



Актуальные киберугрозы

Итоги 2020 года

Содержание

Резюме	3
Рост числа атак на фоне пандемии	4
Подводные камни удаленной работы	7
Вредоносное ПО развивает техники сокрытия	9
Атаки вымогателей: потери на миллионы долларов	10
Тщательный выбор жертв	10
Кража данных и требование двойного выкупа	11
Новые способы влияния	11
Непомерные запросы	11
Простой сервисов и затраты на восстановление	12
Атаки по цепочке: удар по репутации и обвал акций	12
Медицина: первые жертвы среди населения и возврат к бумажным документам	13
Промышленность: реализация рисков на критически важных объектах	15
Об исследовании	17

Резюме

Итоги 2020 года:

- Количество уникальных киберинцидентов в 2020 году выросло на 51% по сравнению с 2019 годом. Семь из десяти атак носили целенаправленный характер. Наиболее интересные отрасли, по мнению злоумышленников, — это государственные и медицинские учреждения, промышленные предприятия.
- Общая тенденция: растет значимость хакинга в атаках на организации. По результатам 2020 года доля этого метода составляет 24% (на 10 процентных пунктов больше, чем в 2019 году). В дарквебе отмечены рост рынков по продаже доступов в компании и повышенный интерес к теме взлома сайтов. Мы связываем это с массовым переходом организаций в онлайн-формат работы.
- Атак с использованием вредоносного ПО с каждым годом становится все больше и больше. В 2020 году количество таких атак увеличилось на 54% относительно прошлогоднего показателя. Разработчики ВПО уделяли много внимания методам сокрытия деструктивного воздействия и совершенствовали способы доставки, переключились на использование уязвимостей на сетевом периметре. Частных лиц в основном атаковали с помощью шпионского ПО и банковских троянов, а организации чаще становились жертвами программ-вымогателей.
- Тренд 2020 года в атаках на организации — применение шифровальщиков, их доля среди ВПО составила 45%. Операторы программ-вымогателей перешли от массовых атак к целенаправленному выбору жертв, увеличили суммы выкупа, открыли новые сайты по продаже украденной информации и начали использовать DDoS-атаки для шантажа жертв.
- Количество инцидентов на промышленных предприятиях увеличилось на 91% по сравнению с 2019 годом. Основное ВПО, применяемое в атаках на эту отрасль, — шифровальщики. Доля хакинга относительно показателя 2019 года выросла в 2,6 раза. Зафиксированы атаки на объекты критически значимой инфраструктуры, приводившие к отключению электроэнергии, а также попытки атак на системы водоснабжения.
- Медучреждения занимают первое место по числу атак с применением шифровальщиков и третье место в общем рейтинге по количеству атак за год. Из-за действий хакеров медицинские системы оказывались недоступны, больницам даже приходилось отказывать пациентам в оказании неотложной помощи.
- Год запомнился атаками, связанными с компрометацией цепочки поставок (supply chain attacks). Наиболее громкие инциденты произошли с компаниями Blackbaud и SolarWinds. В результате этих атак Blackbaud назначен ответчиком по 23 групповым искам от пострадавших клиентов, а акции SolarWinds упали в цене.

Для защиты от кибератак мы, прежде всего, советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. В свете последних сообщений об атаках, направленных на эксплуатацию уязвимостей IT-инфраструктуры компаний, настоятельно рекомендуем обратить особое внимание на защиту сетевого периметра, в том числе своевременно устанавливать обновления, и выстроить автоматизированный процесс управления уязвимостями. Помимо этого, следует использовать современные средства защиты, включая web application firewalls, средства анализа сетевого трафика, SIEM-системы. Для предотвращения атак, связанных с доставкой вредоносных программ по электронной почте, необходимо проверять вложения в песочнице — специальной виртуальной среде, предназначенной для поведенческого анализа файлов. Чтобы построить максимально эффективную систему защиты, нужно руководствоваться принципами риск-ориентированного подхода и проверять возможность реализации конкретных рисков, недопустимых для бизнеса. Оптимальное решение — проверка рисков на киберполигоне, где есть возможность смоделировать атаки без ущерба для реальной инфраструктуры.

Рост числа атак на фоне пандемии

Количество инцидентов в 2020 году увеличилось на 51% по сравнению с 2019 годом; 86% всех атак были направлены на организации. Больше всего злоумышленников интересовали государственные и медицинские учреждения, а также промышленные компании.

