



Кибербезопасность 2020–2021

Тренды и прогнозы

ptsecurity.com

Содержание

Цифры, тренды и новые идеи	3
Великое осадное сидение — 2020	5
Государственные учреждения	9
Атаки на пользователей	10
Атаки на промышленный сектор	11
Телеком-безопасность	14
Безопасность финансовой отрасли	15
Безопасность операционных систем	20
Аппаратные уязвимости	21
Мобильная безопасность	22
Безопасность и искусственный интеллект	24



Борис Симис

Заместитель генерального
директора по развитию
бизнеса Positive Technologies

Цифры, тренды и новые идеи

По итогам 2020 года отечественный рынок информационной безопасности вырос на 25%. Если коротко, то такой рост обусловлен тремя причинами. Во-первых, тематика информационной безопасности становится все более актуальной в том числе и в силу объективных причин: число угроз и активность киберпреступников в целом растут год от года. Проблематика кибербезопасности все больше понятна и близка руководству различных компаний и, соответственно, во главу угла все чаще ставится принцип невозможности реализации тех или иных бизнес-рисков. Очевидно, что построение практической безопасности такого рода идет рука об руку с увеличением соответствующих бюджетов.

Во-вторых, кибербезопасность КИИ, как концепция, начавшаяся несколько лет назад с обследований, категоризации и проектирования, наконец-то дошла до периода реальных внедрений. И это, в свою очередь, обеспечивает рост оборотов производителей средств защиты и их интеграции.

В-третьих, нельзя не отметить, что в этом году бизнес, понимая, что будущий год в новых условиях изменится и с точки зрения привычного бюджетирования на ИТ и ИБ, стремился максимально реализовать планы, намеченные на 2020 год, и использовать имеющиеся для этого ресурсы.

COVID по всем фронтам

Нельзя сказать, что пандемия COVID-19 никак не повлияла на рынок кибербезопасности. Однако, в реальности на эту тему было больше разговоров, чем практического влияния. К концу первого квартала 2020 года начала складываться ситуация, вызывавшая ряд опасений: резко снизилось общее число пилотных проектов. И совершенно понятно, почему это произошло — в обновленных условиях (локдаун, спешный переход на удаленный формат работы) эти проекты стало объективно сложнее (а иногда и вовсе невозможно) проводить на площадках компаний. Одновременно с этим было понятно, что те же самые обновившиеся условия работы заставили бизнес не замораживать проекты по развитию собственной кибербезопасности. В совокупности оба момента рисовали весьма опасную ситуацию, в которой компании-заказчики могли отказаться от пилотирования технологий (как критерия выбора) и начать ориентироваться только на формальные ценовые признаки. Но эти опасения так и остались опасениями: здоровая конкуренция на отечественном рынке ИБ осталась прежней, а общая ориентированность бизнеса именно на практическую безопасность не позволила компаниям пойти по упрощенному пути выбора средств защиты.

Любопытно, что на протяжении 2020 года мы видели два мощных всплеска финансово-проектной активности. Первый, как это ни удивительно, случился в тот момент, когда страна ушла на карантин: службы информационной безопасности на стороне бизнеса к тому моменту уже имели четко сформированные задачи на год, подтвержденные бюджетные планы, но внешние условия схлопнули видимость горизонта планирования практически до нуля. Поэтому часть игроков рынка пошла по пути форсирования проведения конкурсов, старта (или завершения)

проектов и т.д. В итоге апрель продемонстрировал первый всплеск финансовой и связанной с нею проектной активности на рынке. Вторая волна трат на ИБ произошла в четвертом квартале и была связана все с той же необходимостью реализовать утвержденные планы. В целом именно это позволило рынку информационной безопасности в России вырасти, невзирая на все перипетии 2020-го года.

Курс на реальный инфобез

Мы уже отмечали, что парадигма ИБ меняется в принципе: некоторое время назад сообщество отказалось от идеи «построения киберзаборов» и пришло к осознанию того, что цель любой системы безопасности состоит в максимально быстром обнаружении атакующего внутри информационных систем (так как в принципе нет системы защиты, которую невозможно взломать). На практике в течение последнего года эта идея несколько эволюционировала: мы осознали, что вполне реально выстроить такую систему защиты, которая будет гарантированно не допускать реализации потенциальным злоумышленником конкретных бизнес-рисков. Этот подход подразумевает, что любая компания так или иначе может быть взломана в ходе атаки, и задача информационной безопасности — не дать возможности злоумышленнику нанести сколько-нибудь существенный урон. Это тренд, который окончательно оформился буквально в течение прошедшего года, и с большой долей вероятности он будет главенствовать в ближайшие годы. В связи с этим на первый план выйдут задачи создания SOC нового типа — в качестве SLA, оперирующих не доступностью в режиме 24/7 или скоростью реакции на инцидент, а намного более конкретным показателем, основанным на гарантированном недопущении реализации злоумышленником неприемлемых для организации рисков. То есть эффективность такого SOC будет оцениваться в буквальном смысле на уровне «да/нет» — реализован риск или не реализован. В этой концепции особое значение приобретают качественные практические киберучения, как единственное мерило эффективности выстроенной системы защиты. В информационной безопасности легко скатиться в неконкретность оценок, и только правильно организованные киберучения дают возможность не скатиться к потемкинским деревням и максимально конкретизировать результат.

Такой подход, в конечном счете, расширяет рынок, качественно его меняя и оставляя право на жизнь только тем решениям и технологиям, которые реально влияют на результат. То есть мы имеем дело со своего рода интерпретацией теории Дарвина на уровне технологий: выживут только те, кто способен вовремя выявить активность злоумышленника, заблокировать его, исключить возможности для развития атаки и в принципе «вычистить» его из инфраструктуры. И мы, как вендор, также работаем над созданием интеллектуального автоматизированного инструмента, который позволит решать эту задачу быстро и эффективно.



**Алексей
Новиков**

Директор экспертного
центра безопасности,
Positive Technologies

Великое осадное сидение — 2020

Из-за повсеместного внедрения удаленной работы появились новые риски информационной безопасности, социальная инженерия стала часто применяться для проникновения в сети организаций. Глобальный новостной повод — эпидемию — использовали все типы хакерских группировок. С темой COVID-19 были связаны как массовые, так и APT-атаки. При этом, как мы и прогнозировали в 2019 году, число APT-атак в 2020 году продолжило расти.

В 2020 году мы отслеживали деятельность порядка 30 APT-группировок. При этом в России мы отметили деятельность 10 из них. Стоит обратить внимание, что становится все сложнее проводить техническую атрибуцию: часто в рамках одной атаки комбинируются вредоносные программы, приписываемые разным группировкам. Традиционно приходится уведомлять различные компании о том, что они взломаны той или иной APT-группировкой, и для них это, к сожалению, часто оказывается сюрпризом. В целом сотрудники экспертного центра безопасности провели за год 47 расследований.

По итогам 2020 года мы видим, что инсайдеры все еще остаются актуальной проблемой для компаний, как в случае с инцидентом в компании Tesla¹. В эпоху, когда люди постоянно взаимодействуют через соцсети и мессенджеры, все важнее становится вопрос обеспечения их безопасности. Достаточно вспомнить массовый взлом профилей звезд и политиков в Twitter².

Шифровальщики — одна из главных проблем 2020 года: суммы выплат за расшифровку данных были колоссальны, а при отказе платить выкуп утекшие данные публиковались в Сети. Некоторым компаниям пришлось приостановить свою деятельность на несколько дней. Один из самых громких примеров — инцидент с Garmin³. О росте числа деструктивных атак и атак шифровальщиков мы говорили еще в 2017 году. При этом шифрованием инфраструктуры после атаки занимаются не только хакеры с финансовой мотивацией, но и APT-группировки⁴.

