Russia's Cyber Tactics: Lessons Learned 2022

State Service
of Special Communications
and Information
Protection of Ukraine

TABLE OF CONTENTS

**IN THIS REPORT,
YOU'D FIND ANSWERS
TO THE FOLLOWING:**

1. Major targets of russian hackers
2. Is there coordination between hacktivists and government APT groups?
3. Espionage operations vs Influence operations
4. Discoveries on tasking
5. How to get there
6. Adversaries
7. Recommendations

FOREWORD

2,194

incidents manually processed by CERT-UA in 2022

1,148

critical and high-level incidents investigated and mitigated by CERT-UA in 2022

Hackers, who attack Ukrainian civil, military and government organizations, as well as russian hacktivists/cyber criminals, are real people, who live their lives, who have first and last names, who have families, who travel. They have bosses with their specific cultures and management approaches, they have old habits, favorite tools, and techniques they use to simplify their lives. In this report, we attempted to explain our observations of the human context. Since 2014, Ukraine has been a testing ground for russia's cyber capabilities, providing a possibility for others to observe and learn about their tactics, techniques, and procedures. We had many serious breaches that helped the world to better prepare for future attacks.

During 2022, we demonstrated great resilience with the help of our partners, but we have many new lessons to learn from events that happened over the last year, which we would like to share with our friends and the whole cybersecurity community.

Understanding of those events provides insight into the shifting dynamics of adversary tactics, which is critical for staying ahead of today's threats. Attacks are growing more destructive, causing mass disruption in all aspects of our daily lives. This is the challenge we've accepted and a fight that we will win together.

I hope you find this report informative and that it gives you the same insights that I got: to be better prepared to stop adversaries from destroying our way of life and to provide strategic recommendations to organizations worldwide.

Victor Zhora
Deputy Chairman,
State Service of Special Communications
and Information Protection of Ukraine

EXECUTIVE SUMMARY

This report is addressed to those whose activities are somehow associated with cybersecurity: information security specialists in all the sectors of the Ukrainian critical infrastructure, those whose companies can be connected with the services provided to the critical infrastructure and critical information infrastructure facilities of Ukraine, decision-makers for security of their facilities (including cybersecurity), in particular top managers of the central executive authorities of Ukraine, as well as our partners all over the world since last year we saw global active expansion of russia's cyber aggression.

This report contains information on the activity of russian hackers in Ukraine during the second half of 2022 and compares it with their activity during the first half, analyzes the purposes and motives of russian hackers as well as the tools they use.

All the attacks on our country's infrastructure are organized by the specified groups with specific purposes; if we are well aware of the enemy's motivation and tools, we can forecast quite confidently which segments and sectors are most threatened by russian hackers. The purpose of this report is to analyze these connections.

During the second half of 2022, we recorded a shift in the focus of russian hackers from the media and telecommunications industries, which were among the main targets at the beginning of the war, to the energy system, which also turned into one of the principal targets of russia's missile attacks since October last year.

Moreover, the purposes of russian hackers have changed as well, from a large quantity of attacks aimed at disruption to spying and data theft. This indicates that the russian authorities are aware of the importance of the cyber component for their military operations.

Following the study, we recommend to the companies and organizations of potential interest to russian hackers to pay more attention to protection against attacks via their partners and suppliers, protection of web resources, vulnerability control and phishing.

Throughout our engagement, CERT-UA has observed that russia-aligned cyber operations use several common tactics, techniques, and procedures (TTPs) to execute their intrusions. We have been able to turn these observations into actionable guidance for network defenders and security teams. Also, we would like to share the lessons learned and make our hypotheses available for discussion in the wider information security community.

WHAT

...was happening in H2 2022

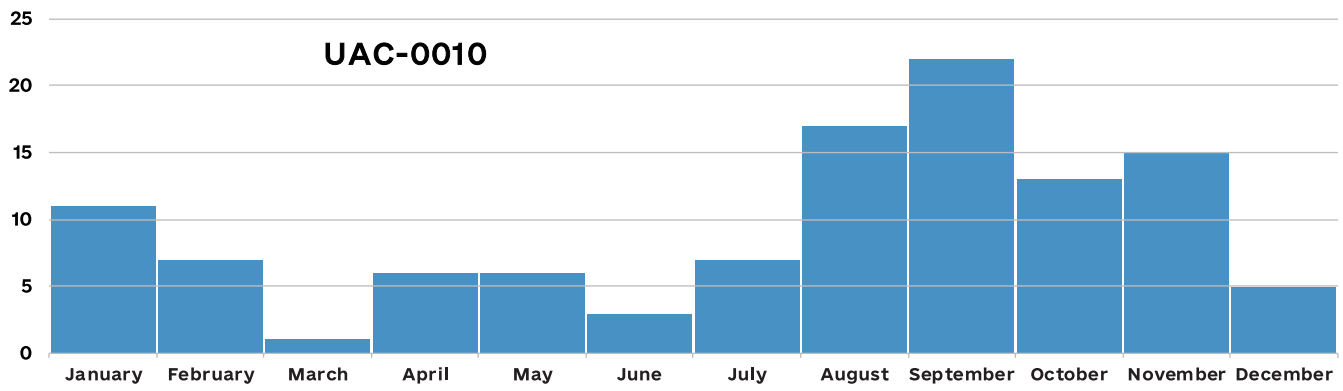
Our colleagues from Microsoft and other partners have done a terrific job mapping the H1 2022 threat landscape and correlating kinetic and cyber events. We would like to express our gratitude for all their support and also recommend checking the following reports as a reference on H1 tactics, techniques, and procedures (TTPs) discovered during the ongoing cyber warfare in H1 2022: Microsoft (Defending Ukraine: Early Lessons from the Cyber War, Special Report: Ukraine), Mandiant, ESET (ESET Threat Report T1 2022, ESET Threat Report T2 2022), Cisco Talos, CrowdStrike, Unit42, Economic Security Council of Ukraine.

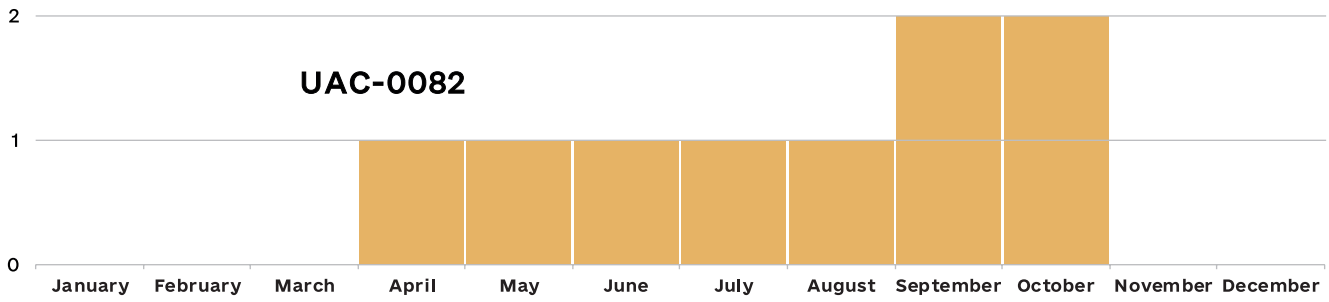
In H1 2022, russian cyber focus was on disruptive operations to suppress Ukrainian resilience, but they struggled to achieve this goal due to Western partners and Ukrainian organizations working closely together to quickly identify and block such attacks.

