RUSSIA'S CYBER TACTICS H1'2023

Lessons Learned:
Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups

Threat Research Report

September 2023

**State Service of Special Communications
and Information Protection of Ukraine**

INTRODUCTION

Cyberwarfare has evolved rapidly since 2022. Russian malicious actors are finding new and effective ways to support Russia's military operations, both on the battlefield and against civilians. This has become a signature strategy of the Russian war against Ukraine, and assessment of their tactics is highly important for the strengthening of security and protection around the globe.

This research is based on data collected by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) during its work to repel attacks by Russian hackers during the war. The SSSCIP constantly analyzes the attackers' behavior, goals, techniques, patterns, and capabilities. This information is essential for understanding the threat posed by Russia to countries around the world.

The report is a summary of the continuous interchange of lessons learned that have been shared with the international expert community, journalists, and IT professionals by SSSCIP and CERT-UA. You can also see the 2022 summary report here and subscribe to receive other analytical documents from the SSSCIP.

We are constantly evolving, and for each cyberattack described in this report, we analyze the context (timing, objectives, impact), victimology (targeted sectors, countries), main tactics, techniques, and procedures (TTPs), and, when applicable, attribution based on our internal experience, markers, and observations.

This is our 2nd analysis of the active phase of cyber component in this war. It is our attempt at taking a step back from the day-to-day events, pierce through the fog of war and reveal a bigger picture. A picture that could enable all our partners to learn and adapt to a new era of active cyber aggression.   Considering the lessons learned from monitoring shifts in Russian cyber tactics during the most active phase of cyber and kinetic operations the Cyber community gain the following value to predict/model:

1. **Future Target Selection:** Analyzing how Russian cyber tactics have evolved in terms of target selection can provide insights into potential future targets. This could include critical infrastructure, government agencies, or specific industries.

2. **Attribution and Deniability:** Understanding how Russian cyber actors have manipulated attribution and maintained deniability can help anticipate their tactics in future operations, especially in terms of false flag operations.

3. **Hybrid Warfare Strategies:** Examining how cyber tactics have been integrated into Russia's hybrid warfare strategies can provide clues about their intentions and how they might employ cyber capabilities in future geopolitical conflicts.

4. **Advanced Malware and Techniques:** Identifying the advanced malware and techniques employed by Russian cyber actors can help forecast the development of new tools and methods in future attacks.

5. Collaborative Threat Actor Networks: Studying the relationships between Russian threat actor groups and their collaboration with other state-sponsored or non-state entities can shed light on potential alliances and cooperative strategies in upcoming conflicts.

To better understand historical changes in objectives of an Russian Advanced Persistent Threat (APT) groups and their hacking teams participating in attack campaigns against Ukraine — we encourage you to read our previous report — Russia's Cyber Tactics: Lessons Learned in 2022.

"WE TAKE A HUGE PAGE OUT OF UKRAINE'S PLAYBOOK. WE'VE PROBABLY LEARNED AS MUCH FROM YOU AS YOU ARE LEARNING FROM US."

Jen Easterly
the director of the US Cybersecurity and Infrastructure Agency

"UKRAINE'S CYBER DEFENSE COMMUNITY IS SINCERELY GRATEFUL FOR THE PROVIDED SUPPORT FROM OUR ALLIES. WE ARE GRATEFUL FOR THE TECHNOLOGIES AND TOOLS THAT HAVE PROVEN INVALUABLE IN HELPING US WITHSTAND THE RUSSIAN THREAT. OUR ANALYSIS OF THE EFFECTIVENESS OF THESE TOOLS AND OUR FIRSTHAND KNOWLEDGE OF THE RUSSIAN ADVERSARY IS A CRITICAL RESOURCE FOR EVERY COUNTRY THAT IS SEEKING TO BUILD STRONGER CYBER RESILIENCE."

Viktor Zhora
Deputy Head of the State Servise of Special Comunications and information Protection of Ukraine

https://www.ft.com/content/c7038f7e-48fb-4d76-a608-96eec217a654

KEY FINDINGS AND INSIGHTS FOR THE FIRST 6 MONTHS OF 2023

The Russian invasion has triggered a notable shift in the Russian cybercriminal ecosystem that will likely have long-term implications for coordination between criminal groups and the scale of cybercrime worldwide.

The shift from hack and encrypt attacks to actual offensive espionage and influence operations will keep the bar for sophisticated instructions high for further escalation around the globe after the Ukrainian victory on the battlefield.

Key Insights:

2X GROWTH IN THE NUMBER OF INCIDENTS WHERE CERT UA WAS INVOLVED IN INVESTIGATIONS & FORENSICS

Despite all improvements implemented by Ukrainian authorities (from utilizing the most modern protection stack to many other enhancements), the number of incidents doubled in the last 6 months: from an average of 1.9 incidents per day (57 per month) in H2'22 to 4-5 per day (128 per month) in H1'23.

Russian state-controlled adversaries brace for the long stand against the West and add more people to increase the capacity and speed of the attacks.

THE CIVIC & LAW-ENFORCEMENT SECTOR IS DOMINATING ACROSS ESPIONAGE TARGETS

In the first half of 2023, we observed a sustained interest in the civic sector and law enforcement organizations. During this period, we encountered espionage operations conducted by military APTs aimed at gaining access to and extracting data from various law enforcement units in Ukraine. Their primary objectives were to identify which evidence of Russian war crimes and exercise control over potential ground-deployed spies have our law enforcement teams.

Additionally, there were more cyberattacks targeting the private sector with the intent to leverage cyber capabilities for monitoring the outcomes of their kinetic operations, including missile and drone attacks. Furthermore, these attacks were aimed at scrutinizing the plans of government contractors and supply chain members, as part of Ukraine's proactive measures for future actions.

ONCE A VICTIM — ALWAYS A VICTIM!

We've uncovered a notable trend where return attempts take precedence. State-sponsored hackers are revisiting known victims who handle and maintain the critical data needed by the Russian military. This approach grants attackers the ability to

strategize future actions and anticipate our responses. Having prior knowledge of a victim organization's network infrastructure, defensive measures, key personnel, and communication patterns provides returning attackers with a substantial advantage when it comes to exploiting organizations that have been compromised in the past.

FOCUS ON IMMEDIATE DATA EXFILTRATION

CERT-UA and our partners have optimized the collection of Threat Intelligence (TI) and reduced the Mean Time to Detect and Respond (MTTD/MTTR). Consequently, Russian threat actors now have limited time for lateral movement, prompting them to place even greater emphasis on a particular tactic: dumping documents, sometimes as many as 21,000 office documents in certain cases, along with browser credentials. They execute this tactic within the first 30 minutes of successfully infiltrating a compromised system. Subsequently, they commence disseminating their malware through various channels, such as email, to other high-profile targets, taking advantage of established trust relationships.

We've observed a shift in tactics that involve infecting systems, prioritizing victims, and gaining access to more valuable assets by replacing compromised Command and Control servers (C2s). The primary payloads still consist of office documents and HTML/ JS-based malware packaged in archives, which remain the most prevalent and favored formats.

THE MEDIA SECTOR IS UNDER CONSTANT ATTACK DURING FIRST SIX MONTHS OF 2023

Throughout the first six months of 2023, the media sector has been subjected to persistent attacks. We've been closely monitoring these attacks, which have been primarily focused on individuals and journalists. The goal behind these attacks is to gain control over media resources and accounts, intending to employ them for disinformation campaigns and influence operations. Notably, many of these attacks have been attributed to the Sandworm group, which is linked to Russia's GRU and is a key player in the broader context of Russia's hybrid warfare efforts.

https://cert.gov.ua/article/4818341

GROWING ON USAGE "LIVING OFF THE LAND"

Intruders employ either built-in system functionalities or external tools to carry out malicious actions on the system.