Атаки на цепочку поставок

Настоящей болью в 2020 году стали supply chain attacks. Об этом мы предупреждали с 2017 года. Наверняка у всех на слуху история с SolarWinds⁵. В нашей практике мы сталкивались с такими же атаками на разработчиков ПО, разработчиков средств защиты, на IT-интеграторов, подрядчиков IT-компаний, на порталы государственных организаций в различных странах. Уровень защищенности крупных компаний повышается, и их становится все сложнее взламывать, особенно если целью злоумышленников является долговременное присутствие, а не разовая атака. И поэтому APT-группировки все чаще

1 bit.ly/2YI8nuJ

2 bit.ly/2M92VIT

3 bit.ly/3a7sj9W

4 bit.ly/2MopwRA

5 bit.ly/3iSEJGv

стали атаковать партнеров и поставщиков жертвы. Защититься от подобных атак очень сложно, это под силу только высококлассным специалистам в области ИБ.

Прогнозы

Мы ожидаем, что в 2021 году будут совершенствоваться методы социальной инженерии, эксплуатирующие темы, связанные с обстановкой в мире, в частности, тему COVID-19. Можно также прогнозировать, что фишинг станет более индивидуальным, злоумышленники будут выходить на жертв через мессенджеры и социальные сети. Для преодоления корпоративных средств защиты взлом все чаще будет производиться через домашние компьютеры работников.

В 2020 году множество APT-атак было направлено на фармацевтические компании, в том числе на лаборатории по разработке вакцин. Вирус мутирует, исследования продолжаются, и эти лаборатории будут интересовать злоумышленников еще какое-то время. Мы также ожидаем традиционного роста числа APT-атак.

Вымогательское ПО все чаще используется в целенаправленных атаках (например, в атаках группировки APT 27). В 2021 году мы прогнозируем рост числа таких атак.

В 2021 году мы можем столкнуться с атаками на цепочки поставок, похожими на взлом SolarWinds, а также с большим количеством атак на компании, работающие в области IT и ИБ, и на облачные инфраструктуры.

Мы рекомендуем всем организациям максимально подробно изучать собственную инфраструктуру, быстро реагировать на аномалии, сосредоточиться на точках входа в сеть, которые используют удаленные сотрудники. Минимальный набор средств защиты: антивирус, SIEM-система, система анализа сетевого трафика (NTA), межсетевой экран уровня приложений.

Обратная сторона «удаленки»: атаки на сервисы для удаленного подключения и взлом ПО для онлайн-конференций

Пандемия и переход на удаленный режим работы спровоцировали во всем мире рост числа атак, направленных на эксплуатацию уязвимостей в корпоративных сервисах, доступных из интернета. Ведь компании в срочном порядке выводили сервисы на периметр. В связи с масштабным переходом на удаленную работу выросло число узлов российских компаний с доступным для подключения RDP. Как следствие, доля атак с эксплуатацией уязвимостей в ПО и недостатков конфигурации ближе к концу 2020 года выросла до 30% (в I квартале было 9%).

С каждым кварталом мы наблюдаем тенденцию к увеличению числа атак, в которых вредоносное ПО распространяется путем эксплуатации уязвимостей на ресурсах сетевого периметра организаций. Злоумышленники активно эксплуатируют уязвимости в VPN-решениях и системах для организации удаленного доступа,

в частности, в продуктах Pulse Secure, Fortinet, Palo Alto и Citrix. Также киберпреступники ищут уязвимости в веб-приложениях, подбирают пароли для доступа по RDP.

Еще один тренд, появившийся на фоне пандемии, — атаки, направленные на кражу учетных данных для подключения к системам аудио- и видеосвязи Skype, Webex и Zoom, а также вмешательство в конференции.

Киберпреступники преследовали самые разные цели — от установки майнеров до кибершпионажа в сетях крупных компаний. При этом злоумышленники не ограничиваются одним типом ВПО: они все чаще используют многофункциональные трояны либо загружают на скомпрометированные устройства набор из различных зловредов; операторы одного вредоносного ПО могут передавать доступ другим преступникам. Сами вредоносы также претерпевают изменения. В первую очередь, изменения направлены на маскировку ВПО, обход антивирусов и средств защиты, в том числе песочниц. Кроме того, преступники дополняют вредоносные программы новыми функциями и эксплойтами для новых уязвимостей.

Бум шифровальщиков

В течение 2020 года мы наблюдали постоянное увеличение числа атак шифровальщиков. Если в первом квартале для организаций доля шифровальщиков в атаках с использованием ВПО составляла 34%, то в третьем квартале она достигла 51%. Операторы шифровальщиков все реже проводят массовые атаки, они целенаправленно выбирают крупные компании, которые в состоянии заплатить большой выкуп, или организации, для которых приостановка деятельности опасна, и наносят точечные удары.

Шифровальщики — одно из самых быстроразвивающихся направлений киберпреступного бизнеса. Шантаж публикацией данных в случае отказа жертвы платить выкуп поставлен на поток. Наибольшую активность в таких атаках в 2020 году проявили операторы Maze, Sodinokibi, DoppelPaymer, NetWalker, Ako, Nefilim, Clor. Некоторые требуют отдельно выкуп за расшифрование данных и отдельно за неразглашение. Для продажи похищенных данных многие операторы шифровальщиков сделали собственные сайты, где публикуют список жертв и похищенную информацию, и даже организуют аукционы по продаже украденных данных. Появляются и объединения шифровальщиков, участники которых публикуют украденную информацию в рамках партнерских соглашений.

Выкуп за неразглашение и доступ на продажу

Тренд на требование выкупа за неразглашение похищенных данных подхватили и другие злоумышленники. Так, взломщики интернет-магазинов предлагают жертвам заплатить выкуп, чтобы преступники не продавали данные третьим лицам. По сравнению с операторами шифровальщиков, требуемые суммы выкупа которых достигают миллионов долларов, их аппетиты гораздо скромнее — порядка 500 долл. США. Тем не менее такая бизнес-модель позволяет злоумышленникам в разы увеличить свои доходы, ведь зачастую законные владельцы баз

данных мотивированы платить, чтобы сохранить свою репутацию, а киберпреступникам не приходится тратить время на поиск покупателей.

Иногда киберпреступники покупают доступы в организации-жертвы у других злоумышленников. Одними из первых по такой схеме стали действовать операторы шифровальщиков, они предлагают сотрудничество, ищут партнеров для распространения их трояна-вымогателя и обещают своим поделщикам долю от суммы выкупа. Рынок доступов к сетям компаний в дарквебе позволяет зарабатывать низкоквалифицированным хакерам, которые могут ограничиться поиском уязвимостей на внешних ресурсах компаний с целью продажи.

Прогнозы

В конце 2020 года мы увидели, что взрывной рост активности злоумышленников, который наблюдался в первом полугодии на фоне пандемии, начал замедляться. Однако число атак остается стабильно высоким, и тенденция к ежеквартальному увеличению количества инцидентов по-прежнему сохраняется.

