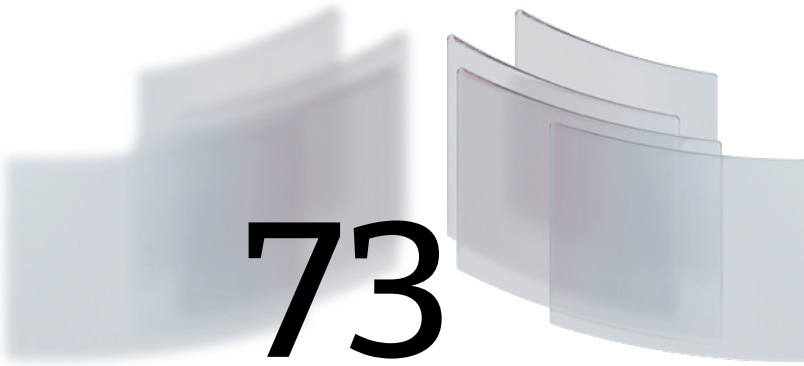
Positive Research 2021

Сборник исследований по практической безопасности

Positive Research 2021

Содержание



От редакции

Мы живем в эпоху тотальной цифровой трансформации, ощущая на себе как сугубо положительные, так и отрицательные ее последствия. Возможно, мы лишь в самом начале этого процесса, но уже сейчас зависимость общества от технологий недвусмысленно намекает: мы не хотим отказываться от удобства, которое дарят нам высокие технологии, часто недооценивая потенциальные угрозы, связанные с информационной безопасностью.

Зависимость от технологий порождает множество рисков и для частных лиц, и для бизнеса, и для государства. От этих рисков не застрахован никто, даже самая крупная и уважаемая компания в любой момент может столкнуться с нежелательными событиями, которые выльются в финансовые или репутационные потери.

Из новостей мы регулярно узнаем о новых утечках и взломах, от которых страдают крупнейшие в своих отраслях компании. Они терпят миллиардные убытки из-за кибератак, производства останавливаются, акции падают, а регуляторы накладывают рекордные штрафы. Кибератаки перестали быть только IT-проблемой или проблемой безопасности, а стали реальной угрозой для бизнеса.

Готов ли бизнес принять этот вызов? Ответ можно найти в материалах журнала Positive Research, который вы сейчас держите в руках. В новом номере мы решили заострить внимание на реальной безопасности и риск-ориентированном подходе бизнеса и государства к защите информационных систем.

Эксперты Positive Technologies:

Представили обзор самых громких взломов и утечек — 6

Отметили актуальные тренды информационной безопасности и поделились своими прогнозами — 12

Рассказали о недопустимых для бизнеса событиях — 66

Об эволюции и роли киберполигонов — 73

О работе глобального SOC в рамках прошедших киберучений The Standoff 2020 — 94

ИБ-2020: самые громкие взломы и утечки

Александр Антипов,
SecurityLab.ru

на чтение
10 мин.

Ушедший 2020 год запомнится не только пандемией COVID-19, но и рядом беспрецедентных событий в сфере ИБ, доставивших немало головной боли как правительственным организациям и частным компаниям, так и рядовым пользователям. К сожалению, коронавирусная инфекция ничуть не снизила уровень киберпреступности. Напротив, в прошедшем году число фишинговых атак, утечек данных, а также инцидентов с участием программ-вымогателей существенно возросло, во многом благодаря массовому переходу на удаленную работу и цифровому общению с друзьями и близкими в условиях карантина. В этом обзоре мы собрали самые значимые с нашей точки зрения инциденты.

Массовый взлом учетных записей Twitter и Nintendo

Одним из самых резонансных событий минувшего года стал массовый взлом аккаунтов знаменитостей в социальной сети Twitter. Злоумышленники скомпрометировали учетные записи ведущих политиков, бизнесменов и звезд, включая Илона Маска, Билла Гейтса и Барака Обаму, и от их имени опубликовали сообщения о бесплатной раздаче криптовалюты. Что интересно, виновниками атаки оказались трое подростков, которые с помощью фишинга завладели «админским» паролем сотрудника Twitter, работавшего из дома.

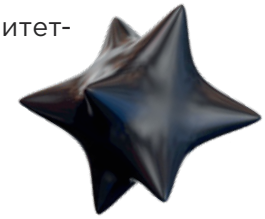
Игровая индустрия также не осталась без внимания злоумышленников: в апреле многие пользователи Nintendo столкнулись со взломом учетных записей, в некоторых случаях хакеры покупали игры Nintendo за чужой счет, но в основном приобретали игровую валюту Fortnite.

Кибератаки на организации, связанные с разработкой вакцин от COVID-19

На протяжении всего года киберпреступные группировки, в том числе проправительственные, активно интересовались информацией о разработке и испытаниях вакцин от коронавируса, атакуя различные компании и исследовательские центры, работающие в этом направлении. Так, в конце года кибератаке подверглось Европейское агентство лекарственных средств, ответственное за сертификацию вакцин. В результате взлома хакеры получили доступ к документам фармацевтических компаний Pfizer, BioNTech и Moderna. Также стало известно о крупной вредоносной кампании, нацеленной на организации, занимающиеся хранением и транспортировкой вакцин, и об организованной северокорейскими хакерами шпионской операции, направленной на производителей вакцин от COVID-19, включая британскую компанию AstraZeneca и американские фирмы Johnson & Johnson и Novavax.

Вымогательские атаки на университетскую клинику в Дюссельдорфе, на Garmin, Software AG и Калифорнийский университет

Прошедший год ознаменовался огромным количеством атак с использованием вымогательского ПО, при которых злоумышленники шифровали компьютеры различных организаций и требовали выкуп за восстановление данных, а в ряде случаев и публиковали похищенную информацию, чтобы стимулировать пострадавших выплатить деньги. Беспрецедентным случаем стала вымогательская атака на университетскую клинику в Дюссельдорфе, нарушившая привычную работу врачей, что повлекло за собой смерть пациентки.



Также в числе самых значимых инцидентов с использованием программ-вымогателей стоит упомянуть атаки на американскую компанию Garmin — производителя цифровых устройств для навигации, активного отдыха и занятий спортом — и одну из крупнейших в мире компаний по разработке программного обеспечения Software AG. В случае Garmin атака группировки WastedLocker привела к четырехдневному сбою в работе сервисов компании и невозможности для миллионов людей получить доступ к GPS-сервисам (в их числе были пилоты, планировавшие полеты). Software AG пострадала от атаки с использованием программы-вымогателя Clop. Хакеры потребовали у компании 20 млн $ выкупа (один из крупнейших выкупов за всю историю вымогательских атак).

Пока весь мир пристально следил за успехами в создании вакцины от коронавируса, группировка Netwalker провела атаку на Калифорнийский университет в Сан-Франциско, занимавший лидирующую позицию среди разработчиков вакцины в США. Хакеры зашифровали важные документы и потребовали выкуп в размере 3 млн $. Представителям университета удалось договориться с вымогателями и снизить сумму выкупа до 1,14 млн $.

Больше новостей из мира информационной безопасности читайте на нашем портале

Утечка учетных данных пользователей Zoom

Из-за пандемии многие организации перешли на удаленную работу, спровоцировав рост популярности приложений для конференц-связи, таких как Zoom, что не осталось без внимания киберпреступников. Сначала на YouTube и Vimeo появились тысячи записей видеоразговоров в Zoom, в том числе записи сеансов психотерапии, школьных занятий с учениками, консультаций с докторами и корпоративных совещаний. Затем на хакерском форуме были бесплатно опубликованы 2300 скомпрометированных учетных записей пользователей.

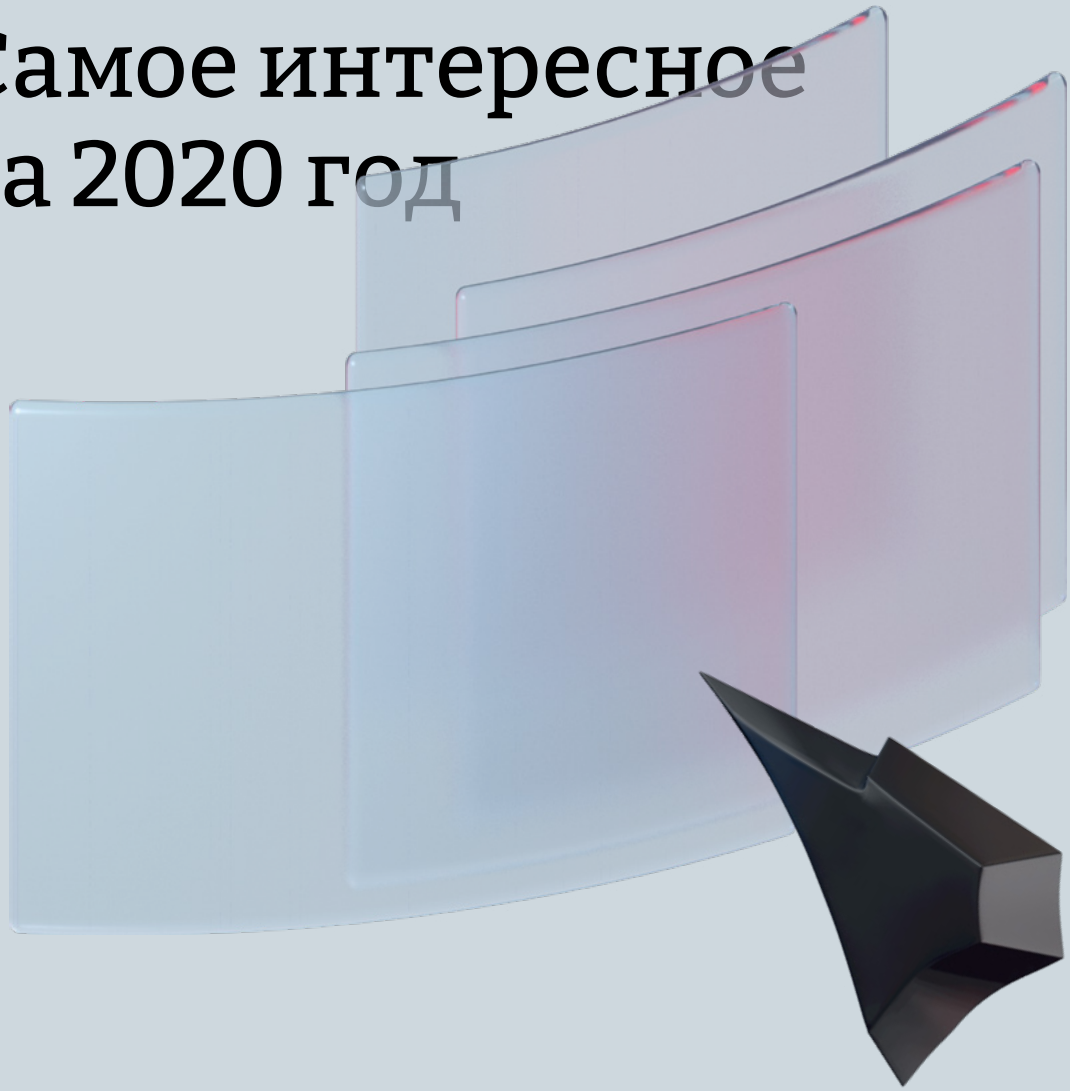
Утечки данных по-прежнему остаются одной из самых распространенных проблем. Год ознаменовался рядом масштабных инцидентов, в числе которых утечки данных 5,2 млн клиентов сети отелей Marriott, 900 тыс. клиентов компании Virgin Media, 4 млн пользователей торговой площадки Quidd, публикация БД с данными 40 млн пользователей популярного мобильного приложения Wishbone, публикация баз данных, содержавших 235 млн профилей пользователей Instagram, TikTok и YouTube, и более 200 млн записей пользователей Twitter и Weibo.

Атака на цепочку поставок SolarWinds — самый резонансный взлом 2020 года

Самым громким событием минувшего года стала атака на цепочку поставок техасской софтверной компании SolarWinds; злоумышленники внедрили бэкдор в обновления для платформы SolarWinds Orion. В результате вредоносное обновление установили порядка 18 тыс. организаций, в частности оно было обнаружено в сетях Министерства финансов США, Управления телекоммуникаций и информации (NTIA) Министерства торговли США, Министерства внутренней безопасности США, компании FireEye, а также в инфраструктуре Microsoft, Mimecast, Palo Alto Networks, Qualys, Fidelis Cybersecurity. Президент Microsoft Брэд Смит охарактеризовал инцидент как «самую крупную и изощренную атаку, которую когда-либо видел мир».

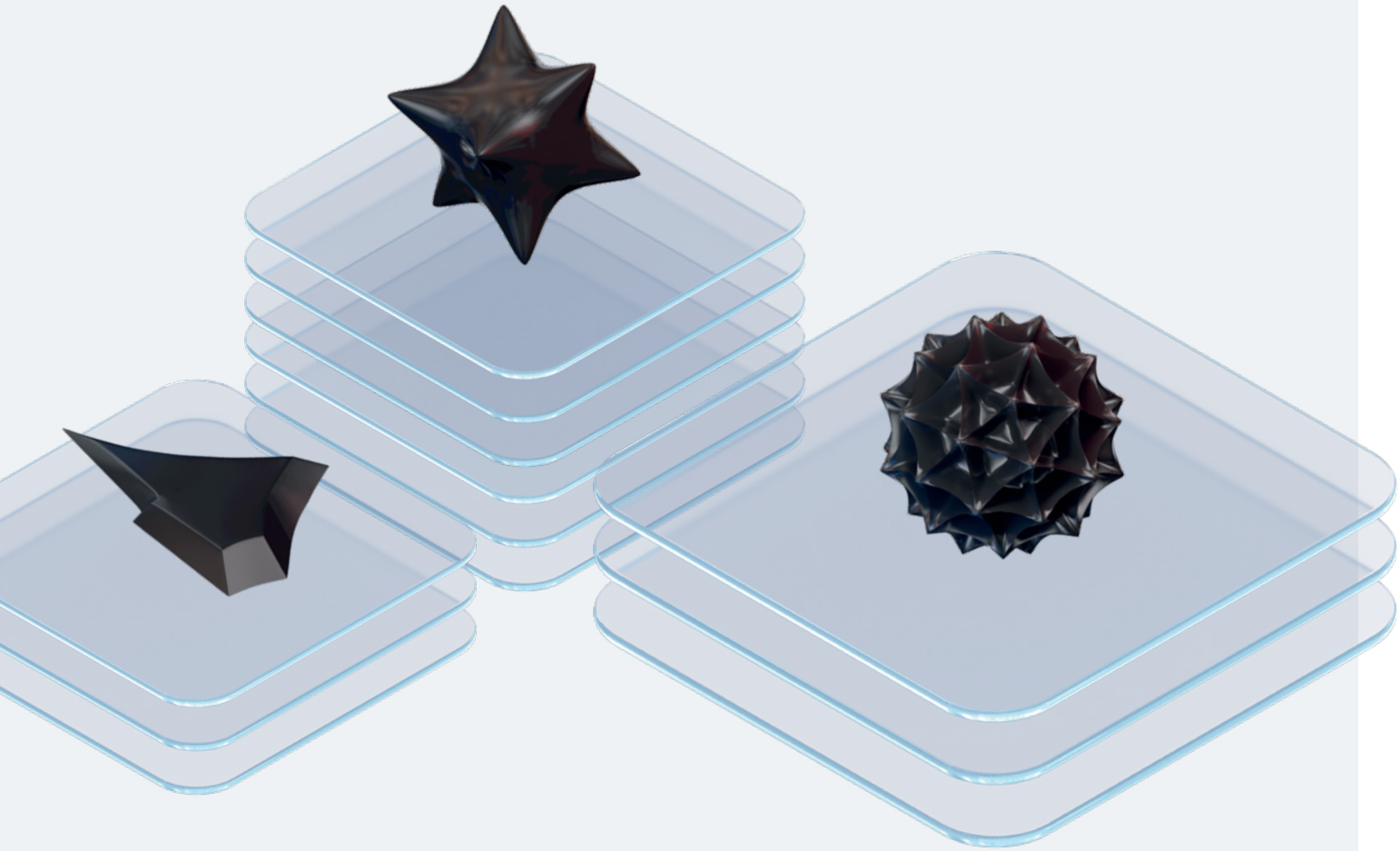
Уязвимости, найденные PT SWARM

Самое интересное за 2020 год



Check Point	ICA Management Tool Argument Injection	CVE-2020-6020	[4,2]	
Cisco	ASA Memory Leak	CVE-2020-3259	[7,5]	
	ASA Unauth File Read	CVE-2020-3452	[7,5]	
	ASA Unauth DoS	CVE-2020-3187	[9,1]	
	Integrated Management Controller Unauth RCE	CVE-2020-3470	[9,8]	
Citrix	XenMobile Unauth Path Traversal	CVE-2020-8209	[7,5]	
Dell	iDRAC 9 ArbitraryFile Read	CVE-2020-5366	[7,1]	
F5	BIG-IP Unauth DoS	CVE-2020-27716	[7,5]	
	BIG-IP Unauth RCE	CVE-2020-5902	[10]	
IBM	Maximo JavaDeserialization	CVE-2020-4521	[8,8]	
Oracle	WebLogic ArbitraryFile Read	CVE-2020-14622	[4,9]	
Palo Alto	PAN-OS Post-Auth RCE	CVE-2020-2037	[7,2]	
	PAN-OS Post-Auth RCE	CVE-2020-2038	[7,2]	
	PAN-OS Unauth DoS	CVE-2020-2039	[5,3]	
SonicWall	SonicOS Unauth Buffer Overflow	CVE-2020-5135	[9,8]	
Sophos	XG Firewall Unauth Heap Overflow RCE	CVE-2020-11503	[9,8]	
VMware	vCenter Unauth Arbitrary File Read	–	[5,3]*	

* По оценке экспертов PT SWARM



на чтение
40 мин.

Кибер-безопасность 2020–2021: тренды и прогнозы

Борис Симис

Заместитель генерального директора Positive Technologies по развитию бизнеса

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, тема ИБ становится все более актуальной, в том числе и в силу объективных условий: общее число угроз и активность киберпреступников растут год от года. Проблема кибербезопасности все больше становится понятной и близкой руководству различных компаний, и соответственно, во главу угла все чаще ставится желание исключить реализацию тех или иных бизнес-рисков. И очевидно, что построение практической безопасности идет рука об руку с увеличением соответствующих бюджетов.

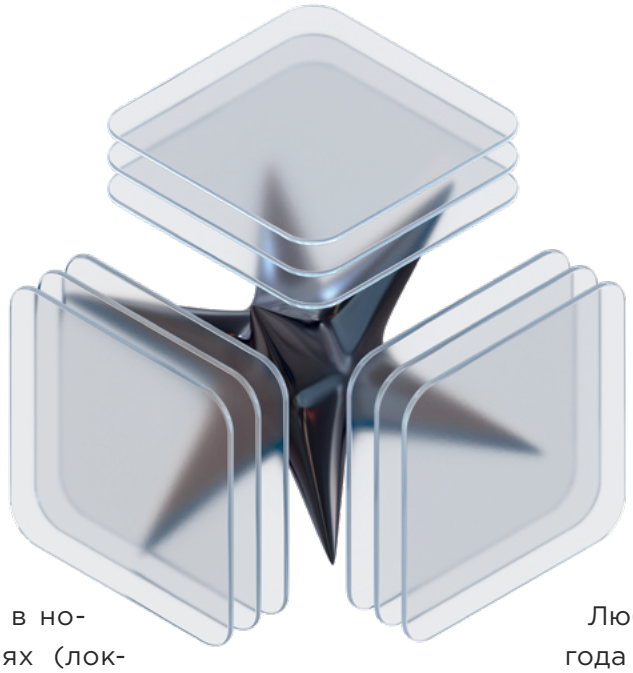
Во-вторых, кибербезопасность КИИ, начавшаяся как концепция несколько лет назад с обследований, категоризации и проектирования, наконец-то дошла до этапа реальных внедрений. И это обеспечивает рост оборотов для производителей средств защиты и интеграторов.

В-третьих, нельзя не отметить, что в минувшем году бизнес, понимая, что год грядущий в новых условиях будет необычным с точки зрения бюджетирования, стремился максимально реализовать намеченные планы по развитию ИТ и ИБ, использовать для этого все имеющиеся ресурсы.

COVID по всем фронтам

Нельзя сказать, что пандемия COVID-19 никак не повлияла на рынок кибербезопасности. Однако на эту тему было больше разговоров, чем реального влияния. К концу первого квартала 2020 года начала складываться ситуация, вызывавшая опасения: резко снизилось общее число пилотных проектов. И совершенно понятно, почему это

На протяжении 2020 года мы видели два мощных всплеска финансово-проектной активности

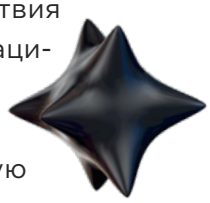


произошло: в новых условиях (локдаун, спешный переход на удаленную работу) эти проекты стало объективно сложнее (а иногда и вовсе невозможно) проводить на площадках компаний. В то же время было понятно, что те же самые новые условия заставили бизнес не замораживать проекты по развитию собственной кибербезопасности. В совокупности оба момента давали весьма опасную ситуацию, в которой компании-заказчики могли отказаться от пилотных проектов и начать ориентироваться только на формальные признаки, в том числе на цену. Но эти опасения так и остались опасениями: конкуренция на отечественном рынке ИБ как была здоровой, так и осталась, а общая ориентированность бизнеса именно на практическую безопасность не позволила компаниям пойти по легкому пути в выборе 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: корпоративные службы ИБ к тому моменту уже имели четко сформированные задачи на год, подтвержденные бюджетные планы, но внешние условия схлопнули оперативную видимость при планировании практически до нуля. Поэтому часть игроков рынка пошла по пути форсирования конкурсов, форсирования старта (или завершения) проектов. В итоге апрель продемонстрировал первый всплеск финансовой и связанной с нею проектной активности на рынке. Вторая волна трат на ИБ прошла 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 года.

