Proprietary + Confidential

Disinfo & Disruption

Alden Wahlstrom, Senior Analyst, Mandiant
Gabby Roncone, Senior Analyst, Mandiant

EU Disinfo 2023

October 2023

Acknowledgements

- Mandiant Research Team
- Mandiant Cyber Espionage Team
- Consultants on Ukraine engagements
- Russia Fusion Cell & Pokemon Masters
- CERT-UA
- Security Service of Ukraine (Cyber department)

Disclaimer

Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.

Agenda

01 The GRU Playbook

02 Telegraphing “Success”

03 Case Study: Solntsepek

04 Conclusions

05 Questions

01

The GRU Playbook

Throughout the war in Ukraine, we have observed distinct patterns of **strategic and tactical cyber- and cyber-enabled IO activity** that enable generic, flexible, and survivable operations. We've deemed these patterns **the GRU's Disruptive Playbook**

The GRU Playbook: A simple, repeatable playbook

Generic

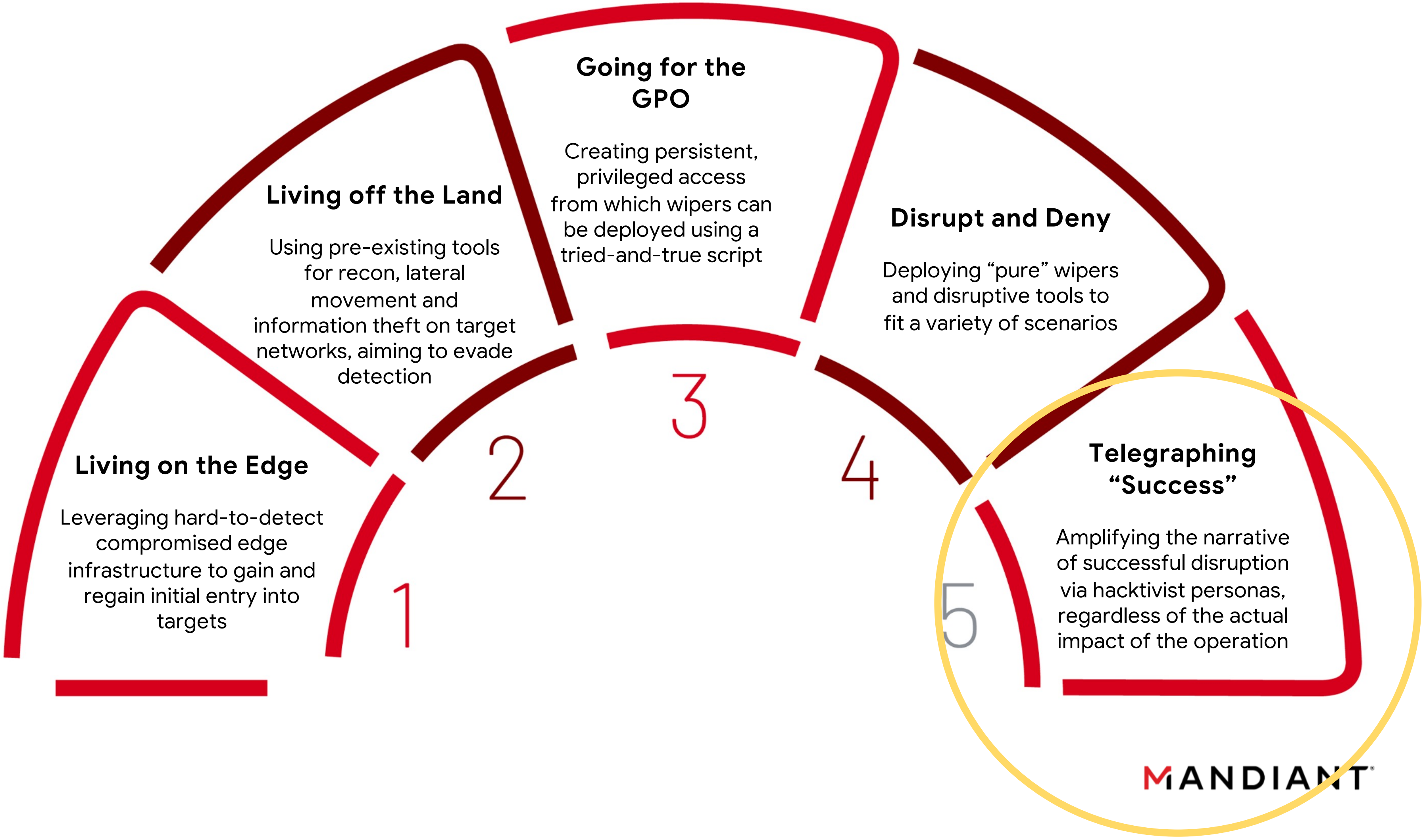
Provides options for a wide range of potential targets

Flexible

Reusable across different tool deployments

Survivable

Difficult to detect; disrupt through countermeasures



Living on the Edge

Leveraging hard-to-detect compromised edge infrastructure to gain and regain initial entry into targets

Living off the Land

Using pre-existing tools for recon, lateral movement and information theft on target networks, aiming to evade detection