In this report, we would like to share our observations and analyses of the tactical shift in H2 2022 as many of the operations prepared before the war and control over many valuable assets were lost. Every 2-3 out of 10 operations are focused on destruction. The remaining 7/10 are sophisticated spear phishing campaigns with the objective of data exfiltration and cyber espionage.

The FSB associated group — Gamaredon — remains the most active group based on the incidents we registered in H2 2022. They are exfiltrating data and conducting a large amount of espionage operations.

We should also mention the GRU associated Unit 74455 known as Sandworm (UAC-0082) — they were especially active with disruptive ops and uses of wipers in H2 (Sandworm is a well-known “old” enemy, famous as the group behind the BlackEnergy & NotPetya attacks).



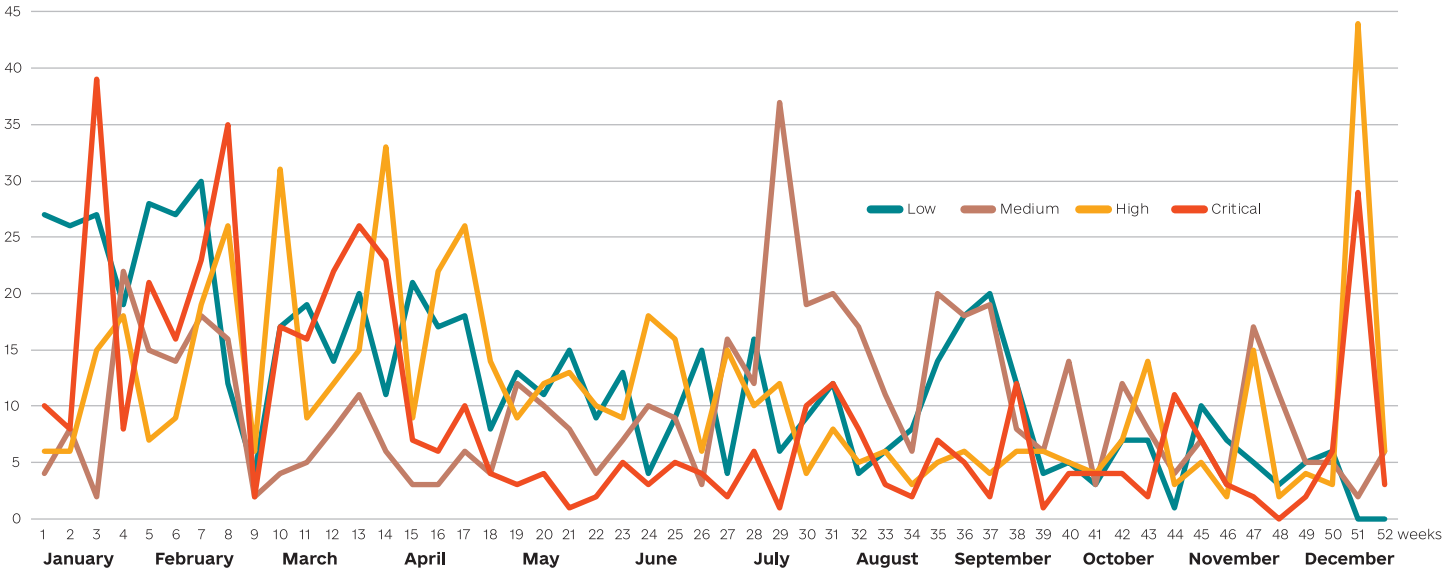


HYPOTHESIS

While Gamaredon is still the most persistent of all groups, the fluctuation in the number of incidents in this diagram which we associate with this actor could be explained by the following factors:

1. Complexity in group attribution
2. Increased concealed activity or mimicry of other groups
3. Improved capacity of defenders and more active measures to protect systems
4. Users don't click as before
5. Vastly improved proactive notification measures by CERT-UA & Partners regarding risky organizations

Overall representation of critical and high-severity incidents distribution over the whole year 2022:

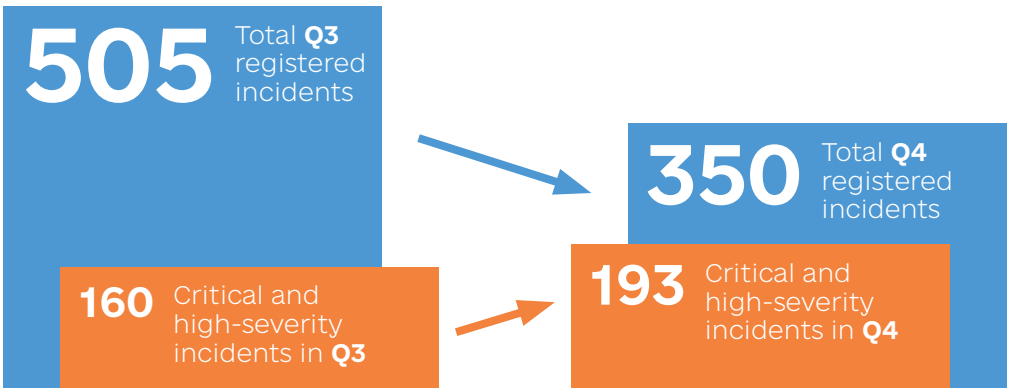


With the help of our partners in discovering and notifying Ukrainian organizations about compromised organizations and risky/exploitable vulnerabilities in H1, our enemies lost control over many critical targets.

HYPOTHESIS

The summertime decrease in cases could be explained by an increased engagement of malicious actors in the active search of new targets/opportunities (based on scan and intrusion attempts reports from our SOC team). Possibly prompted by an internal reprioritization and alignment with top russian military command forces. Another explanation could be the impact of vacations, which would support the assumption of attackers being mostly “hackers in uniform”.

We suspect that Q3 was used by malicious actors to prepare new operations, which actually took place in Q4. As seen in the diagram above and table below, there was a concentration of critical and high-severity incidents in H2 2022 over the last week of December.



