Как выжить в эпоху новых кибер-атак на миллион долларов

pandasecurity.com

panda

О PandaLabs

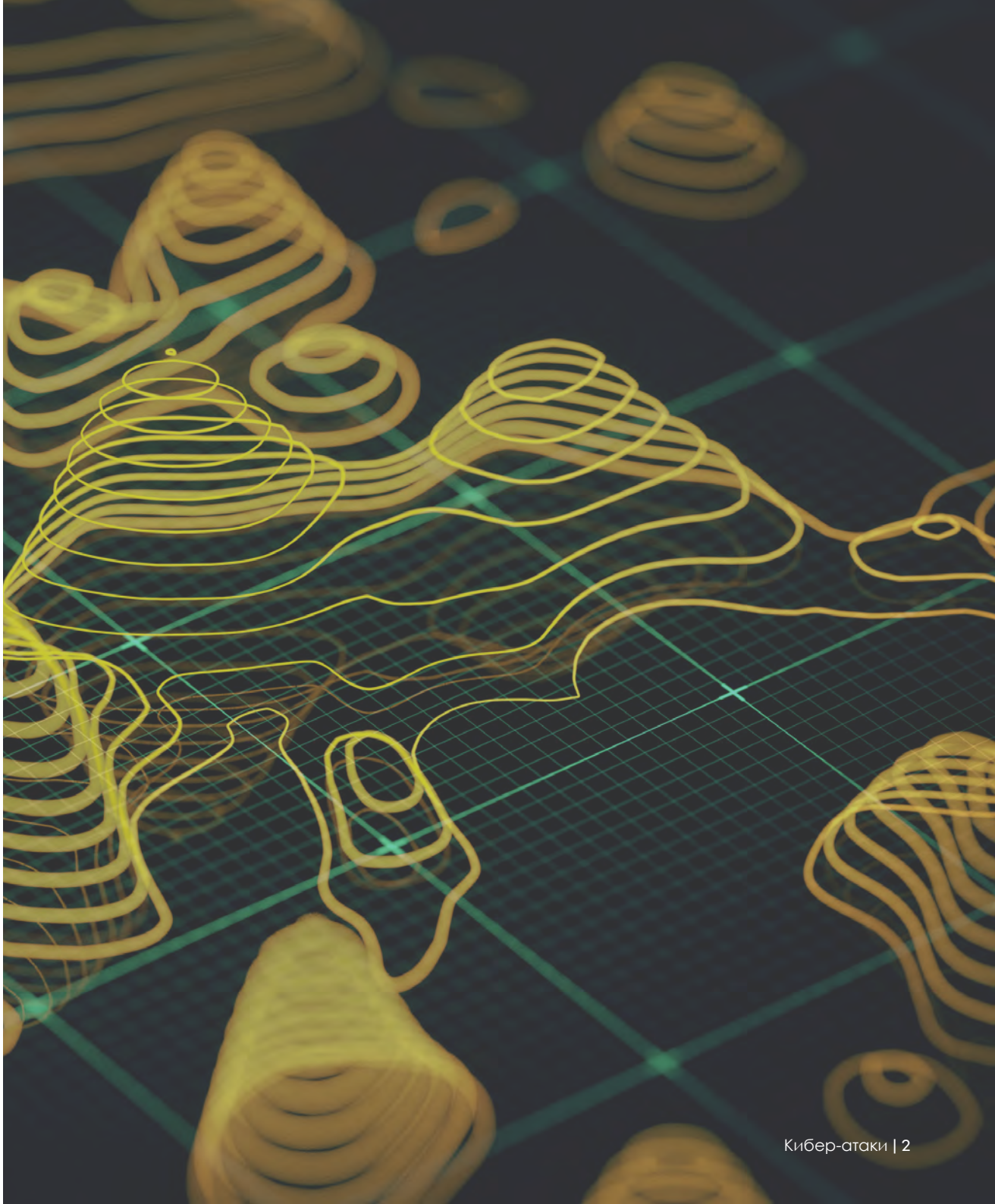
PandaLabs - это антивирусная лаборатория в компании Panda Security, которая представляет собой "нервный" центр для всего, что связано с вредоносными программами.

В лаборатории все контрмеры, необходимые для защиты пользователей Panda Security от всех типов вредоносного кода в глобальном масштабе, создаются постоянно и в режиме реального времени.

PandaLabs отвечает за выполнение тщательного анализа всех типов вредоносных программ с целью повышения уровня защиты, а также информирования общественности о новых угрозах.

Технические специалисты лаборатории постоянно находятся в состоянии повышенной бдительности, внимательно отслеживая различные тенденции и события, происходящие в области вредоносных программ и безопасности.