Курс на реальный инфобез

Мы уже отмечали, что парадигма ИБ меняется: некоторое время назад сообщество отказалось от идеи строительства киберзаборов и пришло к осознанию того, что цель любой системы безопасности состоит в максимально быстром обнаружении присутствия атакующего внутри информационной инфраструктуры предприятия (в том числе и потому, что нет системы защиты, которую невозможно взломать). Теперь главенствует концепция ability to detect. В течение последнего года она несколько эволюционировала: мы осознали, что вполне реально выстроить такую систему защиты, которая гарантированно не допустит реализации потенциальным злоумышленником конкретных бизнес-рисков. Этот подход подразумевает, что любая компания так или иначе может быть взломана в ходе атаки, и задача службы информационной безопасности — не дать злоумышленнику возможности нанести сколько-нибудь существенный урон. Это тренд, который окончательно оформился буквально у нас на глазах, и очень вероятно, что он будет основным в ближайшие годы.



В связи с этим на первый план выйдет задача создания SOC нового типа, которые будут в качестве KPI и условий SLA оперировать не доступностью в режиме 24/7 или скоростью реакции на инцидент, а намного более конкретным показателем, основанным на гарантированном недопущении неприемлемых для организации рисков. То есть эффективность такого SOC будет оцениваться в буквальном смысле на уровне «да или нет» — реализован риск или не реализован. В этой концепции особое значение приобретают практические киберучения как единственное качественные мерило эффективности выстроенной системы защиты. Говоря об информационной безопасности, легко грешить неконкретностью 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. Это своеобразная интерпретация теории Дарвина: выживут только те продукты, которые способны вовремя выявить активность злоумышленника, заблокировать ее, исключить возможности для развития атаки и в принципе «вычистить» нарушителей из инфраструктуры. И мы как вендор тоже работаем над созданием интеллектуального автоматизированного инструмента, который позволит решать эти задачи быстро и эффективно.

Глобальный новостной повод — эпидемию — использовали все типы хакерских группировок

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 около 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 Tesla[1]. 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 Twitter[2].

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 Garmin[3]. 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-группировки[4].

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 SolarWinds[5]. В нашей практике мы сталкивались с такими же

1

2

3

4

5

Supply chain attacks стали настоящей болью в 2020 году

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 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 ИТ 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.

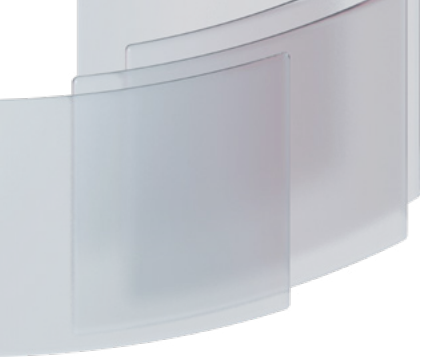
Обратная сторона «удаленки»: атаки на сервисы для удаленного подключения и взлом ПО для онлайн-конференций

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 в IV квартале 2020 года выросла до 36% (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 четвертом квартале она достигла 56%. 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, Clop. 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 подельникам 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 продолжат 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 отнестись 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-го 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 19% от всех атак, направленных на организации. За 2020 год мы зафиксировали 359 атак на государственные учреждения. По сравнению с 2019 годом существенно выросла доля атак с использованием ВПО (71%) и социальной инженерии (64%). Этому могла способствовать пандемия: многие злоумышленники рассылали в госучреждения разных стран письма с вредоносными вложениями на тему коронавирусной инфекции. В 58% случаев атаки проводились с целью шпионажа.

В начале 2020 года были замечены рассылки APT-группировок SongXY, APT36, TA428, TA505 и Higaisa, которые распространяли вредоносные документы, используя тему COVID-19. Эта же тема использовалась в атаках с помощью вредоносных программ Chinoxy 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 понимание вероятного сценария развития такой атаки в инфраструктуре. Методика дорабатывается с учетом мнения специалистов, работающих в отрасли, но уже заметно,

Моделирование бизнес-рисков на киберполигоне станет одним из основных трендов ИБ

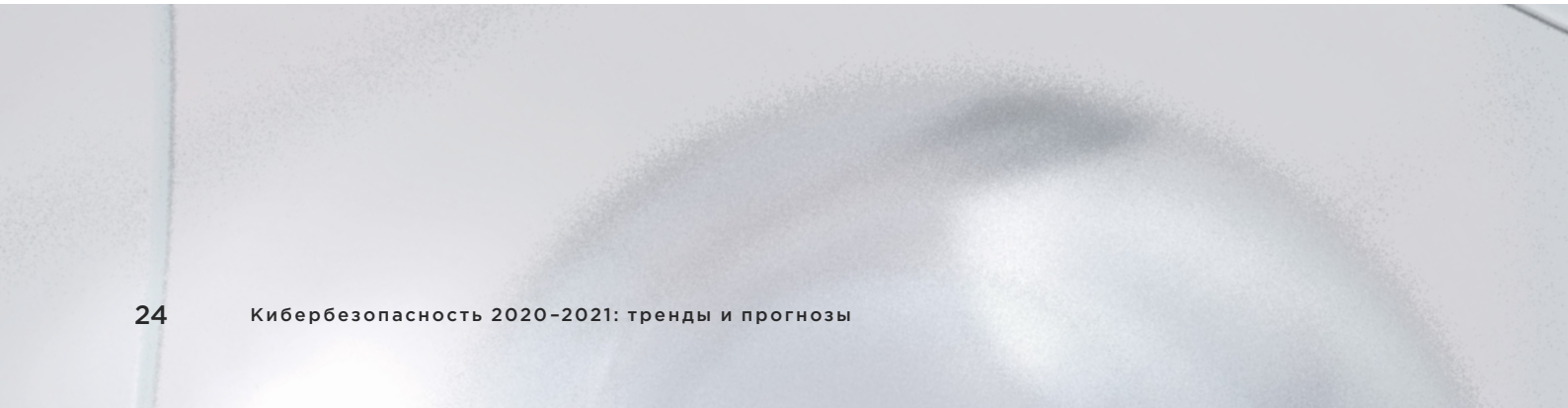
что регулятор взял курс на существенное повышение эффективности ИБ российских компаний с учетом изменяющегося ландшафта угроз.

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.

В 93% случаев рядовые пользователи становятся жертвами массовых хакерских кампаний



Атаки на пользователей

В 2020 году мы отметили 325 кампаний, которые были направлены против частных лиц. Число атак выросло на 11% по сравнению с предыдущим годом. Рядовые пользователи преимущественно становятся жертвами массовых кампаний (в 93% случаев), чаще всего это атаки с использованием социальной инженерии (69%). В 59% случаев злоумышленники заражали устройства пользователей вредоносным ПО. В основном ВПО распространялось через сайты, электронную почту и официальные магазины приложений. Половина атак на частных лиц с использованием вредоносов была проведена с помощью шпионского ПО, в 22% атак использовались банковские трояны. В первую очередь злоумышленников интересовали учетные данные для доступа к сервисам — они составили 36% от общего объема украденной информации, по 19% пришлось на данные платежных карт и персональные данные.

Фишинговые атаки на тему COVID-19 в первую очередь коснулись обычных людей. Злоумышленники не только рассылали фишинговые письма, но и создавали тематические сайты[1], 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[2]. Во время массовой самоизоляции создавалось множество фейковых сайтов[3], 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, нелицензионное ПО, старые неподдерживаемые версии ОС, отсутствие антивирусов, использование простых паролей и прочие ошибки позволяют превратить домашний компьютер сотрудника в источник атак на компанию.

1

2

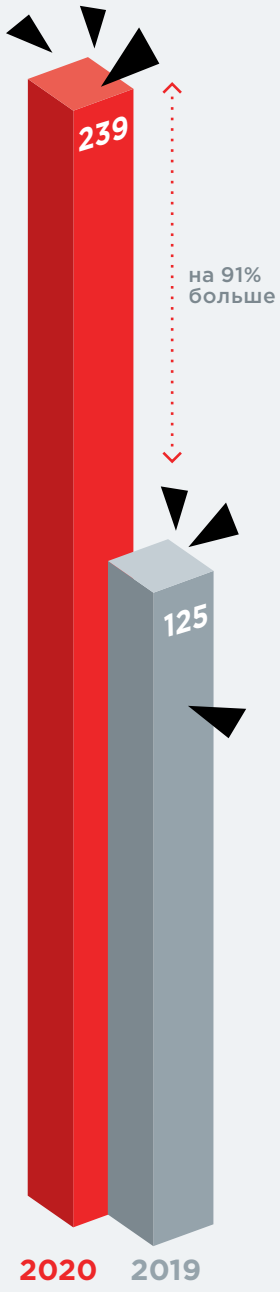
3

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 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. При этом под удар попадают обычные пользователи.



Количество атак на промышленные и энергетические компании

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 239 атак на предприятия из этих отраслей: это на 91% больше, чем в 2019 году (125 атак). В девяти из каждых десяти атак на промышленность злоумышленники использовали вредоносное ПО. На долю шифровальщиков среди них пришелся 41% атак, а шпионское ПО было замечено в 25% 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 шестая 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

С начала 2021 года число атак
на промышленность увеличилось
и держится на стабильно высоком уровне

не снижается актуальность атак группы RTM, за весь 2020 год эксперты PT ESC выявили более 100 фишинговых рассылок этой группы.

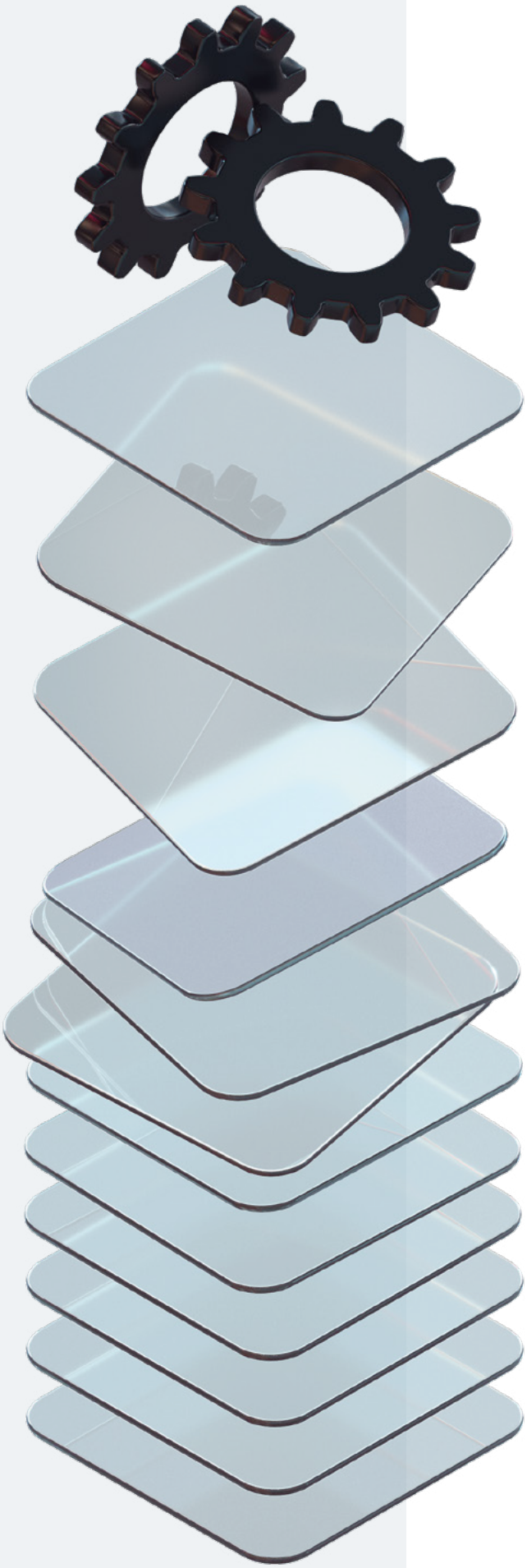
Прогнозы

С начала 2021 года число атак на промышленность увеличилось и держится на стабильно высоком уровне. Мы предполагаем, что инте-рес 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, это целенаправленные атаки с использованием шифровальщиков. Последствия атак, такие как остановка производства или авария, скрывать довольно сложно. А определение источника атаки в случае заражения шифровальщиками не представляет трудности: злоумышленники сами информируют о взломе, когда 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 продолжат 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 получат следующие тренды.



- **Risk-oriented threat modeling.** Применение практик риск-ориентированного моделирования угроз кибербезопасности промышленных объектов. Станет заметен переход от классических вероятностных методов моделирования киберугроз отдельных индустриальных систем к методам, рассматривающим киберугрозы как один из факторов операционных и бизнес-рисков компаний в целом.

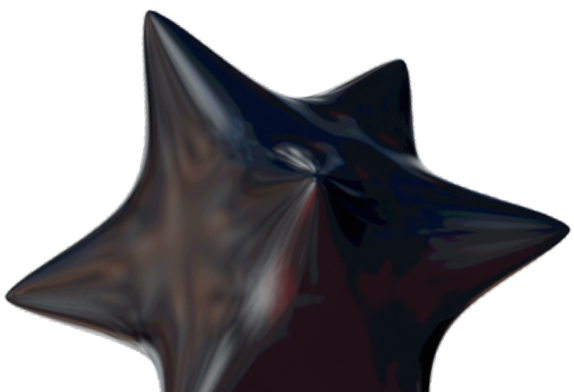
- **SCADA data-driven anomaly detection and response.** Развитие технологий обнаружения аномалий и атак на инфраструктуру индустриальных систем за счет анализа прикладных данных SCADA-систем. Развитие подобных технологий особенно будет заметно в системах таких классов, как NTA/NDR, EDR, SIEM.

- **Security management processes automation.** Расширение автоматизации процессов управления кибербезопасностью, особенно в части обнаружения и реагирования на инциденты кибербезопасности.

- **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 провести несколько атак на нефтехимический завод и нефтяное месторождение, 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.



Основные проблемы безопасности телекоммуникационных сетей все еще кроются в недостатках защищенности протоколов, используемых в сетях 2G, 3G и 4G

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 лишить 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 данных 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.

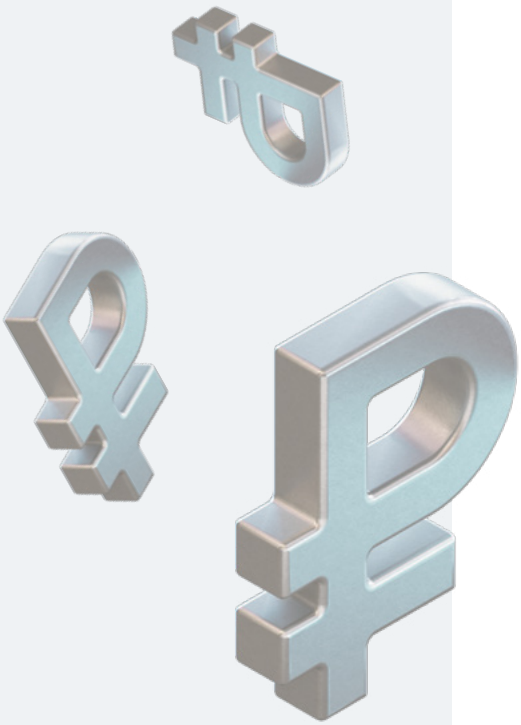
При этом продолжатся исследования архитектуры и протоколов сетей 5G, поиск уязвимостей и недостатков. Хотя при разработке спецификаций были учтены недостатки безопасности предыдущих поколений мобильной связи, новые технологии несут с собой новые риски.

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 126 атак на финансовые компании, что превосходит число атак за 2019 год (их было 92). В 61% атак использовался фишинг: это основной метод проникновения в локальную сеть финансовых организаций; еще в 21% случаев использовался хакинг (эксплуатация уязвимостей и недостатков безопасности). Вредоносное ПО применялось в 65% атак. По большей части это были шифровальщики (29% атак с использованием ВПО), шпионское ПО (28%) и банковские трояны (23%). 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.

1

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 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 продолжат искать известные уязвимости на периметре: результаты пентестов[2], проведенных в финансовых организациях, свидетельствуют о низком уровне защищенности — в семи из восьми компаний внешний злоумышленник смог бы проникнуть в локальную сеть из интернета.

2

Стоит ожидать атак со стороны уже известных групп, которые могут изменять свои техники для сокрытия атак, совершенствовать ВПО, менять регионы атаки

Ключевые проблемы безопасности банкоматов

В настоящее время идет переход банковского ПО на новую операционную систему Windows 10. Она обладает бóльшим 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 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 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 APT. 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, реализовали 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 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 платежам, 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.

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, — это новая для индустрии идея. Нужно нарабатывать опыт, нужно 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,

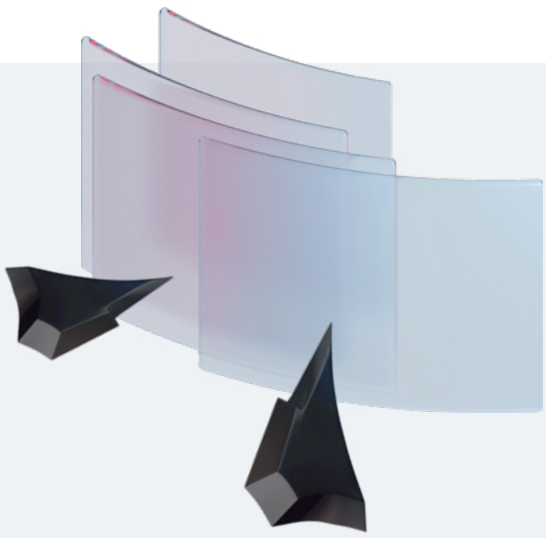
как в отделениях банков, и не по связке «кредитная карта — код подтверждения», как в традиционных системах, использующих протокол 3-D Secure, а по номеру телефона, к которому привязана банковская информация плательщика.

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.



Можно делать супернадежные блокчейн-системы, но все равно останется возможность путем взлома веб-интерфейса или атаки на устройство клиента получить доступ к деньгам

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,
- получить доступ 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. Наметились 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.

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[3].

Хороший пример комплексного подхода к безопасности ОС — недавно опубликованная модель безопасности Android[4], 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, использующей цепочку уязвимостей нулевого дня[5]. 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.

1

2

3

4

5

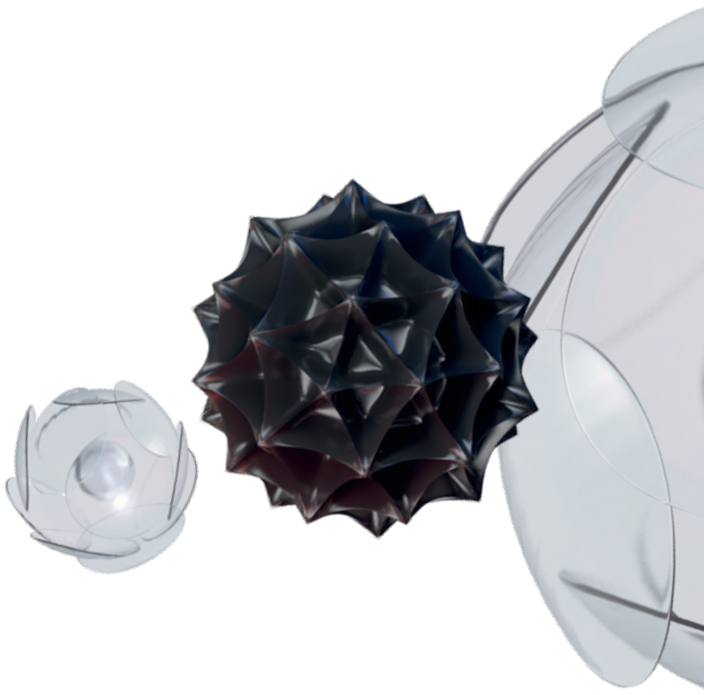
Марк Ермолов

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 чистым research, не тратя время на подготовку к конференциям и другим мероприятиям, и это обязательно найдет свое отражение в ближайшее время.

В будущем можно ожидать шквала новых аппаратных уязвимостей



Exconfidential Lake — утечка, связанная с платформами Intel, которая подстегнула интерес к изучению аппаратной безопасности

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 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 не работает, и я уверен, что в ближайшее время мы будем пожинать горькие плоды решений, принятых когда-то технологическими лидерами отрасли, в виде новых «неустранимых» 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 работы[1]. 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

2

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. В среднем на наших смартфонах установлено по полсотни приложений, 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, нашумевшая 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 пользователями[2]. 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 Notification[3]. 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 человека[4]. 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.

3

4

Александра Мурзина

Ведущий 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 решениями типичных задач. Уже известны как преимущества, так и подводные камни применения техник для анализа, быстрого реагирования и защиты с помощью искусственного интеллекта, поэтому сочетание традиционных техник с новомодными является best practice.

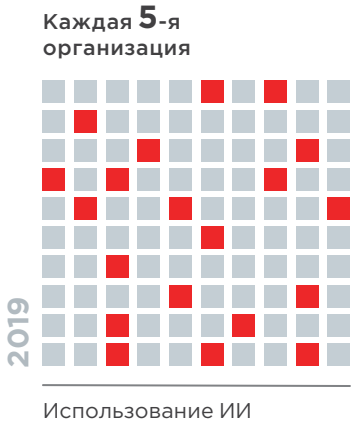
Согласно исследованию, проведенному Capgemini[1] в 2019 году, почти две трети опрошенных компаний считают, что ИИ поможет выявить критически опасные киберугрозы. В то же время 69% организаций считают, что ИИ будет неотъемлемой частью своевременного реагирования на кибератаки. И если

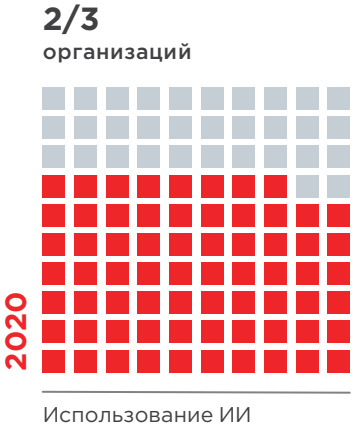
в 2019 году только каждая пятая организация использовала техники, связанные с ИИ, то в 2020 году это были уже почти две трети.

