor tracked by Microsoft, publicly overlapping with Sandworm*’. The attack targeted organisations in the transportation and related logistics industries in Ukraine and Poland.

The deployment of the ransomware started on 11 October with attacks occurring within an hour, one from the other, across all victims. This activity was not connected to any of the 100 ransomware groups tracked by Microsoft as of this writing.

Story:

DDoS used to target organisations across the EU

DDosia is a tool which AVAST, a cybersecurity firm, associates to the pro-Russia supposed hacktivist NoName057(16).

NoName057(16) has regularly called on their social media followers to download and use DDosia to target private and public organisations across EU countries. AVAST observed ‘*roughly 1400 DDoS attack attempts by DDosia project members, with 190 of them being successful, giving the group a success rate of approximately 13%*’.

ATTACKS AFFECTING EUROPE (EXCLUDING THE EU, RUSSIA, BELARUS, AND UKRAINE)

OUR DATA

The UK	63%
Moldova	14%
Switzerland	10%
Georgia	7%
North Macedonia	3%
Serbia	3%

Most cyberattacks in this category targeted the UK.

- To a lesser extent, we observed reports of war-associated cyberattacks against Moldova, Switzerland, Georgia, North Macedonia, and Serbia.
- **79%** of the recorded attacks were DDoS attacks claimed by pro-Russia supposed hacktivists.

Story:

UK charity art sale for Ukraine becomes target of pro-Russia supposed hacktivists

On 10 January 2023, a UK charity 'Legacy of War' held a Banksy art sale to support Ukraine. The website on which the auction took place suffered a DDoS attack.

The DDoS attack reportedly delayed applications to purchase the art works.

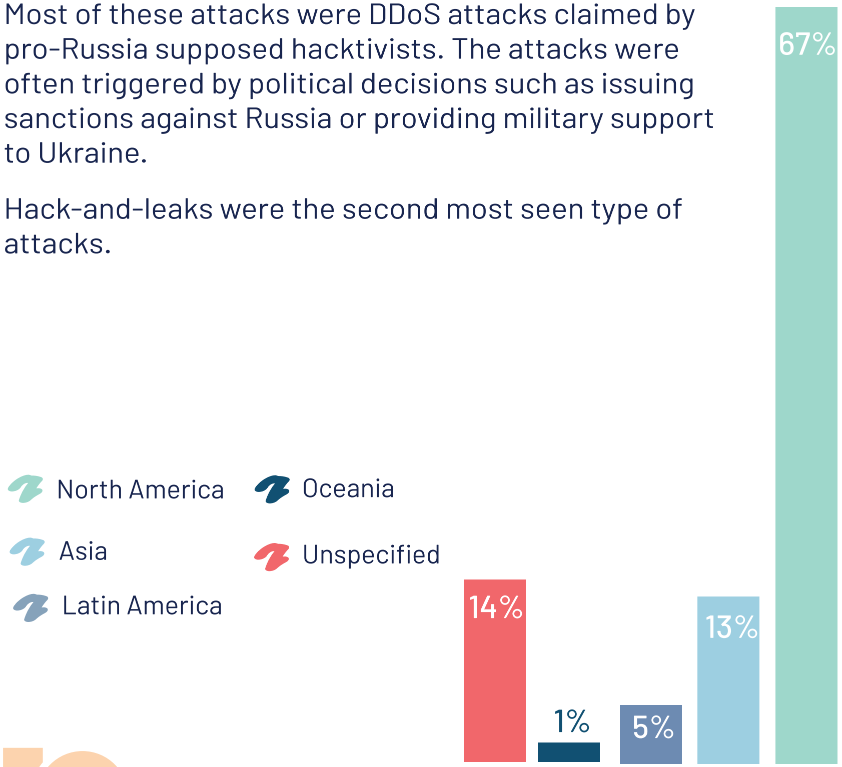
ATTACKS ELSEWHERE

Outside of Europe, we observed reports of cyberattacks related to Russia's war on Ukraine affecting at **least 17 countries**.

The US was by far the biggest target of cyberattacks associated with Russia's war on Ukraine.

Most of these attacks were DDoS attacks claimed by pro-Russia supposed hacktivists. The attacks were often triggered by political decisions such as issuing sanctions against Russia or providing military support to Ukraine.

Hack-and-leaks were the second most seen type of attacks.



Story:

Supposed hack-and-leak of a US defence contractor

On 4 August 2022, From Russia With Love (FRwL), a pro-Russia supposed hacktivist posted details to Telegram about a supposed hack-and-leak operation.
The group alluded to having exfiltrated 800 GB of data from a US company in the defence sector. The group posted a screenshot of a supposed scan of a customer invoice. We couldn't verify the accuracy of the claim.