Going for the GPO

Creating persistent, privileged access from which wipers can be deployed using a tried-and-true script

Disrupt and Deny

Deploying "pure" wipers and disruptive tools to fit a variety of scenarios

Telegraphing "Success"

Amplifying the narrative of successful disruption via hacktivist personas, regardless of the actual impact of the operation

MANDIANT

02

Telegraphing “Success”

When a Cyber Attack isn’t Enough

Compounding effects needed

Disruptive attacks may only achieve temporary effects as organizations quickly engage remediation efforts

Reaching the right audience

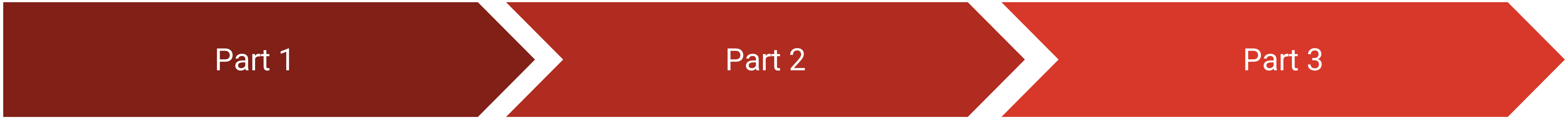
Isolated disruptive attacks may not have psychological effects beyond the organization targeted

Everybody makes mistakes

Disruptive attacks may not even be successful, thus failing to achieve any psychological effect

Telegraphing Success

January 2020 – February 2023



Part 1

Part 2

Part 3

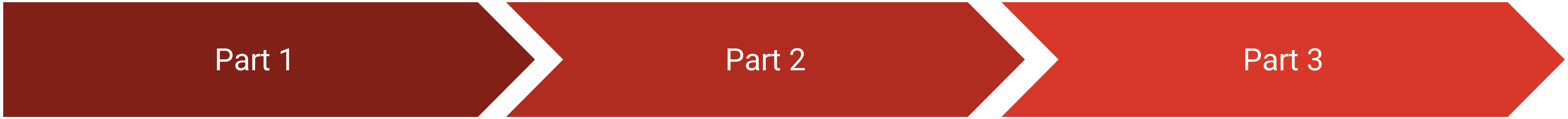
Claim **compromise of target** organization via Telegram channel

Promote purportedly **leaked data as evidence** and the narratives related to the operation

... profit?

Telegraphing Success

April 2023 - Now



Part 1

Part 2

Part 3

Claim **compromise of target** organization via Telegram channel

Promote purportedly **leaked data as evidence** and the narratives related to the operation

Deface website with further promoting the operation’s occurrence and the associated narrative

