State Service
of Special Communications
and Information
Protection of Ukraine

Russian Cyber Operations

APT Activity Report #3
H2 2023

Yevheniia Volivnyk,
Chief of the Computer Emergency
Response Team of Ukraine (CERT-UA)

The protracted conflict in Ukraine has served as a catalyst for the rapid advancement of Russian cyber capabilities. Over the past two years, we've observed a surge in activity by well-established Russian APT groups, coupled with the emergence of new actors and specialized skill sets. This dynamic threat landscape underscores the evolving nature of Russian cyberwarfare, with a focus on leveraging these capabilities for multifaceted objectives.

Key Observations:

- **Enhanced Capabilities**: Last 2 years accelerated the development of Russian cyberwarfare tactics and techniques. Their APT groups exhibit increased sophistication, suggesting the recruitment and integration of new talent.
- **Expanding Threat Landscape**: The emergence of new actors suggests a deliberate strategy by Russia to diversify its cyberwarfare arsenal. These groups may possess unique skill sets or specialize in specific operational objectives.
- **Intelligence Gathering and Amplification**: Russian cyber operations extend beyond traditional disruption. There's a clear focus on utilizing cyber tools for intelligence gathering in support of traditional military operations (kinetic, psychological, and effects-based). This convergence further amplifies the impact of both cyber and physical warfare tactics.

This escalating cyber threat necessitates a heightened state of vigilance and a proactive approach to defense. Collaborative efforts among security researchers, industry leaders, and governments are essential to effectively mitigate the risks posed by Russia's evolving cyberwarfare capabilities.

For a more complete picture, we also ask you to familiarize yourself with our previous reports:

H2 2022

H1 2023

We have observed definitive shifts in the behavior and objectives of the most active APTs. Since the start of the second half of 2023, the attributed activity of known military actors has significantly decreased, while new, previously unidentified groups have emerged, utilizing novel and effective techniques and procedures.

Their origins and participants will still need to be determined, but previous experience and victimology suggests that they are also part of the Russian military machine or are informally funded and coordinated from Russian state command centers.

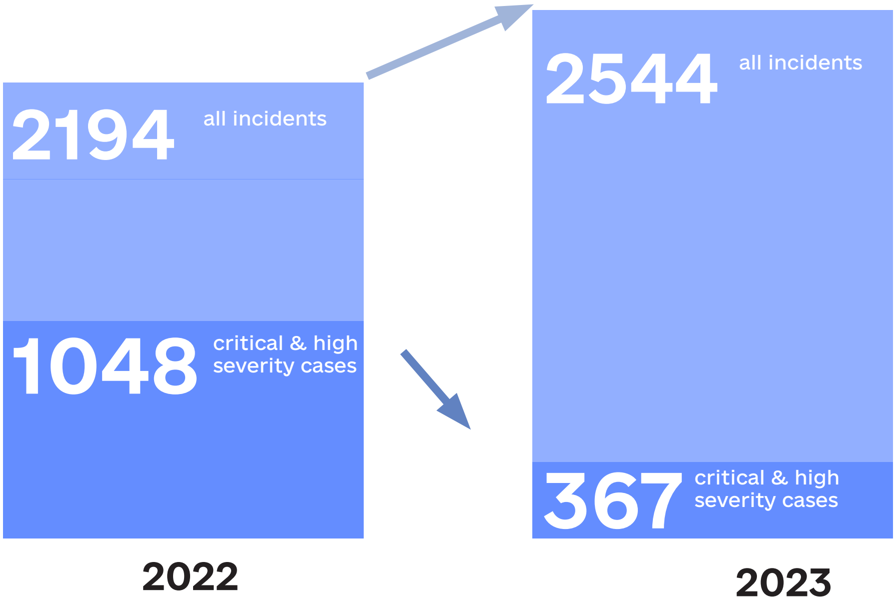
We are witnessing the emergence of a new breed of adversaries employing innovative tactics and shaping a novel vision for cyber operations. These sophisticated actors pose significant challenges that demand our attention and proactive measures to safeguard the digital realm.

The ongoing war in Ukraine has served as a stark reminder of the ever-increasing sophistication and frequency of cyber operations during all kinds of conflicts. We have observed a surge in targeted attacks, many of which exhibit heightened technical complexity. Some Russian operations were bright and effective as destruction, but total fiasco in planning and from a long term perspective. This underscores the critical need to bolster our cybersecurity posture, share experience, cases, enhance collaboration, and foster a robust exchange of information and technologies among partners. The H2’2023 served as a stark reminder of the critical need to prioritize the cybersecurity of Internet Service Providers (ISPs) and Telecommunication companies. While ISPs and Telcos invest in security solutions, complacency can set in, leading to a failure to adapt to the ever-evolving tactics of national threat actors. This creates a gap in defenses that APTs can exploit, potentially causing widespread disruption and compromising national security.

Ukraine, unfortunately, has become a testing ground for the latest cyber weaponry, highlighting the urgency of collective action. The knowledge and skills gained from this confrontation will prove invaluable in shaping our future defense strategies.

KEY FINDINGS AND INSIGHTS

KEY FINDINGS AND INSIGHTS



We managed to reduce the number cyber incidents with critical and high severity incidents in 2023 by

65%

Shifting Targets and No Immunity: While the first half of 2023 saw a focus on exploiting zero-day vulnerabilities in popular client-end software (e.g. Microsoft Outlook) by GRU-linked actors, H2 witnessed a surge in attacks against well-prepared telecommunications providers (with all their budgets and manpower), highlighting their critical role in the digital infrastructure, readiness and recoverability testing.

Continuous Improvement: Security strategies and defenses must undergo continuous evaluation and improvement to stay ahead of emerging threats.

Evolving Tactics: Attackers are increasingly employing N-day exploits, known vulnerabilities for which patches have been released but not yet widely adopted. Additionally, the use of mobile implants, malicious software embedded on mobile devices, has increased.

Emergence of New Actors: New military focused APTs and criminal organizations previously undetected are now dominating the cyber threat landscape in Ukraine, demonstrating the ever-changing nature of cyber threats and rise of Russian cyber capital.

