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

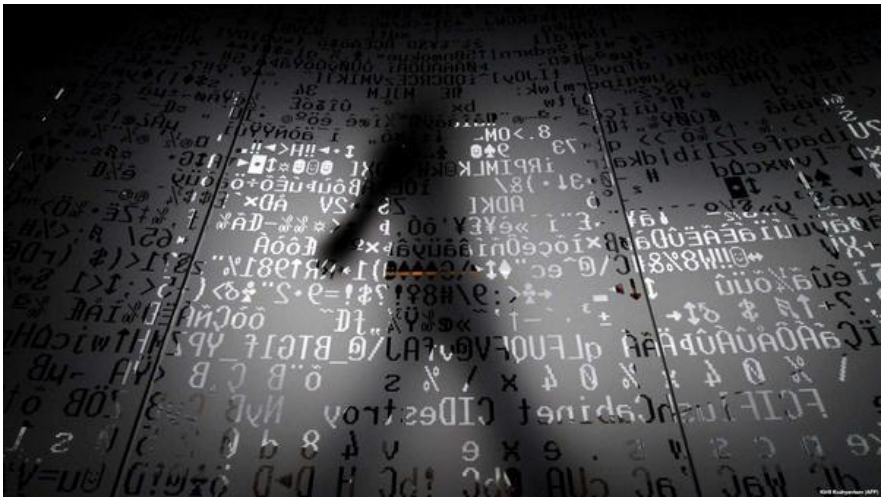
Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Киберхиросима или Удивительные малвари и где они обитают

КІБЕРЗЛОЧИННІСТЬ | ЧТ, 2017-11-23 09:24

Версия для печати



Рассказ о том, как разворачивалась первая мировая кибервойна, какую роль сыграла в нее "Лаборатория Касперского" и что могло случиться с попавшим к ней секретным архивом.

Этой осенью продукты "Лаборатории Касперского" – крупнейшего в мире производителя антивирусного программного обеспечения, красы и гордости российской IT-индустрии – попали под запрет в государственных агентствах США. Вслед за этим Касперский может потерять значительную часть своего американского и западноевропейского рынка, который приносит компании более 60 процентов продаж. **"Лаборатория Касперского"** стала токсичной, и не только потому, что отношения между Россией и США переживают сложные времена, а русские хакеры стали одной из главных страшилок на Западе. Российская компания уже больше 7 лет старательно собирает информацию о кибероружии США, Израиля и Великобритании, публикует аналитические отчеты о нем и предлагает способы защиты. И это давно и многих раздражало.

"Лаборатория Касперского" получила – преднамеренно или нет – исходный код вирусов, созданных Агентством национальной безопасности США, и, как считают некоторые эксперты, поучаствовала в сливе, который нанес больший ущерб репутации американской разведки и национальной безопасности США, чем **Эдвард Сноуден**. Работает ли Касперский на ФСБ или слишком далеко зашел в своем идеализме? Помог ли он создателям вирусов-вымогателей **WannaCry** или все-таки стер случайно попавшие в его руки секретные документы? Разбираемся с историей первой мировой кибервойны, длящейся уже десять лет, в материале, разделенном на две части.

От бани до бана

В середине марта 2015 года один популярный российский тревел-блогер прилетел на Хайнань – тропический остров на юге Китая, на пляжах которого состоятельный путешественник **регулярно** с конца 2000-х устраивал себе короткие передышки от бесконечных перелетов и рабочих встреч. Вот уже несколько дней подряд блогер публиковал фотоотчеты о посещении национальных парков штата Юта в США, но 19 марта вместо однообразных красных скал из песчаника в очередном посте оказался скриншот статьи из издания Bloomberg Businessweek с фотографией самого автора: уперев руки в бока, он из-под густых кустистых бровей уверенно смотрит в объектив. "Компания, которой вы доверяете безопасность вашего интернета, имеет тесные связи с русскими шпионами", – предостерегает заголовок над его головой.

Блогера звали Евгений Касперский, в заметке шла речь о его детище – "Лаборатории Касперского", входящей на тот момент в топ-10 антивирусных компаний мира. Кстати,

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

блог Касперского, заполненный в основном фотографиями из путешествий, сейчас занимает в ЖЖ 346-е место по популярности.

"Я немного был в озлоблении, потом в удивлении, потом в непонятках.. Короче, эмоции танцевали джанго-джанго и пели при этом рэп. – ... а ведь на море, под пальмами, и под мягким мартовским солнышком, пробежавшись рано утром по пляжу, приятно позавтракав настоящей китайчатиной – ай! – ах как хотелось бы продолжить.... чтобы немного отпустить мозг, расслабить тело, и еще денёк полежать.. А хрен тебе, дорогой господин хороший. На тебе порцию говна!" – иронизировал писавший это из номера курортного отеля Marriott Касперский. Он посчитал, что **раскопанные** Bloomberg доказательства связей ЛК и российских спецслужб неубедительны.

Со ссылкой на анонимные источники авторы статьи сообщили, что **Евгений Касперский**, выпускник Высшей школы КГБ, еженедельно посещает баню в компании с сотрудниками российских спецслужб, что после несостоявшегося в 2012 году партнерства по IPO с американской инвестиционной фирмой General Atlantic связи ЛК с ФСБ стали более тесными и в компании ввели мораторий на наем иностранных топ-менеджеров. Наконец, что замглавы компании по юридическим вопросам Игорь Чекунов – лиазон "Лаборатории Касперского" с российскими силовиками и руководит в компании специальным отделом, оказывающим техническую поддержку ФСБ.

"Серьёзное новостное агентство Блумберг искало связь с "русскими шпионами" – и нашло только... баню. Ура!" – писал Касперский из китайских тропиков. Пожалуй, у него действительно был повод для радости, ведь в материале Bloomberg не было ничего о двух событиях, которые к этому моменту уже произошли, но в прессу попали только через два с половиной года. В 2014 году в распоряжение Касперского попали секретные файлы Агентства национальной безопасности США, а внутреннюю сеть компании взломали израильские спецслужбы.

Евгений Касперский

Но Bloomberg написал не про это, а про баню, и заметка не стала серьезным ударом по заокеанскому бизнесу ЛК: созданные компанией программные продукты использовались почти в 20 государственных агентствах США, включая Госдепартамент, министерство обороны, министерство юстиции, армию, флот и военно-воздушные силы. США и страны Западной Европы приносили Касперскому более 60 процентов мировых продаж. Все изменилось в конце весны 2017 года, когда сочетание слов "Россия" и "кибербезопасность" стало устойчиво ассоциироваться с предполагаемым вмешательством российских хакеров в ход президентских выборов в США.

11 мая 2017 года в сенатском комитете по разведывательной деятельности **прошли слушания**, в которых приняли участие руководители ФБР, ЦРУ, АНБ и других силовых агентств США. Речь шла о русских хакерах (на вопрос, вмешался ли Кремль в предвыборную гонку в США с помощью компьютерных взломов, прозвучал единогласный ответ "да"), но на 42-й минуте слушаний сенатор-республиканец из Флориды Марк Рубио поинтересовался, доверяют ли топы разведывательных органов продуктам ЛК. Все шестеро ответили "нет". Вопрос Рубио прозвучал довольно неожиданно; **возможно**, он задал его с подачи кого-то из приглашенных на слушания силовиков. Так или иначе, именно с этого момента у российской компании на рынке США начались серьезные проблемы.

В тот же день, 11 мая, сам Евгений Касперский, отвечая на вопросы читателей популярного ресурса Reddit, заявил, что обмен репликами на слушаниях вызван политическими причинами, которые "лишают этих джентльменов возможности воспользоваться лучшей системой безопасности на рынке без всяких реальных причин или проступков с нашей стороны". Касперский заметил, что готов лично дать показания в американском Сенате (забегая вперед: участие российского предпринимателя в сенатских слушаниях до сих пор так и не состоялось, но все еще **обсуждается**).