Despite Q3 showing more cases overall, the number of critical cases was lower compared to Q4, meanwhile, Q4 was ‘hot’ due to a number of tricky cases.

December 2022 in particular was also marked by complicated attacks against energy infrastructure, even including 4-hop supply-chain attacks.

HOW

INCIDENTS BY CATEGORY

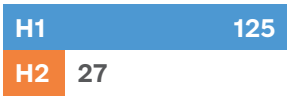
INFORMATION GATHERING

MALICIOUS CODE

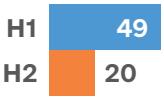
SUCCESSFUL INTRUSION

INTRUSION ATTEMPTS

AVAILABILITY ISSUE

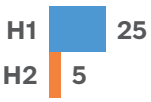


SERVICES OR BUSINESS SYSTEMS

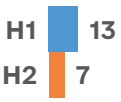


VULNERABILITY EXPLOITATION

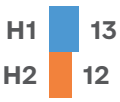
ABUSIVE CONTENT DISTRIBUTION



FRAUD



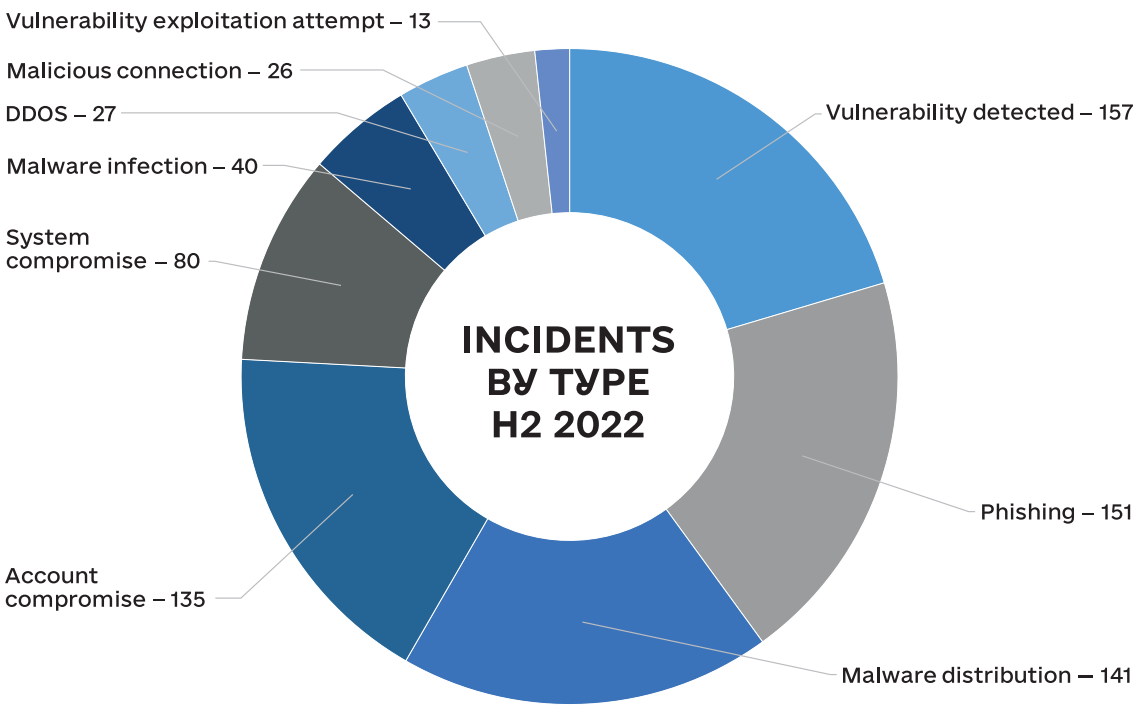
OTHER



Spear phishing remains one of the dominant and still effective techniques. However, we noticed a small shift in the tactics of russian groups compared to previous periods: in Q3 and Q4, rather than attacking the specific primary targets directly (where successful spear phishing could be quite difficult), they started to focus more on exploiting technical vulnerabilities of organizations somehow connected to the main target through the supply chain.

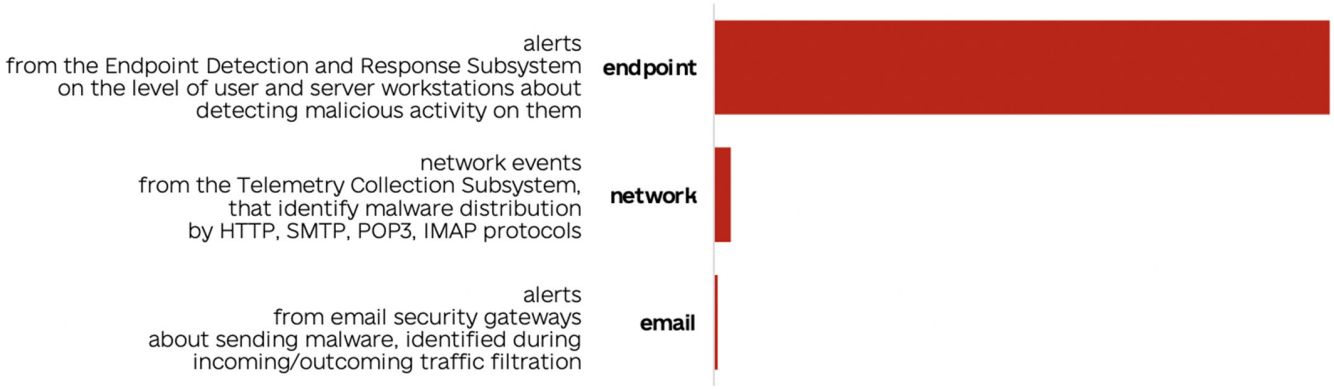
Among the cases that were investigated by the CERT-UA team, you may notice that malicious code/ malware infections are also across the most prominent. Stealers play an important role in gaining access to internal networks via VPN without 2FA. Account compromise via malware infections or CobaltStrike implants brought through exploited vulnerabilities remains an active exploitation/persistence.