*0-day exploits advantage of unknown vulnerabilities which are highly valuable to attackers because they can be used to infiltrate systems undetected. They are often sold on the black market or used by cyber attackers before the vendor becomes aware of the vulnerability and fixes it. Once a 0-day exploit is disclosed or detected, it becomes a known vulnerability, and the race begins to patch the affected systems before widespread damage can occur.

**An N-day exploit leverage vulnerability which is a known security weakness that may or may not be widely patched yet.

*For example activity of APT28

KEY INSIGHTS H2 2023:

TELECOM — A BIG AND FRUITFUL TARGET

A Targeted Campaign by Russian Hackers Targeting Telecommunications Providers

ACTIVE USE OF THE LATEST EXPLOITS AS CYBER WEAPONS

More active use of the latest vulnerabilities in client-side software (client-side attacks) for the purpose of hidden access and implantation.

NEW GROUPS DOMINATE OVERALL STATISTICS

The ranking of the most active threat actors has been topped by groups currently not associated with the special services of the aggressor country (although they operate in the interests of the Russian authorities). They distinguished themselves by using well-thought-out phishing attacks, the main goal of which is to distribute malicious remote control software (RemcosRAT, RemoteUtilities) or data theft programs (LumaStealer, MeduzaStealer).

SURGE IN ACTIVITY FROM FINANCIALLY MOTIVATED CYBERCRIME GROUPS

We are witnessing an increase in activity from financially motivated cybercrime groups targeting Ukrainian businesses and organizations. In the second half of 2023, approximately 40% of registered incidents were related to financial theft. For instance, the UAC-0006 group resumed its operations in May 2023, and the number of incidents associated with their activities grew to 200 in the second half of the year.

TARGETED CYBER ESPIONAGE OPERATIONS AGAINST UKRAINE DEFENSE FORCES (UAF)

Attacks aimed at gaining access, control, and extracting intelligence from specialized battlefield control systems are a strategic military objective of the adversary. To gain access and compromise credentials for such systems, and to access military chats, hackers created and distributed fake versions of software, carried out attacks aimed at compromising messengers actively used by the military.

RAPID EXPLOITATION OF TRENDING TOPICS

A high operational tempo of malware propagation leveraging current news events, such as Ukraine's NATO membership bid or IDF recruitment (during the onset of the Israeli military conflict).Threat actors are demonstrating a keen ability to capitalize on topical events to heighten the effectiveness of their cyberattacks. By aligning their attacks with trending narratives, they can exploit the increased attention and potential complacency of targets.

Automation and Speed: Attackers are increasingly leveraging automation to accelerate their infiltration and control of critical IT systems. The APT28 group is a prime example of this trend.

Threat Intelligence Sharing: Sharing threat intelligence and best practices can significantly enhance collective cybersecurity posture.

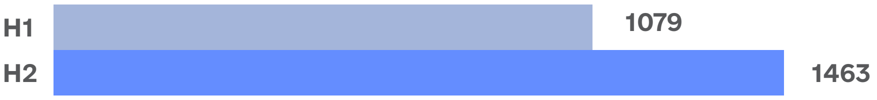
Collaborative Defense: Collaboration among organizations, security researchers, and government agencies is crucial to effectively combat cyber threats. We share this report to express our gratitude for all help provided to Ukraine.

KEY NUMBERS IN H2 2023

Disclaimer: This dataset is compiled based on incident analytics provided by the Computer Emergency Response Team of Ukraine CERT-UA, excluding cases registered by the SOC of the State Center for Cybersecurity of the State Special Communications Service and other cyber centers.

CHANGES: H1 VS. H2 2023

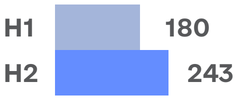
CASES INVESTIGATED BY CERT-UA TEAM



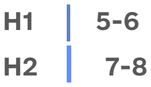
+36%

GROWTH IN THE NUMBER OF REGISTERED INCIDENTS IN THE SECOND HALF OF 2023 (EXCEPT SOC INCIDENTS)

MONTHLY AVERAGE



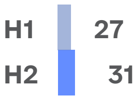
DAILY AVERAGE



+15%

GROWTH IN CRITICAL ONLY INCIDENTS IN THE SECOND HALF OF 2023

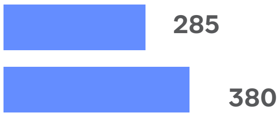
REGISTERED INCIDENTS WITH CRITICAL SEVERITY



+33%**

COMPROMISE ATTEMPTS VIA E-MAIL

IN WHICH THE MALWARE INFECTIONS PREVAILED

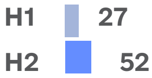


DUE TO STOLEN PASSWORDS TO MAILBOXES WITHOUT MFA

+92%

NEW ATTACKS ON THE ENERGY SECTOR AND A 50% REDUCTION IN THE NUMBER OF CRITICAL INCIDENTS

INCIDENTS IN ENERGY SECTOR



*The report of the The SSSCIP State Cyber Protection Center is available at the following link

**It is worth noting that in the second half of 2023, hostile cyber groups dramatically increased the use of such a tool as the distribution of malicious software via e-mail. The number of attempts at compromise in this way increased by 33% compared to the first half of 2023. If at the beginning of the year, 285 cases were recorded with the predominant use of phishing attacks, then in the second half of the year, 380 were recorded, a significant number of which were carried out from compromised mailboxes, which became possible due to the lack of two-factor authentication.

