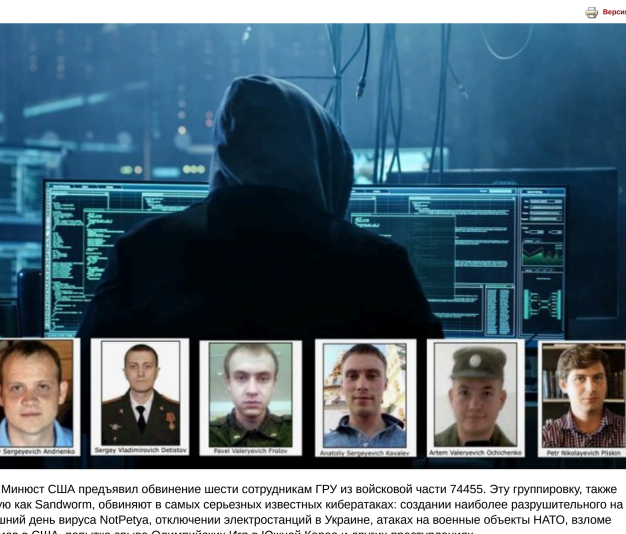
Sandworm. Как хакеры ГРУ отключали энергетику в Украине и взламывали избирком США

КІБЕРЗЛОЧИННІСТЬ | ПНД, 2020-10-26 09:21

Версия для печати



На днях Минюст США предъявил обвинение шести сотрудникам ГРУ из войсковой части 74455. Эту группировку, также известную как Sandworm, обвиняют в самых серьезных известных кибератаках: создании наиболее разрушительного на сегодняшний день вируса NotPetya, отключении электростанций в Украине, атаках на военные объекты НАТО, взломе избиркомов в США, попытке срыва Олимпийских Игр в Южной Корее и других преступлениях.

С заявлением о поддержке этих обвинений выступил и МИД Великобритании. О том, что за группировкой Sandworm стоит эта войсковая часть ГРУ, сообщалось и ранее, однако впервые конкретным военным предъявлены официальные обвинения. В издании **The Insider** смогли подтвердить причастность указанных лиц к указанной войсковой части, а также выяснить некоторые детали их биографии.

На эту тему: **«Хакеры ГРУ действуют как стратегическое оружие российского государства»**

Главные кибератаки Sandworm

Группа хакеров из войсковой части 74455 (Главного центра специальных технологий ГРУ) была названа **«Sandworm»** Джоном Халтквистом из компании iSight (теперь он директор аналитического отдела FireEye). Именно компания iSight в 2014 году обнаружила группу хакеров, стоявшую за атаками на объекты в Украине, а также на участников саммита НАТО в Уэльсе. В тот момент хакеры использовали уязвимости нулевого дня в программе Powerpoint для рассылки вредоносного кода. iSight удалось доказать, что за группой стоят именно российские власти. Но о том, что хакеры служат именно в этой войсковой части, тогда еще известно не было. На самом деле привлечение ГРУ к операциям такого рода началось не позднее чем в 2007 году.

В апреле 2007 года кибератаке подверглись правительственные организации и частные компании в Эстонии. Это совпало с организованными Кремлем уличными беспорядками, последовавшими после переноса Бронзового солдата в Таллине. В ходе кибератак был использован ботнет, включавший от одного до двух миллионов взломанных компьютеров, расположенных в 100 разных странах. Многие страны тогда помогли Эстонии остановить эту атаку. Россия помогать, разумеется, отказалась.

В августе 2008 года, во время войны с Грузией, кибератаке подверглось множество грузинских правительственных сайтов. Хакеры из ГРУ, получившие доступ к сайтам, выкладывали там фотографии с Гитлером. При этом кибератаки были хорошо скоординированы с военными атаками. Скажем, кибератаки на официальный сайт и газету грузинского города Гори начались непосредственно перед тем, как город подвергся российской бомбардировке с воздуха, а затем оккупации российскими войсками.

Также любопытно, что хорошо подготовленная массированная атака на грузинские сайты началась уже 8 августа, то есть сразу после начала войны, хотя по официальной российской версии именно Грузия инициировала неожиданное вероломное нападение. 28 октября 2019 года та же войсковая часть повторила кибератаку на Грузию. Вещание нескольких телеканалов было прервано, правительственные сервера заблокированы, оказалась парализованной работа нескольких общественных учреждений. Во многих случаях главные страницы веб-сайтов были заменены фотографией бывшего президента страны Михаила Саакашвили с подписью «I'll be back».

