State Service of Special Communications
and Information Protection of Ukraine

RUSSIAN CYBER OPERATIONS

APT Activity Report H1 2024

CONTENT

Yevheniya Nakonechna
Head of the State Cyber Protection Centre
of the SSSCIP

The full-scale invasion of Ukraine by the Russian Federation has served as a powerful catalyst for the evolution of cyber threats. Cyber warfare has become a dynamic battleground where tactics and technologies evolve daily.

Russian hacker groups, including those affiliated with Russian intelligence agencies, special services, as well as cybercriminals and hacktivists, are continuously probing Ukraine's information systems, constantly developing new attack vectors against Ukraine and the entire civilized world.

In the first half of 2024, the CERT-UA team, in collaboration with other Defense Forces units, observed a significant change in the use of cyberattacks.

In 2022, the adversary focused on operations aimed at dismantling IT infrastructures of organizations within the critical infrastructure sector and exfiltrating databases and personal data details. Campaigns targeting media and commercial organizations did not induce the desired panic among civilians or achieve a battlefield impact. The so-called "cyber victories" did not produce the intended long-term effects, and Ukrainian IT systems quickly recovered. Enemy hackers targeted organisations with evident flaws in cybersecurity, vulnerabilities, and opportunities they could easily exploit.

By 2023, their strategy shifted from the destruction of infrastructures of ISPs, ministries, and government bodies to securing footholds and covertly extracting information, using cyber elements to gather feedback on the outcomes of their kinetic

PREVIOUS REPORTS:

H2 2022

H1 2023

H2 2023

strikes. IT proved its resilience by rapidly recovering from breaches and becoming stronger.

In 2024, we observe a pivot in their focus towards anything directly connected to the theater of war and attacks on service providers—aimed at maintaining a low profile, sustaining a presence in systems related to war and politics. Hackers are no longer just exploiting vulnerabilities wherever they can but are now targeting areas critical to the success and support of their military operations.

Based on data collected by CERT-UA and other cyber divisions of the State Service for Special Communications and Information Protection, we have analyzed emerging trends in cyber threats, identified weaknesses in our defenses, and evaluated the effectiveness of countermeasures implemented to address these threats.

In this report, we will delve into how the tactics and objectives of Russian hacker groups have evolved, what new threats have emerged, and the lessons we have learned from these experiences.

The findings of this study are crucial for understanding contemporary cyber threats and developing effective counter-strategies.

We hope this report will serve as a valuable resource for both Ukrainian and international cybersecurity professionals, as well as for anyone interested in enhancing their cybersecurity capabilities.

STATISTICS AND TRENDS

Disclaimer: This dataset has been compiled based exclusively on the analysis of incidents handled by the Governmental Computer Emergency Response Team of Ukraine (CERT-UA) and the Security Operations Center (SOC) of the State Cyber Protection Center of the SSSCIP.

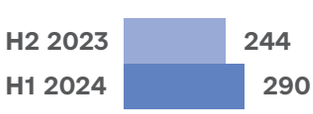
Incidents by Severity Level	H2'2023	H1'2024	Change
Critical	31	3	-90%
High	156	45	-71%
Medium	1264	1670	32%
Low	12	21	75%
Total	**1463**	**1739**	**19%**

QUANTITATIVE METRICS FOR PROCESSED INCIDENTS

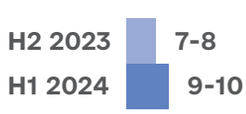
+19%

INCREASE IN THE NUMBER OF REGISTERED INCIDENTS IN H1 2024

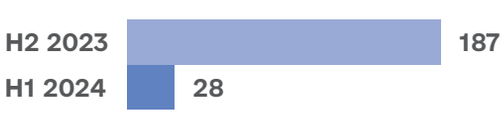
AVERAGE PER MONTH



AVERAGE PER DAY



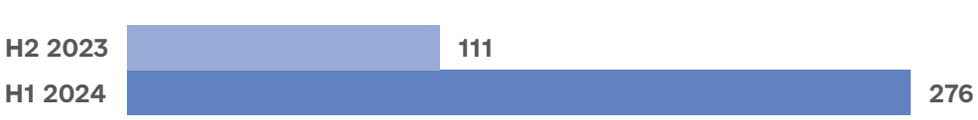
85% DECREASE IN CRITICAL AND HIGH-SEVERITY INCIDENTS:



40% INCREASE IN CYBER INCIDENTS INVOLVING MALWARE DISTRIBUTION

90% INCREASE IN CYBER INCIDENTS INVOLVING MALWARE INFECTIONS*

THE NUMBER OF ATTACKS ON THE SECURITY AND DEFENSE SECTOR HAS INCREASED MORE THAN TWOFOLD



** The increase in cyber incidents related to malware infections is less attributable to changes in TTPs (Tactics, Techniques, and Procedures) and more due to enhanced visibility, as victims are more frequently seeking assistance.*

As evidenced by the charts, the trend of increasing cyber incidents continues, despite a decrease in the number of high and critical severity incidents.

