TABLE OF CONTENTS

Background 3
Trends and Emerging Issues 4
  Ukraine 4
  Russian Federation 8
  Other Countries 11
Harm and Impact 15
Wider Contextual Considerations 20
Other research 22
Report Methodology 23
References 24
Background
January 2022 - June 2023

Since the start of the armed invasion of Ukraine in February 2022, the CyberPeace Institute has been documenting cyberattacks against critical infrastructure and civilian objects in Ukraine and the Russian Federation and cyberattacks against targets beyond the two belligerent countries. Between January 2022 and June 2023, the CyberPeace Institute has documented a total of 2189 cyber incidents conducted by 108 different threat actors. The data is available through the Cyber Attacks in Times of Conflict Platform #Ukraine.

The hacktivist collectives People’s CyberArmy (168) and NoName057 (52) were the most active threat actors targeting Ukrainian entities, while Sandworm (19) and APT28 (7) were attributed with the highest number of attacks among Russia’s state-sponsored actors.

Top 5 targeted sectors:
- Public administration (113)
- Financial (53)
- Media (46)
- ICT (44)
- Transportation (27)

The most active threat actors conducting attacks against Russian entities were the IT Army of Ukraine (72), Anonymous Italia (59), and Anonymous (50).

Top 5 targeted sectors:
- Public administration (47)
- Financial (43)
- Media (30)
- ICT (29)
- Energy (23)

The most active threat actors were the hacktivist collectives NoName057 (780), Anonymous Russia (102), and KillNet (65).

Top 3 targeted sectors:
- Public administration (440)
- Transportation (259)
- Financial (132)

Top 3 targeted countries:
- Poland (238)
- Germany (113)
- Lithuania (111)

The remainder of this report focuses on the incidents documented by the CyberPeace Institute in the second quarter of 2023; April 1 until June 30, 2023. Notably during this period, the CyberPeace Institute identified the 100th threat actor operating within the conflict’s context, based on our research since January 2022.
Trends and Emerging Issues Q2 2023
Ukraine

Incidents: 116 (+9.4%)
Sectors: 17
Threat Actors: 16 (-15.8%)

Trends

- DDoS attacks account for 88.8% of all incidents. The most targeted sectors were the public administration (31), media (11), ICT (11), financial (11), and transportation (10).
- Four Ukrainian nonprofit organizations were targeted by DDoS attacks.

Two cyberespionage campaigns, targeting Ukrainian public administration, have been attributed to APT28², a Russian state-sponsored actor:

- CERT-UA³ has reported on a phishing campaign targeting Ukrainian government entities. The phishing emails contained the subject line “windows update” and instructions to run a PowerShell script. If executed, it could enable the threat actor to steal information from the targeted machine.
- CERT-UA⁴ and Insikt Group⁵ have identified a cyberespionage campaign against Ukrainian public administration entities. Targets were sent phishing emails with news about the conflict as a lure. The phishing emails exploited vulnerable Roundcube servers, immediately compromising the target’s device if opened. More than 40 Ukrainian organizations were targeted. The campaign has been attributed to the threat actor APT28.
Emerging Issues

- Ukrainian civilians were targeted by a phishing campaign, reported by CERT-UA, with the goal of stealing Telegram credentials.

Notable threat actor activity

- Solntsepek, a newly tracked pro-Russian hactivist collective detected on Telegram. Their Telegram channel was created on April 25, 2022 but remained inactive until June 10, 2022. The group primarily focuses on information collection and the dissemination of data concerning members of the Ukrainian armed forces. Solntsepek started conducting cyberattacks in Q2 of 2023. The group mainly targets public administration and media entities in Ukraine. The CyberPeace Institute has recorded two confirmed cyberattacks conducted by Solntsepek. The name, Solntsepek, translates to “blazing sun” and is also a type of military equipment.

Latest malware

- BlackBerry Threat Research and Intelligence Team has reported on a cyberespionage campaign against Ukrainian government officials, attributed to the threat actor RomCom. The pro-Russian threat actor created phishing websites, distributing malicious payloads on the target devices, allowing the threat actor to exfiltrate data.

- CERT-UA has reported on a phishing email campaign targeting entities in Ukraine. The emails were sent by compromised accounts and contained a malicious file, which when executed would launch SmokeLoader malware. CERT-UA has attributed this campaign to the financially-motivated threat actor UAC-0006.

- CERT-UA has reported a cyberespionage campaign targeting a Ukrainian government agency. The agency was sent phishing emails allegedly from the Embassy of Tajikistan in Ukraine on April 18 and April 20, 2023. The emails contained a malicious file that would compromise the target’s device. Malware programs such as LOGPIE keylogger, CHERRYSPY backdoor and STILLARCH malware were used to steal data. CERT-UA uses the identifier UAC-0063 to track the threat actor behind the campaign.
In May 2023, during the month commemorating the Soviet victory over Nazi Germany in World War II, pro-Russian threat actors accounted for 46% of all the incidents recorded during the second quarter of 2023. Furthermore, the pro-Russian hacktivist collective known as People’s CyberArmy claimed responsibility for nearly 60% of all recorded incidents targeting Ukrainian entities in Q2 of 2023.

