

## UPD. Ответственность за атаку на «Киевстар» взяли российские хакеры. Рассказываем, что такое «Солнцепёк» и кто за ним стоит

Archived: 2026-04-05 19:50:58 UTC

Хакерская группа из России «Солнцепёк» взяла на себя ответственность за вчерашнюю мощную атаку на «Киевстар». Ранее они атаковали «Суспільне», провайдеров и Минразвития общин.

Мы решили дополнить наш предыдущий материал о связях этой группировки с элитными хакерами из Sandworm, которые подчиняются российским силовикам.

Вчера [в работе «Киевстар», который имеет 24 млн абонентов, произошел масштабный сбой](#), из-за которого не работает связь и сайт оператора. Впоследствии [СРО «Киевстар» подтвердил хакерскую атаку](#) на компанию. Абонентам, которые не имели связи, пообещали компенсацию.

Генеральный директор «Киевстар» Александр Комаров сообщил, что [атака частично разрушила IT-инфраструктуру](#). По словам источников dev.ua, «Киевстар», вероятно, был вынужден самостоятельно отключить свои сервисы [из-за скомпрометированного «критического аккаунта»](#).

Сегодня в Telegram-канале группировки «Солнцепёк» появилось сообщение, в котором они взяли на себя «полную ответственность за кибератаку на Киевстар».

«Мы уничтожили 10 000 компьютеров, более 4000 серверов, все системы облачного хранения данных и резервного копирования. Мы атаковали „Киевстар“, потому что компания обеспечивает связью ВСУ, а также государственные органы и силовые структуры Украины. Остальным конторам, которые помогают ВСУ, приготовиться!», — заявили российские хакеры.

Они также намекнули, что с атакой им помогли «неравнодушные» сотрудники «Киевстар», и опубликовали скриншоты, которые вероятно должны подтвердить причастность «Солнцепёк».

The screenshot shows a web-based database interface for 'MG01 KYIVSTAR.UA'. The main window displays a table with columns: Серийный номер, Партия, Код товара, Кол-во, Статус, БД, Тип подключения, Центр, Местонахождение, STATE\_ID, ИР упр, ИР завед, ИР завед с. The table contains two rows of data for objects NG11050910 and NG11050910. Below the table, there is a section for 'История движений по объекту' with columns: ИД операции, Тип операции, Дата, БД, Центр отправления, Отправитель, БД, Центр получения, Получатель, УП/ИР, ИР/ИР, Тип УП, Тип строки УП. Two rows of operation history are visible, dated 27.09.2023. The interface includes a sidebar with navigation options like 'Создание объектов', 'Объекты', 'История движений по ОИ', and 'История движений по ОИ'. At the bottom, there are search filters and a status bar.

The screenshot shows the 'Active Directory Users and Computers' window. The left pane shows a tree view of the directory structure, including 'Users' and 'Groups'. The main pane displays a list of users and groups with columns for Name, Full Name, and Group. The list includes various organizational units and users, such as 'A.D.S. Assembly Data System S.p.A.', 'Cambridge Broadband Networks Group Ltd CBNG', and 'Fila Perfomax DP SSM'. The interface includes standard Windows menu options like 'File', 'Action', 'View', and 'Help'.

The screenshot shows the System Center Operations Manager interface. The main area displays a list of alerts under the heading "All Alerts (200)". The alerts are sorted by severity and source. A detailed view of an alert is shown at the bottom, titled "Alert Details".