03

Solntsepek

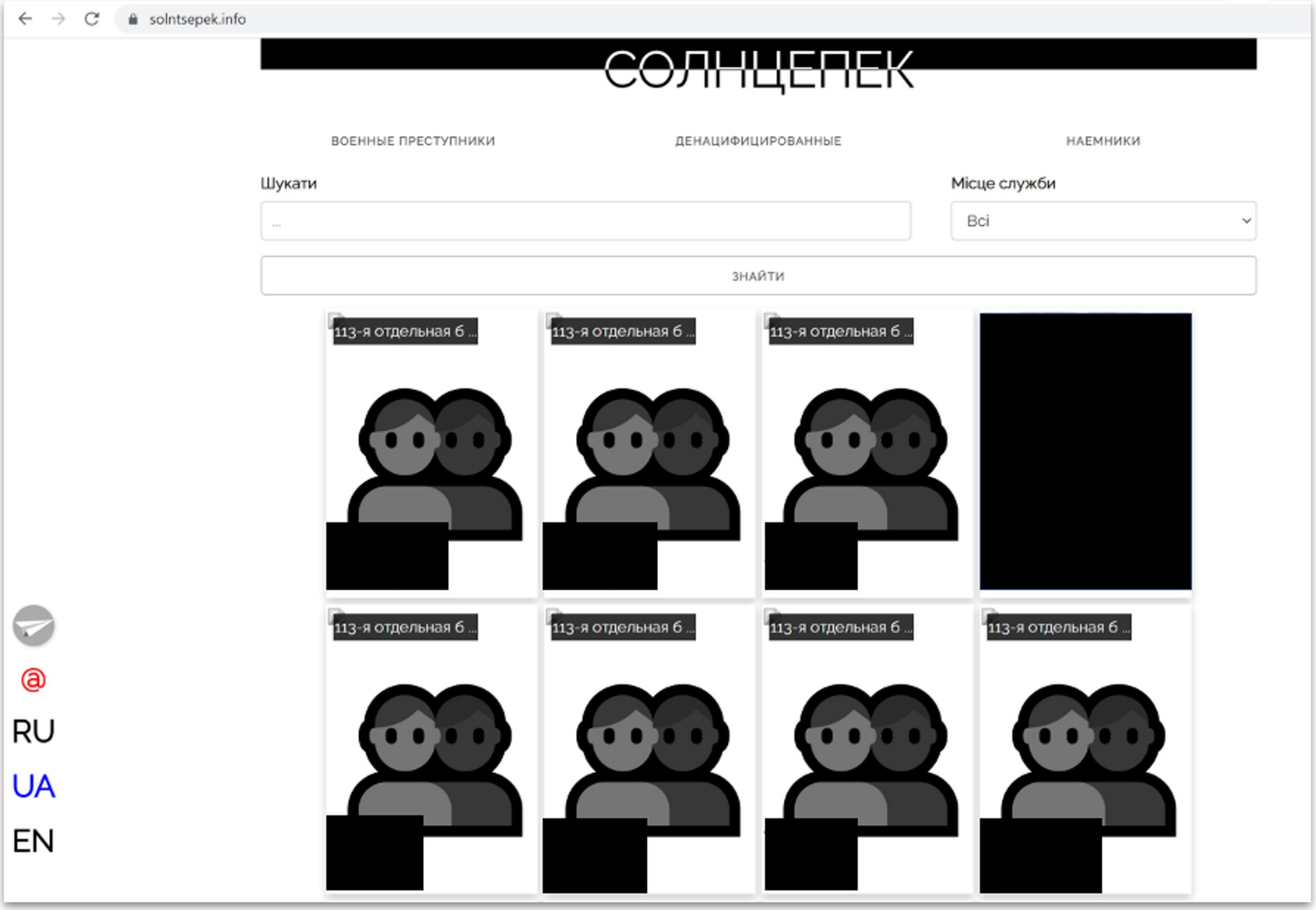
Enter Solntsepek

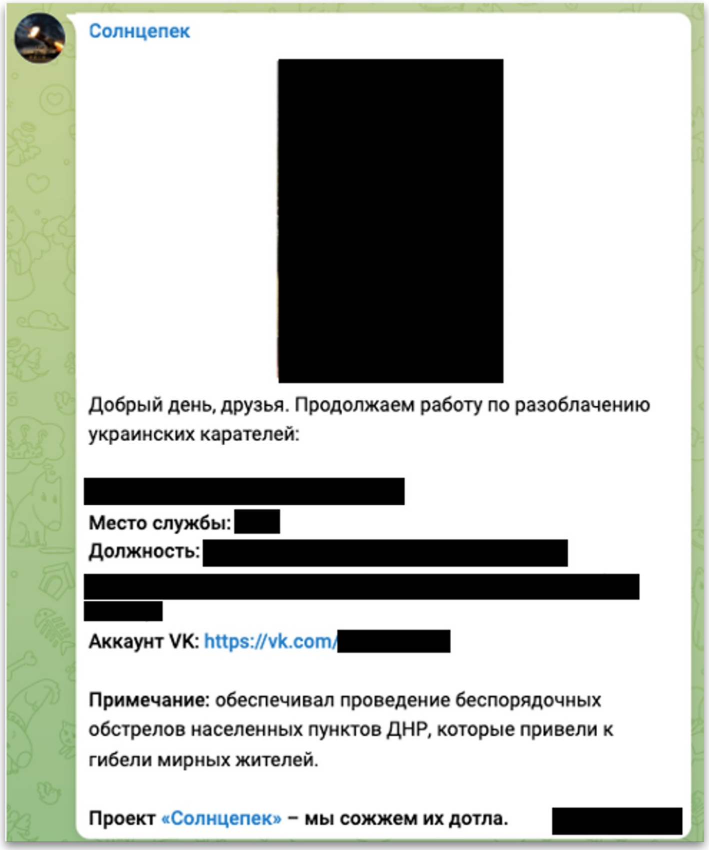
Solntsepek (Солнцепек) is a pro-Russia hacktivist group that has claimed multiple attacks against Ukrainian entities. The group takes its name from a website and Telegram channel maintained by its operators, which is dedicated to doxing members of the Ukrainian military and security services.

- The doxing website and Telegram channel were launched in late Spring / early Summer 2022 in response to the Russian invasion of Ukraine; and it began claiming compromises at least as early as Spring 2023.
- "Solntsepek" is a reference to a Soviet-designed weapons system, the TOS-1 heavy flamethrower.
- Since April 2023, Solntsepek has conducted at least 11 operations involving claimed compromises targeting Ukrainian entities.
- The group's targets include government entities, key service providers like ISPs and energy, and media organizations.
- Narratives promoted by the group include anti-Ukrainian rhetoric, with themes such as alleging Ukrainian government incompetence or corruption; such as narratives repeatedly targeting CERT-UA.

Mandiant has **not attributed** Solntsepek to a specific actor or activity set.