WHERE AND WHY: MOST TARGETED SECTORS

Cyber capabilities during wartime can be critical in shaping outcomes across different levels of military strategy. Here's a concise overview of their approach across the strategic, operational, and tactical layers:

Strategic

- Where to go

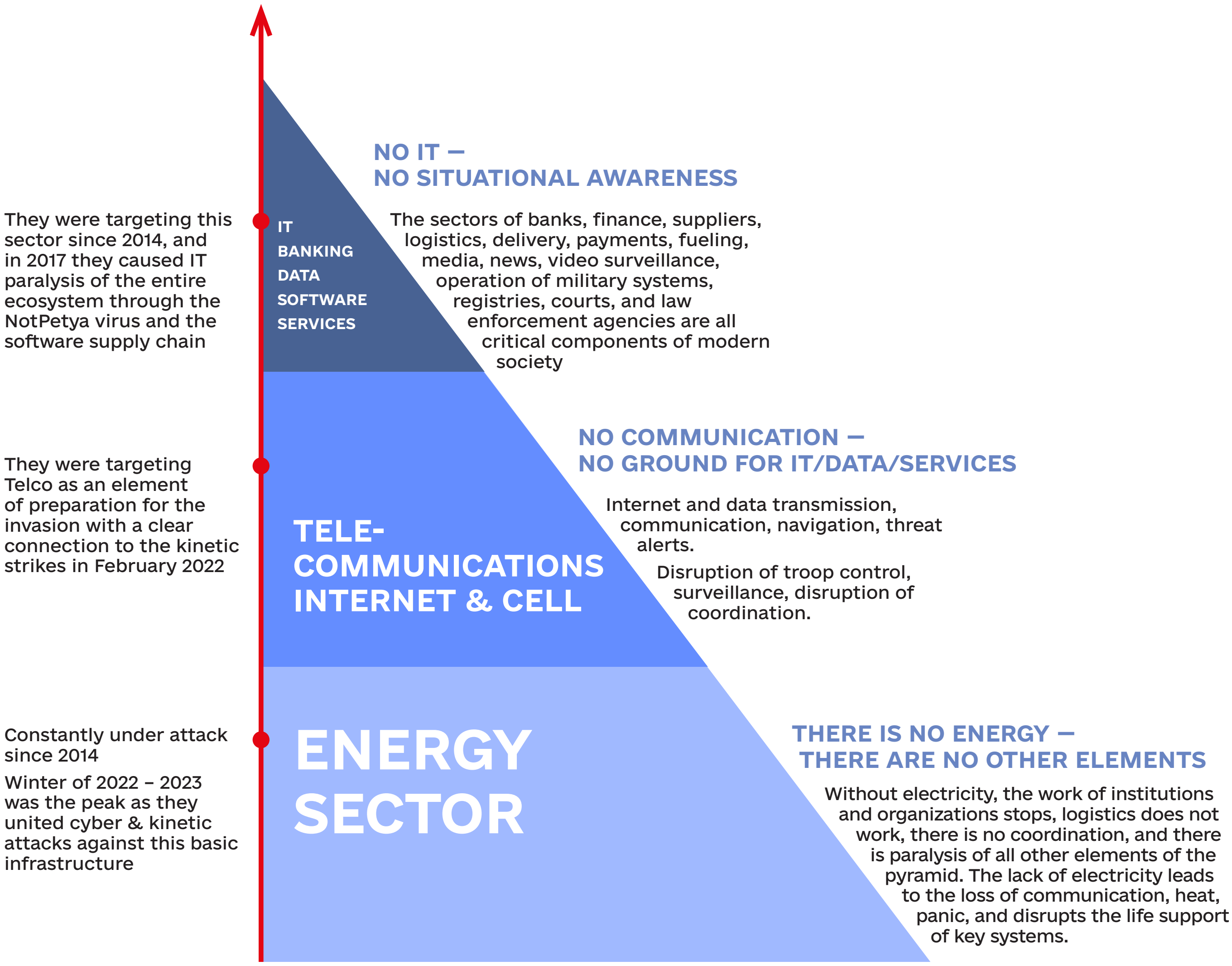
Operational

- How to get there

Tactical

- What to do when you're there

PYRAMID OF TARGETS & DEPENDENCIES IN CYBER ECOSYSTEM



They were targeting this sector since 2014, and in 2017 they caused IT paralysis of the entire ecosystem through the NotPetya virus and the software supply chain

IT
BANKING
DATA
SOFTWARE
SERVICES

NO IT — NO SITUATIONAL AWARENESS

The sectors of banks, finance, suppliers, logistics, delivery, payments, fueling, media, news, video surveillance, operation of military systems, registries, courts, and law enforcement agencies are all critical components of modern society

They were targeting Telco as an element of preparation for the invasion with a clear connection to the kinetic strikes in February 2022

TELE-COMMUNICATIONS INTERNET & CELL

NO COMMUNICATION — NO GROUND FOR IT/DATA/SERVICES

Internet and data transmission, communication, navigation, threat alerts.

Disruption of troop control, surveillance, disruption of coordination.

Constantly under attack since 2014

Winter of 2022 – 2023 was the peak as they united cyber & kinetic attacks against this basic infrastructure

ENERGY SECTOR

THERE IS NO ENERGY — THERE ARE NO OTHER ELEMENTS

Without electricity, the work of institutions and organizations stops, logistics does not work, there is no coordination, and there is paralysis of all other elements of the pyramid. The lack of electricity leads to the loss of communication, heat, panic, and disrupts the life support of key systems.

In 2023, a team of military hackers affiliated with GRU (also known as Sandworm and APT44) implemented 68 attacks, of which 10 were successful cyber operations of influence against telecommunications providers of Ukraine using technical vulnerabilities and the human factor. The cyberattack on Kyivstar is a full-fledged component of this hybrid war.

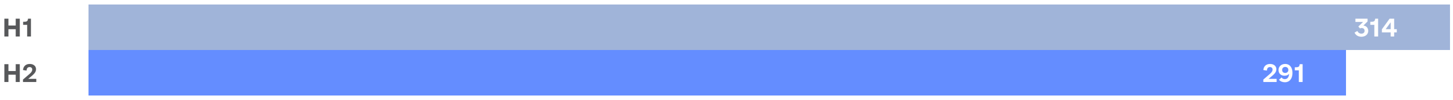
* known as Sandworm

In addition to nation-state actors, we are also observing a surge in activity from criminal groups. These groups are targeting user accounts on email services and cryptocurrency exchanges, aiming to steal large sums of money using malware and remote access trojans (RATs).

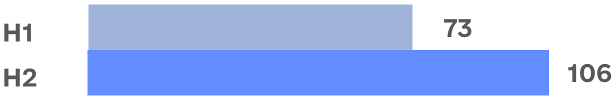
We also observe the active work of criminal groups that are focused on gaining access to the accounts of email services and cryptocurrency exchanges and stealing large amounts of funds using viruses and Remote Access Trojan.