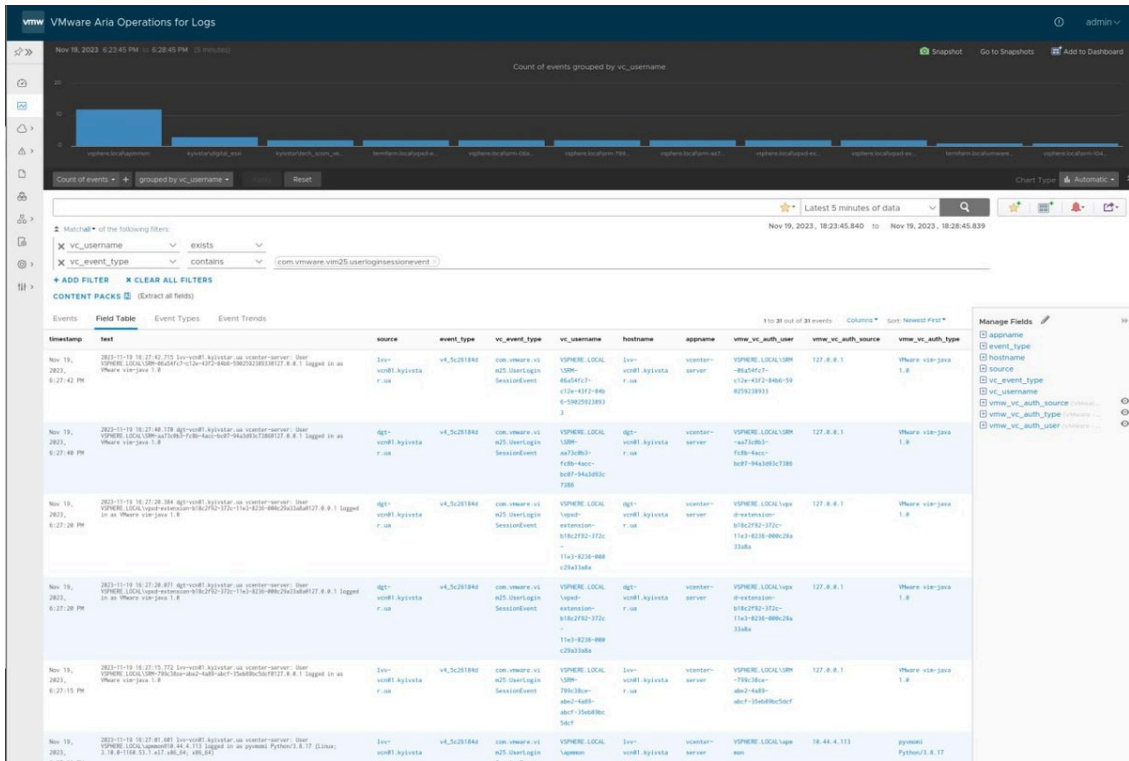
Severity	Source	Name	Resolution State	Created	Age
Critical	ADC-INTERNAL-DGT	ADQ VIP 'PONTIS_VIP' is offline	Assigned To Expert	11/16/2023 8:40:44 PM	1 Hour, 10
Critical	SMS delivery node down 10.48.19.49:8080	Connection Refused	Closed	11/16/2023 8:34:39 PM	1 Hour, 16
Critical	SMS delivery node down 10.48.19.48:8080 TCP Fort Check Group	SMS delivery node down 10.48.19.48:8080 Group Roll-up Monitor	Closed	11/16/2023 8:32:28 PM	1 Hour, 18
Critical	man-d-004	Docker Swarm containers logs rule	Assigned To Expert	11/16/2023 6:01:47 PM	3 Hours, 48
Critical	Mailbox Monitoring Service	Discarded Records in email	Assigned To Expert	11/16/2023 2:20:26 PM	7 Hours, 11
Critical	Cisco - sngn	[Synthetic VPN] TCP Connection Refused	Closed	11/16/2023 2:06:07 PM	7 Hours, 4
Critical	MOBILE APP FOR SELLERS 10.442.137.18080	Connection Refused	Assigned To Expert	11/16/2023 11:22:28 AM	10 Hours, 1
Critical	sdplite-dg2	Log file error	Assigned To Expert	11/16/2023 10:59:12 AM	10 Hours, 1
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/16/2023 10:46:50 AM	11 Hours, 1
Critical	Points SOAP Web Interface	SOAP Request to Points on http://1048.19.109.8080/Points-WebService/services2/Terminals failed	Closed	11/16/2023 9:31:00 AM	12 Hours, 1
Critical	antibot@kyivstar.ua	Agent Unreachable	Closed	11/16/2023 8:26:36 AM	13 Hours, 1
Critical	leaf3201	interface-gig0-3/0-down	Assigned To Expert	11/16/2023 8:22:48 AM	13 Hours, 1
Critical	leaf3207	interface-gig0-down	Assigned To Expert	11/16/2023 8:21:37 AM	13 Hours, 1
Critical	Microsoft Power Automate in Microsoft 365	M365 Services - Status Monitor Alert	Closed	11/16/2023 7:49:01 AM	14 Hours, 1