Прибыль, которую получают операторы шифровальщиков, будет привлекать в этот киберпреступный бизнес новых участников — операторов ВПО и тех, кто будет предоставлять им доступы к инфраструктуре за процент от суммы выкупа. В следующем году мы, вероятно, увидим новые объединения преступников и площадки для продажи украденных данных. Скорее всего, шифровальщики сохранят отработанную в 2020 году стратегию шантажа: запрашивать выкуп за восстановление работоспособности инфраструктуры и отдельно — за то, чтобы преступники не продали или не опубликовали украденные данные. Но и без учета сумм выкупа атаки шифровальщиков дорого обходятся компаниям, ведь общие потери связаны с затратами на восстановление работы систем, упущенной из-за простоя выгодой, с возможным оттоком клиентов и другими последствиями. Например, специализирующаяся на предоставлении IT-услуг компания Sopra Steria, которая в октябре пострадала от действий шифровальщика Ryuk, по предварительным подсчетам оценивает потери в 40–50 млн евро.

Большинство компаний все еще полностью или частично остаются на удаленном режиме работы, а значит, преступники продолжают искать любую незакрытую брешь в системах на периметре сети. Вместе с тем развитие рынка доступов в дарквебе поставит организации, в том числе крупные, под прицел низкоквалифицированных нарушителей, которые нашли способ легкого заработка. Количество внешних атак на инфраструктуру организаций продолжит расти. Поэтому стоит особенно внимательно относиться к анализу сетевого периметра, инвентаризации доступных извне ресурсов и выстраиванию эффективного процесса управления уязвимостями.

Но есть и хорошие новости

Многие компании пересмотрели свое отношение к удаленному режиму работы. Если в начале 2020 года организациям пришлось спешно переводить сотрудников на работу из дома, то в 2021 году у них появится возможность сделать работу над ошибками, предусмотреть

в бюджете средства на обеспечение защиты, организовать работу с учетом лучших практик ИБ.

Сегодня компании не могут игнорировать риски: растет заинтересованность в оценке реальных последствий от возможных киберугроз, компании хотят быть готовыми к встрече с хакерами и снизить возможные негативные последствия. Появляется множество площадок, предлагающих провести разного рода учения, и наиболее эффективны киберучения на основе цифровой модели организации, соответствующей реальной инфраструктуре. Моделирование бизнес-рисков на киберполигоне станет одним из основных трендов ИБ.

Государственные учреждения

Больше всего атак по-прежнему совершается в отношении госучреждений: на них приходится 15% от всех атак, направленных на организации. За 2020 год мы зафиксировали порядка 300 атак на государственные учреждения. По сравнению с 2019 годом существенно выросла доля атак с использованием ВПО (75%) и социальной инженерии (72%). Этому могла способствовать пандемия: многие злоумышленники рассылали в госучреждения разных стран письма с вредоносными вложениями на тему коронавирусной инфекции. В 63% случаев атаки проводились с целью шпионажа.

В начале 2020 года были замечены рассылки APT-группировок SongXY, APT36, TA428, TA505 и Higaia, которые распространяли вредоносные документы, используя тему COVID-19. Эта же тема использовалась в атаках с помощью вредоносных программ Chinoxu и KONNI. Также в течение всего года экспертный центр безопасности Positive Technologies (PT ESC) фиксировал атаки группы Gamaredon, направленные на госучреждения Украины и Грузии.

Отметим, что ФСТЭК выпустила проект новой методики моделирования угроз, в которой основополагающими моментами являются понимание организацией и ее руководством недопустимых последствий от кибератаки, а также вероятного сценария развития такой атаки в инфраструктуре. Методика дорабатывается с учетом мнения специалистов, работающих в отрасли, но уже заметно, что регулятор взял курс на существенное повышение эффективности ИБ российских компаний с учетом изменяющегося ландшафта угроз.

Прогнозы

Многие привычные для граждан сервисы сейчас предлагаются удаленно, без необходимости личного присутствия, даже выборы проходят в электронном формате. Развитию цифровизации поспособствовала пандемия. Появление новых электронных сервисов обязательно заинтересует преступников и потребует особого внимания с точки зрения ИБ.

Некоторые риски, связанные с цифровыми услугами, были продемонстрированы на киберполигоне The Standoff. К примеру, атакующим удалось получить доступ к базе данных городского портала и удалить

информацию о штрафах граждан. Из делового центра были похищены персональные данные и конфиденциальные документы, а на рекламных экранах по всему городу атакующие смогли запустить собственный контент. Это лишь единичные примеры киберрисков, заложенных в виртуальную модель города, а атаки на реальную инфраструктуру могут привести к куда более серьезным последствиям.

Атаки на пользователей

За первые три квартала 2020 года мы отметили 252 кампании, которые были направлены против частных лиц. Число атак выросло на 9% по сравнению с аналогичным периодом предыдущего года. Рядовые пользователи преимущественно становятся жертвами массовых кампаний (в 94% случаев), чаще всего это атаки с использованием социальной инженерии (65%). В 61% случаев злоумышленники заражали устройства пользователей вредоносным ПО. В основном ВПО распространялось через сайты, электронную почту и официальные магазины приложений. Более половины атак на частных лиц с использованием вредоносных (51%) были проведены с помощью шпионского ПО, в 22% атак использовались банковские трояны. В первую очередь злоумышленников интересовали учетные данные для доступа к сервисам — они составили 37% от общего объема украденной информации, на втором месте — данные платежных карт (13%).

Фишинговые атаки на тему COVID-19 в первую очередь коснулись обычных людей. Злоумышленники не только рассылали фишинговые письма, но и создавали тематические сайты¹, на которых скрывалось вредоносное ПО, распространяли вредоносные мобильные приложения. В начале пандемии в своих рассылках злоумышленники предлагали средства защиты или дополнительную информацию о вирусе, а сейчас они чаще спекулируют на теме вакцины (tek.io/3o4xFbO). Во время массовой самоизоляции создавалось множество фейковых сайтов², предлагающих получить пропуск для перемещения по городу, и в случае введения подобных ограничений в 2021 году вероятен аналогичный всплеск активности мошенников.

Важно отметить, что период массовой самоизоляции в первой половине прошлого года сопровождался переводом сотрудников многих компаний на удаленный режим работы. Преступники активно пользовались этим, и атаки на частных лиц проводились, среди прочего, для получения доступа к сетям организаций, в которых эти люди работают. Способствует этому, как правило, непонимание основных принципов ИБ и небрежное отношение к правилам безопасной работы на домашних устройствах. Отсутствие обновлений ПО, нелегальное ПО, старые неподдерживаемые версии ОС, отсутствие антивирусов, использование простых паролей и прочие ошибки позволяют превратить домашний компьютер сотрудника в источник атак на компанию.

1 bit.ly/3iAFHaw

2 bit.ly/2MfguWE

Прогнозы

Тема пандемии будет и дальше использоваться для распространения вредоносного ПО, кражи денег и реквизитов банковских карт у рядовых пользователей. К примеру, одной из популярных схем могут стать сайты, на которых мошенники будут предлагать заказать препараты для лечения коронавируса, записаться на платную вакцинацию, получить справку о прохождении вакцинации. В фишинговых рассылках вредоносное ПО часто будет скрываться под видом информации о вакцинации и ее сроках или о введении «паспортов здоровья».

Еще одной темой для социальной инженерии может стать Чемпионат Европы по футболу. Подобные мероприятия всегда сопровождаются появлением множества мошеннических сайтов для кражи данных и денег у граждан.

Продолжаются атаки типа Magecart, жертвами которых становятся клиенты интернет-магазинов и других сервисов, предоставляющих возможность онлайн-оплаты. В ходе таких атак преступники взламывают сайты компаний и встраивают на их страницы вредоносные скрипты, которые собирают все введенные пользователем данные, в первую очередь реквизиты платежных карт. Такие атаки весьма эффективны, поскольку безопасность веб-приложений не всегда находится на должном уровне, и злоумышленники могут, к примеру, воспользоваться известными уязвимостями в популярных системах управления контентом (CMS). При этом под удар попадают обычные пользователи.