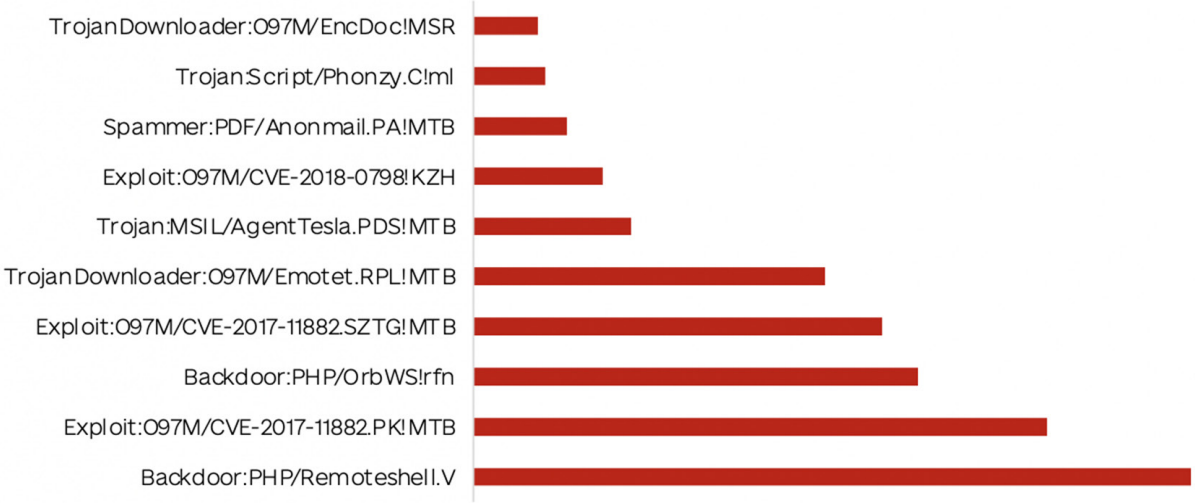
Malicious actors actively exploit email services and trust between recipients for malware distribution, targeting the government segment & Energy/Critical infrastructure segment in Q3–Q4.



Still based on the analytics provided, detection on the Endpoint level drastically predominates compared to Network or Email layers (bypassing spam, malware, and IPS filtering).

Web-based vulnerabilities and persistence methods are still at the top.

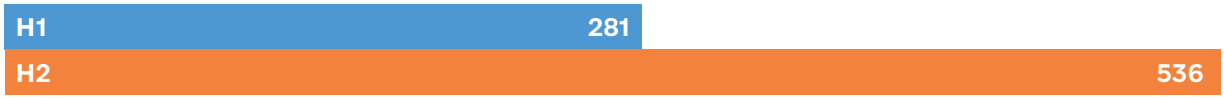




WHY

TOTAL INCIDENTS BY SECTOR

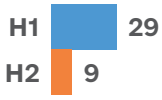
UAGOV



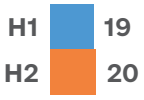
UACOM

FCOM

FGOV



MIXED GOV AND COMMERCIAL SEGMENT



In H2 2022, the FSB/GRU/SVR demonstrated their distinct eagerness for Intelligence collection.

The most heavily attacked sector in terms of cyberespionage and aggressive operations from adversaries remains Ukraine's civilian infrastructure, including government institutions and critical infrastructure (energy companies, commercial organizations, logistics companies, the Ministry of Energy, the Ministry of Finance, the Ministry of Foreign Affairs, etc.). Defense organizations are also targeted, including the Ministry of Defense, the State Border Guard Service etc. The primary focus for the APT listed above was credential-harvesting to gain impersonated and legitimate access through email or VPN without 2FA for collecting data (email communication as the main priority, PII & PHI databases as a second priority).

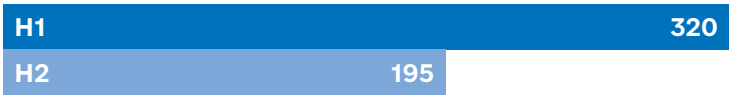
TOTAL INCIDENTS BY SEVERITY

CRITICAL SEVERITY INCIDENTS

HIGH-SEVERITY INCIDENTS

MEDIUM-SEVERITY INCIDENTS

LOW-SEVERITY INCIDENTS



Phishing and spreading malware via email is not an easy task mainly due to the migration of many government organizations into the cloud and greatly improved email filtering/protection. And yet, there remain various weak spots and non-sophisticated users who fall victim to well-crafted phishing emails.

Hacktivists have different tactics. If they find a victim organization with public vulnerability, but that organization is not useful, they dump data but don't wipe. Healthcare data is also an important source of intelligence, as it could be used for psychological operations against important individuals.

Military, Security and Defense sector

Cases: 113

Most active Actors: FSB (Gamaredon UAC-0010 20 cases),
UAC-0097 (5 cases),
UAC-0142 (2 cases),
UAC-0020 (1 case)

MILITARY COMMISSARIATS	Almost all military commissariats before May 2022 were infected because of the lack of centralization, bad asset management and independence of these organizations. Malicious actors were hunting for information about mobilization plans, rotation, promotions, etc. Their primary interest was to have databases of ex-military who have been involved in the Anti-Terrorist Operation on occupied territories during the active phase of 2014–2016, to arrest them.
MILITARY	Interesting cases that should be noted: intelligence and espionage operations against the Security Service of Ukraine and the State Border Guard Service of Ukraine.

Enemy targets: Defensive organizations plans, procurement activities, key personnel, attacks on the Delta platform (new military artillery/fire targeting and intelligence, command and control platform).

In H2 2022, Gamaredon was constantly going after the Security Service of Ukraine (SBU) personnel, to compromise Signal messenger accounts and leak data and impersonate users.

The State Border Guard Service of Ukraine experienced attacks on its communication satellites and the “Shliakh” - a system used by the border guard officers to check the identity of those crossing the State Border of Ukraine.

The Ministry of Defense was among the most actively attacked organizations, with many cases and a variety of groups. The top used scenario was spear-phishing.