Solntsepek (Солнцепек)


solntsepek.info
СОЛНЦЕПЕК
ВОЕННЫЕ ПРЕСТУПНИКИ
ДЕНАЦИФИЦИРОВАННЫЕ
НАЕМНИКИ
Шукати
...
Місце служби
Всі
ЗНАЙТИ
113-я отдельная б ... [redacted]
113-я отдельная б ... [redacted]
113-я отдельная б ... [redacted]
[redacted]
113-я отдельная б ... [redacted]
113-я отдельная б ... [redacted]
113-я отдельная б ... [redacted]
113-я отдельная б ... [redacted]
@
RU
UA
EN


Солнцепек

[redacted]

Добрый день, друзья. Продолжаем работу по разоблачению украинских карателей:

[redacted]

Место службы: [redacted]
Должность: [redacted]

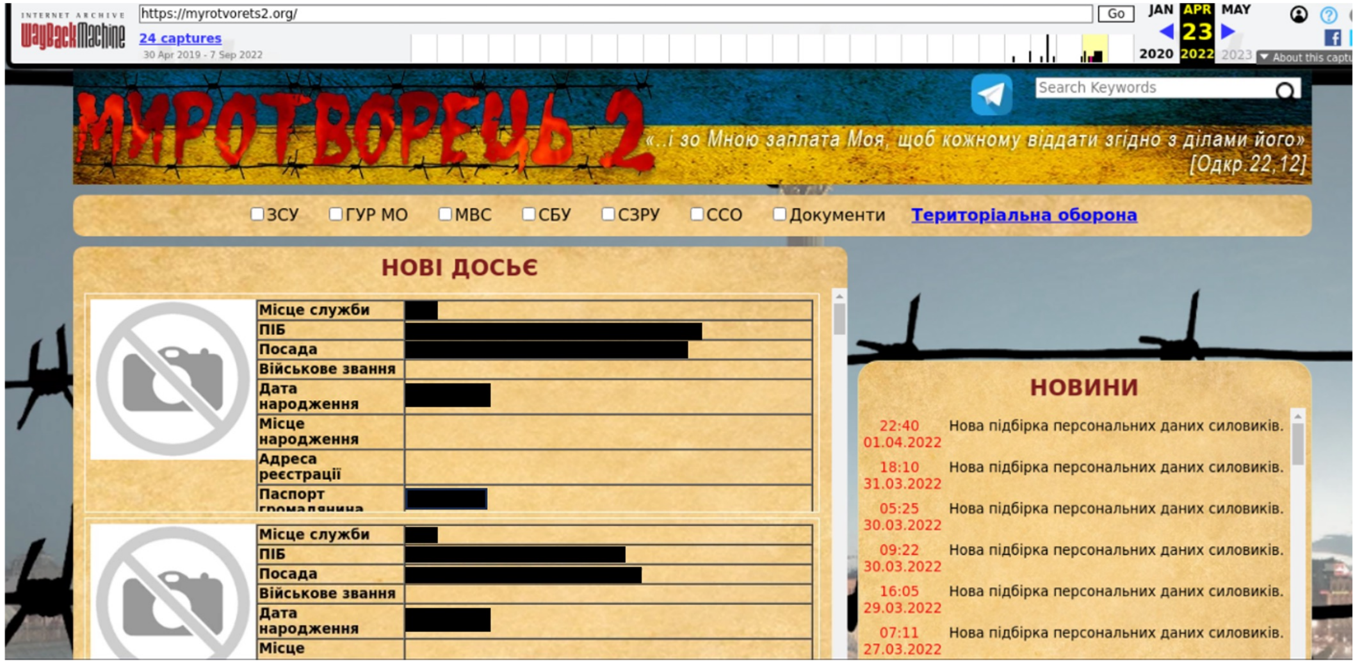
[redacted]

Аккаунт VK: https://vk.com/[redacted]

Примечание: обеспечивал проведение беспорядочных обстрелов населенных пунктов ДНР, которые привели к гибели мирных жителей.

Проект «Солнцепек» – мы сожжем их дотла. [redacted]

Leveraging Established IO Assets



«..і зо Мною заплата Моя, щоб кожному віддати згідно з ділами його» [Одкр.22,12]

□ЗСУ □ГУР МО □МВС □СБУ □СЗРУ □ССО □Документи **Територіальна оборона**

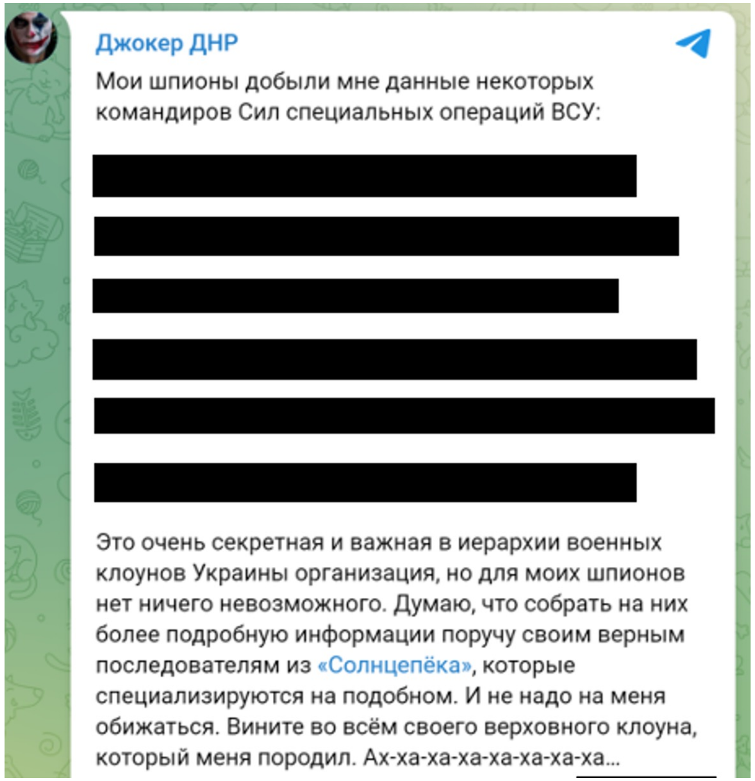
НОВІ ДОСЬЄ

Місце служби	[redacted]
ПІБ	[redacted]
Посада	[redacted]
Військове звання	
Дата народження	[redacted]
Місце народження	
Адреса реєстрації	
Паспорт громадянина	[redacted]