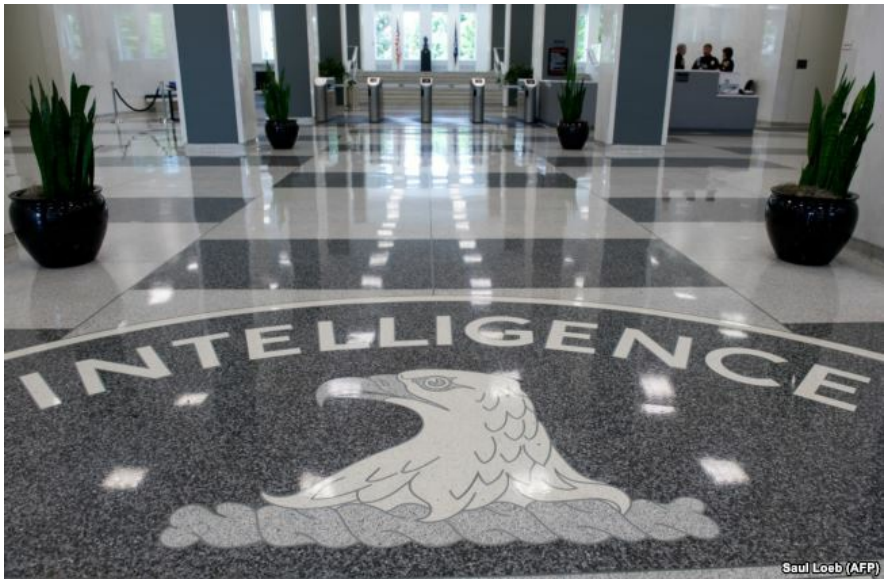
После майских слушаний можно было предположить, что ЛК стала чуть ли не случайной жертвой настороженности американских чиновников и СМИ по отношению ко всему киберроссийскому. Сам Евгений Касперский намекал на это регулярно – в **постах** своего блога, несколько раз прорвавшихся сквозь лавины фотоисторий из экзотических стран, он упоминает и "маккартизм", и "геополитическую турбулентность, от которой страдает бизнес. И причины переживать у него были: поздно вечером 28 июня в личные дома нескольких сотрудников американского офиса ЛК **пришли** агенты ФБР, которые настойчиво интересовались деталями

функционирования компании в США. 5 июля в Сенате **предложили** не включать закупку продуктов ЛК в оборонный бюджет на следующий год. 11 июля агентство Bloomberg (тот же автор, который запустил в 2015 году "**банягейт**") опубликовало новое **расследование** – из попавшей в руки журналистов внутренней переписки следовало, что ЛК участвует в разработке анти-DDoS-систем по заказу ФСБ, а сотрудники участвуют в рейдах силовиков (Касперский подтвердил подлинность переписки, но отверг интерпретацию, сделанную журналистами).

Уже 12 июля General Services Administration, агентство, в частности, отвечающее за госзакупки, **исключило** ЛК из списка авторизованных поставщиков для американских госорганов. В начале осени продукты ЛК исчезают с полок крупнейшего американского ретейлера Best Buy. Наконец, 13 сентября Департамент внутренней безопасности **выпускает директиву**, требующую от всех федеральных агентств США прекратить использование ПО Касперского в течение 90 дней.

Мотивация этого бана – "озабоченность связями некоторых представителей Касперского и российских разведслужб и требования российского закона, которые позволяют российским властям принуждать ЛК к сотрудничеству и получать доступ к данным в российских сетях". Это недвусмысленная отсылка к опубликованному летом расследованию Bloomberg – более убедительному по сравнению с "банягейтом" 2015 года. На этот раз в руки журналистов Джордана Робинсона и Марка Райли попала внутренняя переписка сотрудников ЛК. В письмах 2009 года идет речь о работе над системой, способной защитить клиентов, в том числе правительственные структуры, от DDoS-атак, но в проекте есть и "секретная часть" – поиск источников атаки с помощью хостинговых компаний и разработка "активных ответных мер".

Источник издания заявил, что эти меры – не только ответная атака на хакеров, но и физическое участие специалистов ЛК в рейдах ФСБ. В одном из писем сам Евгений Касперский отмечает, что проект разрабатывается по "большой просьбе со стороны Лубянки". В компании подтвердили подлинность переписки (но не факт участия специалистов в рейдах ФСБ), и на этом основании издание сделало вывод, что "ЛК поддерживает намного более близкие рабочие отношения с ФСБ, чем признает публично".



Лобби ЦРУ

Итак, всего за четыре месяца, прошедшие после как бы случайного вопроса Марка Рубио о доверии ЛК на сенатских слушаниях, компания де-факто лишилась доступа на рынок госструктур США. Примеру федеральных агентств могут последовать, отказавшись от российского антивируса, их многочисленные подрядчики, а вслед за ними другой американский и западноевропейский бизнес и частные лица. И все это – из-за походов в баню с сотрудниками ФСБ и работы над системой, защищающей от хакерских атак? Представители Департамента внутренней безопасности США **признались**, что принимали решение о бане – запрете – продуктов Касперского "по большей части на основе публичной информации". Выходит, Касперский прав, и его американский бизнес страдает от "маккартизма", протекционизма и общей атмосферы недоверия к России, особенно в информационной сфере?

Сожжено перед прочтением

В октябре 2017 года наконец появилось более убедительное объяснение недоверия к Касперскому американской разведки. С 5 по 11 октября в изданиях Wall Street Journal и New York Times вышла **серия** публикаций, в которых **утверждается**, что продукт ЛК, установленный на компьютере у неназванного подрядчика Агентства национальной безопасности США, скачал на сервер "Лаборатории Касперского" секретные файлы АНБ. Бывшие американские разведчики рассказали журналистам, что израильские спецслужбы, взломавшие внутреннюю сеть "Лаборатории Касперского" еще в начале 2014 года, сообщили США, что антивирус Касперского используется для загрузки секретной информации, причем якобы поиск интересных файлов программа осуществляла по ключевым словам вроде top secret.

Разведчики даже специально расставили несколько своеобразных приманок, разместив на компьютерах с установленным российским антивирусом файлы, похожие на секретные, и антивирус, по их словам, на эти приманки "клюнул". Собеседники журналистов назвали случившееся актом шпионажа против США и предположили, что

секретные материалы были украдены "Лабораторией Касперского" по прямому заданию или во всяком случае в интересах российских спецслужб. Именно эта информация, которой американская разведка располагала как минимум с 2015 года, была поводом ответить "нет" на вопрос сенатора Рубио о доверии "Лаборатории Касперского", заданный на сенатских слушаниях весной 2017 года.

У Евгения Касперского есть своя версия развития событий. Однажды поздней осенью 2014 года к нему в кабинет пришел вирусный аналитик. В сеть компании, предназначенную для сбора и анализа потенциально вредоносного программного обеспечения, были загружены файлы, классифицированные системой, как вредоносные и связанные с деятельностью хакерской группировки Equation Group. Один из файлов оказался 7zip-архивом, а внутри него аналитик обнаружил исходные коды вредоносных программ (или, на жаргоне специалистов в компьютерной безопасности, "малварей" – от английского malware) и четыре текстовых документа в формате Word. По заголовкам сотрудник лаборатории понял, что файлы имеют гриф секретности, и сообщил об этом генеральному директору.

Евгений Касперский говорит, что для него сразу стало очевидно, что файлы связаны с АНБ – Агентством национальной безопасности США. Уже несколько месяцев ЛК старательно разыскивала и анализировала вредоносное ПО конкретного типа и, как предполагали специалисты, конкретного авторства. В начале 2015 года Касперский собирался рассказать всему миру о результатах этой работы – об обнаружении "самого продвинутого вредоносного актора, который когда либо-встречался ЛК".

Для него внутри компании уже придумали броское название – Equation Group. Пожалуй, вместо этого подошло бы и другое название – "Те-кого-нельзя-называть". "Знали ли они, что Equation – это спецслужбы? Да, все эксперты это понимали", – говорит специалист по компьютерной безопасности Андрей Споров. Все указывало на то, что в действительности специалисты Касперского обнаружили не хакерскую преступную группировку, а следы деятельности киберподразделения американской разведки.

Логотип АНБ США

"Мы не занимаемся атрибуцией и не знаем, какая именно организация разработала этот зловред, – объясняет Евгений Касперский. – Но учитывая, что мы анализировали эту малварь уже много месяцев, мы знали ее чрезвычайную сложность и полное отсутствие финансовой мотивации у авторов. Кто может разрабатывать сложнейшее вредоносное ПО, при этом без цели заработать денег? Мы были уверены, что за ее разработкой стоят не просто киберпреступники. И поэтому, увидев слова "конфиденциально", я поверил, что это действительно так".