Malicious actors often utilize established, legitimate Windows-based software, such as WinRar (which is popular in the region), sdelete, and various other Windows utilities. This approach serves to conceal their abnormal activities, making it more challenging to detect their actions by antivirus and endpoint detection and response (AV/EDR) systems. Consequently, they can conduct destructive operations without triggering anomalies in AV/EDR monitoring.

https://cert.gov.ua/article/4501891

HACKING AND EXPLOITING OPEN-SOURCE MAIL SYSTEMS

We observe a trend from H2'2022 that threat actors actively develop and distribute exploits against open-source mail systems for known CVEs. Examples: Zimbra and Roundcube

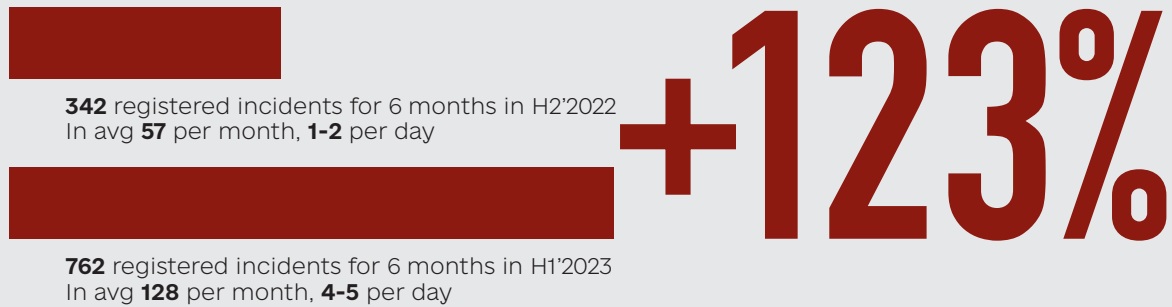**THE ENERGY SECTOR CONTINUES TO BE UNDER ATTACK**

The key problem that leads to successful penetration is the lack of proper isolation between Operational technology (OT) and corporate networks.

Amount of attacks in 2023 dropped after the end of the drone and missile attacks on the civilian energy infrastructure. Still, terrorist-style pressure on the international community over the Zaporizhzhya nuclear plant continued, and key Russian APT groups were tasked to collect information about Ukrainian plans to protect the station and preparedness for the worst-case scenario.
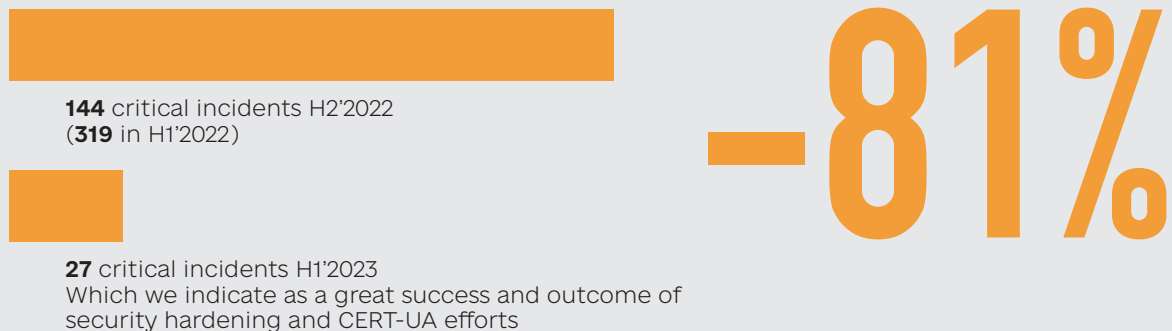
TRENDS AND EMERGING ISSUES H2'2023

This dataset is assembled based on incidents analytics from the CERT-UA unit, without cases registered by SSSCIP SOC.

GROWTH IN THE REGISTERED INCIDENTS RATE IN H1'2023

+123%

342 registered incidents for 6 months in H2'2022
In avg **57** per month, **1-2** per day

762 registered incidents for 6 months in H1'2023
In avg **128** per month, **4-5** per day

DECREASE IN THE RATE OF CRITICAL INCIDENTS IN H1'2023

–81%

144 critical incidents H2'2022
(**319** in H1'2022)

27 critical incidents H1'2023
Which we indicate as a great success and outcome of security hardening and CERT-UA efforts

DECREASE IN THE RATE OF HIGH AND CRITICAL INCIDENTS IN H1'2023

–46%

339 high and critical incidents happened in H2'2022 and **683** happened in H1'2022

183 high and critical incidents happened in H1'2023
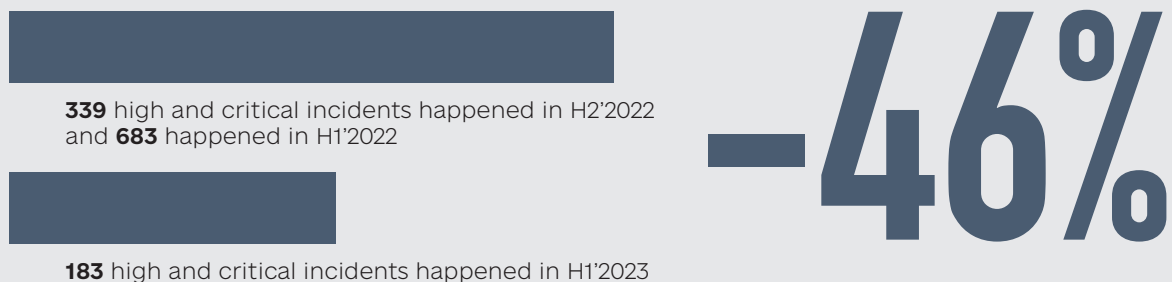
DECREASE IN THE RATE OF MALWARE DISTRIBUTION CASES VIA EMAIL
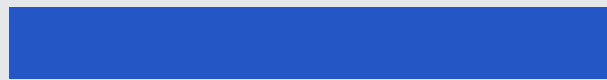
-52,41**%**

290 in H2'2022 where malware
was dominating

138 cases in H1'2023 where phishing was dominating
compared to malware distribution attempts

**DECREASE IN THE RATE OF ATTACKS AGAINST THE ENERGY
SECTOR AND 50% DROP IN CRITICAL INCIDENTS CASES**
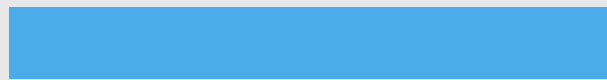
-61%

141 incidents in H2'2022
(**16** critical incidents with registered impact)

55 incidents in H1'2023
(**8** critical incidents with registered impact)

DECREASE IN THE RATE OF CASES WITH IMPACT IN H1'2023

-48%

30 destructive attempts in H2'2022
518 impactful operations in H2'2022

34 destructive attempts in H1'2023
267 impactful operations in H1'2023

From the data presented above, it's evident that the number of critical incidents has notably decreased. Moreover, the ratio of high-level to critical-level incidents has improved. The attackers appear to be using less sophisticated tactics, employing a "spray and pray" approach, while Ukraine's defense of its infrastructure has markedly improved compared to six months ago.