Следующая крупная кибератака произошла в 2015 году в ходе вторжения России в Украину. Все началось 23 декабря под конец рабочего дня в местном «Прикарпаттяоблэнерго», которое снабжает электричеством весь регион. Один из работников предприятия приводил в порядок бумаги на своем столе и вдруг заметил, как курсор его мышки вдруг начал самопроизвольно перемещаться по экрану. На его глазах состоялся запуск программы, управляющей работой областных подстанций, и последующее отключение соответствующих подстанций, лишившее тысячи жителей света и отопления. Все последующие действия оператора, направленные на восстановление контроля над ситуацией и возобновление работы подстанций, не принесли желаемого результата — злоумышленники изменили код доступа к системе. Вследствие атаки в общей сложности было отключено примерно 30 подстанций. Также параллельно были атакованы еще два распределительных центра, что позволило отключить практически вдвое больше подстанций и погрузить около 230 тысяч жителей в темноту. Без света остались не только обыватели и предприятия, но и, например, больницы, где отключение электричества может стоить людям жизни. Помимо электростанций, аналогичной атаке подверглись Минфин и Казначейство Украины. Атака была выполнена с использованием адаптируемого вредоносного ПО, известного как CrashOverride, которое закодировано для автоматического уничтожения сети. CrashOverride мог «говорить» на языке протоколов системы управления сетью и таким образом отправлять команды непосредственно на оборудование.

В 2017 году хакеры из войсковой части 74455 провели свою самую масштабную операцию посредством созданного ими вируса **NotPetya**, поражающим корпоративные сети. Главным объектом атаки, начавшейся накануне 27 июня, снова была Украина, которая в этот момент готовилась отмечать День Конституции. В результате действия вируса, стиравшего жесткие диски, была заблокирована деятельность таких предприятий, как аэропорт «Борисполь», Укртелеком, Укрпочта, Ощадбанк, Укрзализныця, а также ряда крупных коммерческих предприятий. Пострадала даже система радиационного мониторинга в Чернобыльской АЭС. При атаке вирус-вымогатель NotPetya шифровал жесткий диск и требовал у обладателя компьютера деньги за возвращение доступа к компьютеру (разумеется, при выплате денег диск все равно оставался зашифрованным).

После Украины вирус вышел из под контроля и поразил многие другие страны, в том числе и Россию. Пострадали в том числе «Сбербанк», «Роснефть», «Башнефть» и «Евраз». Среди пострадавших оказалась и компания Maersk Line — мировой лидер в морских контейнерных перевозках: вирус на некоторое время вызвал хаос в логистике. Снова пострадало множество больниц и медучреждений. что поставило под угрозу жизни тысяч людей. Общий ущерб от атаки оценивают в $10 млрд, что в разы больше, чем ущерб от второго по масштабу вируса WannaCry ($4 млрд).

9 февраля 2018 года февраля хакеры Sandworm организовали кибератаку на компьютеры комитета зимних Олимпийских игр 2018 года в Пхёнчхане (Южная Корея), использовав вирус Olympic Destroyer для атаки на церемонию открытия игр 9 февраля. При этом хакеры, оставляя ложные следы, пытались выдать себя за северокорейских (что было не очень убедительно, поскольку это был тот редкий момент, когда Северная и Южная Корея переживали период сближения и даже выставили общую сборную в некоторых видах спорта). Благодаря высокому профессионализму южнокорейских программистов ущерб от кибератаки был минимизирован и церемонию открытия сорвать не удалось. Напомним, на Олимпиаду не было допущено 111 российских спортсменов из-за применения допинга (подробнее о системе массового применения допинга в российском спорте — в **докладе** Макларена).