Их цель - выдавать предупреждения о неминуемых опасностях и угрозах, а также формулировать прогнозы на будущее.



Основные выводы: Что означают эти атаки?

Угрозы совершенствуются, вредоносные программы становятся все более сложными, а техники атаки - все более изощренными. Жертвы уже не выбираются случайно, атаки стали направленными, скоординированными и использующими различные направления. Также изменился мотив: он уже не связан с признанием - только экономическая прибыль.

Кибер-преступность - это очень доходный и привлекательный бизнес. Сегодня хакеры стали более профессиональными, они имеют более совершенные технические средства и экономические ресурсы, которые позволяют им делать свои атаки более изощренными. Поэтому они уже не боятся нападать прямо на банки, что было немыслимо еще несколько лет назад.

Для максимального укрепления финансовой системы Евросоюз впервые планирует выполнить проверку всей европейской банковской системы на предмет наличия необходимых систем для защиты от самых современных известных кибер-атак. Эти проверки будут похожи на так называемые "стресс-тесты". Европейская банковская организация (EBA) также хочет запустить ряд инициатив для обеспечения безопасности цифрового банкинга.

И давайте не будем забывать о более традиционных атаках, которые преследуют финансовый сектор и направлены на конечных пользователей банковских институтов, такие как фишинговые атаки или банковские трояны. Они продолжают распространяться и адаптироваться к новым реалиям, например, используют вредоносные программы для Android.

Введение

В течение многих лет накопление денег было основной целью кибер-преступников. Логично, что этот факт ставит финансовые системы "под прицел". На протяжении более чем десятилетия атаки были направлены на самое слабое звено в цепи - конечных пользователей банковских онлайн-сервисов.

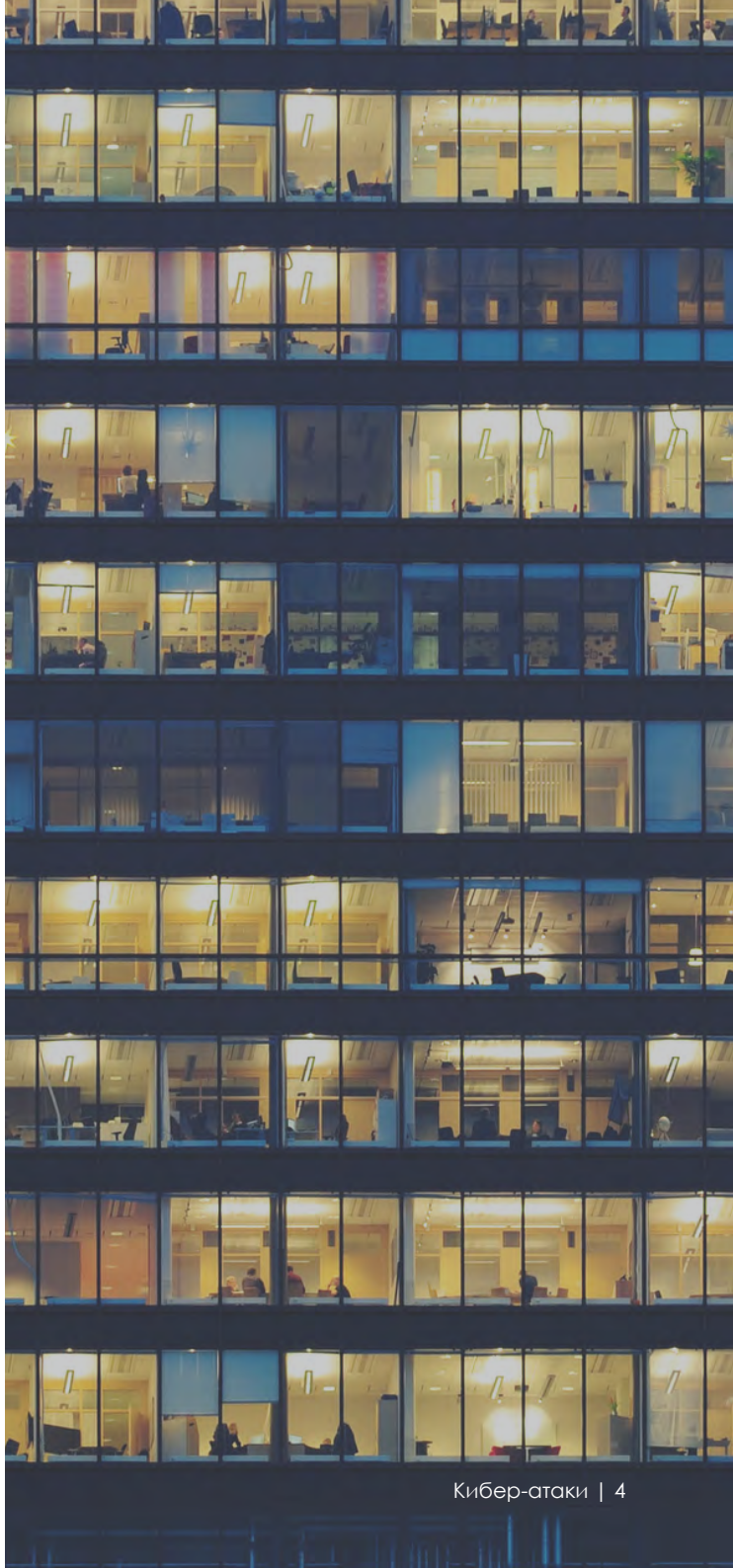
Технологические инновации стали средствами, позволяющими предложить пользователям более высокое качество и удобство обслуживания. Однако эти удобные для пользователей прозрачность и доступность, которые стали возможны с помощью банковских онлайн-сервисов, должны идти "рука об руку" с финансовым благоразумием, чтобы достичь успеха в финансовом секторе.