The continuous and effective cooperation between the divisions of the SSSCIP, whose primary mission is to ensure cybersecurity and cyber defense in Ukraine, has had a significant impact on these statistics.

Cyber Incident Response Operations Center of the State Cyber Protection Center of the SSSCIP (SOC SCPC) utilizes cyber threat indicators obtained by CERT-UA through the investigation of cyber incidents and attacks, along with additional compromise indicators provided by partners and enriched by experts from both units.

Based on these indicators, the SIEM system automatically analyzes data collected from various sources, such as NDR (Network Detection & Response), EDR (Endpoint Detection & Response), and network session streams. It processes billions of events and identifies millions of security incidents across different levels of severity. Following the manual analysis of suspicious events detected by SIEM, SOC specialists identified 525 cyber incidents. Moreover, most of these events were blocked by cybersecurity solutions provided by the Cyber Incident Response Operations Center to more than 70 organizations, and therefore had no impact on the final systems.

As the statistics show, there has been a significant increase in attacks on government organizations and local authorities. The number of processed cyber incidents targeting the security and defense sector, as well as the energy sector, has more than doubled.

However, it is important to mention that these statistics are relative and depend on various factors. In addition to changes in attack trends within cyberspace, these numbers are also influenced by increased visibility (enhanced detection capabilities), growing awareness (more organizations seeking consultation/assistance), and other factors.

KEY FINDINGS AND INSIGHTS FOR H1 2024

NEW GROUPS AND ATTACK METHODS VIA EMAIL, ARCHIVES, AND VIRUSES

At the beginning of the first half of 2024, as in the second half of 2023, cyber espionage attacks were primarily conducted through targeted email campaigns distributing malicious software.

The evolution and transformation of key approaches by established groups are illustrated in the following visualizations.

Throughout H1 2024, we observed significant activity from eight cyber threat clusters that we have been tracking since early this year or late last year. Some of these clusters are well-known, but for various reasons, their operations had not been detected for an extended period:

1. **UAC-0184** (Cyber espionage, Russia)
2. **UAC-0027** (Cyber espionage, China)
3. **UAC-0195** (Messenger account theft)
4. **UAC-0020** (Cyber espionage, temporarily occupied Luhansk)
5. **UAC-0149** (Cyber espionage, Russia)
6. **UAC-0188** (Attacks on financial and insurance institutions in the EU, USA, and Ukraine)
7. **UAC-0063** (Cyber espionage, possibly a sub-cluster of UAC-0001)
8. **UAC-0180** (Cyber espionage)

At the start of H1 2024, the majority of malicious email campaigns were traced back to the Russian hacker group **UAC-0050**, with up to five such incidents being observed weekly.

However, by March, this activity began to decline, and by April, no further email campaigns were detected. During the same period, groups **UAC-0149** and **UAC-0184** became more prominent. Their approach is more sophisticated, with attacks specifically targeting individuals within the Defense Forces.

Meanwhile, attacks from **UAC-0010**, operated by Russia's FSB, have been ongoing since 2014 and continue to this day.

It is also worth mention that hacker groups conducting attacks against Ukraine as part of the so-called "Special Military Operation" (SVO), which have not yet been conclusively attributed by us, may be linked to the following threat clusters:

- **RosGvardia** (National Guard of Russia)
- **MVD** (Ministry of Internal Affairs)
- **Special Communications and Information Service of the Federal Protective Service of the Russian Federation** (Spetssvyaz)
- **General Staff of the Russian Federation**

ANOMALOUS SHIFTS IN ACTIVITY OF FINANCIAL HACKING GROUPS

Similar to **UAC-0050**, the group **UAC-0006**, which had been involved in stealing funds from Ukrainian companies, disappeared from our radar in March 2024, only to resurface in May.

During their absence, several cyberattacks utilizing ransomware occurred, where hackers successfully encrypted data within the networks of commercial companies, including backups. The only option for these companies to recover their data was to comply with the attackers' demands and purchase the

“decryptor.” In such scenarios, it is crucial to maintain backups of critical systems on external media, which are not connected to the network.

Starting from May 2024, **UAC-0006** resumed their operations, distributing malware to new victims and reestablishing access to previously infected computers.

