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.

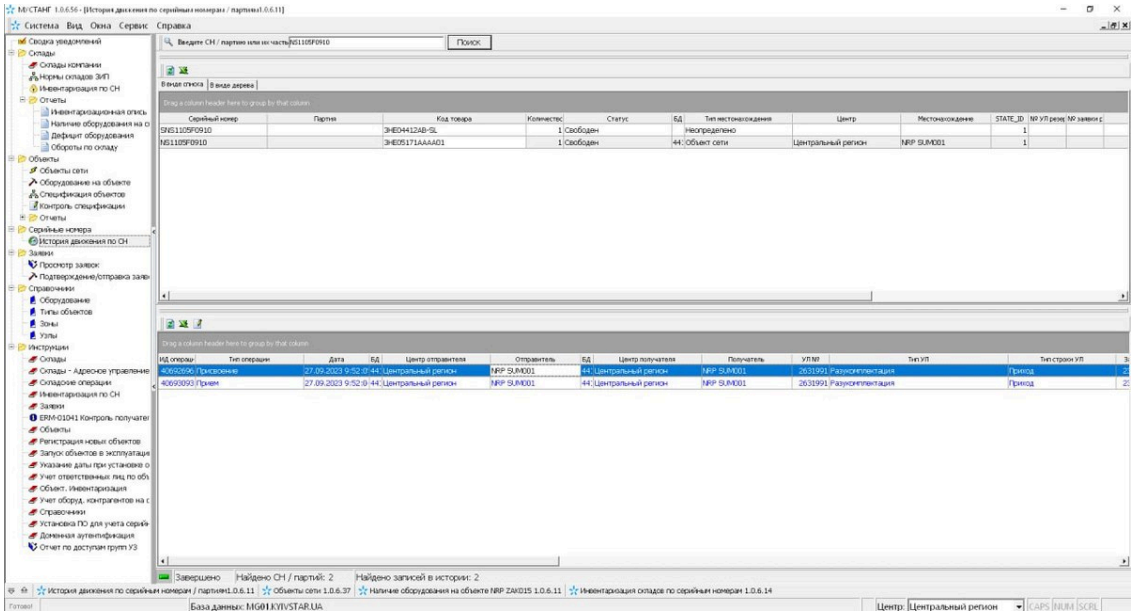
Вчера в работе «Киевстар», который имеет 24 млн абонентов, произошел масштабный сбой, из-за которого не работает связь и сайт оператора. Впоследствии СРО «Киевстар» подтвердил хакерскую атаку на компанию. Абонентам, которые не имели связи, пообещали компенсацию.

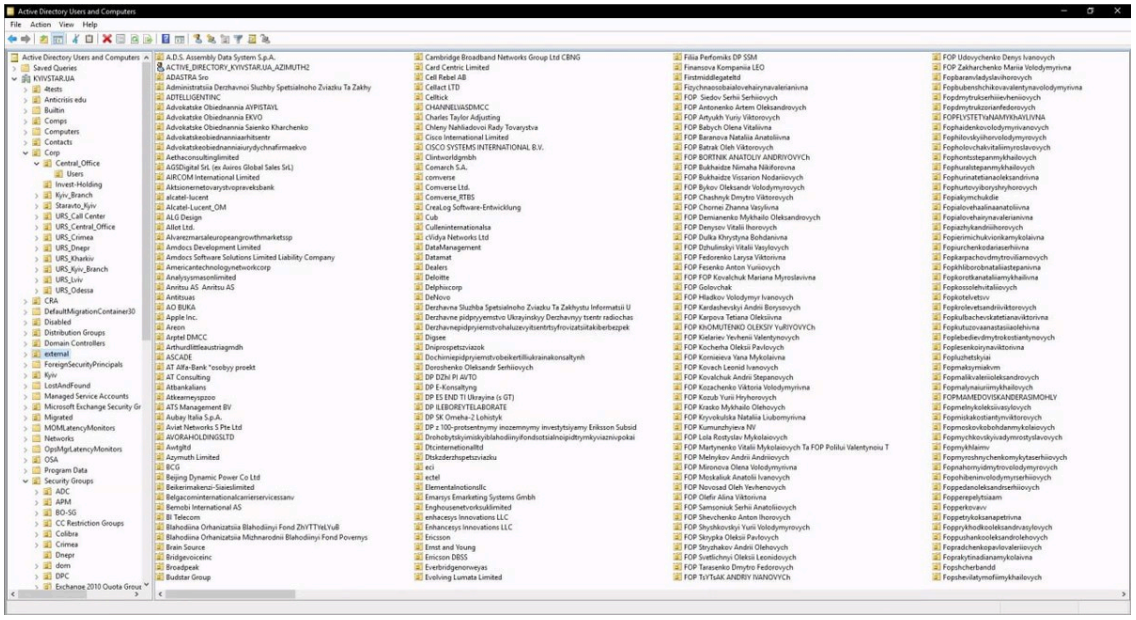
Генеральный директор «Киевстар» Александр Комаров сообщил, что атака частично разрушила IT-инфраструктуру. По словам источников dev.ua, «Киевстар», вероятно, был вынужден самостоятельно отключить свои сервисы из-за скомпрометированного «критического аккаунта».