Это связано с тем, что современные банковские технологии предлагают некоторые преимущества для кибер-преступников, потому что недостаточный уровень безопасности со стороны конечного пользователя дает им возможность воровать небольшими суммами, а это может остаться незамеченным в течение определенного периода времени и т.д.

Впрочем, для них тут есть и определенные недостатки, т.к. необходимо искать и заражать потенциальных жертв, которые являются клиентами атакуемых банков, и преодолевать антивирусные решения.

А теперь вопрос на миллион долларов: где находятся крупные суммы денег? Без сомнения, они находятся в финансовых организациях, например, банках.

Последние события вывели вопросы системных уязвимостей в центр внимания. **Наступила новая фаза кибер-краж, которая подразумевает кражу денег непосредственно из банков, а не у их клиентов, с использованием фишинговых атак для заражения компьютеров банковских служащих.**



Тактика напрямую атаковать эти организации может значительно повысить доходы хакеров, хотя это потребует с их стороны намного больше усилий и более тщательного планирования. Преодоление банковских систем безопасности - это очень непростая задача. Кроме того, она усложняется от того, что требуется изучить внутренние системы банка, чтобы понимать, как они работают - ведь необходимо осуществить виртуальное ограбление, не оставив никаких следов. Чтобы собрать все требуемые данные для осуществления такой атаки, требуются серьезные инвестиции. Хотя, конечно, все эти усилия окупятся, если хакер сможет успешно провести свою атаку "на миллион долларов".

Финансовому сектору нелегко выполнять приоритетные функции, такие как обеспечение эффективного распределения финансовых ресурсов, содействие в развитии страны и ее финансовой стабильности, управление сбережениями и инвестициями. И также нелегко защитить данные клиентов и их счета.

Несмотря на то, что финансовый сектор оснащен самыми передовыми антивредоносными решениями как на периметре сети, так и на конечных устройствах, **усовершенствованные атаки могут скомпрометировать огромные объемы критически важных данных в финансовых организациях.**

Законодательство

Новые правила в Европе: GDPR

Действующее законодательство не адаптировано ни к новым кибер-преступлениям, ни к потребностям, появляющимся в результате использования новых технологий и систем ИТ-управления. Общий регламент Европейской комиссии по защите данных (General Data Protection Regulation, GDPR) вступает в силу 25 мая 2018 года, и он будет регулировать то, как компании собирают и обрабатывают персональные данные жителей всего Европейского союза.

Влияние на финансовый сектор будет значительным, т.к. любая организация, работающая в Евросоюзе и использующая персональные данные своих клиентов в маркетинговых и коммерческих целях, должна будет привести свою работу в соответствии с правилами GPDR менее чем за один год. **Если финансовая организация не будет соответствовать требованиям GDPR, то она может быть оштрафована на сумму в 20 миллионов евро или в размере 4% от своего годового оборота по всем операциям в мире, смотря, какая сумма будет больше. Поэтому если ИТ-специалистам не хватит знаний об этих новых требованиях, то это в конечном итоге может дорого обойтись для банков, которые оставят свои приготовления к GDPR на последнюю минуту.**

Чтобы работать безопасно, защита банковских систем требует постоянного обслуживания. При этом следует иметь в виду, что одна из самых больших проблем, с которой сталкивается финансовый сектор в наши дни, - это защита персональных данных от брешей безопасности, поэтому крайне важно иметь четко спланированный и отработанный план действий на случай кибер-атаки. GDPR требует прозрачности, и мы рекомендуем привести бизнес-операции в соответствии с новыми требованиями как можно быстрее.