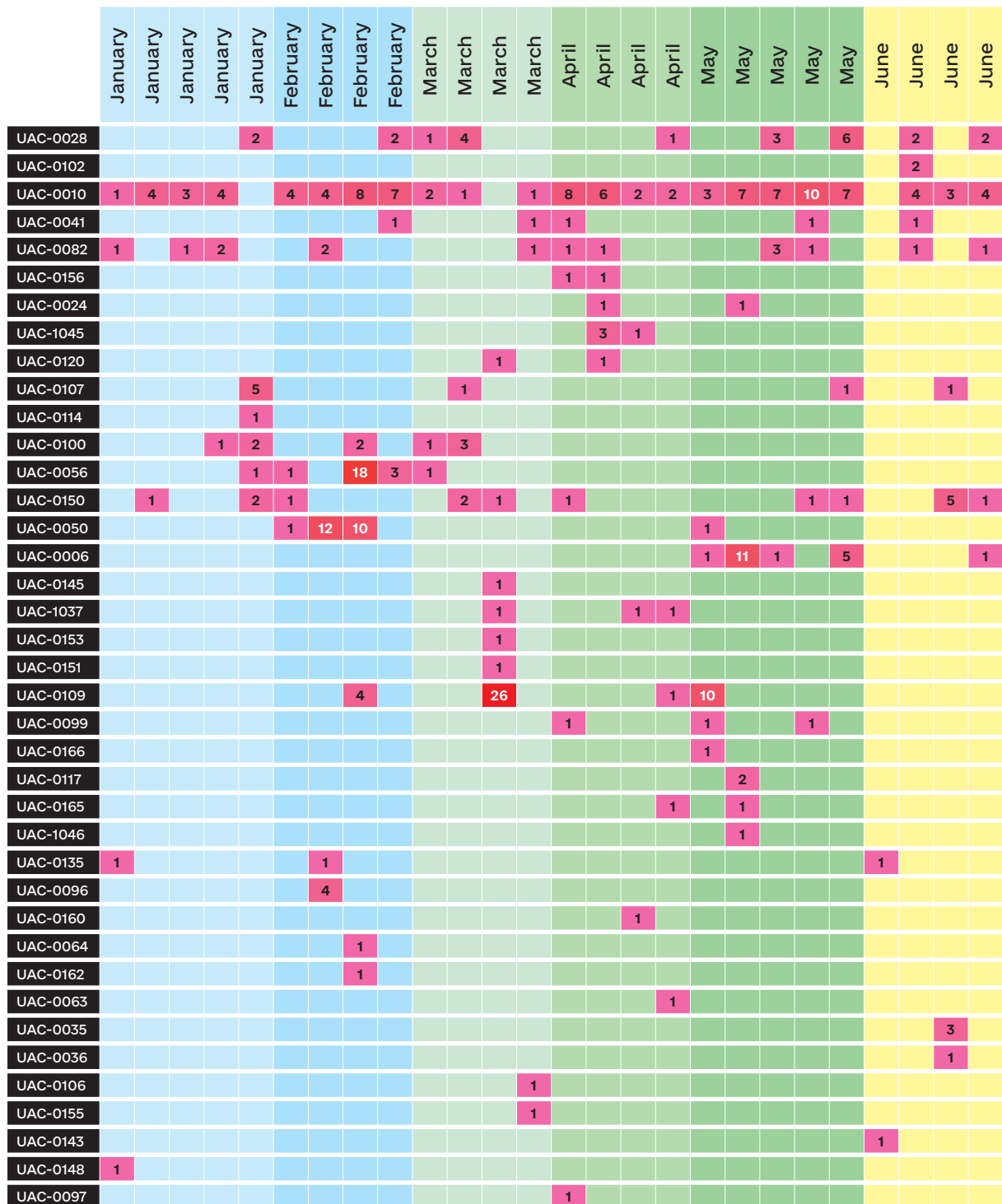Additionally, a new surge in phishing attacks has taken precedence over successful malware infections. Although the attackers are becoming more aggressive, Ukraine's defenses are also bolstering. While it's becoming increasingly challenging for them to have a substantial impact, they have still managed to achieve some success in cases involving attempts at wiping data or other destructive operations.

TIMELINE

The figure below shows the pattern of all threat actors and their ability to conduct specific amounts of cyber operations over time (distribution by weeks). We discovered that every APT team is unique and relies on its talent pool, TTPs, and victimology — so each could perform a limited amount of operations and lateral movement and maintain access to specific targets (also within a limited timeline before being discovered).

THREAT ACTORS DISCOVERIES DEMONSTRATE PATTERN THAT THREAT ACTORS DEPENDING ON TEAM SIZE HAVE CAPACITY TO RUN LIMITED AMOUNT OF NEW OPERATIONS UAC-0010, UAC-0028, UAC-0102 , UAC-0041, UAC-0082...
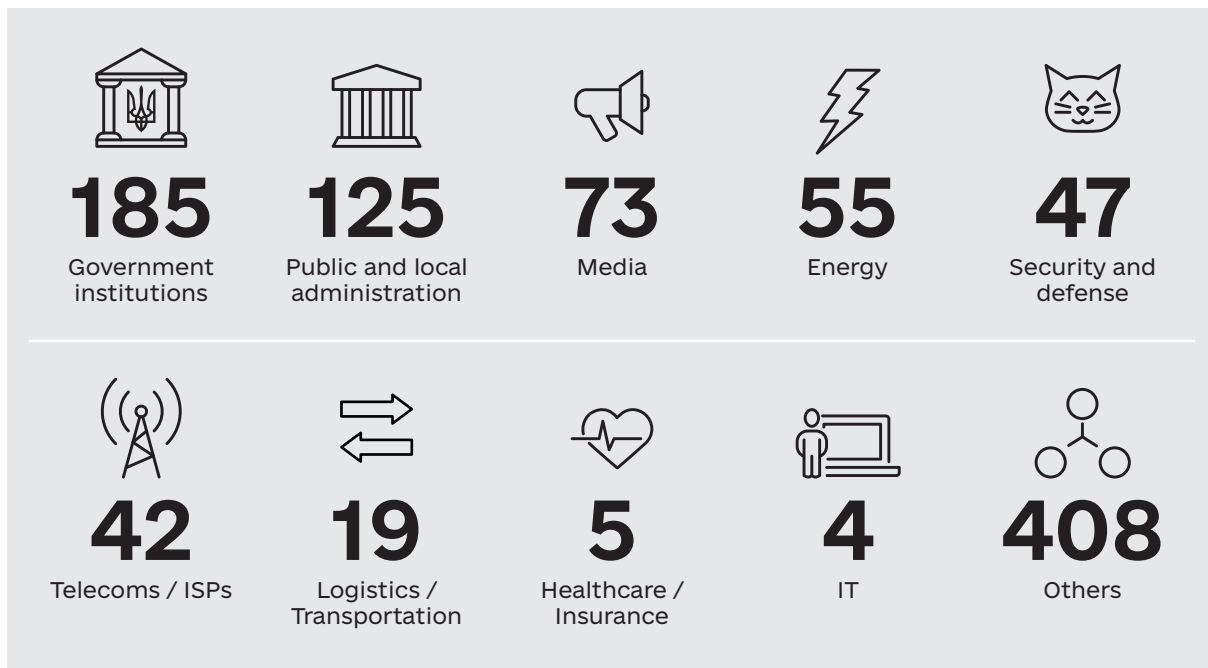
Actor	Jan	Jan	Jan	Jan	Jan	Feb	Feb	Feb	Feb	Mar	Mar	Mar	Mar	Apr	Apr	Apr	Apr	May	May	May	May	May	Jun	Jun	Jun	Jun
UAC-0028				2				2		1	4						1			3		6		2		2
UAC-0102																							2			
UAC-0010	1	4	3	4		4	4	8	7	2	1		1	8	6	2	2	3	7	7	10	7		4	3	4
UAC-0041									1	1	1										1			1		
UAC-0082	1		1	2			2			1	1	1								3	1			1		1
UAC-0156														1	1											
UAC-0024															1				1							
UAC-1045														3	1											
UAC-0120												1			1											
UAC-0107				5						1												1		1		
UAC-0114						1																				
UAC-0100			1	2			2			1	3															
UAC-0056						1	1	18	3	1																
UAC-0150		1				2	1			2	1		1							1	1				5	1
UAC-0050						1	12	10											1							
UAC-0006																		1	11	1		5				1
UAC-0145										1																
UAC-1037										1						1	1									
UAC-0153										1																
UAC-0151										1																
UAC-0109								4			26						1	10								
UAC-0099														1					1		1					
UAC-0166																			1							
UAC-0117																				2						
UAC-0165																	1			1						
UAC-1046																			1							
UAC-0135	1						1																1			
UAC-0096							4																			
UAC-0160																1										
UAC-0064								1																		
UAC-0162								1																		
UAC-0063																1										
UAC-0035																									3	
UAC-0036																									1	
UAC-0106												1														
UAC-0155												1														
UAC-0143																							1			
UAC-0148	1																									
UAC-0097												1														

HERE ARE SOME KEY TAKEAWAYS:

1. **Operation Frequency:** An analysis of the intervals between successful penetrations or initial footholds reveals that most APT groups typically conduct around one operation per month. However, the capacity to handle a higher number of operations varies among groups, depending on their size and talent pool. Notably, Gamaredon doubled its performance in H1'2023 despite facing our organizational efforts, enhancements, and countermeasures.

