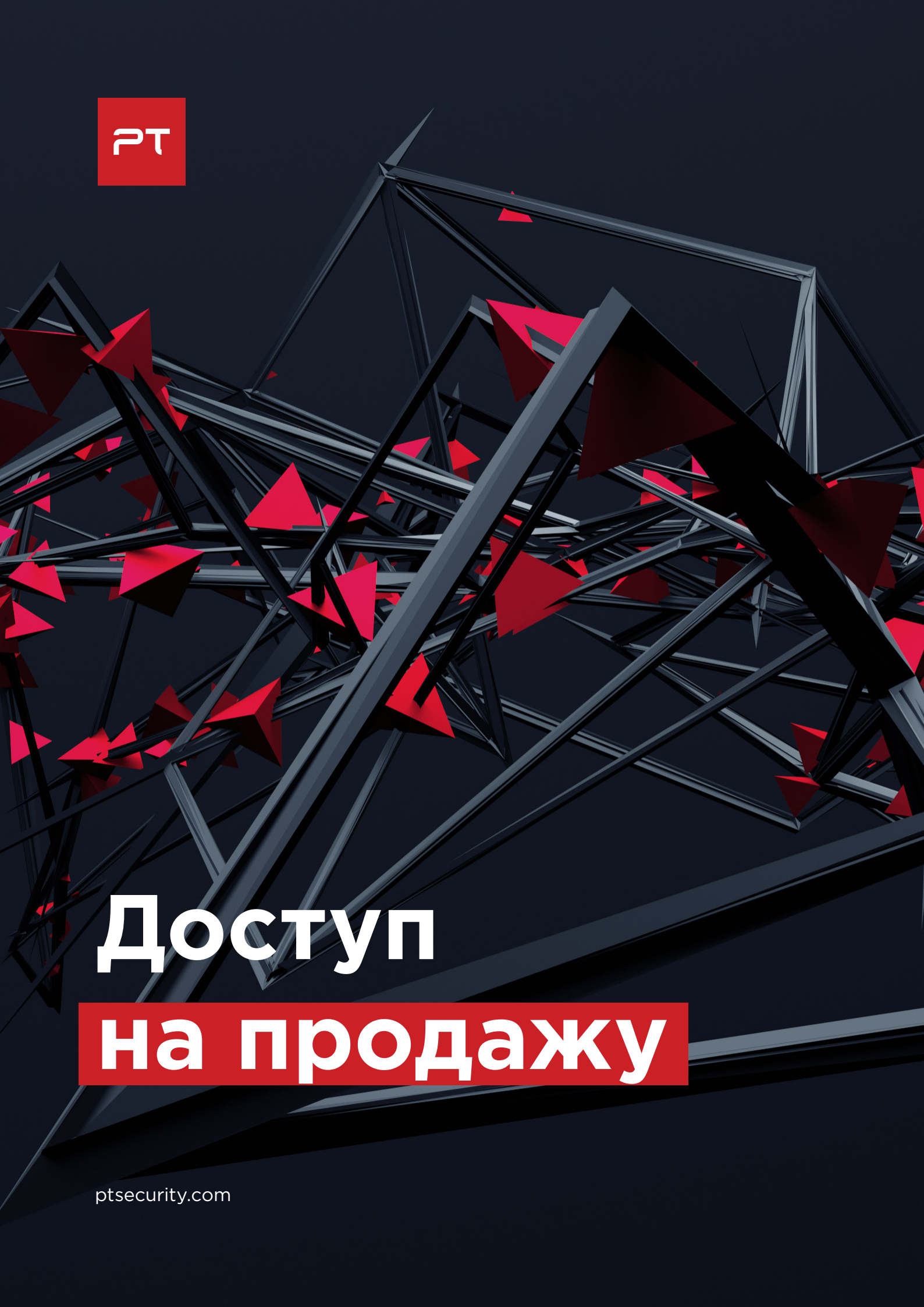




PT



# Доступ на продажу

[ptsecurity.com](https://ptsecurity.com)

Одной из причин ежегодного роста числа кибератак (за 2019 год на 19%<sup>1</sup>) мы называем легкий вход в мир киберпреступности. Это стало возможным благодаря развитию множества нелегальных площадок на теневом рынке киберуслуг. Сформировалось предложение вредоносного ПО и услуг, которые применяются для проникновения в корпоративную сеть. А низкоквалифицированные хакеры быстро научились использовать эти инструменты.

В данной статье мы расскажем о том, что такое «доступ на продажу» и «партнерская программа шифровальщика», покажем актуальность этих угроз и поясним, какие риски они могут нести бизнесу.