В некоторых случаях Sandworm действовал вместе со своими коллегами из ГРУ — группировкой известной как APT28, Fancy Bear и Pawn Storm. В 2017 году The Insider **удалось доказать**, что эта группировка состоит из сотрудников войсковой части 26165 ГРУ. Через год эти данные подтвердил Минюст США, официально **выдвинув** обвинения группе хакеров. Самой известной операцией APT28 стал взлом серверов Демократической партии в 2016 году, призванный помочь Дональду Трампу победить Хиллари Клинтон на президентских выборах. Тогда Трамп не скрывал, что в своих политических целях пользуется информацией, полученной из взлома, и призывал российских хакеров выложить больше писем Хиллари Клинтон. Среди остальных кибератак APT28 можно отметить Белый дом (и другие цели в США), МИД Чехии, Польши, Германии, Италии, Латвии, Эстонии, Украины, Норвегии, Нидерландов и других стран, Минобороны Дании, Италии и Германии, Бундестаг, НАТО, ОБСЕ, МОК, WADA, JIT, ряд редакций иностранных СМИ (в том числе TV5Monde и Аль-Джазира). Эта же группа хакеров атаковала десятки российских оппозиционеров и членов НКО и журналистов, в том числе и сотрудников The Insider, что независимо друг от друга **подтвердили** четыре компании, работающие в области информационной безопасности.

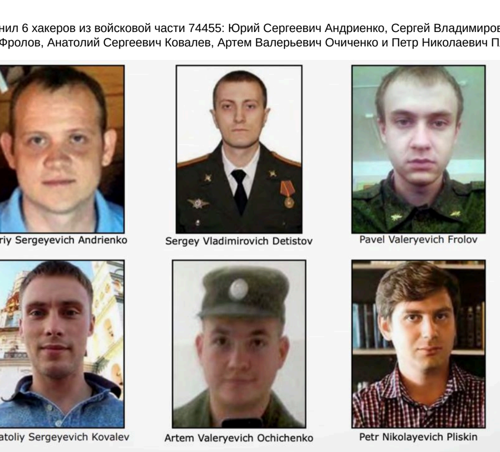
В отличие от Sandworm, Fancy Bear действовали достаточно примитивно — массово рассылая фишинговые письма в ожидании, когда найдется кто-то достаточно невнимательный, чтобы кликнуть на ссылку и выдать свой пароль. Как правило, главной задачей Fancy Bear было получение доступа к информации, которая затем использовалась в политических целях. Например, полученные документы зачастую видоизменялись, к ним добавлялась какая-то компрометирующая информация, после чего это выкладывалось на различных сайтах, принадлежащих неким прокремлевским «активистам», а затем пиарилось кремлевскими медиа и троллями.

Сложно сказать, насколько тесно сотрудничали войсковые части 74455 (Sandworm) и 26165 (Fancy Bear), но как минимум в нескольких атаках они точно участвовали вместе. Это, в числе прочих, взлом предвыборного штаба Эммануэля Макрона перед выборами в 2017 году и атаки на Организацию по запрещению химоружия, когда та расследовала покушение на Скрипаля.

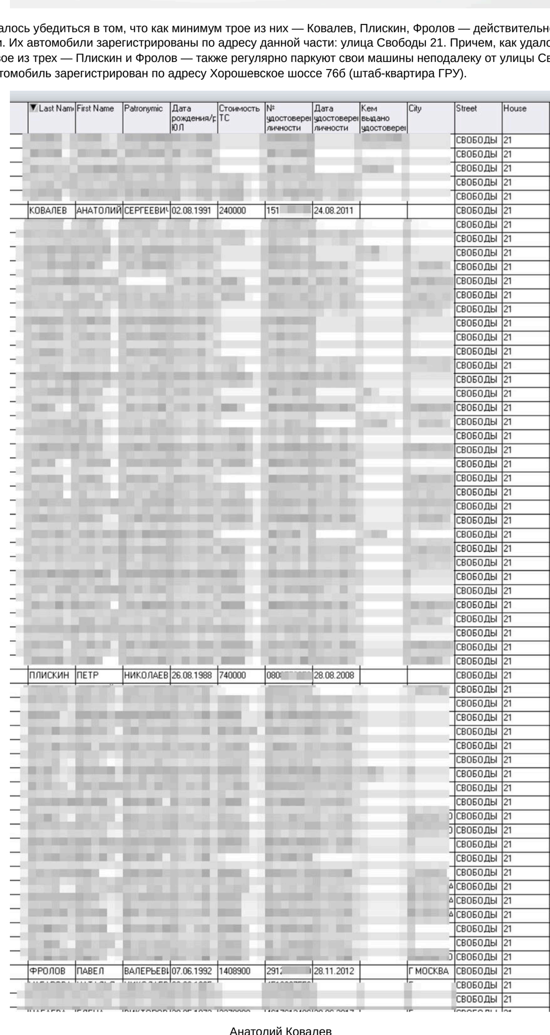
На эту тему: **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб?**

Обвиняемые

Всего Минюст обвинил 6 хакеров из войсковой части 74455: Юрий Сергеевич Андриенко, Сергей Владимирович Детистов, Павел Валерьевич Фролов, Анатолий Сергеевич Ковалев, Артем Валерьевич Очиченко и Петр Николаевич Пліскин.