Story:

The US and other countries warn of possible Russian cyberattacks

On 20 April 2022, the US, Australia, Canada, New Zealand, and the UK released a joint Cybersecurity Advisory (CSA) to warn that *'Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.'* The advisory listed the following organisations as having *'conducted malicious cyber operations against IT and/or OT networks'*:

- The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18.
- Russian Foreign Intelligence Service (SVR).
- Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS).
- GRU's Main Center for Special Technologies (GTsST).
- Russian Ministry of Defence, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM).

TARGETED SECTORS

TARGETED SECTORS

We observed that cyberattacks targeted at least 25 different sectors.

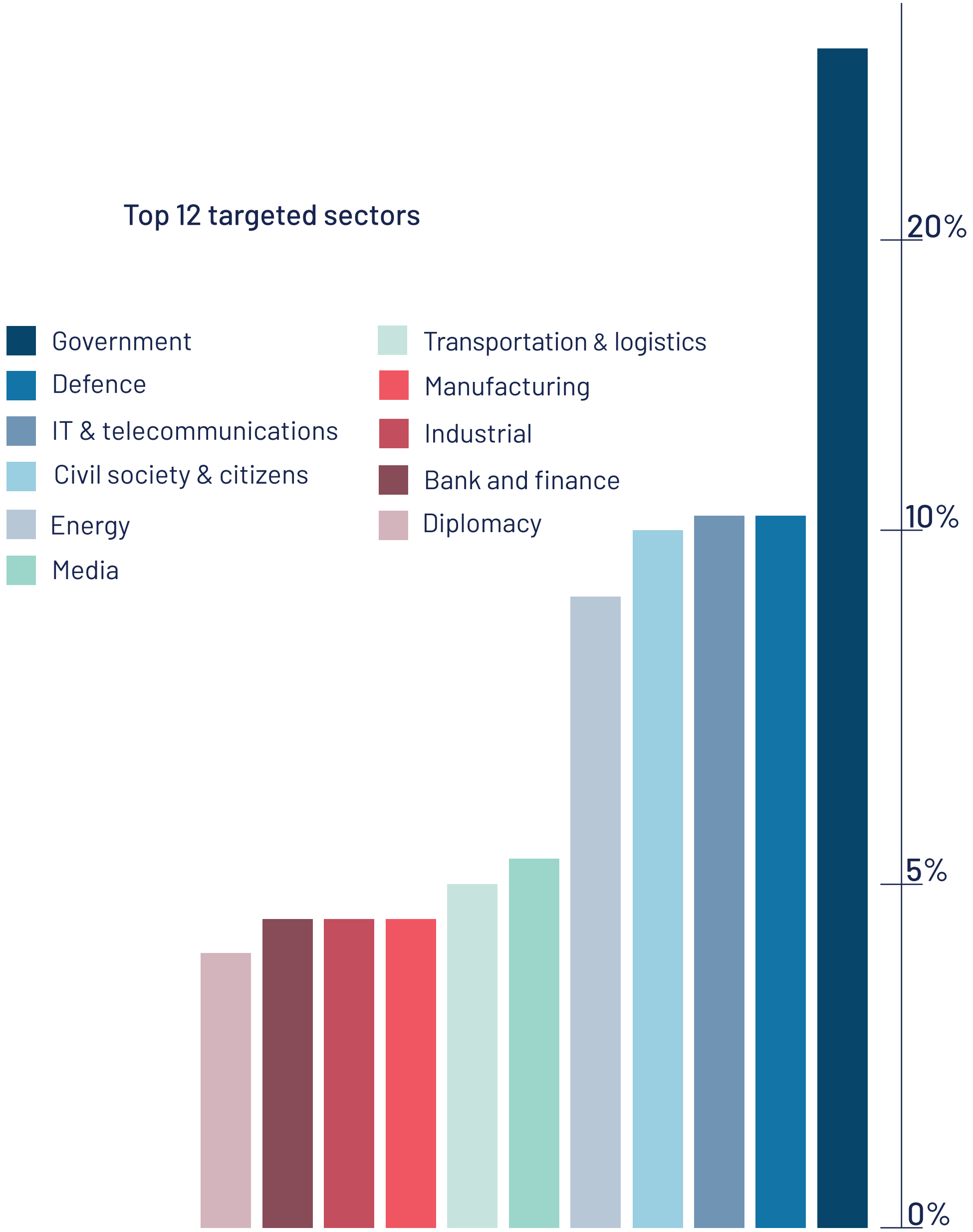
- **Governmental** organisations were by far the most targeted entities. Within governmental organisations, attacks frequently targeted multiple ministries at once.