MASS CAMPAIGNS FOR MESSENGER ACCOUNT THEFT

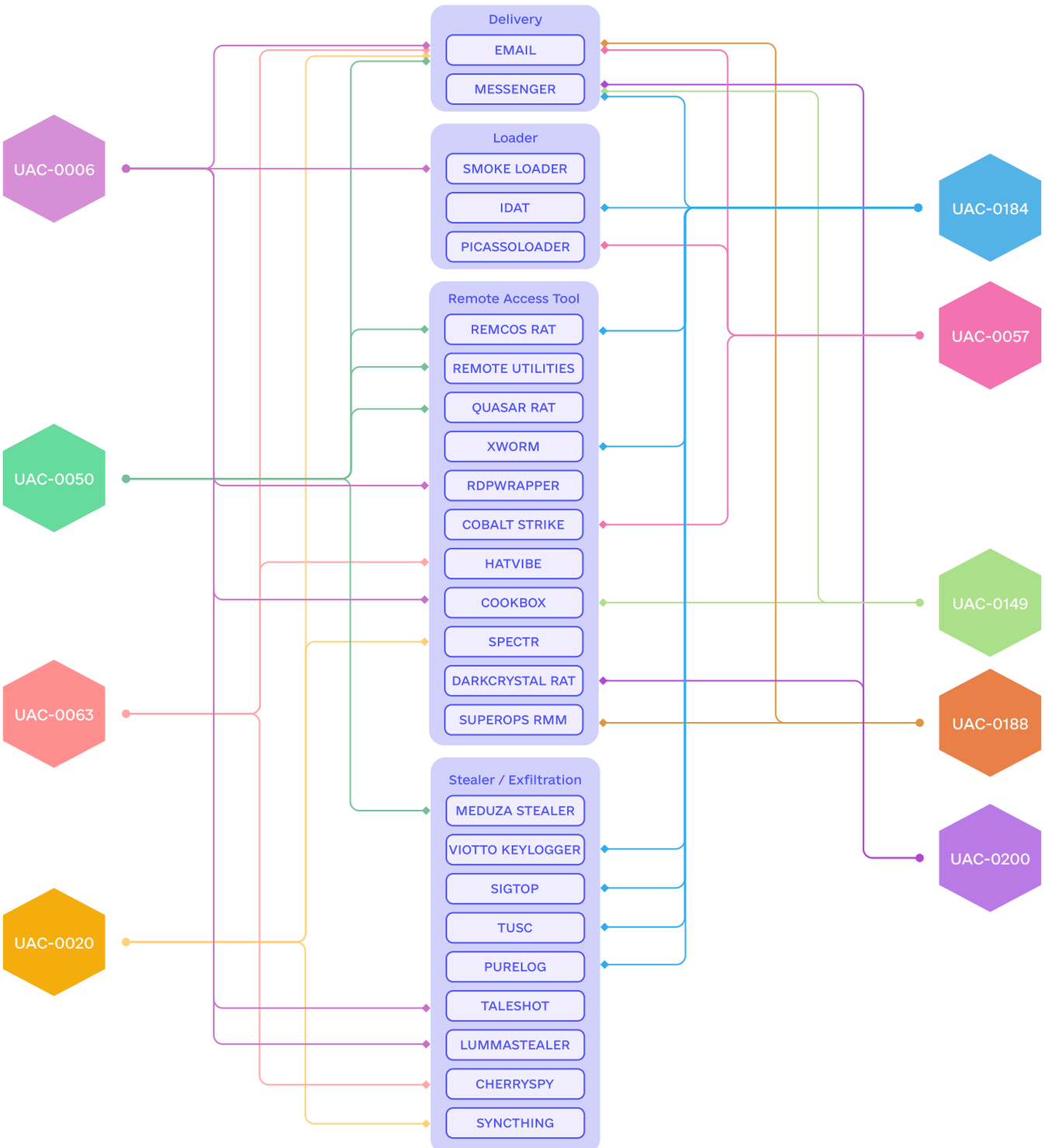
Hackers are increasingly targeting messenger accounts to facilitate the spread of malware and phishing campaigns, aiming to compromise as many users as possible. Among the victim’s contacts, there may be “high-value” targets whose messaging history are of particular interest to various intelligence agencies of the aggressor nation. However, the compromise of accounts is not solely used for espionage; they are also exploited for financial gain.

MALWARE DISTRIBUTION THROUGH "PIRATED" SOFTWARE

A significant portion of “pirated” mention comes pre-packaged with backdoors, leading to system infections. It is important to note that the assistance of international partners in providing licensed software, security tools, and access to cloud services has greatly contributed to minimizing this risk and enhancing overall protection. However, this support alone is not sufficient. We must also emphasize that providing licensed software such as Windows, Office, EDR, MDM, SIEM, and IDM is critically important for both Ukrainian military and civilian organizations to avoid vulnerabilities arising from malware infections through unlicensed software.

TOOLSET

Analyzing the adversary's toolset gives us a possibility to identify similarities in TTPs (Tactics, Techniques, and Procedures), cluster groups accordingly, and determine which groups are purchasing and deploying specific malware.



CASES

Below is an overview of the activities of **UAC-0184**, **UAC-0020**, **UAC-0149**, **UAC-0200**, and **UAC-0180**, which in H1 2024 focused specifically on military targets. They used various versions of RATs and other malware to maintain and remotely control compromised Windows computers belonging to members of the Ukrainian Defense Forces.