As previously noted in Q3 of 2022, it is probable that People’s CyberArmy is affiliated with the broader KillNet collective. However, a recent report published by Microsoft’s Threat Analysis Group indicates that People’s CyberArmy is an online persona created by Sandworm to disseminate stolen data as part of Sandworm’s operations.

During the second quarter of 2023, the CyberPeace Institute documented four possible Distributed Denial of Service (DDoS) attacks against websites belonging to Ukrainian nonprofit organizations. Among the targeted entities were the websites of an anti-corruption project and a charitable foundation. Additionally, the pro-Russian People’s CyberArmy directed DDoS attacks towards the websites of an association and an online resource providing assistance to refugees.

Apart from the observed disruption in website connectivity, no further information is currently available regarding any wider impacts of these incidents.

Cyberattacks on Ukrainian entities [Q2 2023 vs Q1 2023]

- +9.4% cyberattacks
- +120% cyberattacks on the media sector
- +55% cyberattacks on the financial sector

Other notable incidents in Ukraine

Destruction
April 29, 2023
CERT-UA has reported on a cyberattack against a Ukrainian state organization. According to CERT-UA, the threat actor was able to disable computers running Windows OS with RoarBat and computers running Linux with a BASH script. This attack is similar to a previous one reported by the Telegram channel CyberArmyofRussia_Reborn on January 17, 2023. CERT-UA attributes the described activity to Sandworm with a moderate level of confidence, but the corresponding identifier UAC-0165 has been created for its tracking.

Disruption
June 14, 2023
Confirmed cyberattack against a Ukrainian public television and radio company leading to the disruption of services. The pro-Russian threat actor, Solntsepek, claimed responsibility for the attack.
Data

April 18, 2023
CERT-UA\(^4\) has reported a cyberespionage campaign targeting a Ukrainian government agency. The agency was sent phishing emails allegedly from the Embassy of Tajikistan in Ukraine on April 18 and April 20, 2023. The emails contained a malicious file that would compromise the target's device. Malware programs such as LogPie keylogger, CherryPy backdoor and Stillarch malware were used to steal data. CERT-UA uses the identifier *UAC-0063* to track the threat actor behind the campaign.

June 19, 2023
CERT-UA\(^5\) has identified a phishing campaign against users of a Ukrainian email service. Targets were sent phishing emails posing as the Ukrainian email service. These emails contained a PDF file with a malicious link leading to a fraudulent site masquerading as the official Ukrainian email service. The threat actor was then able to obtain the targets' login and passwords. This campaign was attributed to the threat actor *UAC-0102*. 
Trend

- DDoS attacks account for 72.3% of all incidents, followed by Defacement operations (8.5%).

Top 10 sectors impacted in the Russian Federation [April- June 2023]

<table>
<thead>
<tr>
<th>Sector</th>
<th>Incidents</th>
<th>%Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Public administration</td>
<td>7</td>
<td>600%</td>
</tr>
<tr>
<td>2. Manufacturing</td>
<td>7</td>
<td>133.3%</td>
</tr>
<tr>
<td>3. ICT</td>
<td>7</td>
<td>40%</td>
</tr>
<tr>
<td>4. Transportation</td>
<td>4</td>
<td>-66.7%</td>
</tr>
<tr>
<td>5. Media</td>
<td>4</td>
<td>-33.3%</td>
</tr>
<tr>
<td>6. Civilians</td>
<td>3</td>
<td>50%</td>
</tr>
<tr>
<td>7. Administrative / Sup.</td>
<td>3</td>
<td>-40%</td>
</tr>
<tr>
<td>8. Arts</td>
<td>2</td>
<td>0%</td>
</tr>
<tr>
<td>9. Other service</td>
<td>2</td>
<td>0%</td>
</tr>
<tr>
<td>10. Professional/ Scientific</td>
<td>2</td>
<td>100%</td>
</tr>
</tbody>
</table>

- Reduction in incidents likely caused by a decrease of substantiated claims of attacks by the IT Army of Ukraine and Anonymous Italia.

- Continuation of cyber-enabled information operation exploiting radio and television stations:
  - June 5th, 2023 - A radio station broadcasting in different Russian regions was targeted by an unknown, highly likely pro-Ukrainian threat actor in a cyber-enabled information operation. The radio station allegedly played a fake message from President Putin announcing an invasion of the Russian Federation.
  - June 7th, and 12th, 2023 - Cyber-enabled information operations conducted against radio stations in various regions of the Russian Federation. Unknown threat actor(s) targeted radio stations in different Russian regions leading to the broadcast of allegedly pro-Ukrainian messages.

Notable threat actor activity

- Two incidents, purportedly attributed to, albeit unconfirmed officially, Wagner PMC:
  - An unknown threat actor has allegedly conducted an unknown type of cyberattack against a Russian satellite telecommunications company. The attack led to a disruption of service. Initial reports indicated that the threat actor involved was Wagner PMC. However, there was no confirmation from the Wagner group.
• **Cyble**\(^2\) has reported on a so-called "Wagner Ransomware" used to recruit new members to the paramilitary group. The ransomware encrypts files on the target's device. The ransom note also encourages a call to war against the Russian ministry of defense. Wagner PMC has not officially claimed responsibility for the ransomware.