Итак, секретные файлы действительно оказывались в "Лаборатории Касперского" (правда, в 2014-м, а не в 2015 году, как утверждается в материалах WSJ). И израильские спецслужбы могли об этом знать, потому что они в самом деле взломали внутреннюю сеть компании. Об этой атаке сама "Лаборатория Касперского" официально сообщила еще в июне 2015 года.

Заражение началось с компьютера сотрудника одного из небольших офисов "Лаборатории" в Тихоокеанско-Азиатском регионе и произошло, вероятнее всего, через фишинговое письмо. Компания сразу классифицировала атаку как "государственную": "Когда сложное вредоносное ПО пытается атаковать компанию или любую организацию не для кражи денег, то значит, у преступников иная мотивация, то есть шпионаж. Дорогостоящие операции чаще спонсируются кем-то, кто заинтересован в доступе к конфиденциальной информации, а именно государством", – объясняет Евгений Касперский.

Помимо "Лаборатории Касперского" жертвами атаки (специалисты прозвали ее Duqu2.0 за схожесть с вирусом Duqu, о котором будет рассказано позже) стали несколько отелей и конференц-залов в Швейцарии, Австрии и Омане, в которых в 2014 году проходили переговоры международной группы "5+1" по иранской ядерной программе. Это, как и многие другие обстоятельства, указывало на то, что государство, стоящее за атакой – то, которое на эти переговоры не пригласили, – Израиль.

"У инициаторов Duqu 2.0, предположительно, была возможность отслеживать наши

действия, в том числе наблюдать загрузку этого [содержащего секретные файлы АНБ] архива", – признает Евгений Касперский. Вскоре после того, как "Лаборатория Касперского" обнародовала свои данные об Equation Group, антивирусная система обнаружила несколько компьютеров, зараженных вредоносным ПО от этой группы, причем их IP были в том же диапазоне, что и у машины, с которой был загружен секретный архив. "Уже задним числом мы понимаем, что это, скорее всего, были приманки. В тот момент мы просто подумали, что детектировали новый сэмпл зловреда", – говорит Касперский. Таким образом, и факт "ловли на живца", о котором рассказали источники WSJ и NYT, подтверждается.

Итак, секретный архив загружен был, атака на ЛК израильскими спецслужбами тоже была – с этим согласен сам Евгений Касперский. Расхождения начинаются дальше: во-первых, как именно секретные файлы АНБ были загружены в сеть Kaspersky Security Network – случайно или преднамеренно? А во-вторых, что произошло с секретными документами, после того как они оказались в распоряжении ЛК?

Версия Касперского такова. Прямая задача антивируса – искать малвари. И если так получилось, что у кого-то на компьютере нашлись вирусы не потому, что он был ими заражен, а потому что владелец их разрабатывал, можно ли винить в этом антивирус?

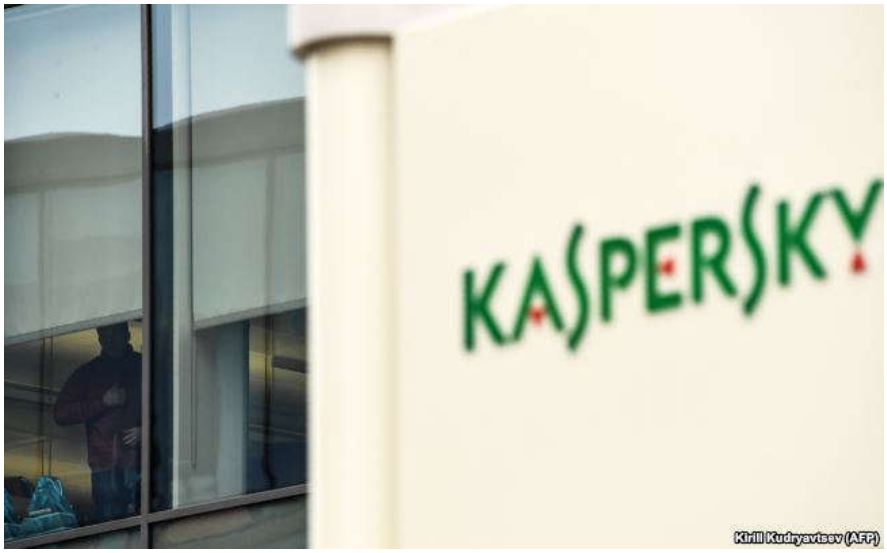
В "предварительном отчете", **опубликованном** ЛК 25 октября (и в его окончательном варианте, который компания **обнародовала** 16 ноября) в ответ на статьи в WSJ и NYT, утверждается, что секретные файлы были загружены в сеть ЛК в период с 11 сентября по 17 ноября 2014 года в ходе нормативной работы домашнего антивируса, установленного на компьютер на территории США.

В настройках такого антивируса можно включить функцию, которая автоматически сканирует память компьютера и загружает в облачное хранилище Kaspersky Security Network образцы потенциально вредоносных программ для дальнейшего анализа. И у американского пользователя эта функция была активирована, то есть пользователь сам предоставил российской компании достаточно широкий доступ к своим данным. Антивирус отправил в свою сеть содержащий малвари архив, а кроме бинарных файлов в нем оказались исходные коды хакерских документов и текстовые документы – так они и попали в компанию, если верить в эту версию.

Источники, упомянутые в статьях WSJ и NYT, утверждают, что все было не так, и антивирус преднамеренно разыскивал секретные документы, причем с особым коварством – по ключевым словам вроде top secret и classified. Евгений Касперский это категорически отрицает: "Наше внутреннее расследование показало, что в "Лаборатории" никогда не производилось детектирование документов по ключевым словам типа "конфиденциально" или "совершенно секретно", – заявил он Радио Свобода.

Впрочем, ответ выглядит несколько уклончиво: "Технически для вендора нет ничего проще, чем вставить в систему поиск строки типа "TS//.*NOFORN" в заголовках документов и таким образом детектировать файлы, помеченные TOP SECRET с предостережением "Не для иностранных граждан", – замечает Николас Вивер, исследователь в области компьютерной безопасности из Международного института компьютерных наук Калифорнийского университета Беркли, США.

Впрочем, Вивер тут же подчеркивает, что никаких публичных доказательств, что ЛК или другой антивирусный вендор когда-либо прибегали к такому методу, нет. Скорее всего, фраза, о том, что антивирус Касперского мог искать секретные файлы по таким ключевым словам - следствие неверно понятой фразы источника, которая затем превратилась в журналистский фольклор. А вот искать по названиям секретных проектов АНБ, обнародованных в сливах Сноудена, смысл был.



Так считает, например, Шон Таунсенд, независимый **исследователь** в области информационной безопасности, участник и спикер **Украинского киберальянса**: "Лаборатория Касперского" разыскивала исходные коды целенаправленно, например, по каталогу проектов и инструментов АНБ, опубликованному Эдвардом Сноуденом после побега в декабре 2013 года. "Искал долго, около года, – уверен украинский исследователь. – Нашел компьютер в США, где нужная информация была, и слил всё к себе".

В "Предварительном отчете" "Лаборатории Касперского" Таунсенд видит несколько технических несостыковок, например, его удивляет заявление специалистов, что содержавший секретные файлы архив был загружен в сеть Касперского, потому что

был определен как вредоносный. "Последняя уязвимость в архиваторе 7zip была обнаружена в 2009 году. Эта отмазка нужна для того, чтобы объяснить, почему был загружен в лабораторию весь архив целиком, а не отдельный файл", – предполагает украинский эксперт.

Вот еще одна несостыковка: в отчете подробно описано, что компьютер, с которого антивирус загрузил секретный архив, был заражен вирусом-троянцем Mokes через пиратский генератор ключей для Microsoft Office, и именно это якобы привлекло особое внимание аналитиков Касперского. Таунсенд говорит, что такого рода инфекции достаточно тривиальны и заинтересовать специалистов не могли, хотя специалисты Касперского подчеркнули факт этого заражения, намекая, что к компьютеру с секретными файлами могли иметь доступ и создатели бэкдора Mokes, который связывают с Китаем. В целом же Таунсенд называет внутреннее расследование компании неуклюжей попыткой откреститься от обвинений в шпионаже.

Второй спорный момент – что случилось с секретными файлами, в частности, с исходными кодами малварей Equation Group, после того как они оказались у Касперского. Сам он утверждает, что они были немедленно удалены по его прямому указанию. "Потому что данный вредонос уже был обнаружен нами ранее и не был нам нужен или интересен в качестве нового образца. Вторая причина – это проблема с обработкой конфиденциальных материалов", – объясняет он мотивацию. Теперь, говорит Касперский, в компании даже введено внутреннее правило, предписывающее сразу удалять любые потенциально секретные материалы, которые могут быть случайно обнаружены вирусными аналитиками компании.