**Дмитрий
Даренский**

руководитель практики
промышленной
кибербезопасности,
Positive Technologies

Атаки на промышленный сектор

В 2020 году увеличилось количество атак на промышленные и энергетические компании. Было зафиксировано около 200 атак на предприятия из этих отраслей: это приблизительно на 60% больше, чем в 2019 году (125 атак). В девяти из десяти атак на промышленность злоумышленники использовали вредоносное ПО. На долю шифровальщиков пришлось 38% атак, а шпионское ПО было замечено в 30% случаев.

Для распространения вредоносных программ и проникновения в локальную сеть злоумышленники прибегали к фишинговым рассылкам, а также эксплуатировали уязвимости на сетевом периметре организаций.

В основном промышленные компании подвергались атакам со стороны шифровальщиков и APT-группировок. В 2020 году на промышленность была направлена примерно каждая пятая из всех атак на юридических лиц с использованием шифровальщиков. В начале года внимание многих специалистов по кибербезопасности привлек новый шифровальщик Snake, который умеет удалять теневые копии и останавливать процессы, связанные с работой промышленных систем управления. В частности, Snake останавливает процессы GE Proficy и GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, ThingWorx Industrial Connectivity Suite. Первыми жертвами Snake стали автомобильный производитель Honda и гигант ТЭК — компания Enel Group. В течение года промышленность

атаковали также операторы шифровальщиков Maze, Sodinokibi, Ryuk, NetWalker, Nefilim, DoppelPaymer, RansomEXX, Conti.

Промышленность является целью для многих APT-групп по всему миру. Так, целью одной из APT-атак группы Bisonal в I квартале 2020 года стали российские организации авиационно-космической отрасли. В России и СНГ не снижается актуальность атак группы RTM, за весь 2020 год эксперты PT ESC выявили более 100 фишинговых рассылок этой группы.

Прогнозы

С начала 2021 года число атак на промышленность увеличилось и держится на стабильно высоком уровне. Мы предполагаем, что интерес злоумышленников не утихнет в ближайшем будущем. Целью атак будет не только шпионаж, но и возможность получить крупную сумму денег в качестве выкупа за восстановление зашифрованных данных и за неразглашение украденной информации.

Раньше редко можно было прочитать в СМИ о том, что промышленная компания остановила производство в результате кибератаки. На это было две причины: во-первых, компании скрывали такие инциденты, а во-вторых, они зачастую не могли определить, что стало истинной причиной сбоя — кибератака или другие факторы. Сегодня регулярно появляется информация о взломах крупнейших энергетических и производственных компаний по всему миру. И как правило, причина известна: это целенаправленные атаки с использованием шифровальщиков. Такие атаки сложно скрыть, а определить их источник очень просто: преступники сами сообщают о взломе и требуют выкуп.

Благодаря этим тенденциям стала очевидной крайне низкая защищенность компаний от внешних угроз, а также неготовность своевременно выявить и остановить злоумышленника. Можно только предположить, сколько шпионских кампаний остаются невыявленными и не предаются огласке. Вероятно, что преступники продолжают атаковать промышленные предприятия и будут ориентироваться на как можно более крупные организации, в то же время предпочитая придерживаться наименьших затрат на взлом или на покупку готового доступа в инфраструктуру. Стоит ожидать, что мы услышим о множестве утечек и об остановке производств и в 2021 году. Скорее всего, повысится и размер выкупов, сегодня в отдельных случаях он уже составляет десятки миллионов долларов, но увеличение числа жертв, готовых платить, лишь стимулирует преступников. Будут появляться и новые группы атакующих, они продолжат кооперироваться и зарабатывать на уязвимости промышленных организаций.

Вместе с тем промышленные предприятия, помимо формального обеспечения соответствия требованиям местного законодательства, все активнее работают над обеспечением практической безопасности своих активов. В 2021 году развитие получают следующие тренды.

1. **Risk-oriented threat modeling.** Применение практик риск-ориентированного моделирования угроз кибербезопасности промышленных объектов. Станет заметен переход от классических вероятност-

ных методов моделирования киберугроз отдельных промышленных систем к методам, рассматривающим киберугрозы как один из факторов операционных и бизнес-рисков компаний в целом.

2. **SCADA data-driven anomaly detection and response.** Развитие технологий обнаружения аномалий и атак на инфраструктуру промышленных систем за счет анализа прикладных данных SCADA-систем. Развитие подобных технологий особенно будет заметно в системах таких классов, как NTA/NDR, EDR, SIEM.
3. **Security management processes automation.** Расширение автоматизации процессов управления кибербезопасностью, особенно в части обнаружения и реагирования на инциденты кибербезопасности.
4. **Digital twins. Cyber polygons.** В целях изучения уязвимостей промышленных систем и моделирования атак на них активно развивается моделирование виртуальных копий (цифровых двойников) промышленных систем. Этот подход получит развитие и в рамках создания киберполигонов, на которых можно безопасно проверить возможность реализации бизнес-рисков и проанализировать потенциальные способы проведения атак.

The Standoff, или Успешные атаки без реальных последствий

Важным вектором развития ИБ становится цифровое моделирование кибератак на информационную инфраструктуру. На полигоне The Standoff участники киберучений получают доступ к реальным оборудованию и ПО, которые используются в промышленных компаниях, и могут проверить возможность реализации различных киберрисков. На прошедшем в ноябре 2020 года мероприятии команды атакующих смогли осуществить несколько атак на нефтехимический и нефтеперерабатывающий заводы, которые в реальной жизни привели бы к серьезному ущербу. Например, атакующим удалось получить доступ к системе управления заводом, что привело к нарушению, а затем и полной остановке производственного процесса: на цифровой модели завода произошла авария и утечка ядовитых веществ. На виртуальной копии нефтяного месторождения из-за кибератаки остановилась работа добывающего оборудования. Кроме того, нападающие смогли получить доступ к системе управления хранилищами нефтепродуктов и нарушили процесс транспортировки нефти в хранилище, а позже остановили работу контроллера, управляющего транспортировкой. Провести аналогичные проверки в рамках пентеста или киберучений на настоящей инфраструктуре компании невозможно, ведь это может привести к повреждению оборудования, остается лишь продемонстрировать условную реализацию риска. Киберполигон позволяет довести атаку до конца и оценить ее реальные последствия.



Павел Новиков

Руководитель группы исследований безопасности телекоммуникационных систем, Positive Technologies

Телеком-безопасность

Основные проблемы безопасности телекоммуникационных сетей все еще кроются в недостатках защищенности протоколов, используемых в сетях 2G, 3G и 4G. К примеру, уязвимости SS7 сетей 2G/3G позволяют проводить все виды атак от раскрытия информации до перехвата SMS, прослушивания разговоров и нарушения доступности абонентов. Протокол Diameter в сетях 4G подвержен уязвимостям, которые позволяют злоумышленнику отслеживать местоположение абонентов, обходить ограничения оператора на использование услуг связи и вызывать отказ в обслуживании устройств пользователей. Недостаточная защита протокола GTP позволяет злоумышленникам нарушить работу сетевого оборудования и лишиться связи абонентов целого города, выдавать себя за другого пользователя при доступе к различным ресурсам, пользоваться услугами сети за счет оператора или абонентов.