SIGNAL AND TARGETED ESPIONAGE ACTIVITIES BY UAC-0184 AGAINST THE MILITARY

Throughout the full-scale invasion, hackers have actively collected personal data of Ukrainian citizens, including military personnel. This data includes names, passport information, and, most importantly the military unit and position. Such information enables hackers to concentrate their efforts on specific individuals rather whose computers are likely to contain important documents.

As most corporate email servers use robust security measures, hackers increasingly avoid sending malware via email. Instead, they favor attacks through alternative communication channels, such as messaging apps widely used by military personnel. Equipped with ample personal data and contact phone numbers, UAC-0184 hackers impersonate others and initiate communication with their intended victims, often through Signal. It's worth noting that they employ any available resources to "groom" their targets, including dating platforms.

After gaining the victim's trust, under the guise of sending documents related to awards, combat footage, or recruitment to other units, the hackers send an archive containing a shortcut file. This list of topics used by attackers is not exhaustive. Special emphasis is placed on ensuring that the target opens the file specifically on their computer.

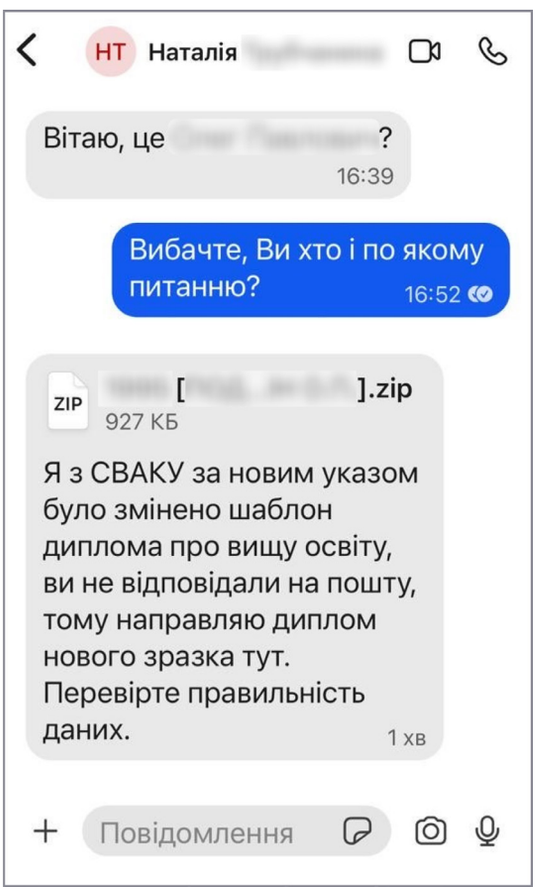
Opening the shortcut file on a computer displays a decoy file relevant to the conversation topic while

simultaneously infecting the system with a downloader malware, which then installs remote control software. This way, UAC-0184 gains full access to the victim's computer.

COMMON ATTACK SCENARIOS:

Request for Information:

- ”Please provide contact details“
- ”Confirm receipt“
- ”You are on the list to receive something, but we can't find the order“
- ”Have you received any documents regarding this?“



Intimidation:

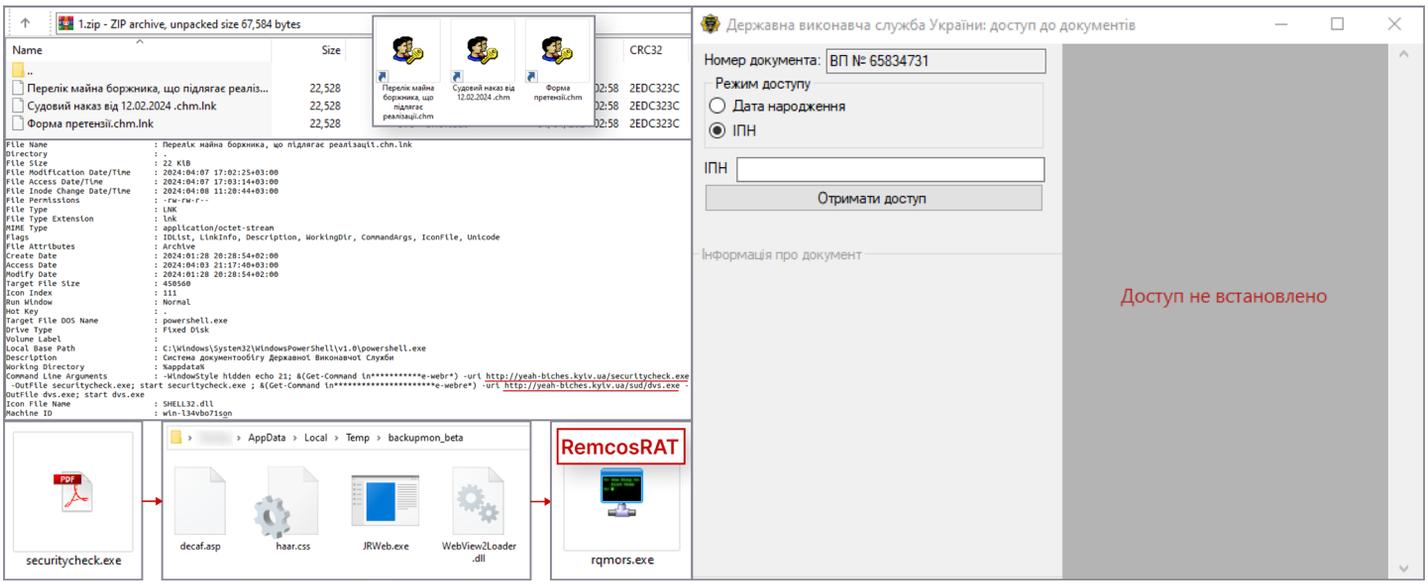
- Opening proceedings against the service member
- ”There is an issue with...“
- ”You have appeared on a list“
- ”There are questions regarding your activities“