2. **Target Switching:** When an APT group is discovered, it usually requires some time to transition to a new target before detection. This pattern is observable in the provided timeline.

3. **Opportunistic Approach:** The principle of "once a target, always a target" prevails. There are always plenty of potential targets, and malicious actors often adopt an opportunistic approach to showcase their impact, maintain a high profile, and emphasize their capabilities in the cyber landscape.

4. **Strategic Targets Limited:** Despite numerous targets, the number of strategic and valuable IT/Cyber targets crucial for supporting Russian military operations in Ukraine is relatively limited. Attackers, therefore, tend to keep a low profile after being discovered and may reuse their knowledge of an organization's internals to regain access or find alternative entry points by exploiting trust and people's behavior (e.g., from emails) and the IT administrator environment. Sometimes, even password wallets are exploited.

5. **Security Measures:** To enhance security, critical steps include disabling executables like mshta.exe, wscript.exe, cscript.exe, and powershell.exe across all organizational machines unless there is a specific need to whitelist them for particular organizational units.

WHERE & WHY: TARGETED SECTORS

Based on our analysis of cases, we present the distribution of cases across various industry segments. The "Other" segment encompasses commercial and civic organizations that do not fall into the specified categories and has the highest number of cases (408).

From our findings, it is evident that the following five sectors have consistently been the primary targets of malicious actors: numerous private companies in the Media & Telecommunications sector, as well as organizations in the Public and Local Administration, Security and Defense, and Government Institutions sectors. Notably, there is a particular emphasis on targeting entities within the Public and Local Administration subcategory of the Government sector.

185 Government institutions

125 Public and local administration

73 Media

55 Energy

47 Security and defense

42 Telecoms / ISPs

19 Logistics / Transportation

5 Healthcare / Insurance

4 IT

408 Others

In the first half of 2023, FSB, GRU, and SVR continued the trend of increasing espionage operations focused on intelligence gathering. Concurrently, some groups maintained their penchant for destructive operations. APT groups frequently revisited their previous targets, capitalizing on their familiarity with the victims' infrastructure and recognizing the significance of these targets for both intelligence collection and destructive purposes.

Based on their observed behavior, which includes persistent espionage attempts, it is reasonable to suggest that their primary mission, as directed by military commanders, was to ascertain the extent of information gathered by Ukrainian Law Enforcement units. This information likely includes evidence, intelligence, and arguments that could be used for criminal proceedings against spies, specific individuals, institutions, or organizations in Russia, potentially leading to sanctions or other actions.

It appears that their objective is to acquire data with the intention of gaining insights into:

- Better situation awareness and cases coming to the court
- What information Security Service of Ukraine and other law enforcement organizations managed to collect as an evidence base for further arrests
- Plans and evidence Ukrainian law enforcement organizations assemble for international court cases

- List of important witnesses and stakeholders for further war criminal cases
- Who was arrested, and how to help these individuals avoid prosecution and move them back to Russia

They utilize this data for counter-intelligence operations and data attribution.

- PII and Personalities that become known to the Ukrainian law enforcement agencies when officers ask court and prosecutors for permission to arrest or interrogate a person

- Which elite soldiers and officers were captured during the siege and could/couldn't be exchanged

The concept of "once a victim, always a victim" underscores how threat actors exhibit a persistent pattern of revisiting targets the threat actors have previously compromised is driven by their ability to leverage the information they've already acquired and their familiarity with the targeted individuals and email accounts.

By revisiting these previously compromised targets, threat actors aim to exploit the knowledge they've gained about the organization's internal workings, personnel, communication channels, and vulnerabilities. They recognize that this acquired intelligence can provide them with a significant advantage in orchestrating future cyberattacks. Consequently, they continue to target the same individuals, email accounts, or even specific departments within the organization, for the purpose of maintaining access, extracting valuable data, and furthering their malicious objectives.

This "once a victim, always a victim" strategy underscores the ongoing and evolving threat that organizations face from cyber adversaries who exploit their knowledge to maximize the impact of their attacks, highlighting the need for robust and adaptive cybersecurity measures to counter such persistent threats.
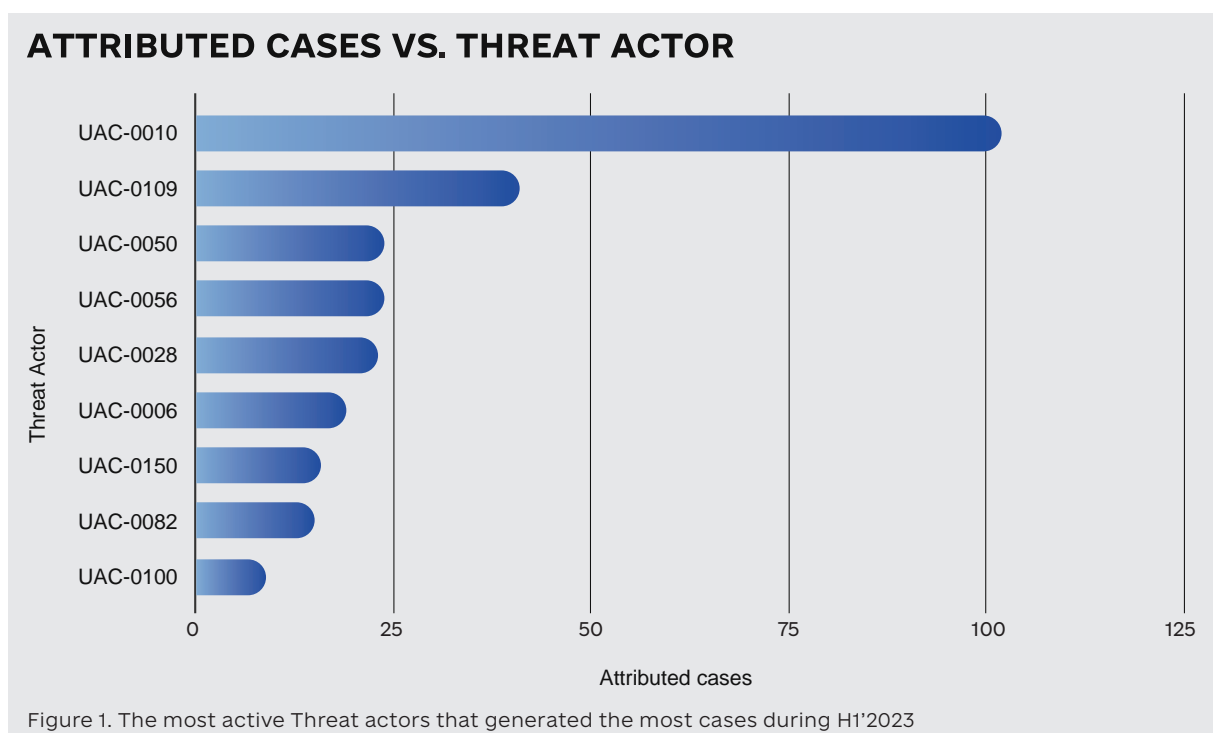
REMARKABLE CASES

Targeting Ukrainian media agencies	On 17 January 2023, CyberArmyofRussia Reborn released data allegedly exfiltrated from Ukrinform, Ukrainian news agency, in what they purported to be a hack-and-leak operation.
	Hacktivists claimed they had 'burned' the victim organization'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 idSwipe.
	We suggest this cyberattack was carried out by the 'UAC-0082 (Sandworm, which is associated with GRU's Main Center of Special Technologies.) group.
	Primary objective: to compromise Ukraine's state information agency and provide ground for better effectiveness of the Russian-sponsored propaganda.
	https://cert.gov.ua/article/4818341

Hack-and-leak against insurance, medical/healthcare organizations	Russian hacker volunteers managed to hack into key insurance companies, and medical/healthcare organizations with dumping personally identifiable information with phone number details, lab analysis outcomes, COVID test results.
	Primary objective: to collect data on Ukrainian citizens, which will enable the following cyber or information operations
Attacks against the energy sector and nuclear plant	The Ukrainian energy sector remains a priority target, well known by attackers who kept their presence on some targets undiscovered for 9 months. There was one case of disruption operation.
	Judging by the registered activity and victimology during April-May, key APTs were tasked to run a campaign of intel collection about Ukrainian preparedness and plans regarding Zaporizhzhya Nuclear Power Plant (ZNPP).
	Suggested primary objective: to support terrorist-type operations on the threat of a nuclear event at ZNPP.

