GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

ПРОДАЖА ДОСТУПОВ

ДИСКЛЕЙМЕР

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

HI-TECH CRIME TRENDS 2021/2022

ГЛАВА 1

Незваные гости: кто продает доступ в инфраструктуру вашей компании

Анализ даркнет-ресурсов по продаже доступов к скомпрометированной инфраструктуре компаний

ОГЛАВЛЕНИЕ

ПОЧЕМУ HI-TECH CRIME TRENDS?

00

Hi-Tech Crime Trends исследует разные аспекты функционирования киберкриминальной индустрии, анализирует атаки и прогнозирует изменение ландшафта угроз для различных отраслей мировой экономики. Отчет выпускается с 2012 года и интегрирует данные собственных исследований компании, реагирований на кибер-инциденты по всему миру.

Применяя уникальные инструменты слежения за инфраструктурой киберпреступников и тщательно изучая исследования специалистов из разных стран, эксперты Group-IB ежегодно находят и подтверждают общие паттерны глобального развития киберугроз На основе этого формулируются прогнозы, которые сбываются каждый год с момента первой публикации отчета Hi-Tech Crime Trends. Они помогают компаниям во всем мире выстраивать эффективные стратегии кибербезопасности с учетом релевантных угроз.

Hi-Tech Crime Trends открывает доступ к максимально полному набору стратегических данных и подробной информации об актуальных киберугрозах в мире, как организациям, которые борются с киберпреступностью, так и потенциальным жертвам

Hi-Tech Crime Trends предназначен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инцидентов, для которых является практическим руководством стратегического и тактического планирования.

Прогнозы и рекомендации Hi-Tech Crime Trends направлены на сокращение финансовых потерь и простоев инфраструктуры, а также на принятие превентивных мер по противодействию целевым атакам, шпионажу и кибертеррористическим операциям.

Команда Group-IB убеждена в том, что постоянный обмен данными, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами – эффективный путь борьбы с киберпреступностью. Осознанное отношение к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

ВВЕДЕНИЕ 01

В прошлом году аналитики **Group-IB Threat Intelligence** впервые представили целостную картину теневой индустрии по продаже на даркнет-форумах доступов к корпоративным сетям компаний. Количество этого “товара” увеличивается ежегодно: оценка общего объема рынка продажи доступов в андеграунде является сложной задачей в силу скрытности сделок. Однако технологии Group-IB по исследованию андеграундных площадок, в том числе с учетом данных, которые пытались удалить или скрыть, позволяют экспертам компании изучать этот рынок, обмениваться данными с правоохранительными органами и оценивать масштабы этой индустрии.

Одной из наиболее явных тенденций на андеграундных форумах последних 4 лет является резкое увеличение количества предлагаемых на продажу доступов к скомпрометированным корпоративным сетям компаний.

Доступ к корпоративной сети компании может представлять собой данные учетных записей RDP, VPN, Citrix Gateway (далее просто Citrix), панели управления, веб-шелл, обратный шелл, сессию Cobalt Strike и др. Наличие доступа дает злоумышленнику возможность проникнуть в сеть компании и получить права легитимного пользователя или администратора.

Эксперты Group-IB выделяют несколько факторов, повлиявших на стремительный рост рынка продажи доступов.

Одним из них стало появление в 2017 году на андеграундных форумах хакера под псевдонимом Fxmsp. Объявления о продаже доступов к корпоративным сетям встречались в даркнете и до него, однако происходило это крайне редко и не было поставлено на поток. Fxmsp стал первым, чья деятельность была сосредоточена исключительно на получении первоначального доступа для последующей продажи.

По подсчетам исследователей команды Group-IB Threat Intelligence, прибыль Fxmsp за все время его активности могла составлять как минимум 1,5 млн долларов. При этом Fxmsp не специализировался на определенных компаниях: среди его жертв были как крупные банки и международные сети отелей, так и, например, сайты школ. Его успешный опыт вдохновил других злоумышленников. Первый и единственный на данный момент аналитический отчет **Fxmsp: «невидимый бог сети»**, посвященный инструментам и тактике этого хакера, доступен на сайте Group-IB.

Спрос рождает предложение. Этот принцип сработал и в случае с рынком продаж доступов ко взломанным сетям компаний. Еще одним фактором роста стало резкое увеличение числа атак с использованием программ-шифровальщиков с 2019 года.

Fxmsp: «невидимый бог сети»

Первым этапом для таких атак является получение доступа к сетям компаний. Деятельность продавцов доступов избавляет преступные группы, проводящие атаки с использованием шифровальщиков, от усилий на этом этапе. Как было отмечено экспертами Group-IB в отчете **«Программы-вымогатели 2020/2021»**, операторами вирусов-шифровальщиков был побит рекорд по полученным выкупам: им удалось заработать не менее 1 миллиарда долларов с 2019 по 2020 год, что сделало этот год для них самым прибыльным, мотивируя подобные преступные группы и дальше продолжать свою деятельность.

Третий фактор — низкий порог входа в эту «индустрию». Злоумышленник может получить доступ с помощью инфостиллера, в результате брутфорса или целенаправленной атаки на жертву. В сценарии с использованием инфостиллера даже не нужно думать о способе доставки этого вредоносного ПО на компьютеры жертв — результаты «работы» инфостиллеров продаются на андеграундных форумах в виде архивов, содержащих различные скомпрометированные учетные записи: как личные, так и рабочие. От злоумышленника требуется лишь отыскать среди такого набора действующие аккаунты корпоративных ресурсов. Сценарий с брутфорсом также не требует серьезных знаний — готовые программы для подбора паролей есть в открытом доступе. Атакующему нужно лишь выбрать жертву.

Доступность необходимых средств для проведения полноценной атаки на корпоративную сеть открыло для многих представителей андеграунда источник прибыли почти без риска и лишних усилий. Так рынок продаж доступов заполонили низкоквалифицированные злоумышленники, слабо ориентирующиеся в технической части, при этом представляющие угрозу для компаний.

Для такого типа атакующих (назовем их «новичками») выбор жертвы обусловлен не известностью, масштабом бизнеса или выручкой, а простотой получения к ней доступа. Примитивный принцип выбора цели для атаки подтверждает тот факт, что компрометации подвержена абсолютно любая компания независимо от ее размера и других важных для высококвалифицированных злоумышленников характеристик.