Rewards:

- Watches
- Payments
- Leave

Transfer:

- To a new unit
- Business trip abroad



MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.001] Command and Scripting Interpreter: PowerShell
- [T1059.003] Command and Scripting Interpreter: Windows Command Shell
- [T1059.005] Command and Scripting Interpreter: Visual Basic
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Defense Evasion [TA0005]
- [T1140] Deobfuscate/Decode Files or Information
- [T1564.003] Hide Artifacts: Hidden Window
- [T1036] Masquerading
- [T1553.005] Subvert Trust Controls: Mark-of-the-Web Bypass

Collection [TA0009]
- [T1560.001] Archive Collected Data: Archive via Utility
- [T1119] Automated Collection

Command and Control [TA0011]
- [T1071.001] Application Layer Protocol: Web Protocols
- [T1105] Ingress Tool Transfer
- [T1095] Non-Application Layer Protocol

https://cert.gov.ua/article/6278521

UAC-0020

The group's activities are conducted by personnel from law enforcement agencies in temporarily occupied Luhansk. These are essentially traitors who have sided with the occupier, similar to the **UAC-0010** group. The last significant activity of this group that we observed was in March 2022.

Victims received an email purportedly containing technical specifications of a new weapons system, with an attachment in the form of a password-protected archive named «туррель.фоп.вовчок.rar» Inside the archive was an RARSFX archive titled «туррель.фоп.вовчок.sfx.rar.scr» which included a decoy file "Wowchok.pdf," an EXE installer "sync.exe," and a BAT file "run_user.bat."

As in previous attacks, they used the SPECTR malware to gather data (documents, files, passwords, and other information). However, for data exfiltration they utilized the synchronization functionality of legitimate software—SyncThing—this time.

https://cert.gov.ua/article/6279600

MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.007] Command and Scripting Interpreter: JavaScript
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1053.005] Scheduled Task/Job: Scheduled Task

Defense Evasion [TA0005]
- [T1036.007] Masquerading: Double File Extension

Credential Access [TA0006]
- [T1528] Steal Application Access Token
- [T1539] Steal Web Session Cookie

Collection [TA0009]
- [T1119] Automated Collection
- [T1074.001] Data Staged: Local Data Staging
- [T1005] Data from Local System

- [T1025] Data from Removable Media
- [T1113] Screen Capture

Command and Control [TA0011]
- [T1071.001] Application Layer Protocol: Web Protocols
- [T1090.003] Proxy: Multi-hop Proxy
- [T1090.004] Proxy: Domain Fronting

Exfiltration [TA0010]
- [T1020] Automated Exfiltration
- [T1048] Exfiltration Over Alternative Protocol

UAC-0006. PLAY, PAUSE, REPLAY

At the beginning of the first half of 2024, the mass phishing campaigns, which started in May 2023 and were carried out by the financially motivated group **UAC-0006**, continued campaigns were primarily targeted at employees within the financial departments of various organizations.

The attackers used polyglot archives (which contained different content depending on the software used to open them) to deliver the SmokeLoader malware onto the computers of accountants. Notably, the configuration of this loader specified several domain names, most of which did not have A-records, meaning they were not registered.

Using SmokeLoader, the hackers installed other malware from their arsenal, such as TALESHOT, which captures screenshots whenever a window related to a banking application is open, including a browser window with the web version of banking app, and transmits these screenshots to the attackers. Depending on their interest in a specific computer, based on the analysis of the collected data, **UAC-0006** deployed a setup consisting of RMS + LOADERX3 + RDPWRAPPER, granting them interactive access to the computer (alongside the legitimate user), thus enabling a more detailed analysis of the victim. The final step involved creating an invoice or editing an existing one.

This wave of cyberattacks, which began in 2023, concluded in March 2024.