Critical	Kyivstar MobileSafety	[Digital dashboards] No data in index for service.	Closed	11/16/2023 2:34:42 AM	19 Hours, 1
Critical	DCP Custom Class	Database query returns more than 100 errors	Assigned To Expert	11/16/2023 12:00:01 AM	21 Hours, 1
Critical	NoNoicer\Multiple service problem(SERVICESERROR)	[P-2311659](TT-A5) Multiple service problems. (Route: NoNoicer)	Closed	11/15/2023 5:06:39 PM	1 Day, 4 H
Critical	MK2_App\Response time degradation(SERVICESPERFORMANCE)	[P-2311637](TT-A5) Response time degradation. (Route: MK2_App)	Closed	11/15/2023 6:54:15 PM	1 Day, 4 H
Critical	10.77.16.77	SMP FLUP connection lost	Closed	11/15/2023 4:05:53 PM	1 Day, 5 H
Critical	ApiLayer_App\Response time degradation(SERVICESPERFORMANCE)	[P-2311646](TT-A5) Response time degradation. (Route: ApiLayer_App)	Closed	11/15/2023 2:01:02 PM	1 Day, 7 H
Critical	10.77.16.82	SMP FLUP connection lost	Closed	11/15/2023 1:49:15 PM	1 Day, 8 H
Critical	DB	Security Incident: Category - DB	Closed	11/15/2023 1:31:39 PM	1 Day, 8 H
Critical	ApiLayer_App\Mobile app slow user actions(APPLICATIONERROR)	[P-2311609](TT-A5) Mobile app slow user actions. (Route: ApiLayer_App)	Closed	11/15/2023 10:46:10 AM	1 Day, 11 H
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/15/2023 10:35:39 AM	1 Day, 11 H
Critical	engage-app01	File was failed while uploading to Points	Closed	11/15/2023 9:34:30 AM	1 Day, 12 H
Critical	cad-d801-whg@kyivstar.ua	Agent Unreachable	Closed	11/15/2023 9:02:54 AM	1 Day, 12 H
Critical	leaf1208	interface-gig0-down	Closed	11/15/2023 3:47:48 AM	1 Day, 18 H
Critical	leaf1731	interface-physical-down	Closed	11/15/2023 3:04:18 AM	1 Day, 18 H