## Что такое доступ к сети

Доступ как объект продажи на теневом рынке — это собирательное понятие, включающее в себя ПО, эксплойты, учетные данные и все остальное, что позволяет несанкционированно управлять конкретным удаленным компьютером или множеством компьютеров. Если один злоумышленник взломал сайт, веб-сервер, базу данных или рабочую станцию, то говорят, что у него есть доступ. Такой доступ можно передать (продать) третьим лицам, как ключи от квартиры. Далее в статье речь пойдет только о доступах к серверам и рабочим станциям.

## Рынок доступов

По нашим наблюдениям, еще год или два назад злоумышленников интересовали доступы к единичным серверам, которые скупались на теневом рынке по цене до 20 долларов.

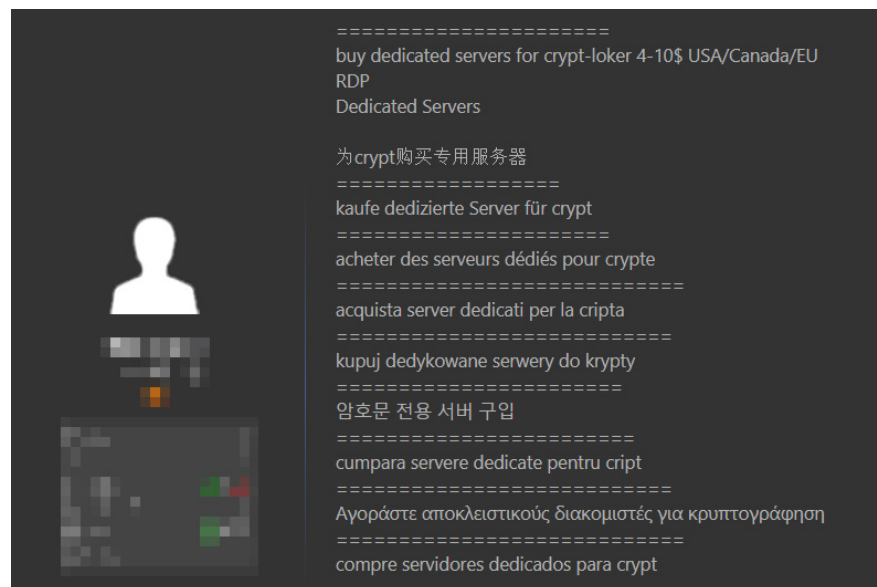


Рисунок 1. Продажа доступов под шифровальщик к удаленным ПК

<sup>1</sup> [ptsecurity.com/ru-ru/research/analytcs/cybersecurity-threatscape-2019/](https://ptsecurity.com/ru-ru/research/analytcs/cybersecurity-threatscape-2019/)

Но уже со второй половины 2019 года мы видим, как на специализированных хакерских площадках<sup>2</sup> растет число новых тем, посвященных покупке доступов к локальной сети компаний.