Это объясняет высокую вероятность компрометации крупных компаний со стороны даже низкоквалифицированных злоумышленников, что в контексте удаленного рабочего режима, обусловленного пандемией COVID-19, становится еще более вероятным сценарием.

Информация о компаниях, предоставляемая продавцами первичных доступов, иногда позволяет аналитикам Group-IB Threat Intelligence определить жертву еще до факта сделки по продаже доступа к ее инфраструктуре. Таким образом, сокращается время обнаружения инцидента, а в ряде случаев удается предотвратить дальнейшее развитие атаки.

В этом отчете специалистами Group-IB рассматриваются ключевые причины и этапы развития рынка продаж доступов к корпоративным сетям, приводится подробный разбор деятельности наиболее активных продавцов доступов и статистика по самым атакуемым странам и отраслям.

Программы-вымогатели 2020/2021

КЛЮЧЕВЫЕ ТРЕНДЫ

02

РОСТ КОЛИЧЕСТВА ПРОДАВЦОВ

На **205%** за период H2 2020 — H1 2021 по сравнению с H2 2019 — H1 2020.

РОСТ ПРЕДЛОЖЕНИЙ О ПРОДАЖЕ ДОСТУПОВ

На **204%** за период H2 2020 — H1 2021 по сравнению с H2 2019 — H1 2020.

ОБЩИЙ РАЗМЕР РЫНКА

В текущем периоде (H2 2020 — H1 2021) **$7 165 387**, что на 16% больше, чем за прошлый период (H2 2019 — H1 2020), когда рынок составлял **$6 189 388**.

ОСНОВНОЙ СПОСОБ ДОСТУПА В СЕТЬ КОМПАНИЙ ДЛЯ БРОКЕРОВ

Эксплуатация уязвимостей в опубликованных приложениях и компрометация учетных записей средств удаленного доступа.

СУММАРНОЕ КОЛИЧЕСТВО ПРОДАВАЕМЫХ ДОСТУПОВ

За период H2 2020 — H1 2021 составляет 1099.

СПИСОК ЛИДЕРОВ ПО ПРОДАЖАМ

35% всех доступов продается пятью брокерами.

НОВЫЕ БРОКЕРЫ

Более 200-х новых брокеров вышло на рынок за период H2 2020 — H1 2021.

ШИФРОВАЛЬЩИКИ ВСЕМ ДАЛИ РАБОТУ

Самыми активными стали следующие партнерские программы: Conti, LockBit, PYSA, Revil.

ПРОДАВАЕМЫЕ ДОСТУПЫ ПО СТРАНАМ

По прежнему остались США (30%), Франция (5%) и Великобритания (4%), однако значительно выросло количество доступов в компании Австралии (4%) и Индии (3%).

ЛИДЕРЫ ИНДУСТРИЙ

В 2020-2021 стали отрасли производства, образования, финансовых услуг, здравоохранения и торговли.

НЕ ВСЕ ДАННЫЕ ПУБЛИКУЮТСЯ НА DLS

На DLS выкладываются данные только 10% процентов атакуемых компаний.

ПРОГНОЗЫ 03

ШИФРОВАЛЬЩИКИ

Останутся основной схемой монетизации доступов

НОВАЯ ТОЧКА ВХОДА

В связи с тем, что все больше компаний переходит на единую авторизацию, то они предположительно станут новой точкой входа в сеть. Злоумышленники будут получать доступ к приложениям и сервисам, доступным через облачную авторизацию.

БРОКЕРЫ И СТОИМОСТЬ

Количество брокеров вырастет, а средняя стоимость доступа уменьшится.

НОВЫЙ РЕСУРС

Брокеры могут создать свой ресурс для проведения аукционов по продаже доступов

ИСТОРИЯ РАЗВИТИЯ РЫНКА

04

Продажа разного рода аутентификационной информации осуществлялась на андеграундных форумах с самого их возникновения, в лице форума CarderPlanet в 2001 году.

Изначально продавались данные, монетизация которых была проста и понятна. Например, банковские аккаунты, с которых выводились деньги на счета подставных лиц, или данные банковских карт, которые использовались для осуществления мошеннических транзакций.

Со временем тренды продаваемой информации менялись, так как в различных системах вводились дополнительные средства безопасности, что не позволяло злоумышленникам так же легко монетизировать скомпрометированные данные.

Доступы к удаленным устройствам появились на черном рынке в начале 2000-х и представляли собой доступы к отдельным серверам за относительно небольшую плату, причем обычно это были шеллы на веб-сайтах или доступ к FTP.

Ниже и далее по тексту мы будем использовать исторические данные и скриншоты, сохраненные нашей системой **Group-IB Threat Intelligence & Attribution**.

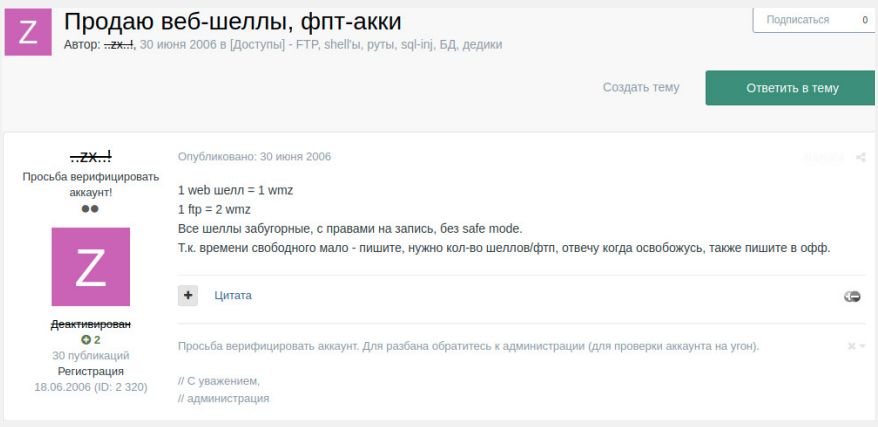


Рис. 1. Пример объявления о продаже веб-шеллов и доступов через FTP

Во второй половине 2000-х стали появляться продажи «сбрученных» удаленных доступов к выделенным серверам из разных стран, которые приобретались в основном для ведения мошеннической деятельности.