TARGET SECTOR ANALYTICS

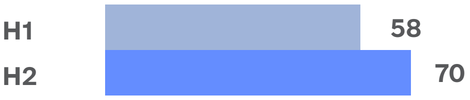
GOVERNMENT ORGANIZATIONS AND LOCAL AUTHORITIES



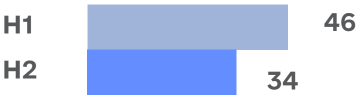
SECURITY AND DEFENSE SECTOR



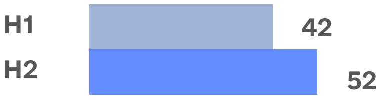
COMMERCIAL SECTOR



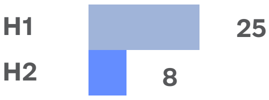
TELECOM AND ISP



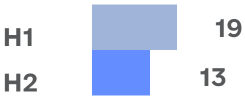
ENERGY SEGMENT



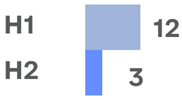
FINANCE



LOGISTICS



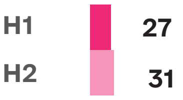
MEDIA



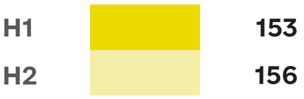
INCIDENTS DISTRIBUTION BY SEVERITY

For more details understanding of changing tactics from 2022 and during 2023 of the year — we recommend to familiarize yourself with content of the previous reports for the H1 2023

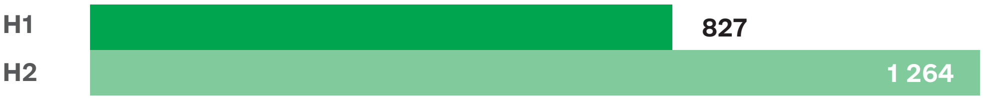
CRITICAL SEVERITY INCIDENTS



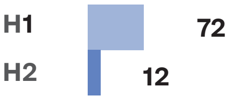
HIGH-SEVERITY INCIDENTS



MEDIUM-SEVERITY INCIDENTS



LOW-SEVERITY INCIDENTS



WHO & HOW

TOP-5 MILITARY HACKING GROUPS

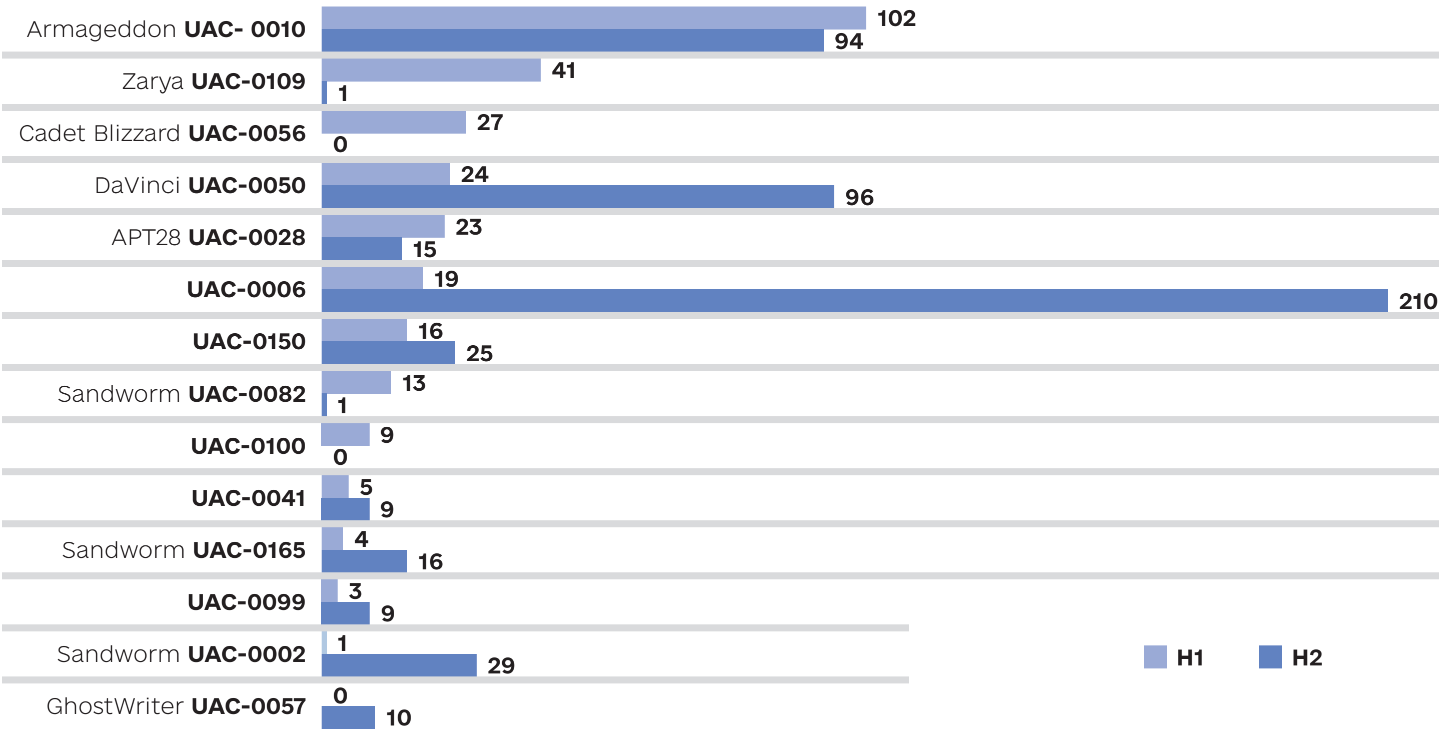
UAC-0010 (Armageddon)	FSB
UAC-0002 (Sandworm)	GRU
UAC-0028 (APT28)	
UAC-0056 (Cadet Blizzard)	
UAC-0057 (GhostWriter)	Ministry of Defense of Belarus