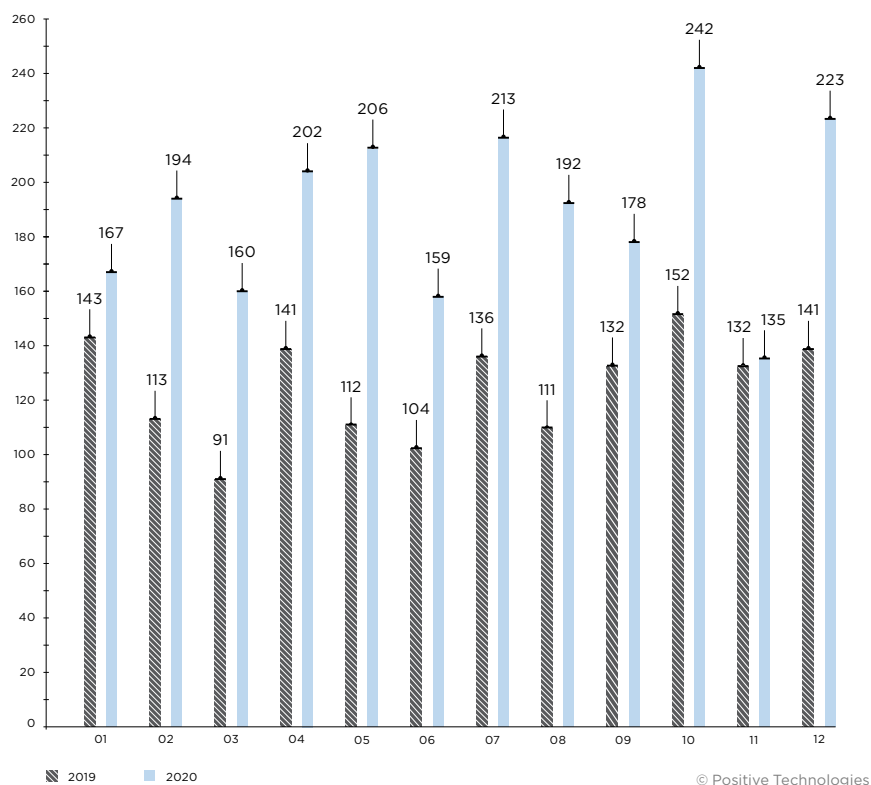


Рисунок 1. Количество инцидентов в 2019 и 2020 годах (по месяцам)

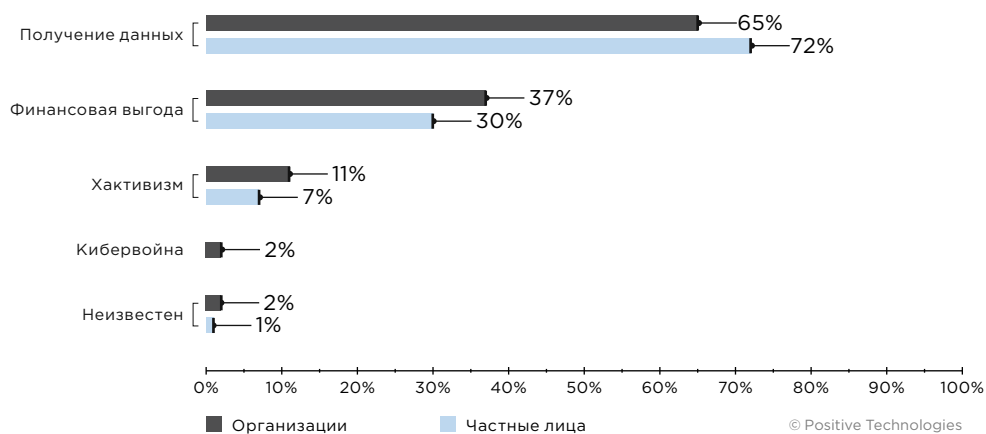


Рисунок 2. Мотивы злоумышленников (доля атак)