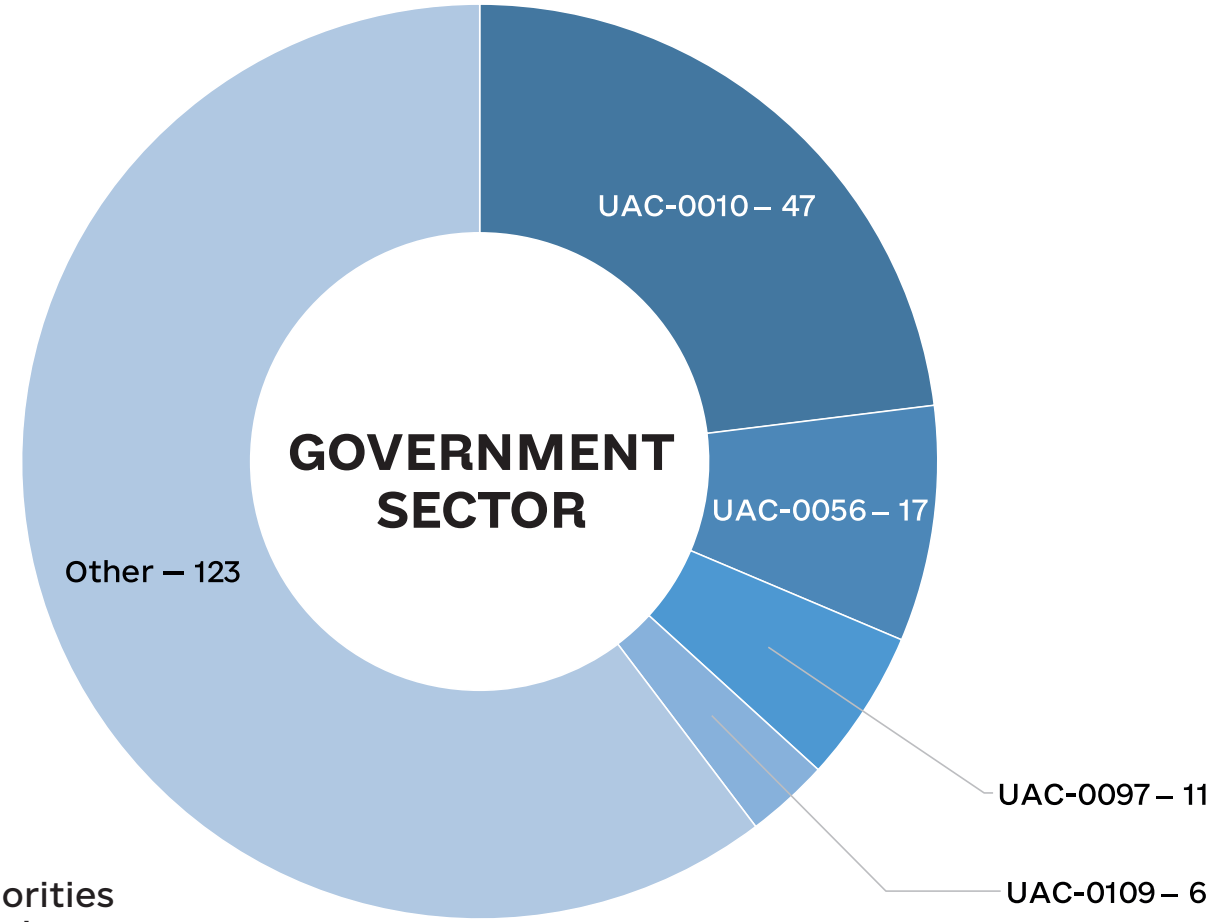
Apart from russian threat actors, activities from groups affiliated with Iran and China were discovered too. However, these were isolated events from APTs we have seen in the past with country origin suggested, and we cannot associate those attacks with state-sponsored attacks.

Defense contractors and manufacturers like Ukroboronprom, a state concern which is a strategic manufacturer of weapons and military hardware in Ukraine, were also under constant monitoring, and many of the discovered complicated cases were directed against them.

Government sector

Cases: UAGOV — 536, UAGOV/UACOM — 20

Most active Actors: UAC-0010/Gamaredon,
UAC-0056,
UAC-0097
and others presented below:



Key targets:
- Local authorities
- Key ministries
- Regional governmental organizations
- State-owned Enterprises and factories

Goals:
- Cyber espionage and continuous access/persistence
- Destructive activity
- Psychological operation
- PII Data
- Account compromise

We are detecting hundreds of cyber operations against governmental organizations in Ukraine.

Telecom and IT

Cases: 43

Most active Actors: UAC-0109

Enemy objective: Lack of connectivity (cellphones and internet) can cause disorganization and panic across the civilian population.

It directly impacts response time and capability to react to any incident or situation. Without the internet, civilians as well as military personnel and intelligence officers can't coordinate to take an action or call for help.

The primary objective of malicious actors in the Telecom sector in H1 was disruption operations or, where feasible, gaining access to all ground IT infrastructure.

In H2, attacks in this sector were targeted primarily on private IT companies that provide services and products to the government segment ("supply chain attacks").

ISP and hosting providers were used as an entry point to commercial businesses (where vulnerable control panels, Zimbra email systems and other components were shared across multiple customers, and all these email servers and other data were misused to conduct further attacks on their customers, often from the government or energy segment). Where attackers were not able to penetrate an organization directly, they were exploring the opportunity to enter via hosting/provider.

Logistics & Transportation

Cases: 19 (including 7 Transportation cases)

Most active Actors: UAC-0082/Sandworm

Enemy objective: Espionage & intelligence collection. Monitoring the ways that Western weapons enter Ukraine and places of their storage. Control over supply chains and military paths.

Key targets:

RAILWAY COMPANIES	They are a key to solid and fast heavy weapon delivery to the bases near the frontline. The enemy's key interest was in understanding supply dependencies, schedules, and specific equipment/machinery.
POST SERVICES / LOGISTICS	The goal was to limit deliverability of goods supply to the frontline, as volunteering is a big part that keeps resistance high.
LOGISTICS CONTRACTORS	Companies contracted by the Ministry of Defense and other critical organizations who have to support combat units.

Related Incidents include attacks on local governments in the Lviv and Odesa regions, which often are entry points for the Western weapon systems supply.

Media

Cases: 29

Most active Actors: UAC-0082/Sandworm

Enemy objective: In H1 2022, we recorded attempts of active exploitation of private media companies' information systems, with attempts to psychologically manipulate the public to destabilize the government and coerce the top decision-makers to benefit the adversary party. They went after radio stations, newspapers, news agencies, and any other entity suitable for injecting their message.

In H2, we faced around 10 serious cases with the primary objective to disrupt business — disruption, wipe, and ransomware. With moderate confidence, we track this malicious campaign as UAC-0082, and attribute the activity to the russia-linked Sandworm advanced persistent threat group.

After penetration and recon, they went after backups, hunting for NAS devices and servers and live broadcasting systems/segments. As an entry point, they often tried to exploit the Follina vulnerability (CVE-2022-30190) to infect the victims' machines with the CrescentImp malware and then re-distribute their malware via 500+ other email addresses selected from victims. CobaltStrike C2 was also a typical toolkit in those campaigns.

The goal was conducting psychological operations against Ukrainian citizens. After the goal was achieved, the threat actor performed destructive actions in the networks of the victims.

Energy sector

Cases: 29

Most active Actors: GRU/Sandworm/UAC-0082 (3 cases),
UAC-0133 (1 case),
UAC-0107 (1 case)

Enemy objective: Limit or disrupt payments from civilians, focusing on payee databases with addresses and PII data.

Key targets:

- Institutions that design and build gas and oil pipelines
- Electricity grids
- Public electricity supply companies

The malicious actors in question have knowledge about Ukrainian energy infrastructure architecture after the April/May cases, which gives them a certain advantage. They actively attack civil and critical infrastructure with the hope that it will open the door for influence operations and further negotiations.