The Insider удалось убедиться в том, что как минимум трое из них — Ковалев, Плискин, Фролов — действительно служат в этой военной части. Их автомобили зарегистрированы по адресу данной части: улица Свободы 21. Причем, как удалось выяснить The Insider, двое из трех — Плискин и Фролов — также регулярно паркуют свои машины неподалеку от улицы Свободы. У Андриенко автомобиль зарегистрирован по адресу Хорошевское шоссе 76Б (штаб-квартира ГРУ).



Last Name	First Name	Patronymic	Дата рождения/р ЮЛ	Стоимость ТС	№ удостоверения личности	Дата удостоверения личности	Кем выдано удостоверение	City	Street	House
КОВАЛЕВ	АНАТОЛИЙ	СЕРГЕЕВИ	02.08.1991	240000	151	24.08.2011			СВОБОДЫ	21
ПЛИСКИН	ПЕТР	НИКОЛАЕВ	26.08.1988	740000	080	28.08.2008			СВОБОДЫ	21
ФРОЛОВ	ПАВЕЛ	ВАЛЕРЬЕВ	07.06.1992	1408900	2912	28.11.2012		Г МОСКВА	СВОБОДЫ	21

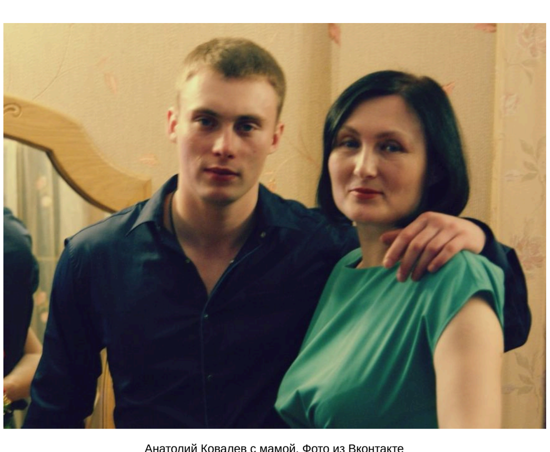
Анатолий Ковалев

Ковалев уже не первый раз засвечивается в обвинениях Минюста США. Ранее он **обвинялся** во взломе компьютеров американских политиков и чиновников с целью вмешательства в выборы 2016 года. Среди прочего, Ковалев и его сообщники «исследовали домены, используемые избирательными комиссиями штатов США, госсекретаря, и другие домены, связанные с выборами, для поиска уязвимости». Примерно в июле 2016 года Ковалев и его сообщники взломали веб-сайт государственного совета по выборам и украли информацию, касающуюся примерно 500 000 избирателей, включая имена, адреса, частичные номера социального страхования, даты рождения и водительские права.

Примерно в августе 2016 года Ковалев и его сообщники взломали компьютеры поставщика из США («Поставщик 1»), который предоставил программное обеспечение, используемое для проверки информации о регистрации избирателей. <...>. Примерно с начала ноября 2016 года и до президентских выборов в США 2016 года Ковалев и его сообщники, используя учетную запись электронной почты, которая выглядела как адрес электронной почты «Поставщика 1», чтобы отправить более 100 фишинговых писем организациям и персоналу, участвующему в администрировании выборов во многих округах Флориды. Письма с целевым фишингом содержали вредоносное ПО, которое сообщники встроили в документ Word с логотипом «Продавца 1».

В **новом обвинительном приговоре** обозначены и другие преступления Ковалева. Так, например, 21 апреля 2017 года он

«опробовал методику рассылки фишинговых писем под видом пересылки Google-документа. Ковалев создал вредоносную программу, встроенную в документ под названием „Qui_peut_parler_aux journalists.docx" (что переводится как „Кто готов разговаривать с журналистами"), где были перечислены девять членов партии „Вперед, Республика!", якобы готовые поговорить с журналистами о террористической атаке, произошедшей накануне на Елисейских полях в Париже. Позже в тот же день эти преступники использовали электронную почту, которая имитировала аккаунт пресс-секретаря Макрона (тогда еще кандидата), чтобы отправить электронное письмо с фишингом, выглядящим как Google-документ, примерно 30 функционерам „Вперед, Республика!". Примерно с 12 апреля 2017 года по 26 апреля 2017 года контролируемые ГРУ социальные медиа-аккаунты связывались с различными французскими лицами, предлагая ознакомиться с внутренними документами партии „Вперед, Республика!"».