Вот в это готовы поверить не все. "Отчет Касперского звучит убедительно, но с одним огромным исключением, – замечает Николас Вивер. – Если он получил исходный код инструментов АНБ, он бы ни за что не уничтожил копии. Обладание исходниками дает огромное преимущество: вредоносное ПО в принципе работает потому, что его сложно отличить от безопасного, антивирусам приходится полагаться на эвристические техники, которые не всегда работают. Поэтому любой антивирусный вендор мечтает заполучить исходные коды".

Даже если исходные коды попались Касперскому случайно, удалять их не имело смысла, но что, если это именно то, за чем аналитики по каким-то причинам охотились? Утечка исходных кодов кибероружия, разработанного АНБ США, в сеть Касперского предшествовала событию, о котором говорят как о причинившем больший ущерб национальной безопасности США, чем деятельность Эдварда Сноудена. Не слишком ли хорошее совпадение? Летом 2016 года американское кибероружие появилось на открытом рынке, а чуть позже с его помощью неизвестными хакерами были нанесены первые удары. Какой могла быть роль "Лаборатории Касперского"?

Для того чтобы разобраться в этом, нужно вспомнить историю самой настоящей кибервойны, которая идет в мире вот уже десять лет. В ней используют оружие стоимостью в миллионы долларов, которое наносит не только виртуальные, но и реальные разрушения. Ее участников все знают, но никто не может назвать официально. Ее последствия опасно недооценивать.

> В тему: **«Антивирус Касперского»: угроза для государства Украина**

В полнолуние они превращаются в хакеров

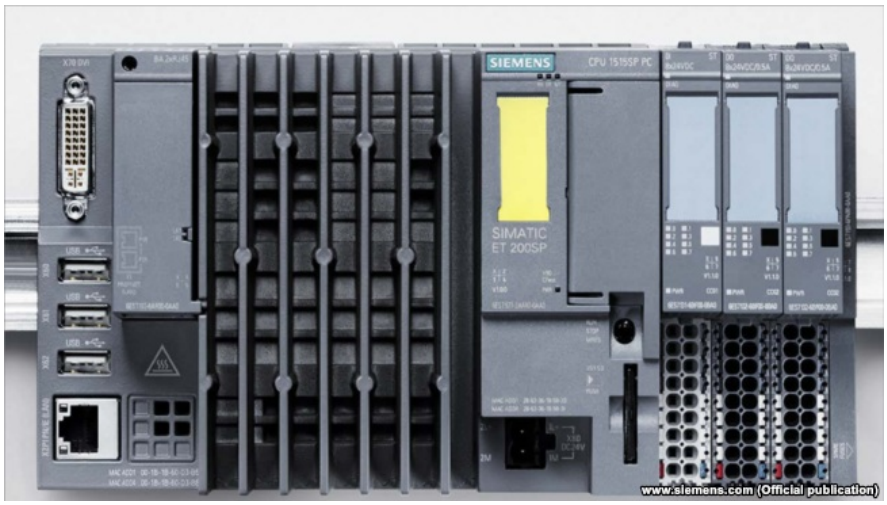
Итак, осенью 2017 года российская "Лаборатория Касперского" оказалась под угрозой лишиться большей части своего прибыльного американского рынка. Причина – подозрения в тесных связях с ФСБ, а особенно информация, что компания преднамеренно выкрала секретные документы Агентства национальной безопасности США, а именно исходные коды созданных американскими разведчиками вирусов. Евгений Касперский заявил, что файлы компания получила случайно и тут же удалила, но поверить ему готовы далеко не все. А если все же не удалила? Вторая часть расследования Радио Свобода – об идущей уже 10 лет мировой кибервойне, в которую ввязалась "Лаборатория Касперского", и о том, как попавший к ней секретный архив мог стать причиной вирусного заражения Чернобыльской АЭС, российских отделений полиции и шоколадной фабрики из Тасмании.

Киберхиросима и другие атаки Equation Group

Одним теплым вечером в июне 2010 года белорусский программист Сергей Уласен **веселился** на свадьбе у друзей в 400 километрах от Минска, когда на его телефон пришло уведомление: с Уласеном хотел срочно связаться абонент из Ирана. Разговор затянулся: “Вокруг ходили разодетые в пух и прах веселые девчонки с игристым в бокалах, никто не мог понять, зачем мне понадобилось висеть на телефоне и объяснять кому-то странные вещи на странном языке, при том что я находился в лесу на свадьбе”, – вспоминал Уласен в интервью.

За пару дней до этого ему, на тот момент сотруднику небольшой белорусской антивирусной компании "ВирусБлокАда" переслали письмо иранского клиента. Клиент жаловался на проблемы с компьютерами в сети – одни стали постоянно перезагружаться, на других появился “синий экран смерти” – критическая ошибка Windows. Сначала Уласен решил, что дело в неправильной конфигурации операционной системы, но почитав отчет более внимательно, понял – сеть пострадала от хакерской атаки.

Специалист по компьютерной безопасности со стороны клиента сказал, что разберется с ней, но когда к субботе – рабочему дню в Иране – ничего так и не вышло, он позвонил белорусскому коллеге с просьбой о помощи. К понедельнику вирус был изолирован, а способы его распространения и эффективной защиты от обнаружения изучены. Так был обнаружен компьютерный червь Stuxnet, который позже стали считать первым в истории наступательным кибероружием.



Программируемый логический контроллер Siemens

Уласен определил, что червь использует уязвимость нулевого дня (то есть ранее неизвестную) Microsoft Windows, распространяется через флеш-накопители и локальные сети и использует украденные цифровые сертификаты. Все указывало на то, что конструировали его специалисты очень высокого уровня. Но зачем? С этим спустя несколько дней смог разобрался немецкий аналитик, изучивший выложенные Уласеном на один из месседж-бордов данные: он выяснил, что необычный вирус предназначен для атаки на программируемые логические элементы фирмы Siemens – устройства, которые используются для автоматизации технологических процессов на производстве.

Фактически Stuxnet был способен нанести физический вред оборудованию, заставляя оборудование работать в нештатном режиме, причем незаметно для инженеров. Переключение сигналов светофора, регулировка систем водоснабжения, работа оборудования атомных электростанций – все это использует программируемые логические элементы, которые оказались уязвимы перед новым вирусом. Червь выглядел первой реальной угрозой человечеству, способной выйти из киберпространства в физический мир – чем-то из фильмов про Джеймса Бонда, и за изучение его функциональной части – необычайно объемной и сложной для компьютерного вируса – взялись независимые эксперты, Microsoft и все крупнейшие антивирусные компании, в том числе "Лаборатория Касперского".

Именно специалисты ЛК первыми установили, что Stuxnet использует не одну, а как минимум четыре уязвимости “нулевого дня” – указание на то, что создатели вируса имеют существенные технологические и финансовые ресурсы. Тогда Евгений Касперский **впервые заподозрил**, что опасный червь сконструирован в интересах государственных структур, вот только в каких? В ноябре 2010 года специалисты американской компании Symantec установили, Stuxnet атакует частотно-регулируемые приводы, устройства, с помощью которых регулируется скорость центрифуг, например, на заводе по обогащению урана в иранском Натанце.

Махмуд Ахмадинежад на обогатительном заводе в Натанце, Иран

Предположения, что Stuxnet специально направлен на иранскую ядерную программу, звучали еще до этого открытия Symantec, а теперь получили дополнительное подтверждение. Гипотеза, что вирус был создан именно с этой целью, а создателями выступили совместно разведывательные органы США и Израиля, становилась все более популярной и находила все больше косвенных подтверждений – от убедительных, вроде соответствия тайминга выхода новых версий Stuxnet и заявлений официальных лиц по ядерной программе Ирана, до конспирологических – например, в коде вируса один раз встречается константа 19790509, а 9 мая 1979 года в Иране был казнен промышленник еврейского происхождения Хабиб Эльганян.