Gas and electricity companies were a primary target as part of russia's general strategy launched in Q3 2022 to cut down the power supply, interrupt logistics and broadcasting (including Internet communication for government and civil society), and limit access to news and information.

Banking

Cases: 12 (registered by CERT-UA,
while the majority is processed by CSIRT NBU)

Most active Actors: UAC-0084,
UAC-0056,
UAC-0100,
UAC-0107

Enemy objective: Interrupt and influence the financial system of Ukraine, spread panic and economic downturn, and make banking services unavailable.

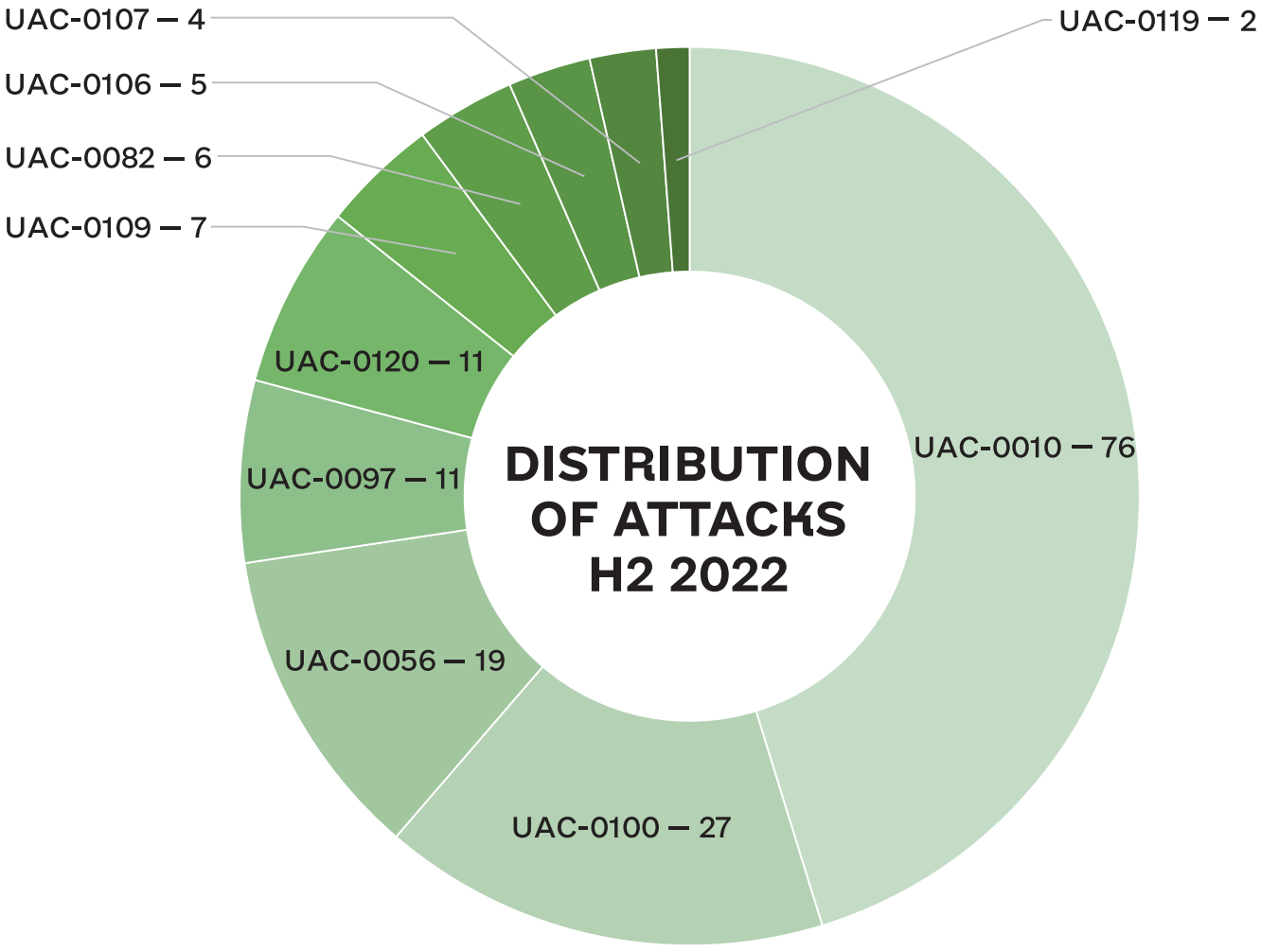
WHO

CERT-UA and other cybersecurity agencies continuously monitor russia-aligned threat groups, which have been waging attacks on critical infrastructure since 2014.

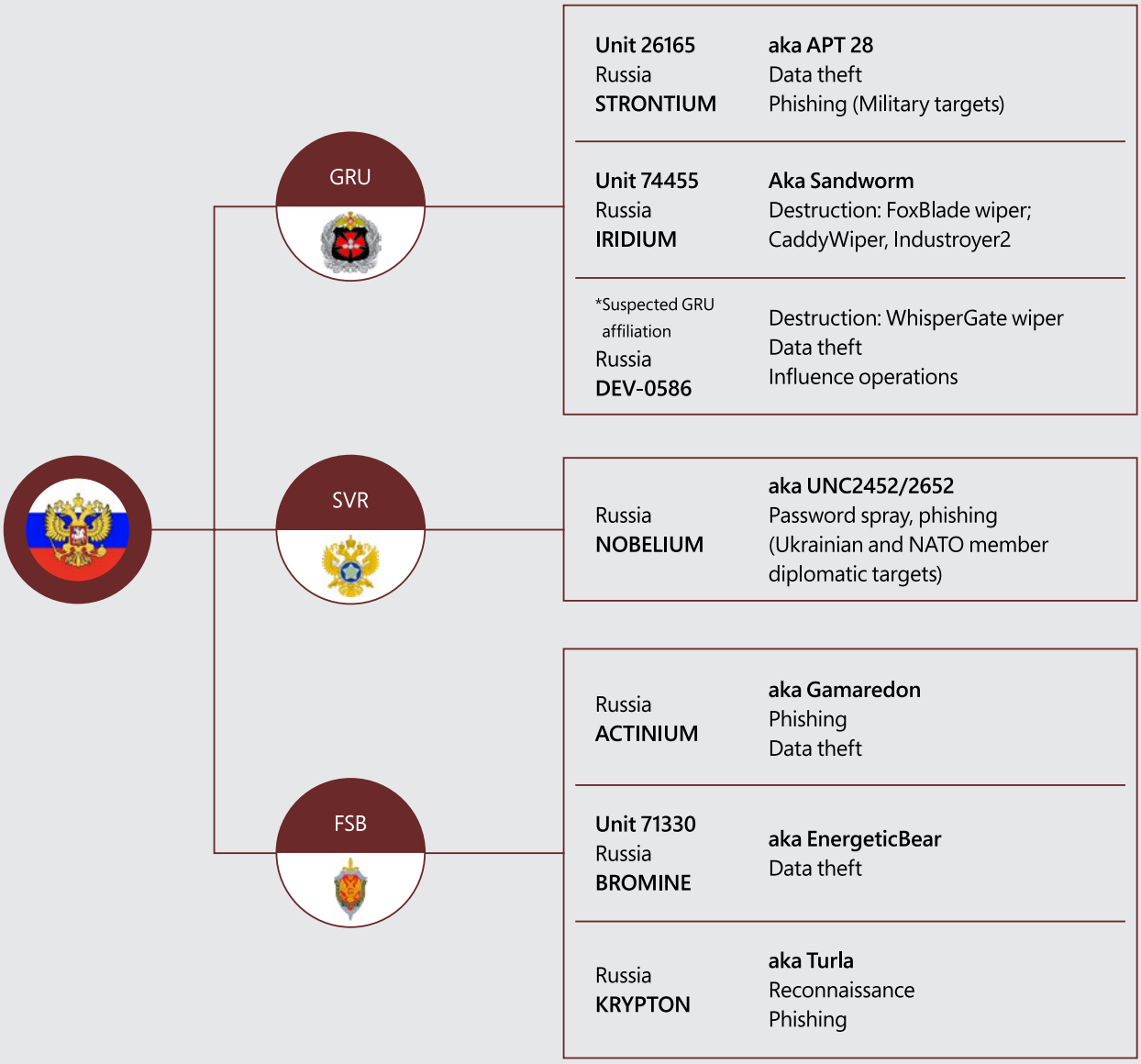
Cyber espionage, destructive and influence operations were clearly connected to support and enable more efficient on-the-ground operations during the planning and active phases of the invasion, especially to identify covert Ukrainian defenders in the occupied territories and eliminate potential partisans.

