Наша Газета
nashagazeta.ch
Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Кибершпионы «Красного октября» проникли в посольства в Швейцарии | «Opération Octobre rouge»: des cyberespions ont attaqué les ambassades en Suisse

Auteur: Людмила Клот, Женева , 22.01.2013.

Сотрудники "Лаборатории Касперского" в Москве (© alternet.org)

Как минимум на протяжении пяти лет преступники воровали информацию у правительственных структур разных стран. По словам эксперта «Лаборатории Касперского», наибольший нелегальный трафик данных шел из Швейцарии.

|

Les pirates sont parvenus à infiltrer des représentations diplomatiques pour y dérober les documents. Parmi les 69 pays visés, la Suisse est le plus touchée selon les sources Le Matin Dimanche.

«Opération Octobre rouge»: des cyberespions ont attaqué les ambassades en Suisse

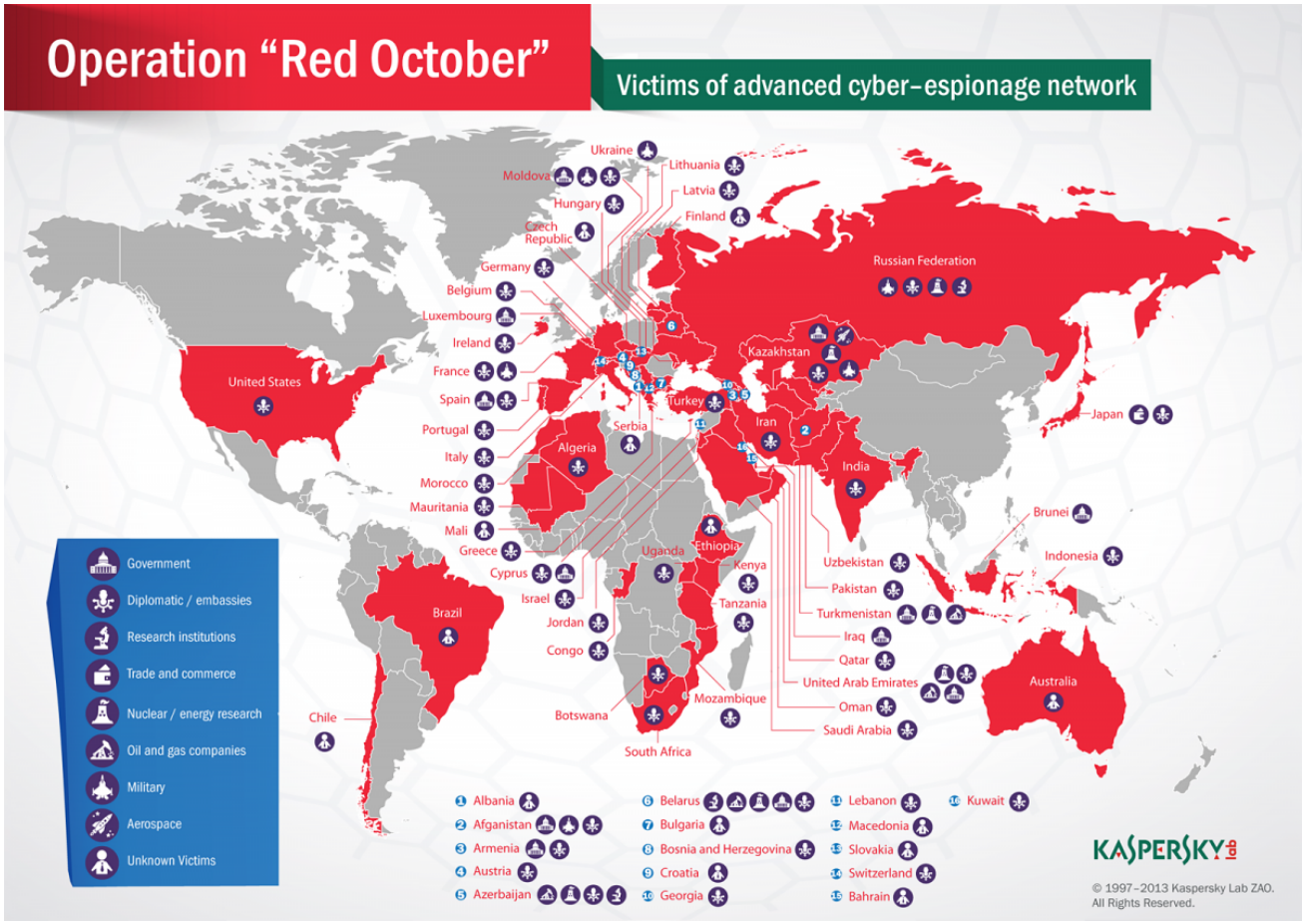
Как стало известно 14 января из обнародованного отчета исследовательского центра «Лаборатория Касперского», эксперты в области компьютерной безопасности вскрыли масштабную шпионскую сеть, которой дали название «Красный октябрь». В течение нескольких лет ее члены нелегально получали через интернет доступ к информации с сотен компьютеров дипломатических представительств, госучреждений и исследовательских институтов по всему миру. Швейцария стала

одной из 69 стран, затронутых этой кибератакой.