Повлияет на компании, которые обрабатывают **персональные данные людей, проживающих в странах Евросоюза.**

Вступит в силу с **25 мая 2018 года.**

Будет применяться к обработке **персональных данных физических лиц в рамках Евросоюза.**

Миграция в облако

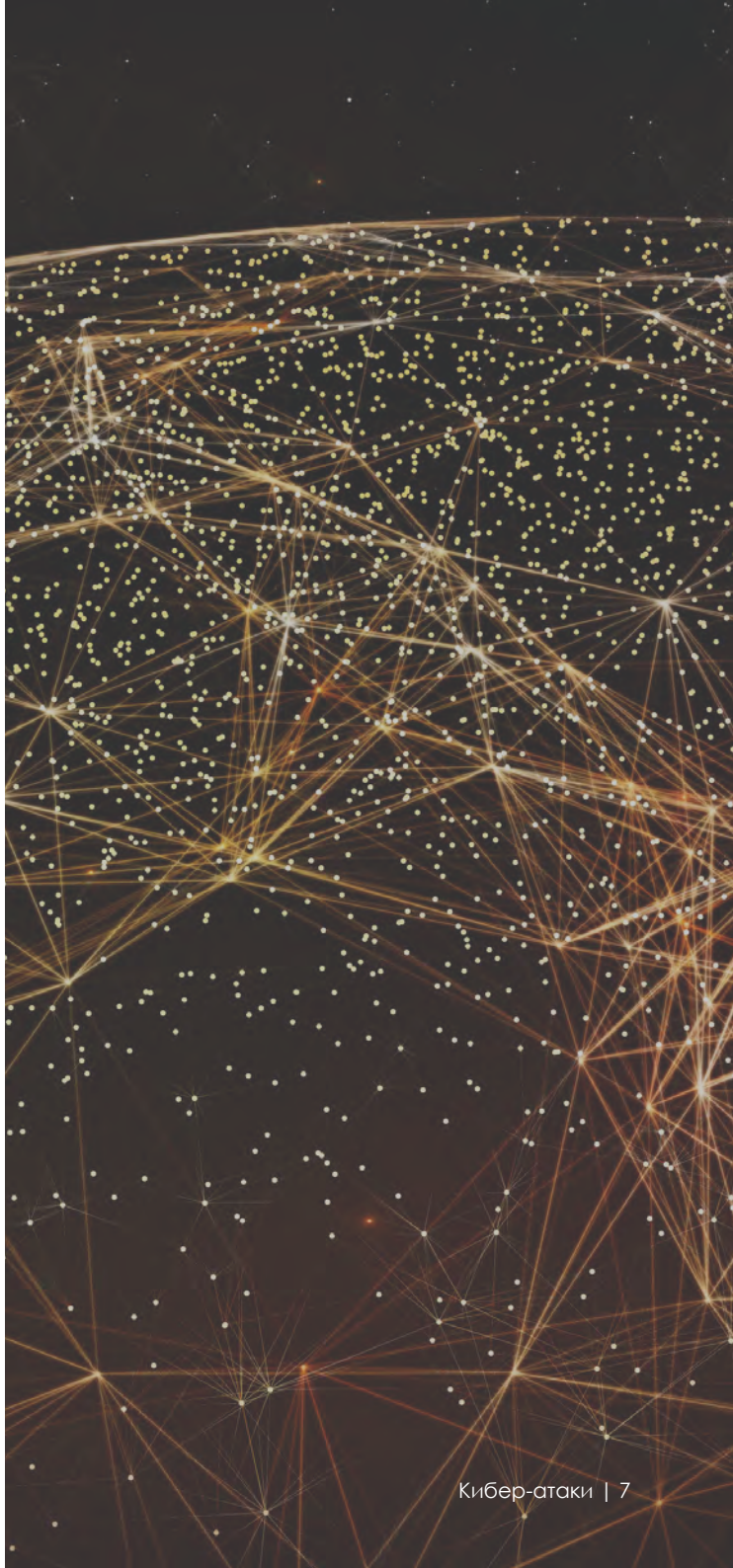
Финансовый сектор представляет собой сложную отрасль с огромным количеством игроков, регулируемую с нескольких различных сторон. Необходимо принимать во внимание охват сети системами безопасности и сведения, оговоренные в различных нормативных документах (например, NIST - Национальный институт стандартов и технологий), а также обязательствах, вытекающих из требований местного законодательства.

Облачные вычисления постепенно адаптируются внутри финансового сектора Евросоюза. Однако процесс миграции в облака еще не достиг своей зрелости. И хотя финансовые учреждения и соответствующие надзорные органы, похоже, имеют четкое видение экономических и технических преимуществ облаков, они все же остаются очень осторожными относительно риска потери контроля над данными. Поэтому большинство из них все же полагаются на свою собственную инфраструктуру.