**Alert Details**  
**Alert Name:** ADQ VIP 'PONTIS\_VIP' is offline  
**Alert Source:** ADC-INTERNAL-DGT  
**Path:** ADC-INTERNAL-DGT  
**Alert Rule:** FS Telemetry VIP Status Last Rule Repeat.  
**Alert Description:** Device: ADC-INTERNAL-DGT  
 ID: PONTIS\_VIP  
 StatusReason: The children pool member(s) are down

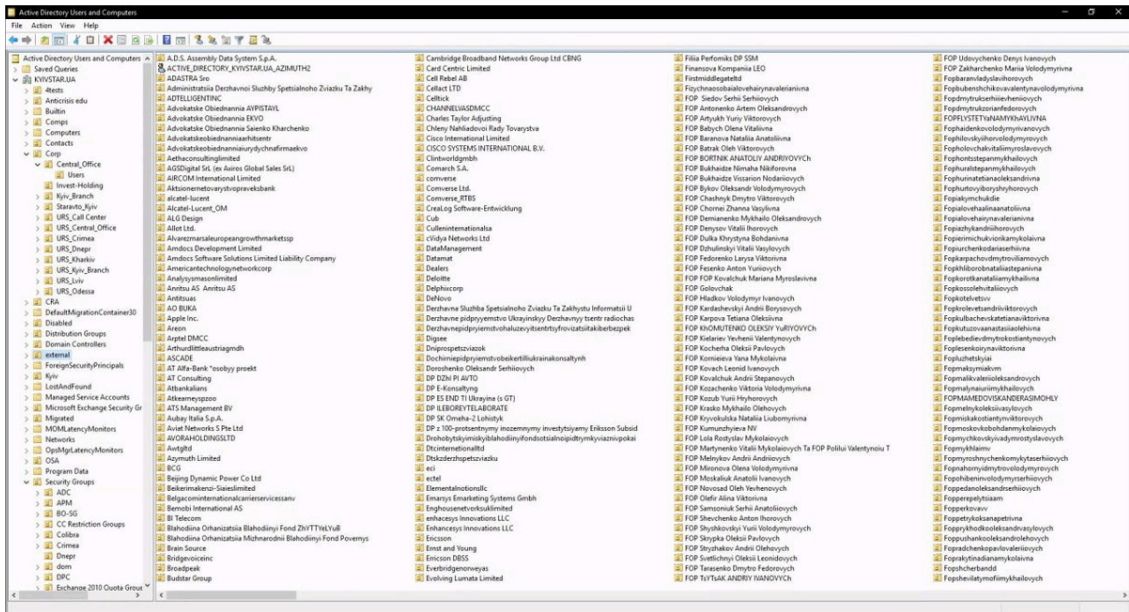
The screenshot shows the Exchange Admin Center interface. The left sidebar contains navigation options like recipients, permissions, compliance management, organization, protection, mail flow, mobile, public folders, servers, and hybrid. The main content area displays a table of database availability groups.

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
backup-e16-08	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
backup-e19-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
backup-e19-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01,EXCG2...	Mounted	0
backup-e19-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
backup-e19-04-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-05-new	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-DGT01	Mounted	0
backup-e19-06-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-07-new	EXCG2019-DGT01	EXCG2019-DGT01	Mounted	0
backup-e19-09	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01	Mounted	0
backup-e19-10	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
MDB-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-04	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-05	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-06	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-07	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-08	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-09	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-10	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-11	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-12	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
restore-partial-backup-e16-...	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01	Mounted	0

1 selected of 23 total



The screenshot shows a database management interface with a sidebar on the left containing a tree view of database objects. The main area displays two tables. The first table has columns: Серийный номер, Пароль, Код товара, Кол-во, Статус, БД, Тип подключения, Центр, Местонахождение, STATE\_ID, NO УЛ реж, NO связи. The second table has columns: ID операции, Тип операции, Дата, БД, Центр управления, Отправитель, БД, Центр получения, Получатель, УЛ реж, Тип УЛ, Тип связи УЛ. The interface includes search bars, table headers, and data rows.



**UPD от 12:50 13.12.2023. В «Киевстар» прокомментировали заявление российских хакеров из «Солнцетёк». В компании заверили, что абонентская информация и персональные данные в безопасности, а системы, в которых эти данные хранятся, не пострадали от хакерской атаки.**

«Все мы видели эти скриншоты из телеграмм-каналов. Но на них изображены наугад собранные технологические данные, которые не относятся к персональным данным наших абонентов. Мы со всей ответственностью заявляем, что ваши персональные данные в безопасности!» — [говорится](#) в сообщении «Киевстар».

В компании также назвали утверждение российских хакеров об уничтоженных компьютерах и серверах «слухами» и «фейком».