Более того, все выводы в отношении защищенности перечисленных сетей актуальны и для сетей 5G Non-Standalone, которые строятся на основе инфраструктуры сетей предыдущих поколений. Таким образом, можно утверждать, что на сегодня большинство 5G-сетей, также как и сетей 4G, уязвимы для раскрытия абонентских данных (например, данных о местоположении), для спуфинга, который может использоваться при различного рода мошенничестве, для атак, направленных на отказ в обслуживании оборудования сети, результатом которых может стать массовое отключение мобильной связи.

Что касается сетей 5G Standalone, то, по нашим данным, несмотря на все принятые меры в области безопасности протокола HTTP/2 (замена SS7 и Diameter в 5G SA), в этих сетях еще остаются возможности для действий злоумышленника: возможны атаки подмены и удаления сетевых элементов, которые могут привести к сбоям в работе сети. Кроме того, если злоумышленник получит доступ к внутренним интерфейсам, то, используя уязвимости протокола PFCP (замена GTP-C в сетях 5G SA), он сможет осуществлять DoS-атаки на абонентов, а также перехватывать их входящий трафик.

Риск отказа в обслуживании представляет прямую угрозу для устройств IoT, которые становятся основными потребителями услуг связи и постепенно начинают обеспечивать важные функции городской и промышленной инфраструктуры, элементов умного дома и других систем.

Операторы осведомлены о существующих угрозах, но системный подход к безопасности встречается редко, что отражается в низком уровне защищенности даже при наличии дорогостоящих специальных решений.

Прогнозы

В ближайшем будущем останутся актуальными все нынешние угрозы для сетей 2G, 3G и 4G, которыми будет пользоваться подавляющее число абонентов. Многие операторы начинают работать над строительством сетей 5G SA уже в 2021 году, но на полноценную коммерческую эксплуатацию пока рассчитывать не приходится, поэтому мы все

еще будем жить в условиях безопасности 2G/3G/4G-сетей. Кроме того, сети 5G должны поддерживать взаимодействие с другими мобильными сетями, и это приводит к возможности кросспротокольных атак, где используются уязвимости сразу нескольких протоколов. К примеру, атака на сети 5G может начинаться с эксплуатации уязвимостей в сети 3G для получения идентификаторов абонентов. Поэтому защита сетей предыдущих поколений — необходимое условие безопасности 5G.

При этом продолжатся исследования архитектуры и протоколов сетей 5G, поиск уязвимостей и недостатков. Хотя при разработке спецификаций были учтены недостатки безопасности предыдущих поколений мобильной связи, новые технологии несут с собой новые риски.

Проблемы безопасности протокола GTP не исчезнут полностью даже с переходом на 5G Standalone. GTP планируется использовать и в сетях архитектуры Standalone, в том числе в роуминге, правда, уже только для передачи пользовательских данных (протокол GTP-U). Атаки на GTP-U позволяют инкапсулировать пакеты управляющего протокола в пользовательскую сессию или получить данные о соединении абонента, поэтому с появлением сетей 5G SA возможность проведения таких атак применительно к новым управляющим протоколам потребует дополнительного изучения.



**Максим
Костиков**

Руководитель группы
исследований безопасности
банковских систем,
Positive Technologies

Безопасность финансовой отрасли

В 2020 году мы зафиксировали более 100 атак на финансовые компании, что превосходит общее число атак за 2019 год (их было 92). За этот период в 64% атак использовался фишинг: это основной метод проникновения в локальную сеть финансовых организаций; еще в 15% случаев использовался хакинг (эксплуатация уязвимостей и недостатков безопасности). Вредоносное ПО применялось в 66% атак. По большей части это были шпионское ПО (34% атак с использованием ВПО), шифровальщики (27%) и банковские трояны (17%). Заметим, что число атак шифровальщиков в отношении финансовых организаций выросло, как и в других отраслях.

По данным экспертного центра безопасности Positive Technologies, на протяжении года группировка RTM продолжала атаковать финансовые организации при помощи вредоносных рассылок, а в первом полугодии были зафиксированы фишинговые рассылки группировки Cobalt.

European Association for Secure Transactions (EAST) [сообщает](#)¹ об увеличении количества логических атак на банкоматы в Европе, причем все зафиксированные атаки в первом полугодии относились к типу black box.

Прогнозы

Новых крупных игроков, нацеленных на вывод денег со счетов в банке, не появляется, и не стоит ожидать их появления в 2021 году. Атаки на небольшие банки не приносят много прибыли, даже по сравнению с целенаправленной атакой шифровальщиков, при этом они намного сложнее в реализации: преступникам нужно разбираться в банковских

1 bit.ly/3sSPuxp

процессах, уметь работать со специализированным ПО. Скорее всего, стоит ожидать атак со стороны уже известных групп, которые могут менять свои техники проникновения и закрепления для сокрытия атак, совершенствовать ВПО, менять регионы атаки.

Возможно увеличение числа атак шифровальщиков на банки: этот бизнес приносит существенный доход преступникам и не требует особых затрат, к тому же поставлен на поток. Для распространения ВПО злоумышленники продолжают искать известные уязвимости на периметре: результаты пентестов¹, проведенных в финансовых организациях, свидетельствуют о низком уровне защищенности — в семи из восьми компаний внешний злоумышленник смог бы проникнуть в локальную сеть из интернета.

Ключевые проблемы безопасности банкоматов

В настоящее время идет переход банковского ПО на новую операционную систему Windows 10. Она обладает большим количеством возможностей по сравнению с предыдущими версиями Windows, и эти возможности увеличивают риск того, что злоумышленник обойдет защиту киоска банкомата и получит доступ к ОС.

Как показывает наш опыт, в банкоматах в настоящее время существует небезопасное разграничение доступа к ПО, что позволяет злоумышленнику после получения доступа к ОС устройства и изменения доступных исполняемых файлов выполнять произвольный код, что может привести к выдаче денежных средств или краже персональных данных.

Атаки типа black box по-прежнему актуальны и приводят к рискам кражи денежных средств из банкомата; банки начинают задумываться о введении аутентификации подключаемых устройств (USB-флешек, клавиатур и др.) к банкоматам, что позволит существенно снизить риски подобных атак, а также обхода киоска.

Что касается сетевой безопасности, мы наблюдаем улучшение сетевых политик и использование VPN для защиты банкоматов. Однако данные защитные меры применяют не все; отсутствие мер защиты может позволить злоумышленнику влиять на трафик между банкоматом и процессингом, что может привести к краже конфиденциальных данных или выводу денежных средств. Также обычно внутри VPN трафик не защищен дополнительным шифрованием, что позволяет внутреннему злоумышленнику проводить аналогичные атаки.

Защищенность банковских веб-приложений

В 2020 году мы увидели положительную динамику по обеспечению безопасности банковских веб-приложений, а именно - тенденцию к переходу на микросервисную архитектуру, повышающую отказоустойчивость системы, и уменьшение количества стандартных веб-уязвимостей (XSS, SQLi, RCE). Из негативных стоит отметить тенденцию к увеличению числа логических уязвимостей, которые могут привести к краже денежных средств, получению преступниками

¹ bit.ly/396ngHe

дополнительной информации о пользователях, отказу в обслуживании. Таким образом, злоумышленники сейчас нацелены не на полную компрометацию системы банковского веб-приложения, а на логические уязвимости, с тем чтобы:

- получить более выгодный курс обмена валют, украсть денежные средства со счетов пользователей, обмануть комиссии;
- получить как можно больше информации о пользователе для использования ее в атаках при помощи социальной инженерии;
- использовать логические уязвимости для повышения нагрузки на систему, чтобы вызвать отказ в обслуживании.