EVERY 10TH

cyberattack against Ukraine is carried out by the hacking teams working for military mission

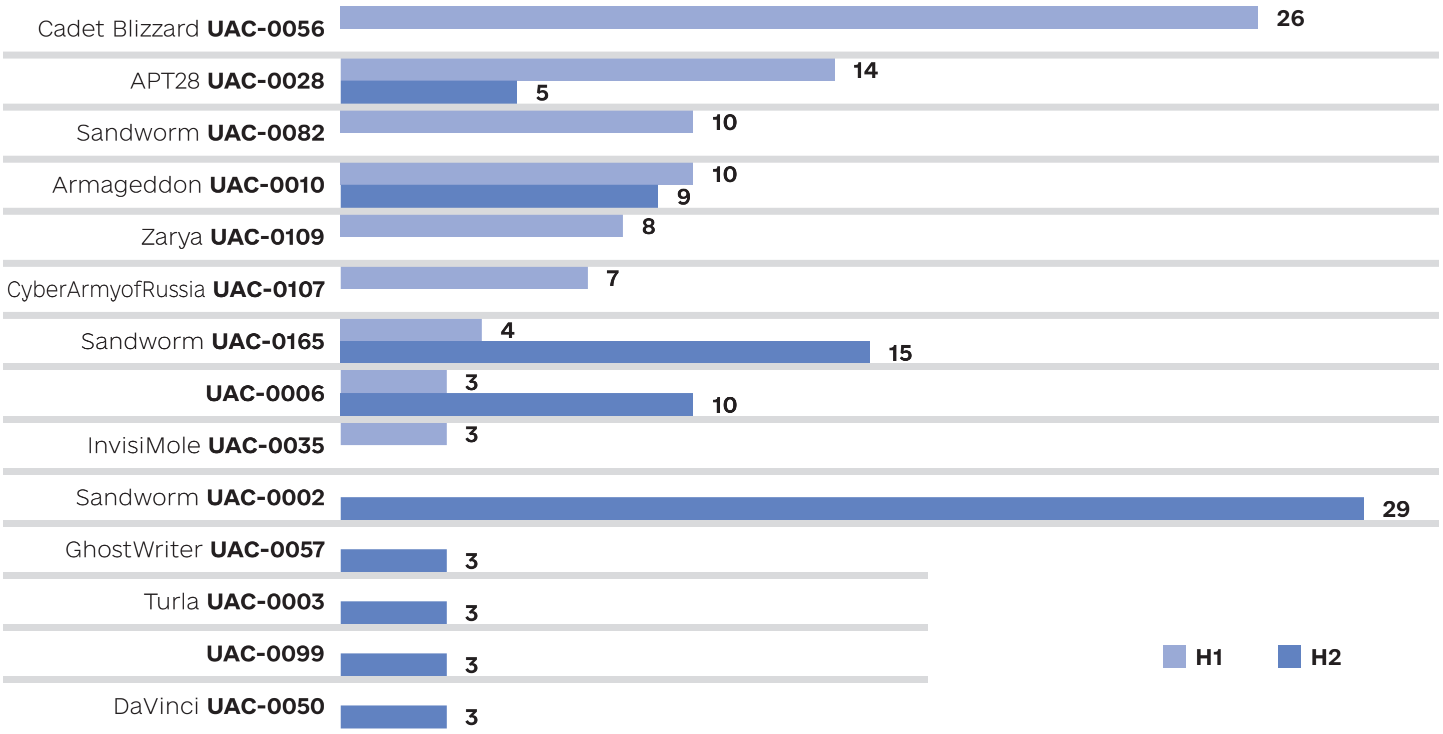
General statistics may not reflect the whole picture. Among the active players, there are many others who generate the maximum number of incidents, and there are those who cause significant damage with their attacks and conduct serious cyber operations.

THE MOST ACTIVE GROUPS THAT GENERATED THE LARGEST NUMBER OF CASES DURING 2023



However, for the completeness of the picture, it is necessary to understand who exactly caused real damage, carried out the most complex cyber operations. For this purpose, we selected those who fell into the segment of critical and high severity incidents and were attributed to well-known groups:

CRITICAL AND HIGH SEVERITY CASES BY THREAT ACTORS IN H1’2023



Among the 80 cases with a critical and high severity of APTs with known attribution (+45 cases without attribution) in the second half of 2023, the military groups affiliated with GRU — are dominating — both old and newly UAC.

Dominance is not observed for a long period of one or another group, which indicates the approach to work in small groups. This, CERT-UA analysts believe, may indicate the competitiveness of Russian hacking groups in the implementation of Effect operations.

NOTABLE CASES

Attacks against ISPs and Telcos

From late spring of 2023, the Russian military cyber command (GRU) tasked the Sandworm group, known for the NotPetya attack of 2017 and attacks on energy facilities, along with other related units, to conduct acts of terrorism against Ukrainian telecommunications and internet companies. Sandworm, the most successful group active against Ukrainian entities since 2014, is noted for initiating the first wave of attacks on Ukraine's energy sector in 2015. This group managed to quadruple the number of documented attacks from 14 in 2022 to 62 in 2023.

From May 11 to September 29, 2023, a coordinated group of cybercriminals, tracked under the identifier UAC-0165, also disrupted the information and communication systems of no fewer than 11 providers. This led to interruptions in internet access, hosting, and email services. A detailed description and technical information can be found at https://cert.gov.ua/article/6123309. Even then, signs of a targeted campaign were evident, about which CERT-UA had previously warned telecommunications companies and providers. After a detailed analysis of the cyber incidents, a connection with the Sandworm threat cluster was established.

Sandworm (APT44) is a military group that has been operating against Ukrainian organizations since 2014. It is known for its attacks on Ukrainian energy distribution companies in 2015, which marked the first-ever wave of attacks on the country's energy sector, as well as the NotPetya attack in 2017. The number of cyberattacks by Sandworm recorded in the second half of 2023 increased by 2.5 times (18 attacks in the first half of 2023 versus 48 attacks in the second).