**Ранее dev.ua рассказывал кто такие «Солнцетёк» в материале от 3 июля 2023 года:**

Хакерская атака на сайты «Суспільного», «24 Канала», на украинских провайдеров, Министерство развития общин, Южного горно-обогатительного комбината и даже на сайт «Гордон» — этой весной российская группировка «Солнцетек» активно публиковала информацию о нанесении ущерба украинским структурам. Мы решили выяснить, кто может стоять за группировкой и насколько опасны его кибератаки.

## Кибератаки из россии

Вот хронология хакерских атак, ответственность за которые на себя взял «Солнцетек»:

**25 апреля** — локальная сеть Министерства развития общин и территорий Украины подверглась хакерской атаке.

**UPD.** Ранее здесь была цитата министра развития общин Александра Кубракова. Но оказалось, что это был российский фейк для дискредитации украинских киберслужб. Поэтому мы удалили фейковую информацию.

**11 мая** — сайт «24 Канала» [подвергся](#) хакерской атаке. Тогда россияне начали оперативно публиковать на сайте фейковые новости с угрозами президенту Владимиру Зеленскому и украинцам.

**11 мая** — [атака](#) на украинских провайдеров. По версии россиян, это были Citylan, Gigabit-net, UOS, UA Group, FiberNet и другие. Провайдеры «Корбина Телеком» и Znet [сообщали](#) о взломе и рассылке пользователям со стороны российских хакеров.

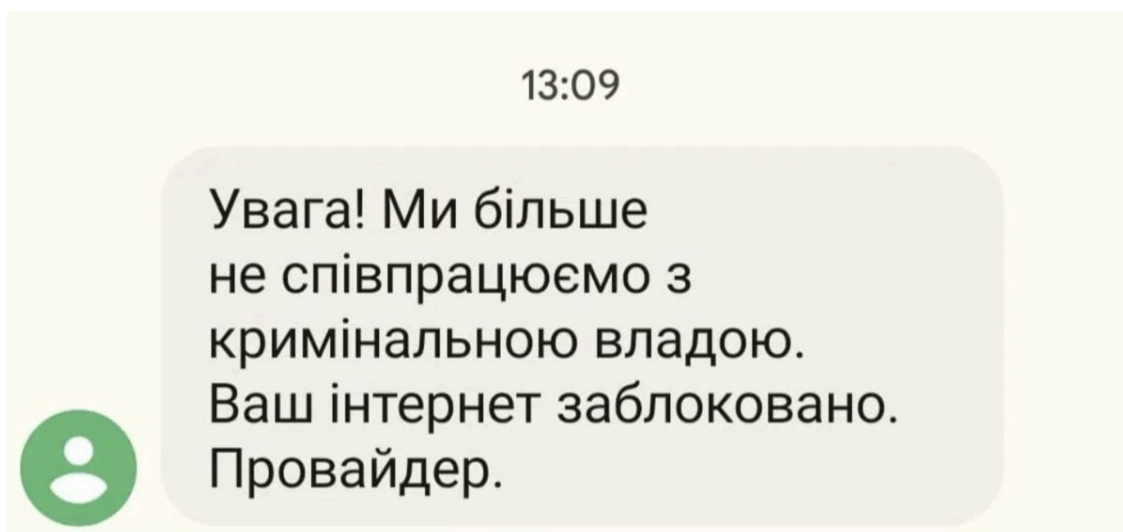


Фото — Сообщение от российских хакеров

**16 мая** — [атака](#) на сайт «Гордон». Тогда редакция на время потеряла доступ к админпанели сайта, из-за чего злоумышленники смогли разместить на главной странице издания заявление антиукраинского содержания. Атака началась около 15:50 по Киеву, но работу сайта удалось возобновить около 17:15.

**25 мая** — [атака](#) на Южный горно-обогатительный комбинат. По заявлению российских хакеров, им удалось «уничтожить более 30 серверов и около 2000 компьютеров». Тогда в пресс-службе украинского предприятия заявили, что если попытки атак и происходили, то они были отражены, а все последствия устранены.