Because of formal attribution complexity, we suggest that in Q3–Q4 2022, russian government-related adversaries focused on pursuing a common set of priorities and not actively coordinating.

They were mostly penetrating the energy segment and pursuing intelligence collection and data exfiltration across all other vulnerable/available targets in Ukraine.



(Source: Microsoft report)



Russian government APTs are usually limited in resources/manpower. They can't involve more people in the agency as there are trust limits and top IT cybersecurity talents who work for the commercial sector don't want to work for the criminal government (in many cases resulting in their leaving the country). Government cyber agencies also have strict rules and serious limitations.

Usually, such a unit comprises 5 to 10 hackers and 10 to 15 analysts.

That's why in 2022, they outsourced part of their targets to affiliated criminal and hacktivist organizations who supply raw data to them.

FSB activities

UAC-0010/Gamaredon/Actinium

Of all the actors CERT-UA monitors, Gamaredon carries out the largest number of cyberattacks — 74 cases registered in total in H2. It is the most actively attributed threat actor. Not a week went by that we didn't record some new mass phishing email attacks waged by Gamaredon.

The main purpose of their activity is cyber espionage. But CERT-UA investigates cases when, after the network was infected by Gamaredon malware, lateral movement within the network began with TTPs belonging to other russia-related threat actors.

The major targets include the key governmental organizations, state-owned enterprises, the security and defense sector.

Their primary method is spreading malware with the help of phishing emails. Their phishing emails are always well-crafted. They use topics that relate directly to the competence of the affected organizations. Another factor of Gamaredon's success is that they actively use email accounts compromised as a result of successful cyberattacks.

They actively utilize the Crimean telecom/hosting provider CrymCom.

Gamaredon demonstrates outstanding performance as their botnet of infected machines used in their campaigns as C2 or malware hosting contains 1000+ machines/compromised servers, and more are added on a daily basis.

They attacked the Ukrainian Police hunting for their privileged/unlimited access to databases/catalogues/ social registers, as the police store and process information about cars, movement, cameras, road situations, arrests etc.

FACT	Personal identifiable information (PII) was used to threaten security researchers right during the initial days of the invasion. https://unit42.paloaltonetworks.com/trident-ursa/

FACT	Russian APT groups reuse the same infrastructure for some of their campaigns.

GRU (military intelligence)

UAC-0082/Sandworm/IRIDIUM

In H2 CERT-UA analyzed 6 incidents, which with a high level of confidence refer to Sandworm. Those analyses help identify the tactics and techniques used by the threat actor in their cyberattacks. They specialize primarily in cyber espionage & destructive activity. Their targets are critical infrastructure organizations such as energy facilities and logistics companies, but also popular media and critical public resources.

Among all the groups, during the full-scale invasion only Sandworm focuses to a greater extent on destructive attacks in Ukraine to promote the interests of their likely supporters or (misplaced) patriotism.

In Q3, the focus remained on the media outlets, while Q4 showed the most remarkable three cases which were associated with successful intrusions into Ukrainian power companies. They possess and utilize solid knowledge of that infrastructure, attained in the previous campaigns.

In October (Q4), we registered Sandworm activity which they tried to disguise as a mere ransomware infection of logistics companies in Ukraine and Poland.

This threat actor's main technique of getting initial access to the internal network is exploitation of the affected public resource's vulnerabilities.

Initial access enables long-time reconnaissance of the affected network. They also create multiple access points to the internal network. Usually, they use open-source tools (like Stowaway, ReGeorg, etc.) for establishing points of access. They also resort to lateral movement with stolen credentials, usage of RDP, Impacket, WMI, VPN.

The final stage for most of their operations is destructive actions in the victim's network. Specific sophisticated malware is executed during this stage. In the arsenal of the threat actor, there are various wipers coded both for Windows (HermeticWiper, IsaacWiper, CaddyWiper) and for various types of Linux systems (AwfulShred, SoloShred).

The use of malware like Industroyer2, which uses industrial protocols for communications with SCADA systems and intervenes in the work of high-voltage electrical substations, indicates a high level of preparation of the actor for their cyberattacks.

In H2 2022, CERT-UA detected the same tactics, techniques and toolset used by Sandworm in waging attacks on energy organizations and popular mass media outlets.

In late autumn, they changed some TTPs, trying to disguise their activity behind the distribution of ransomware, as was the case with attacks on

logistics companies in Poland and Ukraine where Prestige ransomware was used.

Lately, CERT-UA noted some changes in the methods of getting initial access to the internal network. In a few cases at the end of 2022, the threat actor waged spear phishing attacks on energy facilities of Ukraine using attached malware.

