



PT

Теневой рынок доступов

ptsecurity.com

Информационная безопасность — одно из приоритетных направлений для компаний, а на поддержание ее на достаточном уровне тратится огромное количество ресурсов, в том числе финансовых. Согласно исследованию Gartner, общемировые расходы на информационную безопасность в 2020 году выросли на 6,4% по сравнению с 2019 годом, а главным приоритетом при планировании корпоративного бюджета 61% из более чем 2000 опрошенных IT-директоров назвали инвестиции в ИБ. Однако больших денежных вливаний и найма квалифицированных сотрудников может быть недостаточно.

Общепринятые подходы к оценке угроз предусматривают классификацию потенциальных злоумышленников и построение системы защиты с учетом возможностей определенных типов нарушителей. Существует такая практика, когда компании считают, что они не интересны крупным АPT-группировкам и другим злоумышленникам серьезного уровня, а менее подготовленные нарушители не способны причинить ущерб бизнесу. Если неправильно оценить возможности потенциального злоумышленника, то защита окажется неэффективной.



Из-за того, что теневой рынок доступов хорошо развит и широко используется, существовавшая ранее грань между опытными злоумышленниками и низкоквалифицированными — стирается.

Мы уже рассказывали о рынке продажи доступов. В новом исследовании мы оценим, как развивался этот рынок на протяжении 2020 года и в начале 2021 года и какие последствия это несет для бизнеса. Мы проанализировали десять наиболее популярных русскоязычных и англоязычных форумов в дарквебе, где представлены предложения о продаже доступов в компании, объявления о поиске злоумышленников-исполнителей или напарников для взлома. Всего на этих форумах зарегистрировано более 8 млн пользователей, создано более 7 млн тем, в которых опубликовано более 80 млн сообщений.

Как поменялся теневой рынок доступов

Рынок доступов к корпоративным сетям активно формировался в течение последних нескольких лет. О его зрелости уже можно было судить в начале 2020 года. Один из факторов, способствующих такому развитию, — увеличение количества атак с использованием программ-вымогателей: участники партнерских программ шифровальщиков часто пользуются предложениями на рынке доступов.

Историческая справка

Еще лет десять назад на форумах в дарквебе продавались доступы к отдельным компьютерам частных лиц. В основном их скупали мошенники, занимающиеся кардингом, то есть совершающие операции с использованием банковской карты без участия ее владельца. Затем готовые доступы начали приобретать киберпреступники, нацеленные на частных лиц и использующие в своих атаках программы-вымогатели. В какой-то момент распространители шифровальщика приобрели доступ к сети компании, с легкостью провели атаку и получили выкуп: это породило тенденцию к использованию готовых доступов в атаках на организации.

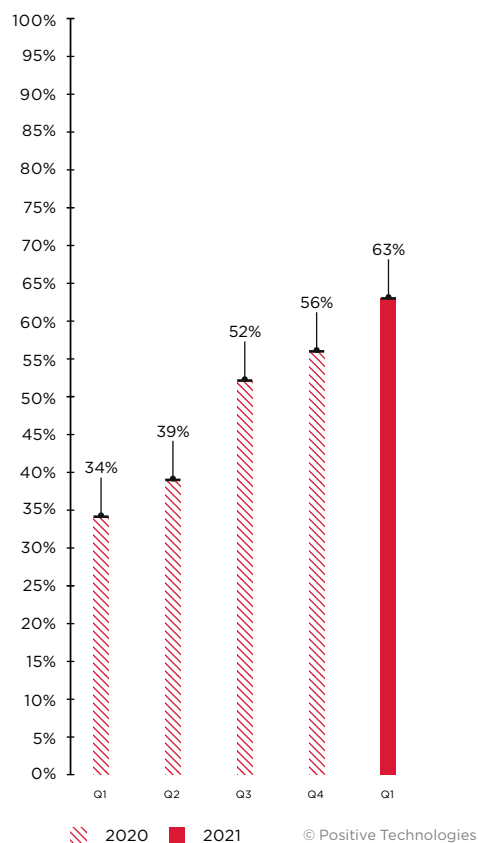


Рисунок 1. Доля атак шифровальщиков среди всех атак на организации с использованием ВПО