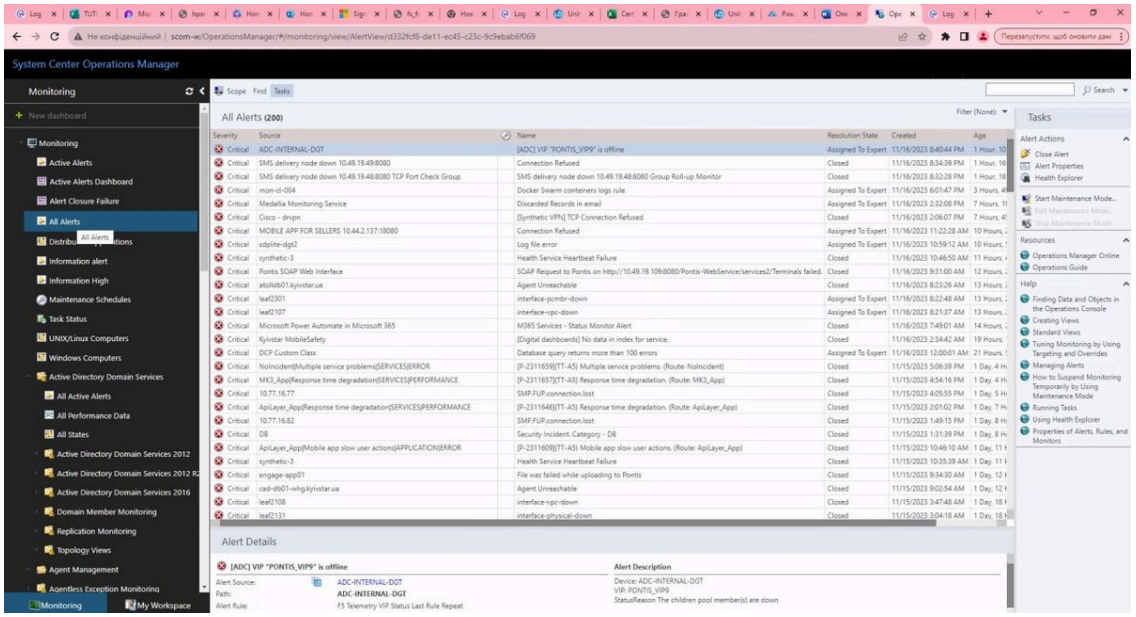
Сегодня в Telegram-канале группировки «Солнцепёк» появилось сообщение, в котором они взяли на себя «полную ответственность за кибератаку на Киевстар».