Місце служби	[redacted]
ПІБ	[redacted]
Посада	[redacted]
Військове звання	
Дата народження	[redacted]
Місце	

НОВИНИ

22:40 01.04.2022	Нова підбірка персональних даних силовиків.
18:10 31.03.2022	Нова підбірка персональних даних силовиків.
05:25 30.03.2022	Нова підбірка персональних даних силовиків.
09:22 30.03.2022	Нова підбірка персональних даних силовиків.
16:05 29.03.2022	Нова підбірка персональних даних силовиків.
07:11 27.03.2022	Нова підбірка персональних даних силовиків.

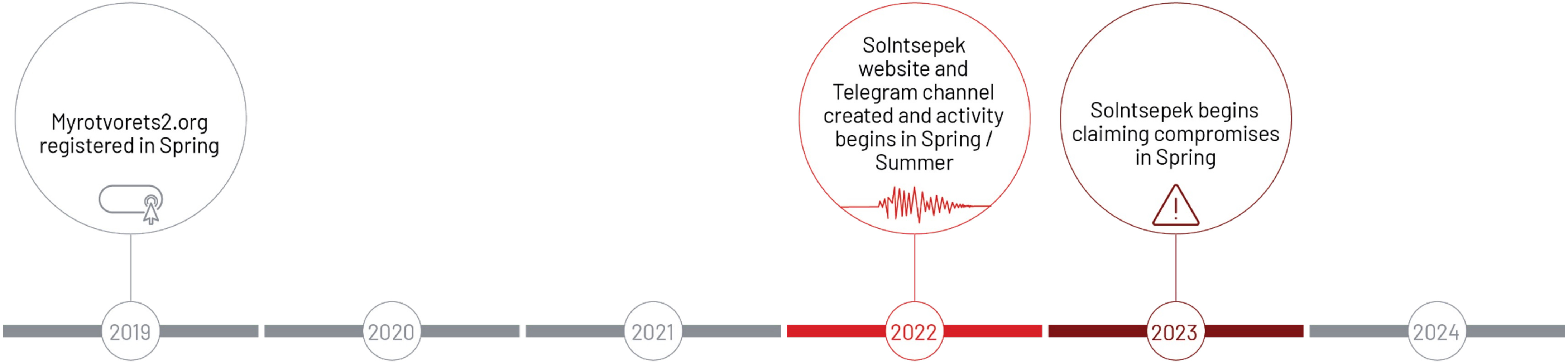


Джокер ДНР

Мои шпионы добыли мне данные некоторых командиров Сил специальных операций ВСУ:

[redacted]

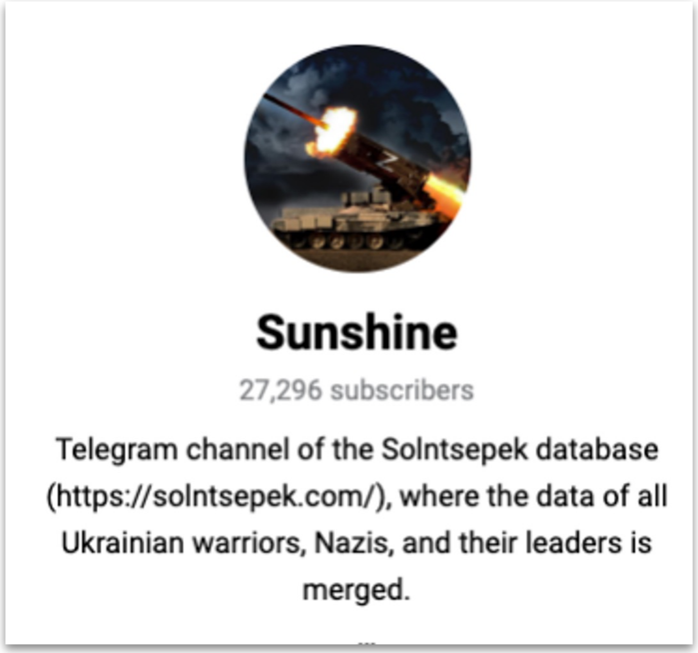
Это очень секретная и важная в иерархии военных клоунов Украины организация, но для моих шпионов нет ничего невозможного. Думаю, что собрать на них более подробную информации поручу своим верным последователям из «Солнцепёка», которые специализируются на подобном. И не надо на меня обижаться. Винипе во всём своего верховного клоуна, который меня породил. Ах-ха-ха-ха-ха-ха-ха-ха...