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. Кроме того, компании могут использовать ИИ 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, поскольку разработчики либо не знают о возможных рисках, либо предпочитают сначала выпустить продукт, а потом уже разбираться с проблемами. Такая ситуация приводит к серьезным последствиям. Только в первом квартале 2020 года количество крупномасштабных утечек данных увеличилось на 273%[2].





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 атак на системы, использующие машинное обучение[3]. В проекте участвовали не только Microsoft, но и еще 16 исследовательских групп. Причем речь идет не просто о потенциальных рисках, 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.

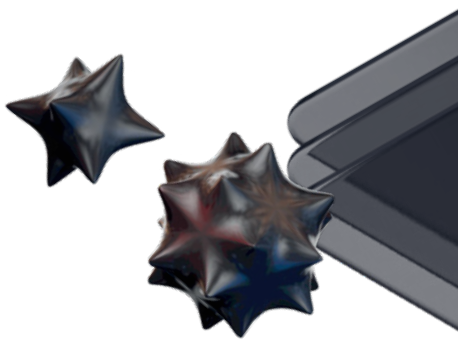
Если говорить про ИИ как инструмент для атак, то стоит выделить активно развивающуюся область deepfake — техники подмены лиц на фото или видео или имитации голоса. В данный момент реалистичная подмена не является сложной задачей. В интернете много примеров и обученных моделей машинного обучения, а в 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 €[4], то в начале 2021 года злоумышленники просто смогли заработать, разместив фейковое объявление и пригласив пользователей от лица основателя компании Dbrain и популяризатора нейронаук Дмитрия Мацкевича на блокчейн-платформу[5].

3

4

5

Не стоит забывать, что ИИ является программным продуктом, который сам по себе может быть уязвим и несет определенного рода риски



6

7

8

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[6] , Amazon[7] , Tesla[8]), 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.

Взлом на заказ

Яна Юракова,
Вадим Соловьев

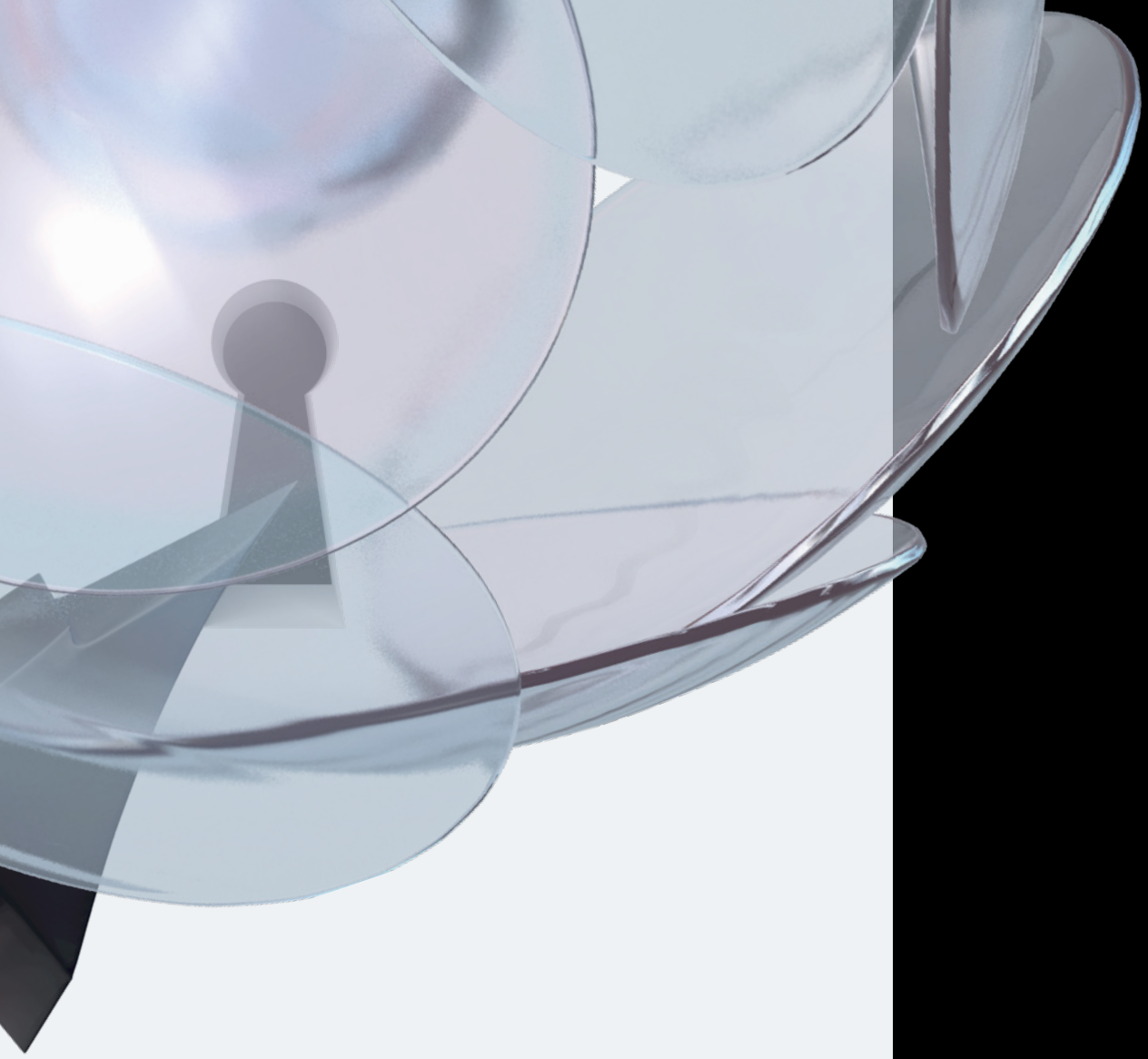
отдел аналитических исследований информационной безопасности Positive Technologies

на чтение
25 мин.

С помощью корпоративных сайтов, интернет-магазинов, веб-сервисов бизнес решает множество своих задач. Клиенты регистрируются на этих площадках, оставляя свои персональные данные, совершают покупки, вводя данные банковских карт, а также используют предоставленные ресурсы для хранения или отправки конфиденциальной информации. Очевидно, что к такому объему данных захотят получить доступ не только конкуренты, но и киберпреступники, поэтому сегодня никого не удивишь новостями об очередной утечке персональных данных в крупной компании. Зачастую эти события связаны с успешной атакой на веб-приложения, в результате которой злоумышленники получили доступ к базе данных пользователей или похитили другую информацию. Например, в сентябре 2020 года хакеры взломали более 2800 интернет-магазинов на платформе Magento и внедрили вредоносный скрипт, который собирал личную информацию и данные платежных карт клиентов[1].

В результате взлома сайта могут пострадать и пользователи, и сама компания. Анализ защищенности веб-приложений, проведенный специалистами Positive Technologies, показывает, что в 92% веб-приложений злоумышленник может проводить атаки на клиентов, в 68% случаев возможна утечка важных данных, а в 16% злоумышленник смог бы получить контроль над приложением и ОС сервера[2].

Мы проанализировали десять наиболее активных форумов в дарквебе[3], на которых представлены услуги по взлому сайтов, покупке и продаже баз данных и доступов к веб-ресурсам[4]. В этой статье мы расскажем о том, зачем хакеры взламывают сайты и к каким последствиям для владельца и пользователей ресурса это может привести.

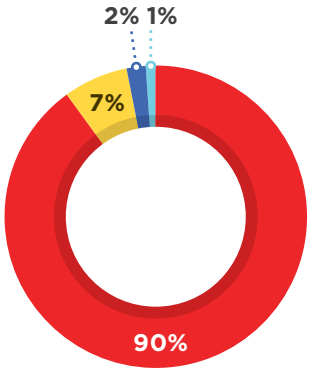


3 Всего на этих форумах зарегистрировано более 8 млн пользователей, создано более 7 млн тем, в которых опубликовано более 80 млн сообщений.

1

2

4 В рамках данного исследования не учитывались объявления, связанные с услугами по организации DDoS-атак на веб-ресурсы.



- Покупка услуг по взлому
- Продажа услуг по взлому
- Продажа сервисов и программ для взлома
- Поиск напарников

Рисунок 1. Категории запросов, связанных со взломом сайтов

Зачем взламывают сайты

В 90% случаев в дарквебе на форумах, посвященных взлому сайтов, ищут исполнителя-хакера, который сможет предоставить заказчику доступ к ресурсу или выгрузит базу пользователей. В 7% записей фигурируют предложения услуг по взлому сайтов. Остальные сообщения направлены на продвижение сервисов и программ для взлома сайтов и поиск единомышленников.

Под предложениями услуг подразумеваются объявления, опубликованные владельцами сервисов и хакерскими группировками. Они не могут выступать в качестве показателей спроса и предложения, так как зачастую размещаются единожды. О величине спроса на вышеперечисленные услуги можно приблизительно судить только по единичным запросам пользователей, которые по различным причинам не воспользовались информацией о предложениях услуг.

Начиная с марта 2020 года мы наблюдаем укрепление интереса к взлому сайтов. К этой тенденции могло привести увеличение количества компаний, представленных в интернете, которое спровоцировала пандемия коронавируса. Организации, ранее работавшие на офлайн-площадках, были вынуждены перейти в онлайн-формат для того, чтобы не потерять клиентов и прибыль, а киберпреступники не могли не воспользоваться этой ситуацией.

На графике справа приведены данные о количестве новых объявлений на форумах в даркнете. Объявления размещаются не только новыми участниками, но и хакерами с репутацией. Последние делают это, чтобы напомнить о себе. Узнать, какие объявления дублируются или потеряли актуальность, сложно, поэтому мы не приводим количество хакеров или группировок, которые активно предоставляли услуги по взлому в начале 2019 года или занимаются этим сегодня.

Примерно в семи из десяти запросов, касающихся взлома сайтов, основной целью является получение доступа к веб-ресурсу. Злоумышленники могут не только похитить конфиденциальную информацию, но и продать доступ к веб-приложению так называемым скупщикам.

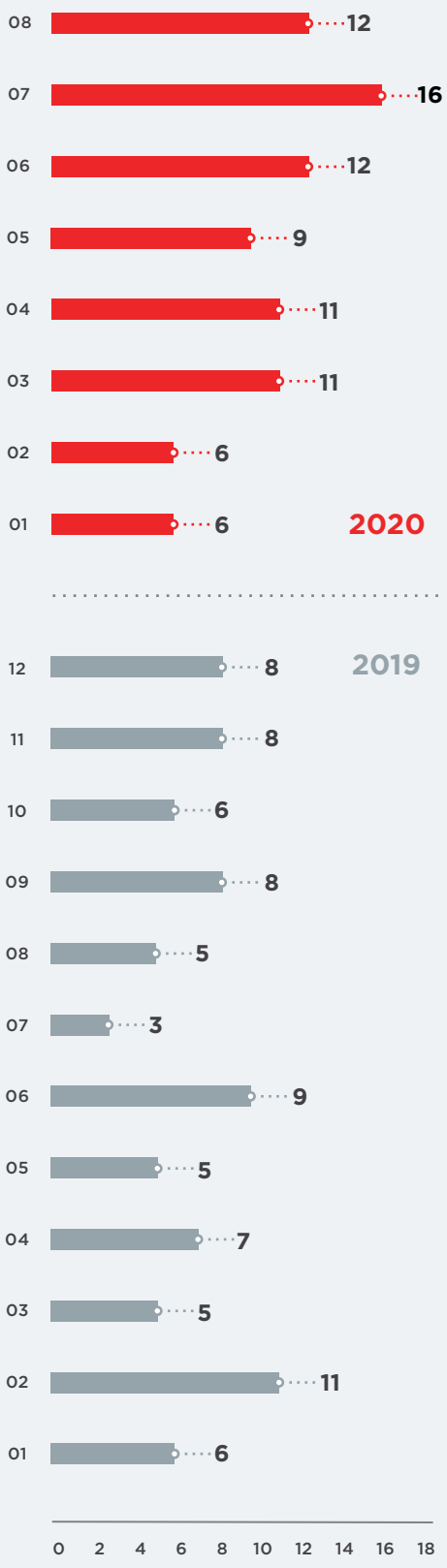


Рисунок 2. Количество новых объявлений про взлом веб-ресурсов на форумах в 2019–2020 годах

Рисунок 3. Распределение запросов по темам

При переходе по ссылке жертве предлагалось пройти процедуру авторизации, а введенные учетные данные отправлялись злоумышленникам

Запросы, направленные на получение баз данных пользователей или клиентов атакуемого ресурса, составляют 21% от всех объявлений. В приобретении такой информации в первую очередь заинтересованы конкуренты и спамеры, которые собирают списки адресов для целевой тематической рассылки, ориентированной на определенную аудиторию (рис. 4, рис. 5).

В 4% запросов основной целью злоумышленников является не взлом сайта, а размещение на нем вредоносных программ, например для проведения атаки типа watering hole или веб-скимминга.

Так, в августе 2020 года APT-группировка Charming Kitten в ходе одной из своих кампаний, направленной на ученых из университетов Хайфы и Тель-Авива, взломала сайт Deutsche Welle для размещения на нем вредоносной ссылки[5]. При переходе по этой ссылке жертве предлагалось пройти процедуру авторизации, а введенные учетные данные отправлялись злоумышленникам (рис. 6).

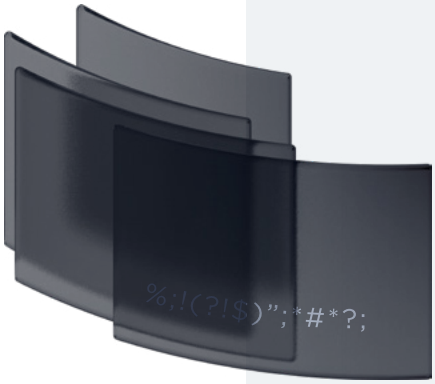
На поиск хакера, который сможет взломать сайт и удалить определенные заказчиком данные, направлены 3% объявлений. Эта услуга может быть, к примеру, востребована среди тех, кто хочет удалить негативные отзывы о компании, размещенные на неподконтрольных этой компании ресурсах (рис. 7).

Предложения о продаже готовых программ и скриптов для взлома встречаются в 2% от общего числа проанализированных запросов.

Атака типа watering hole — это атака, в ходе которой злоумышленники сперва определяют, какие веб-ресурсы часто посещают потенциальные жертвы, а затем взламывают эти ресурсы и размещают на них вредоносные программы

Веб-скиммер — вредоносный код, внедряемый на страницу взломанного сайта, где пользователь вводит данные банковской карты, с целью кражи таких данных

5



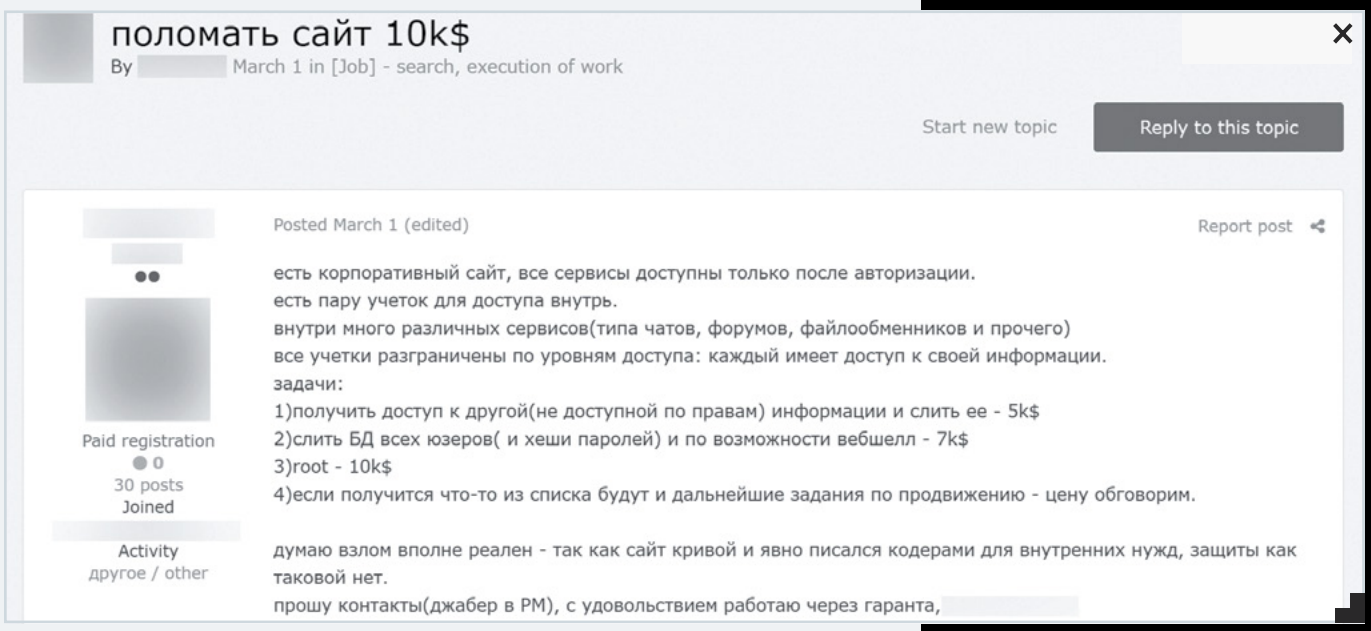
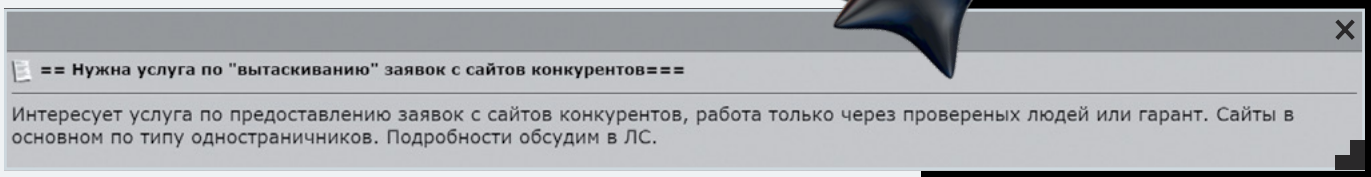


Рисунок 4.
Заказной взлом сайта

Рисунок 5. Сбор сведений
с сайтов конкурентов



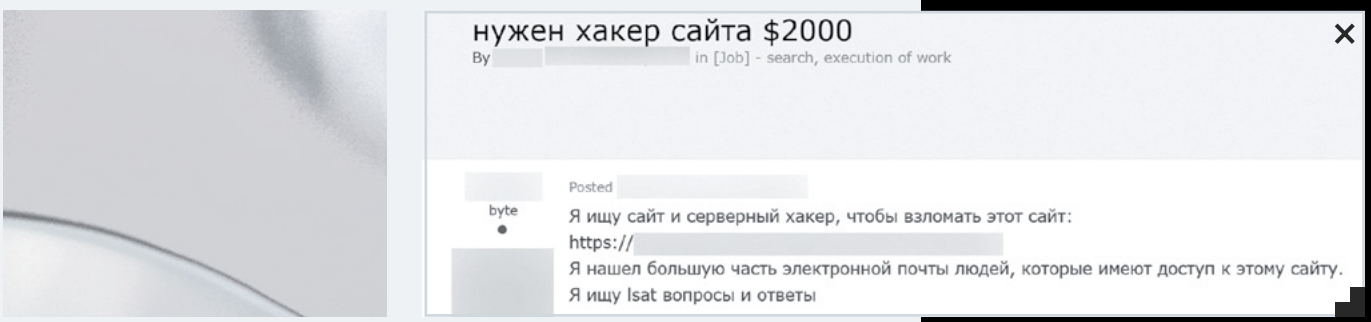


Рисунок 6.
Поиск исполнителя
для взлома сайта

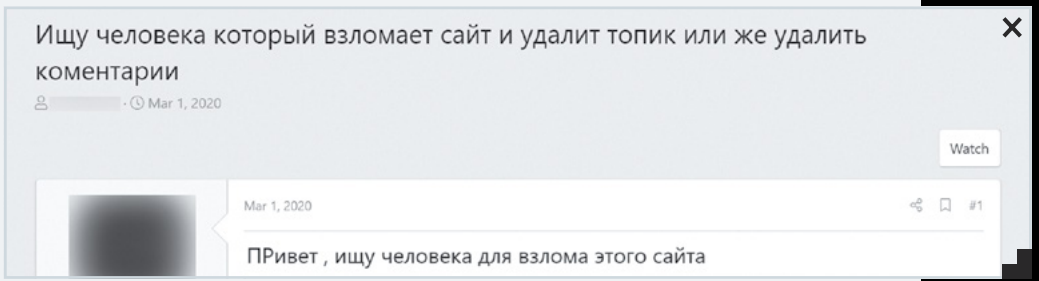


Рисунок 7. Объявление
о поиске злоумышленника-
исполнителя

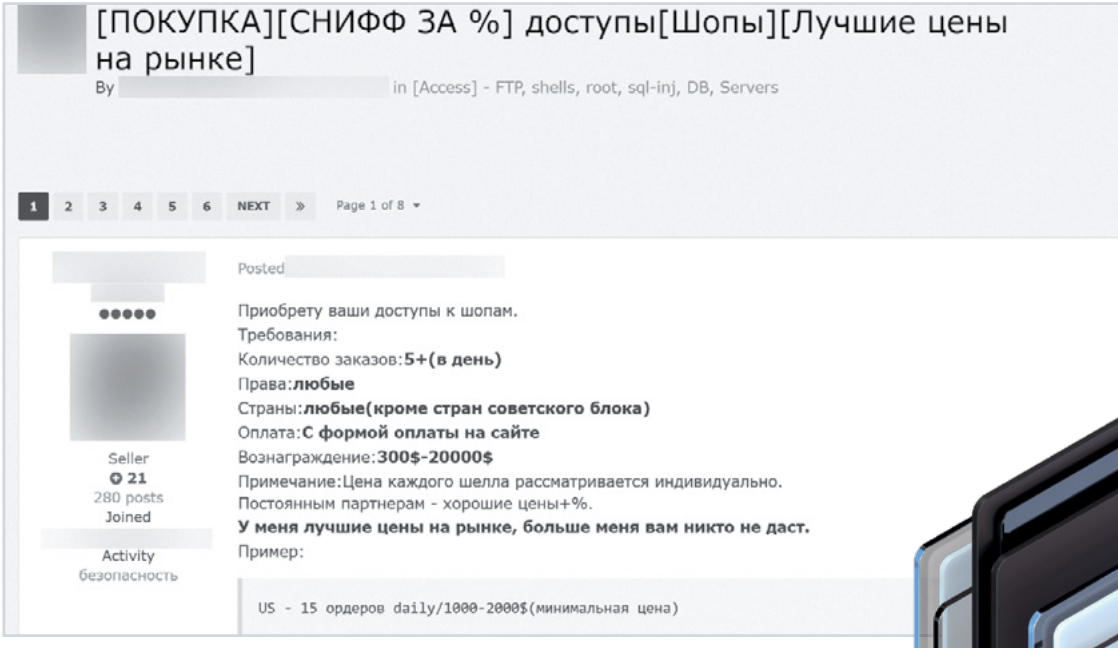
Кто-то ломает, а кто-то покупает

Как мы рассказывали ранее[6], в дарквебе появились скупщики доступов к сайтам Теперь, когда это явление укрепилось, оказалось, что их можно разделить по направлениям. Одни покупают веб-шеллы, другие — доступ к интерфейсам администрирования различных сайтов, а третьи приобретают готовые эксплойты для внедрения SQL-кода применительно к конкретным ресурсам.