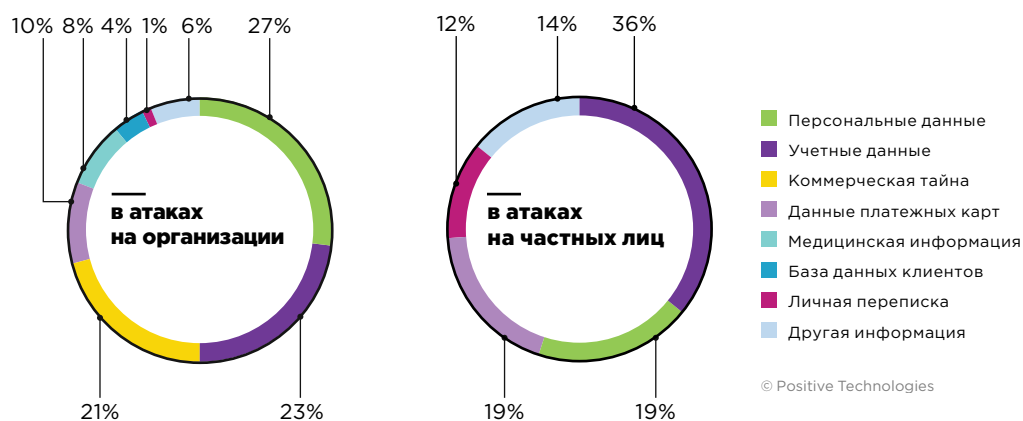


Рисунок 3. Типы украденных данных

70% атак носили целенаправленный характер

14% атак были направлены против частных лиц



Рисунок 4. Категории организаций, ставших жертвами атак

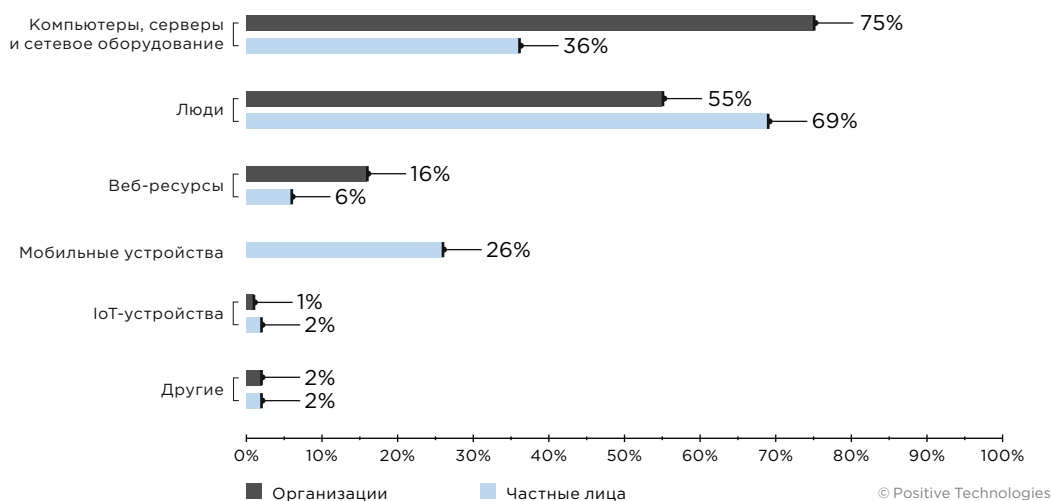


Рисунок 5. Объекты атак (доля атак)



Подводные камни удаленной работы

Активный перевод сотрудников на удаленную работу и вывод внутренних сервисов компаний на сетевой периметр, обусловленные пандемией COVID-19, повлияли на ландшафт киберугроз во всем мире. Лишь немногие компании, которые и так практиковали работу в режиме «удаленки», были готовы справиться со всеми сложностями в обеспечении безопасности, остальные столкнулись с нехваткой времени на продумывание и реализацию всех необходимых мер защиты.

Злоумышленники без промедления приступили к поиску уязвимостей в сервисах на периметрах компаний, в том числе в решениях, используемых для организации удаленной работы, проверяя их на прочность. К примеру, активно эксплуатировались брешы в Pulse Secure VPN, Citrix ADC и Citrix Gateway, в межсетевом экране Cisco ASA. Операторы программ-вымогателей, в частности Netwalker, Clop и REvil, пользовались уязвимыми сервисами для распространения своего ВПО. В целом доля хакинга среди методов атак на организации выросла на 10 процентных пунктов по сравнению с прошлым годом и составила 24%.

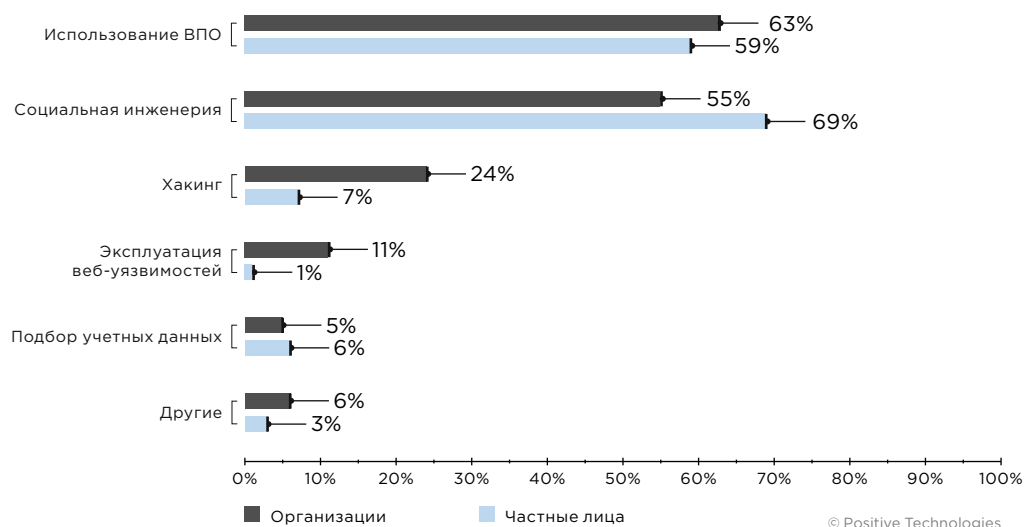


Рисунок 6. Методы атак (доля атак)

Как минимум в 4% атак, где были задействованы уязвимости в ПО на сетевом периметре, эксплуатировалась брешь в Citrix ADC и Citrix Gateway, позволяющая выполнить произвольный код в обход аутентификации, — CVE-2019-19781. Подводя итоги 2019 года, мы прогнозировали, что вырастет число инцидентов с этой уязвимостью, однако многие компании проигнорировали предупреждение и не установили обновления.

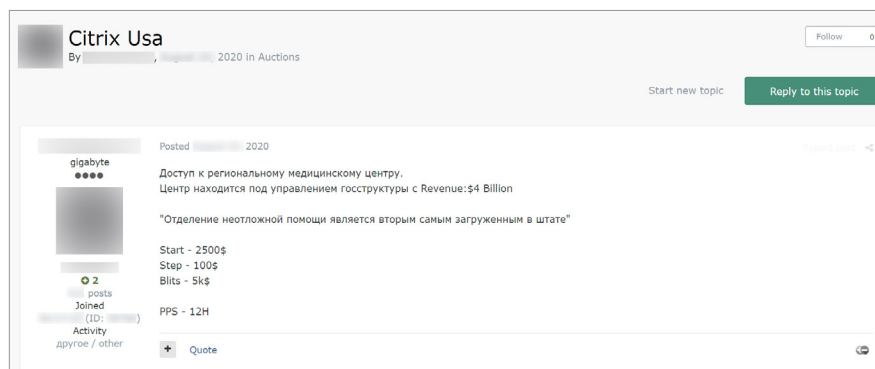


Рисунок 7. Объявление о продаже доступа, полученного путем эксплуатации уязвимости в продуктах Citrix

Другая не менее серьезная уязвимость, которую часто эксплуатировали в 2020 году, — CVE-2019-11510 в VPN-решении Pulse Secure — позволяла не-аутентифицированному пользователю получить имена пользователей и их пароли в открытом виде. Она была использована, к примеру, в атаке, направленной на сбор учетных данных для подключения более чем к 900 серверам различных компаний. Все добытые сведения хакер выложил в открытый доступ в дарквебе.