WHO & HOW:

We recorded claimed attacks by at least 23 Russia-led cyber-terrorist hacking groups. They all serve an offensive military goal and attack an independent state's public and private sectors. We provide an analysis of the activity of the most dangerous and capable groups: Gamaredon (controlled by FSB), Sandworm (controlled by GRU), and "independent hacktivists" that turned out to be an umbrella for state-controlled criminals).

ATTRIBUTED CASES VS. THREAT ACTOR

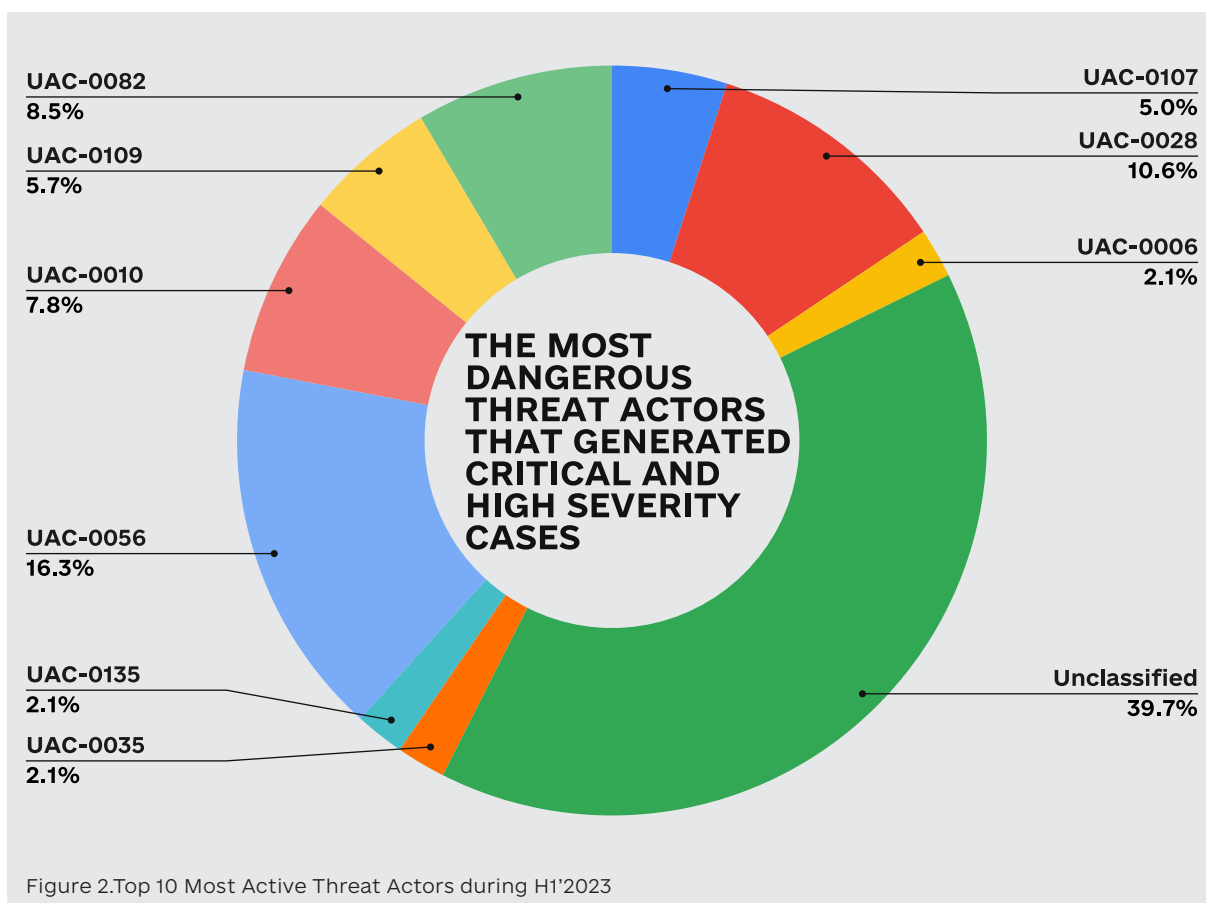Figure 1. The most active Threat actors that generated the most cases during H1'2023

In 2023, the most active groups were UAC-0010 (Gamaredon/FSB), UAC-0056 (GRU), UAC-0028 (APT28/GRU), UAC-0082 (Sandworm/GRU), UAC-0144 / UAC-0024 / UAC-0003 (Turla), UAC-0029 (APT29/SVR), UAC-0109 (Zarya), UAC-0100, UAC-0106 (XakNet), UAC-0107 (CyberArmyofRussia). The recorded cyberattacks had been attributed to these APT groups.

We analyzed the context (timing, objectives, impact), victimology (targeted sectors, countries), main tactics, techniques, and procedures (TTPs), and, when applicable, attribution based on our internal experience, markers, and observations.

When we examine the distribution of incidents and threat actors (presented above) and focus on the most significant and perilous ones (illustrated in the image below), it becomes evident that the GRU teams identified as UAC-0056 (Ember Bear), UAC-0028 (APT-28), and UAC-0082 (Sandworm) play a crucial role by generating 50 serious incidents.
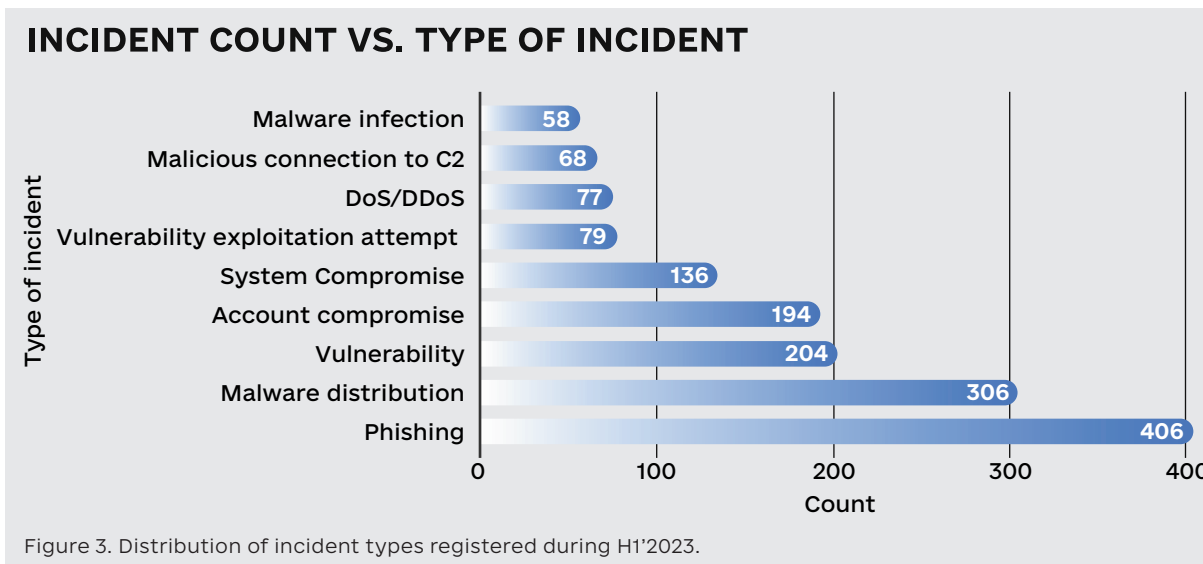
In contrast, the FSB team — UAC-0010 (Gamaredon) — only contributed to 11 critical or high-severity incidents (as presented below) out of a total of 103 incidents associated with their TTPs and observed during the monitoring period in the scope of organizations contacted or protected by us.