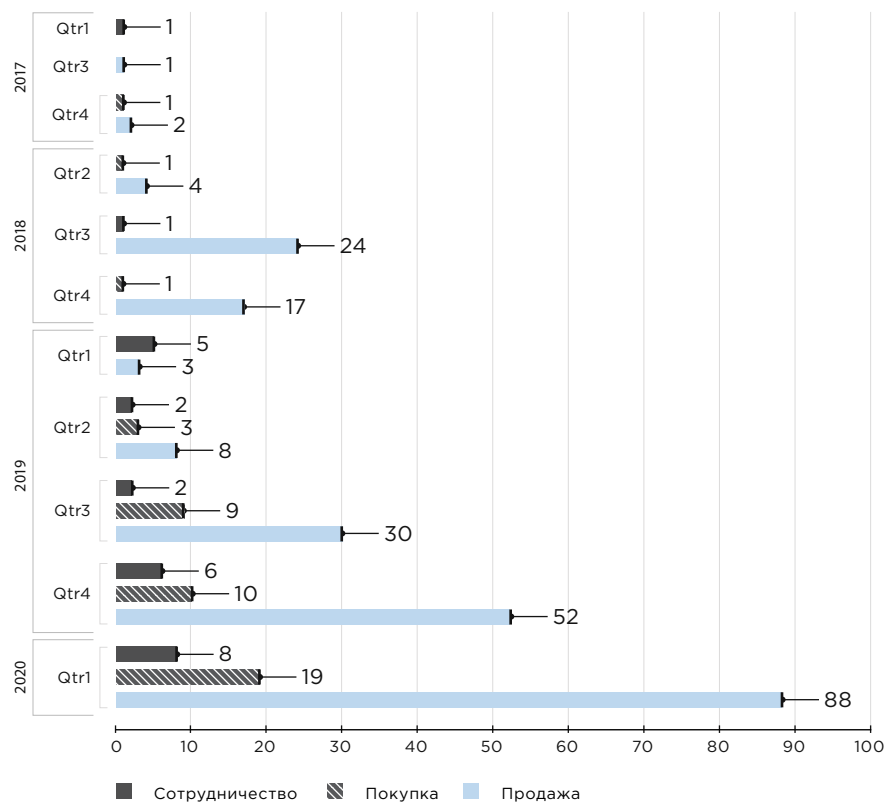


Рисунок 2. Количество новых веток на темных форумах, посвященных доступам к корпоративным сетям

Появились скупщики, которые предлагают пользователям значительно более выгодные условия, а также постоянное сотрудничество. К примеру, если взломана инфраструктура компании с годовым доходом от 500 миллионов долларов, предлагается доля от потенциальной прибыли после завершения атаки, размер которой может достигать до 30%.

<sup>2</sup> Мы изучили 190 площадок в дарквебе, где представлены предложения о покупке и продаже инструментов, используемых в кибератаках, а также объявления о заказной разработке вредоносного ПО. В числе исследованных темных ресурсов форумы, специализированные маркетплейсы и чаты преимущественно с русско- и англоговорящей аудиторией. Средняя общая посещаемость ресурсов — более 70 млн человек в месяц.

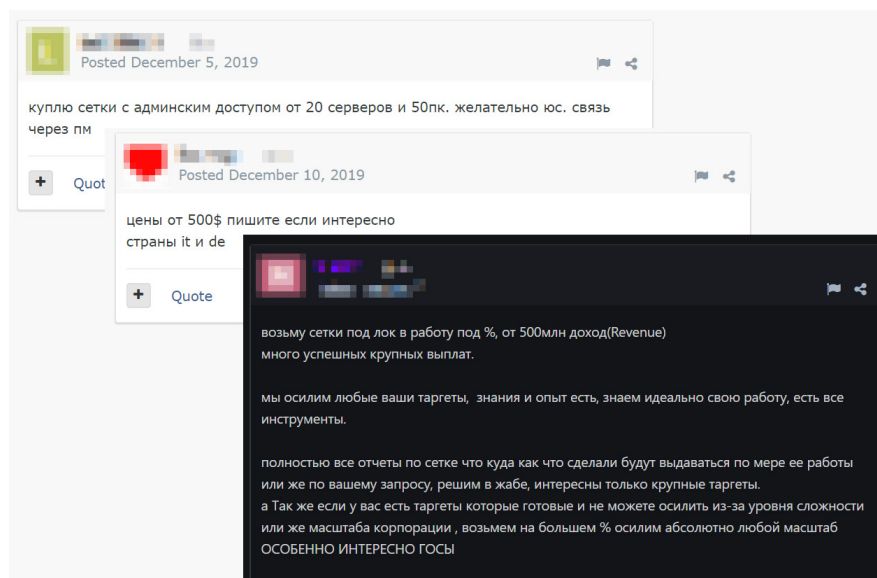


Рисунок 3. Покупка доступов в сети компаний

За спросом подтянулось предложение. Уже в конце 2019 года открыто продавались более 50 доступов в сети крупных компаний со всего мира, а к концу марта их число превысило 80. Среди жертв значились организации с годовым доходом от сотен миллионов до нескольких миллиардов долларов.