**14 июня** — хакеры [атаковали](#) сайты «Суспільного», атаку расследует Госспецсвязи. Из-за кибератаки вещатель обратился в CERT-UA.

## Как действует «Солнцепек»

В сети немного информации о «Солнцепеке». Как только вы начинаете «гуглить» на эту тему, вам будет «выдавать» одноименную тяжелую огнеметную систему России. У «Солнцепека» есть Telegram-канал, который существует с конца апреля 2022-го года. Сейчас на него подписано 28 000 человек.

Почти год там публиковали личные данные украинских военных, называя их военными преступниками. В первых постах канала можно найти фото украинских медийных личностей — активиста Сергея Стерненко и телеведущей Натальи Мосейчук:



← Солнцек 27.2К підписників

← Солнцек 27.2К підписників

Прикріплене повідомлення #1 Підписчики прислали видеобла

Прикріплене повідомлення #1 Підписчики прислали видеобла

23 червня



В нашем распоряжении оказались данные ярой украинской пропагандистки: **МОСЕЙЧУК Наталья**  
Организация: телеканал «1+1»  
Должность: телеведущая  
Примечание: 18 марта 2022 года в эфире своей авторской программы на телеканале «1+1» Наталья Мосейчук обратилась к женам российских летчиков: **«Вы должны бояться за своих мужей. Рано или поздно наша месть вас найдет. Рано или поздно вы станете вдовами, а ваши дети сиротами. Месть**

Публикуем данные очередного украинского нациста: **СТЕРНЕНКО Сергей**  
Организация: «Правый сектор»  
Должность: экс-глава отделения «Правого сектора» в Одессе  
Аккаунт в Facebook: [www.facebook.com/sternenko](http://www.facebook.com/sternenko)  
Примечание: возглавлял Одесскую организацию «Правого сектора». В 2013-2014 годах был активным участником Евромайдана. В сентябре 2015 года обвинялся в похищении человека, но чудесным образом был выпущен из СИЗО пол

«Их план „А“ заключался в том, что после недельного блицкрига (Украина упадет — ред.) и они начнут контрпартизанскую войну. Поэтому „Солнцек“ публикует „деаноны“, это должны быть расстрельные списки. Поскольку никакого „плана Б“ у них не было, то они продолжают заниматься тем же, и пытаются менять тактику», — сказал в комментарии dev.ua украинский хакер **Андрей Баранович (Sean Townsend)**.

Риторика российской хакерской группировки достаточно типично пропагандистская и уже хорошо нам известна. «Каратели ВСУ», «проводили карательные операции в Донбассе», «соучастник киевской власти»

и т. д. Публикации по личным данным украинских военных продолжаются и сегодня, но весной 2023 года к ним добавилась информация о хакерских атаках в Украине.

## Кто может стоять за группировкой

«Активность освещаемой в части деструктивных кибератак отслеживается CERT-UA с идентификатором UAC-0165. При этом с высоким уровнем уверенности эта активность ассоциируется с деятельностью группировки Sandworm», — рассказали dev.ua в Госспецсвязи.

**Sandworm** — это элитное подразделение российских хакеров, работающее на Кремль. Именно оно [распространяло](#) вируса NotPetya, который уничтожал данные на компьютерах коммерческих и правительственных структур во всем мире, нанося лишь одной диверсией убытки на \$10 млрд. Sandworm [подчиняется](#) **Главному разведывательному управлению России (ГРУ РФ)**.

«Если внимательно посмотреть на их канал, то совершенно очевидно, что это никакая не „группировка“, а очередная вывеска ГРУ РФ. Они невнимательны и допускают ошибки», — рассказал dev.ua хакер Андрей Баранович.