- Cyberattacks against the **defence** sector often targeted those entities directly involved in the war such as the Ukrainian and Russian Armed Forces or Wagner Group, a Russian paramilitary organisation. Organisations that provided support to Ukraine, such as Western defence contractors who produce weaponry, were also targeted:

    - Cyberattacks against the Ukrainian defence organisations focused on targeted intrusions, potentially to collect strategic information.
    - Cyberattacks against Western defence organisations were often symbolic: for example DDoS attacks against websites.

- The **IT & telecommunications** sector was the third most targeted sector. Attackers used a large variety of techniques against this sector. The most impactful attacks were a series of Internet access disruptions affecting cities or oblasts in Ukraine, especially in February and March 2022.

- **Civil society & citizens** were most often targeted by information operations in the form of coordinated inauthentic social media behaviour that pushed narratives in favour of Russia's war on Ukraine, in an attempt to sway the targeted audience's opinion on the war.



TARGETED SECTORS

Energy infrastructure globally saw an uptick in targeting in 2022:

- In Ukraine we observed reports of wiper attacks against energy infrastructure.
- Within the EU, there were cyberattacks against the energy infrastructure, but no reports of wiper attacks. DDoS attacks against the websites of energy infrastructure operators could be associated with Russia's war on Ukraine because pro-Russia supposed hacktivists sometimes claimed responsibility for the attacks.
- The motive behind ransomware attacks against European energy infrastructure could be financial, political or both, but we couldn't find evidence associating such ransomware attacks with Russia's war on Ukraine.

Media organisations were targeted with a number of defacement attacks by threat actors wanting to relay political messages. Malicious actors also leveraged social media in information operations.

Transportation & logistics organisations were targeted with a variety of techniques including ransomware, hack-and-leaks, or DDoS, but we didn't notice any report of significant disruption.

Other targeted sectors include: manufacturing, industrial, bank & finance, diplomacy, space, business, healthcare, education, police & law enforcement, food & agriculture, aerospace, arts & culture, border control, automotive manufacturing, consulting, accounting, environment, and mining.

Story:

Coordinated defacement and wiper attacks of several Ukrainian governmental ministries

On 14 January 2022, the websites of several Ukrainian ministries were defaced. The defacements affected the Ukrainian Ministry of Foreign Affairs, Ministry of Education and Science, Cabinets of Ministers and a governmental application.

This attack illustrates how governmental entities were a strategic target due to their visibility throughout 2022, and how one attack can affect multiple ministries at once. This was the first publicly reported large scale cyberattack against Ukrainian organisations in 2022.

It likely served as a distraction from more covert malicious activities happening at the same time on Ukrainian governmental networks: the deployment of wipers.

THREAT ACTORS

THREAT ACTORS

PRO-UKRAINE SUPPOSED HACKTIVISTS

OUR DATA

Name	Share
Anonymous	23%
Team OneFist	16%
DDoSecrets	15%
IT Army of Ukraine	12%
NB65	6%
AgainstTheWest	4%
DepaixPorteur	3%
Cyber Partisans	3%
KromSec	2%
GhostSec	2%
Aggressive Griffin	2%
National Republican Army	2%
Other entities	10%

We recorded claims of cyberattacks by **at least 33 pro-Ukraine supposed hacktivist groups or collectives.**

- We recorded the most claims from Anonymous, Team OneFist, DDoSecrets, IT Army of Ukraine, and NB65.
- We observed claimed collaboration between several supposed hacktivist groups. For example, NB65, Anonymous, and DepaixPorteur cooperated with DDoSecrets, a transparency collective publishing hack-and-leaks.

Story:

IT Army of Ukraine

On 26 February 2022, Ukraine's Deputy Prime Minister, Mykhailo Fedorov, announced the creation of the volunteer cyber army.

'We have a lot of talented Ukrainians in the digital sphere: developers, cyber specialists, designers, copywriters, marketers,' he said in a post on his official Telegram channel.

'We continue to fight on the cyber front.'

THREAT ACTORS - PRO-UKRAINE SUPPOSED HACKTIVISTS

...