Myrotvorets2.org registered in Spring

Solntsepek website and Telegram channel created and activity begins in Spring / Summer

Solntsepek begins claiming compromises in Spring

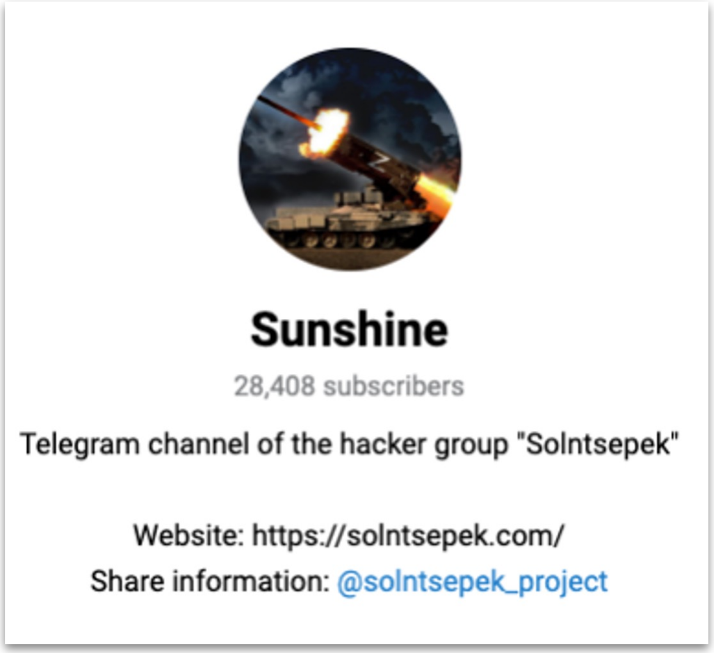


Sunshine

27,296 subscribers

Telegram channel of the Solntsepek database (https://solntsepek.com/), where the data of all Ukrainian warriors, Nazis, and their leaders is merged.

Rebrand



Sunshine

28,408 subscribers

Telegram channel of the hacker group "Solntsepek"

Website: https://solntsepek.com/
Share information: @solntsepek_project

* Images are machine translated from Russian

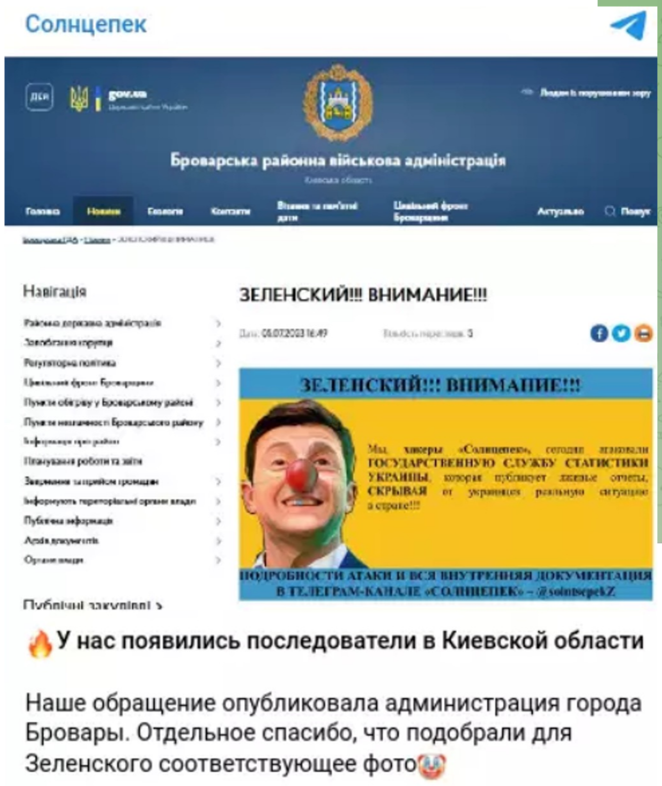
July 5: Solntsepek Claims Attack on the State Statistics Service of Ukraine

ZELENSKY!!! ATTENTION!!!

We, Solntsepek hackers, today attacked **the State Statistics Service of Ukraine** , which publishes false reports, **HIDING** the real situation in the country from Ukrainians. In addition, Ukrstat maintains **statistics of the male population of military age** and transfers it to Ukrainian military registration and enlistment offices for the implementation of mobilization activities.

We destroyed the department's domain controllers and servers, erased information from all computers of the organization's employees and managers, including the statistical database. Our attack disrupted the process of replenishing that part of the Ukrainian Armed Forces personnel who died in the senseless "counter-offensive."
We post INTERNAL DOCUMENTATION

* Excerpt from Telegram post machine translated from Russian


Солнцепек
ДІЯ
gov.ua
Броварська районна військова адміністрація
Київська область
Головна
Новини
Екологія
Контакти
Візити та пам'ятні дати
Цивільний фронт Броварщини
Актуально
Пошук
Навігація
Районна державна адміністрація
Запобігання корупції
Регуляторна політика
Цивільний фронт Броварщини
Пункти обігріву у Броварському районі
Пункти незламності Броварського району
Інформація про район
Планування роботи та звіти
Звернення за громадян
Інформують територіальні органи влади
Публічна інформація
Архів документів
Органи влади
Публічні закупівлі ›

ЗЕЛЕНСКИЙ!!! ВНИМАНИЕ!!!