Веб-шеллы стоят сравнительно не так дорого, как, например, базы данных, о которых мы расскажем далее, — цены на них варьируются от нескольких центов до тысячи долларов США. В основном это связано с тем, что полученные в результате загрузки веб-шелла привилегии в файловой системе сильно ограничены. Продажа веб-шелла заключается в передаче ссылки на путь к файлу и, возможно, данным для авторизации. Наиболее распространены веб-шеллы на сайтах в доменной зоне .com — 54,3% предложений о продаже.

Скупщикам в первую очередь приходится следить за тем, что интересно рынку потребителей. Явную отраслевую специфику по продаваемым или покупаемым доступам проследить сложно, однако можно смело утверждать, что доступы к интернет-магазинам

Рисунок 8. Объявление о покупке доступов к интернет-магазинам



6

Веб-шелл — это загруженный на сервер файл, с помощью которого злоумышленник может выполнить команды ОС на сервере через веб-интерфейс и получить доступ к другим файлам

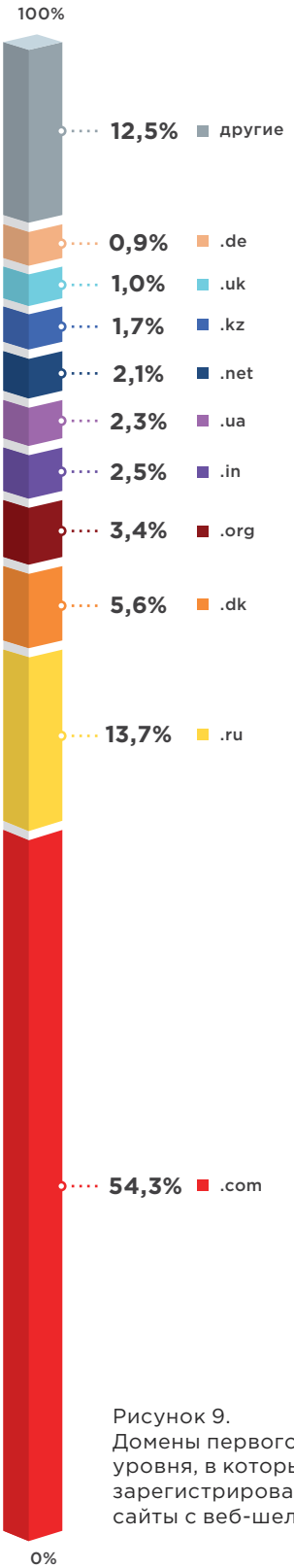


Рисунок 9.
Домены первого уровня, в которых зарегистрированы сайты с веб-шеллами

(«шопам») стоят особняком. Спрос на них стабильно высокий: это обусловлено тем, что при оплате товаров пользователь вносит данные своей банковской карты. Таким образом, хакеру достаточно внедрить на сайте вредоносный код на языке JavaScript, который будет перехватывать вводимую покупателем информацию, и использовать полученные сведения в корыстных целях. Еще один способ нажиться на пользователях это получить привилегированный доступ к интернет-магазину, чтобы оформлять заказы, используя данные чужих банковских карт или вовсе не оплачивая их. Цены на доступы к интернет-магазинам варьируются в диапазоне от 50 до 2000 долл. США.

Если веб-сервис размещается на сервере, подключенном к внутренней сети компании, то главный риск для организации заключается в том, что атакующий (или тот, кто купит доступ к серверу через веб-шелл) сможет развить атаку и проникнуть в инфраструктуру компании. Результаты

проведенных нами внешних пентестов показывают, что в 86% компаний существует хотя бы один вектор проникновения в локальную сеть, который связан с недостаточной защитой веб-приложений[7]. В каждой шестой компании были обнаружены следы атак злоумышленников — выявлены веб-шеллы на ресурсах сетевого периметра, вредоносные ссылки на официальных сайтах или валидные учетные записи в публичных базах утечек.

Доступы к веб-интерфейсам администрирования популярных CMS злоумышленники используют для того, чтобы размещать на сайтах веб-шеллы, вредоносное ПО и использовать их в незаконных рекламных схемах. К примеру, в августе и сентябре 2020 года была замечена серия атак, направленных на сайты ЮНЕСКО, ВОЗ[8], американских правительственных и образовательных учреждений[9]. На этих ресурсах хакеры разместили фишинговую рекламу инструментов для взлома аккаунтов в популярных соцсетях и читерства в онлайн-играх. Они преследовали две цели: кражу данных платежных карт и распространение вредоносного ПО. Часть пользователей перенаправлялась на страницу оплаты, где нужно было ввести реквизиты карты, а другие сразу загружали вредоносы на свои устройства.

Стоит отметить, что участие сайта в незаконных рекламных кампаниях может негативно сказаться на его позиции в списке выдачи в популярных поисковых системах.

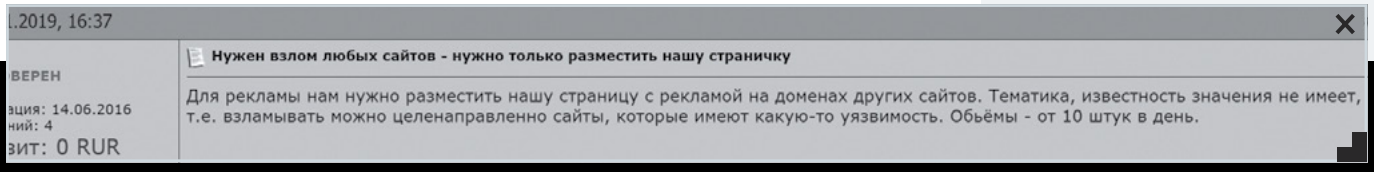


Рисунок 10. Поиск взломщика с целью размещения рекламы

7 8 9

Базы пользователей

Дампы или базы данных со взломанных сайтов могут покупать конкуренты или злоумышленники, которые планируют целевые фишинговые рассылки (рис. 11).

Базы, которые добывают на заказ, стоят от 100 до 20 000 долл. США или от 5 до 50 долл. за 1000 записей о пользователях (рис. 12).

Записи о пользователях содержат, к примеру, адрес электронной почты, имя и фамилию, номер телефона, адрес проживания, номер паспорта, дату рождения. Эти сведения могут использоваться для проведения атак с использованием методов социальной инженерии.

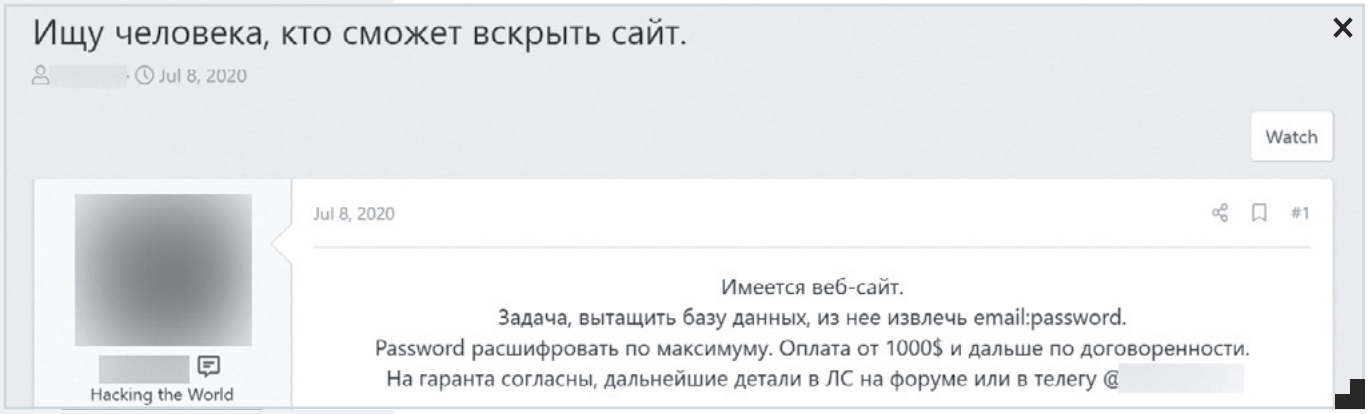


Рисунок 11. Объявление о поиске взломщика сайта

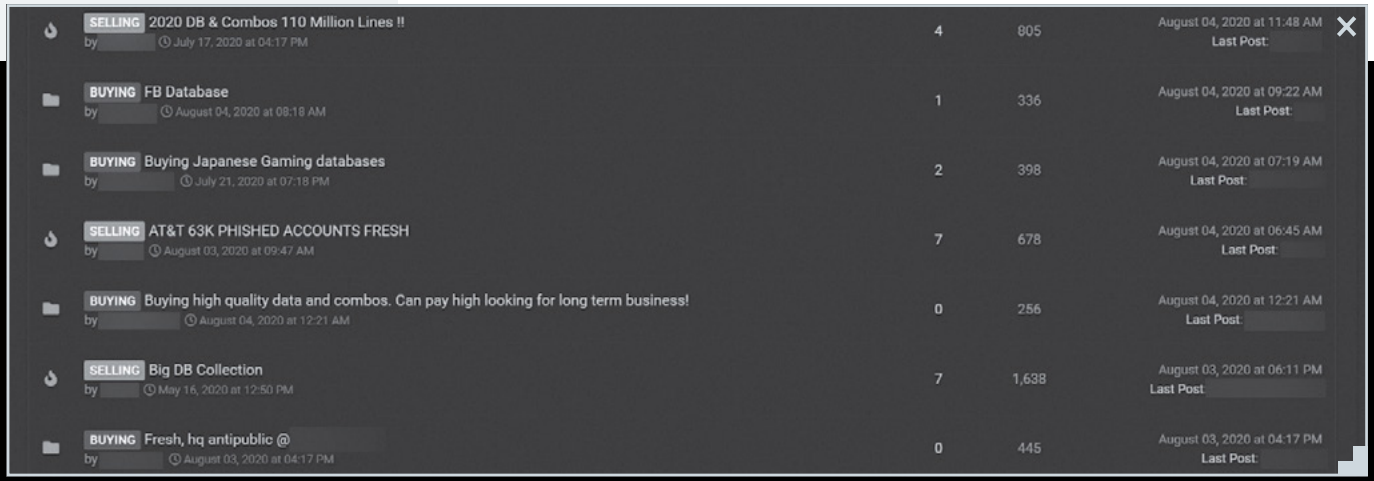
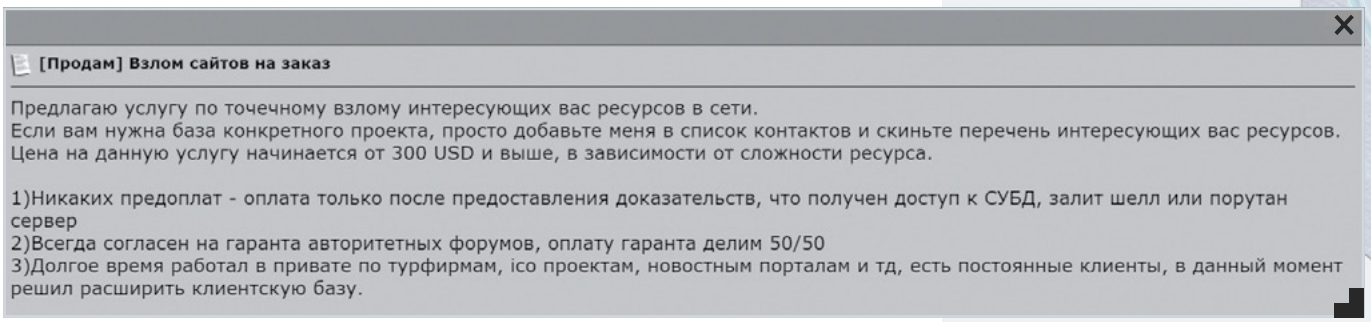


Рисунок 12. Объявления о продаже учетных записей, полученных с помощью фишинга

Сложно ли взломать сайт

В ходе проведенного нами анализа защищенности веб-приложений было выявлено, что в среднем в одном веб-приложении имеется четыре уязвимости высокой степени риска и 12 средней[10]. Даже если не принимать во внимание большое количество уязвимостей, злоумышленники могут воспользоваться методами социальной инженерии и, например, провести целенаправленную фишинговую атаку на администратора ресурса с целью получения учетных данных — логина и пароля. Эти данные позволяют получить доступ к сайту компании.

Основываясь на данных наших исследований, можно сделать вывод о том, что большинство веб-ресурсов недостаточно защищены от воздействия злоумышленников. Также стоит учитывать количество объявлений в дарквебе, в которых предлагаются услуги по взлому веб-сервисов. При желании преступники могут без особых сложностей найти опытного исполнителя или, например, приобрести у скупщика уже готовый инструмент для взлома.


[Продам] Взлом сайтов на заказ

Предлагаю услугу по точечному взлому интересующих вас ресурсов в сети.
Если вам нужна база конкретного проекта, просто добавьте меня в список контактов и скиньте перечень интересующих вас ресурсов.
Цена на данную услугу начинается от 300 USD и выше, в зависимости от сложности ресурса.

1)Никаких предоплат - оплата только после предоставления доказательств, что получен доступ к СУБД, залит шелл или порутан сервер
2)Всегда согласен на гаранта авторитетных форумов, оплату гаранта делим 50/50
3)Долгое время работал в привате по турфирмам, ico проектам, новостным порталам и тд, есть постоянные клиенты, в данный момент решил расширить клиентскую базу.

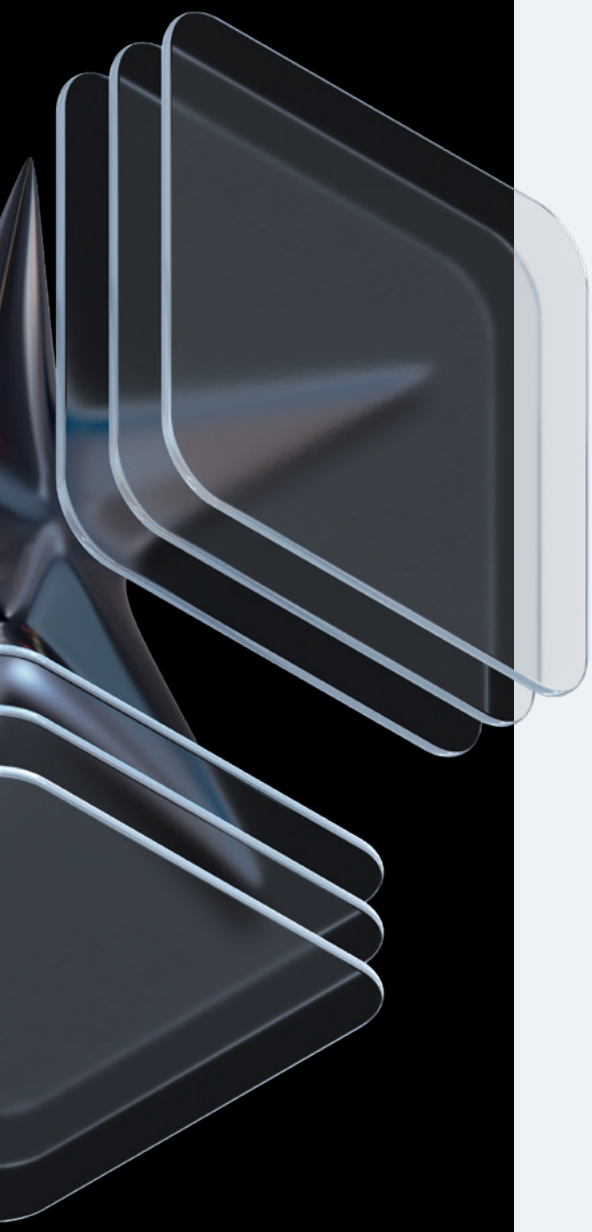
Рисунок 13. Объявление о взломе сайта на заказ

10

Выводы и рекомендации

Услуги по взлому веб-приложений пользуются большим спросом. Объявления о взломе сайтов на заказ не имеют привязки к определенной отрасли, но больше всего клиенты злоумышленников, предоставляющих такие услуги, интересуются интернет-магазинами. В первую очередь это связано с тем, что пользователи оставляют там личные данные и реквизиты банковских карт. Мы считаем, что наметилась определенная тенденция к дальнейшему увеличению спроса, так как все больше компаний переходят в онлайн: этому тренду поспособствовала пандемия COVID-19.

Взлом веб-приложений компании может повлечь за собой серьезные последствия, от утечек данных и санкций за нарушение законодательства (например, GDPR) до проникновения в локальную сеть компании, использования ее ресурсов в последующих атаках — в виде платформы для распространения ВПО или хранения инструментов,



Наметилась тенденция на увеличение спроса услуг по взлому веб-приложений — этому тренду поспособствовала пандемия COVID-19

которые будут загружены в ходе атаки. При построении системы защиты мы советуем использовать риск-ориентированный подход, основанный на оценке уровня допустимого негативного эффекта. Проще и дешевле будет превентивно защитить уязвимую часть сети компании, чем оплачивать огромные штрафы и терять репутацию.

Чтобы защитить свою компанию, следует придерживаться принципов безопасной разработки и использовать средства автоматизированного анализа исходного кода на предмет ошибок и уязвимостей; анализ защищенности веб-приложений в 2019 году показал, что 82% всех уязвимостей сосредоточены именно в коде приложения. Необходимо регулярно проводить анализ защищенности веб-приложений, а также использовать в качестве превентивной защиты межсетевой экран уровня приложений — web application firewall, WAF.

Киберриски: устраняем противоречия, определяем критерии

2000 г.
Бразилия

Авария на нефтеперераба-тывающем заводе Petrobras

2009 г.
Россия

Авария на Саяно-Шушен-ской ГЭС

2019 г.
Китай

Взрыв на химическом заводе

2020 г.
Россия

Авария на ТЭЦ-3 в Норильске

Руководство компании выстраивает стратегию, разрабатывает бизнес-планы, пытается удержать ключевые показатели эффективности, но в один момент все может выйти из-под контроля — когда реализуется риск. Любой бизнес-риск — это потенциальная проблема, которая в конечном счете может привести к финансовым потерям или даже человеческим жертвам.

Приведем несколько примеров из промышленной сферы, где реализация бизнес-рисков обычно приводит к наиболее ощутимым последствиям.

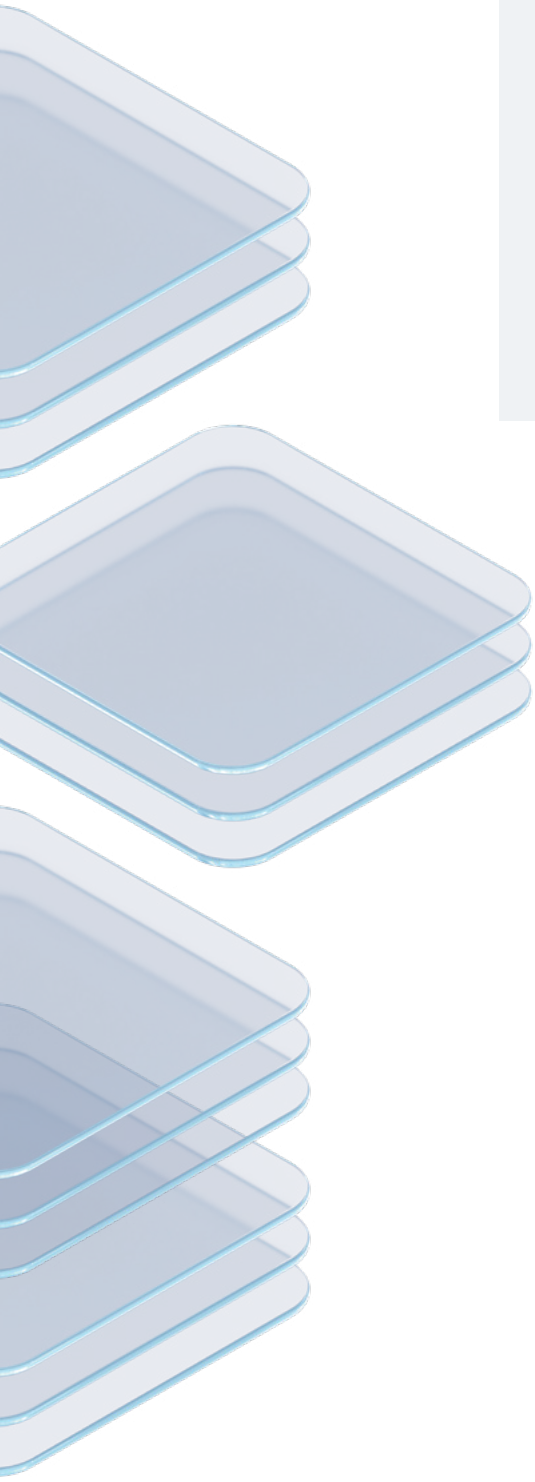
Ольга Зиненко,

отдел аналитических исследований информационной безопасности Positive Technologies

на чтение
10 мин.