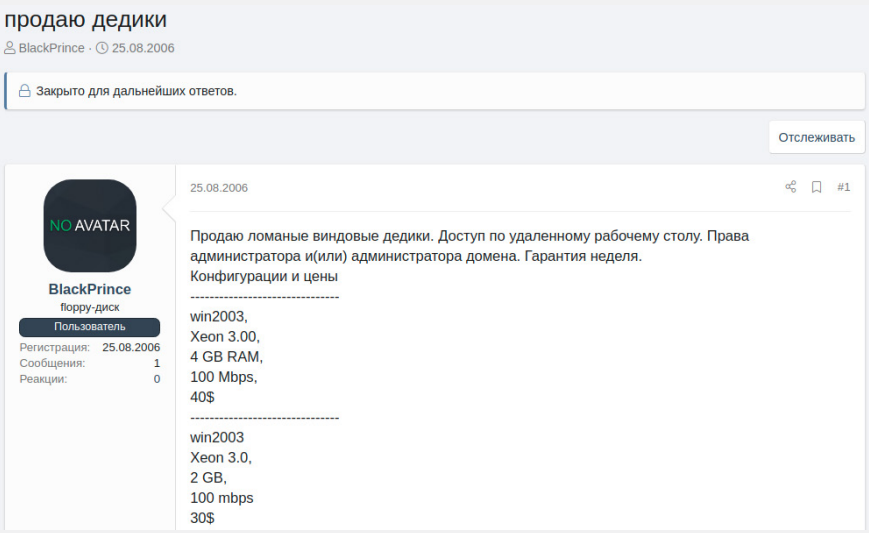


Рис. 2. Пример объявления о продаже доступа к выделенным серверам

Характерной особенностью того времени было то, что злоумышленники после нахождения каких-либо серверов и получения к ним доступа не проводили дополнительного исследования и, следовательно, не осознавали, что скомпрометированные серверы могли принадлежать крупным компаниям, и их можно было бы выгодно монетизировать.

На тот момент основную ценность для злоумышленников представляли вычислительные мощности скомпрометированных серверов, объем доступной на них памяти и полоса пропускания для интернет-трафика.

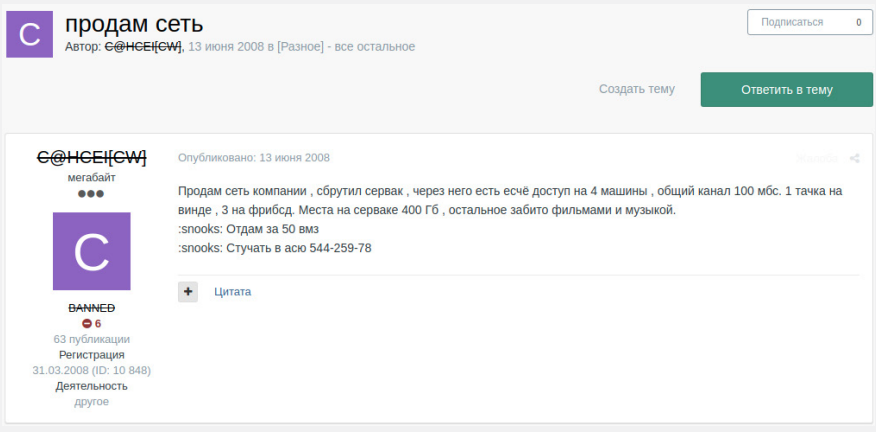


Рис. 3. Пример объявления о продаже доступа к серверу с указанием технических характеристик

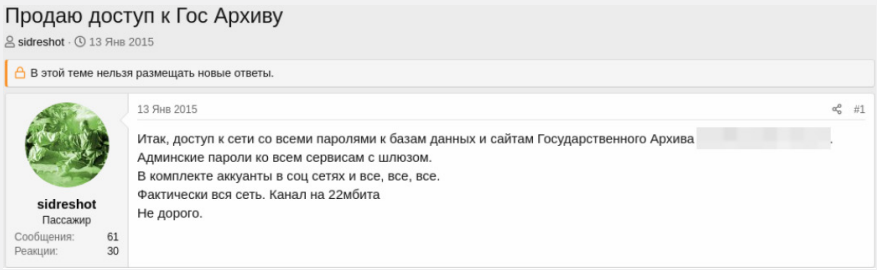
Значительно позже, ближе ко второй половине 2010-х годов, для злоумышленников стала представлять интерес информация, находящаяся на серверах.

Однако не всегда тот, кто её заполучил, знает, как ее использовать. Такая ситуация характерна для случаев, когда злоумышленник ставит своей целью получение доступа не к определенному объекту, а выбирает жертву, для взлома которой достаточно небольшого набора навыков и начальных знаний о возможных уязвимостях.

Тем не менее, именно смещение фокуса на имеющуюся на сервере информацию стало толчком к исследованию — кому же принадлежит скомпрометированное устройство.

Интересно, что несмотря на технически одинаковый механизм доступов, их описание в темах о продаже на форумах менялось вместе с представлениями о монетизации. Если в 2005-2014 годах самым распространенным названием являлось “Продам дедик”, то начиная с 2015 года подобные темы чаще называются “Продам доступ к сети” или “Продам доступ к компании”. Злоумышленники начинают ставить в приоритет не технические возможности сервера, к которому им удалось получить доступ, а то, кому этот сервер принадлежит, какую информацию содержит.

В начале развития рынка продажи доступов злоумышленники зачастую не могли понять, как можно монетизировать захваченную информацию.


Продаю доступ к Гос Архиву

sidreshot · 13 Янв 2015

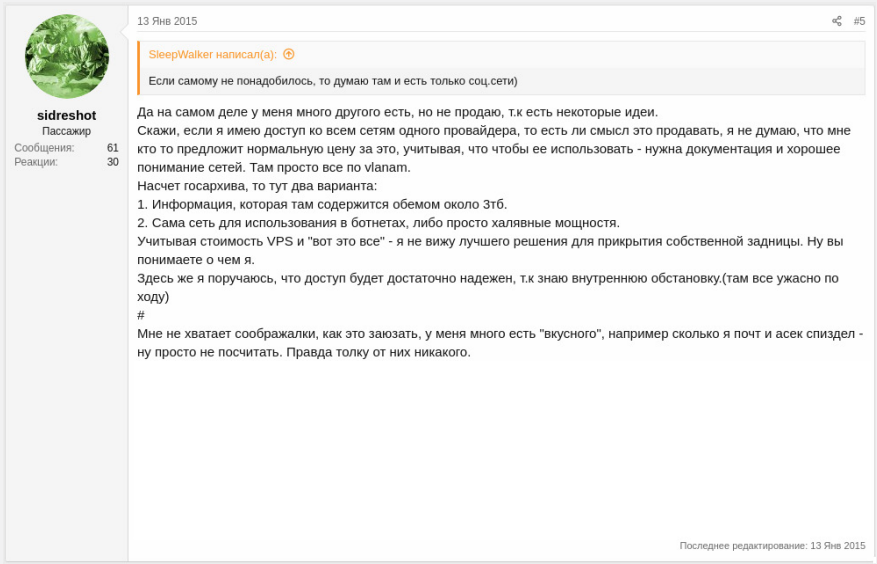
В этой теме нельзя размещать новые ответы.