Дата: 05.07.2023 16:49

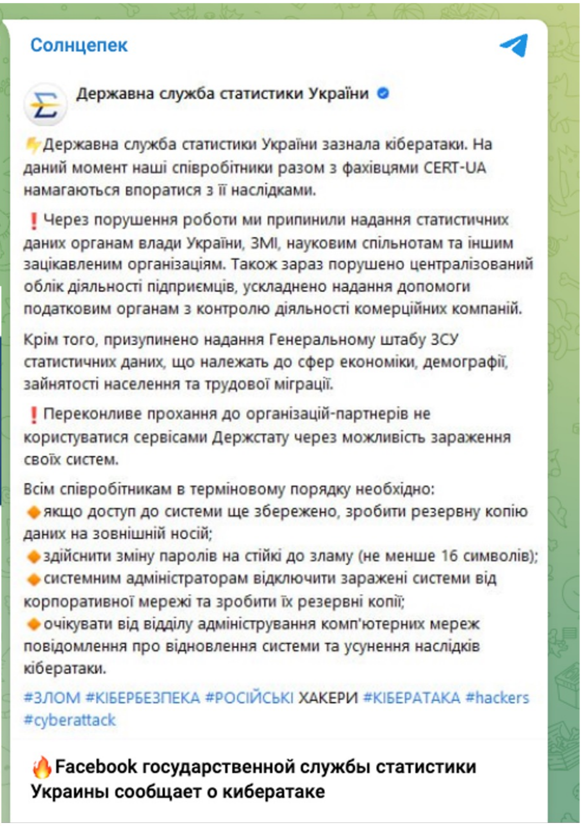
ЗЕЛЕНСКИЙ!!! ВНИМАНИЕ!!!

Мы, хакеры «Солнцепек», сегодня атаковали ГОСУДАРСТВЕННУЮ СЛУЖБУ СТАТИСТИКИ УКРАИНЫ, которая публикует ложные отчеты, СКРЫВАЯ от украинцев реальную ситуацию в стране!!!

ПОДРОБНОСТИ АТАКИ И ВСЯ ВНУТРЕННЯЯ ДОКУМЕНТАЦИЯ В ТЕЛЕГРАМ-КАНАЛЕ «СОЛНЦЕПЕК» – @solntsepekZ

🔥У нас появились последователи в Киевской области

Наше обращение опубликовала администрация города Бровары. Отдельное спасибо, что подобрали для Зеленского соответствующее фото🤡



Державна служба статистики України

⚡Державна служба статистики України зазнала кібератаки. На даний момент наші співробітники разом з фахівцями CERT-UA намагаються впоратися з її наслідками.

❗Через порушення роботи ми припинили надання статистичних даних органам влади України, ЗМІ, науковим спільнотам та іншим зацікавленим організаціям. Також зараз порушено централізований облік діяльності підприємців, ускладнено надання допомоги податковим органам з контролю діяльності комерційних компаній.

Крім того, призупинено надання Генеральному штабу ЗСУ статистичних даних, що належать до сфер економіки, демографії, зайнятості населення та трудової міграції.