UAC-0082 8.5%
UAC-0109 5.7%
UAC-0010 7.8%
UAC-0056 16.3%
UAC-0135 2.1%
UAC-0035 2.1%

THE MOST DANGEROUS THREAT ACTORS THAT GENERATED CRITICAL AND HIGH SEVERITY CASES

UAC-0107 5.0%
UAC-0028 10.6%
UAC-0006 2.1%
Unclassified 39.7%

Figure 2.Top 10 Most Active Threat Actors during H1'2023

Based on our analysis it seems like FSB cyber unit Gamaredon managed to significantly increase the total amount of operations and cases registered by CERT (from 128 for the full 2022 to 103 just in H1'2023), but not all of them were that successful and converted into high severity issues.

When examining the Figure 3 — the prevalence of techniques recorded by CERT-UA, it becomes apparent that phishing was the most prominent tactic employed by malicious actors in H1'2023. However, malware infections involving command-and-control (C2) connections and breaches through known exploitable vulnerabilities or account compromises stand out as favored and highly effective strategies across the board.
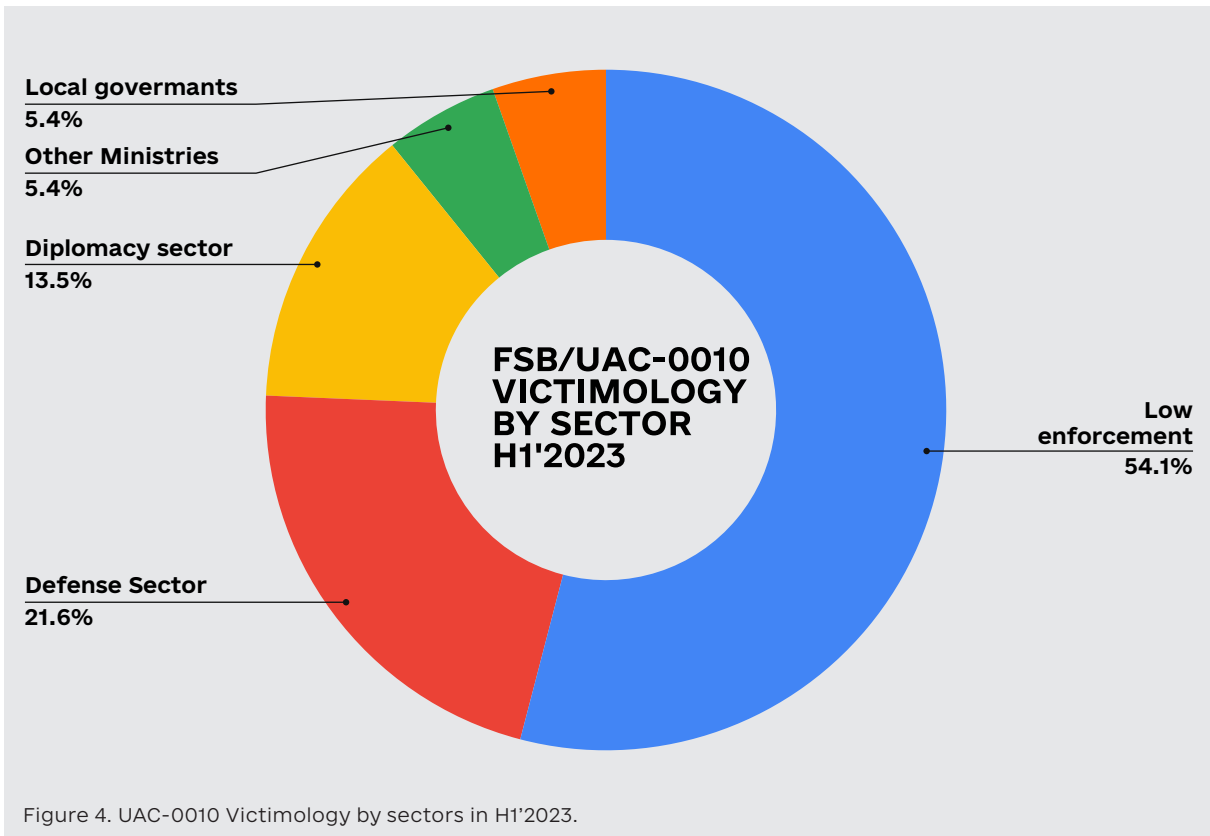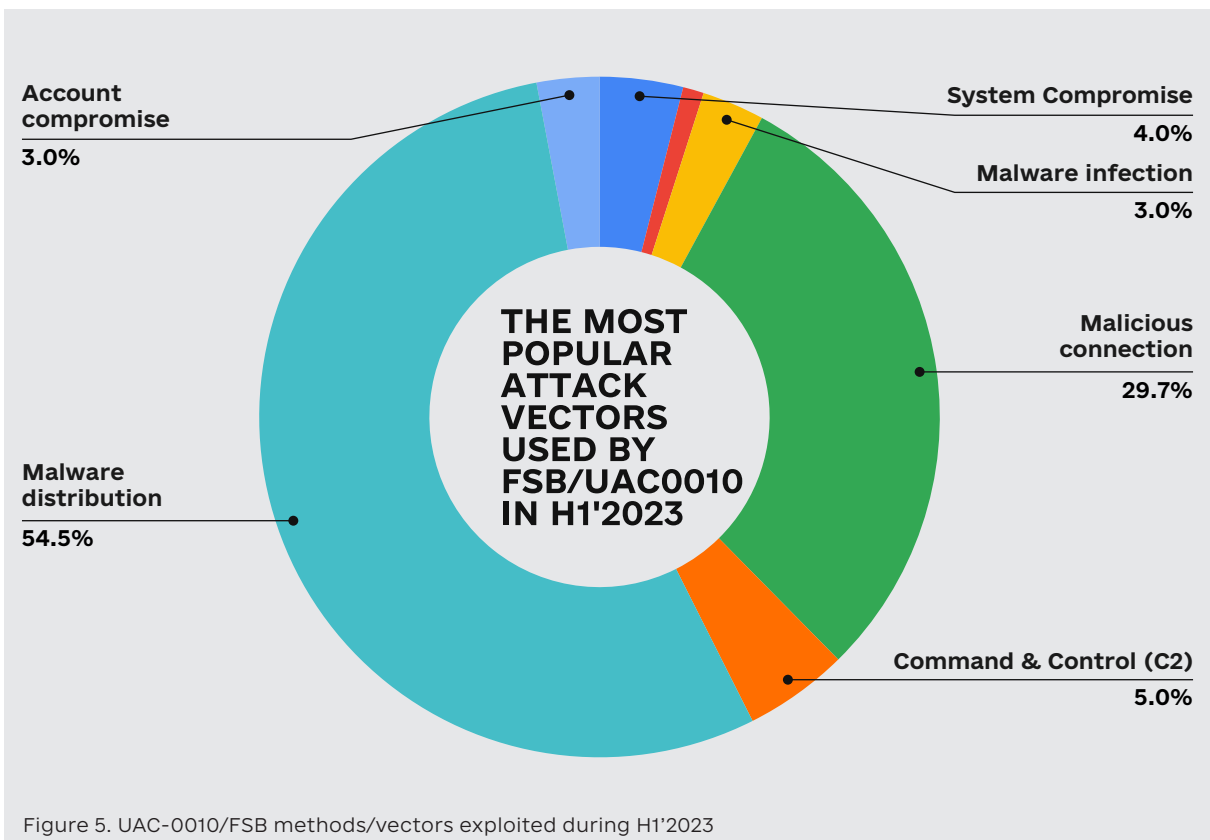
INCIDENT COUNT VS. TYPE OF INCIDENT

Type of incident	Count
Malware infection	58
Malicious connection to C2	68
DoS/DDoS	77
Vulnerability exploitation attempt	79
System Compromise	136
Account compromise	194
Vulnerability	204
Malware distribution	306
Phishing	406

Figure 3. Distribution of incident types registered during H1'2023.