Газета Le Matin Dimanche привела комментарии ведущего эксперта по безопасности «Лаборатории Касперского» Костина Раю. По его словам, пираты скачали сотни тысяч гигабайтов информации. «Клик мыши на документ Word, прикрепленный к е-майлу - и вот открывается безобидное объявление: «Продается автомобиль для сотрудников дипломатических представительств, черная «Мазда» 1998 года выпуска, пробег 145 000 км, в превосходном состоянии». Пока работник посольства читает эти строчки, вирус уже загрузился в его компьютер, связывая его со шпионским сервером».

Рутинная работа быстро превратилась в серьезное расследование, и тут эксперты Касперского столкнулись с подобием складного швейцарского ножа для хакеров, пишет Le Matin Dimanche. «Мы идентифицировали более 1000 модулей, которые могут быть использованы в зависимости от надобности», - цитирует газета слова Костина Раю. Например, эти модули позволяли отыскать документы в формате PDF, Word или Excel, подключаться к истории поисков в интернете и зарегистрировать все, что пользователь набирал на клавиатуре.

В числе уже идентифицированных жертв хакеров – посольства, правительственные агентства и армии 69 стран. Основная цель выглядит как желание собрать секретные документы и геополитические данные.



Карта пиратских действий с обозначением наиболее затронутых атаками стран

Пираты зарегистрировали более 60 доменов в Австрии, Германии и России, передавая через них информацию. Правда, за последние месяцы они возобновили

абонементы только для шести из них. «Лаборатория Касперского» воспользовалась этим и выкупила те, что больше не использовались, чтобы извлечь из них информацию, поступавшую от зараженных компьютеров. «Мы получили доступ примерно к 10% трафика», - пояснил Костин Раю. К его удивлению, из тысяч подключений, зарегистрированных между 2 ноября 2012 года и 10 января 2013 года, 20% были сделаны из Швейцарии. Эта пропорция делает Швейцарию наиболее затронутой «Красным октябрем» страной, за ней следует Казахстан (15%).

Часто становились целью кибератак Россия и Азербайджан. Зараженные компьютеры находились в странах бывшего СССР, но также и в странах Европы, Ближнего и Среднего Востока.

«Лаборатория Касперского» передала швейцарским властям адреса IP жертв шпионажа уже в ноябре. «Насколько нам сегодня известно, были затронуты только иностранные представительства, находящиеся в Швейцарии», - пояснил газете Le Matin Пьер-Ален Эльчингер, спикер Федерального департамента иностранных дел. – У нас нет сведений о швейцарских представительствах и компаниях, которые пострадали в результате этой атаки».

Федеральный аналитический центр по безопасности информации MELANI пришел к тому же выводу. «Сейчас мы предупреждаем тех, кого это касается, чтобы они приняли необходимые меры», - прокомментировал аналитик MELANI Мауро Виньяти.

Специалисты из «Лаборатории Касперского» не смогли добраться до истоков атаки. «Мы обнаружили зашифрованными в коде вируса слова из русского арго, что наталкивает на предположения, что атака идет из стран, где используют русский язык», - констатировал Раю.

«Это не говорит о том, что органы государственной власти России связаны со шпионажем, во множестве стран работают говорящие по-русски программисты», - отметил еще один аналитик, заместитель директора Центра глобальных исследований и анализа угроз «Лаборатории Касперского» Мангус Калькул для информационного агентства dpa.

А вот швейцарский эксперт Мауро Виньяти считает, что «очень вероятно, у истоков «Красного октября» стоит какое-либо правительство». Размах и сложность дела исключают работу любителей.

Специалистам «Лаборатории Касперского» пока не удалось обнаружить местоположение основного сервера сети, на который направлялась вся полученная информация. С момента, когда операция «Красный октябрь» была предана гласности, пираты закрыли свои серверы и прервали связь с жертвами. Возможность добраться до них еще сильнее уменьшилась…
кибершпионы
Швейцария
шпионы в швейцарии
кибербезопасность
Статьи по теме
Борьба с вирусами перемещается в швейцарскую глубинку

Source URL:

http://www.nashagazeta.ch/news/politique/kibershpiony-krasnogo-oktyabrya-pronikli-v-posolstva-v-shveycarii