Story: *DDoSecrets*

DDoSecrets defines itself as a *'non-profit and transparency collective, devoted to enabling the free transmission of data in the public interest'*.
Between March and June 2022, DDoSecrets **published data from at least 30 supposed hack-and-leak operations.**

The Russian and Belarusian targets of these operations included:

- Roskomnadzor (Russia's Internet regulator agency)
- entities in the energy and extraction sector (Rosatom State Nuclear Energy Corporation, Gazprom Linde Engineering, SOCAR Energoresource, Neocom Geoservice, McLanahan Russia)
- IT companies (NPO VS, Synesis)
- media organisations (Vyberi Radio, VGTRK)
- investment or law firms (RKP Law, Metprom Group, CorpMSP, Russian Worldwide Invest, Tendertech, Thozis Corporation)
- construction firms (Gazregion, GUOV i GS)
- a transportation operator (Port and Railway Projects Service)
- a research institute (Polar Branch of the Russian Federal Research Institute of Fisheries and Oceanography)
- and a regional administration (Achinsk city government).

Story: *Team OneFist*

On 15 January 2023, Team OneFist announced that it had conducted Operation Turn Ruzzia Off which supposedly took down 316 metro and edge network routers across Russia and disabled a further 944 devices.

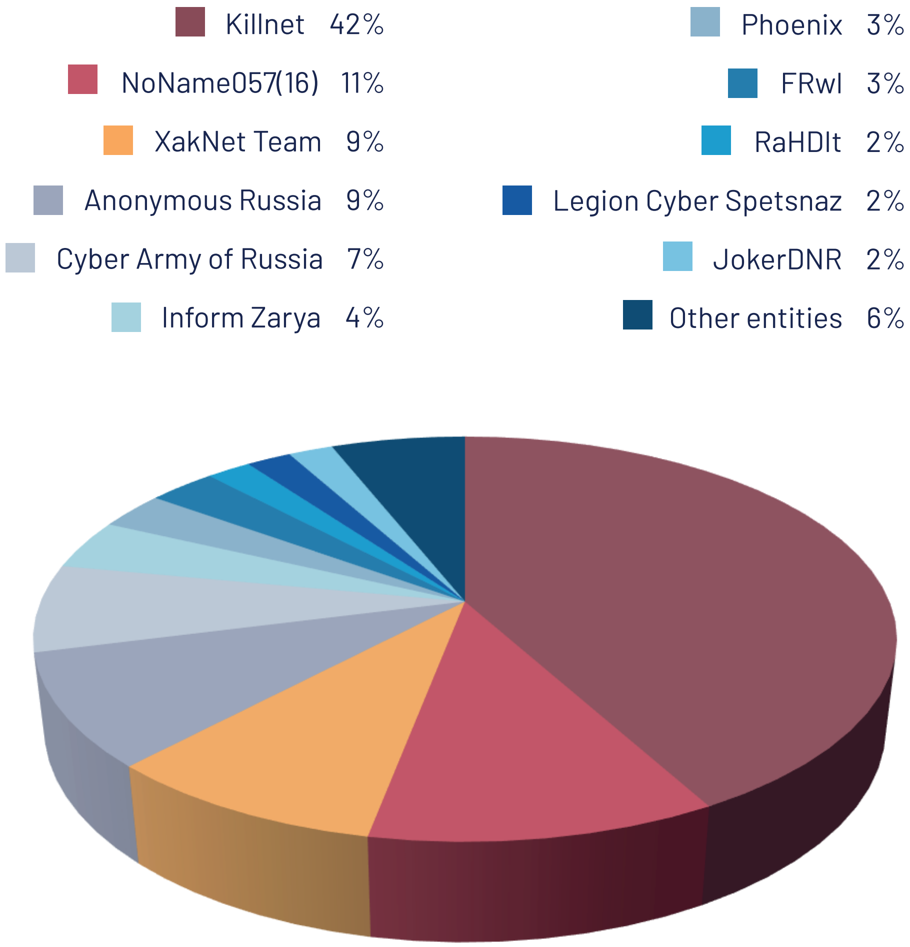
These uncorroborated claims come after a long series of equally uncorroborated claims of attacks against Russian critical infrastructure, including attacks on:

- a power grid SCADA/ICS (Op Neutrino - Nov 2022)
- payment systems (Op Pasłęk - Nov 2022)
- a military truck repair facility (Op Positiron - Nov 2022)
- a Wi-Fi router management system (Op Wimark - Nov 2022)
- a Rostelecom's edge router (Op Dark Fiber - Oct 2022)
- 'strategically valuable' switch devices (Op Switchblade - Oct 2022)
- 224 routers (Op Kazimierz Pulaski - Oct 2022)
- the Yamal satellite communication network (Op Polaris - Sep 2022).

THREAT ACTORS
PRO-RUSSIA SUPPOSED HACKTIVISTS

We recorded claimed attacks by **at least 18 pro-Russia supposed hacktivist groups or collectives**.

