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

Евгений Касперский: От кибербезопасности к кибериммунитету | Evgeny Kaspersky: De cybersécurité au cyberimmunité

Автор: Надежда Сикорская, Цюрих , 02.10.2019.

Евгений Касперский в Цюрихском политехе (c) Robert Hradil, ETH-Zurich

Летом 2019 года Высшая федеральная техническая школа Цюриха (ETH) при содействии Швейцарско-российского форума организовала встречу с Евгением Касперским, генеральным директором «Лаборатории Касперского» – одной из крупнейших в мире частных компаний, работающих в сфере информационной

безопасности. Лекция на тему «Глобальное состояние кибербезопасности» привлекла внимание продвинутых студентов и их профессоров, зал не смог вместить всех желающих. Дождавшись начала нового учебного года, мы делимся с вами основными моментами встречи с российским предпринимателем, избравшим Швейцарию новым направлением развития своего глобального бизнеса.

|
Evgeny Kaspersky: De cybersécurité au cyberimmunité

Постоянные читатели Нашей Газеты еще в мае 2018 года узнали, что компания, разрабатывающая системы защиты от киберугроз, перенесет датацентр и сборку программного обеспечения в Цюрих. В частности, речь шла о том, что в Цюрихе будут находиться системы, на которых происходит обновление антивирусных баз и создаются продукты компании. Кроме этого, в Конфедерации будут размещены серверы, на которых хранятся и обрабатываются данные пользователей из Европы, Северной Америки, Японии, Южной Кореи, Австралии и Сингапура, т.е. из всех стран, кроме России. Особо подчеркивалось, что каждый факт доступа к данным будет регистрироваться, и журналы регистрации можно будет в любой момент посмотреть. Изменения не коснутся российских пользователей: их данные по-прежнему будут храниться на территории России.

«Лаборатория Касперского» анонсировала открытие в Цюрихе первого центра прозрачности, в котором можно будет проверить исходные коды любого продукта компании и облачных сервисов, где хранятся и обрабатываются данные пользователей. В центре будет предоставляться доступ к документации по разработке программного обеспечения и инструментам, используемым для создания продуктов, антивирусных баз и облачных сервисов. «Ответственные государственные и частные организации, располагающие необходимыми знаниями и опытом, смогут проверить наше программное обеспечение и убедиться в том, что оно работает именно так, как заявлено», – говорилось в коммюнике. Дополнительные центры прозрачности планируют открыть в Азии и Северной Америке к 2020 году.

Год спустя, на Петербургском международном экономическом форуме, нам удалось из уст самого Евгения Касперского услышать, почему именно маленькая Швейцария была избрана компанией, созданной супругами Касперскими в 1997 году, а сегодня обеспечивающей работой свыше 4000 высококвалифицированных специалистов в 30 с лишним странах и поставляющей свою продукцию 400 млн человек по всему миру. «По очевидным причинам – из-за своей двухсотлетней истории нейтралитета, репутации безопасного центра и надежной законодательной базы», тогда сказал российский предприниматель.

Тогда же г-н Касперский поздравил Швейцарию с полученной возможностью хранить на своей территории огромное количество европейских данных под присмотром «the best security guy», в очередной раз блеснув чувством юмора, не покидающим его даже в самые серьезные моменты.

Не будем кривить душой и уверять, что решение обосноваться в Швейцарии компания, входящая в четвёрку ведущих мировых производителей программных решений для защиты конечных устройств (Endpoint Protection), приняла по собственному желанию. При всех швейцарских прелестях истинная причина, как и усилившийся интерес к прозрачности, в том, что, после обвинений в сотрудничестве

с ФСБ, ряд западных правительств запретил использование ее продукции на территориях своих стран. Надо сказать, что Касперский не скрывает того факта, что в 1987 году он окончил 4-й (технический) факультет Высшей школы КГБ (в настоящее время этот факультет известен как Институт криптографии, связи и информатики Академии ФСБ России).

В начале октября 2018 года все программы Касперского были официально запрещены к использованию федеральной администрацией США, после чего нацеленность компании, отрицающей все обвинения в кибершпионаже и других вредоносных действиях, на сотрудничество со Швейцарией еще укрепилась. Что же касается отношений с Америкой, то кратко Касперский суммирует ситуацию так: «Продажи в США упали на 25%, в остальном мире выросли».

Показательно, что Швейцария не испугалась ни мощного заокеанского партнера, ни самого Касперского, продукцией которого, кстати, пользуется и федеральная администрация. Конфедерация не скрывает своего намерения «создать общие условия, благоприятствующие развитию экономики и цифрового общества во всей Швейцарии», и тот факт, что первое публичное выступление Евгения Касперского состоялось в стенах лучшего университета страны, занявшего шестое место и опередившего Кембридж в рейтинге вузов мира, опубликованного британской консалтинговой компанией Quacquarelli Symonds в 2019 году, подтверждает это стремление.