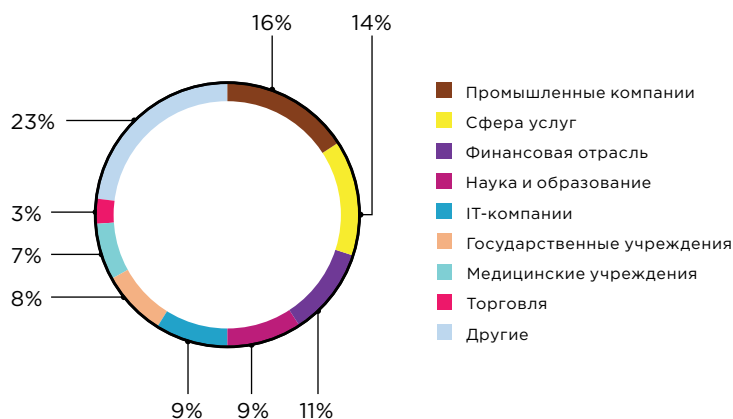


Рисунок 4. Распределение взломанных организаций по отраслям

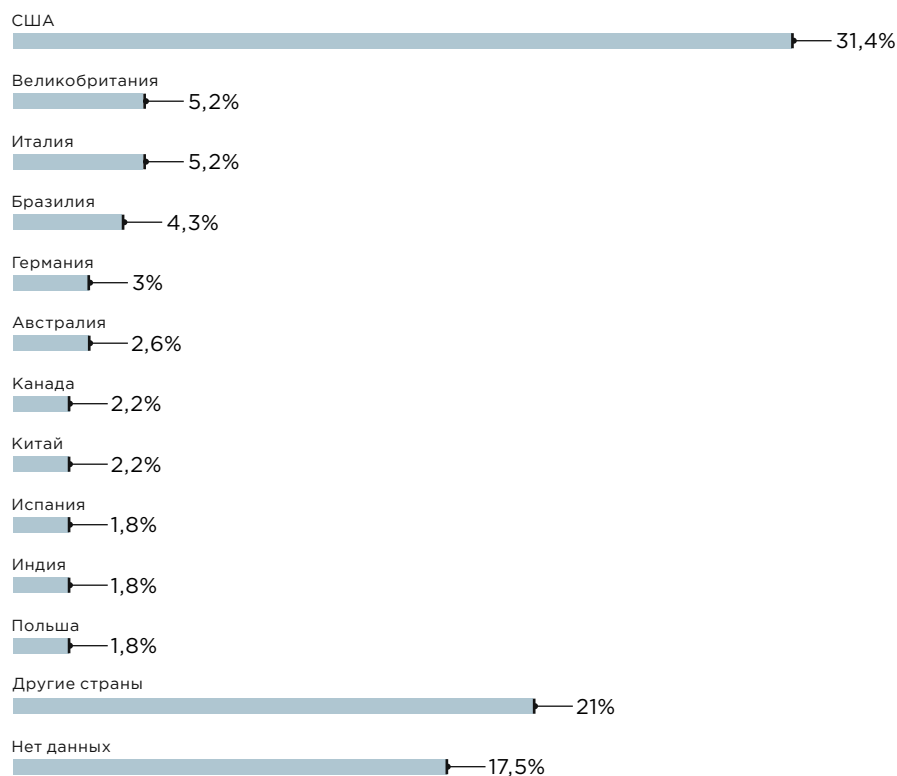


Рисунок 5. География взломанных компаний

При этом в случае США чаще всего продаются доступы в организации сферы услуг (20%), промышленные компании (18%) и государственные учреждения (14%). В Италии отрасли, доступы в компании которых продаются чаще всего, иные: промышленность и сфера услуг в 25% и 17% случаев соответственно. В Великобритании: сфера услуг (33%), наука и образование (25%), финансовая отрасль (17%). В Бразилии в 20% случаев речь идет о продаже доступа к сетям государственных учреждений и в 10% — медицинских. По 29% всех продаваемых доступов в немецкие компании приходится на сферу ИТ и сферу услуг. Прямых свидетельств продажи доступов в российские организации не зафиксировано, однако надо учитывать, что 17,5% всех подобных предложений на теневом рынке не имеют географической привязки, а также что часть данных продаются и покупаются вообще без подобных объявлений.

Продавцы оценивали свой товар в суммы от 500 до 100 000 долларов. Средняя стоимость привилегированного доступа к локальной сети сейчас составляет порядка 5000 долларов.

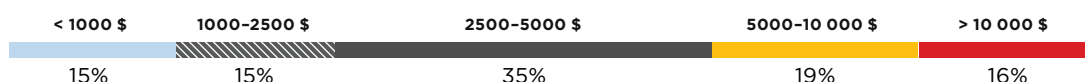


Рисунок 6. Предложения о продаже доступов к сетям на теневом рынке

## Продам доступ к внутренней сетке канадских department store

Reply to this topic



Posted September 5, 2019



существуют с 1960 года  
**100** оффлайн магазинов + онлайн шоп  
 Права админа домена

**100 000 usd**

Рисунок 7. Стоимость некоторых доступов доходит до 100 тысяч долларов

Раньше низкоквалифицированным злоумышленникам было сложно монетизировать свои атаки, ведь у них недостаточно навыков, чтобы после проникновения развить атаку до получения какой-либо ценной информации или вывода денег. Теперь же, с появлением спроса на доступы, у них появился постоянный источник дохода.

Покупателями выступают другие злоумышленники. Они могут либо сами развить атаку до интересующих их бизнес-систем, либо нанять команду более квалифицированных хакеров, которые за короткое время смогут получить привилегии администратора домена и разместят вредоносные файлы на критически важных для жертвы серверах.