However, after a two-month break, much like the previous year, UAC-0006 returned in May. In addition to launching new phishing campaigns to gain fresh victims, they registered the domains that had been part of previous SmokeLoader configurations, enabling them to regain control over computers that had been previously infected.

For the reporting period, in collaboration with the Cyber Incident Response Operations Center of the State Cyber Protection Center (SOC SCPC), 251 cyber incidents related to this group's activities were handled. 36% of them were detected by the tools of SOC SCPC.

https://cert.gov.ua/article/6279366

MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.001] Command and Scripting Interpreter: PowerShell
- [T1059.003] Command and Scripting Interpreter: Windows Command Shell
- [T1059.005] Scheduled Task/Job: Scheduled Task
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

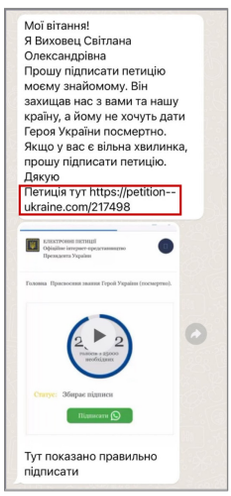
Defense Evasion [TA0005]
- [T1562.004] Impair Defenses: Disable or Modify System Firewall
- [T1036] Masquerading
- [T1036.007] Masquerading: Double File Extension
- [T1027.010] Obfuscated Files or Information: Command Obfuscation
- [T1553.005] Subvert Trust Controls: Mark-of-the-Web Bypass

Command and Control [TA0011]
- [T1071.001] Application Layer Protocol: Web Protocols
- [T1105] Ingress Tool Transfer
- [T1095] Non-Application Layer Protocol

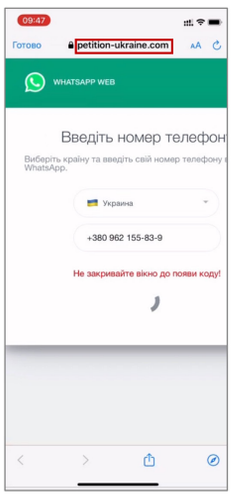
VOTING IN MESSENGERS: A NEW METHOD FOR ACCOUNT THEFT

WhatsApp and access widely popular among Ukrainians. They are used for communication, quickly learning the latest news, or spreading specific information. This popularity has made these messengers a prime target for Russian hackers this spring.

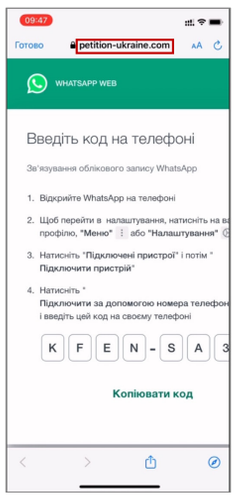
The **UAC-0195** group has focused its attacks on gaining access to the messengers of Ukrainian citizens, employing a “spray & pray” tactic for maximum spread and infection. The objectives of these attacks include stealing passwords, gaining access to email accounts and files, conducting espionage (stealing data from chats), further spreading malware through phishing (to increase the number of victims), and financial exploitation (scamming money).



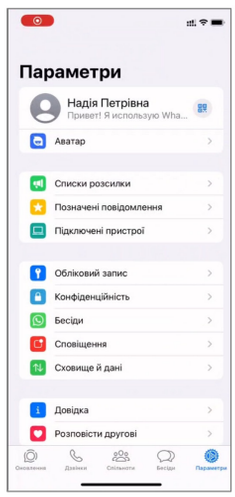
The attacker sends a message with a link and a video guide



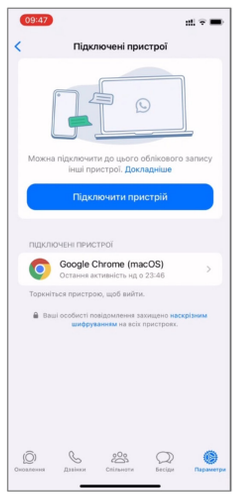
The victim **clicks** on the link and enters their phone number



The attacker's website initiates a request to WhatsApp and receives a code



The victim **opens** WhatsApp settings "Linked Devices"



The victim **clicks** "Link Device"

The victim **enters** the previously received code. The WhatsApp account is compromised

The first wave involved stealing WhatsApp accounts. The hackers used the pretext of signing a petition on the President’s website to award the title of ”Hero of Ukraine“ to a fallen defender. They directed people to a site that mimicked the official website of the President of Ukraine, where users were required to ”authenticate“ via WhatsApp to sign the petition, resulting in the addition of a hacker’s device to the victim’s account. A video tutorial of the necessary steps was even attached to the message.