* Detailed description with technical information

Moreover, Russia continues to employ hybrid attacks that combine cyber elements with missile strikes, aimed primarily at exacerbating the psychological impact on civilians. Their way to implement Effects Operations have multiple layers:

1. The effect itself
2. The perception of the effect
3. The psychological impact of the effect

With high certainty, the cyber attack on Kyivstar, Ukraine's largest mobile operator serving 25 million subscribers, can be attributed to these hybrid attacks. This attack coincided with missile strikes that resumed after a period of quiet. Please check the timeline of missile attacks here: https://en.wikipedia.org/wiki/Timeline_of_the_Russian_invasion_of_Ukraine_(1_December_2023_%E2%80%93_31_March_2024)

On December 8, Russian military forces conducted a massive missile attack on Kyiv, launching 20 missiles. Subsequently, on December 12, an attack was carried out on Kyivstar's virtual network. The next day, December 13, as many of Kyivstar's customers still experienced service disruptions, the aggressor launched an additional 10 missiles against Kyiv to intensify the «effect.»

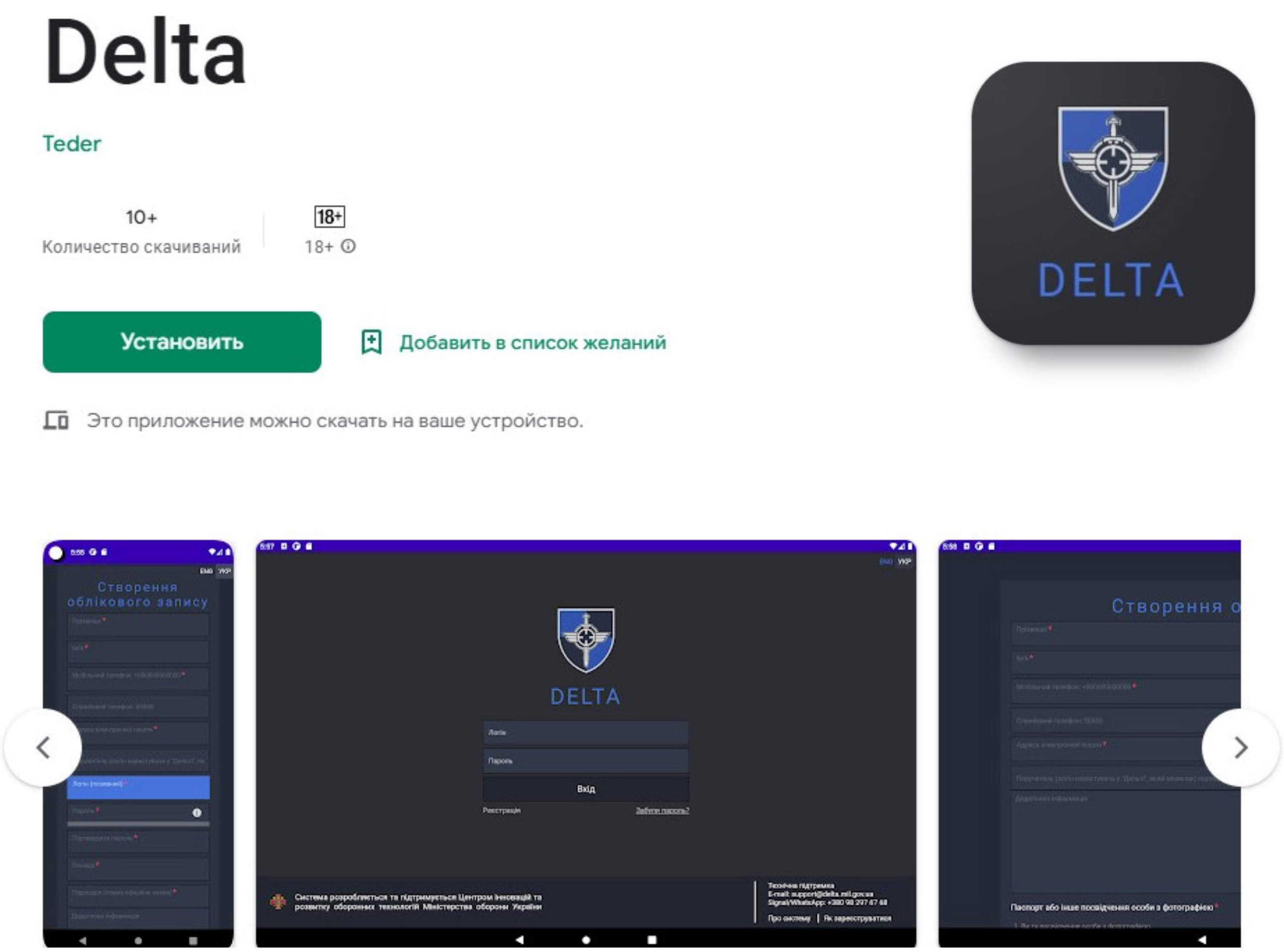
We can conclude that the Effects operations against KyivStar was potentially useful in the context of

- supplemental damage
- enabling information operations

Attacks against Military

During the second half of 2023, a notable series of attempts to breach national military situational awareness systems utilized by the Security and Defense Forces of Ukraine were observed. Although less frequent, attacks on mobile devices and supply chains have increased significantly in number over the year.

A particularly notable case involved a hacker group from the Russian military intelligence agency GRU, which deployed a mobile application mimicking the «DELTA» military app on Google Play before the Ukrainian Ministry of Defense could launch their official version. Russian hackers promoted the down-



Delta

Teder

10+
Количество скачиваний

18+

Установить

Добавить в список желаний

Это приложение можно скачать на ваше устройство.

DELTA

Створення облікового запису

Логін
Пароль
Вхід
Реєстрація
Забули пароль?