The decrease noted by the CyberPeace Institute can likely be attributed to the Institute's inclusion criteria\(^2\) for data collection and processing. The CyberPeace Institute focuses on substantiated claims of attacks and other reports of malicious cyber activities. Consequently, claims of successful attacks by threat actors lacking additional proof are excluded from the platform. Nevertheless, the CyberPeace Institute continues to monitor the social media channels of threat actors that fail to provide supplementary evidence for their claims.

An illustrative example of potentially unrecorded activities is that of Team OneFist, a pro-Ukrainian hacktivist collective, one of whose members was interviewed by the *BBC*\(^2\). Despite ongoing monitoring of Team OneFist's official communication channels for a year, only one self-attributed incident by this threat actor has been processed and published on the platform. Therefore, it's important to note that a decrease in processed incidents does not necessarily indicate a reduction in the activities of pro-Ukrainian threat actors against Russian entities.

Lastly, the CyberPeace Institute has documented three instances of cyber-enabled information operations that directly impacted the citizens of the Russian Federation. Continuing the trend observed in Q1 of 2023, unidentified pro-Ukrainian threat actors targeted Russian radio stations on three separate occasions in June 2023\(^2\)\(^6\)\(^7\). Two of the cyber-enabled information operations conveyed pro-Ukrainian messages, while the third operation broadcasted an alleged message attributed to Russia's President, stating that a full-scale invasion of Russia is currently underway.

In the second quarter of 2023, the CyberPeace Institute documented a decrease of 30.9% in malicious activities and a 16.7% decrease in active threat actors targeting Russian entities compared to Q1 of 2023. Additionally, the two most active pro-Ukrainian threat actors, namely *Anonymous Italia* and *IT Army of Ukraine*, have also seen a decline in incidents attributed to them by 49% and 24%, respectively.

The decrease noted by the CyberPeace Institute can likely be attributed to the Institute's inclusion criteria\(^2\) for data collection and processing. The CyberPeace Institute focuses on substantiated claims of attacks and other reports of malicious cyber activities. Consequently, claims of successful attacks by threat actors lacking additional proof are excluded from the platform. Nevertheless, the CyberPeace Institute continues to monitor the social media channels of threat actors that fail to provide supplementary evidence for their claims.

An illustrative example of potentially unrecorded activities is that of Team OneFist, a pro-Ukrainian hacktivist collective, one of whose members was interviewed by the *BBC*\(^2\). Despite ongoing monitoring of Team OneFist's official communication channels for a year, only one self-attributed incident by this threat actor has been processed and published on the platform. Therefore, it's important to note that a decrease in processed incidents does not necessarily indicate a reduction in the activities of pro-Ukrainian threat actors against Russian entities.

Lastly, the CyberPeace Institute has documented three instances of cyber-enabled information operations that directly impacted the citizens of the Russian Federation. Continuing the trend observed in Q1 of 2023, unidentified pro-Ukrainian threat actors targeted Russian radio stations on three separate occasions in June 2023\(^2\)\(^6\)\(^7\). Two of the cyber-enabled information operations conveyed pro-Ukrainian messages, while the third operation broadcasted an alleged message attributed to Russia's President, stating that a full-scale invasion of Russia is currently underway.
**Notable incidents in the Russian Federation**

**Other**

April 4, 2023

*Cyber Resistance*, a pro-Ukrainian threat actor, has breached the account of and committed financial fraud against a Russian blogger, spending $25,000, originally raised for the Russian military, on adult toys.28

**Disruption**

April 10, 2023

A confirmed cyberattack carried out by an unidentified pro-Ukrainian threat actor targeted a Russian federal agency. Although certain IT services have been reinstated, several others remained offline, leading to the necessity of employing conventional paperwork at certain checkpoints.29

**Data**

May 28, 2023

A Russian high-technology project confirmed they had been targeted by a hack and leak operation conducted by a pro-Ukrainian threat actor. The threat actor gained partial access to a number of information systems and network resources, specifically the file exchange, located at the physical facilities of the organization. The target's public information resources, such as the website and online services, were also temporarily inaccessible.30

**Destruction**

June 8, 2023

*Cyber Anarchy Squad*, a pro-Ukrainian threat actor, has conducted an unknown type of cyberattack against a Russian Internet services provider. The threat actor was able to breach the target's IT systems, damaging a part of the network equipment and taking down the ISP services for 33 hours. Various clients of the ISP were reportedly cut off from the Internet as a result.31
Trends

- DDoS attacks account for 94.1% of all incidents recorded in countries which are not belligerents in this conflict.

- Most targeted sectors were the public administration (156), transportation (98), and financial (39).

- Sharp increase in attacks against Italian, French, Canadian, and Swiss entities with 100%, 428.6%, 866.7%, and 2500% respectively.