Один из главных сдерживающих факторов основан на аргументах Европейского центрального банка и его национальных представительств, а также нормативных актах (таких как NITS), т.к. эти структуры обязаны жестко контролировать местоположение данных и их отслеживаемость, особенно когда дело касается конфиденциальных данных.

Хотя наиболее распространенный подход, использующийся финансовыми учреждениями, - это гибрид частных и публичных облачных сервисов, в регулирующих документах указано, что при работе с критически важными данными необходимо наличие частного облака. Этот механизм, как правило, считается наиболее подходящим для обработки данных, и он поддерживается национальными финансовыми надзорными органами, поскольку обеспечивает более высокий уровень контроля над информацией и операциями.

Отсутствие формальных руководящих принципов для облачных сервисов является препятствием для адаптации облачных вычислений в качестве "драйвера" для инноваций, хотя они широко пропагандируются Еврокомиссией в качестве таковых при формировании единого цифрового рынка.



Случаи миллионных кибер-краж

Когда кибер-преступники впервые нацелились на финансовый сектор, то они знали, что их основной целью должен стать клиент. У клиентов меньше ресурсов на безопасность, а потому достаточно просто будет украсть их данные и от их лица совершить финансовые операции. Так что клиент - это слабое звено.

Впрочем, за последние два года появились профессиональные и амбициозные группы хакеров, которые пошли дальше. Теперь их цель - проникнуть в банки и украсть у них миллионы долларов.

Банк Бангладеш

Одним из наиболее ярких примеров этому стала кража в Центральном банке Бангладеш, когда группа хакеров успешно заразила системы банка с помощью вредоносной программы, специально созданной для данной атаки, и попыталась совершить серию операций на общую сумму в 951 миллион долларов США. Эта сумма могла быть найдена на счете Банка Бангладеш в Федеральном резервном банке Нью-Йорка. К счастью, большинство операций было заблокировано, но хакеры смогли украсть "только" 81 миллион долларов США. Но это не единственный случай.

Tien Phong Bank

Коммерческий вьетнамский банк Tien Phon Bank пережил подобную атаку в четвертом квартале 2015 года. Хакеры снова попробовали сделать операции через сеть SWIFT, но банк во время заметил эти операции и сумел заблокировать операции на сумму более 1 миллиона долларов США.

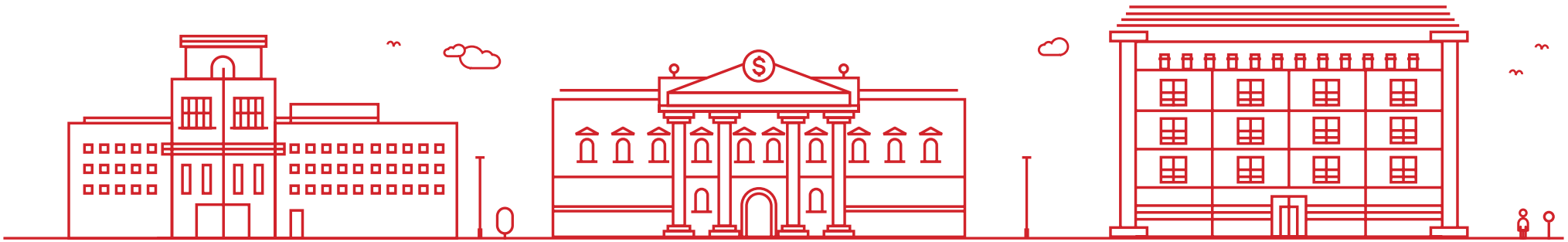
Banco del Austro

Ранее, в январе 2015 года эквадорский банк Banco del Austro также столкнулся с подобной атакой, в результате чего из банка было украдено порядка 9 миллионов долларов США.

Банк Бангладеш
Бангладеш — **81 млн.$**

Tien Phong Bank
Вьетнам — **1 млн.$**

Banco del Austro
Эквадор — **9 млн.$**



Во всех этих случаях для выполнения атаки использовались вредоносные программы, а финансовые операции осуществлялись через сеть SWIFT. Направленные атаки против этой сети, которая обеспечивает безопасные трансферы по всему миру, могут быть весьма разрушительными. К счастью, похоже, что SWIFT не пал жертвой этих успешных атак, как было сказано в пресс-релизе этой организации: "В первую очередь мы хотели бы заверить вас снова, что сеть SWIFT, основные сервисы обмена сообщениями и ПО не были взломаны".

Однако это зависит от вашей точки зрения: фактически кибер-преступники успешно использовали сеть SWIFT для совершения этих краж. Опять же, они избрали целью для своих атак самое слабое звено. SWIFT предоставляет банкам безопасную систему для коммуникаций друг с другом, но в конце этой цепочки, в самом банке, есть своя собственная внутренняя система для коммуникаций с этой глобальной сетью. Подобно тому, как хакеры атаковали клиентов банков с помощью банковских троянов, то теперь вместо того, чтобы атаковать саму SWIFT, они атакуют банки, которые подключены к этой сети.