А вот официальных подтверждений, разумеется, не было и нет – ни со стороны предполагаемых создателей, ни со стороны жертв атаки. Наверняка неизвестно и то, смог ли Stuxnet нанести заметный ущерб иранской ядерной программе – по **косвенным данным отчета** МАГАТЭ можно предположить, что на производстве в Натанце пострадали около 1000 центрифуг, которые, впрочем, были быстро заменены. Кстати, в 2013 году Евгений Касперский со ссылкой на анонимный источник **сообщил**, что Stuxnet заразил внутреннюю сеть одной из российских АЭС. По его словам, это произошло в период наибольшей активности вируса (то есть в 2009–2011 гг). Так или иначе, за Stuxnet закрепилась репутация “киберхиросимы” – первого в истории кибероружия.

Но далеко не последнего: в сентябре 2011 года был обнаружен вирус Duqu – троянская программа, предназначенная для кражи информации с зараженного компьютера. Исследователи – российская "Лаборатория Касперского", американский Symantec и многие другие – сразу заявили, что это вредоносное ПО создавали авторы Stuxnet, во всяком случае, люди, имевшие доступ к исходному коду Stuxnet. Заражение Duqu также использовало уязвимость нулевого дня Microsoft Windows, троян использовал украденный цифровой сертификат, принадлежащий тайваньской корпорации.

Дальнейший анализ показал, что большинство заражений DUQU произошли в Иране, инициаторов атаки интересовала, как утверждается в **отчете**, подготовленном ЛК, “любая информация о системах управления производством в различных отраслях промышленности Ирана, а также информация о торговых отношениях ряда иранских организаций”. Интересно, что заражение Duqu не было массовым – всего по имеющимся данным от атаки пострадали не более 50 объектов. Специалисты Symantec **считают,** что задачей Duqu был сбор данных для более точной настройки очередной версии Stuxnet.

Весной 2012 года был обнаружен вирус Flame – как и Duqu, этот червь занимался сбором информации: он мог делать скриншоты экранов зараженных компьютеров, записывать аудио, используя встроенный микрофон, скрытно передавать собранные данные на командно-контрольный сервер. Возможности Flame были крайне широки – вирус пользовался огромной библиотекой функций, это пакет программных модулей общим объемом в небывалые для вирусов 20 мегабайт (для сравнения, размер функциональной части Stuxnet – всего 500 килобайт). Значительная часть жертв Flame **находились** на Ближнем Востоке, большинство из них все в том же Иране (среди первых обнаруженных случаев заражения были компьютеры иранского министерства нефти).

Изначально специалисты ЛК посчитали Flame самостоятельным проектом, который развивался параллельно Stuxnet и Duqu, однако после более глубокого анализа заявили, что авторы – те же, причем Flame как платформа разрабатывался еще в 2007–2008 годах, и ее модули позже были использованы в Stuxnet. Через несколько дней после того, как ЛК опубликовала эти выводы, в издании The Washington Post вышла **заметка**: авторы со ссылкой на анонимные источники в американском разведывательном сообществе заявили, что Flame и Stuxnet – совместная разработка АНБ, ЦРУ и израильских военных, эти инструменты были созданы в рамках программы с кодовым названием “Олимпийские игры”, задачей которой было затормозить развитие иранской ядерной программы.

Операция, якобы, была начата еще в середине 2000-х, во время второго президентского срока Джорджа Буша-младшего. Источники заявили газете, что апрельская атака на иранское министерство нефти была произведена Израилем без согласования с американской стороной, и последовавшее за этим обнаружение Flame вызвало недовольство в США. Еще одно свидетельство – попавший в открытый доступ **документ** АНБ, в котором упоминается, что обнаружение Flame должно стать одной из тем обсуждения представителей АНБ и электронного подразделения британской разведки GCHQ. Официального подтверждения, разумеется, не последовало, но публикация WP стала еще одним подтверждением того, на что уже давно намекали в ЛК: Flame, Stuxnet, Duqu и некоторые другие вирусы, созданные на той же технологической платформе (например, Gauss, троянский вирус, предназначенный для кражи разведывательной информации финансового характера, пострадали от него в первую очередь клиенты ливанских банков), – кибероружие, созданное усилиями двух государств для атаки на третье государство.

"Группа уравнения" и "Теневые брокеры"

В 2009 году некий ученый побывал на международной конференции в Хьюстоне, штат Техас. Некоторое время спустя он, как и другие участники, получил стандартный сувенир – компакт-диск с фотографиями с конференции. Ученый вставил его в свой компьютер и начал просматривать снимки, при этом он “понятия не имел о том, что стал жертвой могущественной организации, занимающейся кибершпионажем и только что заразившей его компьютер вредоносным кодом, применив при этом три эксплойта, два из которых были эксплойтами нулевого дня”. Эта история об анонимном ученом, настоящее имя которого не называется для “защиты тайны частной жизни”, **рассказана** в блоге ЛК, “могущественная организация” – группировка хакеров под условным названием Equation Group, об обнаружении которой специалисты Касперского объявили на саммите по кибербезопасности в Мехико в феврале 2015 года.

Если Stuxnet, Flame, Duqu одновременно исследовали аналитики из крупнейших антивирусных компаний мира, то Equation Group – собственный трофей ЛК. Именно в московской лаборатории придумали это название для “одной из наиболее изощренных хакерских группировок в мире”, именно специалисты Касперского выпустили **подробный отчет** о деятельности EG – практически одновременно с объявлением о ее существовании.

Согласно этому отчету, группировка действовала как минимум с 2001 года, а возможно и раньше – с 1996-го. За это время хакеры разработали несколько платформ вредоносного ПО, которые и стали основой для атак Stuxnet, Flame, Duqu, Gauss и

даже Regin – вирусом, который **связывают** с британским управлением радиоэлектронной разведки GCHQ (буквально – “Центр правительственной связи”). Получается, Equation Group – сборное подразделение разведок США, Израиля и Великобритании?

ЛК как обычно нигде не говорит об этом прямо, но намеков дает достаточно. Например, в программных модулях EG “забыты” некоторые ключевые слова, в том числе “GROK”, “STRITACID”, “DRINKPARSLEY”, “STEALTHFIGHTER”. Эти слова совпадают (или крайне похожи) с названиями некоторых проектов и файлов Tailored Access Operations, киберподразделения АНБ, которые упомянуты в **секретной презентации АНБ**, слитой неизвестным инсайдером немецкому журналу **Der Spiegel** в 2013 году, и в **данных**, предоставленных журналистам Эдвардом Сноуденом в 2014 году.

Авторы отчета не утверждают прямо, что Stuxnet, Flame и другие известные “государственные” кибератаки – дело рук Equation Group, но дают понять, что они использовали схожие эксплойты, программные модули, имели близкие наборы целей. “[EG] много лет взаимодействует с другими влиятельными группировками, такими как Stuxnet и Flame”, – уклончиво предполагают в ЛК. Кстати, список наиболее пострадавших стран, красноречиво приведенный в отчете ЛК, выглядит еще одним подтверждением связи между АНБ и EG: это главным образом Иран и Россия, а также Пакистан, Афганистан, Индия, Китай, Сирия и Мали. Некоторые из атак EG были направлены очень точно, в частности – на посетителей форумов исламских джихадистов, причем с некоторыми исключениями: заражению не должны были подвергнуться посетители из Турции, Египта и Иордании.

Итак, многие факты указывают на то, что “инструменты Equation Group” (которая, возможно, существует только на бумаге и в воображении специалистов ЛК) – кибероружие, разработанное специальными подразделениями разведок нескольких стран, в первую очередь ТАО, входящей в АНБ США. И это оружие вскоре попало в другие руки – и показало человечеству, чем может обернуться кибератака в современном мире.