<table>
<thead>
<tr>
<th>Country</th>
<th>Incidents</th>
<th>%Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. POLAND</td>
<td>65</td>
<td>-11%</td>
</tr>
<tr>
<td>2. GERMANY</td>
<td>36</td>
<td>4.5%</td>
</tr>
<tr>
<td>3. FRANCE</td>
<td>37</td>
<td>428.6%</td>
</tr>
<tr>
<td>4. CANADA</td>
<td>29</td>
<td>866.7%</td>
</tr>
<tr>
<td>5. LITHUANIA</td>
<td>29</td>
<td>-12.1%</td>
</tr>
<tr>
<td>6. ITALY</td>
<td>28</td>
<td>100%</td>
</tr>
<tr>
<td>7. SWITZERLAND</td>
<td>26</td>
<td>2500%</td>
</tr>
<tr>
<td>8. SWEDEN</td>
<td>26</td>
<td>23.8%</td>
</tr>
<tr>
<td>9. GREAT BRITAIN</td>
<td>23</td>
<td>-8%</td>
</tr>
<tr>
<td>10. ESTONIA</td>
<td>22</td>
<td>∞</td>
</tr>
<tr>
<td>11. SPAIN</td>
<td>20</td>
<td>42.9%</td>
</tr>
<tr>
<td>12. DENMARK</td>
<td>16</td>
<td>23.1%</td>
</tr>
<tr>
<td>13. LATVIA</td>
<td>16</td>
<td>-46.7%</td>
</tr>
<tr>
<td>14. CZECHIA</td>
<td>16</td>
<td>-48.4%</td>
</tr>
<tr>
<td>15. NETHERLANDS</td>
<td>14</td>
<td>55.6%</td>
</tr>
</tbody>
</table>

© 2023 CyberPeace Institute. All rights reserved | TLP:WHITE - Disclosure is not limited. Information may be distributed freely.
Notable threat actor (in)activity

For the second consecutive quarter, the notorious hacktivist collective *KillNet*, purportedly composed of 50 groups totaling 1250 individuals, including *Anonymous Russia*, has had a reduction in their malicious cyber activities. This decline can be attributed to an internal dispute within the larger collective resulting in the doxing of the leader of *Anonymous Russia*. Subsequently, the leader was apprehended in Belarus, prompting a significant restructuring of the group’s framework with the intent of commercializing the hacktivist collective’s endeavors. For further details on this topic, please refer to the Harm and Impact section later within this report.

**Bloodnet**

A pro-Russian threat actor tracked through its Telegram channel, which was created on January 24, 2023. The group was originally affiliated with *Phoenix* until June 11, 2023. The group likely has affiliations with other pro-Russian groups like *KillNet*, given their reposting of *KillNet*’s messages. The Institute started tracking this threat actor in April 2023. *Bloodnet* conducts DDoS attacks against non-belligerent countries such as Germany (11), Hungary (11), Poland (8), and Ukraine (6).
Poland and Germany – Continuing Targeted Actions

For the second consecutive quarter, pro-Russian threat actors have focused their efforts on entities located in Poland and Germany. The CyberPeace Institute has recorded 65 incidents against entities in Poland and 46 incidents against entities in Germany. Notably, a significant portion of these incidents, approximately 70%, can be attributed to attacks by NoName057(16), particularly impacting the public administration (14), transportation (13), and financial (9) sectors in Poland. Similarly, attacks attributed to NoName057(16) account for 54% of all documented incidents targeting German entities. Within Germany, the public administration (17), manufacturing (6), and other services (5) sectors have been the primary targets of these attacks.

Switzerland

Throughout the second quarter of 2023, the CyberPeace Institute documented a significant increase in cyberattacks targeting Swiss entities, with attacks escalating by 2,500% compared to the previous quarter. This surge is highly likely linked to Switzerland’s Council of State’s decision in early June to permit arms re-exports to Ukraine. In the subsequent weeks, the CyberPeace Institute recorded 69% of all cyberattacks conducted against Swiss entities in Q2, 2023.
**Notable incidents**

**Disruption**

April 4, 2023

NoName057(16) claimed responsibility for a confirmed DDoS attack against the website of the Finnish parliament.\(^{37}38\)

May 5, 2023

NoName057(16) claimed responsibility for two confirmed DDoS attacks against the website of the French senate.\(^{30}404142\)

June 12, 2023

NoName057(16) claimed responsibility for a confirmed DDoS campaign against Swiss entities, targeting the websites of two federal departments, two federal offices and the parliament.\(^{43}4445464748\)

June 19, 2023

KillNet and Anonymous Sudan have conducted DDoS attacks against two websites of a European financial institution.\(^{4950}\)

**Disinformation**

June 13, 2023

French authorities have reported on an ongoing cyber-enabled information operation against French government websites and French news media. Doppelganger websites have been discovered promoting disinformation in regards to the ongoing armed conflict in Ukraine. This campaign has been attributed to Russian state actors by French authorities.\(^{51}\)
In the second quarter of 2023, the CyberPeace Institute discovered the 100th threat actor, conducting malicious cyber activities in the context of the conflict in Ukraine. Currently, the CyberPeace Institute monitors, on a daily basis, the activities of more than 100 threat actors.