Эта группа хакеров ответственна за все эти три кражи, и на сегодняшний день все доказательства указывают на КНДР. В декабре 2016 года стало известно, что SWIFT отправил своим клиентам предупреждение о том, что стали возникать новые случаи атак. По словам Руководителя программы безопасности пользователей в SWIFT Стефана Джилдердейла, о чем он заявил в Reuters, банки, использующие сеть SWIFT, будь то центральные банки стран или коммерческие банки, были многократно атакованы после случая с кибер-кражей в Банке Бангладеш. Причем в 20% случаев хакеры смогли успешно своровать деньги.

Другая тактика, которая в последнее время стала применяться все чаще, - это атака на терминалы оплат (POS-терминалы) для кражи информации с банковских карт. В нашем анализе гостиничного сектора мы видели, как большинство атак против этого сектора было связано с вредоносными программами, которые были направлены на POS-терминалы с целью кражи данных клиентов с их кредитных и дебетовых карт. Но эта практика затрагивает все области торговли, от небольших ресторанов до крупных сетей гипермаркетов.

Мы в антивирусной лаборатории PandaLabs проанализировали различные атаки, совершенные специально разработанными для них вредоносными программами, такими как PunkeyPOS, когда хакеры скомпрометировали заведения в США.

POS-терминалы, пострадавшие от PunkeyPOS

Информацию о других вредоносных программах, ориентированных на POS-терминалы, такие как Multigrain или PosCardStealer, вы можете найти в Медиацентре Panda Security.

Тенденции в финансовых кибер-преступлениях

Первые атаки против финансового сектора случились в 2003 году. В то время набирал популярность онлайн-банкинг, и количество банковских онлайн-операций стремительно росло. Меры для идентификации клиентов, предпринятые банками, были весьма просты: имея только имя пользователя и пароль, вы могли получить доступ ко всем вашим данным и сделать любой вид операций.

Первые атаки, в основном, относились к фишингу - электронным письмам, которые якобы приходили от банка с предупреждением о проблемах безопасности с регистрационными данными получателя письма. Согласно этим письмам, счет в банке замораживался до тех пор, пока клиент не перейдет на страницу, указанную в письме. При клике на ссылку, клиент попадал на поддельный веб-сайт. Думая, что он/она находится на сайте банка, клиент вводил свои регистрационные данные, которые тут же попадали в руки кибер-преступников.

Спустя примерно год на сцене появились первые **банковские трояны**. Эти трояны преследовали такую же цель, как и фишинговые атаки: кража регистрационных данных клиента для обмана банка при переводе денег на требуемые счета. Но эти угрозы также стали более сложными, и эти новые трояны уже могли преодолевать техники защиты.

Техники, используемые для кражи данных, стали лучше, хотя и банки, осознавая угрозы, связанные с этими троянами, значительно усилили безопасность своих веб-сайтов. Например, банки внедрили виртуальные клавиатуры для ввода регистрационных данных клиентов, что стало большим шагом в повышении безопасности онлайн-банков. Благодаря этому уже бессмысленно стало использовать **кейлоггеры** для перехвата регистрационных данных пользователей.

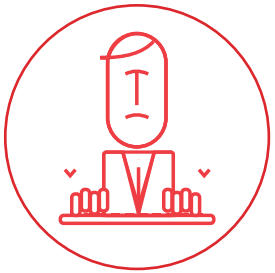
Впрочем, создатели вредоносных программ разработали новую функциональность для банковских троянов, предоставив им возможности для записи движений мышки и даже перехвата и записи изображения с экрана монитора, как было в случае с Trj/Banbra.DCY.

Фишинг

Создает поддельный сайт для получения ваших данных и кражи вашей регистрационной информации.

Банковские трояны

Устанавливают различные приложения, которые позволяют хакерам получить контроль над вашим ПК и украсть вашу информацию.



Кейлоггер

Записывает, хранит и отправляет каждое нажатие клавиш, которые пользователи делают на своей клавиатуре.