Поэтому мы можем предположить, что в 2021 году банки будут уделять больше внимания устранению логических уязвимостей.

Безопасность банковской инфраструктуры

Финансовые институты все еще недостаточно хорошо защищены от атак типа АРТ. Нарушители успешно реализуют самые опасные для бизнеса риски — получают доступ к АРМ КБР, системам управления банкоматной сетью, карточному процессингу. В ушедшем году пентестеры Positive Technologies неоднократно оказывали услугу верификации бизнес-рисков для банков (обычно верифицируется от трех до пяти бизнес-рисков), и каждый раз команду, эмулирующую деятельность нарушителей, ждал успех.

В случае реализации модели «внутренний нарушитель» в 100% случаев наша команда пентестеров получала максимальные привилегии в инфраструктуре, демонстрировала возможность реализации бизнес-рисков. Под бизнес-рисками мы понимаем заранее обговоренные с заказчиками недопустимые события, несанкционированный доступ к критически важным системам — к АРМ КБР, SWIFT, банкоматной сети, процессингу или иным, исходя из специфики того или иного банка.

Важно упомянуть, что в ряде случаев наши специалисты выполняли работы не от лица внутреннего нарушителя, а по модели «внешний нарушитель», когда к моменту начала работ у них не было ни доступов, ни каких-либо привилегий в исследуемых системах, то есть от лица условного «человека с улицы». При этом мы также успешно достигали заявленных целей работ — преодолевали внешний периметр организации-заказчика, получали максимальные привилегии в инфраструктуре, реализовывали ключевые бизнес-риски.

Проблемы новейших технологий финансового сектора

Как плюсы, так и минусы содержат в себе современные технологии кредитно-финансового сектора — от платежей с помощью ссылок, QR-кодов и цифровой валюты до биометрии и новейших веб-технологий.

Проблемы антифрод-решений

Ошибки автоматизации и связанные с ними риски — основная проблема современных антифрод-решений. Попытки выявить платежи,

нехарактерные для клиента, иногда приводят к ложным срабатываниям и блокированию легитимных платежей. Уменьшить количество ложных срабатываний и предотвратить ошибочную блокировку платежей поможет широкое внедрение автоматизации с использованием больших данных. При этом полностью избежать ложных срабатываний антифрод-решений вряд ли удастся.

Чем больше банки пытаются обезопасить своих клиентов, тем с большим количеством трудностей клиенты будут сталкиваться из-за ошибок защиты. Любая автоматизированная система строится на основе анализа эффективности. Алгоритм определения мошеннических транзакций может быть строгим — тогда растет количество выявляемых подозрительных операций, но чаще останавливаются платежи, либо, наоборот, более щадящим — тогда уменьшается количество ошибочно остановленных платежей, но и больше мошеннических платежей проходят незамеченными. Решением проблемы станет баланс между безопасностью и своевременным исполнением платежей, потребностями бизнеса.

Цифровой рубль и риски блокчейн-технологий

Одним из путей повышения эффективности анализа платежей является блокчейн и распределенные реестры, обеспечивающие прозрачность платежа на каждом этапе. Необходимые шаги в этом направлении уже делаются: недавно анонсированный Центробанком цифровой рубль, например, основан именно на блокчейн-технологиях. Как и все новое, это направление порождает риски, с которыми индустрия еще не сталкивалась.

В подобных системах самым слабым местом всегда является доступ клиента к системе платежей, к самому электронному кошельку. Можно делать супернадежные блокчейн-системы, но все равно останется возможность путем взлома веб-интерфейса или атаки на устройство клиента получить доступ к деньгам клиента.

Бизнес позитивно оценивает возможность использования смарт-контрактов, когда условия договора оформляются не в виде юридического текста, а в виде алгоритма, где на каждом этапе можно вычислить, выполнил контрагент свои обязательства или не выполнил. Но это алгоритм, который пишут люди, а людям свойственно ошибаться. В код смарт-контракта могут быть внесены ошибки и даже умышленные закладки, что открывает совершенно новую страницу в истории финансовых махинаций. Проблема в том, что сама идея уязвимости в тексте договора, которая может использоваться злоумышленником, нова для индустрии. Нужно набирать опыт, учиться находить такие уязвимости и противодействовать мошенничеству, связанному с их использованием.

Серьезную проблему представляет проблема распределенных реестров в случае совершения мошеннических действий. Одну отдельную финансовую операцию невозможно «откатить» назад, потому что в этом случае непонятно, что делать с легитимными операциями, происходившими в это же время. Ключевым аспектом использования цифровых денег является обеспечение подлинности операций, для чего операция криптографически подписывается. При этом важна реализация отечественных криптографических алгоритмов

в программном обеспечении, обеспечивающем существование цифровых денег и смарт-контрактов.

Объединение усилий бизнеса и регуляторов — залог успешной реализации смарт-контрактов и распределенных реестров. Это задача, которую предстоит решить в будущем.

Киберриски быстрых платежей и телефон как платежное средство

Система быстрых платежей, запущенная 28 февраля 2019 года, позволяет клиентам банков переводить деньги по номеру мобильного телефона и платить за товары в торговых точках по QR-коду вне зависимости от того, в каком банке открыты их счета. Кроме несомненного удобства, система быстрых платежей принесла пользователям и новые риски, ведь клиент идентифицируется не по паспорту, как в отделениях банков, и не по связке «кредитная карта — код подтверждения», как в традиционных системах, использующих протокол 3-D Secure, а по номеру телефона, к которому привязана банковская информация плательщика.

Использование телефона в качестве удостоверения личности (и даже в качестве идентификатора получателя, как это делает система быстрых платежей) несет дополнительные риски. Например, процедуры восстановления утерянных сим-карт позволяют мошенникам получить в свое распоряжение сим-карту клиента банка, а уязвимости банковских приложений — привязать номер телефона жертвы к своему собственному счету. К традиционным способам мошенничества добавляются новые, связанные с использованием телефона.

Биометрия как способ идентификации клиента набирает популярность, но и она несет в себе серьезные риски. Говоря об очень высокой надежности биометрической идентификации, обычно приводят в качестве примера идентификацию по отпечаткам пальцев или радужной оболочке глаза: такие методы действительно имеют очень низкий коэффициент ошибок. Но для дистанционной идентификации клиентов предлагаются совсем другие биометрические методы — идентификация по изображению лица и записи голоса. Такие методы имеют сравнительно низкую надежность, делающую возможным применение дипфейков — автоматической генерации изображения и голоса, которые успешно проходят биометрическую верификацию.

При этом практика показывает, что надежность идентификации практически не влияет на возможности мошенников: в большинстве случаев злоумышленники обходят механизмы аутентификации клиента или с помощью социальной инженерии, или с помощью уязвимостей в платежных приложениях.

К сожалению, многие инициативы банковского сектора по противодействию мошенникам, такие как создание единого реестра сим-карт, введение ограничений на разовую операцию в системе быстрых платежей, — клиенты часто воспринимают негативно. Переломить подобное отношение, привить пользователям навыки элементарной цифровой гигиены — серьезная задача для банковского сообщества на ближайшие годы.