Иранский ядерный завод в Натанце

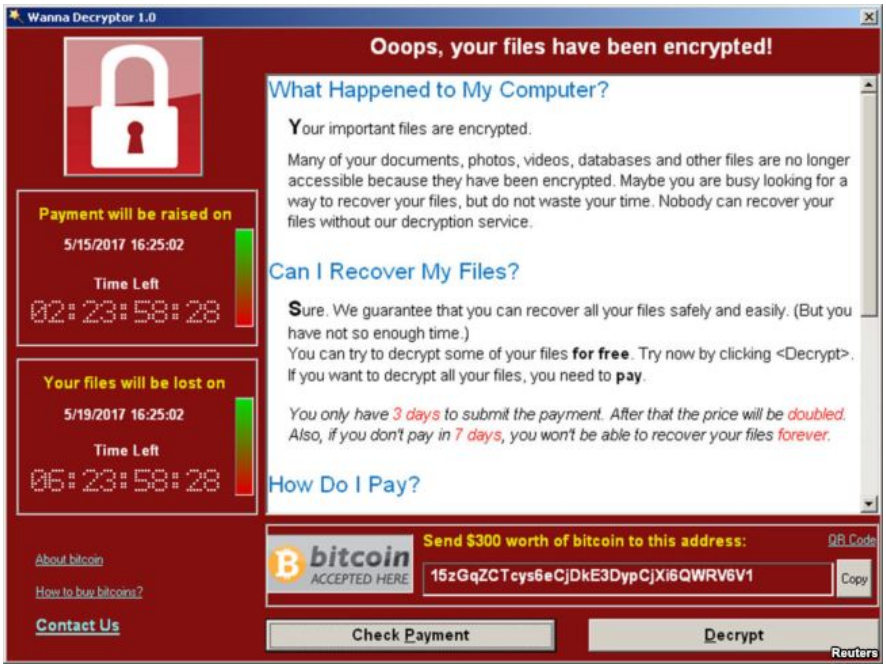
В мае 2017 года компьютерные вирусы на некоторое время стали главными героями передовиц: массовое заражение червем-вымогателем WannaCry на некоторое время парализовало работу некоторых отделений МВД в России, заводов Renault во Франции, энергетической компании в Испании, больницы на Тайване, шоколадной фабрики в Тасмании. На экране инфицированных компьютеров появлялось сообщение, что все данные зашифрованы и расшифровать их можно, только заплатив выкуп – биткоины в эквиваленте 300 долларов США. Всего атаке подверглись более полумиллиона устройств по всему миру, но больше всего случаев заражения было зафиксировано на Украине, в России и Индии. Позже эксперты установили, что злоумышленники заработали всего несколько десятков тысяч долларов, а система получения ключа за выкуп изначально была реализована с ошибкой, то есть отправлять хакерам деньги не имело никакого смысла. Кто стоял за этой атакой, неизвестно до сих пор.

Месяц спустя произошла еще одна очень похожая атака. Вирус-вымогатель, который специалисты окрестили Petya2.0 или NotPetya, поразил в первую очередь государственные и коммерческие компании Украины, в том числе правительственную сеть, Национальный банк, аэропорты Киева и Харькова и даже службу радиационного контроля Чернобыльской АЭС, которая была вынуждена временно отключиться от интернета. Позже заражению подверглись устройства и в других странах – России, странах Западной Европы, США и Индии.

Как и WannaCry, вирус Petya2.0 требовал выкуп за расшифровку данных – и снова в этом изначально не было смысла, другими словами, атака была произведена не ради наживы, а для нанесения ущерба. Российская компания Group-IB **считает**, что за этой атакой стоит “прогосударственная группа Black Energy”. Впрочем, на самом деле BlackEnergy – название не группировки, а хакерской атаки, произведенной на украинские энергетические объекты в декабре 2015 года. Этот вирус **связывают** с российской группой Sandworm, регулярно атакующей украинские объекты на фоне конфликта между двумя странами.

Обе атаки, помимо псевдовымогательства и акцента на Украине, объединяет любопытный факт: они использовали уязвимости, предположительно разработанные

Equation Group. Эти инструменты каким-то образом попали в распоряжение загадочной хакерской группировки The Shadow Brokers, которая летом 2016 года выставила их на открытый аукцион.



Экран компьютера, зараженного вымогателем WannaCry

The Shadow Brokers возникли летом 2016 года словно бы из ниоткуда. 13 августа в только что созданном твиттер-аккаунте @shadowbrokerss появилась ссылка на **приглашение** поучаствовать в “аукционе кибероружия Equation Group”. На ломаном (пожалуй, даже нарочито) английском языке его авторы сообщают: “Мы взломали Equation Group. Мы нашли много-много кибероружия Equation Group. Вы видите картинки. Мы предлагаем вам некоторые файлы Equation Group бесплатно, видите? Это достаточное доказательство нет? Вы наслаждайтесь!!!”.

Это как если бы у армии США украли ракеты "Томагавк"

Одним из выложенных группировкой инструментов был эксплоит EternalBlue, и именно на нем спустя несколько месяцев были построены атаки WannaCry и Petya2.0. В день, когда была обнаружена атака WannaCry, 14 мая 2017 года Microsoft опубликовал о**фициальное заявление**, в котором открыто раскритиковал АНБ и ЦРУ за “накопление [компьютерных] уязвимостей”. Государственные разведывательные структуры знают о дырах в компьютерных системах, например той, которую использует эксплойт EternaBlue, но хранят эту информацию при себе, не позволяя вендорам выпускать заплатки.

А что, если такое кибероружие попадет в руки преступников? “Тот же сценарий в обычных вооружениях – это как если бы у армии США украли ракеты "Томагавк”, – заметил президент Microsoft Брэд Смит. Аутентичность дампа The Shadow Brokers позже подтвердил и бывший министр обороны США и директор ЦРУ Леон Панетта, **признавший** в интервью в ноябре 2017 года, что “эти утечки нанесли огромный ущерб нашим разведывательным и кибернетическим возможностям [...] Когда такое происходит, приходится начинать все сначала”.

Так в чьи же руки попали кибертомагавки? The Shadow Brokers продолжили публиковать утечки до апреля 2017 года. Каждое объявление сопровождалось текстом анархистского толка, например, утечка конца октября 2016 года содержала **призыв** “взламывать” президентские выборы в США или мешать им – “Может, люди не идут на работу, ищут местные места для голосования, протестуют, блокируют, мешают, ломают оборудование, рвут бюллетени?”. В другом сообщении авторы иронизируют: “Российские безопасники по ночам превращаются в российских хакеров, но только при полной луне”. Но корявый английский язык, намеки на связь с Россией, идеологизированное содержание этих сообщений могли быть умелой маскировкой. Примечательно, что финансовый вопрос как будто с каждым сообщением все меньше интересует хакеров – они готовы отдать инструменты едва ли не бесплатно.

В ноябре 2017 года газета New York Times **рассказала**, что продлившееся полтора года внутреннее расследование АНБ слива The Shadow Brokers (который охарактеризован как больший ущерб американской разведке, чем действия Сноудена) изначально разрабатывало две версии – внутреннюю утечку и внешнюю атаку, причем вероятнее всего со стороны России. Или и то, и другое. В связи с расследованием были арестованы как минимум три сотрудника АНБ (один из них – тот самый, с чьего компьютера антивирус Касперского сгрузил секретные файлы).

Эдвард Сноуден выступает на конференции по кибербезопасности через видеосвязь

Но рассуждая о второй версии – внешней хакерской атаке, журналисты упоминают российскую компанию, которая “готовила отчет, который позволил поменяться с США местами [в направлении хакерских атак], (...) охотилась на шпионское ПО, установленное хакерами АНБ отчасти на основе ключевых слов и кодовых имен, озвученных в файлах мистера Сноудена и опубликованных журналистами”. Эта компания, разумеется, – "Лаборатория Касперского", а отчет – описание инструментов Equation Group, которое можно сравнить с досье кибернетических возможностей АНБ.

Жертва навета или жертва провала

Итак: "Лаборатория Касперского" год за годом изучает, анализирует, описывает “государственные” атаки – Stuxnet, Duqu, Flame, Gauss, Regin, за которыми, на что регулярно намекают отчеты компании, стоят спецслужбы США, Израиля и Великобритании. Некоторые из этих вирусов ЛК анализирует параллельно с другими крупными вендорами, как например со Stuxnet, наиболее подробный отчет о котором составила калифорнийская Symantec. Другими малварями, как с Flame, российский вендор занимается заметно обстоятельнее конкурентов.