- We recorded the most attacks from Killnet, NoName057(16), XakNet Team, Anonymous Russia, and Cyber Army of Russia.
- The pro-Russia supposed hacktivists appear to collaborate. They regularly claim to have targeted the same or similar targets and repost each other's content on social media.
- Although their claims rarely describe the nature of the supposed cyberattack, most of their activity appears to consist of DDoS attacks against websites.
- At least one pro-Russia supposed hacktivist group has claimed a hack-and-leak which the Ukrainian government later considered possibly associated with Sandworm.



THREAT ACTORS - PRO-RUSSIA SUPPOSED HACKTIVISTS

...

Story:

Killnet and the Russian domestic audience

Between 15 and 18 April 2022, Killnet, a pro-Russia supposed hacktivist, claimed a series of DDoS attacks against 18 European and US targets, including a German governmental ministry, a US energy corporation, and 12 European airports.

At that time the campaign represented a notable uptick in Killnet's pace of operations. It coincided with a Russian press interview of the group published on April 15. This illustrates the information operation component towards the Russian audience of Killnet activity.

Between March 2022 and early February 2023, Killnet claimed about 90 attacks (mostly DDoS on websites) against organisations in Europe and North America.

Story:

Hacktivism triggered by political events

Between 22 and 25 January 2023, Anonymous Russia, Killnet and other pro-Russia supposed hacktivists claimed to have conducted DDoS against at least 36 German public and private websites.

The website of KMWEG, the manufacturer of the Leopard 2 tanks, was among the targets. The attacks were part of a #GermanyRIP campaign launched by Killnet in retaliation for the German government's planned tank deliveries to Ukraine. At least 14 of the targeted websites were inaccessible during the alleged operation, suggesting some likely impacts. Other events which triggered pro-Russia supposed hacktivist attacks included:

- Slovak arms deliveries to Ukraine (June 2022)
- Norway's enacted restrictions on the transit of goods to Russia (June 2022)
- Announcement of Finland's planned entry into NATO (August 2022)
- The Latvian parliament's resolution that Russia is a state-sponsor of terrorism (August 2022)
- Estonia's Foreign Minister congratulating Ukrainian Special Forces for damaging the Crimean bridge (August 2022)
- The European Parliament's recognition of the Russian Federation as a state-sponsor of terrorism (November 2022).

Story:

CyberArmyofRussia Reborn claimed responsibility for an attack which CERT-UA possibly associates with Sandworm

On 17 January 2023, CyberArmyofRussia Reborn released data allegedly exfiltrated from Ukrinform, a Ukrainian news agency in what they purported to be a hack-and-leak operation.

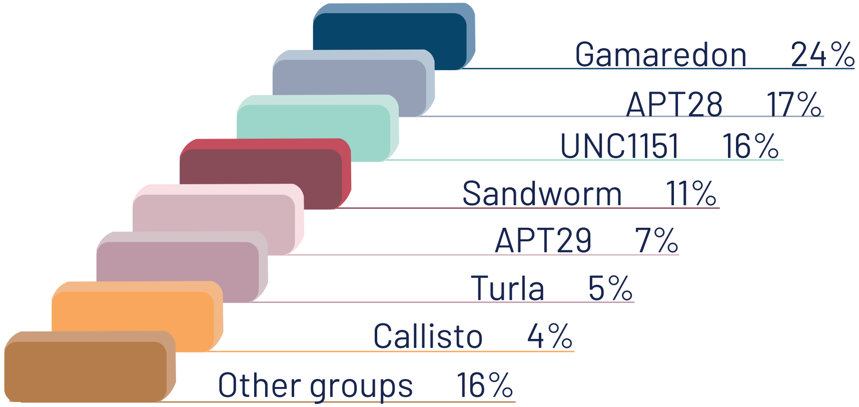
The pro-Russia supposed hacktivist claimed it had '*burned*' the victim organisation's '*entire network infrastructure*' in an effort to prevent news from populating the website. CERT-UA later released a report about a cyberattack with the same target and timing, but concluded that they observed five strains of wiper malware used in that attack: CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe.

CERT-UA concluded there's a possibility that the cyberattack was carried out by the '*UAC-0082 (Sandworm) group whose activities are associated with the Russian Federation.*' The US CISA publicly associates Sandworm to the Russian GRU's Main Center of Special Technologies.

APT GROUPS

We recorded cyberattacks associated with **at least 12 separate APT groups associated with Russia or Belarus.**

- The most active groups were Gamaredon, APT28, UNC1151, Callisto, Sandworm, APT29, and Turla.
- The recorded cyberattacks had been attributed to these APT groups by trusted third parties such as CERT-UA and industry partners.