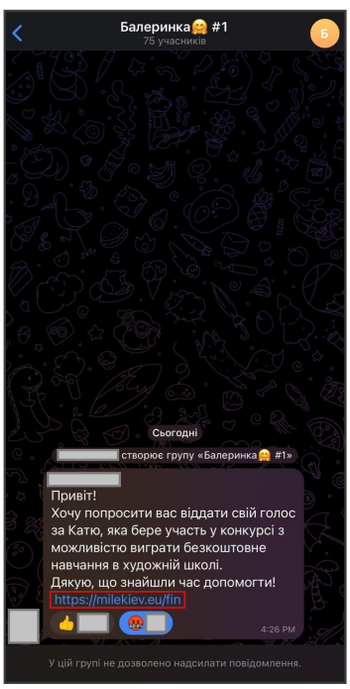
https://cert.gov.ua/article/6278735

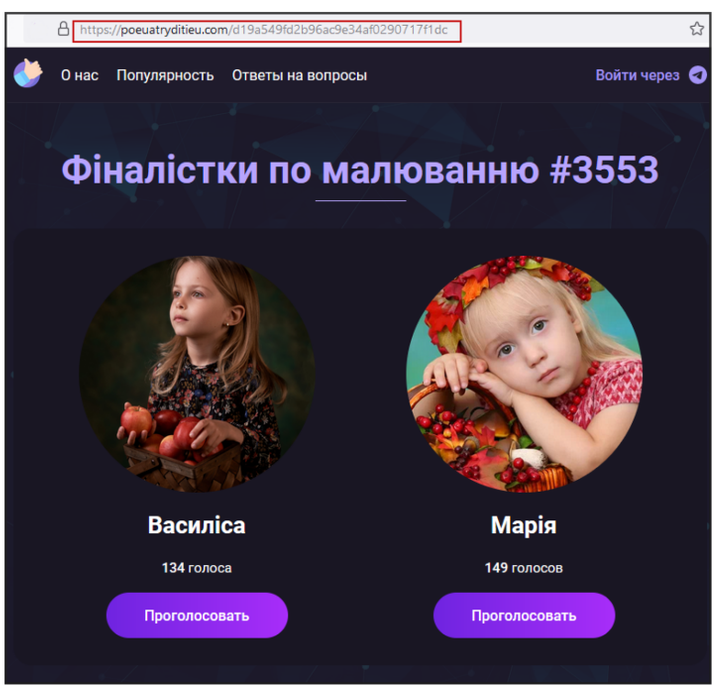
The second wave targeted Telegram users. This time, the pretext was voting for a child participating in an art competition.

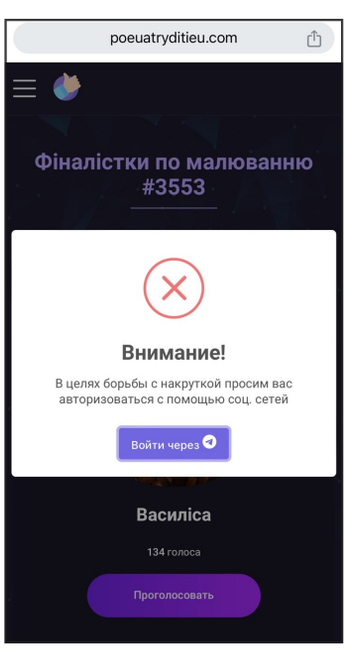
Again, users were asked to “authenticate” via the messenger to cast their vote, which also resulted in the addition of a hacker’s device.

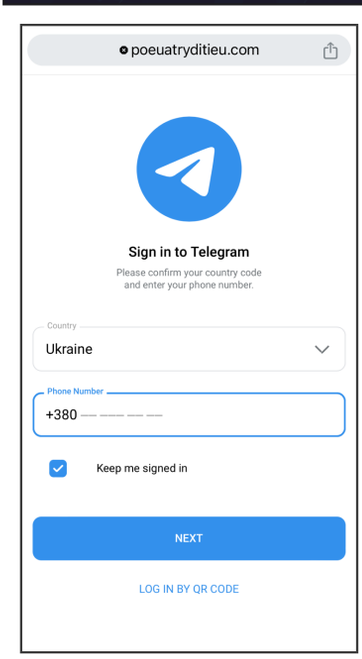
Given the number of domain names registered for use in these cyberattacks and the known number of victims, this threat is extremely widespread and remains active.