Наиболее часто эксплуатируемые уязвимости (2020 год)

[CVE-2019-19781](#) (Citrix ADC и Citrix Gateway)
[CVE-2017-11882](#) (Microsoft Office)
[CVE-2019-11510](#) (Pulse Secure VPN)
[CVE-2020-11651](#) и [CVE-2020-11652](#) (SaltStack Salt)
[CVE-2020-14882](#) (Oracle WebLogic)
[CVE-2019-0708](#) (RDP)

Начиная со II квартала 2020 года мы наблюдали также увеличение числа атак, направленных на кражу корпоративных учетных данных сотрудников. Для достижения этой цели хакеры взламывали веб-ресурсы и похищали базы с учетными данными, подделывали формы аутентификации, распространяли шпионское ПО в корпоративной сети и подбирали пароли для подключения к службам на сетевом периметре. Например, в августе злоумышленники отправляли жертвам ссылки на официальные документы, размещенные на поддельном ресурсе, имитирующем интерфейс облачного хранилища Google. Для просмотра документа требовалось пройти процедуру аутентификации, введя корпоративные учетные данные для Microsoft Office 365.

Еще один тренд 2020 года — рост рынков по продаже доступов к серверам компаний. На сегодняшний день, даже если хакеры не смогли продвинуться в атаке дальше найденной уязвимости и получения доступа к серверу, они могут легко продать этот доступ на форуме в дарквебе. Заметим, что пострадать может не только IT-инфраструктура компании, но и ее лицо в интернете — сайт. С начала марта 2020 года мы наблюдаем укрепление интереса к теме взлома сайтов. Мы связываем такую тенденцию с глобальным переходом организаций к работе онлайн.

Вредоносное ПО развивает техники сокрытия

Количество инцидентов с использованием вредоносного ПО увеличилось на 54% по сравнению с 2019 годом. Среди всех вредоносов, используемых в атаках на организации, бесспорным лидером на протяжении двух лет остаются программы-вымогатели. В инцидентах, направленных на частных лиц, чаще всего фигурировали шпионское ПО и банковские трояны.

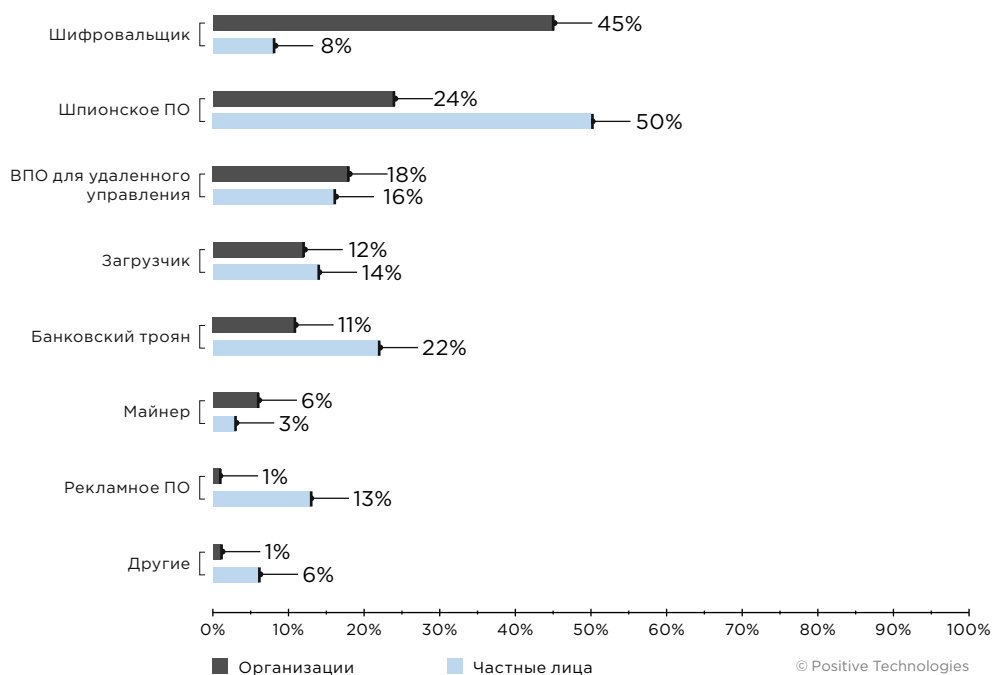


Рисунок 8. Типы вредоносного ПО (доля атак с использованием вредоносного ПО за весь 2020 год)

В атаках на организации основными векторами доставки вредоносного ПО остаются электронная почта (71%) и компрометация компьютеров, серверов и сетевого оборудования (24%), а в атаках на частных лиц хакеры отдают предпочтение электронной почте и веб-сайтам (по 32%).