Вход в Цюрихский политех (c) Nashagazeta

Не стоит удивляться, что большая аудитория была заполнена до отказа, пришлось даже организовывать стриминг в соседней – кибербезопасность давно стала общей проблемой, и даже нашей скромной редакции довелось столкнуться с ней, когда в 2012 году сайт Нашей Газеты подвергся хакерской атаке и чудом выстоял. А потому мы с большим интересом слушали признанного эксперта, взошедшего на кафедру в джинсах, стараясь разобраться в сложных терминах и выявить понятную простому смертному суть. Вот что из этого вышло.

Существуют три категории вредоносных программных обеспечений (ПО) и использующих их кибератак: массовые, но средней сложности; целевые атаки, организуемые высококвалифицированными хакерами, и атаки на критические инфраструктуры, на промышленные предприятия.

Цифры, иллюстрирующие атаки первый категории, впечатляют: если в 1998 году в день фиксировалось 50 вредоносных действий разного масштаба, то в 2018-м их было уже 380 000. «То есть из двух миллионов ежедневно аккумулируемых файлов 380 тысяч содержат новые, еще не известные вредоносные программы. Собираются они со всего мира, и не всегда можно точно определить местонахождение источника, однако эксперты Лаборатории Касперского в большинстве случаев способны расшифровать их "язык"», – рассказал Евгений Касперский. По его словам, накопленные данные позволяют утверждать, что самый распространенный язык в киберпространстве – китайский, за ним следуют испанский и португальский (причем можно отличить истинно испанский источник от латиноамериканского), русский, ломаный и родной английский, арабский и так далее. «Атаки на ретороманском языке пока на фиксировались, как, впрочем, и на японском!», – пошутил эксперт, уже на полном серьезе подведя первый итог: киберпреступность многоциональна и многоязычна.

Разумеется, невозможно вручную разбираться со всеми этими тысячами мелких атак, для этого существуют специальные системы, с помощью компьютерного осмысления обрабатывающие 99.999% всей получаемой информации. Научно доказано, что невозможно разработать алгоритм, который распознавал бы другие алгоритмы в 100% случаев, значит, надо подобраться к этой цифре как можно ближе. «Мы работаем над этим с помощью инженеров, математиков, представителей других наук, учась узнавать вредоносов в лицо, по запаху, по поведению и т.д., – приоткрыл Евгений Касперский дверь за кулисы своей профессии. – Этот процесс мы называем «дятлом»: как он долбит червяков, там мы – хакеров. С оставшимся 000,1% разбираемся вручную, подключая наших человеческих «дятлов». Это невероятно увлекательная работа!»

(c) Nashagazeta

С целевыми атаками дело обстоит гораздо сложнее, но их, к счастью, и значительно меньше – чуть более сотни в год. Иногда это так называемые семьи вредоносных ПО, иногда одни и те же ПО, подгоняемые под конкретную цель/жертву. 90% таких атак, осуществляемых профессиональными инженерами, финансируются государствами, остальные 10% – чисто преступные. «Как отличить первых от вторых, шпионскую деятельность от киберпреступления? – задал Евгений Касперский вопрос аудитории и сам на него ответил: Очень легко! Если цель атаки – деньги, то это преступление, а если особая информация – шпионаж. Исключение составляет Северная Корея, где нет частных компьютеров, так что за любой атакой стоит государство». При этом установить авторство таких атак крайне сложно, а тыкать пальцем, рискуя попасть в невинного, – нецелесообразно. Иногда удается получить доказательства – либо через программный код, или благодаря утечке информации, полученной агентствами компьютерной контрразведки. Так удалось доказать, что за вредоносным ПО Stuxnet, направленным против ядерных проектов Ирана, стояли американские и израильские спецслужбы, и правительство США в итоге подтвердило это информацию.

«Самые активные шпионские атаки, «говорящие» по-английски, происходят в атлантической временной зоне, по-русски – в восточно-европейской (и обычно прекращаются в период новогодних праздников), как и те, что используют разговорный китайский язык, замирают во время китайского Нового года», – продолжал Касперский смешивать почти анекдоты с правдой, подводя слушателей к ключевому заявлению: родной язык всех главных профессиональных

киберпреступников без исключения – русский. «Русские разработчики программ – лучшие в мире», и это не мои слова, а Кондолизы Райс, бывшего госсекретаря США, позволившей мне ее цитировать. А русские киберпреступники – худшие, – не без определенной гордости сообщил Евгений Касперский, уточнив, что под «русскими» надо понимать русскоязычных хакеров, среди которых замечены граждане не только Российской Федерации, но и Украины, стран Прибалтики, США, Израиля, многих европейских стран. «Общее у них одно, все они – выпускники советских или уже российских вузов».

Лучшие – они же худшие! – кибервредители не разменываются на мелочи и концентрируются на атаках третьего уровня, поражающих инфраструктуры. «Обезвредить их крайне сложно: проникнув в сеть, злоумышленники могут делать с ней все, что им заблагорассудиться. Достаточно вспомнить кибербанду Carbanak, с помощью фишинговой рассылки с вредоносными вложениями получавшую доступ к внутренней сети банка и похитившей в общей сложности миллиард долларов! К счастью, их удалось раскрыть и арестовать».