Количество новых объявлений на тему доступов на теневых форумах увеличивалось с каждым кварталом на протяжении всего рассматриваемого периода. Чаще всего это были объявления о продаже уже полученных доступов к корпоративным сетям. На протяжении 2020 года мы выявили 707 новых объявлений о продаже доступов. В сравнении с 2019 годом количество новых объявлений увеличилось более чем в семь раз. И за один только I квартал 2021 года было обнаружено уже 590 новых предложений. Число новых объявлений о поиске напарников и злоумышленников-исполнителей также выросло: можно предположить, что это связано с появлением новых партнерских программ шифровальщиков и расширением старых группировок, распространяющих этот тип вредоносного ПО.

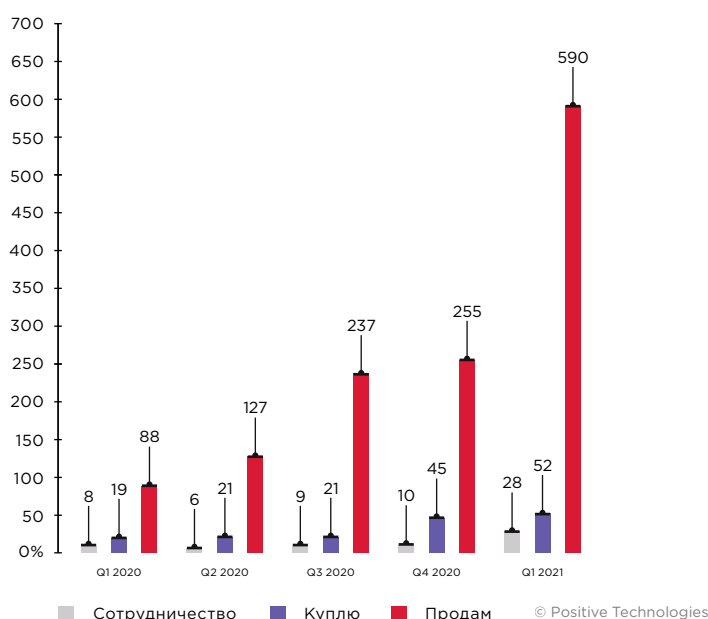


Рисунок 2. Количество новых объявлений на теневых форумах, посвященных доступам к корпоративным сетям

Интерес к доступам подтверждается и количеством пользователей, которые размещают объявления о покупке, продаже или сотрудничестве. Относительно I квартала 2020 года в I квартале 2021 года количество пользователей увеличилось в три раза.

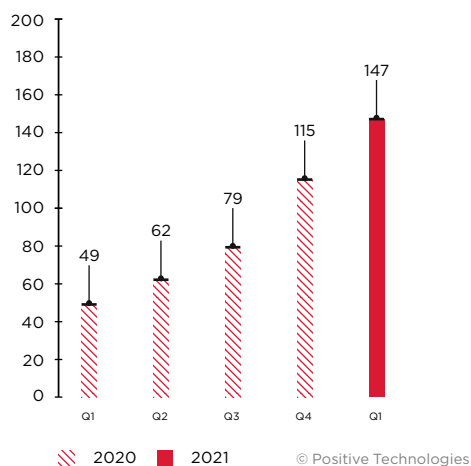


Рисунок 3. Количество пользователей, размещающих на форумах объявления о продаже доступов

В среднем в дарквебе ежеквартально продаются доступы в корпоративные сети на сумму около 600 000 долл. США. Хотя количество предложений на рынке растет, совокупная стоимость изменяется незначительно, что свидетельствует о том, что средняя цена, запрашиваемая за один доступ, снижается. Недорогие доступы, как правило, без привилегий — и чаще всего их продают неопытные злоумышленники, которые опасаются развивать атаку дальше. В целом стоимость доступа обычно зависит:

- от количества компьютеров, к которым преступник получит доступ;
- привилегий учетной записи;
- размера компании;
- доходов компании и других ее финансовых показателей;
- отрасли, к которой принадлежит компания.