В реку вытекло порядка 1,3 млн литров нефти	На ликвидацию аварии компания потратила более **100 млн долларов**
Погибли 75 человек, 13 человек пострадали	Ущерб от аварии превысил **40 млрд рублей**, включая ущерб экологии. **К уголовной ответственности** привлечены семь руководителей и инженерно-технических работников электростанции
Погибли 78 человек, более 600 человек пострадали	Прямой финансовый ущерб — порядка **280 млн долларов**
Разлилось порядка 20 тыс. тонн дизельного топлива	Ущерб экологии — **148 млрд рублей**. Компания «Норникель» обязуется ликвидировать последствия аварии

Проверить возможность возникновения таких серьезных технологических аварий в результате кибератак можно, если тщательно верифицировать все риски. Важно не только знать, какие бизнес-риски актуальны для компании, но и понимать, при каких условиях они могут осуществиться, каковы критерии их реализации. Так, критериями могут быть возможность изменения прошивки ПЛК или получения привилегий оператора.



Лишь каждая четвертая компания обозначает цели для пентеста

Типовой подход к ИБ предполагает проведение тестов на проникновение. Это одна из наиболее востребованных на рынке услуг по анализу защищенности. Но пентест не дает никаких гарантий защиты. Может ли пентест защитить бизнес от нежелательных событий? Можно ли измерить реальный уровень защищенность компании при помощи пентеста? Попробуем ответить на эти вопросы.

Для того чтобы оценить, насколько хорошо инфраструктура защищена от действий злоумышленников, необходимо, в первую очередь, понимать, какие бизнес-системы критически важны для бизнеса и что в них может привлечь хакеров. Как показывает практика, не все заказчики знают о том, что польза от пентеста напрямую зависит от задач, которые ставятся перед экспертами по ИБ. Как правило, перед пентестерами ставят абстрактную задачу по получению максимально возможных привилегий в домене. Только 28% компаний

В 16% компаний за последние два года проводились работы по верификации рисков

до начала работ по анализу защищенности указывают, для каких конкретных систем необходимо проверить возможности злоумышленников[1]. В этом случае цели для пентеста, как правило, формулируют специалисты по ИТ и ИБ компании-заказчика.

Еще реже — в 16% компаний за последние два года — проводились работы по верификации рисков, во время которых руководство компании-заказчика принимало непосредственное участие в определении рисков, реализацию которых необходимо проверить. Однако представители заказчика не всегда могут определить условия, при которых будут реализованы конкретные риски.

Некоторые риски легко проверить, например определить, какие данные могут быть похищены, если скомпрометирован компьютер топ-менеджера. А другие риски, такие как вмешательство в технологические процессы, проверить гораздо сложнее. Определить критерии реализации таких рисков особенно важно, поскольку ущерб от них может быть огромен.

По результатам проектов по анализу защищенности корпоративных информационных систем от внутренних нарушителей

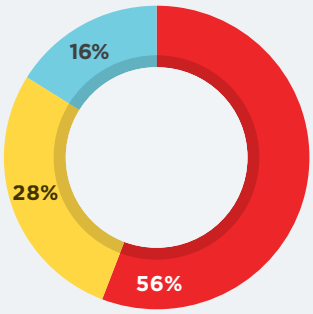


Рисунок 1. Доля компаний, заказывавших работы по анализу защищенности и верификации рисков в 2019–2020 годах

1 Данные по результатам 42 проектов по анализу защищенности корпоративных информационных систем от внутренних нарушителей и верификации рисков, проведенных экспертами Positive Technologies в 2019–2020 годахв 32 компаниях.

Отсутствие очевидной демонстрации последствий атаки позволяет сомневаться в реализуемости киберриска

В 75% промышленных компаний злоумышленник может проникнуть в технологическую сеть

было установлено, что в 75% промышленных компаний[2] злоумышленник может проникнуть в технологическую сеть, получить доступ к оборудованию, отправлять команды на контроллеры и изменять действующую конфигурацию АСУ ТП. Потенциально подобные действия могут привести к авариям, поломке оборудования, остановке производства, порче продукции, нарушениям контрактных обязательств, затратам на восстановление. Так, в одной из компаний был получен доступ к АРМ оператора АСУ ТП, используемому для мониторинга технологических параметров оборудования. В рамках пентеста мы можем лишь предположить, что злоумышленник сможет изменить параметры обработки информации, получаемой от оборудования, что в дальнейшем приведет к сбою в работе этого оборудования. Развить этот вектор атаки в реальной инфраструктуре невозможно, ведь это чревато негативными последствиями, а отсутствие очевидной демонстрации последствий атаки позволяет сомневаться в реализуемости киберриска.

В финансовой сфере доступ к управлению банкоматами из внутренней сети удалось получить в каждом пятом банке[3]. Так, в одном банке злоумышленник мог получить доступ к программам для мониторинга и управления сетью банкоматов и в дальнейшем создавать собственные наборы команд и загружать их на любые банкоматы. Но из-за риска нарушить работу банкоматов загрузка команд, естественно, не проверялась, а значит и оценка последствий атаки была лишь гипотетической.

Уже получив результаты, специалисты заказчика и пентестеры зачастую расходятся в оценке опасности выявленных векторов атаки и в оценке возможных последствий. Специалисты компании-заказчика по ИТ и ИБ уверены, что в случае атаки сработает защитная автоматика, обеспечивающая бесперебойную работу технологических процессов, антифрод-система пресечет подозрительные транзакции хакеров или иные меры защиты укажут на злоумышленников и не позволят им реализовать кибериски. И пентестеры не могут их убедить в обратном, поскольку для этого необходимо проверить все выдвинутые предположения на реальном оборудовании.

2 Данные по результатам 12 проектов по анализу защищенности корпоративных информационных систем от внутренних нарушителей в промышленных компаниях, поставивших цель проникновения в технологический сегмент сети, проведенных экспертами Positive Technologies в 2018–2020 годах.

3 Данные по результатам 15 проектов по анализу защищенности корпоративных информационных систем от внутренних нарушителей в компаниях финансовой сферы, проведенных экспертами Positive Technologies в 2018–2020 годах.

Киберполигон устраняет противоречия в восприятии рисков

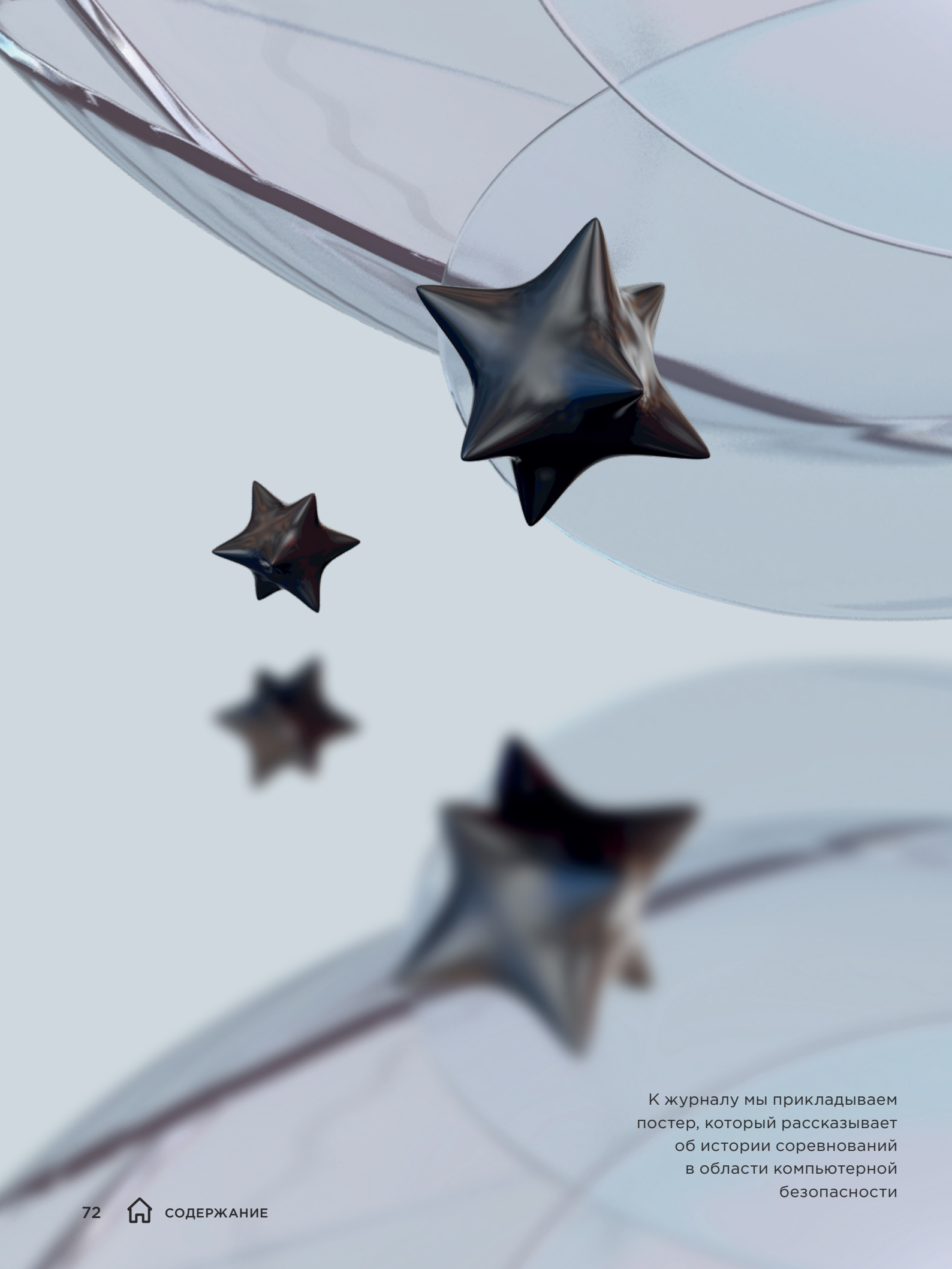
Моделирование инфраструктуры компании на специальном полигоне становится наилучшим решением проблемы восприятия киберрисков. Именно киберполигон позволяет протестировать критически опасные риски, учитывая при этом все связанные с ними бизнес-процессы и системы, и определить критерии реализации этих рисков — те условия, при которых неприемлемое событие может произойти. Обладая информацией о критериях реализации рисков, можно проводить пентест или верификацию рисков в реальной инфраструктуре, поставив целью их достижение.

Как показали киберучения The Standoff, злоумышленник может вызвать пожар на химическом заводе, перекрыв клапан охлаждения в программе для диспетчеров Rapid SCADA. Это значит, что получение доступа к удаленному рабочему столу оператора АСУ ТП во время работ по анализу защищенности будет говорить о фактической реализуемости данного риска. В парке развлечений хакеры могут вмешаться в работу системы управления аттракционами, получив административные права на узле с соответствующей SCADA-системой. Риск будет реализован, если отправить команду на изменение скорости вращения колеса обозрения. В результате колесо сорвется с опор и рухнет (читайте об этом на стр. 89).

Всего во время соревнований The Standoff было реализовано 47% рисков, заложенных в масштабную городскую инфраструктуру. На реализацию первого риска — получение доступа к конфиденциальным документам нефтехимического завода — у атакующих ушло всего 2 часа 50 минут.

Верификация рисков и определение критериев их реализации дают бизнесу бесценную информацию: откуда и какой опасности ждать. А значит, можно заблаговременно спланировать и внедрить меры защиты, которые позволят гарантированно исключить нежелательные события — и в итоге обеспечить необходимые бизнес-показатели.

Всего во время соревнований The Standoff 2020 было реализовано 47% рисков, заложенных в масштабную городскую инфраструктуру



К журналу мы прикладываем постер, который рассказывает об истории соревнований в области компьютерной безопасности

Киберучения на цифровом двойнике инфраструктуры

Оценка реальных рисков для бизнеса

Ольга Зиненко,

отдел аналитических исследований информационной безопасности Positive Technologies

на чтение
15 мин.

Затраты на обеспечение корпоративной безопасности оправданы, ведь ущерб в случае реализации кибератак огромен

Расходы предприятий на кибербезопасность продолжают расти, преодолевая вызванный пандемией экономический спад, который влияет на глобальные расходы в сфере информационных технологий. Согласно данным аналитического агентства Gartner, мировые расходы на ИТ в 2020 году составили порядка 3,6 трлн долларов, что на 5,4% ниже показателей 2019 года[1]. При этом расходы на информационную безопасность по предварительным прогнозам этого же агентства должны были вырасти на 2,4% и достигнуть 123,8 млрд долларов в 2020 году[2]. Основные расходы направлены на защиту инфраструктуры и сетей, а также на обеспечение безопасности пользовательских данных.

Затраты на обеспечение корпоративной безопасности оправданы, ведь ущерб в случае реализации кибератак огромен. Cybersecurity Ventures прогнозировал, что к 2021 году киберпреступность будет стоить миру более 6 трлн долларов в год[3]. Эта сумма включает в себя ущерб от повреждения и уничтожения данных, от потери производительности, кражи денег, интеллектуальной собственности, личных и финансовых данных, потери от нарушения бизнес-процессов после атаки, репутационные потери и многое другое.

1

2

3

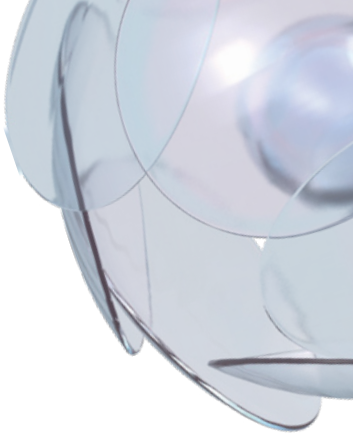
4

5

Уже 50 лет эксперты по безопасности ищут способы наиболее точно оценить ущерб от кибератак

Цифры подсчитаны исследовательскими компаниями, специализирующимися на изучении рынка, но эти цифры не отвечают на вопрос «Чем грозит кибератака моей компании?». Уже 50 лет эксперты по безопасности ищут способы наиболее точно оценить ущерб от кибератак. За это время были разработаны сценарии аудита[4] и придумана методология оценки рисков[5], специалисты начали проводить анализ защищенности информационных систем и тесты на проникновение, компании стали уделять внимание обучению и проверке уровня осведомленности сотрудников в вопросах ИБ, поскольку пользователи — это слабое звено в защите и злоумышленники успешно используют социотехнические атаки. Перечисленные меры хорошо справляются с задачей повышения уровня защищенности компаний, однако они не позволяют проверить реализуемость рисков.

Тестирование на проникновение в режиме red team — это способ приблизиться к условиям реальной атаки. Эксперты имитируют целенаправленные атаки на компанию. В отличие от классического пентеста служба ИБ оказывает противодействие и тем самым повышает свою готовность к реагированию на киберугрозы. Однако недостатком этого способа, как и в случае с пентестом, является использование реальной инфраструктуры компании, из-за чего опять невозможно реализовать риск до конца.



Поэтому среди экспертов по ИБ так популярны соревнования capture the flag. На CTF-площадках участники могут искать уязвимости в сервисах и использовать их для развития векторов атак на другие команды без негативного влияния на бизнес-функции какой-либо компании. Кроме того, такие соревнования — отличный способ обучения исследователей, пентестеров, участников red teams и баг-хантеров. И если раньше бизнес не относился серьезно к подобным соревнованиям, считая их лишь развлечением, то сейчас мы видим, что многие из тех, кто когда-то принимал участие в CTF, теперь сами стали признанными экспертами в области ИБ и занимают в российских компаниях высокие должности.

Аппетит злоумышленников растет с каждым годом, как и ущерб, наносимый организациям в ходе кибератак. Публичные примеры серьезных потерь заставляют компании всерьез относиться к киберрискам и принимать меры, чтобы снизить их вероятность, а ущерб минимизировать.

Движение бизнеса в сторону практической безопасности привело к абсолютно новому формату соревнований. Этим форматом стали киберучения, в которых одновременно могут принять участие все специалисты по компьютерной безопасности — пентестеры, исследователи, сотрудники службы ИБ и центра мониторинга.

Киберучения — это контролируемые атаки, проводимые с целью проверки и улучшения навыков службы ИБ по обнаружению киберугроз и реагированию на них. Сценарии атак для киберучений могут быть полностью автоматизированы, а могут реализовываться с привлечением команды атакующих, состоящей из экспертов по ИБ. Red team имитирует действия настоящего злоумышленника, что делает обучение реалистичным. Если же в мероприятии участвуют одновременно несколько команд атакующих, то появляется возможность всесторонне проанализировать защищенность той или иной инфраструктуры и проработать больше техник и сценариев атак. Может использоваться

Киберучения — это контролируемые атаки, проводимые с целью проверки и улучшения навыков службы ИБ по обнаружению киберугроз и реагированию на них

реальная инфраструктура компании (в этом случае риски реализуются условно), а может применяться специально подготовленная платформа — киберполигон.

Существуют масштабные киберучения, например Locked Shields, организованные Киберцентром НАТО в Таллине, в которых в 2019 году приняло участие более 1200 экспертов по ИБ, или мероприятие Cyber Defense Exercise Агентства национальной безопасности США, которое проходит с 2001 года. Бывает, что киберучения организуются на какую-то определенную тему. Так, Европейское агентство кибербезопасности (ENISA) в декабре 2020 года должно было провести Cyber Europe 2020, где организаторы планировали смоделировать сценарии атак на систему здравоохранения, однако из-за неблагоприятной эпидемиологической обстановки мероприятие перенесено на неопределенный срок.

В 2016 году Gartner впервые разработал документ с критериями выбора поставщика данных услуг, который обновляется ежегодно, что говорит о востребованности киберучений[6].

6

Актуальность киберучений глазами наших респондентов

87% опрошенных хотели бы принять участие в учениях

75% повысить квалификацию сотрудников

66% проанализировать защищенность систем

59% протестировать средства защиты в процессе киберучений

так ответили 2/3 тех, кто считает, что у них в компании применяется недостаточно средств защиты.

55% верифицировать потенциальные риски

Их актуальность подчеркнули и наши респонденты в ходе опроса на портале SecurityLab.ru и в ряде отраслевых сообществ: 87% опрошенных хотели бы принять участие в учениях и с их помощью повысить квалификацию сотрудников (75% респондентов), проанализировать защищенность систем (66%), верифицировать потенциальные риски (55%). Протестировать средства защиты в процессе киберучений хотели бы 59% опрошенных, причем так ответили две трети тех, кто считает, что у них в компании применяется недостаточно средств защиты.

Треть респондентов (32%) готовы потратить на киберучения не более 2 млн рублей. Когда речь идет о небольшой компании с ограниченным бюджетом, у которой потенциальные потери от реализации киберрисков невысоки, можно рассмотреть варианты небольших тренировочных платформ с заранее определенными сценариями кибератак. Такие платформы сейчас набирают популярность за счет невысокой стоимости и широкого охвата аудитории — от рядовых сотрудников до руководителей. Так, примерно за 90 тыс. долларов компания Cyberbit предлагает провести обучение для ключевых сотрудников компании длительностью от трех часов для руководителей и до двух дней для сотрудников SOC. Учения, предлагаемые компаниями CrowdStrike, Security Innovation, Vector Synergy, направлены на проработку сценариев реагирования на кибератаки, включают имитацию действий злоумышленников, но при этом выполняются на заранее подготовленной инфраструктуре (как вариант — облачной) и не учитывают особенности каждого заказчика.

На сегодняшний день лучшим решением является проведение киберучений с привлечением нескольких команд, атакующих цифровую

Впервые цифровые двойники стали использовать в промышленной сфере для моделирования различных нештатных ситуаций на заводах

[7]

модель организации, соответствующую ее реальной инфраструктуре, — цифрового двойника. Впервые цифровые двойники стали использовать в промышленной сфере для моделирования различных нештатных ситуаций на заводах с учетом таких факторов, как расположение оборудования или перемещение сотрудников. Согласно отчету консалтинговой компании Grand View Research, мировой рынок цифровых двойников в 2018 году оценивался в 3,3 млрд долларов США и, по прогнозам, достигнет 38,61 млрд долларов к 2026 году, увеличиваясь в среднем на 35% в год[7].

Использование киберполигона, объединяющего все преимущества технологии цифрового двойника и киберучений, целесообразно для крупных компаний, для которых актуальны риски, несущие огромный ущерб. Киберполигон подходит для организаций со зрелыми процессами, стремящихся к практической безопасности — прозрачной, результативной и обоснованной. У каждой компании своя уникальная инфраструктура и свои бизнес-риски. Для того чтобы корректно верифицировать риски и последствия их реализации, необходимо считаться с этой уникальностью. Киберполигон позволяет оценить значимость ресурсов и определить, что именно может заинтересовать злоумышленников, а red team, в свою очередь, помогает в верификации рисков, актуальных для компании, и их последствий. Кроме того, в отдельных случаях верифицировать риски без киберполигона попросту невозможно, например когда риски связаны с авариями на производстве, охраной окружающей среды, с жизнью и здоровьем людей. Также стоит отметить, что киберполигон позволяет моделировать киберриски не только отдельной компании, но и целого города, отдельной отрасли или даже целого государства.