Как же защитить себя и свой бизнес от киберпреступников? По словам Евгения Касперского, сегодня в мире существуют несколько достойных антивирусных решений, способных предоставить практически стопроцентную защиту от атак первой категории. Что же касается атак, совершаемых целенаправленно квалифицированными профессионалами, то тут стандартными мерами предосторожности не обойдешься: надо заниматься постоянным анализом своих ресурсов, обращая внимание на малейшие аномалии.

Атака на инфраструктуру, то есть на любое производство, в принципе угрожает любому предприятию, от шоколадной фабрики до атомной станции. Вот как обрисовывает возможную ситуацию Евгений Касперский. «Вы просыпаетесь утром, привычно идете на кухню, чтобы сварить кофе, принимаете душ… Вся эта информация передается в систему резервного копирования, «iCloud», которая уже знает, что через 45 минут вы вызовите такси. Автоматический автомобиль еще до вызова подъезжает к вашей двери. Системе известно и о двух соседях, с которыми вы делите такси…» Таким образом, вся наша личная и профессиональная жизнь копируется на «облаке». «Вы думаете, что сами управляете своим роскошным автомобилем? Не обольщайтесь! Просто вы еще не ощутили вмешательства, а оно уже возможно». И в этом заключается дилемма Индустриальной революции 4.0, делающая ее уязвимой: без резервного копирования вы – банкрот, потому что ваши соперники это сделают, а с ним вы – покойник, потому что хакеры могут проникнуть в систему и все уничтожить. «Не знаете, что выбрать, обратитесь к Касперскому!», – без лишней скромности посоветовал Евгений Валентинович и тут же сменил тон.

«Если серьезно, то настоящее решение заключается в постепенном переходе от кибербезопасности к кибериммунитету, который можно определить так: стоимость атаки должна быть выше, чем стоимость преодоления ее последствий». По мнению эксперта, прийти к этому можно, более того, в теории решение выглядит довольно просто: надо создать такую архитектуру операционных систем и приложений, чтобы финансовые вложения хакера для ее взлома превосходили урон, который он способен нанести. «Иными словами, если у вас есть турбина стоимостью миллион франков, то атака на нее должна стоить больше миллиона». Лаборатория Касперского уже сегодня предлагает возможное решение – микроядерную архитектуру, в которой все компоненты «общаются» друг с другом исключительно через безопасные каналы. Для атаки на такую систему надо проникнуть в слишком много индивидуальных систем одновременно, что повышает для хакера риск быть разоблаченным.

Первое совещание, посвященное безопасным операционным системам, состоялось в Лаборатории Касперского еще в 2002 году. Затем эту идею на несколько лет оставили за отсутствием нужного финансирования, но потом вернулись к ней, серьезно взявшись за дело. На сегодняшний день уже имеется начальное оборудование, есть камеры безопасности, установленные в одном из районов Москвы в рамках проекта «умный квартал», есть прототип чипа, собираемого из ненадежных компонентов, но в итоге становящегося надежным – по примеру автомобилей. «Мы контролируем поведение каждой составляющей системы и не даем им вести себя плохо», – объясняет Евгений Касперский, чтобы даже далеким от этой темы слушателям стало ясно. «В настоящий момент мы реально создаем новую экосистему и ищем достойных партнеров – сделать предстоит многое, места хватит всем, а заинтересованность в успехе у нас общая, поскольку и враг общий». На логичный вопрос прагматичного швейцарского студента, как зарабатывать деньги на иммунитете, если он создается непосредственно на охраняемом объекте, а не привносится извне, Евгений Касперский немедленно ответил: «Гугл тоже в начале не знал, как заработать. Важно иметь яркую идею, деньги придут!»

(c) Nashagazeta

4000 сотрудников, половина из которых – математики, разработчики программ, инженеры разных направлений, специалисты по кибербезопасности. Как привлекать таланты? «Найти хорошего начальника отдела кадров! А если серьезно: работаем со многими университетами, активны на рынке труда. Большинство IT-инженеров и разработчиков – русские, а эксперты – из разных стран, от Бразилии до Австралии, единственное принципиальное исключение – Северная Корея. Наши центры, разбросанные по всему миру, выступают в роли датчиков, собирающих информацию и предупреждающих наших партнерах о возможных угрозах».

Число кибератак, увы, растет, проблема уже прибрела глобальный размах, а значит, будет расти спрос и на услуги «Лаборатории Касперского». Интуиция подсказывает, что в недалеком будущем в мирную армию ее сотрудников вольются и швейцарские специалисты.
отношения сша и швейцарии
кибербезопасность
Статьи по теме
«Лаборатория Касперского» переведет часть инфраструктуры из России в Швейцарию
Швейцария не боится Касперского
ПМЭФ-2019: открытые площадки и кулуары

Source URL:
https://nashagazeta.ch/news/les-gens-de-chez-nous/evgeniy-kasperskiy-ot-kiberbezopasnosti-k-kiberimmunitetu