Некоторые образцы, например, связанные с семейством BankoLimb, имели файл со списком URL атакуемых банков. Когда пользователь, зараженный BankoLimb, подключался к любому сайту, чей адрес совпадал с веб-сайтом в данном списке, троян активировался, после чего он внедрял дополнительный html-код на веб-сайт банка. В дополнение к обычным полям, которые пользователь должен был заполнить при авторизации, ему следовало также предоставить дополнительную информацию. Получается, что **пользователь находился на реальной странице своего банка, но немного модифицированной. По этой причине, если вы подключаетесь к веб-сайту своего банка и вас просят ввести дополнительную информацию, то лучше не делать этого и уточнить в банке, потому что вы можете быть заражены специальным трояном и все ваши действия будут перехватываться.**

В других случаях трояны накладывали ложную страницу поверх оригинальной, в результате чего пользователь даже не предполагал, что имеет дело с имитацией. После того как пользователь вводил свои регистрационные данные на ложной странице авторизации, он мог получить сообщение об ошибке или перенаправлялся на реальный веб-сайт, чтобы клиент не мог что-либо заподозрить. Некоторые варианты семейства троянов Sinowal действительно очень сложные, и они могут модифицировать данные "на лету".

Например, если пользователь осуществляет трансфер через веб-сайт своего банка, то эти варианты троянов могли менять получателя этого денежного перевода. Более того, подделывалось и оригинальное подтверждение успешного осуществления операции, чтобы пользователь оставался в полном неведении относительно того, что его уже обманули.

Другие варианты связывались с сервером, чтобы понять, требуется ли им выполнять какие-либо действия в соответствии с веб-сайтоми, посещаемыми пользователем. Таким образом, вредоносная программа не зависела от конфигурационного файла, а потому кибер-преступники могли в любой момент расширить или изменить список веб-сайтов, где они хотели бы внедрить вредоносный код, или чью информацию они хотели бы украсть и т.д.

Чем больше мы подключаемся к банковским онлайн-системам со своих смартфонов, **тем больше хакеры готовы выделять средства на разработку банковских вредоносных программ для Android, преследуя те же цели, что и в случае с ПК.** Смартфон имеет операционную систему, приложения и пр., так что по сути это всего лишь другой компьютер.

Количество семейств банковских вредоносных программ просто поражает. Для упрощения мы разделим их на две основные группы:

1. Бразильские

(Banbra, Banker, Bancos и пр.)

Они ориентированы на клиентов бразильских, южноамериканских и частично испанских и португальских банков. С технологической точки зрения они не являются революционными творениями. Но они являются одними из самых креативных в плане использования техник социальной инженерии для обмана своих жертв.

2. Русские

(Bankolimb, Zeus, Sinowal, SpyEye, Citadel, Dyreza и пр.)

Они нацелены на клиентов из банков Европы и США. Они всегда являлись и являются самыми сложными с технической точки зрения.

Многие из них имеют очень много сходств, потому как во время их расцвета был опубликован исходный код Zeus, из которого потом возникло множество других семейств: SpyEye, Citadel, Ice IX, Ramnit, Zberp, Kins, Murofet, GameOver (Zeus P2P) и пр.

Эти атаки традиционно были направлены на клиентов финансовых учреждений, т.к. они являются самым слабым звеном и их проще всего скомпрометировать.

Однако в последние годы мы видим, как криминальные группы диверсифицируют свои направления работы, выискивая новые места для получения денег:

POS-терминалы, контролируемые компьютером

Как говорилось выше, существуют вредоносные программы, специально разработанные для таких терминалов, и они используются для кражи информации с банковских карт через терминалы оплаты в ресторанах, гостиницах, супермаркетах и т.д.

Банкоматы

Это тоже практически те же компьютеры, только с весьма специфической целью. Были зафиксированы случаи, когда хакеры проникали в них, чтобы снимать деньги напрямую в банкомате. Этого можно достигнуть за счет манипуляций непосредственно с самим банкоматом (например, с помощью установки скиммеров карт) или в результате взлома внутренней сети банка, откуда доступны их банкоматы.

Банки

Из всех возможных жертв, у кого больше всего денег? Конечно, у самих банков. Такие сложнейшие атаки требуют больших ресурсов и изобретательности, но возможность украсть миллионы долларов сильно привлекает кибер-преступников.

Рекомендации во избежание кибер-краж

Одной из самых неприятных вещей для потерпевших является отсутствие у них информации о нападении. Например, после атаки на Банк Бангладеш были обнаружены три образца вредоносных программ - и это все, что осталось. Злоумышленники, конечно же, использовали многие другие инструменты, которые были удалены после их использования, и о которых жертвы никогда не узнают.

Знание - это сила, а потому знание о том, как произошел инцидент, - это ключ к исправлению брешей безопасности и работа на опережение будущих атак. Наличие неограниченной видимости за всем, что происходит в вашей ИТ-инфраструктуре, позволяет вам осуществлять тщательный контроль и избегать потенциальных атак прежде, чем они могут произойти.