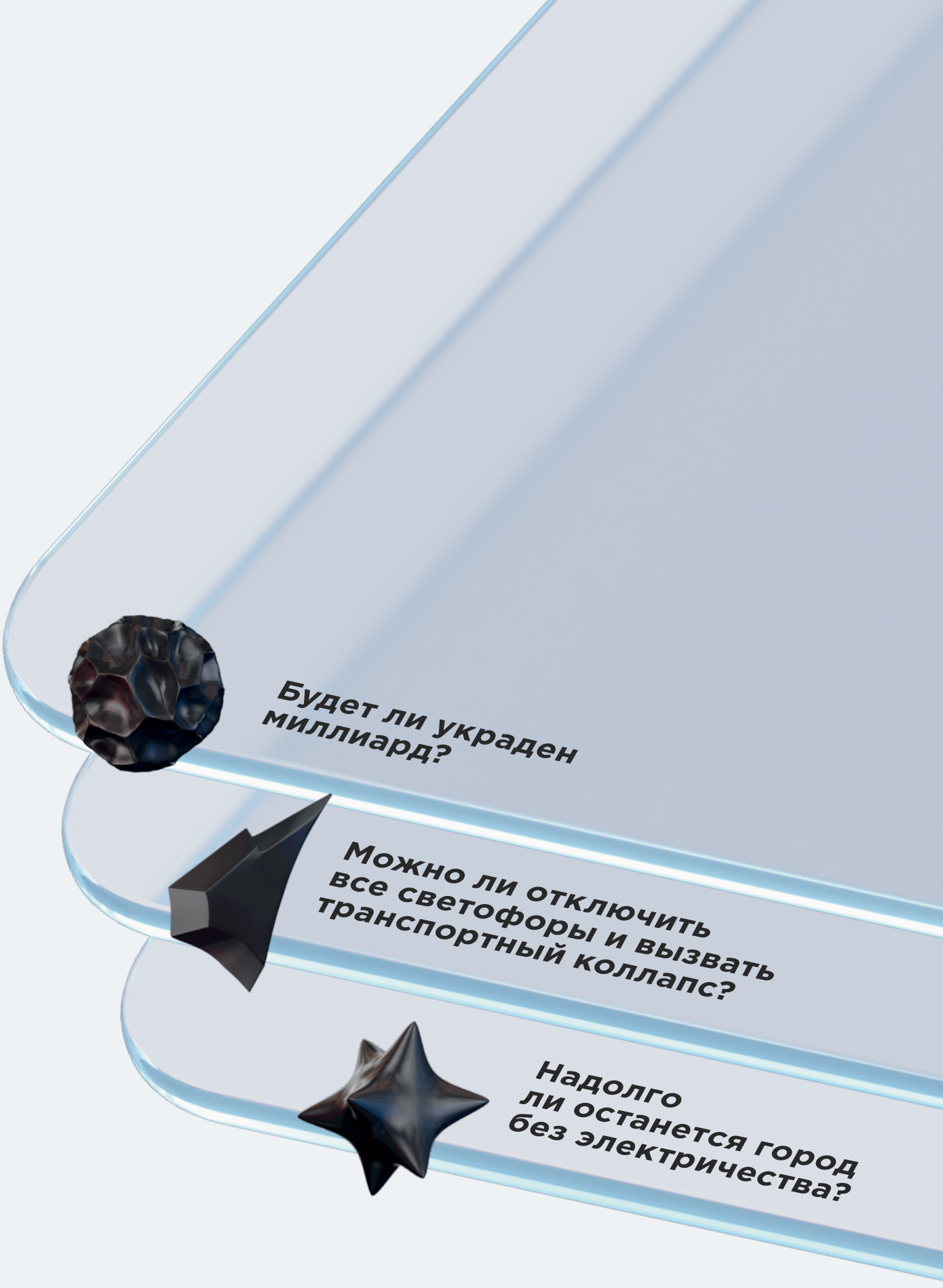
The Standoff — это уникальная возможность довести вектор атаки до конца и посмотреть, к чему это приведет

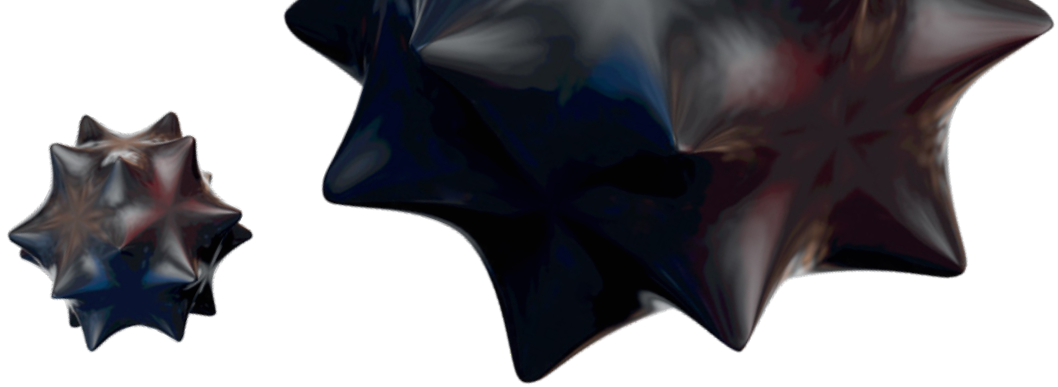
Создание киберполигонов — это дорогостоящая и трудозатратная задача, поэтому в основном ею занимаются на государственном уровне. К примеру, на построение национального киберполигона в США компании Lockheed Martin было выделено 33,9 млн долларов[8]. В России субсидию в размере 364,55 млн рублей получил «Ростелеком» для создания киберполигона в рамках программы «Цифровая экономика»[9]. А компания Positive Technologies, уже своими силами, организовала киберполигон, аккумулирующий опыт международных киберучений, которые компания в течение десяти лет проводила в рамках форума Positive Hack Days. За это время понимание концепции киберполигона в Positive Technologies неоднократно эволюционировало. Сначала до формата противостояния на искусственно смоделированной инфраструктуре, потом — до глобального киберполигона, The Standoff, на котором присутствуют инфраструктуры реальных организаций и реальные технологические и бизнес-процессы, реальные средства защиты и реальные защитники, отвечающие за безопасность этой инфраструктуры. Здесь нападающие не решают абстрактные задачи, они реализуют конкретные бизнес-риски, сформированные для развернутого прототипа конкретной организации.

С появлением The Standoff у сообщества появилась среда для моделирования кибератак, для оценки значимости ресурсов и проверки реализуемости рисков на цифровом макете мегаполиса. В инфраструктуру виртуального города заложены живые бизнес-сценарии нефтяной компании, ТЭЦ и подстанций, химического завода, аэропорта, банка, железной дороги, морского порта, а значит участники киберучений столкнутся с настоящим оборудованием и сервисами, используемыми в этих отраслях. The Standoff — это уникальная возможность довести вектор атаки до конца и посмотреть, к чему это приведет: будет ли украден миллиард и надолго ли останется город без электричества после выхода из строя турбины ТЭЦ. При проектировании The Standoff используются те же самые контроллеры, как на аналогичных объектах критически значимой инфраструктуры. Если атака будет успешной и электростанция остановится, значит, она остановилась бы и в реальной жизни.

8 

9 


Будет ли украден миллиард?
Можно ли отключить все светофоры и вызвать транспортный коллапс?
Надолго ли останется город без электричества?



сайт The Standoff

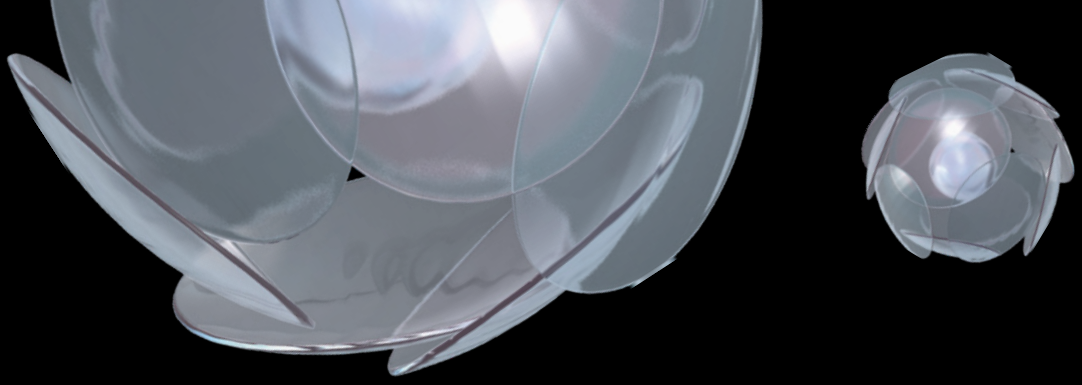
The Standoff 2020:

12–17 ноября

29 команд атакующих

6 команд защитников

13 инфраструктурных объектов города



Ольга Зиненко,
Яна Юракова

отдел аналитических исследований информационной безопасности Positive Technologies

на чтение
20 мин.

как это было

С 12 по 17 ноября прошли масштабные киберучения на полигоне The Standoff. В рамках соревнований боролись 29 команд атакующих и 6 команд защитников. Для этой масштабной кибербитвы был создан цифровой двойник целого города, в котором были представлены 13 объектов:

- парк развлечений, деловой центр и светофорная сеть — под управлением компании 25 Hours;
- аэропорт, железнодорожная станция и морской порт — под управлением Heavy Ship Logistics;
- нефтяное месторождение и нефтехимический завод — под управлением компании Nuft;
- банк — под управлением компании Bank of FF;
- телерадиокомпания, газораспределительная станция, трансформаторная подстанция — под управлением компании Tube;
- электростанция — под управлением Big Bro Group.

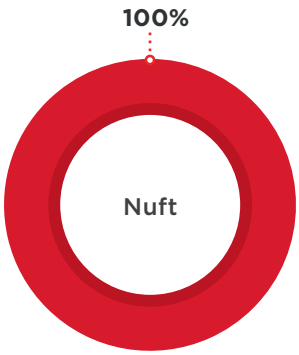
Основной задачей атакующих была реализация бизнес-рисков, актуальных для каждой из компаний, кроме того они могли искать уязвимости в инфраструктуре офисов и устанавливать майнеры, получая за это дополнительные баллы.

От команд защитников требовалось своевременно выявлять инциденты и обеспечивать доступность инфраструктурных объектов города.

Для обеих сторон эта кибербитва стала источником бесценного опыта. Команды атакующих познакомились с оборудованием и программами, используемыми в реальных компаниях, а защитники попрактиковались в быстром детектировании и расследовании инцидентов и увидели новые траектории развития атак вживую без реального ущерба для бизнеса и «боевой» инфраструктуры.

Условия на киберполигоне были максимально приближены к реальной жизни, например даже сетевое взаимодействие происходило по распространенным протоколам АСУ ТП:

- OPC DA,
- Modbus TCP,
- UMAS,
- IEC 60870-5-101,
- Siemens Simatic S7,
- Siemens DIGSI,
- Vnet/IP,
- CIP (Ethernet/IP),
- IEC 61850,
- BACnet/IP.



Что удалось сделать хакерам

В общей сложности атакующие реализовали 47% от общего числа заложенных рисков. Наибольшее число рисков было реализовано в отношении аэропорта, нефтяного месторождения и нефтехимического завода.

В ходе соревнований были обнаружены два новых уникальных бизнес-риска, которые не были предусмотрены организаторами. На киберполигоне можно не только верифицировать известные риски, но и выявлять новые, не определенные заранее.

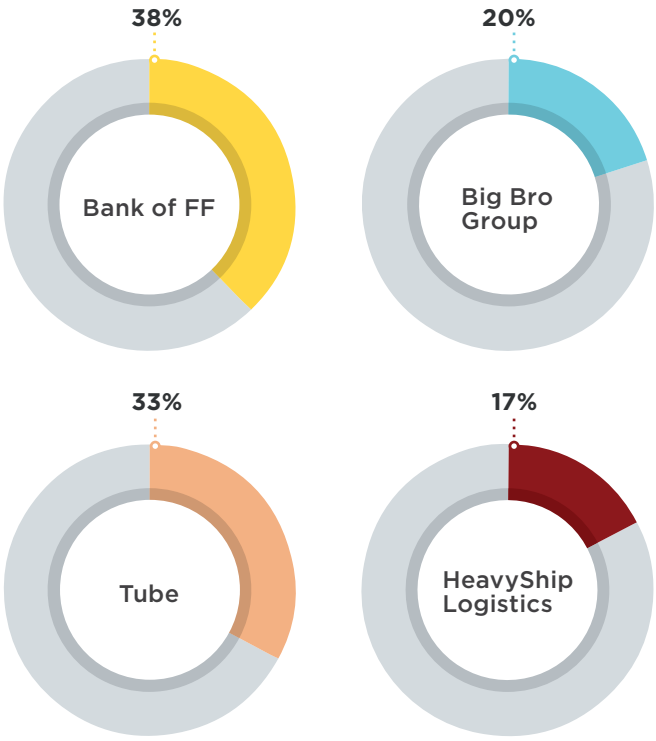
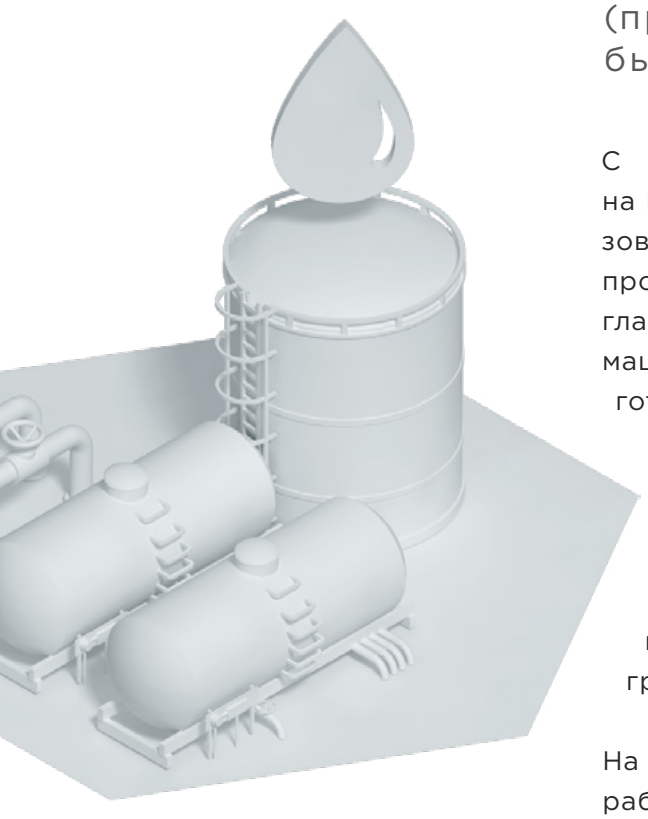


Рисунок 1. Доля реализованных бизнес-рисков

Рисунок 2. Последствия атак на The Standoff 2020 (указана доля реализованных рисков для каждой компании)

Техногенная катастрофа

60% промышленных компаний считают, что нарушение технологического (производственного) процесса может быть основной целью кибератак



С первых минут соревнований атакующие нацелились на инфраструктуру компании Nuft. Именно здесь был реализован первый риск в рамках кибербитвы: команда back2oaz проникла в сеть организации, получила доступ к компьютеру главы нефтяного департамента и похитила файлы с информацией о тендерах. В реальной жизни такая атака может готовиться неделями, а порой и годами, поскольку злоумышленники стараются действовать скрытно, чтобы собрать как можно больше полезной им информации.

Позднее атакующими был получен доступ к системе управления нефтехимическим заводом. Они закрыли входной клапан в холодильный контур, что привело к перегреву и нарушению процесса производства.

На нефтяном месторождении атакующие смогли остановить работу добывающего оборудования. Сразу две команды смогли получить доступ к системе управления хранилищами нефтепродуктов и нарушили процесс транспортировки нефти в хранилище, переполнив его. Позже работа контроллера, управляющего транспортировкой нефтепродуктов, была полностью остановлена. Такие инциденты могут привести к утечке нефти и загрязнению окружающей среды.

1

Отметим для примера, что для очистки акватории от 64 тыс. тонн мазута, попавших в море в результате разлома нефтяного танкера Prestige в 2002 году, были привлечены 300 000 добровольцев со всей Европы, а общий ущерб от катастрофы оценивается в 4 млрд евро[1]. Еще один пример: в 2000 году на ликвидацию аварии на нефтеперерабатывающем заводе Petrobras в Бразилии, в результате которой в реку вытекло порядка 1,3 млн литров нефти, компания потратила более 100 млн долларов[2].

2

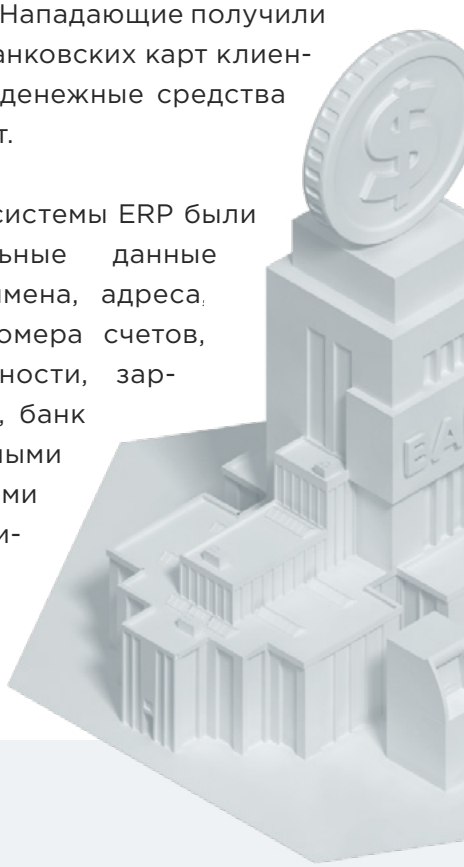
Ограбление банка

В 2020 году 71% атак в финансовой сфере был нацелен на кражу информации

Банк, построенный на киберполигоне, ничем не отличался от настоящего: в нем были эквайринг, система переводов, процессинговый центр. Виртуальные банковские системы выполняли стандартные операции с банковскими счетами и картами, позволяли клиентам расплачиваться в интернет-магазине, а также обеспечивали внутреннюю деятельность банка. Банк обрабатывал 236 счетов: у всех жителей и хакеров имелись виртуальные банковские карты (у жителей было по 10 тыс. рублей, у хакеров — по 1 тыс.). Кроме того, у каждой компании был свой расчетный счет, на котором лежал 1 млн рублей. Специальные боты обеспечивали регулярный трафик: они каждые 15 минут совершали транзакции, сумма которых варьировалась от 10 до 1000 рублей.

На третью ночь киберучений команда DeteAct смогла атаковать банк. Нападающие получили доступ к реквизитам банковских карт клиентов банка и перевели денежные средства с этих карт на свой счет.

Позже из внутренней системы ERP были похищены персональные данные сотрудников банка (имена, адреса, номера телефонов, номера счетов, информация о должности, зарплате). Таким образом, банк столкнулся с прямыми финансовыми потерями и утечкой конфиденциальных данных.



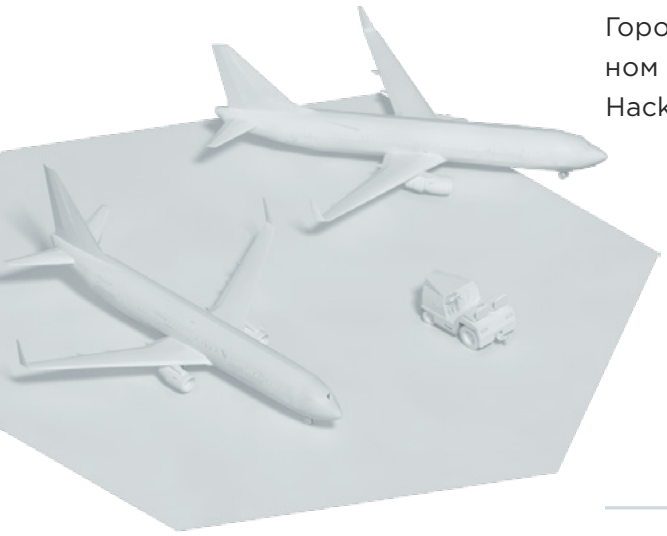
Кража информации в финансовой сфере в 2020 г.

25%	кража персональных данных
14%	кража учетных данных
11%	кража данных банковский карт

В 2020 году 71% атак в финансовой сфере был нацелен на кражу информации. Такие утечки грозят банку серьезным вниманием со стороны регуляторов и СМИ, как, например, в позапрошлогодней истории с базой данных 900 000 клиентов Альфа-Банка, Банка Хоум Кредит и ОТП Банка[3].

[3]

Продажи авиабилетов приостановлены

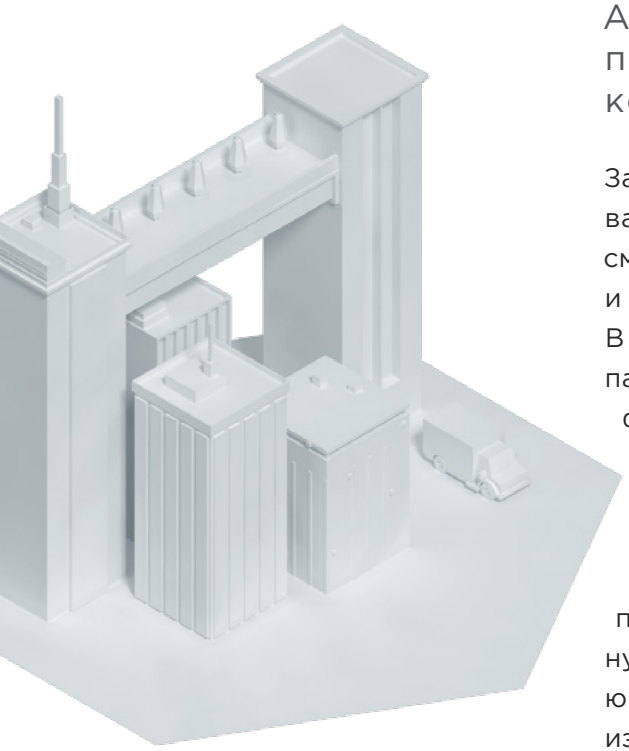


Горожане, напуганные авариями на химическом заводе и нефтяном месторождении, поспешили в аэропорт. Однако команда Hack.ERS реализовала бизнес-риск, связанный с утечкой персональных данных пассажиров аэропорта виртуального города FF. В этот же день из-за действий команды DeteAct произошел сбой системы продажи билетов и системы регистрации пассажиров в аэропорту. Жители города не могли купить билеты через сайт аэропорта, а те, кто приобрел билеты заранее, не могли пройти процедуру регистрации на рейс.

