Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»

Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

«Русские грубо делают свою работу»

КІБЕРЗЛОЧИННІСТЬ | СР, 2018-02-07 09:22

Версия для печати

Как российские хакеры, связанные со спецслужбами, взламывали серверы за океаном. Об этом изданию The New Times рассказал автор сенсационного расследования о группировке Cozy Bear Хауб Моддерколк.

В Нидерландах не утихает эхо скандала вокруг российской хакерской группировки Cozy Bear («Уютный Медведь»), чью причастность к взлому серверов Госдепа США в 2014 году и Национального комитета Демократической партии США (DNC) полутора годами позже удалось установить Управлению общей разведки и безопасности (AIVD) Нидерландов.

Об этом говорится в сенсационном совместном **расследовании** журналистов Элко Босха ван Розентала и Хауба Моддерколка, которое увидело свет 25 января. Журналисты нашли подтверждения того, что **Cozy Bear** — группа, контролируемая Службой внешней разведки России (СВР). Как отмечалось в расследовании, «логово» Cozy Bear **располагается в «университетском здании рядом с Красной площадью»**, в котором, меняясь в составе, обычно работают порядка десяти человек.

Об этом голландские спецслужбы узнали благодаря взлому не только внутренней системы российских хакеров, но и камеры безопасности, установленной на входе в «офис» Cozy Bear: все, кто входил в эту комнату, голландским спецслужбам давно известны. На днях глава **AIVD** Роб Бертхоли заявил, что у него «нет сомнений» в том, что Кремль несет прямую ответственность за российские кибероперации против правительственных агентств США. Бертхоли также заявил, что уже обсуждал этот вопрос с директором Национальной разведки США Джеймсом Клеппером.

Журналист The New Times поговорил с одним из авторов расследования, корреспондентом газеты **Volkskrant** Хаубом Моддерколком.

НОВИНИ

20:00 **Погода в Україні на 8 травня: місцями короткочасні дощі та грози**

19:09 **Павло Казарін: Пастка безстроковості**

18:04 **Олег Чеславський: ЦПК і розкрадання стратегічних активів**

17:10 **Геннадій Левітас: Піхота - рід військ, який зникає**

16:04 **Касьянов: Вони крадуть 4 млн доларів на добу**

15:10 **Батьки очільника столичної прокуратури Сергія Ходаківського та судді Соборного суду Дніпра Максима Ходаківського у 2020 році придбали квартиру в Москві**

14:59 **ВАКС засудив заступника голови Рівненської облради за хабар до 9 років позбавлення волі**

13:01 **2500 гектарів лісу палає на Чернігівщині через російські обстріли**

12:19 **Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех**

11:50 **УПЦ МП має повернути державі споруди Богоявленського монастиря у Кременці - суд**

ПІДПИСКА НА КАНАЛ

Хауб Моддерколк Фото: flickr.com

> В тему: **Исповедь хакера, взломавшего почту Клинтон: «В ФСБ дали выбор: работать с ними или сесть за взлом»**

ОСОБЫЙ СЛУЧАЙ

— Когда и почему вы решили начать свое расследование?

— Это было в июле 2017 года. Мы с моим коллегой Элко Босхом ван Розенталем из новостной телепрограммы Nieuwsuur работали над другим расследованием, когда вдруг один из наших источников сообщил нам, что голландская разведка предоставила американцам некую информацию о российской кибератаке на Демократическую партию.

Это на самом деле не удивительно, потому что все западные разведки, а помимо них и множество частных компаний, плотно отслеживают деятельность двух хакерских групп — Cozy Bear и **Fancy Bear**. Мы тоже не особо удивились и продолжили то, чем занимались. Но вскоре мы получили новые сведения, в которых утверждалось, что голландцы предоставили американцам еще и информацию о взломе системы Госдепартамента и Белого дома.

Тогда мы крепко задумались и решили: хорошо, бросаем все и копаем здесь. Нас заинтересовало, прежде всего, то, что AIVD сохраняла доступ к внутренним системам Cozy Bear на протяжении как минимум года, а может, и двух лет. К тому же от нашего первого источника мы знали, что голландская разведка буквально видела всю изнанку Cozy Bear. Стало ясно, что это особый случай. Я написал много статей о кибербезопасности, и важно понимать, что в Нидерландах очень хорошая ICT-инфраструктура: спецслужбы фиксируют множество APT-атак, проходящих через страну, отслеживая их происхождение и дальнейшее направление.