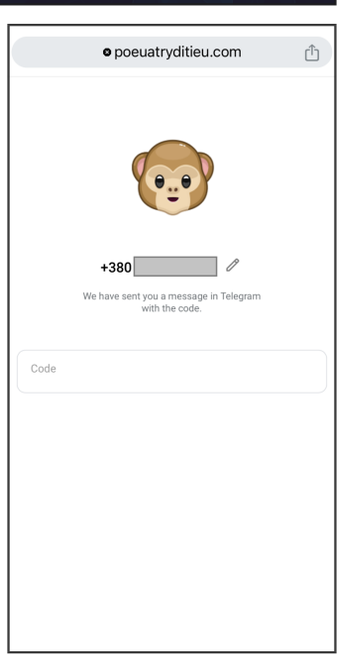
https://cert.gov.ua/article/6279491











MITRE ATT&CK

Resource Development [TA0042]
- [T1583.001] Acquire Infrastructure: Domains
- [T1586.001] Compromise Accounts: Social Media Accounts

Initial Access [TA0001]
- [T1566.002] Phishing: Spearphishing Link

Persistence [TA0003]
- [T1098.005] Account Manipulation: Device Registration

UAC-0002 REENTRY INTO ENERGY COMPANIES' NETWORKS VIA SUPPLY CHAIN ATTACK

In March 2024, we detected a breach within one of the energy companies. A thorough investigation of this cyber incident provided us with indicators and leads to identify other victims, as the initial infection occurred through a shared service provider (a commercial company).

It was revealed that the **UAC-0002** had once again attempted a destructive attack against nearly 20 Ukrainian energy infrastructure entities, including power, heat, and water supply facilities.

Targeting such a large number of organizations individually is a challenging task. Therefore, this time, they executed a supply chain attack, targeting at least three supply chains simultaneously. This conclusion was drawn from the fact that in some cases, the initial unauthorized access correlated with the installation of specialized software containing backdoors and vulnerabilities, while in others, the attackers compromised employees' accounts of the service provider who routinely had access to the Industrial Control Systems (ICS) of organizations for maintenance and technical support.

During the investigation of this cyber incident on Linux-based systems where the specialized software was installed, we discovered malware known as

LOADGRIP and BIASBOAT. The last of them is an analog of the QUEUESEED backdoor (also known as KNUCKLETOUCH, ICYWELL, WRONGSENS, KAPEKA), which was found during the investigation of destructive cyberattacks by **UAC-0133** (a subcluster of **UAC-0002**) on water supply facilities, particularly involving the use of SDELETE. All victims shared the use of the same software, which served as the initial vector of compromise.

Given the operation of these specialized software systems within the ICS of targeted objects, the attackers utilized them for lateral movement and escalation of the cyberattack against the corporate networks of the organization. For example on such systems, pre-created PHP web shells like WEEVELY, the PHP tunnel REGEORG.NEO, or PIVOTNACCI were found in specialized software directories.

It is likely that the unauthorized access to the ICS of a significant number of energy, heat, and water supply facilities was intended to amplify the impact of missile strikes on Ukraine's infrastructure in the spring of 2024.

CONCLUSIONS

The trend observed in the previous half-year—namely, an increase in the overall number of cyber incidents accompanied by a decrease in high and critical severity incidents — continues to hold. Thanks to the diligent efforts of Ukraine's cybersecurity entities, collaboration with vendors and partners, the deployment of modern technologies, and a reduction in the attack surface, significant progress has been made in minimizing risks and enhancing the protection of many key systems.

However, the capabilities of hackers are continually growing, and we must also continue to improve. Increasing the security of Industrial Control Systems (ICS) and raising awareness among all citizens without exception are key aspects that require ongoing attention.

The war persists, and cyberspace remains a battlefield in its own right. The enemy is determined to gather intelligence by any means necessary, leading us to believe that cyberattacks targeting military personnel and government bodies will remain prevalent. Phishing and malware infections are the primary tools of cyber espionage, with human behavior being the weakest link. Therefore, the primary means of cybersecurity must focus on continuously raising citizens' awareness of fundamental cyber hygiene practices and current cyber threats.

Another direction for the enemy is to destabilize the country's situation. To destroy civilian critical infrastructure (particularly energy facilities), the enemy employs not only kinetic attacks but also destructive cyberattacks. These are less costly than launching a ballistic missile yet can lead to equally devastating consequences. Thus, terrorist cyber operations against critical infrastructure are unlikely to cease. Following the standard requirements published on the CERT-UA website (https://cert.gov.ua/article/5436463) is the minimum necessary foundation for ensuring the protection of ICS from cyberattacks.

Lastly, cyber looters—those fraudsters who will always be around—pose a constant threat. While it's hard to predict what theme or platform they will choose next to scam people out of money or steal their banking information, one thing is certain: we will continue to hear about them for a long time to come.

Let us remain conscious and responsible. Together toward Victory. Glory to Ukraine!

PREVIOUS REPORTS

To provide a complete picture and understanding of the transformations in cyber capabilities during the full-scale war, previous analytical reports are available at the following links:

1. Russia's Cyber Tactics: H2'2022-EN

2. Russia's Cyber Tactics H1'2023-EN

3. Russia's Cyber Tactics H2'2023-EN

For more information, subscribe here:
Media Contact Center
press@cip.gov.ua

STAY CONNECTED:

https://twitter.com/SSSCIP

https://twitter.com/_CERT_UA

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

RUSSIAN CYBER OPERATIONS

APT Activity Report H1 2024

State Service
of Special Communications
and Information
Protection of Ukraine