Story:

Gamaredon, almost exclusively focused on Ukraine, with some exceptions

Gamaredon (aka Temp.Armageddon, UAC-0010) is an APT group which reputable sources associate with Russia. Their primary objective is reportedly cyberespionage. The group has a long history of targeting Ukraine.

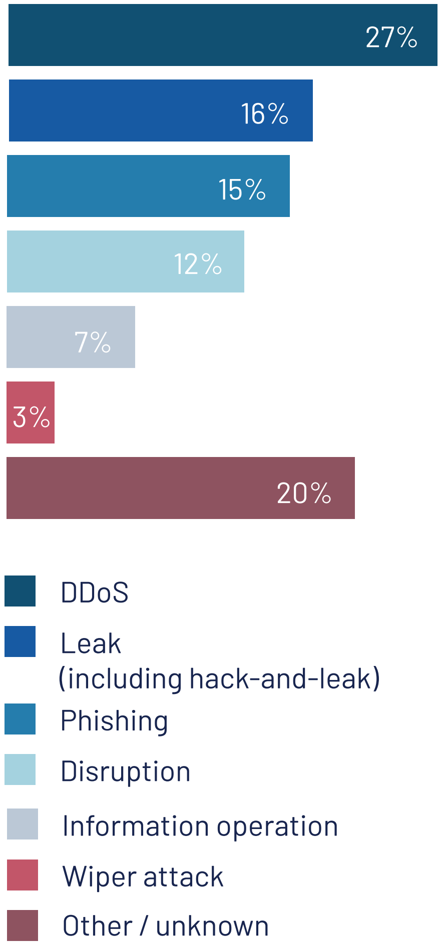
It was first reported targeting Ukrainian organisations in June 2013. In November 2021, the Ukrainian government publicly attributed Gamaredon to Russia's Federal Security Service (FSB) Center 18. Industry partners confirm that Gamaredon almost exclusively targets Ukrainian entities. According to CERT-UA, in 2022, Ukraine registered more than 70 incidents related to the group. On 4 April 2022, CERT-UA reported on Gamaredon spearphishing using EU-themed lures.

The campaign reportedly used documents related to the assistance to Ukraine as lures (e.g. *'List of necessary things for the provision of military humanitarian assistance to Ukraine.lnk'*, *'Providing military humanitarian assistance to Ukraine.lnk'*).

According to CERT-UA, *'the use of the English language in the file names and text of the email, as well as the fact that the letter was sent to the address of a state body in Latvia, clearly indicates that attacks by the UAC-0010 (Armageddon) group are carried out on state bodies of European Union countries.'*

TACTICS, TECHNIQUES AND PROCEDURES

TACTICS, TECHNIQUES AND PROCEDURES



The observed tactics, techniques and procedures (TTPs) were mainly DDoS, leaks (including hack-and-leaks), phishing, system disruptions, information operations, and wiper attacks.

We observed that some of the reported cyberattacks leveraged several TTPs.

For example:

- Hack-and-leak started with a phishing email
- DDoS executed in support of an information operation
- Wiper was deployed after obtaining initial access via successful phishing

❯ **Website DDoS.** Throughout the conflict, supposed hacktivists conducted DDoS attacks against the websites of their targets.
The impact was usually limited, the attacks causing temporary unavailability or instability.

In several cases the DDoS attacks were triggered by political events (e.g. announcement of assistance to Ukraine, official condemnation of Russia as a state supporting terrorism).
DDoS attacks carry an information operation component: supposed hacktivists attempt to sway the opinions of domestic or global audiences on topics related to Russia's invasion of Ukraine.

❯ **Leak (including hack-and-leak).** Threat actors published supposedly exfiltrated data for various reasons: to prove a claimed targeted intrusion, to inflict reputational damage on the victim, to influence public opinion, or as a sample of a larger dataset up for sale.

❯ **Phishing.** Phishing campaigns seem to have targeted Ukrainian entities on a continuous basis. We also recorded several phishing campaigns associated with Russia's war on Ukraine targeting EU countries, likely for cyberespionage reasons.

❯ **System disruption.**
We recorded cyberattacks that are not of a DDoS nature but which caused serious disruptions. Attacks in this category included attacks affecting IT systems belonging to critical infrastructure such as a ransomware attack against an energy provider or a SCADA attack. Some wiper attacks cover several categories at once.