Служба разведки и безопасности Нидерландов (AIVD) Фото: commons.wikimedia.org

> В тему: **Голландский университет заявил об увольнении российского физика-шпиона**

И я сперва подумал, что речь шла о чем-то именно таком: ну вот, наши увидели атаку,

вычислили источник и, может быть, продвинулись на один шаг вперед. Но сразу же возникло много вопросов. В итоге мы с Элко поехали в Вашингтон и встретились с американскими источниками. И уже они рассказали нам об атаках на DNC, о Белом доме (хакерам из Cozy Bear удалось с адреса Госдепартамента «отправить» письмо одному из сотрудников Белого дома, тот открыл письмо и ввел свой логин и пароль. — NT) и даже о попытках взлома электронной почты Барака Обамы (хакеры пытались взломать Blackberry Обамы, на котором хранилась значительная часть секретных файлов, но этого им так и не удалось. — NT). Так мы поняли, что за проделками Cozy Bear парни из AIVD следили довольно длительное время. И уже после этого через зашифрованный канал (encrypted channel), я получил от своих источников информацию об университетском комплексе, про который мы рассказали в расследовании.

— Вы написали, что хакеры сидели рядом с Красной площадью. Вы знаете точный адрес?

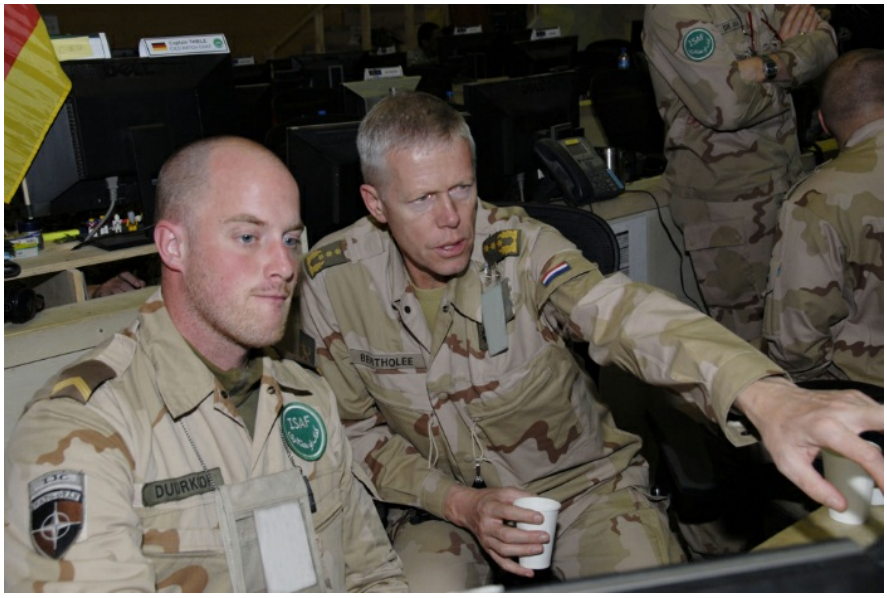
— Нет. Но если вы на google-картах увеличите центр Москвы в радиусе 1 км от Кремля и зададите поиск «университет», то — конечно, это только догадка — одним из результатов будет «университет, занимающийся радиотехникой и электроникой».

— Я уже пробовал. Это Институт радиотехники и электроники при РАН. (Кстати, этот вуз уже не отображается в Google-maps при запросе «университет», только в Яндексе. — NT).

— Да. Но, конечно, я не знаю наверняка: возможно, если вы хотите замести следы, вы будете сидеть и на факультете психологии (факультет психологии МГУ, еще один вуз, находящийся в заданном районе Москвы, также как и факультет журналистики МГУ. — NT). Ведь речь идет о рабочем месте всего лишь для 10 человек, оно не такое уж большое.

— Хорошо. Какого уровня были сотрудники голландских и американских спецслужб, которые поделились с вами информацией? Это были рядовые сотрудники?

— Я не могу об этом говорить, такая информация строго засекречена. У нас было 6 источников, голландских и американских, непосредственно знакомых с материалом. А в общей сложности мы поговорили с 15 осведомленными людьми. Если кто-то из осведомленных источников говорил нам что-то конкретное о Cozy Bear, то мы шли к знакомым людям в частные компании и спрашивали: знаете ли вы что-нибудь про это? Насколько это вообще правдоподобно? Так мы проверяли сведения, которыми нас снабжали.