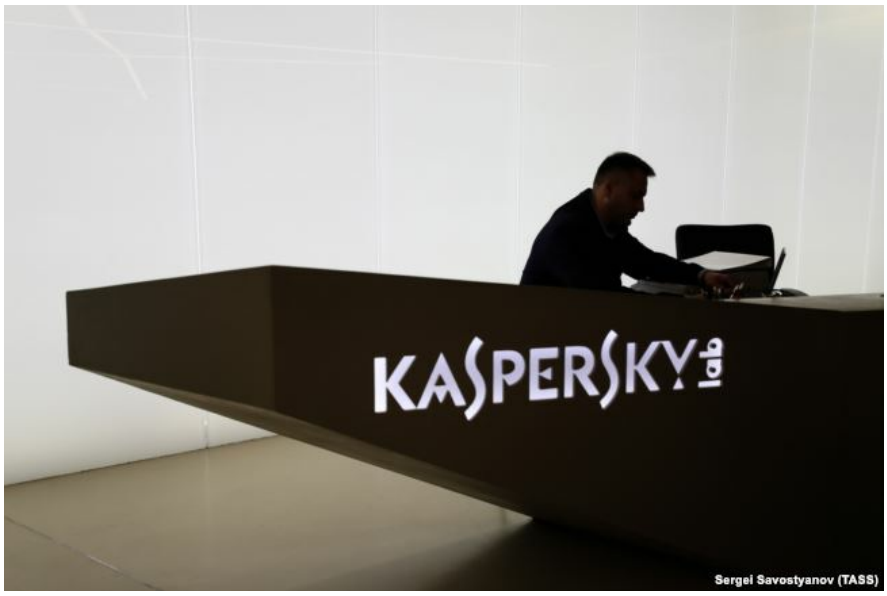
Наконец, ЛК полностью самостоятельно и первой в мире описывает самый мощный киберарсенал, принадлежащий Equation Group, а на самом деле, и в этом мало кто сомневается, киберподразделению АНБ (и, возможно, аналогичным структурам некоторых союзников США). В какой-то момент в руки компании попадает архив, содержащий некоторые исходные коды этих инструментов. И вот год спустя в интернете возникает таинственная группировка, называющая себя The Shadow Brokers, которая предлагает приобрести исходные коды малварей Equation Group (используя название, изобретенное ЛК).

Кто еще, кроме "Лаборатории Касперского", так давно и старательно соблюдал информацию об арсенале АНБ, кто имеет для этого технические возможности, чей еще антивирус способен “случайно” зацепить и загрузить на свой сервер секретные документы и исходные коды малварей? Предположение, что между The Shadow Brokers и "Лабораторией Касперского" можно поставить что-то вроде знака равенства, не выглядит таким уж диким.

Эксперт по кибероружию и бывший хакер Андрей Споров уверен, что между ними во всяком случае существует связь, то есть The Shadow Brokers выставили на продажу файлы, доставшиеся им напрямую или опосредованно, например, через российские спецслужбы, от "Лаборатории Касперского". “Это мое субъективное профессиональное экспертное мнение. Я говорил про SB, когда никто в СМИ не говорил, что ЛК получила что-то, имеющее отношение к Equation. Для меня просто было очевидно сочетание всех фактов. Я никогда не верил в то, что SB видит своими целями какие-то продажи и т. п. Для меня это так же было очевидно, что это "увод в сторону", цель не в этом”, – объясняет Споров.

При этом все случившееся – от интереса Касперского к Equation Group через дамп The Shadow Brokers и к проблемам американского бизнеса ЛК эксперт называет провалом российских спецслужб. Споров рассуждает о том, что могло произойти на самом деле: компания могла передать силовикам попавшее к ней импортное кибероружие в качестве оперативных материалов, то есть для изучения и внутренней работы, но не для публичного использования или тем более публикации.

Спецслужбы же из собственных политических соображений могли организовать слив информации через выдуманную группировку The Shadow Brokers и тем самым, во-первых, раскрыли свой источник и методы получения информации, во-вторых, походя, разрушили зарубежный бизнес одного из самых успешных российских несырьевых экспортеров, а в-третьих, сделали российский софт на много лет вперед токсичным, как и многое, что происходит из страны “водки, медведей и КГБ”.



В лобби "Лаборатории Касперского"

В том, что The Shadow Brokers слили файлы, полученные Касперским, уверен и украинский эксперт по кибербезопасности Шон Таунсенд. Он напоминает о порядке событий, описанном в начале этой главы: интерес ЛК к Equation Group, признанная компанией загрузка исходных файлов инструментов АНБ и – спустя год, как раз вскоре после обвинений в адрес России во взломе серверов комитета Демократической партии США, – появление инструментов **АНБ** на открытом рынке. “С моей точки зрения, не так уж важно, кто именно стоит за TSB, – это мог быть сотрудник Касперского, сам Касперский или к примеру **ФСБ**. Касперский мог отдать информацию чекистам, а реализовать ее (не в техническом, а в политическом плане) могла другая спецслужба, даже не понимая, что при этом случится с ЛК”, – рассуждает Таунсенд.

Может быть, Касперский передал ФСБ секретные файлы АНБ из патриотизма – чтобы помочь защитить страну от угрозы извне? Евгений Касперский категорически отрицает, что в принципе мог иметь такую мотивацию. “Если мы получим образец наступательного кибероружия, то мы тут же разработаем способ защиты наших пользователей и распространим его через обновления, – заявил он Радио Свобода. – Я неоднократно подчеркивал, что как частная компания мы не имеем никаких политических связей с каким бы то ни было правительством. Мы гордимся своим партнерством в сфере борьбы с киберпреступностью с властями разных стран и международными правоохранительными организациями, включая Интерпол, Европол и ООН. Повторюсь, мы сотрудничаем исключительно с борцами с киберпреступностью”.

В убедительно выглядящих описаниях того, как могла выглядеть связь ЛК и The Shadow Brokers, не хватает одного – доказательств. Евгений Касперский настаивает, что стер попавший в компанию секретный архив, и утверждает, дамп The Shadow Brokers в любом случае состоит из других файлов: “Насколько мы можем судить по телеметрии, это были разные архивы”, – утверждает он.

Независимый американский специалист Николас Вивер отмечает, что в версии о существовании связи между ЛК и сливом SB есть нестыковки: “The Shadow Brokers выложили четыре транша данных. Два из них были точно украдены с отладочных серверов под Linux, через которые аналитики из АНБ атакуют свои цели, еще один очевидно был с рабочей Windows-системы аналитика, и еще там был один набор инструментов под Windows неизвестного происхождения (возможно, с той же рабочей станции), – рассуждает Вивер. – К тому же тайминг не совпадает. Словом, есть НОЛЬ улик, что Касперский связан с The Shadow Brokers и много улик, доказывающих противоположное”.

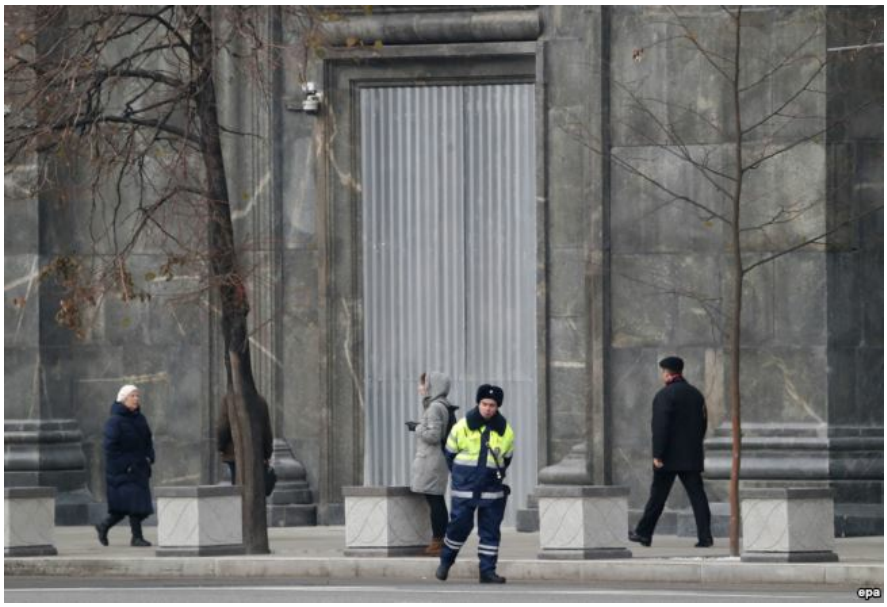
В окончательном отчете о загрузке секретного архива в 2014 году специалисты Касперского делают особый упор на то, что американский компьютер, с которого файлы попали в сеть Касперского, был заражен более чем сотней вирусов, в том числе бэкдором Mokes, связанным с китайской хакерской группой (в начале 2010-х его предлагали приобрести в российском киберподполье, замечают авторы документа), и все это является прямым намеком на то, что секретная информация из того же архива могла оказаться не только у Касперского и именно от третьей стороны попасть в руки The Shadow Brokers.