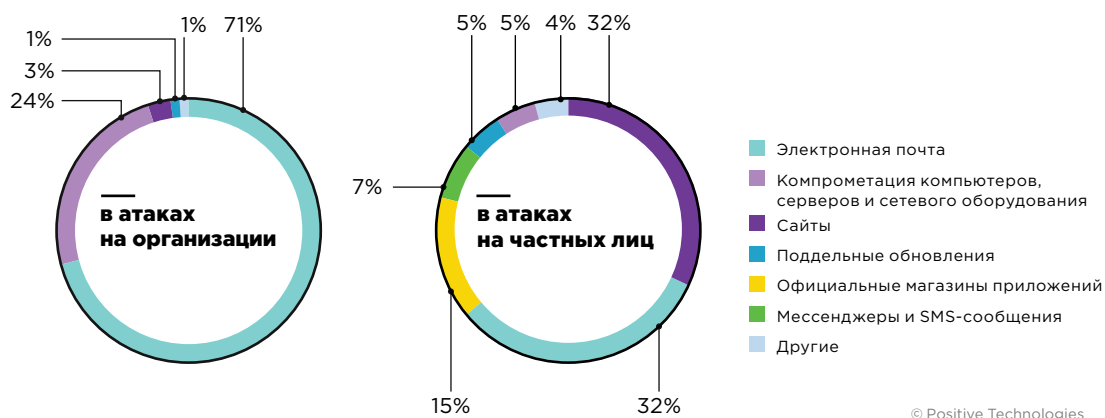


Рисунок 9. Способы распространения ВПО

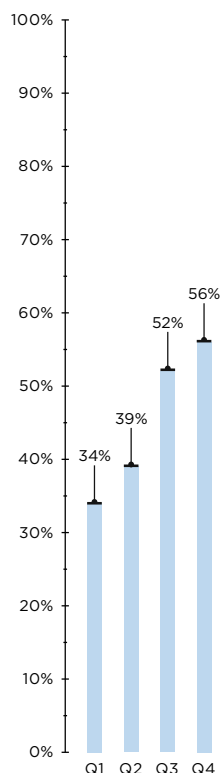


Рисунок 10.
Доля атак шифровальщиков
среди всех атак
с использованием ВПО

В 2020 году мы заметили, что злоумышленники стали тщательнее скрывать свои действия, а вредоносные программы все чаще обзаводятся функциями, способствующими сокрытию заражения и работы ВПО. Если раньше достаточно было скрываться от антивирусных программ, то сейчас, с общим ростом уровня ИБ в компаниях, нужно уметь обходить и песочницы. Для этого как минимум необходимо проверять среду для запуска. Разработчики вредоносов не стоят на месте, совершенствуя методы обхода средств защиты, а в одном продукте может использоваться сразу несколько методов. По данным нашего исследования, чаще всего функции обхода песочниц присутствовали в ВПО для удаленного управления и загрузчиках.

Один из простых способов сокрытия от статического анализа в песочнице был реализован в программе-вымогателе Zeppelin — приостановка вредоносной деятельности на некоторое время после заражения. Вредоносное ПО, выдаваемое за плагин Autodesk 3ds Max, проверяло, запущен ли диспетчер задач или Process Monitor на компьютере жертвы. Обфускация кода также стала отличной практикой для злоумышленников, ведь этот метод затрудняет проверку кода как для автоматического анализатора, так и для специалиста по безопасности.

Атаки вымогателей: потери на миллионы долларов

Доля атак на организации с использованием программ-вымогателей росла с каждым кварталом 2020 года, а по итогам IV квартала оказалось, что больше половины атак, где использовалось ВПО, были проведены с помощью шифровальщиков.

Наиболее активные шифровальщики (2020 год)

1. Netwalker
2. Revil
3. Maze
4. Ryuk+Conti
5. DoppelPaymer

Тщательный выбор жертв

За минувший год операторы вымогателей определенно вышли на новый уровень. В первую очередь, они изменили подход к выбору жертв и, продолжив тренд 2019 года на переход от массовых атак к целевым, стали тщательней выбирать цели — изучая финансовое положение компаний на рынке, оценивая значимость отрасли и потенциальные последствия атаки для компании-жертвы.

Чаще всего под руку операторов программ-вымогателей попадали медицинские (17%) и государственные учреждения (16%), а также промышленные предприятия (15%).