13 Янв 2015 #1

Итак, доступ к сети со всеми паролями к базам данных и сайтам Государственного Архива [redacted].
Адмиские пароли ко всем сервисам с шлюзом.
В комплекте аккуанты в соц сетях и все, все, все.
Фактически вся сеть. Канал на 22мбита
Не дорого.

sidreshot
Пассажир
Сообщения: 61
Реакции: 30

Рис. 4. Объявление пользователя sidreshot на форуме Rutor


13 Янв 2015 #5

SleepWalker написал(а):

Если самому не понадобилось, то думаю там и есть только соц.сети)

Да на самом деле у меня много другого есть, но не продаю, т.к есть некоторые идеи.
Скажи, если я имею доступ ко всем сетям одного провайдера, то есть ли смысл это продавать, я не думаю, что мне кто то предложит нормальную цену за это, учитывая, что чтобы ее использовать - нужна документация и хорошее понимание сетей. Там просто все по vlanam.
Насчет госархива, то тут два варианта:
1. Информация, которая там содержится обемом около 3тб.
2. Сама сеть для использования в ботнетах, либо просто халявные мощностя.
Учитывая стоимость VPS и "вот это все" - я не вижу лучшего решения для прикрытия собственной задницы. Ну вы понимаете о чем я.
Здесь же я поручаюсь, что доступ будет достаточно надежен, т.к знаю внутреннюю обстановку.(там все ужасно по ходу)
#
Мне не хватает соображалки, как это заюзать, у меня много есть "вкусного", например сколько я почт и асек спиздел - ну просто не посчитать. Правда толку от них никакого.

sidreshot
Пассажир
Сообщения: 61
Реакции: 30

Последнее редактирование: 13 Янв 2015

Рис. 5. Комментарий злоумышленника о поиске способа монетизации доступов

Отсутствие идей о монетизации в свою очередь вызывало трудности и с определением стоимости доступов. В примере ниже злоумышленник пытается выяснить это у других пользователей форума.

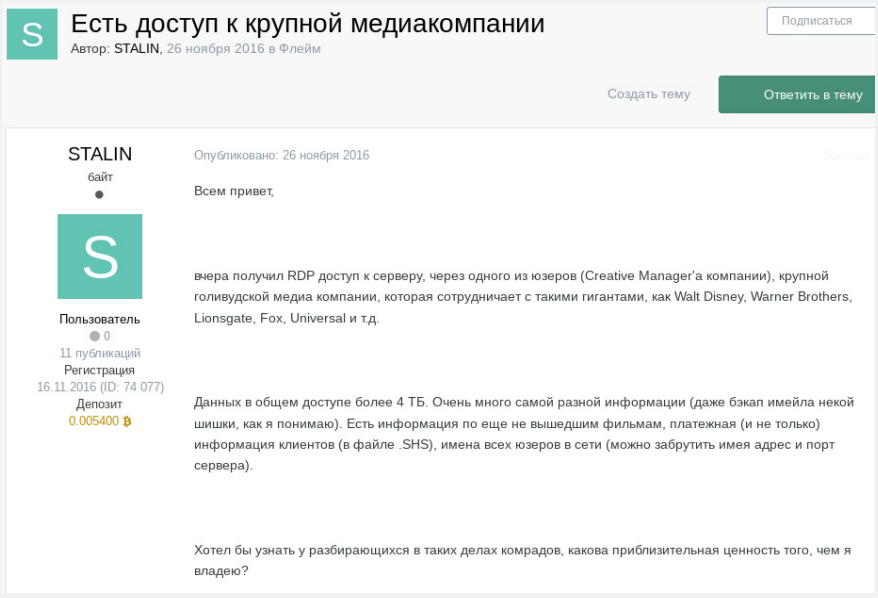


Рис. 6. Сообщение пользователя STALIN на форуме Exploit

Один из вариантов, что приходил на ум злоумышленнику, завладевшему RDP-доступом — это атака с использованием методов социальной инженерии. Ниже пример объявления, датированный 2016-м годом.

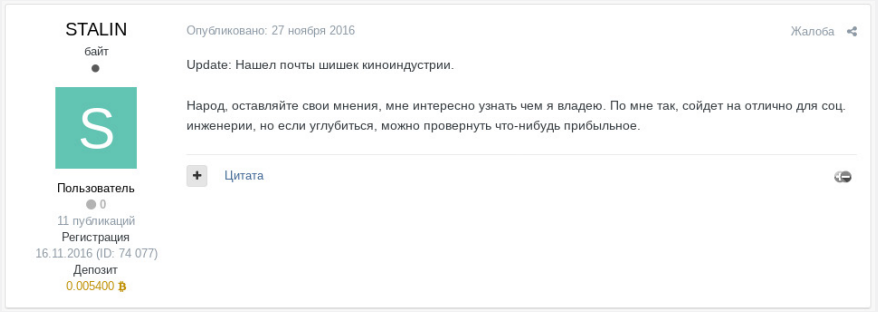


Рис. 7. Комментарий пользователя STALIN на форуме Exploit

Хотя стоит заметить, что уже тогда на андеграундных форумах появились идеи, ставшие реальностью, в которой мы сейчас живем: один из пользователей форума оставил шуточный комментарий, предложив загрузить в сеть компании шифровальщик. Очевидно, тогда никто не представлял, что альянс продавцов доступов и операторов программ-шифровальщиков станет одним из самых опасных и прибыльных в истории киберпреступности.

Рис. 8. Комментарий пользователя stack.kuku на форуме Exploit

Попытки продаж доступов к корпоративным сетям встречались, однако они не были поставлены на поток, являясь разовыми предложениями. Вместе с подобными темами появлялись идеи о монетизации, большинство из которых, в силу типа доступа, были применимы и к веб-шеллам, предлагаемым на форумах с момента их создания.