❯ **Information operations with a cyber component.** This category ranged from coordinated inauthentic behaviour on social media pushing narratives associated with Russia's war on Ukraine to hack-and-leaks from supposed hacktivists which attempted to cause reputational damage to the victims.

TACTICS, TECHNIQUES AND PROCEDURES

Data destruction or wiping.
The most commonly reported destructive attack against Ukraine was wiper deployment and activation. A wiper is a destructive piece of malware intended to delete the target's data and programmes in order to render that target's networks and systems inoperable. Russia-linked threat actors started to use wipers against Ukrainian targets before and throughout the war. The malware used in these attacks are likely reworked versions of known wiper malware families (as opposed to self-built malware).

The observed wiper malware in Ukraine included at least WhisperGate, HermeticWiper, IsaacWiper, DesertBlade, DriveSlayer, AcidRain, CaddyWiper, DoubleZero, AwfulShred, Soloshred, ZeroWipe, SDelete and BidSwipe.
Some wiper attacks were disguised as ransomware attacks: the data was wiped with little to no chance to recover it.

Story:

Whispergate

On 15 January 2022, Microsoft reported having observed a wiper attack using the Whispergate strain. The wiper was designed to look like ransomware but lacked a ransom recovery mechanism.
The wiper attack coincided with a wave of website defacements targeting the Ukrainian government. Two days after the defacements occurred, Serhiy Demedyuk, Deputy Secretary of Ukraine's National Security and Defense Council, said that the defacements were *'just a cover for more destructive actions that were taking place behind the scenes and the consequences of which we will feel in the near future.'*
The wiper may have been an attempt to weaken the information systems of critical organisations in Ukraine ahead of the February invasion.

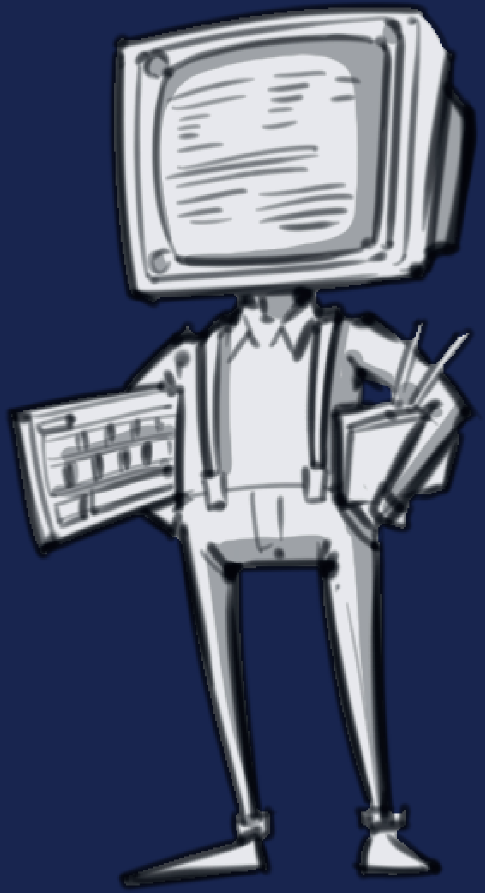
Story:

Internet access disruption and hijacking

NetBlocks presents itself as *'a global internet monitor working at the intersection of digital rights, cybersecurity and internet governance*.' Between 24 February and 28 March 2022 alone, Netblocks reported **at least 12 cases of Internet connectivity disruption.**

The disruptions affected multiple Internet service providers and usually had a regional impact. In regions occupied by Russia, there were cases of traceroute metrics showing Ukrainian Internet service providers connected via Russia's infrastructure instead of Ukraine's.