Кража документов из государственной компании

64% атак на госучреждения в 2020 году были реализованы с помощью ВПО

Атакующие удаленно выполняли код при реализации 73% киберрисков компании 25 Hours

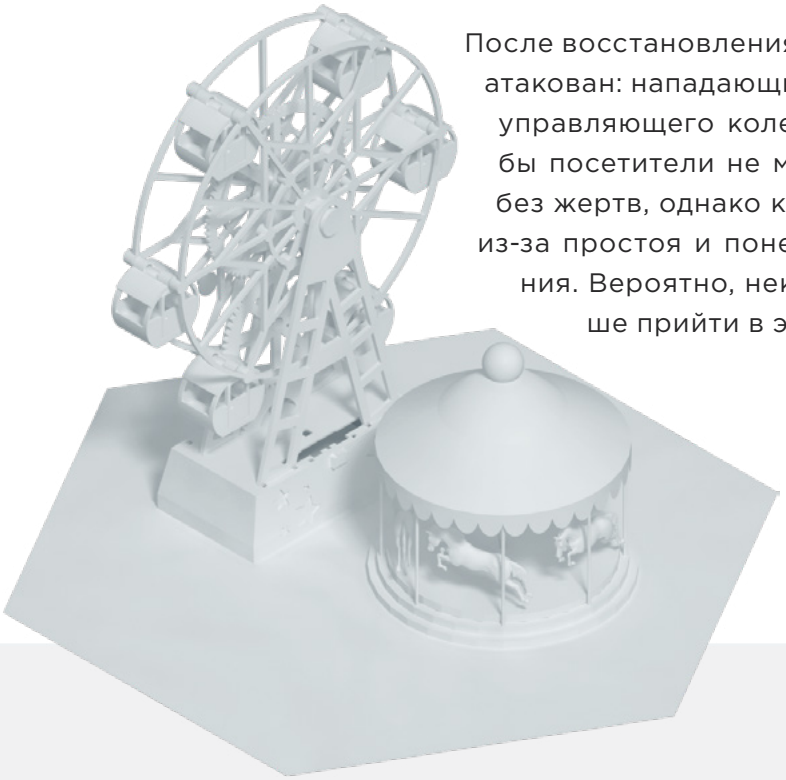


За первую ночь кибербитвы деловой центр города был атакован дважды. Две команды атакующих с разницей в пару часов смогли получить доступ к базе данных городского портала и удалить информацию о штрафах и задолженностях граждан. В ходе этого инцидента злоумышленники проникли в сеть компании через уязвимость в веб-приложении, загрузив вместо фотографии в личном профиле вредоносный файл.

Позже нападающие похитили персональные данные сотрудников, получили доступ к зашифрованному хранилищу директора и украли важные документы. Теперь они могли передать конкурентам или публично раскрыть конфиденциальную информацию. А в последние минуты соревнований атакующие получили доступ к системе кондиционирования и смогли изменять температуру воздуха в офисных зданиях.

Поломка аттракциона

В парке развлечений компании 25 Hours были реализованы не только все бизнес-риски, но и обнаружен новый, не предусмотренный в условиях соревнований. Атакующие выполнили свою детскую мечту — бесплатно получили билеты на аттракционы и могли раздать их всем желающим. Возможно, именно в этом и был злой умысел нападающих — собрать как можно больше посетителей в парке, а затем нанести удар. Они получили доступ к системе управления аттракционом «Колесо обозрения». Участники команды back2oaz смогли повысить скорость вращения колеса так, чтобы оно сорвалось с опор и рухнуло на землю. Сложно даже представить сколько жертв это могло бы повлечь в реальности!..



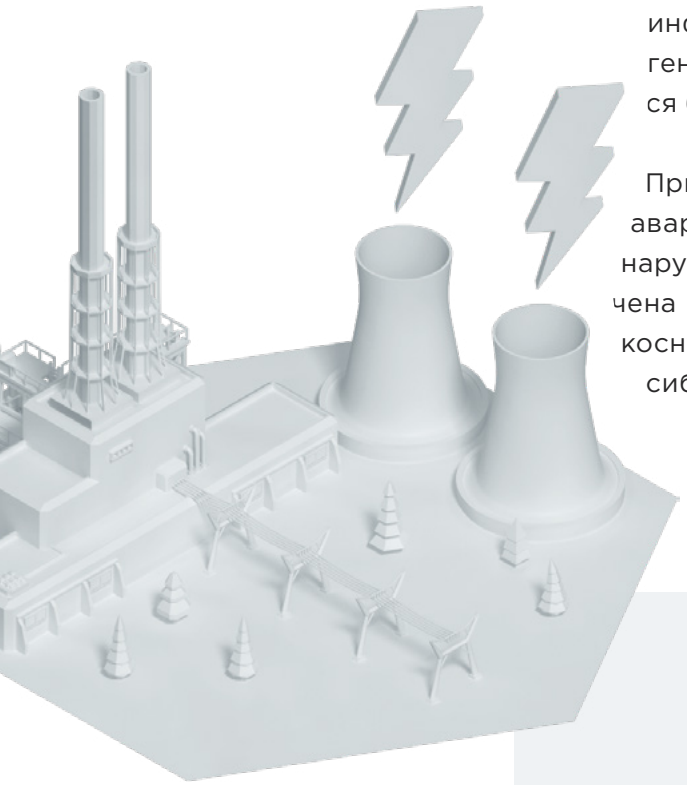
После восстановления работы аттракциона он вновь был атакован: нападающие остановили работу контроллера, управляющего колесом, и отключили освещение, чтобы посетители не могли покинуть кабинки. Обошлось без жертв, однако компания не получит часть прибыли из-за простоя и понесет затраты на ремонт оборудования. Вероятно, некоторые горожане не рискнут больше прийти в этот парк.

Участники команды back2oaz смогли повысить скорость вращения колеса так, чтобы оно сорвалось с опор и рухнуло на землю

Энергетика под угрозой

Как и в реальной жизни, большинство атак злоумышленники проводили ночью, стараясь незаметно прокрасться в инфраструктуру жертвы

В последнюю ночь противостояния была атакована компания Big Bro Group, обеспечивающая город электричеством. Нападающие получили доступ к базе данных ERP и похитили информацию о сотрудниках компании. К счастью, процесс генерации электричества не был нарушен и город не остался без света.



Пример остановки процесса генерации электричества — авария на Саяно-Шушенской ГЭС в 2009 году. Тогда было нарушено энергоснабжение сибирских регионов, ограничена подача электроэнергии в Томске, веерные отключения коснулись ряда промышленных предприятий, в том числе сибирских алюминиевых заводов. В результате аварии погибли 75 человек, 13 пострадали. Ущерб от аварии превысил 7,3 млрд рублей, включая ущерб экологии[4].

4

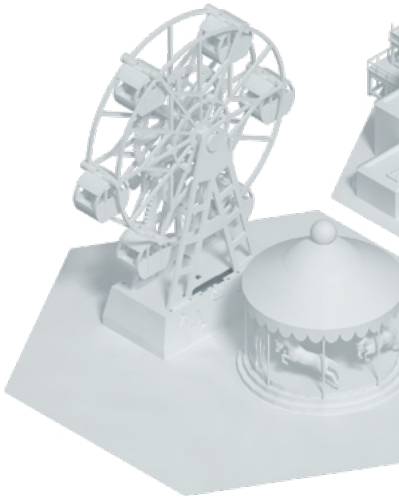
Запрещенная трансляция

Компания Tube, которая занимается телерадиовещанием, многократно подвергалась атакам киберпреступников. Нападающие получали доступ к системе управления рекламными экранами в городе и запускали трансляцию собственных материалов.

Реализовать подобную атаку оказалось возможным даже без знаний пароля, воспользовавшись уязвимостью стриминг-платформы. Хакеры сбросили пароль администратора и заменили его своим, а затем загрузили собственное видео, которое транслировалось по всему городу.

В жизни подобная подмена контента, во-первых, вызовет финансовые потери из-за нарушения договоренностей с рекламодателями, а во-вторых — может вызвать недовольство местных жителей и даже судебные иски в случае, если транслироваться будут запрещенные материалы, например пропагандирующие насилие.

Как работали защитники

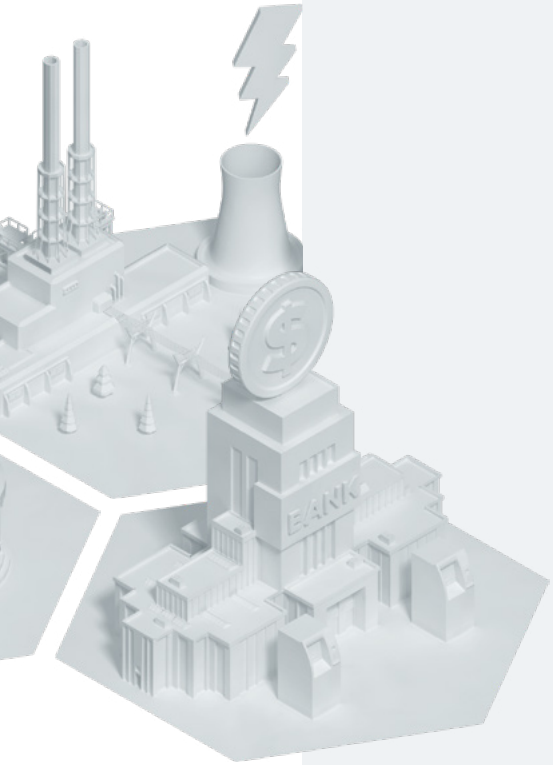


Защитники фиксировали все инциденты и по мере сбора информации расследовали атаки, которые приводили к реализации рисков. В среднем защитники фиксировали по 35 инцидентов в день[5]. Всего было выявлено 213 инцидентов, каждый пятый из них свидетельствовал о получении первоначального доступа, примерно четверть была связана с исполнением вредоносного кода.

В среднем на одно расследование и полный сбор необходимых сведений командам требовалось 11 часов 50 минут. Больше суток ушло на расследование утечки персональных данных авиапассажиров и сбоев в работе онлайн-касс в парке развлечений. Часть рисков так и не была расследована за отведенное на соревнованиях время. Сложности в работу защитников добавляло то, что несколько атакующих могли одновременно использовать схожие техники и требовалось определить цепочку действий для каждой команды хакеров.

В ходе сражений защитники столкнулись на практике со множеством техник из матрицы MITRE ATT&CK. В основном применялись техники living off the land, представляющие собой использование уже имеющихся в системе инструментов во вредоносных целях, например запуск скриптов PowerShell, создание задач в системном планировщике. Аналогичным образом действует и множество APT-группировок.

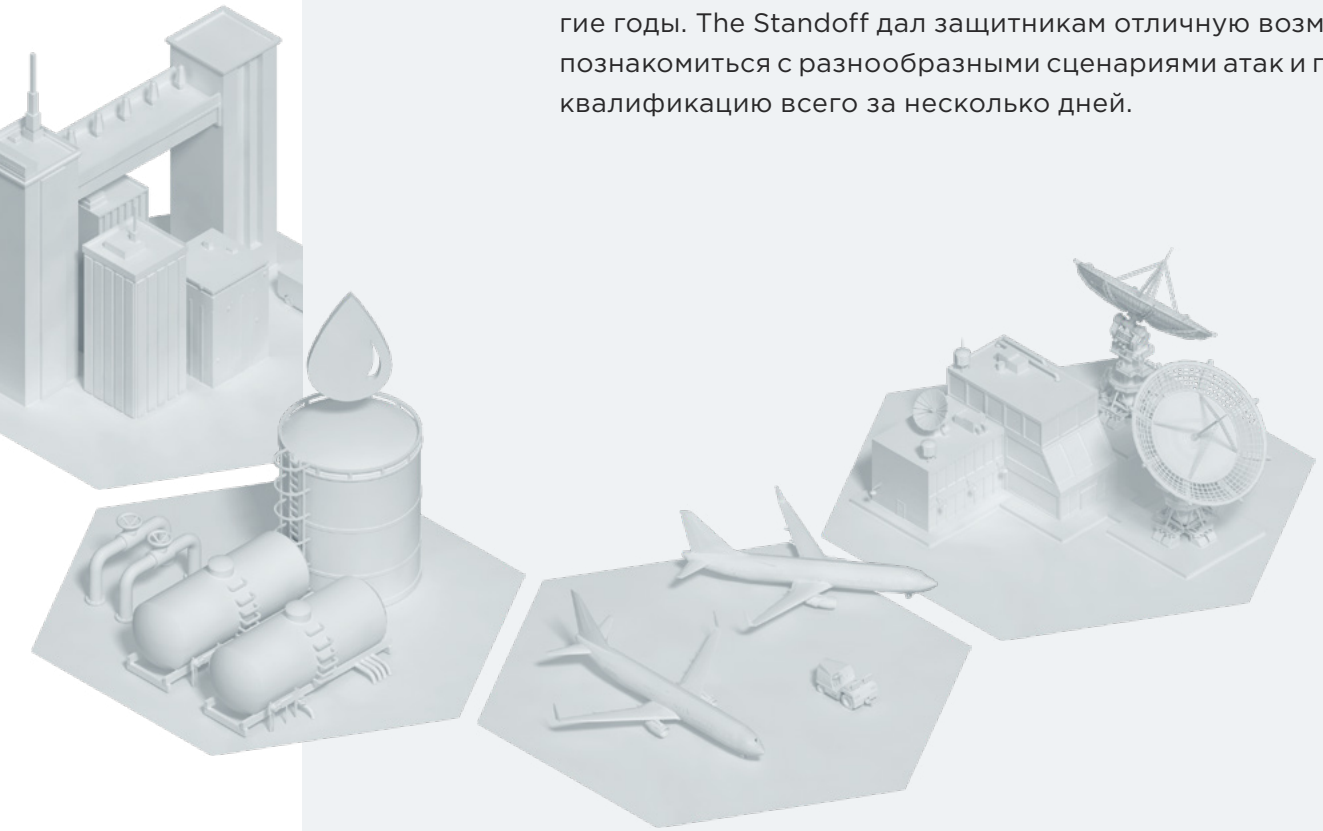
5 Для сравнения, внутренняя служба реагирования на инциденты в Cisco обрабатывает в среднем 22 инцидента ежедневно.



Как трактовать результаты

Стоит отметить, что не все команды хакеров смогли довести атаки до реализации бизнес-рисков — несмотря на то, что многие из них нашли уязвимости на сетевом периметре компаний. Аналогично и во время тестирования на проникновение не каждая команда пентестеров сможет смоделировать сложную многоступенчатую атаку, которая приведет к реализации риска. Кроме того, ряд рисков невозможно подтвердить в рамках пентеста, поскольку они могут, помимо угрозы для бизнес-процессов, представлять угрозу для окружающей среды, для жизни и здоровья людей. Яркий пример — инцидент с переполнением нефтяного хранилища.

Подобные киберучения — это, помимо прочего, тренинг для сотрудников любого отдела информационной безопасности, ведь в реальной своей работе они могут не столкнуться с таким большим количеством киберинцидентов даже за многие годы. The Standoff дал защитникам отличную возможность познакомиться с разнообразными сценариями атак и повысить квалификацию всего за несколько дней.



Глобальный SOC на The Standoff 2020: всевидящее око

Павел Кузнецов,

Заместитель управляющего директора по технологиям кибербезопасности

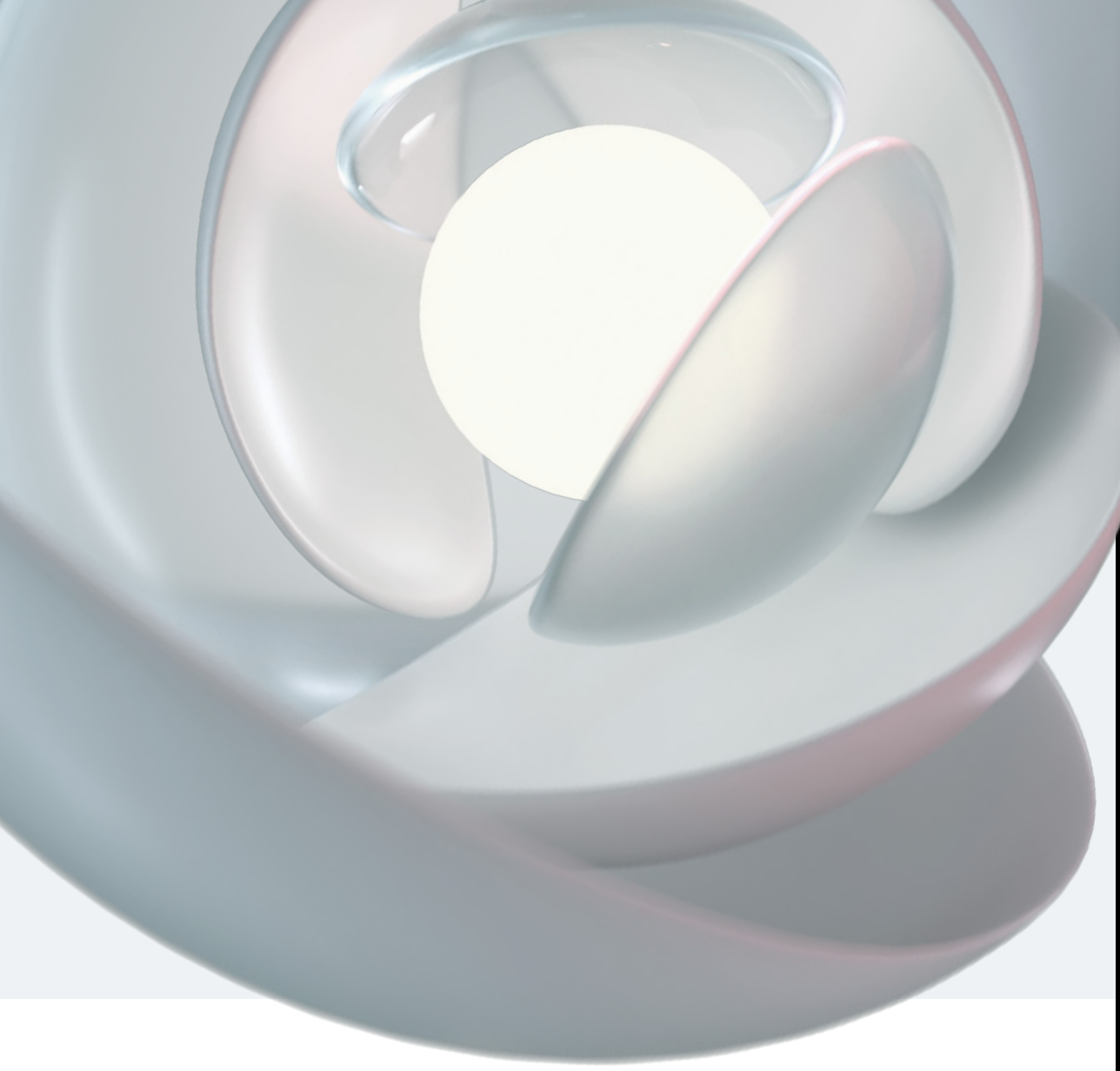
на чтение
20 мин.

Сотрудники экспертного центра безопасности Positive Technologies участвуют в противостоянии The Standoff уже несколько лет — с 2018 го, когда оно было частью Positive Hack Days. В первый год мы следили за игровыми трендами и событиями, используя MaxPatrol SIEM, решение для анализа сетевого трафика PT Network Attack Discovery и многоуровневую систему выявления и блокировки вредоносного контента PT MultiScanner[1]. Наша задача состояла в том, чтобы изучить активность участников, отследить тактики и инструментарий, ими используемый, и, конечно же, поработать со своими продуктами при повышенной нагрузке. Во время подобных мероприятий наши инструменты используются на полную мощность (и даже еще немного больше): в 2018 году мы двое суток следили за 12 командами, MaxPatrol SIEM обрабатывал в среднем 20 000 EPS, PT NAD проанализировал более 3 ТБ сетевого трафика, а наша команда определяла успешные атаки, искала следы компрометации (веб-шеллы, удаленные консоли, авторизацию на узлах и проч.), а накопленные знания в дальнейшем в числе прочего легли в основу обновлений наших продуктов.

Год спустя мы увеличили количество «глаз» нашего SOC на The Standoff в рамках очередного PHDays:

1

2



к предыдущим трем добавились еще PT Application Firewall и PT Industrial Security Incident Manager[2]. Это позволило нам получить максимально полную картину противостояния во всех элементах инфраструктуры цифрового мегаполиса. Все длилось также двое суток, но следили мы за бóльшим числом участников (в тот году было уже 18 команд атакующих, шесть команд защитников и три команды SOC), которые вели очень активную деятельность в городской инфраструктуре. В отличие от команд, мы не вмешивались в события на площадке соревнований, а только лишь наблюдали за ними . Ключевая наша задача состояла в том, чтобы продемонстрировать на практике эффективность современных систем для выявления и расследования киберинцидентов. Ну и конечно же — изучить те тактики и техники, которыми пользовались участники, в режиме реального времени, поскольку на The Standoff команды атакующих традиционно используют самые актуальные средства и приемы.

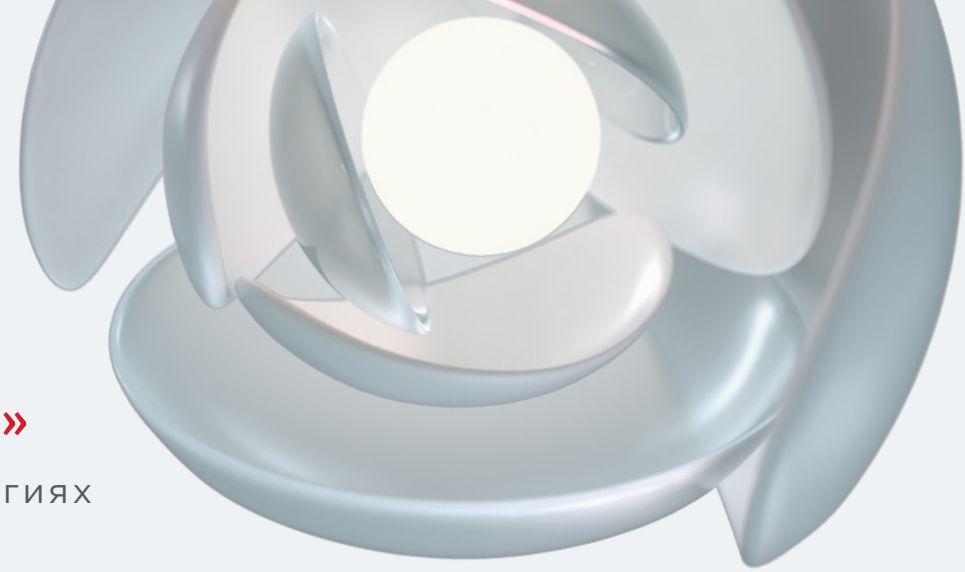
Поэтому, с одной стороны, в преддверии The Standoff в 2020 году наши задачи, цели и планы нам были ясны — не первый раз, как говорится. Однако масштаб мероприятия наложил-таки свой отпечаток на нашу работу.