О Sandworm очень хорошо знают в мире. В 2020-м Министерство юстиции США [обвинило](#) шестерых российских хакеров — вероятных офицеров ГРУ — в кибератаках в Украине, США, Франции и Южной Кореи и взломе программного обеспечения, причинившем ущерб почти на \$1 млрд.

В то время подозреваемые находились в России. Это офицеры ГРУ — Юрий Андриенко, Сергей Детистов, Павел Фролов, Анатолий Ковалев, Артем Очиченко и Петр Плискин. Тогда же были опубликованы фотографии. Считается, что все шестеро — члены Sandworm, которая стоит за такими кибератаками как KillDisk (кибератака на энергетические компании Украины, 2015-й год — ред.) и OlympicDestroyer (атака на зимнюю Олимпиаду в Южной Корее, 2018-й).



Фото — Члены Sandworm

«Большая часть взломов — это работа спецслужб, роль „хакеров-волонтеров“ невелика. У последних просто недостаточно мотивации и ресурсов, чтобы работать в таком темпе», — говорит Андрей Баранович.

Весной 2022-го Sandworm [возглавил Евгений Серебряков](#). О нем мало что известно. Есть информация, что Серебряков родился в 1981 году в Курске, но о его образовании или карьере до начала работы в ГРУ рф нет никаких данных. Хакер тщательно следит за своей анонимностью и не допускает утечки. В сети есть лишь несколько его фото не лучшего качества, предоставленных спецслужбами Евросоюза.



Фото — Евгений Серебряков

В 2018 году голландские правоохранители арестовали Серебрякова и его команду. Это произошло возле Организации по запрещению химического оружия в Гааге (ОЗХО). Тогда правоохранители изъяли рюкзак Серебрякова, полный технического оборудования, его ноутбук и другие устройства, доказывающие его причастность к мировым кибератакам. Но Серебрякова и его группу отпустили и вернулись в Россию. Считается, что имели место тайные договоренности спецслужб ЕС и России.

## Насколько вредны последствия

«Их атаки на каналы информации были направлены на распространение дезинформации, в том числе относительно работы правительственной команды реагирования на компьютерные чрезвычайные события CERT-UA», — рассказали в Госспецсвязи.

В ходе атаки пострадала часть сайтов «Общественного». «Речь идет о корпоративном сайте, сайтах местных вещателей, освещающих работу компании. На них, в том числе, зрители имели возможность посмотреть онлайн-трансляцию прямого эфира телеканала своего региона», — рассказали **dev.ua** в «Суспільному».

При этом телеканалы, радио и новостной сайт «Общественные Новости», включая сеть страниц в соцсетях, вещания не прекращали. Также в режиме базовой функциональности работа сайтов была возобновлена сразу после начала работ по ликвидации последствий атаки.