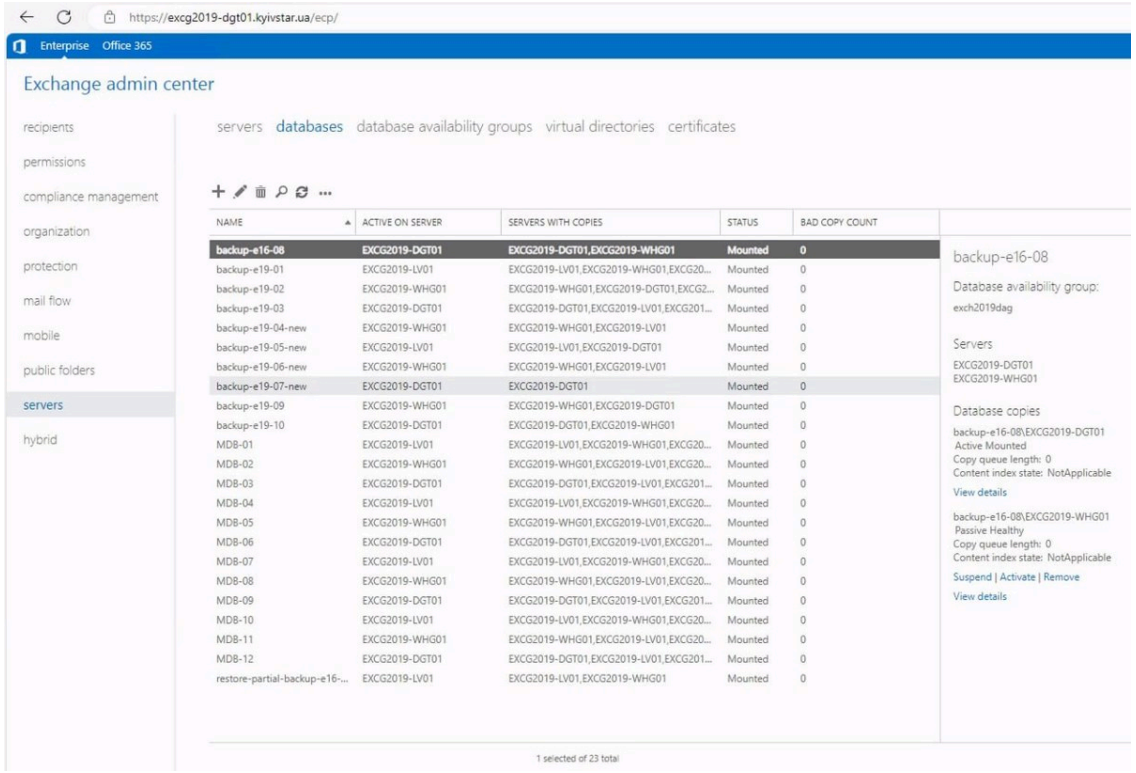
«Мы уничтожили 10 000 компьютеров, более 4000 серверов, все системы облачного хранения данных и резервного копирования. Мы атаковали „Киевстар“, потому что компания обеспечивает связью ВСУ, а также государственные органы и силовые структуры Украины. Остальным конторам, которые помогают ВСУ, приготовиться!»,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

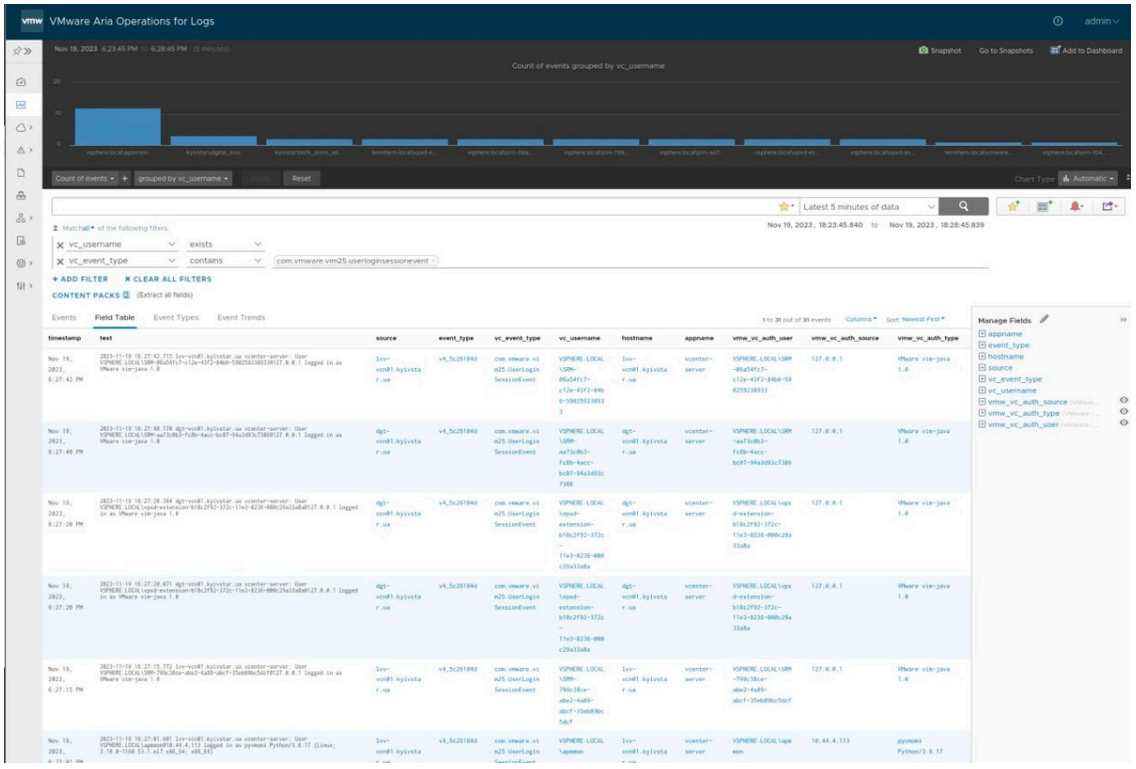
Они также намекнули, что с атакой им помогли «неравнодушные» сотрудники «Киевстар», и опубликовали скриншоты, которые вероятно должны подтвердить, причастность «Солнцепёк».