Глава AIVD Роб Бертоли (справа) на днях заявил, что у него «нет сомнений» в том, что Кремль несет прямую ответственность за российские кибероперации против правительственных агентств США Фото: m.habrahabr.ru

В «МЕДВЕЖЬЕМ» ЛОГОВЕ

— Судя по вашему расследованию, AIVD в течение как минимум двух лет следила за людьми в той самой «университетской» комнате, заполучив доступ к камере на одном из компьютеров. И что теперь будет с этими данными? Попадут ли эти «люди в кадре» в какие-то «черные» или санкционные списки?

— Голландская разведка, в отличие от ФБР или ФСБ, занимается только разведкой, ей не свойственны репрессивные функции или функции дознания и уголовного преследования. Короче, AIVD — не правоохранительный орган. Поэтому оно воспользовалось информацией с камер для своих разведывательных нужд, а потом передала эту информацию американцам. В ходе расследования нас заверяли, что эта информация была критически важна для американцев, чтобы они могли с «большей степенью» быть уверены в причастности Кремля к кибератакам. И этому есть логическое объяснение: благодаря работе AIVD впервые можно утверждать, что Cozy Bear связана с СВР, которая находится в прямом подчинении у Путина.

— Сейчас AIVD больше не имеет доступа к системе Cozy Bear?

— Нет, не имеет.

— А почему?

— Я думаю, нужно иначе ставить вопрос. Иметь такого рода доступ на протяжении такого долгого времени, с 2014 по 2017 год, — это ведь редкая удача. Достаточно сменить настройки firewall или начать использовать другой антивирус — и все, вы доступа лишаетесь.

— Когда конкретно AIVD лишилась доступа?

— Мы этого не знаем. Совершенно точно, что сейчас доступа нет. Мы знаем также, что американцы публично похвастались сотрудничеством с AIVD — мол, есть «западный союзник», обладающий очень хорошей информацией. Реакция в Нидерландах была весьма раздраженной: мы снабдили вас жизненно важной информацией, а вы взяли и рассказали, откуда все получено. Так не делается.

— Вы сказали, что давно работаете с темой кибербезопасности. Насколько опасны Cozy Bear сегодня?

— Я этого не знаю. Конечно, они сменили свой modus operandi и будут менять его и дальше. Кстати, по сравнению с Fancy Bear у них другие методы — они кроты, предпочитающие глубоко шпионить в течение нескольких лет. И они продолжат делать это. Как и американцы, англичане, израильтяне...

Тут важно добавить, что на Западе чаще всего, если не постоянно, говорят о российских хакерах. Объяснений тому два. Первое — политический климат. Второе — российские хакеры довольно грубо делают свою работу, и их нередко вычисляют. Возможно, они делают это преднамеренно, демонстрируя свои возможности и силу, не знаю. Но они точно не одни в этом мире. Американцы и англичане, например, проникали в **Belgacom** (бельгийский оператор связи, атака была в 2013 году. — NT). И, конечно, американцы что-то делают здесь и сейчас в Нидерландах, и англичане в преддверии Brexit тоже. Но они умнее, они лучше шифруются и, может быть, даже работают лучше.

— Раз шпионят все, то можно ли из этого сделать вывод, что атака на Госдепартамент просто шпионаж? Или все-таки прицеливались к выборам 2016 года?

— Думаю, это был рядовой шпионаж, которым занимаются разведки по всему миру. В преддверии выборов все хотят знать, чего ожидать, — тут нет ничего удивительного. Но нужно помнить, что у Хиллари Клинтон и Владимира Путина, так сказать, специфические отношения. Может, именно это и объясняет, почему русская кибератака на Госдепартамент в 2014 году была такой мощной.

> ***КОММЕНТАРИЙ NT:***
>
> *В ноябре 2014-го AIVD успела вовремя предупредить Госдепартамент США о начавшейся атаке со стороны Cozy Bear. Получив доступ к электронной почте и логинам сотрудников Госдепартамента, российские хакеры проникли в незасекреченную часть компьютерной сети. Заметив подготовку, AIVD связалась с представителем Агентства национальной безопасности (АНБ) США в американском посольстве в Гааге, и тот немедленно оповестил об угрозе американские спецслужбы. Последующие 24 часа продолжалась довольно редкая в истории кибербезопасности рукопашная «битва» — Cozy Bear атаковала Госдепартамент вновь и вновь, но благодаря данным голландцев, следивших за группировкой, американцам удавалось отбиваться вручную и с невероятной скоростью.*

В тему: **Георгий Рошка — российский террорист. Почту президента Франции взломали сотрудники ГРУ**

СЛЕД MH-17

— Вы упомянули в расследовании, что, возможно, голландские разведданные были обменяны на какую-то информацию об MH17 (малайзийском Boeing. — NT), которой могли владеть американцы...