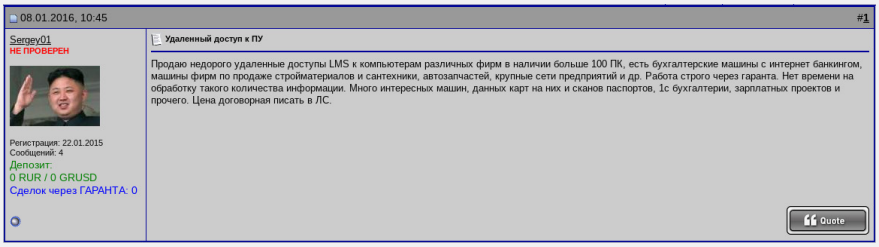


Рис. 9. Пример продажи доступа в 2016 году

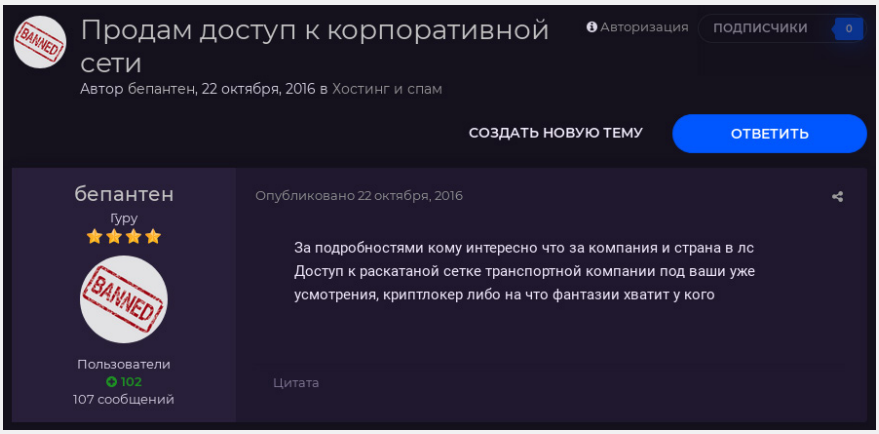


Рис. 10. Продажа доступа к корпоративной сети в 2016 году

В 2017 году ситуация изменилась: появились злоумышленники, чья деятельность была сосредоточена исключительно на продаже доступов к корпоративным сетям. Одним из самых известных хакеров, положившим начало продаже доступов, был **Fxmsp**.

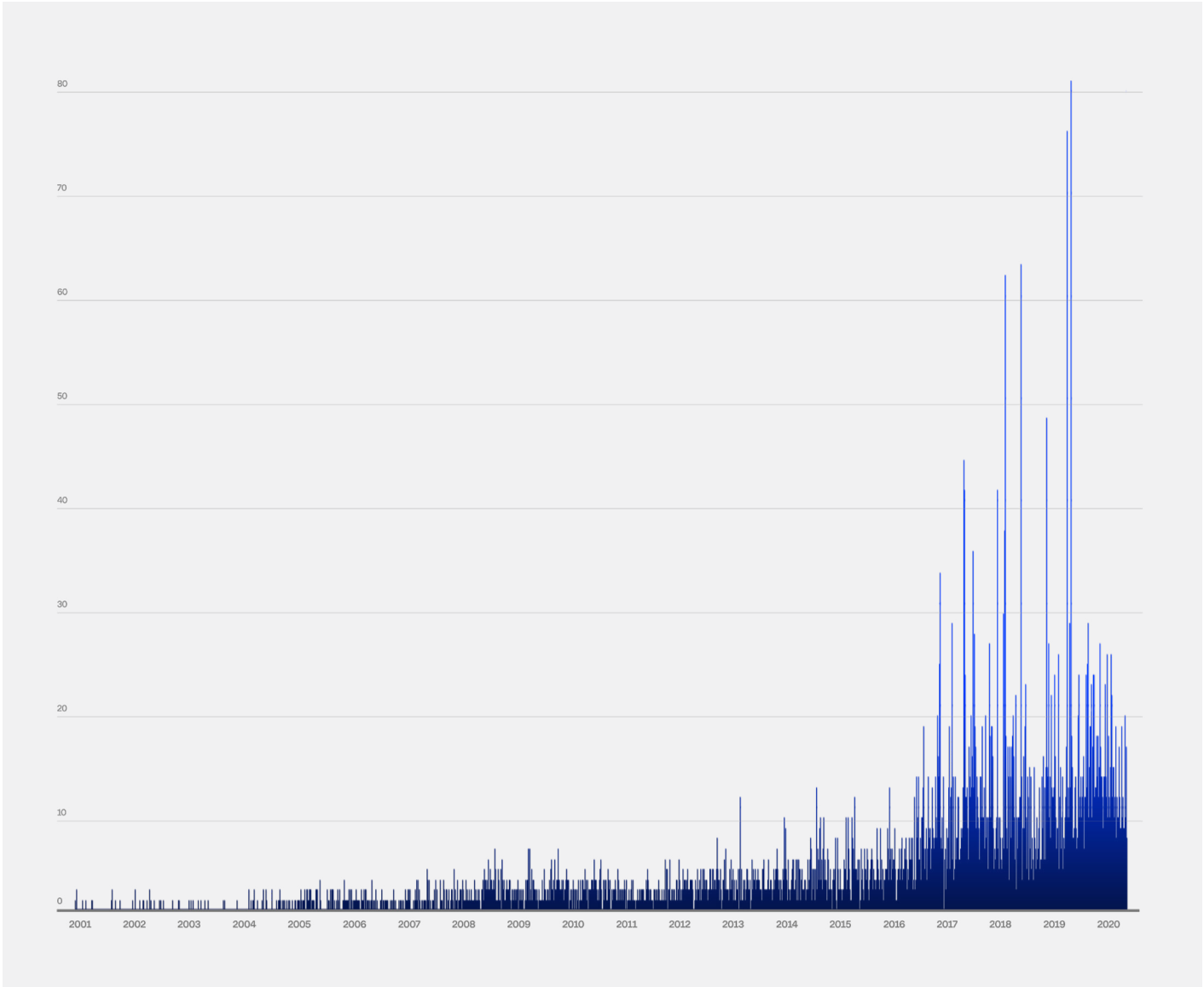
Fxmsp: «невидимый бог сети» ↗

КАК FXMSP ИЗМЕНИЛ РЫНОК ДОСТУПОВ

05

До появления на рынке Fxmsp количество предложений о продаже доступов было устойчивым и не превышало 10 объявлений за 2015-2016 год. Эта цифра сохранялась и до октября 2017 года. Начиная с этого момента, наблюдается экспоненциальный рост предложений о продаже доступов к корпоративным сетям на андеграундных форумах.