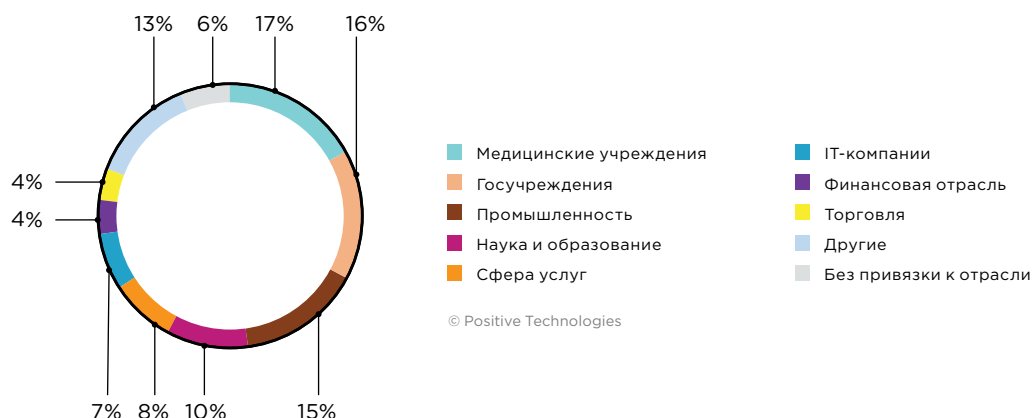


Рисунок 11. Категории жертв, которые были атакованы шифровальщиками в 2020 году

Кража данных и требование двойного выкупа

В конце 2019 года мы отмечали единичные случаи атак операторов программ-вымогателей, которые похищали данные перед шифрованием. В 2020 году эта стратегия — с последующим требованием двойного выкупа за дешифровщик и неразглашение украденной информации — стала трендом. На наш взгляд, это обусловлено тем, что специалисты по ИБ стали считать надежным средством против этого типа ВПО наличие системы резервного копирования. Использование бэкапов облегчает последствия от такого типа атак, поэтому для некоторых компаний не было повода покупать у хакеров дешифровщик. Злоумышленников такой подход, конечно же, не устроил, поэтому в течение всего 2020 года постоянно появлялись новые сайты операторов программ-вымогателей (к примеру, [Ranzy Locker](#), [Avaddon](#) и [Mount Locker](#)) для размещения похищенной информации, за которую владельцы отказались платить.

Новые способы влияния

Операторы шифровальщиков не только шантажировали жертв разглашением украденной информации, но и устраивали DDoS-атаки в случае отказа платить или обсуждать выкуп. Также они объединялись в новые группировки и спекулировали на своей причастности к более «могущественным» преступникам.

Непомерные запросы

Но вот что действительно поразило, так это баснословные суммы запрашиваемых выкупов. По данным компании CrowdStrike, средняя сумма, направляемая хакерам в качестве выкупа, составляет 1,1 млн долл. США. В целом у вымогателей есть все основания запрашивать все большие суммы выкупов, ведь многие компании идут у них на поводу и платят, как это, к примеру, сделали Калифорнийский университет в Сан-Франциско, который заплатил 1,14 млн долл., канадская страховая компания, выплатившая злоумышленникам около 1 млн долл., или американская компания Carlson Wagonlit Travel, отдавшая 4,5 млн долл. за восстановление зашифрованных данных.

Простой сервисов и затраты на восстановление

Последствия от атак шифровальщиков более чем масштабны. Операторы программ-вымогателей оказывают влияние на финансовое состояние компаний, а также могут влиять на их репутацию. Порой восстановить работоспособность сервисов не удастся даже за нескольких дней. Яркий пример — [ситуация с компанией Garmin](#) в III квартале 2020 года. Однако даже в том случае, если компании удалось практически сразу заметить и пресечь инцидент, потери могут исчисляться в миллионах долларов, как это было с ИТ-провайдером [Cognizant](#), который оценил ущерб от атаки в 50–70 млн долл. США, и компанией [Sopra Steria](#), которая оценивает потери в 40–50 млн евро.

Атаки по цепочке: удар по репутации и обвал акций

Атаки, связанные с компрометацией цепочки поставок (supply chain attacks), произошедшие в 2020 году, по-настоящему захватили внимание всего ИТ-мира. В начале атаки злоумышленники выбирают менее защищенную компанию, чтобы получить доступ к ее клиентам. Такие инциденты имеют долгосрочные последствия: в первую очередь, это репутационные потери и отток клиентов, а также финансовый ущерб, связанный со штрафами от контролирующих органов и компенсациями пострадавшим клиентам.

Наиболее громкие инциденты произошли с компаниями Blackbaud и SolarWinds. В ходе майской [атаки на поставщика облачных сервисов Blackbaud](#) в сети компании был запущен шифровальщик и похищены данные клиентов. Компания заплатила выкуп и надеялась, что злоумышленники не воспользуются украденной информацией, однако доверять им было очень опрометчиво. Клиенты компании начали один за другим сообщать о фактах компрометации данных. Еще одна ошибка компании состояла в том, что она не предупредила своих клиентов об инциденте и не сообщила в контролирующие органы. Компания публично признала факт атаки только в середине июля. [В числе пострадавших](#) благотворительные, некоммерческие, образовательные учреждения, фонды и университеты США, Канады, Великобритании и Голландии. В связи с произошедшим инцидентом компании Blackbaud предъявлено 23 коллективных иска с обвинениями в причинении ущерба.

В декабрьском инциденте с SolarWinds ущерб оказался гораздо масштабней. [Были затронуты](#) госучреждения, образовательные, медицинские, консалтинговые, технологические и телекоммуникационные компании в США, Европе, Азии и на Ближнем Востоке. После того как стало известно об атаке, акции SolarWinds за неделю обрушились в цене на 40%, и до сих пор котировки не вернулись к прежнему уровню. Стоит заметить, что в результате атаки на клиентов SolarWinds злоумышленники украли программное обеспечение для проведения тестов на проникновение компании FireEye, которое может быть использовано в новых атаках в ближайшее время.



Рисунок 12. Обвал котировок SolarWinds после новостей об атаке

Другие атаки на цепочку поставок затрагивали поставщиков программных и аппаратных продуктов для медицинских учреждений, разработчиков ПО для финансовых компаний.