The CyberPeace Institute generally delineates the threat actors in three groups: state-sponsored actors, cybercriminals, and hacktivist collectives, of which the latter group accounts for 52% of all tracked threat actors. The modus operandi of the vast majority of hacktivist collectives, both pro-Russian and pro-Ukrainian, is conducting DDoS attacks, which account for 83% of all incidents documented by the CyberPeace Institute, since the start of the monitoring in 2022.

Impact and harm of DDoS attacks

Denial-of-service (DoS) attacks occur when malicious threat actors disrupt the availability of online resources. Distributed denial-of-service (DDoS) attacks, on the other hand, are more powerful and involve a coordinated effort to target the availability of internet services and resources. These attacks use similar techniques as regular DoS attacks, but on a larger scale. They involve multiple sources or locations simultaneously. In practice, DDoS attacks cause an online resource, such as a website with crucial information or an online service portal, to become inaccessible or unavailable to visitors for a period of time during or following an attack.

One of the primary methods used to execute successful DDoS attacks is through the use of botnets. A botnet is a network of internet-connected devices that have been infected with malware and are controlled by a single entity known as a “bot-herder.” The bot-herder manages the bots within the network and can orchestrate DDoS attacks by leveraging the resources of all the infected devices simultaneously. NoName057(16) is a known threat actor utilizing a botnet, operating a network established by the Bobik malware, with a significant number of bots located in Brazil, India, and Southeast Asia.

However, malware infection is not the sole method for constructing a botnet. Some threat actors, like the pro-Russian Anonymous Sudan collective, opt to pay for servers through which they carry out DDoS attacks. Others choose to crowdsource their DDoS activities by distributing downloadable software that adds volunteers’ devices into a botnet. Both NoName057(16) and IT Army of Ukraine have used this approach, the former using an offensive crowdsourcing DDoS tool called DDOSIA Project, while the latter is employing both offensive and defensive crowdsourcing DDoS projects, such as disBalancer and Liberator.

The impact of DDoS attacks can be direct and indirect. For targeted organizations, immediate consequences include disruptions to resource availability, leading to potential financial and reputational losses. Often, due to concerns about reputation, many businesses choose not to disclose DDoS incidents. As Arora, Kumar, and Sachdeva note, the challenge for researchers is obtaining details about these attacks, as disclosure is often limited.

DDoS attacks also have repercussions for the general population. The unavailability of online
resources can disrupt daily lives, leading to widespread issues such as anxiety or loss of confidence in governmental authorities. Research suggests that people are more likely to react to the effects of a cyberattack than the attack itself.\textsuperscript{59}

In the context of a conflict, DDoS attacks can directly impact civilians by disrupting the availability of critical online resources. For example, non-governmental organizations play a pivotal role in providing humanitarian aid during conflicts. However, if their online resources are inaccessible, civilians may not be able to access essential services. The CyberPeace Institute has documented DDoS attacks against ten humanitarian funds operating in Ukraine.

The financial sector has been a primary target, with DDoS attacks affecting institutions in Ukraine, other countries, and Russia. Reports have also highlighted an increase in DDoS activities targeting financial institutions.\textsuperscript{60} Such attacks may result in monetary losses and reputational damage for financial organizations.

DDoS attacks can hinder healthcare provision by disrupting access to online resources and interrupting business continuity. Healthcare professionals' work can be impacted due to disrupted access to critical assets like health records, medical equipment, or communication channels. Moreover, disruptions in the availability of online resources can affect the prescription of drugs, potentially endangering patients' well-being. Healthcare encompasses various organizations critical to the general population, such as suicide-prevention hotlines. Attacks against these services could have severe consequences. Lastly, an additional impact is caused when devices become corrupted or misconfigured following a crash, placing a significant additional burden on technical and medical staff due to diversion of resources.

Public administration has been a primary target in Ukraine, Russia, and countries which are not belligerents in this conflict. Such attacks not only impact government activities but can also directly and indirectly affect citizens. A DDoS attack that allegedly targeted Russia's only product authentication system, Chestny Znak, serves as an example of the direct impact such attacks can have.\textsuperscript{61}

As each product in Russia requires its unique identifier and company barcode to be scanned, from production to sale, the DDoS attack on Chestny Znak's servers purportedly led to the inability to authenticate products within the country for several days. Thus, making economic consequences highly likely. DDoS attacks carry significant implications, impacting organizations, populations, and even influencing narratives amidst a conflict.
Monetization of hacktivism

In the second quarter of 2023, two prominent pro-Russian hacktivist collectives, NoName057(16) and KillNet, continued to be responsible for a significant portion of Distributed Denial of Service (DDoS) attacks targeting both Ukrainian and non-belligerent entities in the conflict. Notably, NoName057(16) maintained its malicious activities, while KillNet underwent significant changes in its structure and ideology.