Рис. 11. Распределение количества объявлений о продаже доступов по годам



В октябре 2017 года на самом известном русскоязычном андеграундном форуме **Exploit** появилось объявление о продаже доступа к корпоративным сетям ряда компаний. Его автор впервые предложил доступ ко всем критически важным сегментам сетей скомпрометированных им организаций и заявил, что среди его жертв есть банк — уникальный по меркам того времени лот.

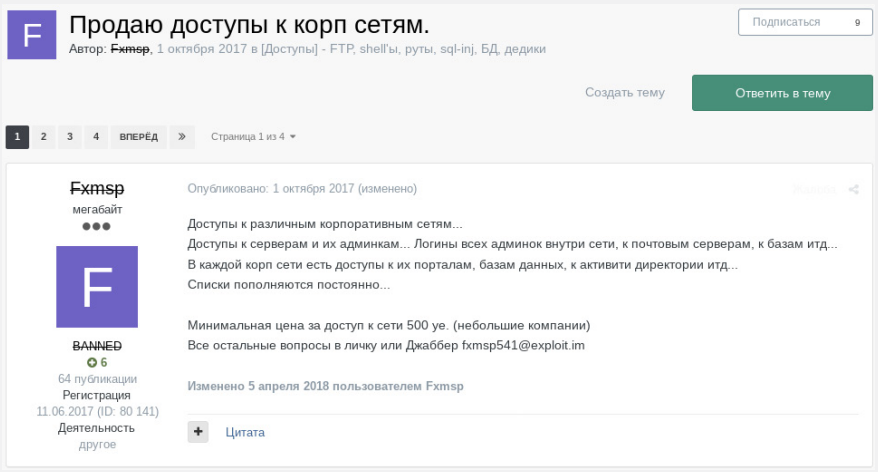


Рис. 12. Первое объявление Fxmsp о продаже доступов на форуме Exploit

С самого начала своей деятельности Fxmsp понял, что отсутствие конкретного представления о жертве значительно снижает спрос и, как следствие, увеличивает время реализации.

Уже через неделю после публикации своего первого поста, в котором отсутствовали какие-либо конкретные детали о жертвах, он оставил сообщение, где явно указал название компании, к которой предлагал доступ. Это был 2017-й год, который можно назвать переломным для индустрии продажи доступов в скомпрометированные сети компаний.

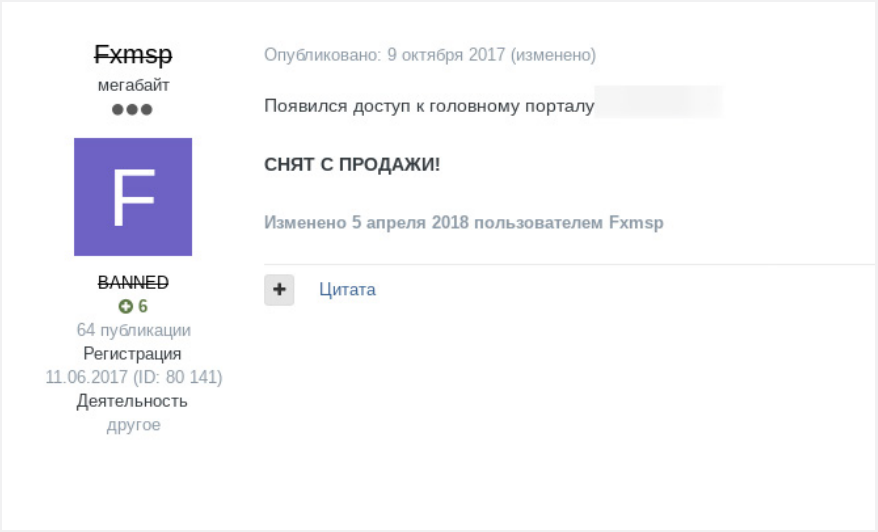


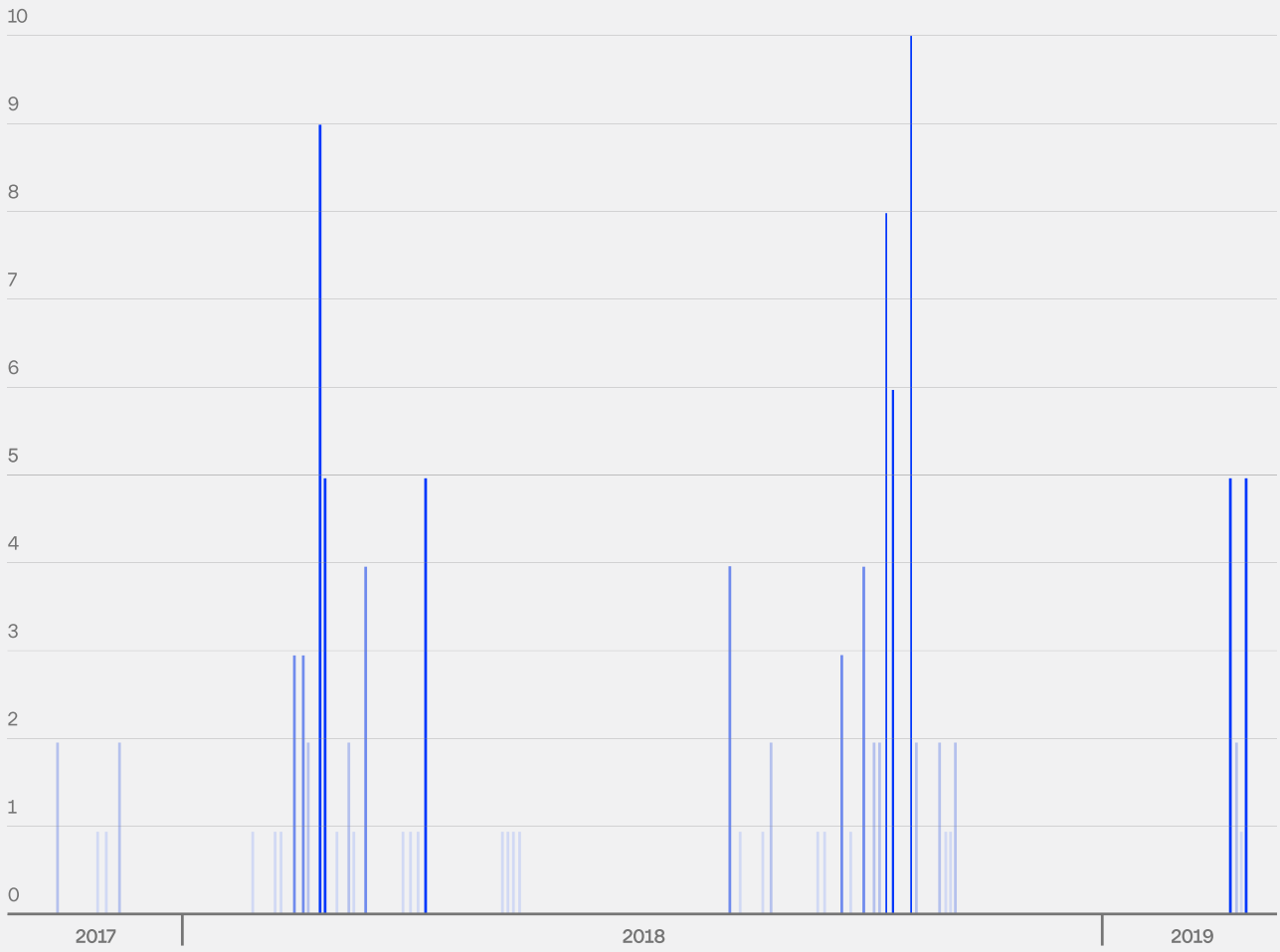
Рис. 13. Объявление Fxmsp о продаже доступа с указанием названия жертвы