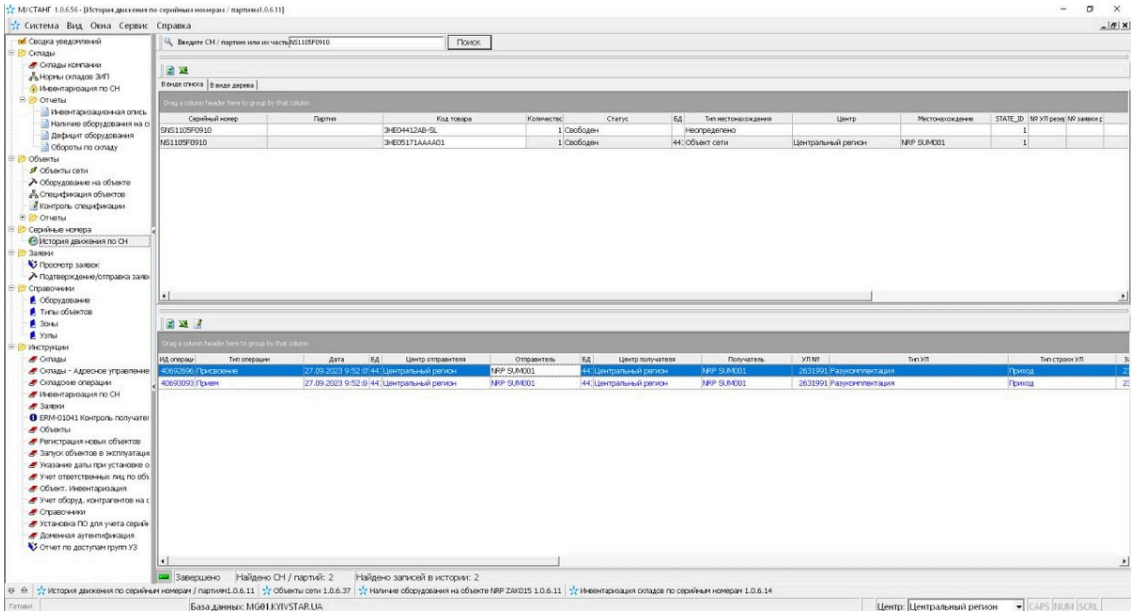


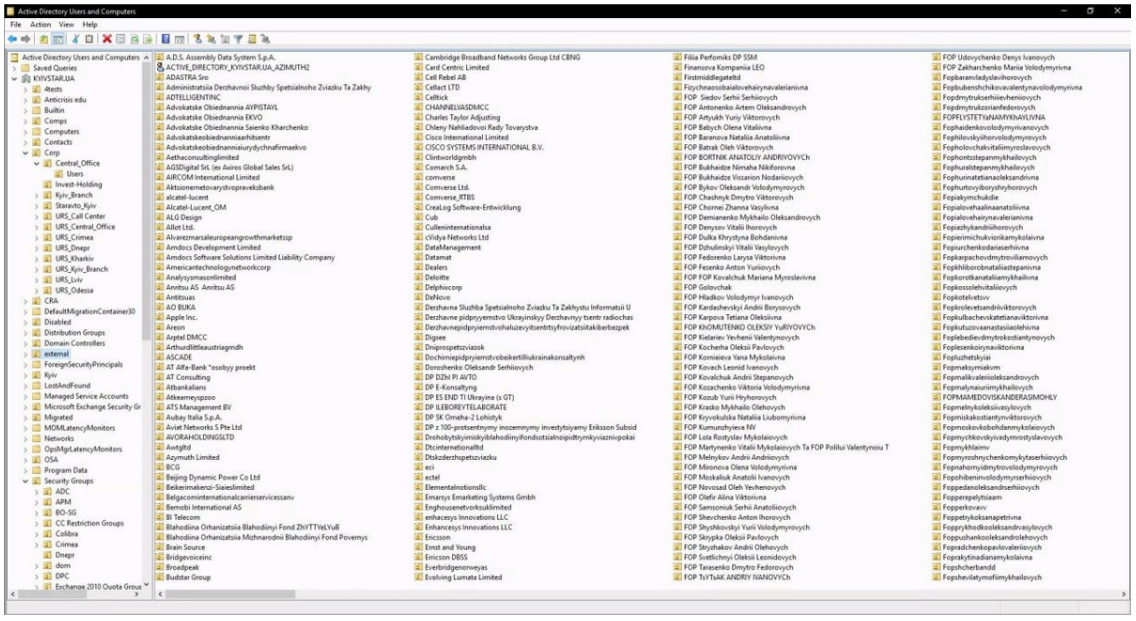



System Center Operations Manager
Monitoring
All Alerts (200)
Alert Details
Tasks


https://excg2019-dgt01.kyivstar.ua/ecp/
Enterprise Office 365
Exchange admin center
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers
hybrid
servers databases database availability groups virtual directories certificates
backup-e16-08
Database availability group:
exch2019dag
Servers
EXCG2019-DGT01
EXCG2019-WHG01
Database copies
1 selected of 23 total


VMware Aria Operations for Logs
admin
Count of events grouped by vc_username
Snapshot
Go to Snapshots
Add to Dashboard
Latest 5 minutes of data
vc_username
exists
vc_event_type
contains
com.vmware.vim25.userloginsessionevent
+ ADD FILTER
× CLEAR ALL FILTERS
CONTENT PACKS
Events
Field Table
Event Types
Event Trends
Manage Fields
timestamp
text
source
event_type
vc_event_type
vc_username
hostname
appname
vmw_vc_auth_user
vmw_vc_auth_source
vmw_vc_auth_type


Система Вид Окна Сервис Справка
Поиск
Серийный номер
Партия
Код товара
Количество
Статус
БД
Тип местонахождения
Центр
Местонахождение
SNS1105F0910
NS1105F0910
Завершено
Найдено СН / партий: 2
Найдено записей в истории: 2
Центр: Центральный регион



UPD от 12:50 13.12.2023. В «Киевстар» прокомментировали заявление российских хакеров из «Солнцепёк». 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 «Солнцепёк» 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 «Солнцепек» 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 «Солнцепек»:

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.