Анатолий Ковалев с мамой. Фото из Вконтакте

Поучаствовал Ковалев и в атаке на Олимпийские игры в Южной Корее.

«Примерно 28 ноября 2017 г. Ковалев написал фишинговое письмо от лица председателя комиссии МОК. В электронном письме предлагалось получить список делегатов и их контакты, которые якобы готовы помочь разобраться с любыми проблемами во время Олимпиады. Позднее в тот же день сообщники разослали другую версию этого фишингового письма (на этот раз от лица вице-президента МОК) 29 адресам, чьи аккаунты зарегистрированы в домене МОК pyeongchang2018.com. <...> Примерно 6 и 7 декабря 2017 г. сообщники, используя адрес **olympicgameinfo@gmail.com**, отправили 23 фишинговых писем с темой „предложение о сотрудничестве" на 220 адресов, зарегистрированных на доменах, принадлежащих нескольким олимпийским партнерам, а также МОК».

...и в атаке на британскую лабораторию Портон-Даун, расследовавшую отравление Скрипаля, и на ОЗХО:

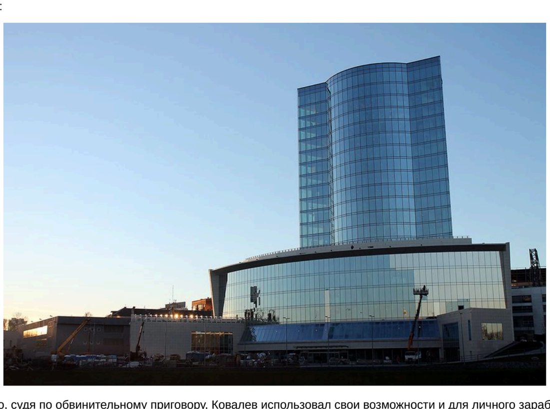
«3 апреля 2018 года лаборатория Портон-Даун объявила, что идентифицировала яд, использованный против Скрипаля, как тип боевого отравляющего вещества „Новичок". Примерно 5 апреля 2018 года Ковалев создал учетную запись электронной почты с именем пользователя, который имитировал название немецкой национальной еженедельной газеты, после чего разослал фишинговые письма по поводу „Инцидента в Солсбери" от лица немецкого журналиста примерно на 60 официальных адресов лаборатории в Портон-Даун. На следующий день он также разослал по этим адресам письма с вредоносным кодом, которые выглядели как отправленные с адреса Портон-Даун».

6 апреля 2018 года сообщники провели три фишинговые кампании, нацеленные на ОЗХО и организации в Великобритании, участвовавшие в расследовании отравления. Сообщники использовали аккаунт, имитировавший аккаунт британского журналиста, для отправки примерно 20 писем с фишингом по заголовком „Salisbury Spy Poisoning Investigation" на официальные адреса ОЗХО. В этих фишинговых письмах сообщники якобы хотели поделиться информацией относительно отравления. После того, как сообщники получили электронное письмо от ОЗХО с указанием вместо этого поделиться информацией с Великобританией и дали три конкретные адреса электронной почты, сообщники направили свои фишинговые письма туда».

А вот пример участия Ковалева в атаке на Грузию:

«В 2018 году сообщники организовали массовую кибератаку на государственные и частные структуры в Грузии (подобную аналогичной атаке 2015 года на Украину). Атаке подвергся парламент Грузии и крупное СМИ. Атака была нацелена на деморализацию и дестабилизацию Грузии. 25 января 2018 года Ковалев создал учетную запись электронной почты, имитировавшую адрес грузинского СМИ, которое специализируется на освещении новостей. Вскоре после этого Ковалев использовал этот аккаунт для отправки восьми зараженных фишинговых писем 68 адресатам, зарегистрированным в домене, принадлежащем тому же самому СМИ».

Ковалев родился 2 августа 1991 года и вырос в поселке Суземка Брянской области. После школы он начал службу в армии и сейчас официально служит в войсковой части 74455 как «инженер». Работает он из здания в Химках, известного как «башня» (ул. Кирова 22):



Любопытно, что, судя по обвинительному приговору, Ковалев использовал свои возможности и для личного заработка, устраивая фишинговые кампании в адрес крупных российские риэлторских компаний, автодилеров, майнеров криптовалюты, а также криптовалютные биржи, расположенные за пределами России.