FSB. UAC-0010 Gamaredon

A closer examination of the recorded incidents, as outlined in the general Threat Actors Analytics above, reveals that UAC-0010 exhibited a notable performance increase. The number of registered cases for this group rose from 76 cases in H2'2022 to 103 cases in H1'2023. This substantial growth in the volume of cyber operations, accompanied by shifts in focus and tactics compared to previous periods, can be attributed to several factors. These include an expansion in manpower and team capacity, the infusion of new talent from Russia's abundant pool of skilled individuals, and the mobilization of IT professionals from the private sector to serve in the military.

In H1'2023 UAC-0010 demonstrated explicit interest in all the law enforcement directions (54.1% of their cases), also expressing persistent interest in all organizations related to Ukrainian Defense Forces. This group has a huge human resource and applies primitive methods that nonetheless are quite resultative.

Analysis of UAC-0010 team activity by timeline and a number of showcasing that their increased number of incidents (comparing to H1 and even more to H2'2022) and regularity of discoveries in different Ukrainian organizations/networks is achieved through adding more man-power, new talents to support their operations. We suggest that old operators return to well-known targets while newcomers are working to penetrate new victims (access brokers). They experience trouble persisting and maintaining access because of Ukrainian cyber defenders activities, so they have to accelerate with getting in and out, and not burn the victims where they successfully maintain access.

FSB/UAC-0010 VICTIMOLOGY BY SECTOR H1'2023

- Local govermants **5.4%**
- Other Ministries **5.4%**
- Diplomacy sector **13.5%**
- Defense Sector **21.6%**
- Low enforcement **54.1%**

Figure 4. UAC-0010 Victimology by sectors in H1'2023.

The figure below presents an analysis of methods registered across SOC and CERT cases used by UAC-0010 during its campaigns. Malware distribution is the dominating tactic for this group, while other groups heavily rely on phishing campaigns.

THE MOST POPULAR ATTACK VECTORS USED BY FSB/UAC0010 IN H1'2023

- Account compromise **3.0%**
- Malware distribution **54.5%**
- System Compromise **4.0%**
- Malware infection **3.0%**
- Malicious connection **29.7%**
- Command & Control (C2) **5.0%**

Figure 5. UAC-0010/FSB methods/vectors exploited during H1'2023

UAC-0010 TEAM ACTIVITY VS. WEEKS/MONTHS
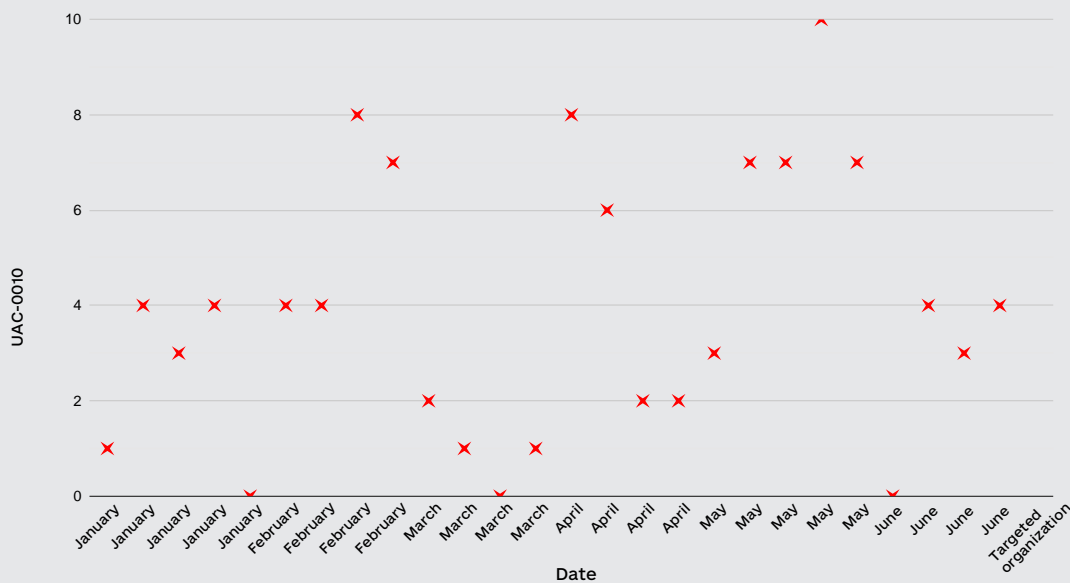
Figure 6 illustrates the UAC-0010/Gamaredon campaigns and activities throughout H1'2023, providing a visual representation of the time intervals in weeks between the discovery of this threat actor on various victims. This representation effectively portrays the velocity and speed at which their team penetrates both new and previously targeted entities.

Still, to have a more precise picture of truly dangerous intrusions being discovered, we build the following analytics which confirms our guess that for more serious operations, threat actors require more time to run a campaign and get a foothold. In a range, as we see, it is 20-30 days for one initial access operation or return attempt.

To enhance the effect of their hacking campaigns even more, starting from April 2023, hackers are using tactics of compromising news agencies and Facebook pages where they publish provocative and controversial information, blaming CERT-UA for the breach and losing competition.

During the war, there takes place an obvious "merging" between criminal hacker groups and the aggressor state. There are numerous cases of using a toolset of Trickbot/Conti hacker groups for performing attacks toward objects of critical infrastructure, in particular energy infrastructure. Another example is the activity of the Tropical Scorpius group utilizing a RomCom backdoor during their attacks.

GRU. Sandworm UAC-0082/UAC-0165

The media is a target for military hackers from the Main Intelligence Directorate of the Ministry of Defense of the Russian Federation, despite being a civilian target. From the perspective of the Russian command, it is critical for military and informational operations, so the media will continue to be the focus of all Russian hackers in uniform. Since this hybrid warfare is characterized by the use of hacking tools for influence operations, it is a hallmark of the Russian Federation.

This marks a continuation of the Russian approach aimed at impacting civilian infrastructure outside of traditional battlegrounds. This approach involves the use of aggressive propaganda as well as missile and drone strikes targeting crucial energy and agriculture export facilities. This strategic outlook is mirrored in the objectives assigned to military hackers, as a significant portion of their cyberattacks is directed at essential civilian services such as media, communication networks, and the public sector.