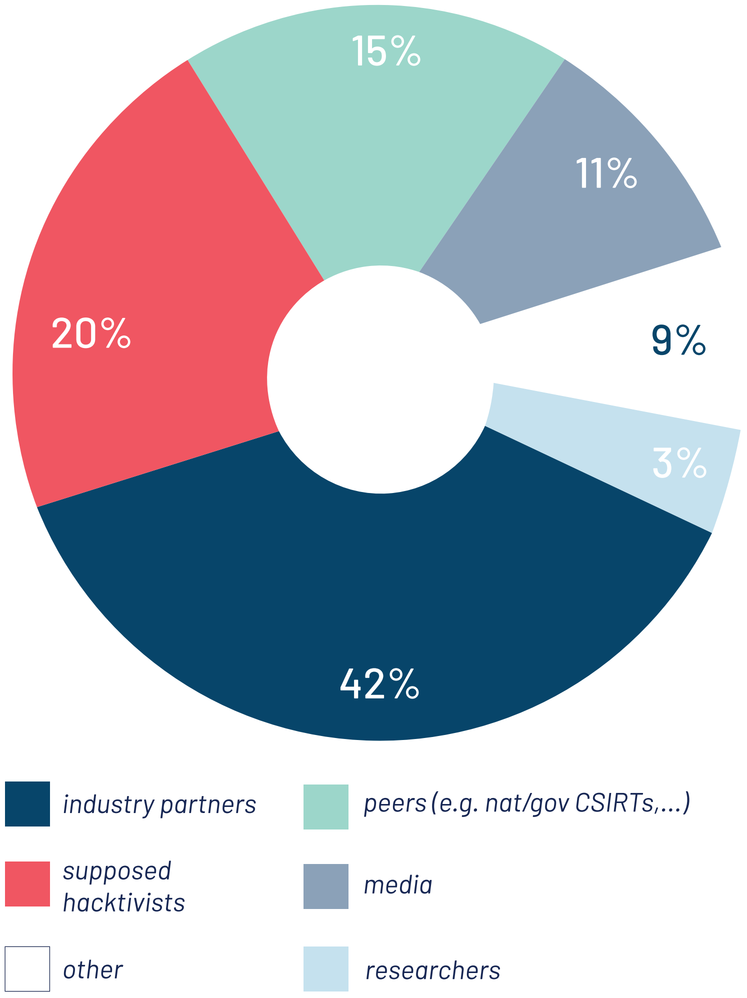
ANNEXES

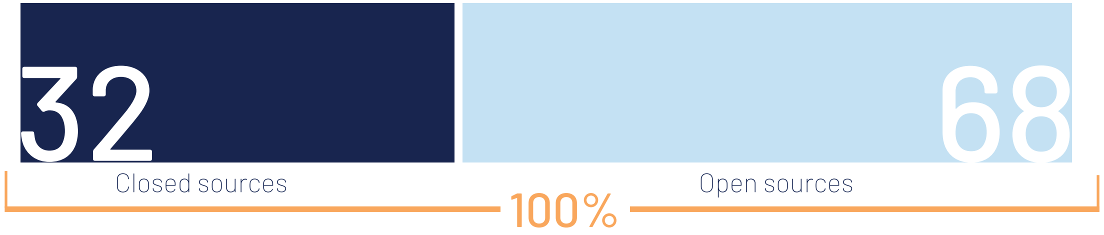


ANNEX 1: ACRONYMS AND DEFINITIONS

- CERT-EU: the Computer Emergency Response Team for the European Union institutions, bodies, and agencies (well, that's us 😉)
- CERT-UA: the national Computer Emergency Response Team for Ukraine
- DDoS: Distributed denial-of-service
- EU: European Union
- EUIBA: European Union institution, body, or agency (EUIBAs are our constituents)
- ICS: Industrial Control System
- Information operation: Also known as influence operation. An activity that attempts to influence the decision-making or opinion of a target audience
- NATO: North Atlantic Treaty Organisation
- RU: Russian Federation
- SCADA: Supervisory Control and Data Acquisition
- TTPs: Tactics, Techniques and Procedures
- UA: Ukraine
- UK: United Kingdom

ANNEX 2: OUR SOURCES





ANALYSIS

We analysed cyberattacks based on information coming from **over 142 different sources**:

- Many industry sources and researchers have scrutinised the threat landscape and used their telemetry to detect cyberattacks related to the war.
- National and governmental CSIRTs we closely cooperate with have fully used the existing information sharing frameworks to circulate their observations.
- Media have been extensively relaying cyberattacks of all kinds, at times inflating their impact for pure clickbait reasons. We had to frequently verify their reporting with trusted sources and victims.

We split activities per category and per threat actor. So while reading these pages, please keep the following caveats in mind:

- The lines between the activities and the actors are blurry. One cyberattack can be a blend of several activities that belong to several categories. Also, **threat actors may appear to be closely related.**
- We could only analyse what was publicly reported or shared with us by our peers and partners. Spearphishing attacks, wiper attacks, DDoS attacks and information operations with a cyber component are more visible due to their nature, if compared to supply-chain attacks or targeted attacks on critical infrastructure, for example. It doesn't take a rocket scientist to make the plausible assumption that some sophisticated activities haven't been identified or reported.
- **We have excluded most cybercrime activities** such as ransomware from the statistics for this report because we could not associate them with Russia's war on Ukraine. We can't distinguish between war-related cybercrime and non-war-related cybercrime with sufficient accuracy.

10 years CERT-EU

cert.europa.eu

services@cert.europa.eu

twitter.com/certeu

infosec.exchange/@cert_eu