Явное указание жертв сохранялось на протяжении всего периода активности Fxmsp.

Специалистами Group-IB была проанализирована преступная деятельность Fxmsp с момента его регистрации на первом андеграундном форуме в сентябре 2016 года до фактического прекращения его активности в конце 2019 года. Подробнее она представлена в отчете “Fxmsp: невидимый бог сети”.

За всю историю активности злоумышленником было выставлено 135 объявлений о продаже доступов к корпоративным сетям на сумму как минимум 1,5 миллиона долларов. На рисунке ниже представлен таймлайн публикаций Fxmsp о продаже доступов к сетям на андеграундных ресурсах.

Рис. 14. Таймлайн публикаций Fxmsp на андеграундных форумах



В конце октября 2018 года деятельность Fxmsp оказывается под угрозой. Выясняется, что они вместе с сообщником — менеджером по продажам под псевдонимом Lampeduza — пытались продавать доступ к одной и той же сети разным людям. 24 октября того года оба пользователя были заблокированы на основном андеграундном ресурсе. Группа замораживает активность на всех остальных форумах и предположительно уходит в «приват», то есть начинает работать только с ограниченным кругом доверенных клиентов. Однако пример эффективной работы злоумышленника сподвигает огромное количество хакеров начать похожий «бизнес».

В 2018 году на андеграундном форуме Exploit начинают активно появляться новые темы о продаже доступов к корпоративным сетям, принадлежащие другим пользователям.

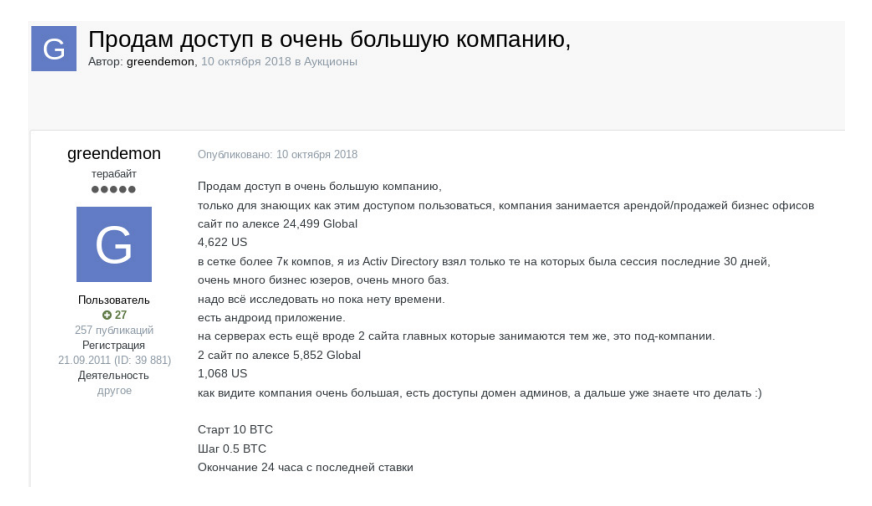


Рис. 15. Объявление о продаже доступа к крупной компании на форуме Exploit в 2018 году

В 2018 году системой Group-IB Threat Intelligence & Attribution была зафиксирована 141 тема о продаже доступов, 98 из которых принадлежат Fxmsp и его менеджеру по продажам Lampeduza.

Спустя год общее количество подобных тем оставалось на таком же уровне, однако “вес” доступов, предоставляемых Fxmsp значительно сократился: сам он не разместил на форумах ни одного объявления, а Lampeduza опубликовал всего лишь 22 вместо 65 годом ранее.

Статистика по основным продавцам доступов за 2018 год

Название	%
Lampeduza	47
Fxmsp	23
BartSimpson	1
x999xx	1
Jendely	2
jabber	2
raf	2
Другие	22

Статистика по основным продавцам доступов за 2019 год

Название	%
Lampeduza	18
Network	15
B.Wanted	15
toon1c3	2
streetskip	3
greendemon	3
nikolaruss	3
x999xx	4
SilvioBerlusconi	4
bc.monster	7
Другие	28

Из двух диаграмм выше видно, что если в 2018 году абсолютными лидерами рынка являлись Fxmsp и Lampeduza, оставляя далеко позади конкурентов, то уже в 2019 появились злоумышленники, готовые предложить объем доступов, сравнимый с тем, который предлагали некогда ведущие продавцы.

Тем не менее, именно Fxmsp и Lampeduza сформировали рынок доступов к корпоративным сетям в том виде, в котором мы видим его сейчас. Fxmsp создал представление об отдельном виде злоумышленников в андеграунде — продавцах первоначальных доступов к корпоративным сетям. Став первопроходцем, он своим примером показал другим злоумышленникам способы реализации полученных доступов и заработка на черном рынке.