Медицина: первые жертвы среди населения и возврат к бумажным документам

В 2020 году количество атак на медицинские организации по сравнению с 2019 годом выросло на 91%. Доля атак на медицину составила 9% от общего числа инцидентов. На фоне пандемии COVID-19 и повышенной нагрузки на лечебные учреждения хакеры подливали масла в огонь, нарушая доступность медицинских информационных систем своими многочисленными атаками. Эту проблему признают во всем мире, к примеру Франция выделит 1 млрд евро на укрепление кибербезопасности после серии атак на больницы: в этой стране доля атак на медучреждения в 2020 году составила 11% от общего количества зафиксированных инцидентов.

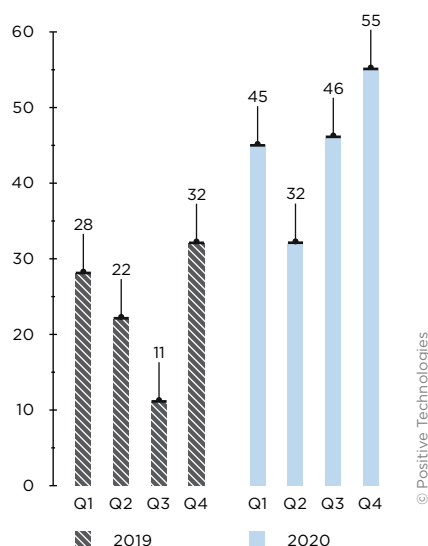


Рисунок 13. Число атак на медучреждения в 2019–2020 годах

Злоумышленники используют преимущественно методы социальной инженерии (66%) и хакинг (21%). В 68% атак применялось вредоносное ПО. В основном это были шифровальщики: доля инцидентов, в которых они были использованы, составила 81% всех атак с применением вредоносов.

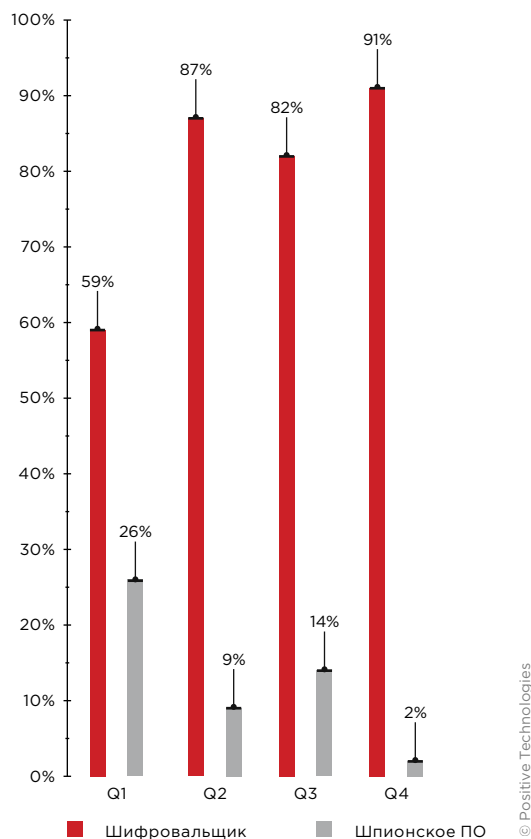


Рисунок 14. Основные типы вредоносного ПО в атаках на медучреждения (доля атак с использованием ВПО)

Последствия от реализации атак с этим типом ВПО колоссальные. К примеру, общий ущерб в 2020 году от атак шифровальщиков на американские медучреждения оценивается в 20,8 млрд долл. Но для этой отрасли более опасны не финансовые последствия, а сложности с оказанием медицинской помощи людям. Такая ситуация произошла, к примеру, в сети больниц Universal Health Services и в медицинском центре Университета Вермонта. Сотрудники больниц UHS не могли получить доступ к результатам анализов пациентов и ранее сделанным назначениям, получить данные с диагностических приборов и оказать неотложную медицинскую помощь, поскольку все необходимые данные хранились в электронном виде и оказались зашифрованы в результате атаки. А в медицинском центре в Вермонте сотрудникам пришлось восстанавливать по памяти протоколы химиотерапии, так как на восстановление системы требовалось время, которым пациенты не располагали. Подобные ситуации, когда медучреждение не может оказать неотложную помощь, а пациентов в срочном порядке приходится переводить в другие клиники, могут привести к трагическим последствиям, как, например, случай в больнице Дюссельдорфа.

Атакам подвергались не только медучреждения, оказывающие непосредственную помощь в борьбе с пандемией, но и компании, задействованные в производстве и поставке вакцин, — лаборатории, логистические и фармацевтические компании (Fareva и Dr. Reddy's), а также Европейское агентство лекарственных средств, которое выдает разрешения на использование вакцин.

Промышленность: реализация рисков на критически важных объектах

Количество атак на промышленность увеличилось почти в два раза по сравнению с 2019 годом: прирост составил 91%.