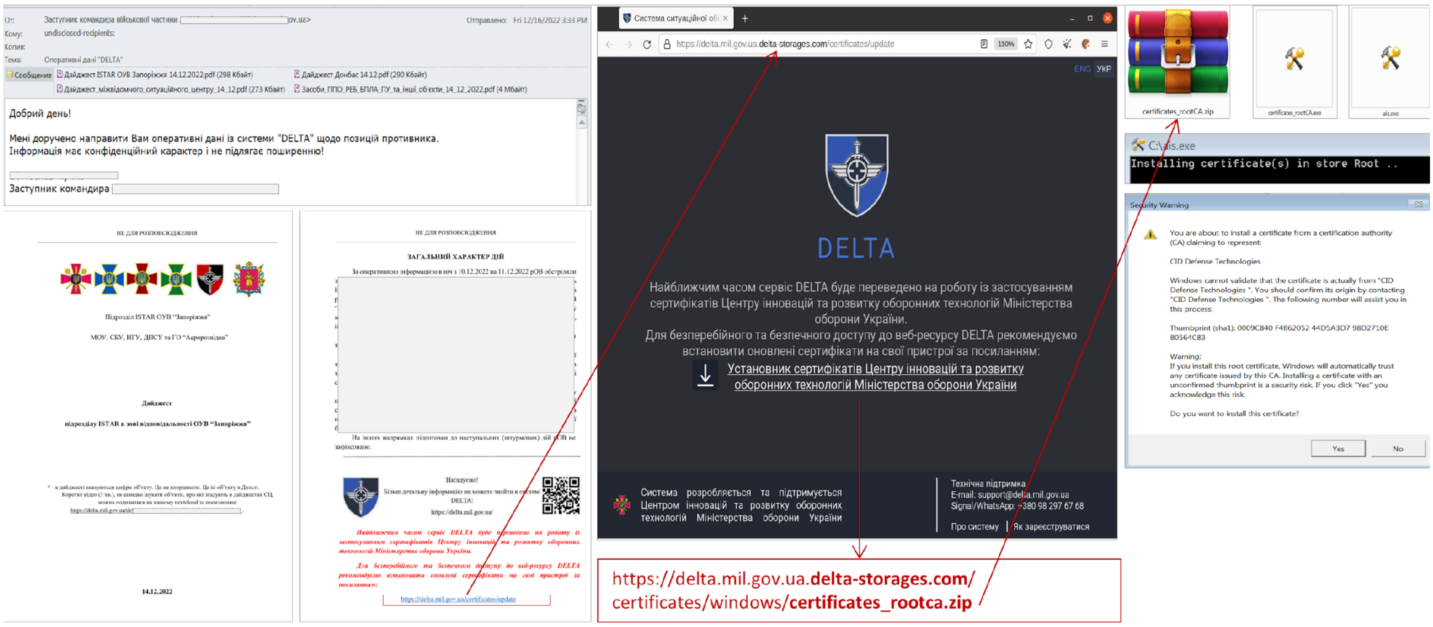
Система розробляється та підтримується Центром інновацій та розвитку оборонних технологій Міністерства оборони України

Технічна підтримка
E-mail: support@delta.mil.gov.ua
Signal/WhatsApp: +380 98 297 67 68
Про систему | Як зареєструватися

Створення о

Паспорт або інше посвідчення особи з фотографією load of this deceptive application among Ukrainian military personnel and senior officers. Such operations indicate the GRU's substantial reserve of development and distribution resources, as well as their strategic planning capabilities, suggesting a significant pool of developers actively engaged in various implantation and presence operations.

Additionally, we observed the distribution of an email urging updates to certificates within the "DELTA" system, utilizing a compromised email address from the Ukrainian defense ministry. The emails included PDF attachments mimicking legitimate ISTAR unit "Zaporizhzhia" digests, containing links to a malicious ZIP archive. Cybercriminals employed long-named domains and phishing sites to execute the infiltration, with the links appearing legitimate upon cursor hover, e.g., hXXps://delta.mil.gov.ua.delta-storages[.]com/certificates/update, enhancing their effectiveness in deceiving the targets.



От: Заступник командира військової частини [redacted]ov.ua> Отправлено: Fri 12/16/2022 3:33 PM
Кому: undisclosed-recipients:
Копия:
Тема: Оперативні дані "DELTA"

Сообщение | Дайджест ISTAR ОУВ Запоріжжя 14.12.2022.pdf (298 Кбайт) | Дайджест Донбас 14.12.pdf (290 Кбайт) | Дайджест_міжвідомчого_ситуаційного_центру_14_12.pdf (273 Кбайт) | Засоби_ППО_РЕБ_БПЛА_ПУ_та_інші_об'єкти_14_12_2022.pdf (4 Мбайт)

Добрий день!

Мені доручено направити Вам оперативні дані із системи "DELTA" щодо позицій противника.
Інформація має конфіденційний характер і не підлягає поширенню!

[redacted]
Заступник командира [redacted]

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ

Підрозділ ISTAR ОУВ "Запоріжжя"

МОУ, СБУ, НГУ, ДПСУ та ГО "Аеророзвідка"

Дайджест

підрозділу ISTAR в зоні відповідальності ОУВ "Запоріжжя"

* - в дайджесті вказуються цифри об'єкту. Це не координати. Це іd-об'єкту в Дельті.
Коротке відео (3 хв.), як швидко шукати об'єкти, про які згадують в дайджестах СЦ, можна подивитися на нашому nextcloud за посиланням:
https://delta.mil.gov.ua/de[redacted].

14.12.2022

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ

ЗАГАЛЬНИЙ ХАРАКТЕР ДІЙ

За оперативною інформацією в ніч з 10.12.2022 на 11.12.2022 рОВ обстріляли [redacted]

На інших напрямках підготовки до наступальних (штурмових) дій рОВ не зафіксовано.

Нагадуємо!
Більш детальну інформацію ви можете знайти в системі DELTA:
https://delta.mil.gov.ua/

Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.