— Мы точно знаем, что американцы дали что-то взамен. Но что именно — непонятно.

— Кстати, в свете продолжающегося расследования по Boeing Нидерланды стараются вести себя с Россией весьма осторожно. Ваша же статья, наоборот, подливает масла в огонь.

— Соглашусь с вами. Но ведь не все же замыкается на MH17. Например, голландская полиция тесно сотрудничает с российской ФСБ. Это, в свою очередь, очень не по душе голландской разведке, потому что полиция таким образом впускает в страну сотрудников ФСБ. Полиция, в свою очередь, парирует: мы должны бороться с киберпреступностью, и мы это делаем, сотрудничая в том числе с нашими российскими партнерами. Наша полиция и **ФСБ** доверяют друг другу, хоть это и сложные отношения. И, конечно, если в руки голландцев или русских попадает какая-то критически важная информация о терроризме, они этой информацией делятся друг с другом С другой стороны, если посмотреть на ежегодные доклады AIVD, там постоянные предупреждения о вмешательстве российских спецслужб во внутренние дела Нидерландов, о российском шпионаже и шпионах. В последние годы уровень такой инфильтрации существенно возрос.

— Какой была реакция на ваше расследование?

— Оглушительная. Особенный резонанс был в США. Я думаю, это связано с тем, что Белый дом до сих пор не признает, что россияне стоят за этими атаками.

— А в Нидерландах что говорят?

— Многие гордятся нашими спецслужбами. Но не утихает и дискуссия о том, насколько такие методы работы в принципе допустимы.

НОВИНИ ПАРТНЕРІВ

РЕКЛАМА

—

Эд ван дер Ваарт, Амстердам: опубликовано в издании The New Times

---

В тему:

- **Киберпространство Украины: кремлевское нашествие**
- **«Анонимный интернационал»: «Шалтай-Болтай - побочный продукт других игр»**
- **Российские спецслужбы ведут кибервойну против Германии, - Bild**
- **Виртуальные опричники. Насколько значима российская киберугроза**
- **Как российские хакеры взламывали избирательную систему США. Секретный отчет АНБ«Аргумент»**

Share 0

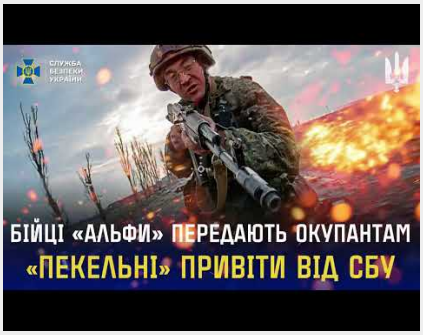
Читайте «Аргумент» в **Facebook** и **Twitter**

Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

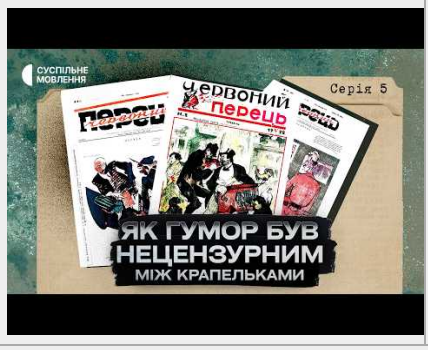
Коментарі

ВІДЕО

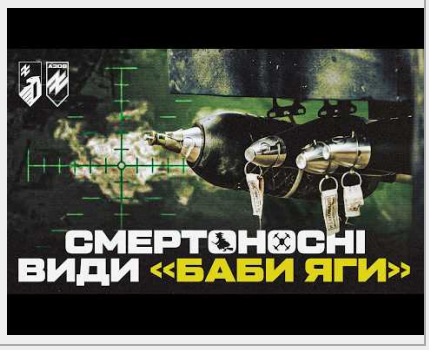
Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні



Про що не можна було жартувати в СРСР



HEAVY SHOT, VAMPIRE, NEMESIS: як «Баба Яга» б'є ок*пантів



© 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 вміст веб-сайтів, на які дано гіперпосилання.
Контакт: ***uargumentum@gmail.com***