От комментария The Insider Анатолий Ковалев отказался, сделав вид, будто он не Анатолий Ковалев.

Петр Плискин

Петр Плискин сыграл важнейшую роль в этой группе как один из создателей кода самого разрушительного в истории вируса NotPetya, а также вируса Olympic Destroyer, который он создал вместе с Андриенко для срыва Олимпийских игр. Минюст США сообщает, что Плискин служил в этой войсковой части до июня 2018 года и руководил командой разработчиков.

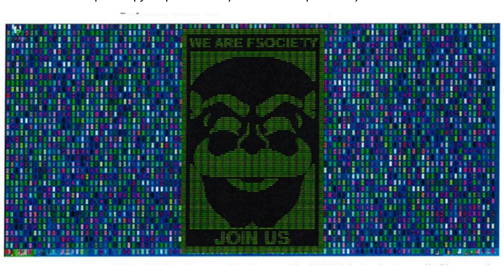
Петр Плискин, селфи из здания мэрии Москвы

Плискин родился 26 августа 1988 года в Хабаровске, учился в Военно-космическом кадетском корпусе Петра Великого в Санкт-Петербурге, участвовал в олимпиадах по физике. Затем поступил на службу в **ГРУ**. Сразу после ухода со службы летом 2018 года создал свое ИП по разработке компьютерного обеспечения — правда, вскоре сам же его закрыл.

Петр Плискин сообщил The Insider, что он «не тот человек, о котором идет речь в приговоре Минюста США», хотя именно тот телефон, по которому связывался The Insider, использовался для парковки его автомобиля у войсковой части на улице Свободы.

Павел Фролов

Фролов участвовал в создании вируса NotPetya, а также вируса, который использовался при атаке на Минфин Украины. Кроме того, Фролов с сообщниками разработали вредоносного ПО KillDisk, посредством которого перезаписывались жесткие диски пораженных компьютеров (это ПО использовалось при отключении украинских электростанций и при атаке вируса NotPetya). Именно Фролову пришла в голову идея сделать так, чтобы срабатывании KillDisk на экране появлялась маска и надпись «We are FSOCIETY» (это название хакерской группировки из сериала «Мистер Робот»).



Фролов родился 6 июня 1992 года в Калуге, где и закончил школу, а затем калужский филиал МГТУ им Баумана (кафедра «Программное обеспечение ЭВМ, информационные технологии, прикладная математика»).

На эту тему: **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб? Часть 2**

Сергей Детистов

Детистов служил в войсковой части 74455 в звании капитана, занимался разработкой вируса NotPetya и подготавливал инфраструктуру для рассылки фишинга во время Олимпийских игр в Южной Корее.

Детистов родился 21 июля 1985 года в Ростове-на-Дону и до сих пор зарегистрирован в этом городе. Детистов — самый скрытный из этой шестерки, он не засвечен в соцсетях, на его имя не зарегистрирован автомобиль, нет данных и о учебе.

Юрий Андриенко

Согласно обвинительному приговору, Андриенко был одним из разработчиков вируса NotPetya и вируса Olympic Destroyer, предназначенного для саботажа Олимпийских игр.

Андриенко родился 30 мая 1988 года, вырос в селе Мещерино Ступинского района Московской области. Судя по всему, на военную службу пошел сразу после школы.

На эту тему: **Как выглядит кибервойна с Россией**

Артем Очиченко

В войсковой части 74455 Очиченко занимался разработкой вредоносных вложений к фишинговым письмам при саботаже Олимпийских игр 2018 года. Он также участвовал в атаках на официальные сайты Грузии в 2019 году.

Очиченко родился 8 ноября 1992 года, он вырос в Кубинке, в Московской области.

—

Источник: The Insider

На эту тему:

- «Русские грубо делают свою работу»
- Запоздавшее понимание
- «Дать бой гангстерскому государству Путина» - The Times
- Как «хакер» из Беларуси был осужден в США: приключенческая и поучительная история
- «Всемирноизвестный кибермошенник», разыскиваемый ФБР, идет на выборы от блока Петра Порошенко
- Взлет и падение CarderPlanet глазами участника движения

Share 0

Коментарі

A Billionaire's Reading List: 5 Books
Blinkist Magazine

ТАКОЖ НА АРГУМЕНТ

FT: Трамп відмовив Зеленському ... — місяць тому · 1 коментар — Президент США Дональд Трамп під час зустрічі з президентом України ...