Для безперебійного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:

https://delta.mil.gov.ua/certificates/update

Система ситуаційної обі
https://delta.mil.gov.ua.delta-storages.com/certificates/update
110%
ENG
УКР
DELTA

Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.
Для безперебійного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:
Установник сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України

Система розробляється та підтримується Центром інновацій та розвитку оборонних технологій Міністерства оборони України

Технічна підтримка
E-mail: support@delta.mil.gov.ua
Signal/WhatsApp: +380 98 297 67 68

https://delta.mil.gov.ua.**delta-storages.com/**
certificates/windows/**certificates_rootca.zip**

```
Installing certificate(s) in store Root ..
```

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CID Defense Technologies

Windows cannot validate that the certificate is actually from "CID Defense Technologies ". You should confirm its origin by contacting "CID Defense Technologies ". The following number will assist you in this process:

Thumbprint (sha1): 0009C840 F4B62052 44D5A3D7 98D2710E 80564C83

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Attacks against mobile users

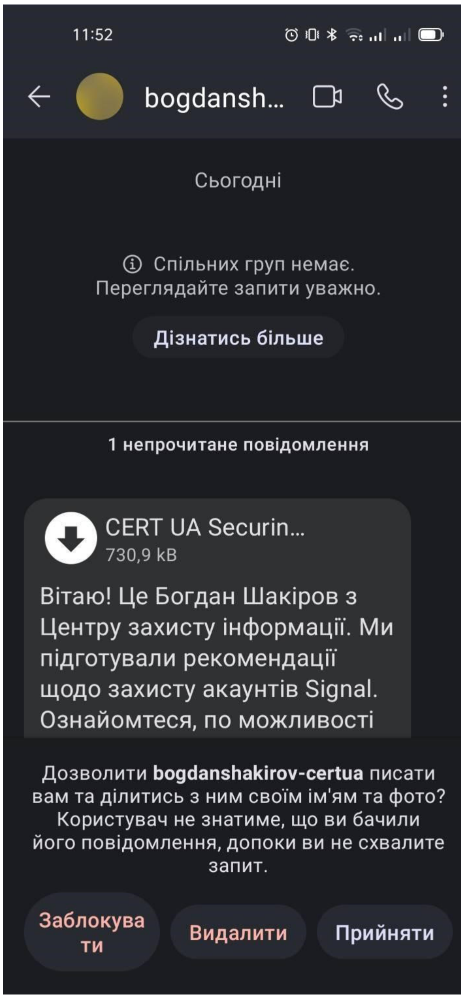
The attention of Russian hackers to attacks on mobile devices is growing steadily. This is primarily due to the convenience of messengers for quick information exchange and their popularity, including among the military. The adversary is attracting more and more developers to provide and develop tools for remote retrieval of information from mobile devices.

This is a complex job that requires a special approach to a potential victim, so we often see cases of linking a specialized System Security Plan (SSP) to legitimate products.

In one of the cases of the second half of 2023, the Russian military intelligence agency disguised the open source code of the spy program for Android - SPYNOTE (SpyMax) - as the Nettle system installer. Unfortunately, we have to state that the main delivery channel outside of Google Play, which is blocked by the SPZ, remains social engineering during communication via Signal and Telegram. In August 2023, the State Intelligence Service prepared and published material on Signal's security settings. Therefore, we encourage you to familiarize yourself with it again (https://cip.gov.ua/ua/news/chi-zlamali-signal-ta-yak-ubezpechiti-sebe-vid-rizikiv) and disable the automatic download of files to your computer.

The same instruction began to be actively distributed through the Signal messenger between representatives of the security and defense forces in the form of a PDF document, as it contained important security information. The adversary decided to use this material to implement his social engineering campaign. After 13 hours, the attackers began to distribute malicious software, allegedly on behalf of CERT-UA, under the guise of the same instructions.

"Has Signal been hacked? How to reconfigure Signal to minimize risks?"



Сьогодні

Спільних груп немає.
Переглядайте запити уважно.

1 непрочитане повідомлення

CERT UA Securin...
730,9 kB

Вітаю! Це Богдан Шакіров з Центру захисту інформації. Ми підготували рекомендації щодо захисту акаунтів Signal. Ознайомтеся, по можливості

Дозволити **bogdanshakirov-certua** писати вам та ділитись з ним своїм ім'ям та фото? Користувач не знатиме, що ви бачили його повідомлення, допоки ви не схвалите запит.

The speed of reaction and exploitation of a new vector of infection, phishing and social engineering is particularly impressive. This observation also supports the hypothesis that there is a large amount of available human resources to implement such campaigns «on the fly», since, as a rule, such attacks take much longer to plan and execute.

Virtually all targeted attacks through messengers aim to distribute SMPs for the Windows operating system, because their computer or web versions are often used for communication in messengers. Cases were recorded when attackers prepared and packaged fake software in the form of an update to a specialized complex of situational awareness on the battlefield. Bait files are often distributed as Zip or Rar archives. In particular, we detected the distribution of remote computer control malware contained in an archive exploiting a WinRAR vulnerability.

CONCLUSIONS AND FORECASTS

INCREASED FOCUS ON TARGETED COVERT CYBER RECONNAISSANCE OPERATIONS

In 2024, information assets of security and defense sector organizations, as well as the individual computers and devices of their employees and officers, will be prime targets. Targeted social engineering is becoming an increasingly effective method for delivering malware to endpoints.

ENERGY FACILITIES AND CRITICAL CIVIL INFRASTRUCTURE TO REMAIN KEY FOCUS AREAS FOR HACKERS

As kinetic strikes on critical infrastructure increase, there will likely be a corresponding rise in malicious cyber activity by affiliated organizations seeking feedback on the impacts and outcomes of these strikes. Cybercriminal groups will explore new methods for penetrating networks of critical infrastructure, including through the compromise of service providers within these sectors. Software developers will be under special scrutiny.

INCREASE IN THE NUMBER AND COMPLEXITY OF FINANCIALLY MOTIVATED CYBER ATTACKS

There is an anticipated increase in cyber attacks aimed at financial theft. These attacks will primarily target the commercial sector and involve two main strategies:

1) Infection and penetration of company networks to access banking credentials, and

2) The use of ransomware to encrypt data and subsequently demand ransom for decryption.

The property of the State Service for Special Communications and Information Protection of Ukraine

Stay connected:

https://twitter.com/SSSCIP

https://twitter.com/_CERT_UA

Requests for public information, statements, complaints and suggestions: press@cip.gov.ua

+38 (044) 281-88-25, +38 (044) 281-88-05
+38 (044) 281-88-01

Russian Cyber Operations

APT Activity Report #3

H2 2023

State Service
of Special Communications
and Information
Protection of Ukraine