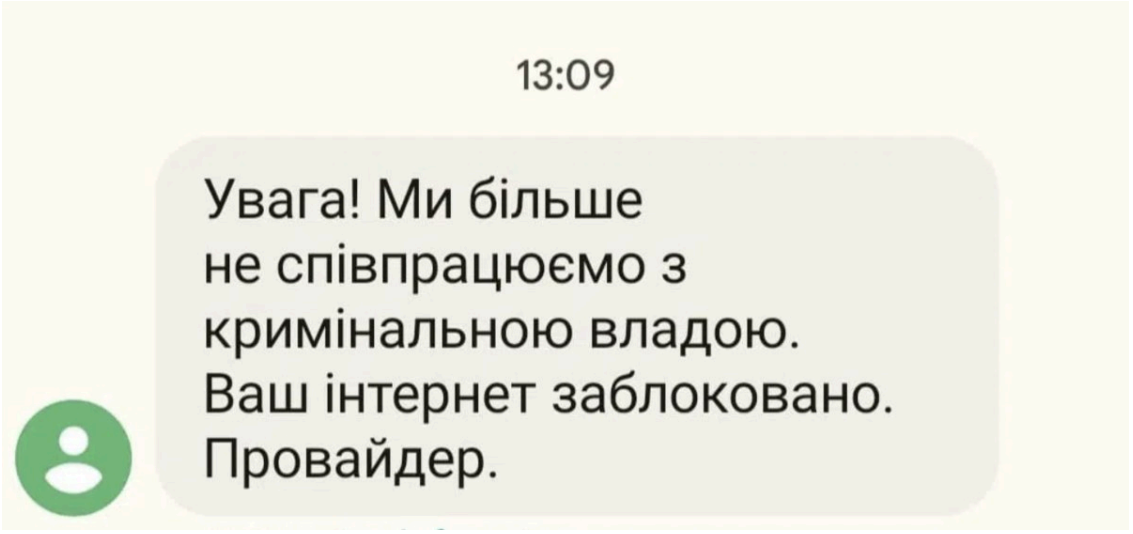


Фото — Сообщение от российских хакеров

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.

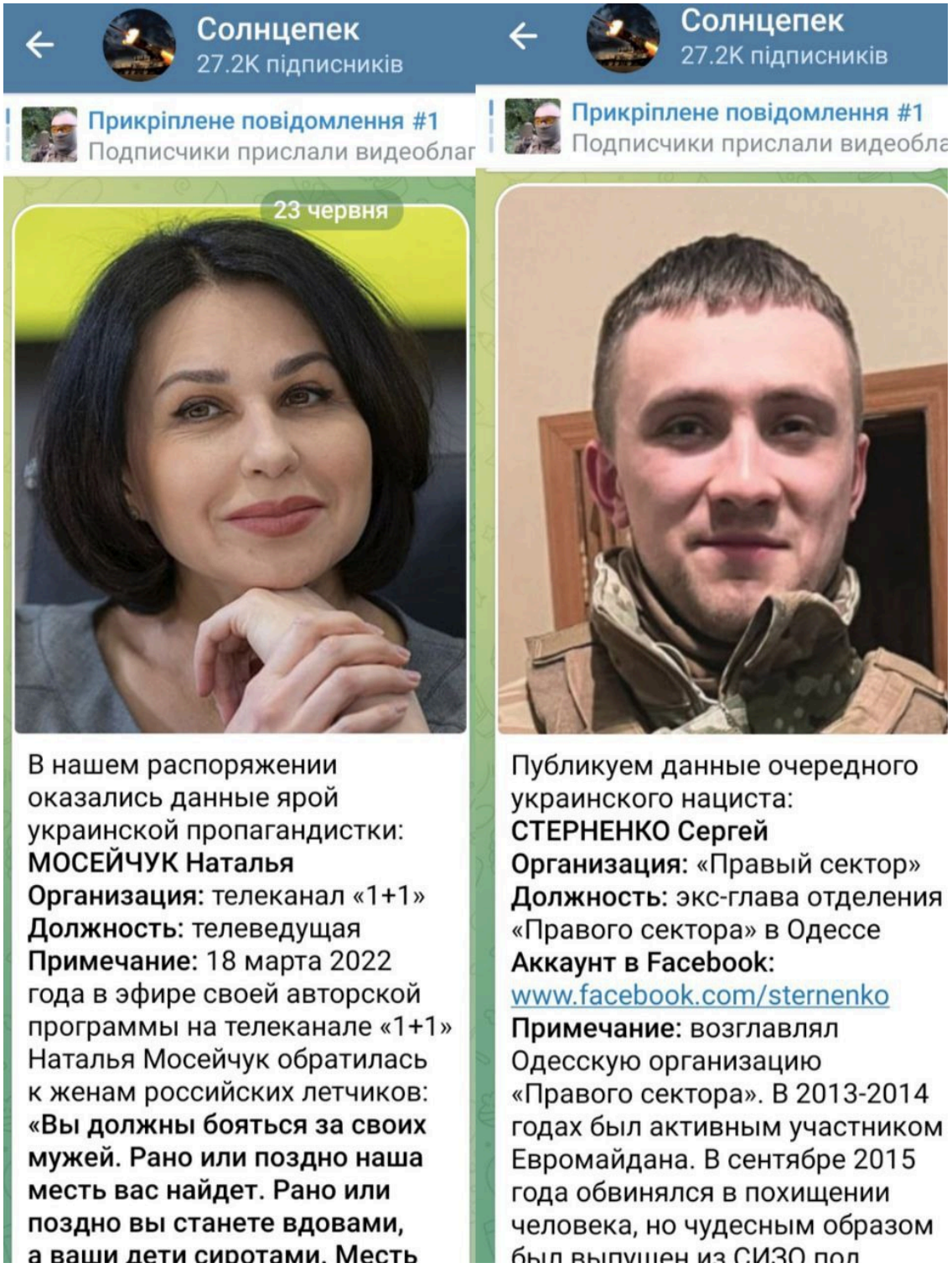
25 мая — атака на Южный горно-обогатительный комбинат. По заявлению российских хакеров, им удалось «уничтожить более 30 серверов и около 2000 компьютеров». Тогда в пресс-службе украинского предприятия заявили, что если попытки атак и происходили, то они были отражены, а все последствия устранены.