Марина Данилюк-Єрмолаєва: ... — 17 днів тому · 1 коментар — Володимир Олександрович і його пажі часто хизуються, що він ...

«Країна з брехні»: ... — місяць тому — Система ді комунікації час війни п...

Sponsored

A Billionaire's Reading List: 5 Books Cuban Says Everyone Should Know — Blinkist Magazine

Try to find single women here — Asiavibe — Learn More

Incredible: This cushion allows seniors to sit comfortably for hours — Ergonomic Seat Cushion

Incredible: This Cushion Lets Seniors Sit for Hours in Comfort — Ergonomic Seat Cushion

Meet women who want to date online — Japanstates — Learn More

by Taboola

0 Коментарів — Увійти

Розпочати обговорення...

УВІЙТИ ЗА ДОПОМОГОЮ — АБО ЗАРЕЄСТРУВАТИСЬ У DISQUS — Ім'я

Поділитися — Найкращі | Найновіші | Найстаріші

Залиште перший коментар.

Підписатись | Приватність | Не продавати мої дані — DISQUS

ВІДЕО

Друг «Хорус» – про взаємодію штабу та бійців «Азову» — Успіх відбитого штурму не залежить від одного підрозділу.

«Хтось у цьому житті має бути Потапом». Як розпізнавати публічних людей-паразитів на прикладі Потапа і Насті

Будинки та паспорти Росії: що знайшли журналісти в оточенні «Канцлера» з Генпрокуратури

НОВИНИ

15:04 Новини судової мафії України: корумпований Верховний Суд скасував звільнення трьох суддів Київської апеляції, викритих на хабарі $35 тисяч
14:02 Бізнес стрімко адаптує АЗС до ворожих атак, дефіциту пального немає - експерт
13:06 Атака на АЗС столиці: померли двоє поранених, у лікарнях ще шестеро
12:41 Вимагав $5 мільйонів за закриття кримінальної справи - у Києві затримали адвоката
12:05 Іран відновив виробництво балістичних ракет. США заявляли, що іранська ракетна програма знищена
11:40 Трамп зрадив військового союзника - Саудівську Аравію
10:56 У Києві росіяни уразили дві АЗС, є вбитий і поранені
09:01 «Рознесли до бісаₑ» у США визнали знищення бази в Бахрейні ударами Ірану
08:17 У Саратові дрони уразили НПЗ та логістичний хаб Ozon, вирують масштабні пожежі
08:00 Росіяни уразили багатоповерхівку в Києві, двоє поранених

ПІДПИСКА НА КАНАЛ

Додати як бажане джерело в Google

НОВИНИ ПАРТНЕРІВ

У Мукачеві патрульні зупинили водія: під час перевірки... ДЕТАЛЬНІШЕ
В Австралії сексуальне насильство сягнуло 33-річного... ДЕТАЛЬНІШЕ
16-річну дівчину знайшли мертвою у квартирі: поліція... ДЕТАЛЬНІШЕ

РЕКЛАМА

Богдан Сташинський. Що сталося з убивцею Степана Бандери ДЕТАЛЬНІШЕ
Чому осушене Каховське водосховище в Україні має стратегічне... ДЕТАЛЬНІШЕ
Росію хочуть розділити на 4–5 частин: що пропонують? ДЕТАЛЬНІШЕ

© 2011 «АРГУМЕНТ»
Републікація матеріалів: для інтернет-видань обов'язковим є пряме гіперпосилання, для друкованих видань – за запитом через електронну пошту. **Посилання або гіперпосилання повинні бути розташовані при використанні тексту - на початку використовуваної інформації, при використанні графічної інформації - безпосередньо під об'єктом запозичення.** При републікації в електронних виданнях у кожному разі використання вставляти гіперпосилання на головну сторінку сайту argumentua.com та на сторінку розміщення відповідного матеріалу. За будь-якого використання матеріалів не допускається зміна оригінального тексту. Скорочення або перекомпонування частин матеріалу допускається, але тільки в тій мірі, якою це не призводить до спотворення його сенсу.
Редакція не несе відповідальності за достовірність рекламних оголошень, розміщених на сайті, а також за зміст веб-сайтів, на які дано гіперпосилання.
Контакт: uargumentum@gmail.com