## Selling USA 2 State Government Network Access

Reply to this topic



Posted February 8



- Microsoft Based Windows
- Access To DC + All Server
- High Priviledged User (Admin Of Network)

\*Sensitive Target, Detail In Contact  
 \*Access From 2 Different State



Posted February 15



\*\*\* Update

Now there are 3 access.

for 3, price is = 80.000\$

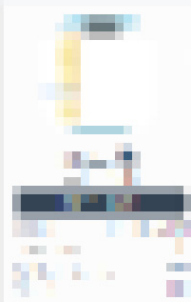
Рисунок 8. Продажа доступа к сети госорганизации с правами администратора домена

Одними из первых такую схему взяли на вооружение операторы шифровальщиков, скупая доступы за фиксированную плату у одних преступников и нанимая других уже для размещения ВПО в локальной сети за высокий процент от полученного с жертвы выкупа. На теневых форумах такая схема получила название «партнерская программа шифровальщика» (ransomware affiliate program).

### Пентестерам, локальщикам, сетевикам.

Jul 17, 2019

Watch



Jul 17, 2019

Thread starter

#1

Наидобрейшего времени суток уважаемые пользователи данного ресурса.

В команду профессионалов требуются сотрудники, имеющие не только представление о таких продуктах как metasploit, cobaltstrike, но и опыт работы с сетями.

Со своей стороны мы предоставляем доступы к серверам, которые находятся доменных и локальных сетях, а так же средство монитизации - стабильный и удобный ransomware.

В задачи пентестера входит:

Сканирование и составление карты сети, снятие дампа памяти на доступных хостах. Взятие доменного админа и полный доступ ко всей сети, (пк, сервера, NASы, Гиперы, бэкапы). Запуск локера на всех доступных хостах.

Для вступления в команду нужен всего лишь готовый сервер или впс с настроенным metasploit или cobaltstrike, а так же серьезный настрой, ответственность и желание заработать.

У нас все прозрачно, 30% с выкупа ваши. вы получаете доступ к переписке с клиентами, тем самым имеете представление о размере выкупа и о том, как продвигаются дела с нашей стороны.

Рисунок 9. Поиск хакеров для атаки на компании на этапе постэксплуатации



## Чем это грозит организациям

Мы ожидаем, что в ближайшее время крупные организации могут попасть под прицел низкоквалифицированных нарушителей, которые нашли способ легкого заработка. Количество внешних атак на инфраструктуру организаций существенно вырастет. Эта проблема особенно актуальна сейчас, когда множество компаний в спешке переводят сотрудников на удаленную работу. Хакеры будут искать любую незакрытую брешь в системах на периметре сети, например забытое незащищенное веб-приложение, необновленное ПО или некорректно сконфигурированный сервер со слабым паролем администратора. Чем крупнее взломанная компания и чем выше полученные привилегии, тем более выгодную сделку может провести преступник.

Распространено мнение, что проблема кибератак со стороны низкоквалифицированных хакеров (так называемых скрипт-кидди<sup>3</sup>) более актуальна для небольших компаний, которые не готовы вкладывать значительные средства в защиту своих ресурсов. Крупные организации вкладывают гораздо больше средств в информационную безопасность и, казалось бы, должны быть лучше защищены. Но наш опыт тестов на проникновение демонстрирует уязвимость даже крупных компаний. Наши эксперты находят простые способы проникновения в локальную сеть, не требующие высокой квалификации от потенциального злоумышленника. Логично предположить, что средний и малый бизнес находятся в еще большей опасности ввиду того, что имеют меньше возможностей для защиты.

Мы хотим обратить внимание организаций, что следует уделять внимание комплексной защите инфраструктуры — как на сетевом периметре, так и в локальной сети. Мы рекомендуем убедиться, что все сервисы на периметре сети защищены, а в локальной сети обеспечен достаточный уровень мониторинга событий безопасности для выявления нарушителя. А регулярный ретроспективный анализ событий безопасности позволит обнаружить пропущенные ранее кибератаки и устранить угрозу до того, как злоумышленники украдут информацию или остановят бизнес-процессы.

---

<sup>3</sup> Люди, которые используют программы, разработанные другими, для атак на компьютерные системы и сети и для повреждения веб-сайтов. Обычно считается, что большинство их — подростки, которым не хватает способностей самостоятельно писать сложные программы или создавать эксплойты, и что их цель — произвести впечатление на своих друзей или завоевать репутацию среди компьютерных энтузиастов. Тем не менее термин фактически обозначает нарушителей любого возраста.

### О компании

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

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