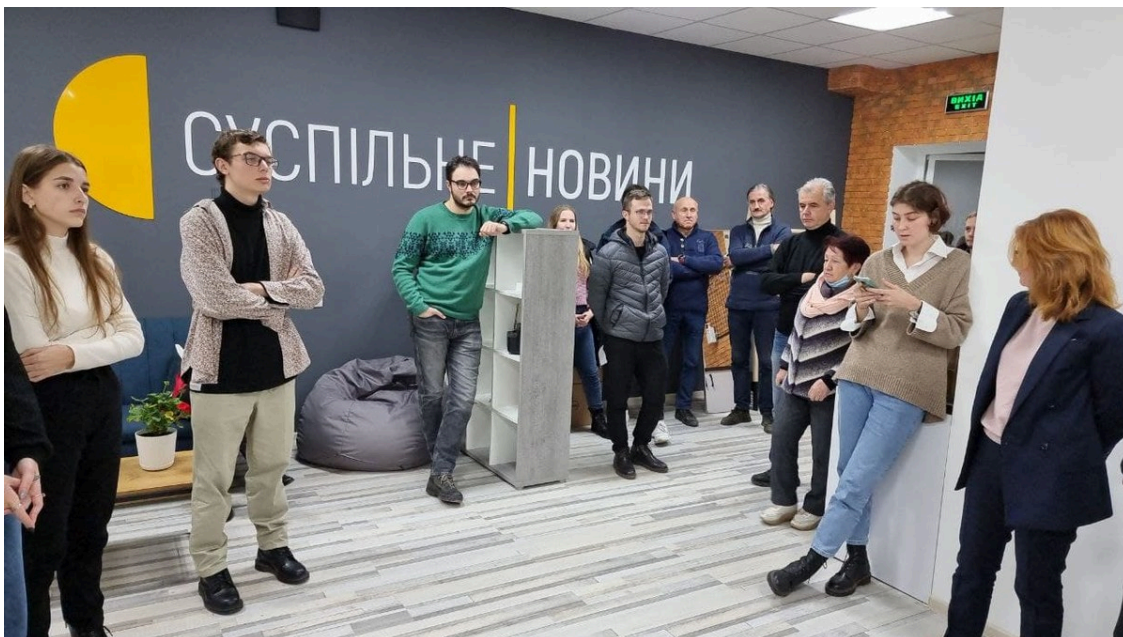


Фото — «Суспільне»

Из соображений безопасности на «Общественном» не стали озвучить меры по усилению инфраструктуры. Но добавляют, что по этому направлению сотрудничают с международными экспертами и государственными органами.

Заместитель главного редактора «**24 Канала**» Вероника Гавриленко рассказала dev.ua, что работа сайта в день хакерской атаки не прекращалась, лишь некоторое время продолжались технические работы. «В тот момент мы закрыли доступ к админке сайта для всех пользователей, поэтому около 40 минут не появлялось новых публикаций в новостной ленте», — добавляет специалист.

«Однако у нас не было ситуации, чтобы разработчики лишились доступа к сайту или хакеры могли силой кого-то выбивать из админки», — говорят на «24 Канале».

На канале говорят, что российская хакерская атака не нанесла никакого материального ущерба и действовала в определенном положительном смысле, указав на что нужно обратить внимание.

Что касается последствий атаки, то на канале не захотели вдаваться в детали, но сообщили, что проделали основательную работу: проработали и максимально сделали невозможными пути проникновения посторонних лиц в админку, изменили подход к логированию и подтверждению юзеров.

Мы обратились в Министерство развития общин и территорий по хакерской атаке «Солнцёпка» и ее последствиям, но на момент выхода материала ответа не получили.

В Службе безопасности Украины ограничились общим ответом: киберспециалисты ведомства системно и в круглосуточном режиме мониторят все, что происходит в сети интернет. Однако информирование общества о работе осуществляется с учетом правовых ограничений на разглашение информации о контрразведывательной и оперативно-розыскной деятельности. «О результатах работы спецслужбы обязательно будет проинформирована общественность», — написали в СБУ.



Фото — Госспецсвязи

«Публикации с дезинформацией были удалены владельцами ресурса, было опубликовано их опровержение. Поэтому, по нашему субъективному мнению, значительного информационного влияния на украинское общество данная тактика не имела», — рассказали dev.ua в Госспецсвязи.

Чего можно ожидать от «Солнцепека» (ФСБ) в будущем?

В Госспецсвязи говорят, что к сожалению, этого предусмотреть невозможно, но при ответственном отношении к киберзащите и своевременном выявлении угроз, такие атаки можно предотвратить.

«Их привычные, обкатанные схемы просто перестали работать, вот они пытаются менять свою тактику — и в техническом, и в медийном отношении. Пока что без особых результатов, по-моему», — подытожил Андрей Баранович.

---

Source: <https://dev.ua/ru/news/atakovali-suspilne-provaidеров-i-minrazvitiya-obschin-kto-stoit-za-rossiiskoi-gruppirovkoi-solntsepek-kotoraya-aktivizirovala-napadeniya-na-ukrainskie-struktury>