Отсутствие единого кибер-пространства, законодательства, сертификации, взаимозаменяемости и правовой защиты является одним из самых больших препятствий, с которыми сталкиваются банки, чтобы осуществить переход к облачным вычислениям - системе, которая позволяет финансовым учреждениям получить преимущества от требуемого ПО: сокращение расходов, повышение системной производительности, более высокая точность данных, обеспечение универсального доступа к документам и т.д.

Итак, как ПО для обеспечения ИБ должно относиться к данным, которые хранятся в облаке, чтобы максимально эффективно соответствовать законодательным нормам?

Информация под грифом "секретно": облачный сервис не должен иметь доступ к конфиденциальной персональной информации или информации, которая имеет высокий уровень защищенности в соответствии с законодательством о защите персональных данных, или классифицируемой банками как "секретная информация". Единственный возможный нюанс - косвенный сбор данных, связанных с использованием компанией своих ИТ-ресурсов в результате активности пользователей. Данная информация может быть включена в виде ограничения во внутренние правила поведения, и быть доступна только ограниченному кругу лиц (операторы защиты и персонал банка).

Информация под грифом "конфиденциально": сервис имеет доступ к информации пользователей с более низкими уровнями защищенности. Например, данные пользователя для входа в систему (но не пароль, который никогда не должен собираться), название устройства и его IP-адрес, если они однозначно идентифицируют пользователя. Эти данные необходимы для корректной работы облачного сервиса, а потому понятно, что провайдеры сервиса могут быть авторизованы для доступа к таким данным.

Эти два качества лежат в основе модели безопасности Adaptive Defense 360 - первого облачного сервиса информационной безопасности с функциями расширенной защиты, сочетающего защиту устройств следующего поколения (NG EPP) и технологии обнаружения и реагирования на атаки (EDR) с возможностью классификации 100% запущенных процессов.

Благодаря этой модели **банки смогут защищать свои основные активы (данные и критически важная информация о своих клиентах) с помощью решения, способного обнаруживать утечку данных вне зависимости от того, произошла ли она в результате применения вредоносной программы или из-за действий сотрудников банка.**

Это одна из наиболее ценных функций в финансовом секторе. Adaptive Defense 360 получает данные и передает их в SIEM-систему, которая позволяет получить полную видимость всех процессов на каждом конечном устройстве.

В дополнение к этому, а также к способности обнаруживать и блокировать любые виды атак (включая неизвестные), направленные против системы, **Adaptive Defense 360** позволяет обнаруживать и закрывать уязвимости в системе и ее приложениях, а также предотвращать использование нежелательных программ, таких как навигационные панели, рекламное ПО или дополнения и расширения.

Корпоративное решение Panda Security - это часть платформы, использующей контекстную логику, которая анализирует, классифицирует и сопоставляет данные по кибер-угрозам для выполнения операций по предотвращению, обнаружению, реагированию и восстановлению.

Эффективность данного решения информационной безопасности с опциями расширенной защиты от неизвестных угроз подтверждена независимой тестовой лабораторией AV- Comparatives. **Мы переосмысливаем информационную безопасность.**

Adaptive Defense 360

Филиалы Panda Security:

СТРАНЫ БЕНЕЛЮКСА
+32 15 45 12 80
belgium@pandasecurity.com

БРАЗИЛИЯ
+55 11 3054-1722
brazil@pandasecurity.com

ФРАНЦИЯ
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

ГЕРМАНИЯ И АВСТРИЯ
+49 (0) 2065 961-0
sales@de.pandasecurity.com

ВЕНГРИЯ
+36 1 224 03 16
hungary@pandasecurity.com

ИТАЛИЯ
+39 02 24 20 22 08
italy@pandasecurity.com

МЕКСИКА
+52 55 8000 2381
mexico@pandasecurity.com

НОРВЕГИЯ
+47 93 409 300
norway@pandasecurity.com

ПОРТУГАЛИЯ
+351 210 414 400
geral@pt.pandasecurity.com

ЮАР
+27 21 683 3899
sales@za.pandasecurity.com

ИСПАНИЯ
+34 900 90 70 80
comercialpanda@pandasecurity.com

ШВЕЦИЯ, ФИНЛЯНДИЯ И ДАНИЯ
+46 0850 553 200
sweden@pandasecurity.com

ШВЕЙЦАРИЯ
+41 22 994 89 40
info@ch.pandasecurity.com

ВЕЛИКОБРИТАНИЯ
+44(0) 800 368 9158
sales@uk.pandasecurity.com

США И КАНАДА
+1 877 263 3881
sales@us.pandasecurity.com

Подробная информация:

www.pandasecurity.com/russia/enterprise/solutions/adaptive-defense-360/

По телефону:

+7 495 105 94 51

или по почте sales@rus.pandasecurity.com

panda

Adaptive Defense 360

Неограниченная видимость, абсолютный контроль

pandasecurity.com

panda