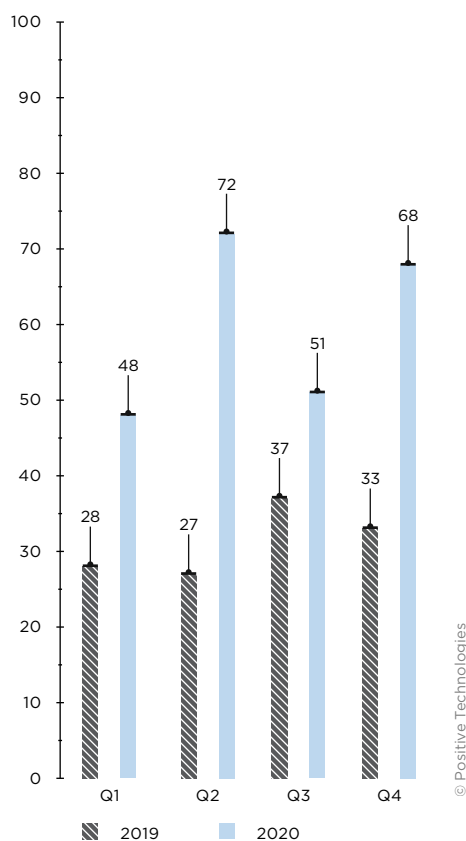


Рисунок 15. Количество атак на промышленность

В основном эту отрасль атаковали операторы программ-вымогателей, в частности RansomExx, Netwalker, Clop, Maze, Ragnar Locker, LockBit, DoppelPaymer, Snake. Последний из них перед началом шифрования удаляет теневые копии, а также имеет функции, которые позволяют принудительно остановить процессы, связанные с АСУ ТП. Из-за атак некоторые компании, например Hubert+Suhner и Honda, были вынуждены приостановить производство.

Интерес шифровальщиков спровоцировал и увеличение доли атак, мотивом которых была финансовая выгода, до 36% (на 26 п. п. больше, чем в 2019 году). Еще одна деталь — увеличение доли атак с применением хакинга в 2,6 раза по сравнению с 2019 годом.

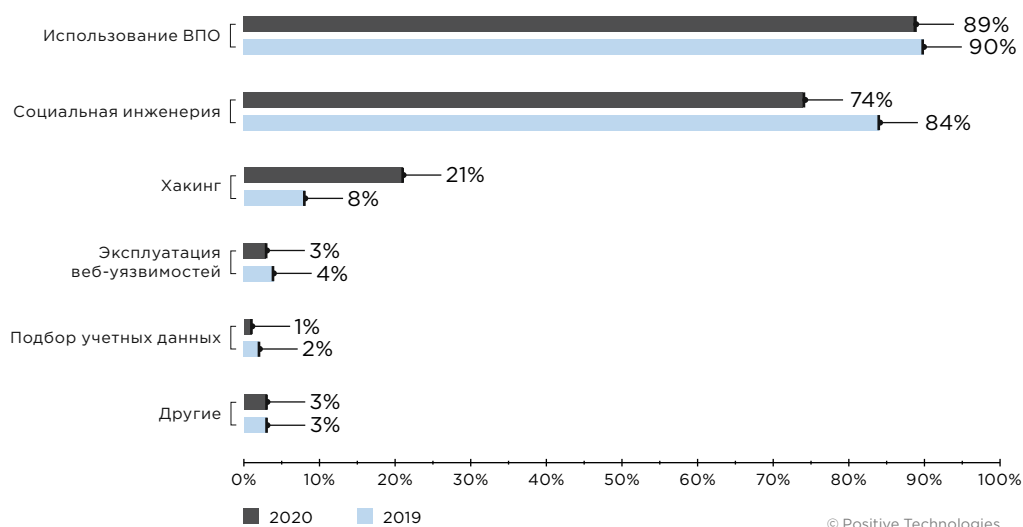


Рисунок 16. Методы атак на промышленность

На промышленность нацелены и многие APT-группировки. К примеру, в III квартале была обнаружена группировка TinyScouts, которая атакует российские предприятия в сфере энергетики. Для стран СНГ остаются актуальными атаки группировки RTM: за 2020 год эксперты PT ESC выявили более 100 ее фишинговых рассылок.

Реализация рисков в промышленной отрасли влечет за собой глобальные последствия. Например, в ходе атаки на инфраструктуру водоснабжения и канализации в Израиле хакеры планировали изменить концентрацию хлора в подаваемой в жилые дома воде, что привело бы к массовому отравлению, а инцидент с отключением электроэнергии из-за кибератаки в Индии сказался на работе фондовой биржи, больниц и транспортной системы нескольких городов.

Предугадать возможность реализации самых страшных рисков и оценить масштаб последствий на объектах критически значимой инфраструктуры сложно, поскольку даже самые опытные специалисты не могут дать гарантию, что все предусмотренные защитные механизмы сработают как нужно. Для адекватной оценки актуальных рисков предприятия недостаточно тестов на проникновение, потому что на реальной инфраструктуре сбоев в работе допустить нельзя. Имитировать ход атаки хакеров и при этом не навредить «боевым» системам можно на киберполигоне, где в безопасной среде есть возможность получить наиболее полное представление о том, реально ли осуществить конкретные риски (например, переполнение нефтяного хранилища), проверить, сработают ли механизмы защиты и успеет ли команда специалистов по безопасности вовремя увидеть инцидент и предотвратить его развитие.

Об исследовании

Данный отчет содержит информацию об общемировых актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах многочисленных расследований, а также на данных авторитетных источников.

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, в связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Наше исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены [в глоссарии на сайте Positive Technologies](#).

О компании

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

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

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

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