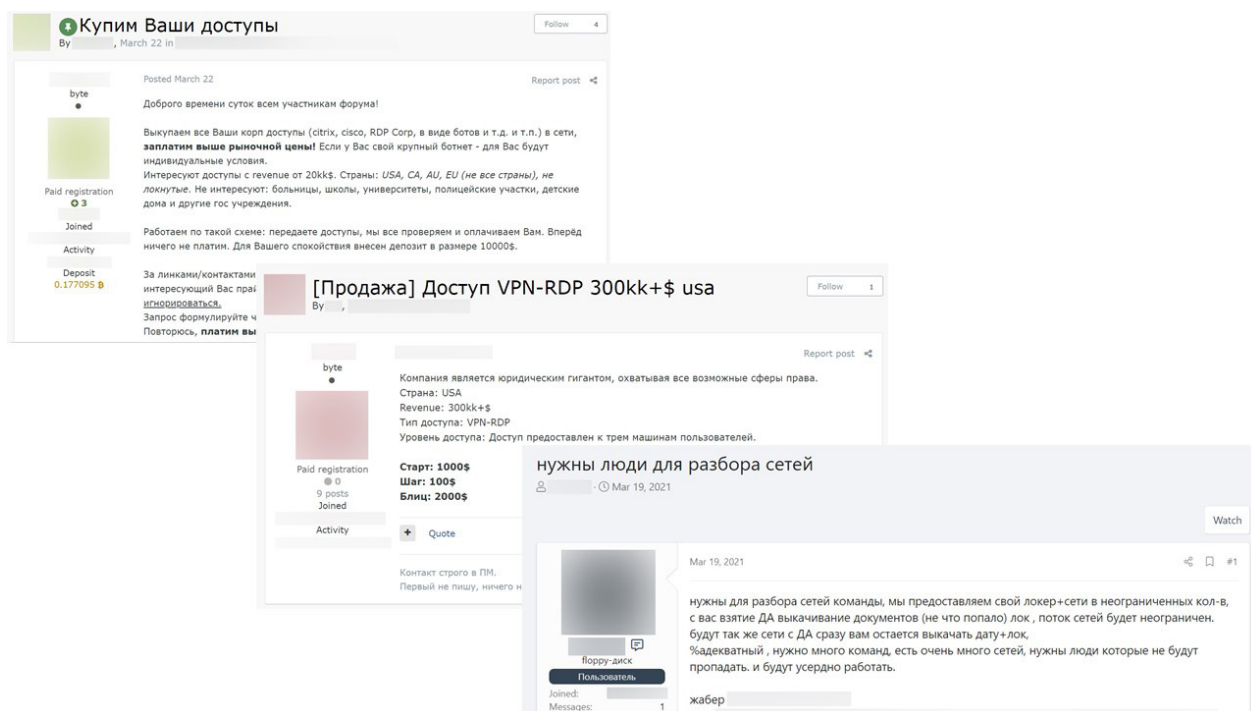


Рисунок 4. Примеры объявлений на форуме в дарквебе

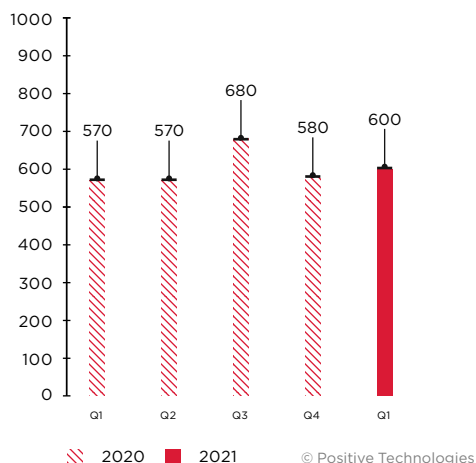
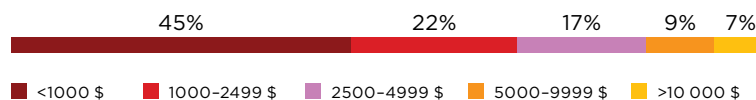


Рисунок 5. Совокупная стоимость доступов, продаваемых на форумах в дарквебе (тыс. долл. США)

С 2017 года по I квартал 2020 года доля объявлений, где была указана цена менее 1000 долл. США за доступ в одну компанию, составляла 15%, а в период со II квартала 2020 года по I квартал 2021 года она выросла на 30 процентных пунктов и составила уже 45%. Доля дорогих доступов, стоимость которых превышает 5000 долл. США, за тот же период сократилась практически в два раза. Такие изменения могут быть следствием активного выхода на рынок злоумышленников-новичков.