Purple teaming как он есть

В этом году команда нашего SOC включала специалистов, которые отвечали за непрерывный мониторинг и поддержание процесса threat hunting в наблюдаемом виртуальном окружении, передачу информации работающим посменно аналитикам, составлявшим общую картину происходящего, с помощью которой возможно было строить kill chains реализации конкретных угроз и рисков. Также мы включили в команду экспертов со специфическими навыками: например, в области АСУ ТП, анализа вредоносного кода, написания детектов для выявления действий хакеров в инфраструктуре. Такой состав команды позволяет максимально полно оценивать происходящее, обнаруживать, классифицировать и исследовать вплоть до мельчайших технических деталей все векторы атак в контексте конкретных киберрисков.

В ходе всего мероприятия наши специалисты в режиме 24/7 отслеживали события безопасности, происходившие в развернутой инфраструктуре виртуального города (который, однако, имел и физическое воплощение в виде масштабного макета). Иными словами — наблюдали за действиями команд атакующих, red teams. А затем на основе полученной информации оценивали качество, полноту и справедливость представленных атакующими отчетов о выполнении того или иного игрового задания. Результатом этой постоянной работы стала полная хронология происходящего, которая затем использовалась жюри как некий базовый справочник, а также чтобы своевременно предоставлять информацию профессиональному сообществу, наблюдавшему за происходящим на портале The Standoff. Примерно таким же образом осуществлялась оценка полноты сведений, представленных командами защитников, blue teams, уже в их собственных отчетах о зафиксированных инцидентах.

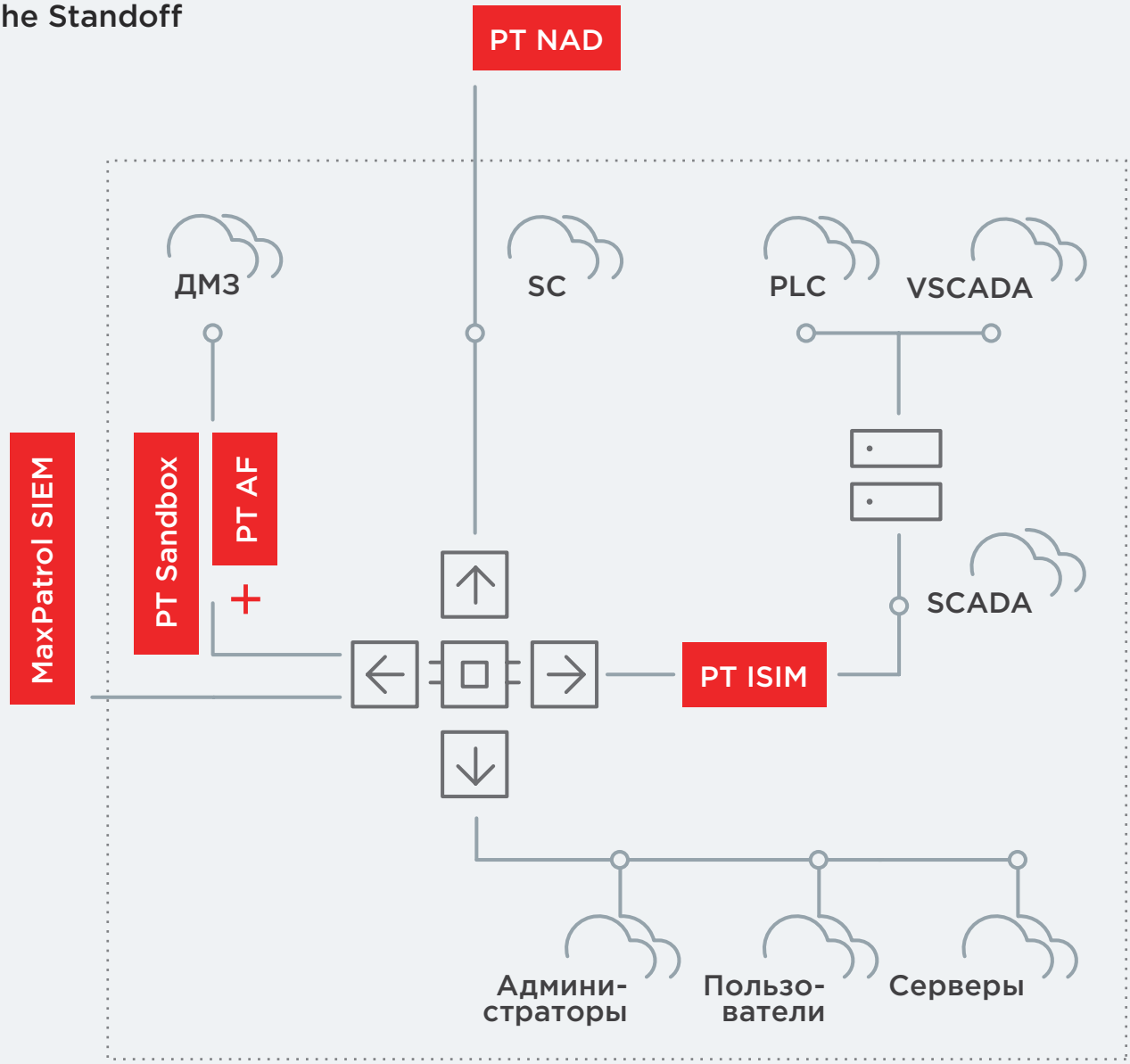
В этот раз мы включили в команду экспертов со специфическими навыками



Инструментарий «всевидящего ока»

Итак, на каких технологиях работал наш SOC?

Инфраструктура одного из офисов, созданных для The Standoff

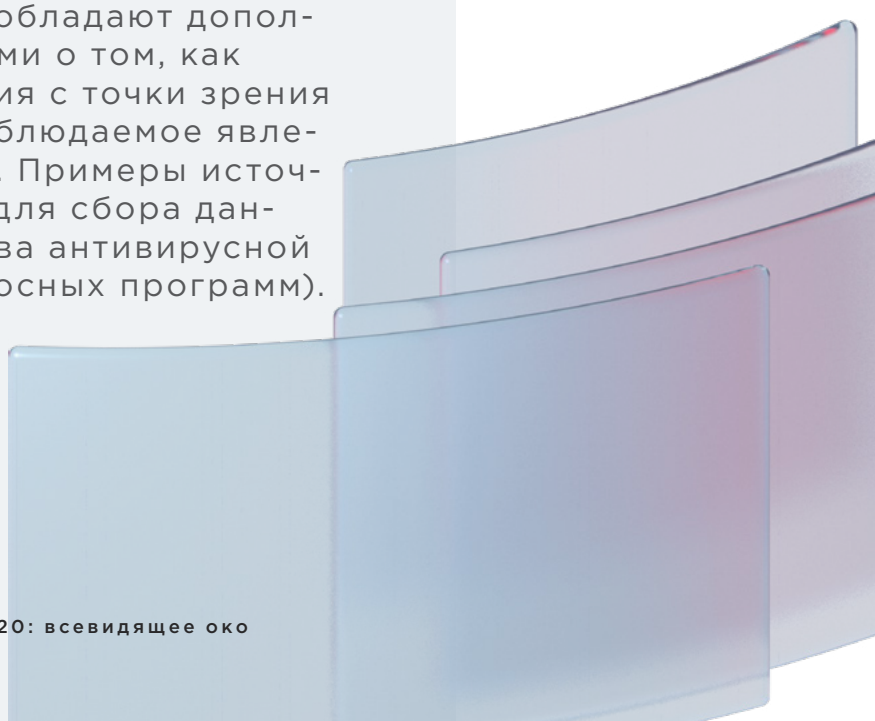


Защита периметровых сервисов (сервисов так называемой демилитаризованной зоны) и мониторинг атак на них были построены на базе PT Application Firewall. Сердцем нашего SOC стала система MaxPatrol SIEM.

SIEM-системы традиционно применяются для сбора, хранения и оперативной обработки данных особытиях безопасности. Однако область применения этим не ограничивается: с помощью SIEM-систем решаются такие важные задачи, как выявление и расследование инцидентов ИБ, инвентаризация активов, контроль защищенности информационных ресурсов.

Поиск инцидентов начинается с подключения источников, которые генерируют разнородные события. Для получения наиболее полного представления о том, что происходит в инфраструктуре компании, рекомендуется подключать все имеющиеся источники IT-событий и событий ИБ.

Источники событий ИБ — специализированное программное и аппаратное обеспечение для информационной безопасности, порождающее события ИБ. Такие источники обладают дополнительными внешними знаниями о том, как трактовать те или иные события с точки зрения безопасности (является ли наблюдаемое явление «хорошим» или «плохим»). Примеры источников событий ИБ — IDS/IPS (для сбора данных о сетевых атаках), средства антивирусной защиты (обнаружение вредоносных программ).



К SIEM-системе в качестве источников событий были подключены почти все узлы информационной инфраструктуры нашего виртуального города. Почему «почти все»? Потому что в сетевых сегментах АСУ ТП мы, по понятным причинам, в большей степени полагались на систему PT Industrial Security Incident Manager. Своеобразным швейцарским ножом специалиста нашего глобального SOC стал PT Network Attack Discovery, в комбинации с MaxPatrol SIEM позволяющий проводить глубокий анализ сетевого трафика и выявлять в нем аномалии и вредоносные воздействия как автоматически, так и при непосредственном участии эксперта. Ну и, last but not least, оперативно выявлять атаки, связанные с применением социальной инженерии, в том числе фишинга, и проводить их анализ позволила система PT Sandbox, песочница с возможностью кастомизации виртуальных сред. Благодаря PT Sandbox у нас появилась возможность с большей эффективностью выявлять атаки, в ходе которых red teams применяли вредоносное программное обеспечение.

В данном контексте под атакой подразумевается любая зафиксированная нами попытка нелегитимного воздействия на находящиеся под наблюдением системы для достижения определенных целей, например для получения информации о подсети или доступа с возможностью выполнения команд ОС на конкретном узле. Но в тот момент, когда полученные данные позволяли нам судить о том, что атака оказалась успешной, уже уместно было применять термин «инцидент». По зафиксированным же инцидентам впоследствии строились цепочки реализации рисков. Кроме того, в ходе расследования цепочек проводилась привязка атомарных инцидентов к активности различных команд атакующих (атрибуция), в том числе с применением экспериментальных модулей профилирования сетевого поведения.

47% киберрисков
были реализованы
командами атакующих
в виртуальном городе

В ходе подготовки такого мероприятия мы и наши коллеги, отвечавшие непосредственно за инфраструктуру, разумеется, столкнулись с определенными сложностями. Необходимо было «подружить» между собой огромное количество различных технических решений, имитирующих реальные бизнес-процессы виртуального города, скоммутировать подсети, добиться устойчивой работы всех систем. А уже нам как специалистам SOC критически важно было добиться на 100% чистой и стабильной видимости всего, что происходило на полигоне, и при этом снятием, например, сетевого трафика не мешать работающим процессам ни в корпоративных, ни в технологических сетях — а также, конечно, ничего не упустить. Ради этого на проект еще на этапе строительства инфраструктуры со стороны SOC были выделены два архитектора мониторинга, каждый из которых кропотливо, с привлечением профильных специалистов по обнаружению атак на узлах и в сети, проверял сетевую доступность, видимость сетевого трафика во всех сегментах инфраструктуры, фактическую видимость запросов к веб-приложениям в PT AF.

Мы подготовили набор решающих правил для MaxPatrol SIEM, сигнатур для PT ISIM и PT NAD, в том числе экспериментальных, требовавших обкатки как раз в условиях, максимально приближенных к реальным.

Мониторинг в действии

Наши предварительные ожидания — что в первые дни противостояния команды атакующих будут в основном заниматься разведкой и только готовиться к серьезным действиям — не оправдались. Red teams пошли в бой с первой минуты после старта мероприятия и сохраняли такой напор практически на всем его протяжении. Количество выявленных нашим SOC событий безопасности, которые можно было квалифицировать как инциденты, перевалило за сотню уже к наступлению первой же ночи, и заданный темп впоследствии не снижался, а в последние дни, когда командам особенно важно было стало добрать очков с помощью реализации дополнительных рисков, даже возрос.

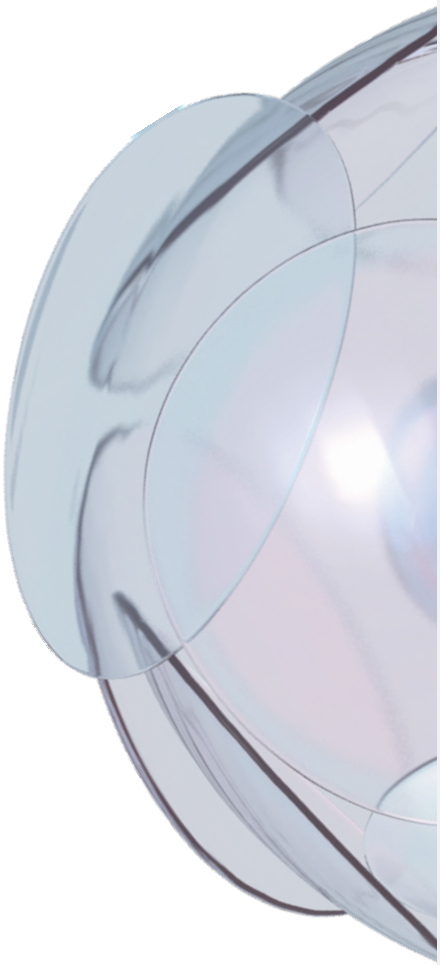
К концу противостояния команды защитников смогли объединить в цепочки и зафиксировать более 200 инцидентов

К концу противостояния команды защитников смогли объединить в цепочки и зафиксировать более 200 инцидентов (некоторые из них включали инциденты, которые наш глобальный SOC фиксировал как атомарные, в рамках одного сообщения об инциденте) и провести 21 расследование

Что интересно, на расследование отдельных инцидентов у команд защитников иногда уходили считаные минуты, но вот среднее время полноценного расследования составило порядка 11 часов. Команды атакующих реализовали 47% всех киберрисков виртуального города, заложенных в инфраструктуру полигона, — от падения колеса обозрения в парке аттракционов до хищения персональных данных пассажиров авиакомпании.

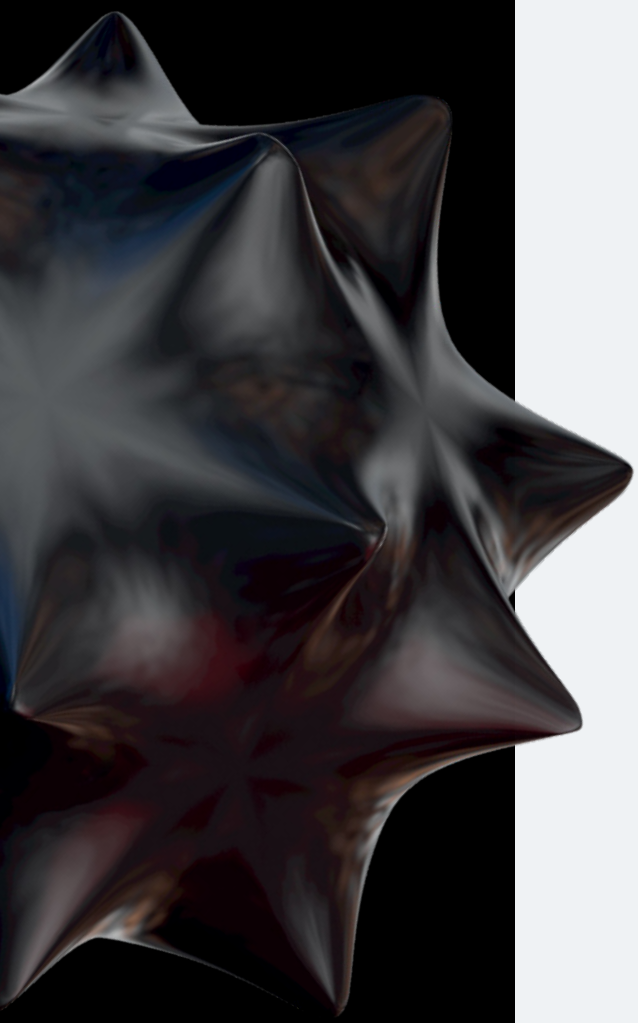
Пока мы отслеживали происходящее на поле боя, выяснилось несколько любопытных моментов. К примеру, команды защитников часто выявляли действия атакующих уже на этапе разведки на конкретном узле или в начале попыток перемещения в сети офиса, но пропускали первичный вектор проникновения, такой как брутфорс с попытками входов, грамотно разнесенными по времени. А наш SOC смог выявить такие инциденты с помощью профилирования поведения пользователей и решающих правил, в которые была заложена логика, учитывающая техники обхода средств защиты, основанные на временных задержках. Кроме того, разработанные нами правила корреляции позволили нашим специалистам определить отдельные действия атакующих в офисах как инциденты ИБ, связав их с первоначальной компрометацией узлов и учетных записей. Подобные действия при отдельном рассмотрении выглядят легитимными, и здесь помогало именно выстраивание цепочки от точек первичного проникновения. Таким же образом нашему SOC удавалось выделять нелегитимные запуски различных утилит, в том числе предназначенных для разведки на узлах и в сети, а также получение доступа к файлам. С помощью нашего решения для глубокого анализа трафика и песочницы мы выявляли успешные попытки фишинговых атак. И безусловно, нашим преимуществом в данном случае стало то, что мы включили в процесс мониторинга экспертов по анализу сетевого трафика. Хочется отдельно подчеркнуть важную при непрерывном мониторинге роль оперативной доработки решающих правил (как минимум — дополнение связанных табличных списков), на которых основываются решения о легитимности выявляемых событий. Именно такие гибкие контроли позволили нам «ловить» атакующих на определенных шагах и далее отслеживать всю их активность. Этот подход доказал свою эффективность и в конечном счете обеспечил нам ряд преимуществ перед играющими командами защитников.

В рамках подобных масштабных киберучений производители прикладного ПО и аппаратуры получают отличную возможность проверить свои продукты на прочность под реальным натиском профессионалов из offensive security



Кому и зачем показан The Standoff

Выводы по итогам The Standoff каждый может сделать для себя сам. Лично для меня мероприятие стало отличным подтверждением того, что сообщество специалистов по информационной безопасности в наше время должно двигаться в сторону постоянного взаимодействия и сотрудничества. Например, в рамках подобных масштабных киберучений производители прикладного ПО и аппаратуры получают отличную возможность проверить свои продукты на прочность под реальным натиском профессионалов из offensive security. Вендоры, сервис-провайдеры и интеграторы в области информационной безопасности — опять же проверить в деле свои продукты и свои команды специалистов, взявшись за защиту какого-то из объектов инфраструктуры. По итогам мероприятия все участники получают новые технические данные о продуктах, уязвимостях, о методах и средствах



С расследованиями экспертного центра безопасности Positive Technologies можно ознакомиться в блоге

проведения, выявления и предотвращения последствий компьютерных атак — и могут, безусловно, впоследствии применить новый опыт для укрепления безопасности любого реального объекта, а значит помочь нам всем сделать еще один шаг в безопасное будущее.

По итогам The Standoff всей команде PT ESC удалось проверить свои возможности по организации полноценного мониторинга информационной безопасности на действительно сложной инфраструктуре, собрать данные для дальнейшего обучения наших решающих модулей, а также отработать взаимодействие непосредственно SOC с другими подразделениями. Противостояние стало для нас, среди прочего, поводом взглянуть на процессную сторону такого взаимодействия под новым углом.

Авторы статей

Николай Анисеня

Руководитель группы исследований безопасности мобильных приложений

Александр Антипов

Главный редактор портала SecurityLab.ru

Евгений Гнедин

Руководитель отдела аналитики информационной безопасности

Дмитрий Даренский

Руководитель практики промышленной кибербезопасности

Марк Ермолов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений

Ольга Зиненко

Старший аналитик информационной безопасности

Екатерина Килюшева

Руководитель исследовательской группы отдела аналитики информационной безопасности

Максим Костиков

Руководитель группы исследований безопасности банковских систем

Дмитрий Кузнецов

Директор по методологии и стандартизации

Павел Кузнецов

Заместитель управляющего директора по технологиям кибербезопасности

Александр Морозов

Руководитель отдела тестирования на проникновение

Александра Мурзина

Ведущий специалист группы перспективных технологий отдела исследований по защите приложений

Алексей Новиков

Директор экспертного центра безопасности

Павел Новиков

Руководитель группы исследований безопасности телекоммуника-ционных систем

Александр Попов

Ведущий специалист отдела исследований безопасности ОС и аппаратных решений

Борис Симис

Заместитель генерального директора по развитию бизнеса

Вадим Соловьев

Старший аналитик информационной безопасности

Яна Юракова

Аналитик информационной безопасности

Над журналом работали

Главный редактор Наталья Фролова
Литературный редактор Алексей Чернозубов
Дизайнер-верстальщик Яна Аксакова
3D-иллюстратор Тимофей Литовченко

О компании

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, 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».

ptsecurity.com

standoff365.com

phdays.ru

Positive Technologies

PHDays

Positive Technologies

PHDays

PT SWARM

Positive Technologies

PHDays

t.me/positive_investing

Positive Research 2021