Киберполигон как решение проблем банков

В ноябре 2020 года прошло онлайн-мероприятие [The Standoff](#), в рамках которого проводилось моделирование кибератак на цифровые копии компаний, соответствующие реальной инфраструктуре. Одним из корпоративных сегментов, представленных на киберполигоне, был банк. Участникам предлагалось реализовать следующие риски: нарушить работу процессингового центра, похитить деньги со счетов банка или с карт клиентов, украсть персональные данные сотрудников или клиентов банка. В результате атакующим удалось осуществить половину рисков: они смогли перевести деньги с карт пользователей на собственные счета, получить доступ к персональным данным сотрудников и персональным данным клиентов системы ДБО. Подчеркнем, что практически все атаки на банк (кроме одной, проведенной в последние минуты соревнования) были выявлены и расследованы командой защитников. Участие в киберполигоне дает специалистам по ИБ возможность получить уникальный опыт и повысить свою квалификацию.

Отметим, что бизнес-риски, заложенные в программу The Standoff, весьма актуальны для финансовых организаций. По результатам внутренних пентестов во всех финансовых организациях нам удалось получить максимальные привилегии в корпоративной инфраструктуре. В тех проектах, где стояла дополнительная цель — продемонстрировать возможность хищения денежных средств банка потенциальным злоумышленником, удалось реализовать такую возможность. Проблемы с безопасностью отмечаются и по итогам анализа защищенности мобильных банков: было установлено, что в каждом втором мобильном банковском приложении возможны проведение мошеннических операций и кража денежных средств.



Александр Попов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений, Positive Technologies

Безопасность операционных систем

В 2020 году шла продуктивная работа над повышением безопасности операционных систем. В этой области произошел ряд важных событий, год получился насыщенным. Очевидно, не сбылись пессимистичные прогнозы о падении темпов разработки системного ПО из-за пандемии. И [Linux Foundation](#)¹, и [GitHub](#)² в своих годовых обзорах даже фиксируют рост активности в открытых сообществах разработчиков.

Безопасность операционных систем продолжает быть важным направлением для инноваций. В этой области не может быть простых универсальных решений, нужен комплексный подход. Намечились три основных вектора движения, которые в совокупности позволяют вывести безопасность ОС на более высокий уровень.

Первое направление — использование подходов безопасной разработки ПО. Невозможно говорить о безопасности ОС, если в процесс ее разработки не интегрированы кросс-ревью, фаззинг-тестирование, статический анализ, контроль цепочки поставки программных компонентов.

¹ bit.ly/3p5fPG9

² bit.ly/39OZ6R2

Второе направление — разработка и внедрение механизмов ОС, затрудняющих эксплуатацию уязвимостей. Цель в том, чтобы максимально помешать атакующему, который пытается воспользоваться ошибкой в программном коде ОС.

Третье важное направление — использование новых аппаратных средств, которые позволяют избавиться от целых классов уязвимостей в операционных системах. В частности, речь об ARM Pointer Authentication Code (PAC), ARM Memory Tagging Extension (MTE), Intel Control-flow Enforcement Technology (CET). Взаимосвязь этих и других технологий с классами уязвимостей и методами их эксплуатации отражена в разработанной мной [карте средств защиты ядра Linux](#)¹.

Хороший пример комплексного подхода к безопасности ОС — недавно опубликованная [модель безопасности Android](#)², ее вторая редакция вышла в декабре 2020 года. Безопасность системы строится исходя из актуальной модели угроз. Каждый компонент системы безопасности выбран осознанно и закрывает конкретную угрозу.

Вместе с тем, 2020 год показал, что в области безопасности ОС еще очень много работы. Специалисты Google Project Zero [опубликовали анализ сложной системы вредоносного ПО](#)³, использующей цепочку уязвимостей нулевого дня. Серьезное вредоносное ПО — это качественный продукт, имеющий модульную архитектуру, систему управления и взаимозаменяемые компоненты с эксплойтами. Поэтому нам как защитникам не стоит недооценивать атакующих. Более того, только взгляд на операционную систему с точки зрения атакующего позволит нам разработать действительно эффективные средства защиты.



Марк Ермолов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений, Positive Technologies

Аппаратные уязвимости

В прошедшем году мы могли наблюдать некоторый спад интереса к информационной безопасности, и к безопасности аппаратного обеспечения в частности, но это связано, на мой взгляд, больше с тем, что все конференции по ИБ перешли в онлайн-формат, тем самым резко сократив число участников. Однако это не означает, что специалисты перестали изучать аппаратные уязвимости. По моему мнению, сейчас мы наблюдаем некоторое затишье перед бурей, когда исследователи просто не раскрывают найденные ошибки, с тем чтобы более выгодно подать их на будущих конференциях. Исследователи в 2020 году получили уникальную возможность заняться наконец чистыми исследованиями, не тратя время на подготовку к конференциям и другим мероприятиям, и это обязательно найдет свое отражение в ближайшее время.

Так что в будущем можно ожидать шквала новых аппаратных уязвимостей. Безусловно, недавняя утечка большого объема конфиденциальной информации, связанная с платформами Intel (Exconfidential Lake), подстегнула интерес к изучению аппаратной безопасности. Можно сказать, что это уникальное событие: в общем доступе оказались программные эмуляторы еще не вышедших в продажу новейших платформ Intel, что позволяет исследовать микропрограммное

¹ bit.ly/3615NhG

² arxiv.org/abs/1904.05572

³ bit.ly/3pOHfNf

обеспечение на наличие уязвимостей, не покупая реальное оборудование. Исследователи получили значительное преимущество: можно познакомиться с аппаратной платформой задолго до ее выхода на рынок. И это с большой долей вероятности приведет к росту числа найденных ошибок в firmware и hardware (в микропрограммном обеспечении и на уровне оборудования) новых систем Intel в наступившем году. Конечно, отдельно стоит вопрос о законности использования материалов из недавней утечки, и исследователи не будут ни афишировать факт изучения незаконно полученной информации, ни как-то ссылаться на нее в своих статьях, но это никак не будет препятствовать тому, чтобы многие аспекты, связанные со внутренним устройством оборудования, производимого компанией Intel, наконец-то стали понятны специалистам. Эта утечка — красноречивый пример того, что безопасность через неясность (security through obscurity) не работает, и я уверен, что в ближайшее время мы будем пожинать горькие плоды решений, принятых когда-то технологическими лидерами отрасли, в виде новых «неустраняемых» аппаратных уязвимостей и архитектурных изъянов, которые можно исправить только в новых продуктах, что будет негативно сказываться как на конечных пользователях, так и на авторитете производителей.



**Николай
Анисеня**

Руководитель группы
исследований безопасности
мобильных приложений,
Positive Technologies

Мобильная безопасность

В 2020 году мир немного замедлился, это коснулось даже такой «виртуальной» сферы, как IT, и, в частности, мобильных приложений. В условиях новой реальности мы были вынуждены научиться жить по новому распорядку. Но несмотря на это, в сфере мобильной безопасности не обошлось без интересных поворотов.

Девиз прошлой весны — «Stay home». К этой важной мере так или иначе призывало руководство большинства стран. Бизнес также был вынужден принять новые правила игры и по возможности перейти на удаленную работу. Сотрудник на удаленке — это не только вопросы контроля и самоорганизации, но и повышенные требования к безопасности. В мире насчитывается 10 миллиардов мобильных устройств, а две трети пользователей используют личные устройства для работы¹. Нетрудно догадаться, что многие используют для работы более одного устройства, и чаще всего это именно смартфоны. Пандемия сподвигла всех перейти на удаленку, а значит данные показатели — это всего лишь оценка «снизу», и они могут еще подрасти.

При настройке удаленного рабочего места у администраторов гораздо больше возможностей для защиты десктопных компьютеров и ноутбуков, ведь операционные системы допускают запуск защитных программ с привилегиями суперпользователя, а сам сотрудник может работать под учетной записью с ограниченными правами, достаточными для выполнения рабочих задач. С мобильными устройствами ситуация другая: популярные мобильные ОС не предоставляют возможность повышения привилегий, и администраторы вынуждены полагаться на средства MDM (mobile device management), предоставляемые операционной системой.