© Positive Technologies

Рисунок 6. Распределение предложений о продаже доступов к сетям компаний по их стоимости

Наш прогноз подтверждается: у злоумышленников появилась новая специализация — «добытчики доступов», и она привлекает новичков легким заработком. Их основная задача — получить первоначальный доступ в сеть компании для последующей реализации на рынке в дарквебе.

Может ли компания выявить факт продажи доступа?

Обнаружить факт компрометации учетных данных можно, к примеру, на этапах верификации доступа продавцом перед продажей (или покупателем — после продажи). Для этого необходимо настраивать средства защиты, в том числе SIEM-системы, средства анализа сетевого трафика, на выявление аномальных подключений к инфраструктуре.

Чаще всего злоумышленники выставляли на продажу доступы к компаниям из сферы услуг (17%), промышленности (14%) и учреждениям в сфере науки и образования (12%). В прошлом рассматриваемом периоде тройка наиболее часто встречающихся отраслей выглядела следующим образом: промышленные компании (16%), предприятия сферы услуг (14%) и финансовые организации (11%). Организации сфере науки и образования занимали четвертое место, и их доля среди всех объявлений о продаже доступов в сети компаний составляла 9%. Отметим, что доля промышленных компаний и финансовых организаций, доступы в которые традиционно стоят дороже, несколько уменьшилась. Мы можем связать это с тем, что рынок доступов наполняется низкоквалифицированными игроками, которые предпочитают жертв «попроще».

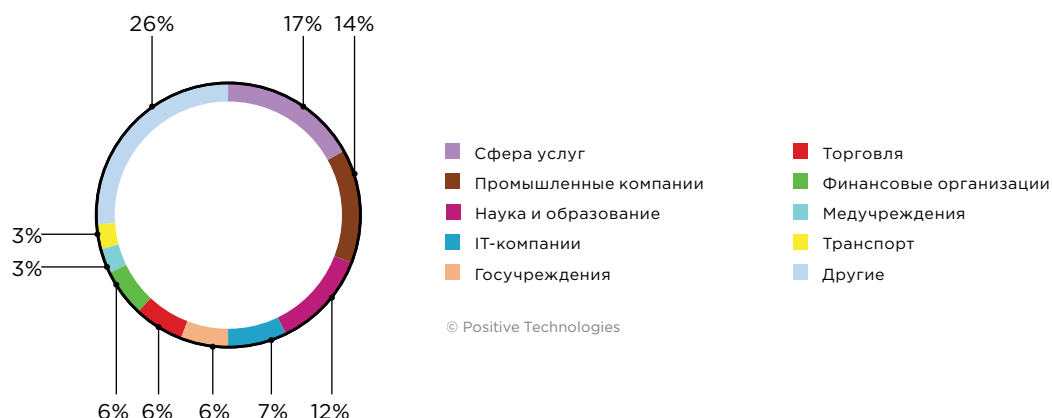


Рисунок 7. Распределение взломанных организаций по отраслям

Последствия для бизнеса

Мы видим, что модель нарушителя меняется: внешний нарушитель, который получает первоначальный доступ к сети компании, и нарушитель, который развивает атаку внутри, — абсолютно разные по уровню подготовки. Даже если периметр будет взломан новичком, в локальной сети атаковать будут уже профессионалы. Они обладают всеми ресурсами для достижения цели — реализации самых опасных для компании событий (от кражи денег со счетов до полной остановки бизнес-процессов на длительное время). А значит, и выстраивать систему защиты от кибератак необходимо с учетом новых реалий.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/
PositiveTechnologies
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.