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:



«Их план „А“ заключался в том, что после недельного блицкрига (Украина упадет — ред.) и они начнут контрпартизанскую войну. Поэтому „Солнцепек“ 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 Sandwarm 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 Корее 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 кибератаки 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.

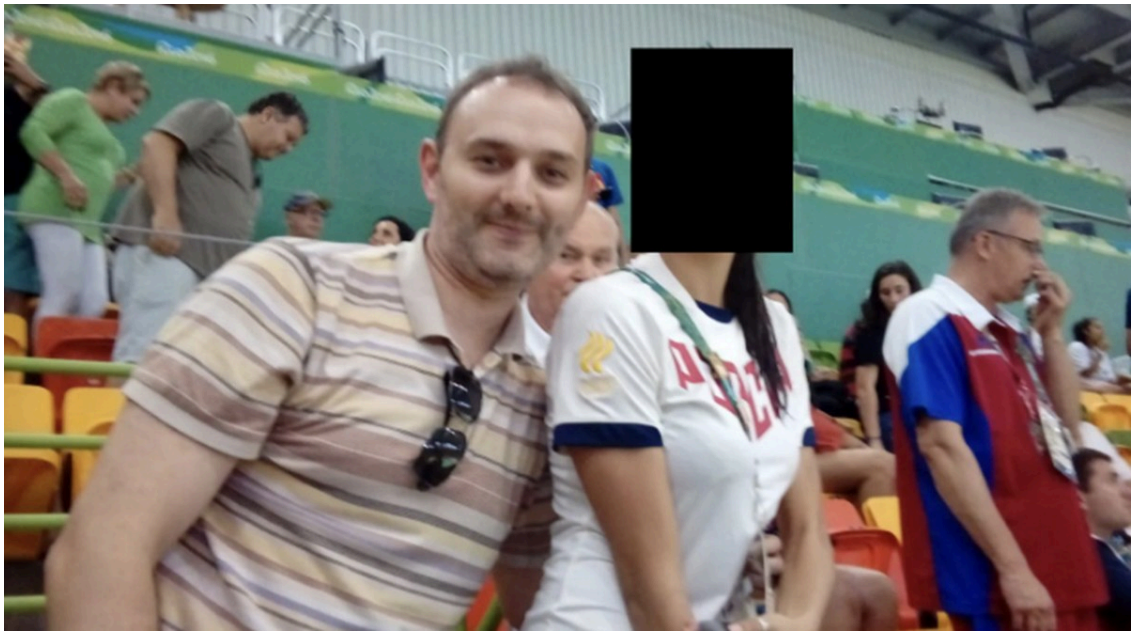


Фото — Евгений Серебряков

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 «Общественное 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 подействовала 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 «Солнцепёка» 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.