Originally established by an individual using the pseudonym KillMilk as a DDoS-as-a-service in late 2021, KillNet began its participation in response to the global hacktivist collective Anonymous declaring a "cyber war against the Russian Federation". Over time, KillNet expanded and evolved into one of the most prominent politically motivated pro-Russian hacktivist groups. However, beginning in 2023, a gradual decline in KillNet’s activities was observed by the CyberPeace Institute. KillMilk announced a restructuring of KillNet into the “Private Military Hackers Organization Black Skills,” (Black Skills) citing a dispute within the Russian cyber community as a contributing factor. This reorganization signaled a shift towards monetization of the hacktivist collective’s activities, potentially posing threats to Ukrainian civilians and populations in other countries.

Shortly after the announcement of Black Skills, KillNet's Telegram channel promoted the potential sale of the source code of a well-known spyware. Subsequently, KillNet introduced Dark School, an educational initiative aimed at teaching individuals various malicious cyber techniques. This "school" offered nine courses in four languages – Russian, English, Spanish, and Hindu. Later, another dispute led to the exposure of Anonymous Russia's founder, a member of KillNet since September 2022. Following this, an individual using the pseudonym Radis was appointed as the new leader of Anonymous Russia. Radis quickly declared a shift in Anonymous Russia's approach by offering paid services, thereby also embracing monetization. Throughout Q2 of 2023, Anonymous Russia introduced a rental service for the TITAN Stealer malware.

The TITAN Stealer is a type of information-stealing Trojan, written in Golang, designed to surreptitiously extract sensitive data from infected systems. It primarily targets financial institutions and organizations, stealing login credentials, passwords, credit card details, and other personal or financial information. Distribution typically occurs through malicious email attachments, compromised websites, or social engineering tactics. Once installed, TITAN Stealer collects data from the target’s computer and sends it to a remote server controlled by the attackers. This stolen information can be exploited for identity theft, financial fraud, or other illicit activities.

On April 26, 2023, KillMilk officially announced the establishment of the "Russian private military hacker company KillNet," signaling the end of KillNet’s “altruistic activities." A week later, KillNet introduced an official crypto-exchange market. On May 15, 2023, Radis similarly announced the cessation of "altruism" and transitioned to commercial activities, potentially establishing an online dark market for trading malware and malicious services.

On May 24, 2023, KillMilk confirmed the disbandment of KillNet's core, attributing it to the collective's perceived shift away from hacktivism. Radis announced his departure a week later, citing a lack of progress on the dark web and a desire to avoid resentment.
The CyberPeace Institute is unaware of the chronological progression of events that led to the disbandment of the KillNet group and the subsequent alterations within its structure. KillNet reportedly reemerged with a new core on June 12, although no incidents have been conclusively attributed to them for the remainder of the quarter due to a lack of substantiating evidence for their attack claims.

While internal conflicts have disrupted the KillNet collective, NoName057(16) has shown a continued escalation in its malicious activities, primarily targeting entities situated in countries which are not belligerents in this conflict. Radware's positions NoName057(16) as the most prolific threat actor, aligning with the findings of the CyberPeace Institute based on the incidents cataloged on the Cyber Attacks in Times of Conflict Platform #Ukraine. Notably, the Institute's data collection has unveiled a discernible pattern in NoName057(16)'s actions – the threat actor predominantly employs Distributed denial-of-service (DDoS) attacks as a responsive measure to geopolitical events. Examples of these events include official visits by Ukraine's President Zelenskyy or media reports concerning new military and economic assistance for Ukraine.

Displayed below is a graphical representation wherein the CyberPeace Institute has categorized the rationales presented by NoName057(16) behind executing DDoS attacks on entities across several countries. These rationales have been compartmentalized into eight distinct classes. The term "Aid" pertains to financial and/or civilian support extended to Ukraine by countries which are not belligerents in the conflict, while "Military" signifies any form of military assistance. "Narrative" denotes motivations for attacks aimed at advancing specific narratives related to the conflict, usually coined by official governmental bodies within the Russian Federation. "NATO" encompasses rationales tied to official announcements or training activities by NATO.

The "Official Visits" category encompasses motives for attacks arising from visits of Ukrainian officials to other countries. "Political" refers to motivations related to official political shifts categorized as Russophobic by NoName057(16). "Sanctions" encompasses motives for attacks triggered by

Reason for DDoS attacks self-attributed by NoName057(16).
by the imposition of global and/or national sanctions targeting the Russian Federation. "Statements" covers rationales stemming from statements made and/or endorsed by official entities in the targeted countries. Lastly, "Unknown" encompasses any motivations that do not fit within the scope of the other seven categories.
Wider Contextual Considerations

Events

During the second quarter of 2022, the most notable kinetic development affecting one of the belligerent nations in the conflict was Wagner’s advance toward Moscow. The CyberPeace Institute did not observe any escalation in malicious cyber activities targeting Russian entities during Wagner’s PMC march to Moscow. The incident was widely seen as a challenge to the legitimacy of the Russian Federation’s official government from Yevgeny Prigozhin.

In the heatmap depicted below, the CyberPeace Institute has documented instances of cyberattacks associated with geopolitical occurrences, specifically focusing on non-belligerent countries’ responses concerning sanctions, military assistance, and public statements related to the conflict.