UAC-0028/APT28/STRONTIUM/Fancy Bear

GRU team APT28 is well known for penetrating private groups in the popular messaging applications, used by the Ukrainian military, by using valid passwords of the existing users. They get passwords by means of phishing, stealers, re-use of passwords from compromised web resources rather than compromising messaging applications.

Our analytics show that typical operations require one month for successful execution. Because of attribution complexity, we don't have a clear indication of APT28 across our cases.

SVR (Foreign Intelligence Service)

UAC-0035 (InvisiMole)

UAC-0035 (InvisiMole) specializes purely in cyber espionage. Their operations were focused on individual diplomats deployed outside Ukraine as well as the Ministry of Foreign Affairs of Ukraine. The complexity and sophistication of their activities are comparable to the other groups covered in this report. With a pure focus on persistence, their operations are slow but silent. Their backdoor RC2 provides extensive espionage capabilities such as recording from the victim's webcam and microphone, tracking the geolocation of the victims, and collecting recently accessed documents. A modern approach to utilizing Bring Your Own Vulnerable Driver (BYOVD) indicates a sophisticated development team behind operators.

They are further known as a team that managed to get access to closed systems with crypto gateways to protected communication networks in H2 2022. One of their tactics inside a compromised network was to distribute

implants with reasonable file names across network shares and drives to be executed by users out of curiosity.

Also, they trojanized ISO and binaries with their malware and distributed it for free on torrents, as system administrators in post-soviet countries sometimes rely on torrents more than official resources.

UAC-0029/APT29/NOBELIUM/Cozy Bear

SVR team APT29 is widely known for targeting political parties, governments, international organizations, think tanks and NGOs. They mostly focus on cyber espionage in the political sphere. The group is considered responsible for SolarWinds supply chain attack. They are known for having their own malware toolset and high proficiency in targeting Microsoft products and services.

CERT-UA is still attributing some low-confidence cases to APT29 because of attribution complexity.

FACT	Russian military officers acquire access credentials from captured Ukrainian militaries and personnel of various organizations on the occupied territories (telecom, energy, government) and use them to access infrastructure, systems and applications, registers, and DBs.

FACT	On compromised machines and captured phones, malicious actors hunt for ".set» files. «*.set» files are in use by the Android ArmySOS application used by Ukrainian military artillery prospectors to provide GPS pointers of enemy artillery, infantry and command center.

Belorussian group UAC-0105 / GhostWriter

GhostWriter is a state-sponsored cyber espionage actor that is engaged in credential harvesting and malware campaigns. Despite recorded activity during Q1 and Q2 (4 cases), no attributed activity was registered in Q3 or Q4.

Hacktivists & Cybercrime units

According to our observations, multiple threat actors are involved. At least 9 known or russia-affiliated cyber threat teams in addition to other unattributed

threat actors are engaged in activities that range from phishing and malware distribution via email for initial access to pervasive lateral movement, data theft, and data deletion.

Regular public reports of their successful operations posted in Telegram channels suggest that these threat actors are positioning themselves as a persistent malefactor, and they will continue to target Ukrainian networks for the duration of this war and beyond. They try to mirror and augment actions/targets of military command, so it seems they closely coordinate their operations with the decision-making centers.

Because of the targeting specifics mentioned above, decisions on cyber and military goals and priorities come from putin's presidential administration, and then the FSB curator (who also protects cyber criminals from prosecution) contacts their network of affiliated ransomware groups or hacktivists to communicate the general direction of targeting or certain industries.

Some of these groups also focus on intelligence operations, and some on the promotion of their activities to attract younger, highly motivated, but less experienced volunteers. It therefore increases the number of potential cybercrime groups that will also work against Western companies to gain profit from their operations.

The most active groups were:

- Hacktivists (XakNet) UAC-0106
- Hacktivists (CyberArmyofRussia) UAC-0107
- Hacktivists (Zarya) UAC-0109

UAC-0108 / KillNet

KillNet is among the most active russian hacktivist groups that posted their activity reports on Telegram channels. This group was first identified in March 2022.

According to the activity monitoring results, it is impossible to single out specific techniques and tactics of this formation. The main targets of this group are the Ukrainian critical infrastructure and various ministries, with the most notable cases being breaches of the Ministry of Foreign Affairs of Ukraine and the Ministry of Economics. They were publishing information about DDoS-attacks, documents received as a result of the espionage cases, and dissemination of propaganda and fake information. Their attacks do not harm the regular functioning of the systems.

Based on the analysis and correlation of data obtained while investigating the incidents mentioned in the KiilNet Telegram channel, CERT-UA can confidently assert that this group works with UAC-0082. At the same time, some cybersecurity vendors associate their activities with UAC-0028.

RECOMMENDATIONS

As more large businesses and corporations invest in cybersecurity tools, hackers are increasingly targeting small and medium-sized businesses and using them as supply chains. Some of the most common intrusion techniques used in H2 2022 campaigns include:

- Exploitation of public-facing applications or spear phishing with attachments/links for initial access.
- Credential theft and use of valid accounts throughout the attack lifecycle, making 'identities' a key intrusion vector. This includes Active Directory Domain and through VPNs or other remote access solutions.
- Use of valid administration tools and practices for lateral movement, relying on compromised identities with administrative privileges.
- Use of known publicly available offensive arsenal like CobaltStrike, Sliver and others, sometimes obfuscated using actor-specific methods to defeat static signatures.

Based upon these observations, we recommend taking the following actions:

1. Minimize credential theft and account abuse: Protecting the identities of your users is a key requirement to secure your network and resources from attackers. We recommend enabling multifactor authentication everywhere and Active Directory hardening (or migrating Domain Controllers to Azure AD).
2. We also urge the application of the least privileged access and additionally securing access to the most sensitive and privileged accounts and systems.
3. Secure internet-facing systems and remote access solutions: Internet-facing systems should be secured against external attacks by ensuring they are updated to the most secure levels, regularly evaluated for vulnerability, and audited for changes to the integrity of the system. Anti-malware solutions and endpoint protection should be enabled for the detection and prevention of attackers. Legacy systems should be isolated to prevent them from being an entry point for persistent threat actors. Remote access solutions should require two-factor authentication and be patched to the most secure configuration. Remove or restrict outbound access wherever possible to mitigate egress-based kill chains.
4. Leverage anti-malware, intrusion detection, flow monitoring, endpoint detection, and identity protection solutions with a central management console: the State Cyber Protection Center has a toolset and sensors which can be provided to organizations for free.
5. A combination of defense-in-depth security solutions, paired with trained and capable personnel, can empower your organization to identify, detect, and prevent intrusions impacting your business. Enabling native cloud workloads protection allows the identification and mitigation of known and novel threats to your network at scale.

Russia's Cyber Tactics:
Lessons Learned 2022

State Service
of Special Communications
and Information
Protection of Ukraine