1 techjury.net/blog/byod/

Охрана приватности

Встает и другой вопрос: вопрос приватности. Не так важно, какой смартфон вы используете, личный или рабочий. Вы вполне можете установить на него приложения, не предназначенные для работы. Среднее количество приложений на наших смартфонах варьируется, по разным оценкам, и может достигать до 67¹, что заставляет задуматься о безопасности такого соседства.

С выходом iOS 14 компания Apple сделала большую ставку на усиление приватности пользовательских данных. Появились такие интересные фишки, как разделение геопозиции на точную и приблизительную, то есть теперь у пользователя есть выбор, какую геопозицию предоставить приложению. Также появилась возможность узнать, собирается ли приложение вас отслеживать, и если такая функциональность присутствует, у пользователя необходимо будет явно запросить разрешение. Ну и, конечно, нагнетавшая опция — уведомление о чтении из буфера обмена, то есть оттуда, где хранится скопированная вами информация. В первые же дни после релиза этой версии десятки популярных приложений были уличены в том, что они могли шпионить за пользователями². Если учесть, что смартфоны все чаще используют для удаленной работы, подобные инциденты могут стать серьезной угрозой для бизнеса и корпоративной тайны. Со стороны Apple это огромный шаг к повышению прозрачности работы приложений.

Но вопросом охраны своей приватности должен быть обеспокоен не только бизнес, но и вообще каждый житель кибервселенной. С благими намерениями крупнейшие игроки рынка мобильных устройств и операционных систем, компании Google и Apple, выпустили API для отслеживания контактов с зараженными новой коронавирусной инфекцией — Exposure Notification³. Он уже давно доступен в последних версиях Android и iOS. Но, как и любую технологию, Exposure Notification API можно попытаться использовать во вред, а именно — для отслеживания пользователей: попытаться вычислить реально заболевших или составить карту перемещения конкретного человека⁴. Это убедительный пример того, как новое решение порождает новые проблемы, ставит человечество перед новыми вопросами, а безопасникам подкидывает новые задачи.

Кстати, этими вопросами не стоит задаваться владельцам новых устройств Huawei: данная функция на них отсутствует. Все дело в том, что компания Huawei в 2020 году перешла от слов к делу и постепенно отказывается от сервисов Google и даже планирует перейти с операционной системы Android на собственную разработку — Harmony OS 2.0. Первые смартфоны под управлением этой ОС должны поступить в продажу уже в 2021 году. Похоже, двум гигантам придется потесниться на мобильном рынке, а мы сможем с интересом наблюдать за тем, как будет меняться данная отрасль, и строить безопасность мобильных устройств в 2021 году.

1 bit.ly/3nSPUjq

2 bit.ly/2Nfzyol

3 bit.ly/3oXLoSc

4 bit.ly/3sF49Mw



**Александра
Мурзина**

Специалист группы
перспективных технологий
отдела исследований
по защите приложений,
Positive Technologies

Безопасность и искусственный интеллект

Машинное обучение в информационной безопасности уже давно перестало быть rocket science, превратившись в норму со своими сформировавшимися подходами и решениям типичных задач. Уже известны как преимущества, так и подводные камни применения техник для анализа, быстрого реагирования и защиты с помощью искусственного интеллекта (ИИ), поэтому сочетание традиционных техник с новомодными является наилучшей практикой.

Согласно исследованию, проведенному Capgemini¹ в 2019 году, почти две трети опрошенных компаний считают, что ИИ поможет выявить критически опасные киберугрозы. В то же время 69% организаций считают, что ИИ будет неотъемлемой частью своевременного реагирования на кибератаки. И если в 2019 году только каждая пятая организация использовала техники, связанные с ИИ, то в 2020 году это были уже почти две трети.

Список возможностей ИИ, которые могут укрепить кибербезопасность, длинный. ИИ может анализировать поведение пользователей, выводить закономерности и выявлять различные отклонения от нормы, что позволяет быстро выявлять уязвимые области в сети. ИИ также может позволить компаниям автоматизировать рутинные обязанности по обеспечению безопасности с высоким качеством результатов и сосредоточиться на делах с более высоким уровнем вовлеченности, требующих человеческого суждения. Компании также могут использовать его для быстрого поиска признаков вредоносного ПО.

При этом ИИ все чаще применяется не только в сфере ИБ, но и в других отраслях. Техники ИИ, в частности машинного обучения, требуют большого количества данных. Кто-то собирает данные, чтобы улучшать свои продукты, а кто-то — чтобы анализировать пользователей и продавать результаты анализа.

Учитывая нехватку экспертов по безопасности и специалистов по анализу данных и машинному обучению, людей, которые являются экспертами в обеих областях, еще меньше. Заниматься вопросами безопасности становится все труднее только потому, что разработчики либо не знают о возможных рисках, либо стараются прежде всего сначала выпустить продукт, а потом разбираться с проблемами. Такая ситуация приводит к серьезным последствиям. Только в первом квартале 2020 года количество крупномасштабных утечек данных увеличилось на 273%².

При этом не стоит забывать, что ИИ является программным продуктом, который сам по себе может быть уязвим и несет определенного рода риски. В связи с этим осенью 2020 года MITRE совместно с Microsoft выпустили матрицу атак³ на системы, использующие машинное обучение. В проекте участвовали не только Microsoft, но и еще 16 исследовательских групп. Причем речь идет не просто о потенциальных рисках,

1 bit.ly/38WimwC

2 cnb.cx/2NmINDm

3 github.com/mitre/advmthreatmatrix

а именно о тех, которые были проверены на эффективность. В результате было сформирована таблица в стиле матрицы ATT&CK, которая уже знакома исследователям. В таблице выделены риски, характерные только для сервисов, использующих техники машинного обучения, и общие риски, которые могут напрямую не относиться к машинному обучению, но косвенно влиять на него, так как машинное обучение часто является частью программного продукта.

Если говорить про ИИ как инструмент для атак, то стоит выделить активно развивающуюся область *deepfake* — техники подмены лиц на фото или видео или имитации голоса. В данный момент реалистичная подмена не является сложной задачей. В интернете много примеров и обученных моделей машинного обучения, а в магазинах приложений много программ, которые позволяют простому пользователю заменять лица и делают это очень реалистично. Если в 2019 году такие техники помогли злоумышленникам украсть 220 000 €¹, то в начале 2021 года злоумышленники просто смогли заработать, разместив фейковое объявление² и пригласив пользователей от лица основателя компании Dbrain и популяризатора нейронаук Дмитрия Мацкевича на блокчейн-платформу.

С одной стороны, небольшое количество общеизвестных инцидентов, связанных с безопасностью ИИ, не перерастает в злободневную проблему кибербезопасности, на которую стоит бросать все ресурсы, с другой стороны, уже есть прецеденты у крупных компаний ([Google](#), [Amazon](#), [Tesla](#)), которые заставляют академическое сообщество и индустрию задуматься и активно изучать данный вопрос. Видится тенденция к осознанию проблем безопасности ИИ, выработке подходов и, соответственно, применению их на практике.

1 on.wsj.com/3sJC1rg

2 bit.ly/3qz9AKU

О компании

ptsecurity.com
pt@ptsecurity.com
[facebook.com/](https://facebook.com/PositiveTechnologies)
[PositiveTechnologies](https://facebook.com/PHDays)
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте ptsecurity.com.