Heat matrix indicating the number of incidents per week for all countries with more than 10 incidents in Q2 2023 overlaid with documented
At the beginning of April, Ukraine’s military initiated the deployment of the first MiG-29 fighters aircrafts received from Poland. It is highly likely this action led pro-Russian threat actors to intensify attacks against Polish entities, with Poland becoming the most targeted country beyond the 2 belligerent countries, during Q2 of 2023. During March, Slovakia had also announced their decision to deliver 13 MG-29 aircraft to Ukraine.83

The delivery of tanks has also continued, with Germany, Canada, and the United Kingdom successfully completing the transfer of Leopard 2 and Challenger tanks84, which highly likely caused an increase of attacks against entities in Germany and Canada by 4.5% and 867%, respectively. In a continuation of support from European Union members, Spain dispatched six Leopard 2A4s. It’s highly likely that this action contributed to a 43% surge in attacks against Spanish entities in Q2.85 Throughout April, additional commitments were made for tank transfers, including Denmark and the Netherlands pledging to send 14 more Leopard 2 tanks, likely leading to a 23%, and 56% increase in attacks against entities in the two countries respectively.86 Denmark later announced, in early May, the intention to transfer an additional 80 Leopard 1 tanks to Ukraine, in conjunction with Germany.

Over the course of the second quarter, countries including the United Kingdom, Latvia, Estonia, Canada, Italy, Denmark, the Netherlands, Sweden, and Poland continued, or made promises, to provide training for Ukrainian soldiers to effectively operate the weaponry supplied by Ukraine's allies.87 88 89 90 91 92 93 94 95

The landscape of sanctions and official statements also saw notable developments. In the second quarter of 2023, several countries imposed fresh sanctions against the Russian Federation. Latvia enhanced regulations governing the presence of Russian citizens within its territory, while Bulgaria closed off access to all ports for Russian vessels.96 97 The general secretary of Japan's government declared new sanctions against Russia.98 However, the CyberPeace Institute did not document any pronounced surge in cyberattacks targeting entities within these mentioned countries. By the conclusion of the quarter, the European Union collectively agreed on the 11th sanctions package, specifically targeting the Druzhba oil pipeline.99 100
Other Research

In recent months, several significant developments have emerged in the realm of cyber operations and threat activities, particularly within the context of the ongoing Russia-Ukraine conflict. These events shed light on evolving tactics, potential risks, and the intricate interplay between cyber warfare and kinetic actions.

Stiftung Wissenschaft und Politik (SWP) published an insightful analysis on the role of cyber operations in the Ukraine conflict. The report delves into Russia's cyber strategies, emphasizing intelligence gathering, data destruction, and Denial-of-Service (DoS) attacks on critical infrastructure. While acknowledging Ukraine's proactive cyber defense measures and societal resilience, the analysis questions the strategic effectiveness of Russia's cyber warfare in terms of substantial gains. The importance of cyber resilience is underscored, along with key takeaways from Ukraine's wartime cyber efforts.

ESET released a comprehensive report summarizing observations and analyses of advanced persistent threat (APT) groups from Q4 2022 to Q1 2023. The report highlights APT activities across various countries, including China, India, Iran, North Korea, and Russia. In this period, ESET researchers provided a critical assessment of APT group operations, shedding light on their evolving tactics and potential implications for cybersecurity.

Microsoft Threat Intelligence presented an updated evaluation of a threat actor, now identified as Cadet Blizzard, previously known as DEV-0586. This actor is associated with the Russian General Staff Main Intelligence Directorate (GRU). Microsoft highlighted Cadet Blizzard's resurgence in early 2023, engaging in heightened operations across Ukraine and Europe. The report emphasizes the importance of protective measures against Cadet Blizzard's activities, accompanied by discussions on detection and prevention strategies.

Sekoia's blog post delves into the DDoSia project, a Distributed Denial of Service (DDoS) attack toolkit attributed to the pro-Russian hacktivist group NoName057(16). The analysis uncovers the project's mechanics, communication channels, registration processes, and execution of attacks. Notably, the report highlights the project's primary targets: Ukraine, NATO countries, and select Western nations supporting Ukraine. Various sectors, including education, finance, government, and transport, are among the specific targets.

Mandiant's M-Trends 2023 Special Report offers insights from consulting investigations spanning January 1, 2022, to December 31, 2022. The report covers diverse topics, such as cyber operations within the Ukraine conflict, notable threat groups, vulnerabilities, and North Korean cybercrime. An intriguing highlight is the potential overlap between cyber operations and kinetic warfare, as evidenced by Russian actions impacting industrial control systems and critical infrastructure.