Токсичность

В мае – июне 2017 года издание The Insider **опубликовало** несколько материалов о взломе почты президента Франции Эммануэля Макрона. В частности, журналисты рассказали о том, что один из взломщиков косвенно **связан** с Центром специальных разработок Минобороны России. Об этом же достаточно новом подразделении российской армии **писало** и издание Meduza в материале, описывающем, из каких частей могут состоять российские кибервойска или пресловутые “российские государственные хакеры”. Центр специальных разработок активно нанимает программистов и специалистов в криптографии. Чтобы привлечь талантливых студентов, эта любопытная организация даже **регулярно** поддерживает **соревнования** CFT (Capture The Flag) – популярную в России командную игру для white hats, то есть хакеров, которые занимаются не атаками, а защитами от них. Другим

активным участником CFT-движения является "Лаборатория Касперского".

Следует ли из этого, что Касперский связан и с армейскими хакерами? Нет, но очевидно, что крупнейшая в стране компания, занимающаяся кибербезопасностью, регулярно сталкивается с соответствующими подразделениями в разведке, полиции и Министерстве обороны. В конце концов, кадров соответствующей квалификации в стране не настолько много, чтобы эти структуры не боролись за одни и те же таланты, не знали друг друга по конференциям, не были однокашниками, не перетекали между одними и теми же организациями.

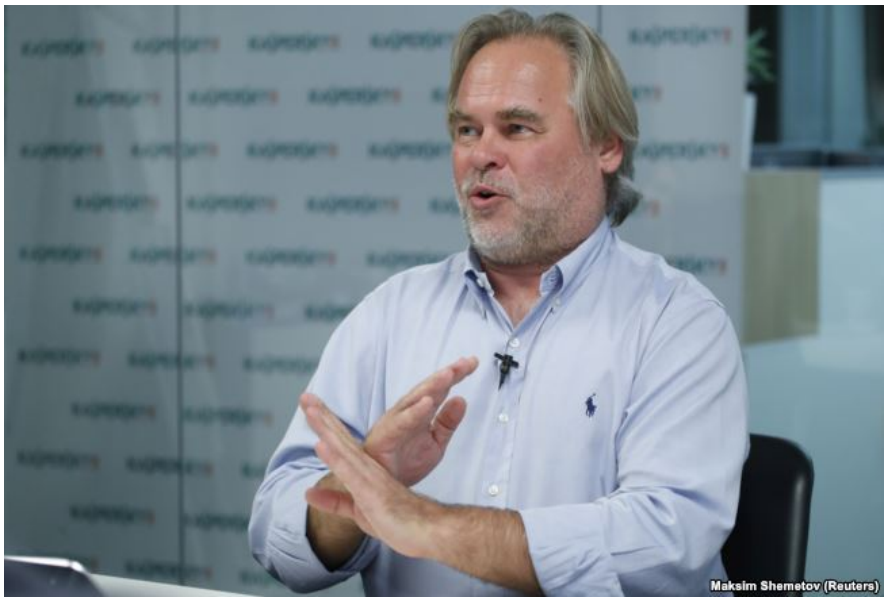


Вход в здание ФСБ после акции Павленского

Яркий пример – бывший сотрудник подразделения по борьбе с киберпреступностью (управления “К”) ГУВД Москвы майор Руслан Стоянов, в 2012 году ставший главой отдела расследований "Лаборатории Касперского". МВД и ФСБ привлекали подразделение Стоянова к поиску и задержанию группировки хакеров, создавшей вирус Lurk. С его помощью со счетов пользователей в России и странах бывшего СНГ была похищена астрономическая сумма.

В конце весны 2016 года правоохранители с удовлетворением **отчитались** о задержании преступников. А через полгода Стоянова, а также сотрудников Центра информационной безопасности (ЦИБ) ФСБ России Сергея Михайлова и Дмитрия Докучаева **арестовали** по обвинению в госизмене – по данным Reuters, “фигуранты дела передавали секретные данные американской компании Verisign и другим коммерческим организациям, которые в свою очередь передавали эти данные спецслужбам США”. Кстати, не задержание ли группировки Lurk, к которому привлекли "Лабораторию Касперского", имели в виду авторы расследования в Bloomberg?

Еще одна публичная связь между ЛК и спецслужбами – центр реагирования на инциденты в сфере информационной безопасности (CERT), который создается "Лабораторией Касперского" для отражения атак на ключевые объекты российской инфраструктуры, такие как атомные электростанции, предприятия ядерно-топливного, нефтегазового и энергетического комплексов. Вероятно, этот центр будет **работать в связке или как часть системы** "ГосСопка" (системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы), создание которой в январе 2013 года Владимир Путин поручил ФСБ. Комментируя эту работу, Евгений Касперский заявил: “Мы вовлечены в экспертную работу и используем все возможности сотрудничества для борьбы с вредоносным кодом и хакерами. При этом мы всегда действуем как независимая коммерческая компания, не ангажированная госструктурами”. Кстати, не об этой ли системе защиты от хакерских атак, которой ЛК занимается по “большой просьбе с Лубянки”, идет речь в материале Bloomberg?



Евгений Касперский: Мы сотрудничаем только с теми спецслужбами, которые борются с преступниками. Точка

“Мы сотрудничаем с российскими спецслужбами в той же мере, что и с любыми другими международными правоохранительными организациями. Наше взаимодействие строится исключительно на совместном расследовании киберпреступлений. Точка. Мы сотрудничаем только с теми спецслужбами, которые борются с преступниками” – так выглядит стейтмент Евгения Касперского по поводу подозрений о связи его компании с ФСБ (отдельно он подчеркнул, что истории о “группе Чикунова” в ЛК – “бред и неправда”). Можно ли было увязнуть коготком, а всей птичке не пропасть – и ограничиться совместным походом в баню, поимкой преступников и работой над большой оборонительной системой?

Неизвестно, но крестовый поход Касперского против “государственных” вирусных атак не мог не заинтересовать российские спецслужбы и не стать раздражителем для американских. Теперь "Лаборатория Касперского" декларирует **принцип прозрачности** и готова открыть код своих продуктов, чтобы все убедились – они не занимаются поиском по ключевому сочетанию “top secret”. Основатель компании рвется свидетельствовать перед Сенатом США. Но уже, вероятно, поздно – чекистская токсичность, все сильнее поражающая Россию, перекинулась и на “Лабораторию Касперского”, словно какой-нибудь компьютерный вирус.

—

Сергей Добрынин, опубликовано в издании Радио Свобода

В тему:

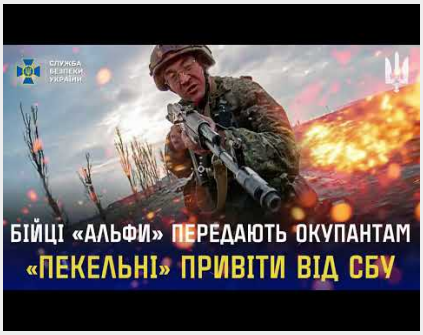
- **Интернет-троллинг превратился в индустрию**
- **Конец Mega-D. Житие и бИтие Великого Спамера: как не стоит зарабатывать деньги**
- **Взлет и падение CarderPlanet глазами участника движения**
- **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб?**
- **Кибер-война: в атаку идут только хакеры и боты**

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

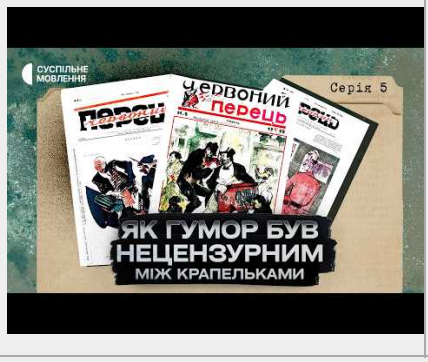
Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

Коментарі

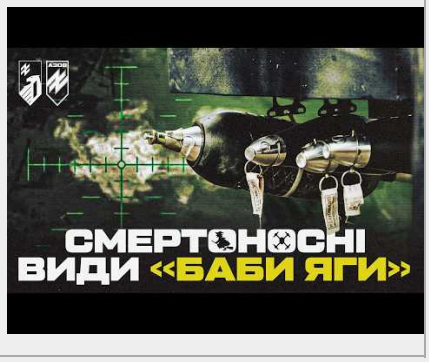
Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні



Про що не можна було жартувати в СРСР



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



Контакт: ***uargumentum@gmail.com***