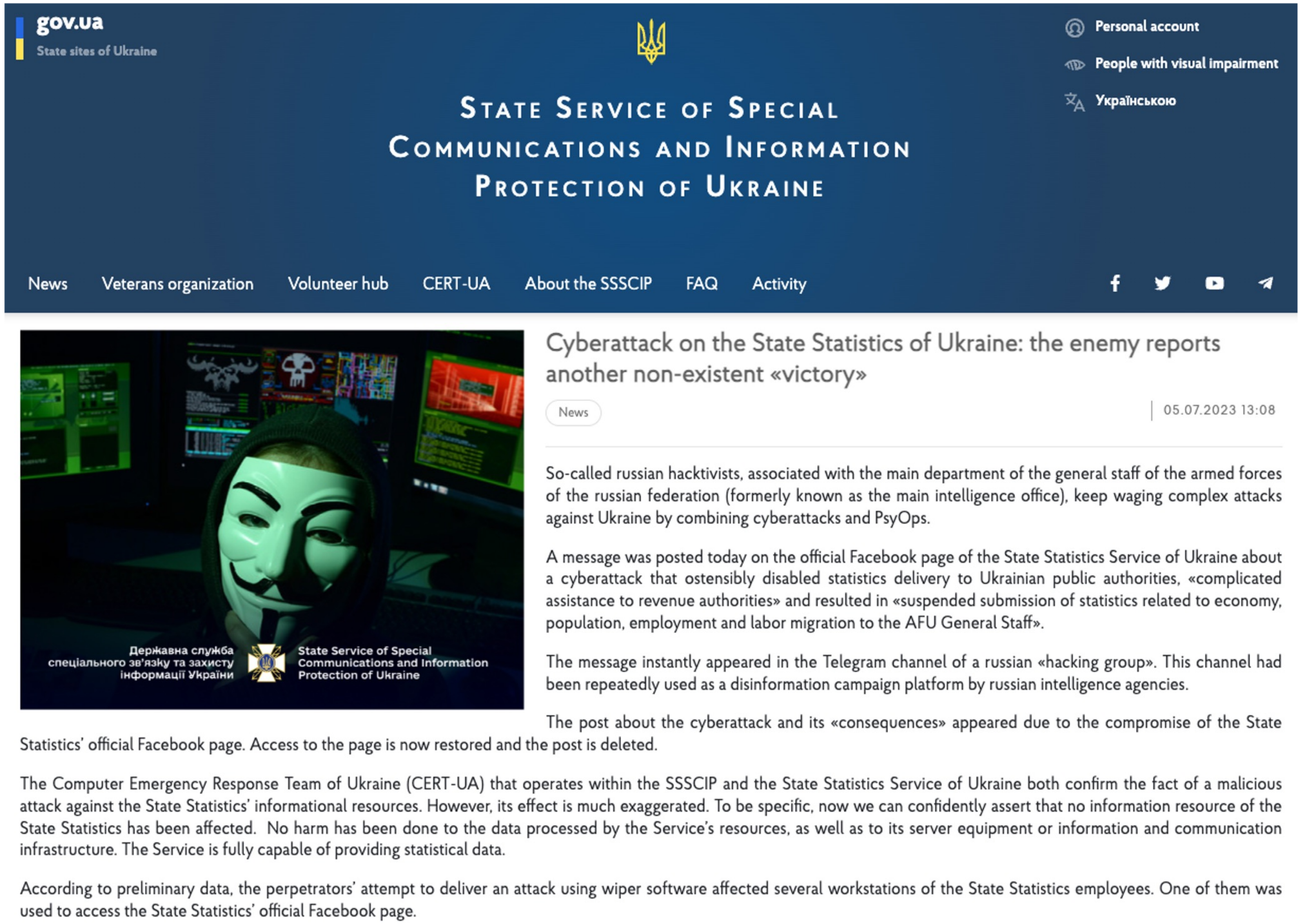
❗Переконливе прохання до організацій-партнерів не користуватися сервісами Держстату через можливість зараження своїх систем.

Всім співробітникам в терміновому порядку необхідно:
🔶якщо доступ до системи ще збережено, зробити резервну копію даних на зовнішній носій;
🔶здійснити зміну паролів на стійкі до зламу (не менше 16 символів);
🔶системним адміністраторам відключити заражені системи від корпоративної мережі та зробити їх резервні копії;
🔶очікувати від відділу адміністрування комп'ютерних мереж повідомлення про відновлення системи та усунення наслідків кібератаки.

#ЗЛОМ #КІБЕРБЕЗПЕКА #РОСІЙСЬКІ ХАКЕРИ #КІБЕРАТАКА #hackers #cyberattack

🔥**Facebook государственной службы статистики Украины сообщает о кибератаке**

Hacktivism: the Art of ~~Under~~Overstatement



gov.ua
State sites of Ukraine
Personal account
People with visual impairment
Українською
News
Veterans organization
Volunteer hub
CERT-UA
About the SSSCIP
FAQ
Activity
Державна служба спеціального зв'язку та захисту інформації України
State Service of Special Communications and Information Protection of Ukraine

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE

Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent «victory»

News | 05.07.2023 13:08

So-called russian hacktivists, associated with the main department of the general staff of the armed forces of the russian federation (formerly known as the main intelligence office), keep waging complex attacks against Ukraine by combining cyberattacks and PsyOps.

A message was posted today on the official Facebook page of the State Statistics Service of Ukraine about a cyberattack that ostensibly disabled statistics delivery to Ukrainian public authorities, «complicated assistance to revenue authorities» and resulted in «suspended submission of statistics related to economy, population, employment and labor migration to the AFU General Staff».

The message instantly appeared in the Telegram channel of a russian «hacking group». This channel had been repeatedly used as a disinformation campaign platform by russian intelligence agencies.

The post about the cyberattack and its «consequences» appeared due to the compromise of the State Statistics' official Facebook page. Access to the page is now restored and the post is deleted.

The Computer Emergency Response Team of Ukraine (CERT-UA) that operates within the SSSCIP and the State Statistics Service of Ukraine both confirm the fact of a malicious attack against the State Statistics' informational resources. However, its effect is much exaggerated. To be specific, now we can confidently assert that no information resource of the State Statistics has been affected. No harm has been done to the data processed by the Service's resources, as well as to its server equipment or information and communication infrastructure. The Service is fully capable of providing statistical data.

According to preliminary data, the perpetrators' attempt to deliver an attack using wiper software affected several workstations of the State Statistics employees. One of them was used to access the State Statistics' official Facebook page.

04

Conclusions

IO in the GRU Playbook

Cyber & IO: better together

The GRU favors this combination in concert with disruptive attacks during wartime

Manifesting “success”

Influence designed to look successful rather than be successful

Multi-level operations in a wartime attention economy

Enhanced IO components can increase perception of threat activity and expand audience size for associated messaging

05

Questions?

Thank you!