GRU UAC-0082 ATTACKED SEGMENTS H1'2023

- Others — 6.7%
- Local municipalities — 13.3%
- Govermant — 13.3%
- Private businesses — 13.3%
- Energy sector — 6.7%
- Telco & ISP — 13.3%
- Media — 33.3%
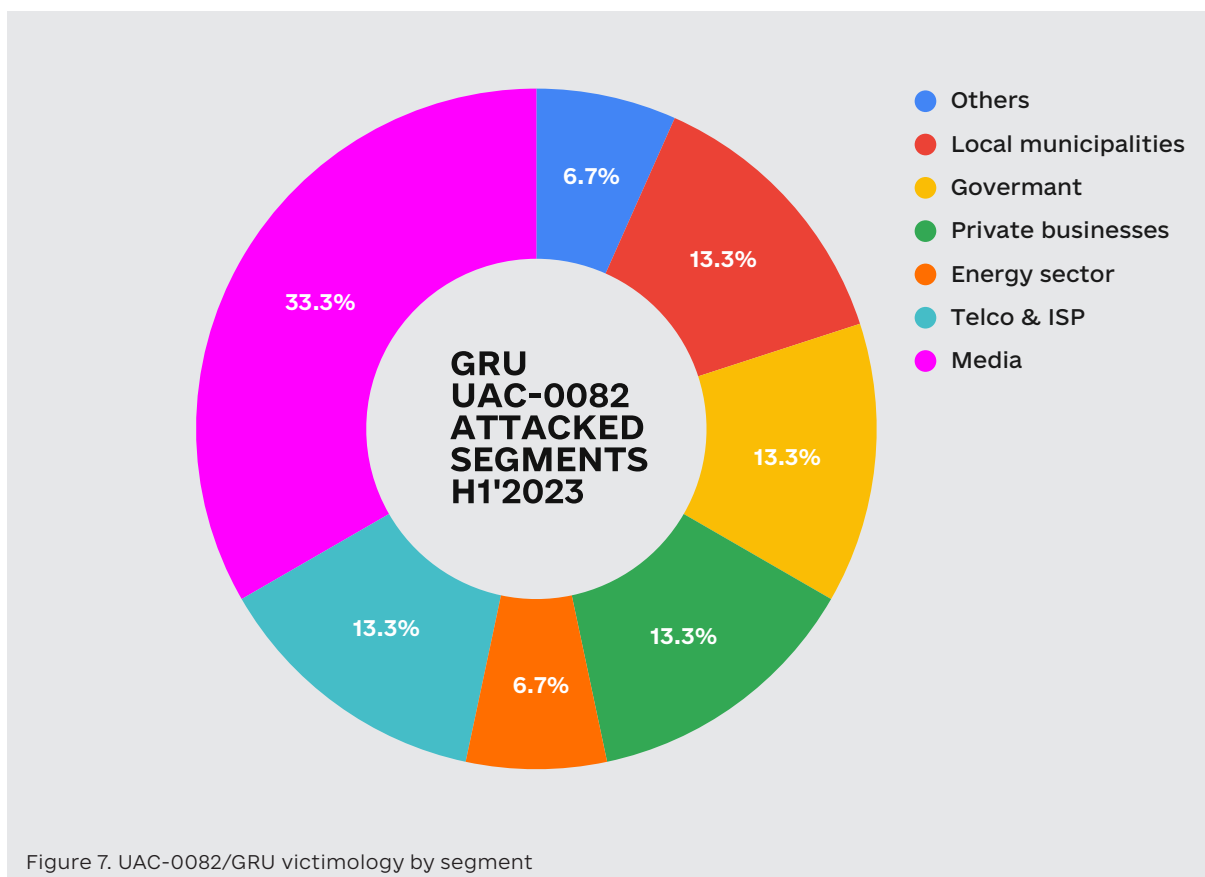
Figure 7. UAC-0082/GRU victimology by segment

They also actively hunt after military personnel who have access to some military platforms

New OpSec Trend

A vast majority of destructive attacks have been performed by the Sandworm group managed by GRU.

In order to make these events public, such attacks have been followed by leaks of documents, schemas, and technical documentation in Telegram channels de-facto controlled by the group mimicking "independent volunteers".

Previously, the Sandworm group used @CyberArmyofRussia_Reborn Telegram channel to publish the results of their activity.

However, starting from the 25th of April 2023, they are using a @solntsepekZ Telegram channel instead for better OpSec.

The most related story — https://cert.gov.ua/article/3718487

Since the full-scale invasion, in most Sandworm incidents, the final intention of this APT is to carry out destructive cyberattacks, which involve wiping servers, crashing virtualization systems, disabling active network equipment, wiping data storage systems, and encrypting endpoints. During the last 6 months, they developed new variants of malicious software (there are more than 10 new samples) using legitimate utilities (like SDelete, WinRaR) or built-in features of systems (for example NAS storages).

Energy sector. In some cases, timely revealed hackers' intentions to perform cyber attacks on energy facilities prove the fact of using specific tactics of multi-phase influence: power outage, destruction of substations control, destruction of underlayer telecommunication substation (modems), smashing employees workstation, and wiping server equipment.

The complexity of attacks against the energy sector was significantly raised, as they knew these networks and companies (since 2014) are built similarly and have the same weak spots or defense best practices, which allowed them to better prepare the operations.

Story

In one of the investigations on one of the energy objects, we managed to collect evidence of initial access to that network dated by mid-2021, which links to a part of a broader campaign of similar cases. This indicates the planning of intrusion, and proactive cyber operations, including hacker groups involvement in conventional m

ilitary operations with the aim of enhancing their effect and performing a negative influence on industrial control systems, etc.

The plan of that influence operation utilized dependencies on electricity of the telecom, transportation, banking, and other organizations from the critical infrastructure list. Malicious actors were utilizing gained accesses depending on situation development in conventional operations.

"Hacktivists"
Killnet, HackNet, Zarya, NoName057, Anonymous Russia

We recorded the most attacks from Killnet, NoName057(16), XakNet Team, Anonymous Russia, and Cyber Army of Russia.

- These hacking groups actually collaborate. They targeted the same or similar targets and reposted each other's content on social media.

- Although their claims rarely describe the nature of the supposed cyberattack.

During H1'2023, we noticed a rise in information operations with a cyber component. This category ranged from coordinated inauthentic behavior on social media pushing narratives associated

with Russia's war on Ukraine to hack-and-leaks from supposed hacktivists who attempted to cause reputational damage to the victims.

Threat actors published supposedly exfiltrated data (including hack-and-leak) 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

New Trend

Also, they are now combining hack-and-leak with publishing fake news through compromised media resources to reach a wider audience.

Relevant cases:

https://cip.gov.ua/ua/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo

https://cip.gov.ua/ua/news/rosiiski-khakeri-namagayutsya-diskredituvati-uryadovu-komandu-reaguvannya-na-komp-yuterni-nadzvichaini-podiyi-cert-ua

References

We recommend checking the following materials:

1. https://cert.gov.ua/article/5213167
2. https://cert.gov.ua/article/5160737
3. https://cert.gov.ua/article/4905829
4. https://cert.gov.ua/article/4905718
5. https://cip.gov.ua/ua/news/cert-ua-zavdyaki-spivpraci-z-recorded-future-viyaviv-shpigunsku-kampaniyu-grupi-apt28-bluedelta-proti-ukrayinskikh-organizacii
6. https://cert.gov.ua/article/3947787

Our expectations and forecasts, considering the existing context, observations, and lessons learned.

GROWTH OF A SOPHISTICATED SUPPLY CHAIN

We expect that companies developing software for critical infrastructure and the military would be actively targeted in a long-term perspective. IT managers have to carefully watch every commit and protect their Intellectual property software by obfuscation and advanced authentication.

EVEN BIGGER SHIFT TO ESPIONAGE

We anticipate a deceleration in lateral movement within the network and a shift towards greater user impersonation. Malicious actors are becoming increasingly cautious about avoiding detection, prompting them to refrain from deploying custom malware that could raise alarms. Instead, they are leaning towards utilizing legitimate tools and processes, blending into the environment more effectively to avoid drawing attention to their activities.

MORE COMPLEX OF ATTACKS AND TOOLSET

Our forecast indicates that threat actors are intensifying the complexity of their attack chains. They are leveraging advanced techniques to create more intricate attack scenarios. This includes the development and deployment of highly sophisticated malware that boasts a wider distribution, capable of targeting various operating systems and even exhibiting cross-platform capabilities. This escalation in attack sophistication highlights the need for organizations to continually enhance their cybersecurity defenses to stay ahead of evolving threats.

MORE PEOPLE IN RUSSIAN CYBER CRIMINAL AND MILITARY

We are already observing the rise of successful operations and distribution campaigns. Russia actively engages young people sharing Western materials to train and educate them, preparing a new generation of patriotically motivated hackers who could easily become cyber-criminal threat actors/ransomware operators in the future.

If you wish to discover more,
please subscribe here
https://share-eu1.hsforms.com/1SNVq2857Q82uZWUfbxCyhw2b2xj0

Media contact center
press@cip.gov.ua

The property of the

State Service of Special Communications and Information Protection of Ukraine