These reports provide a comprehensive view of recent cyber operations, threat activities, and their implications. The evolving nature of cyber warfare underscores the necessity for enhanced cyber resilience and adaptive strategies in conflicts.
Report Methodology

This report focuses on the incidents documented by the CyberPeace Institute in the second quarter of 2023. Therefore, analysis only covers attacks and campaigns between April 1 and June 30, 2023. For trends-based analysis, the CyberPeace Institute may refer to numbers during a wider date range, in this case the dates are referenced accordingly in the report. Information within the report is generated from data collected by the CyberPeace Institute and made accessible through the Cyber Attacks in Times of Conflict Platform. Specific details and sources of information regarding any individual cyber incidents referenced in this report can be found in the Attack Details page.

As there is a reliance on publicly available data, the data on documented cyberattacks has been given a classification of certainty based on the reliability of the information source. The classification levels are Possible, Probable and Confirmed. Additionally, the CyberPeace Institute distinguishes between singular incidents and campaigns. When conducting analysis it is instrumental to accurately communicate probability in the assessment of our findings and inferences. The CyberPeace Institute uses the UK’s Defence Intelligence standard for conveying probability; the ‘Professional Head of Intelligence Assessment (PHIA) probability yardstick’. This scale demonstrates broad ranges of certainty or uncertainty that can be translated into consistent language; this language is used throughout this report.

Disclaimer: Base maps are for graphical purposes only and there should be no inference of the borders of a country or territory. The CyberPeace Institute used the naming convention of countries and their categorization based on the United Nations Statistics Division.
References


18 Operatyvnyj shtab - Krasnodarskij kraj (2023) [Telegram]. Available at: [https://t.me/opershtab23/7041](https://t.me/opershtab23/7041) (Accessed: 13 June).

19 Operatyvnyj shtab - Krasnodarskij kraj (2023) [Telegram]. Available at: [https://t.me/opershtab23/7054](https://t.me/opershtab23/7054) (Accessed: 13 June).

20 News Media Source


26 Operatyvnyj shtab - Krasnodarskij kraj (2023) [Telegram]. Available at: [https://t.me/opershtab23/7041](https://t.me/opershtab23/7041) (Accessed: 13 June).

27 Operatyvnyj shtab - Krasnodarskij kraj (2023) [Telegram]. Available at: [https://t.me/opershtab23/7054](https://t.me/opershtab23/7054) (Accessed: 13 June).


30 Skolkovo Live (2023) [Telegram]. Available at: [https://t.me/skolkovolive/4497](https://t.me/skolkovolive/4497) (Accessed: 30 May 2023).


32 KillMilk (2023) [Telegram]. Available at: [https://t.me/killmilk_rus/836](https://t.me/killmilk_rus/836) (Accessed: 25 May 2023).

33 KillMilk (2023) [Telegram]. Available at: [https://t.me/killmilk_rus/724](https://t.me/killmilk_rus/724) (Accessed: 20 April 2023).


35 Phoenixinform (2023) [Telegram]. Available at: [https://t.me/phoenixinform/2118](https://t.me/phoenixinform/2118) (Accessed: 12 June 2023).

36 NoName057(16) (2023) [Telegram]. Available at: [https://t.me/noname05716/2656](https://t.me/noname05716/2656) (Accessed: 5 April 2023).

37 [https://www.eduskunta.fi/EN/tiedotteet/Pages/ddos_web serviço_parliament_20230404.aspx](https://www.eduskunta.fi/EN/tiedotteet/Pages/ddos_web serviço_parliament_20230404.aspx)

38 NoName057(16) (2023) [Telegram]. Available at: [https://t.me/noname05716/3110](https://t.me/noname05716/3110) (Accessed: 6 May 2023).

39 Senat (2023) [Twitter]. Available at: [https://twitter.com/Senat/status/1654408818934120448?cxt=HHwWgIC83cWD0vUtAAAA](https://twitter.com/Senat/status/1654408818934120448?cxt=HHwWgIC83cWD0vUtAAAA) (Accessed: 6 May 2023).

40 NoName057(16) (2023) [Telegram]. Available at: [https://t.me/noname05716/3262](https://t.me/noname05716/3262) (Accessed: 16 May 2023).


42 NoName057(16) (2023) [Telegram]. Available at: [https://t.me/noname05716/3660](https://t.me/noname05716/3660) (Accessed: 13 June 2023).
43 NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3659 (Accessed: 13 June 2023).
44 NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3658 (Accessed: 13 June 2023).
45 NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3657 (Accessed: 13 June 2023).
46 NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3655 (Accessed: 13 June 2023).
55 https://disbalancer.com
64 KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5681 (Accessed: 13 March 2023).
65 KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5740 (Accessed: 19 March 2023).
66 KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5967 (Accessed: 5 April 2023).
67 KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/724 (Accessed: 18 April 2023).
70 Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/3 (Accessed: 17 April 2023).
71 Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/6 (Accessed: 17 April 2023).
72 Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/94 (Accessed: 23 April 2023).
73 Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/217 (Accessed: 4 May 2023).
76 KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/794 (Accessed: 27 April 2023).
77 KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6595 (Accessed: 10 May 2023).
78 Radis (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6668 (Accessed: 16 May 2023).
79 KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/836 (Accessed: 26 May 2023).
80 Radis (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6830 (Accessed: 6 June 2023).
89 Ibid
91 Ibid
107 Ibid
109 Ibid