Доподлинно неизвестно, продолжает ли злоумышленник Fxmsp вести свою нелегальную деятельность.

В ходе исследования его деятельности специалистами Group-IB были выявлены инструменты, которые он использовал для компрометации компаний. В нашем отчете об Fxmsp мы впервые раскрыли детали личности этого хакера, а также дали рекомендации, позволяющие защититься от подобных атак.

ВЛИЯНИЕ RANSOM-WARE-AS-A-SERVICE НА РЫНОК

06

Если раньше продавцы доступов указывали количество хостов в скомпрометированной сети и их характеристики или делали упор на большие объемы имеющихся в сети данных, то с ростом популярности атак с использованием шифровальщиков подобная информация перестала привлекать покупателей. Ниже представлен пример объявления о продаже доступа, когда Ransomware-as-a-Service (RaaS), как модель продаж, не была столь популярна как сейчас.

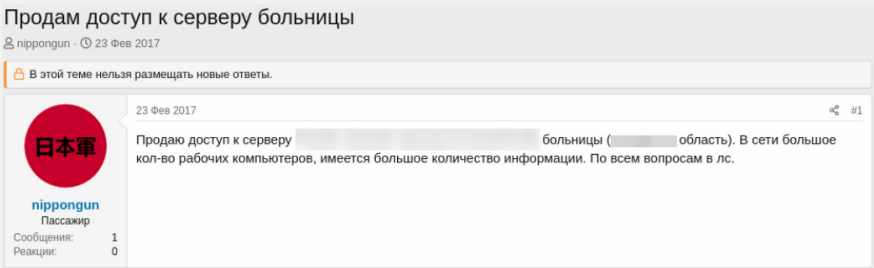


Рис. 16. Объявление пользователя nippongun на форуме Rutor в 2017 году

При получении доступа злоумышленники начинают выяснять информацию о жертве с целью определения цены, за которую они его в дальнейшем предлагают на рынке. На цену влияют следующие характеристики компании:

- выручка;
- известность;
- индустрия;
- масштаб бизнеса.

Наличие этой информации привлекает больше внимания и, как следствие, помогает быстрее найти покупателя, сократив время продажи лота.

Ниже представлен пример темы о продаже доступа, опубликованной во время зарождающейся популярности Ransomware-as-a-Service (RaaS).

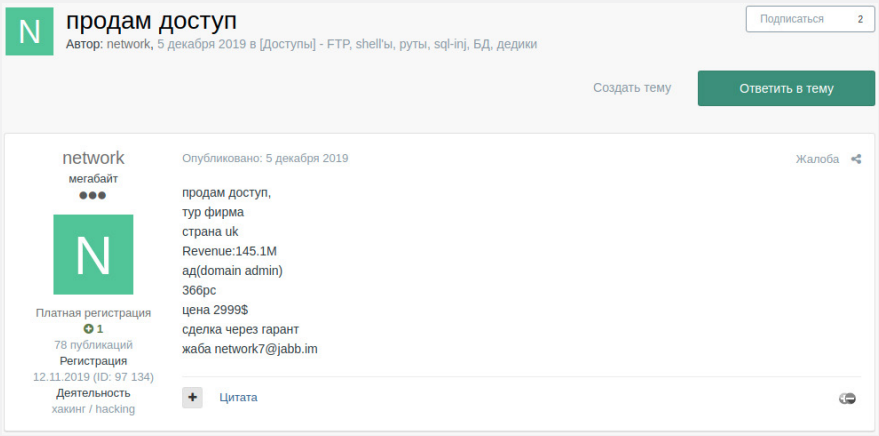


Рис. 17. Объявление пользователя network в 2019 году

Информация о выручке компании является определяющим фактором для преступных групп, проводящих атаки с использованием шифровальщиков, позволяющая им определить сумму запрашиваемого выкупа.

Как правило, особой популярностью среди покупателей пользуются доступы в сети компаний с наибольшей выручкой. В примере ниже пользователь с псевдонимом babam выставил на продажу доступ к корпоративной сети одного из крупных банков с выручкой более 30 миллиардов долларов.

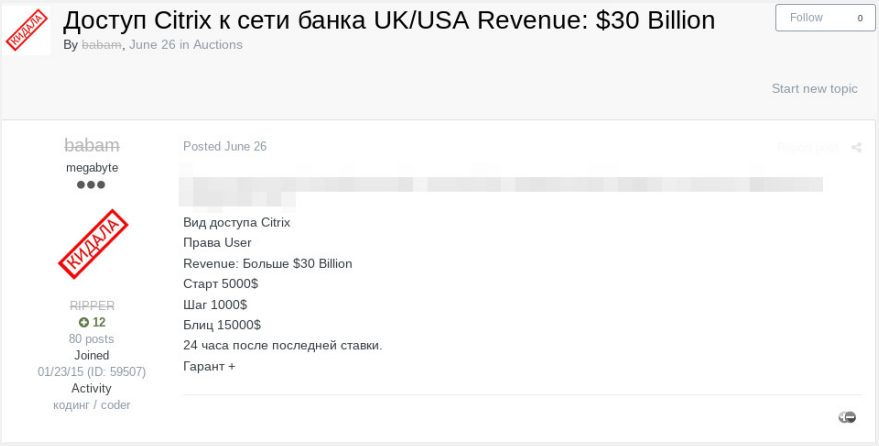


Рис. 18. Объявление пользователя babam о продаже Citrix доступа к крупному банку

Спустя несколько часов после публикации в теме уже появилось сообщение от заинтересовавшегося покупателя, после которого лот был выкуплен.

Какие доступы покупают операторы программ-шифровальщиков

Значимым критерием в выборе жертвы является ее известность. После заражения сети шифровальщиком, компанию шантажируют публикацией в открытом доступе всех данных, находящихся в корпоративной сети, при отказе платить выкуп. Такой исход грозит репутационным ущербом для жертвы, а в случае широкой известности компании атака на нее может стать причиной полного прекращения ее дальнейшей деятельности.

Такие характеристики жертвы, как индустрия и масштаб бизнеса, также играют не последнюю роль для злоумышленников, использующих RaaS. Они позволяют сделать предположение об известности и выручке компании и поэтому часто появляются в объявлениях о продаже. Более того, индустрия, в которой работает компания, позволяет атакующим предположить, какими данными они могут завладеть в случае получения доступа.

Учитывая эти особенности, преступные группы оценивают целесообразность атаки с точки зрения удовлетворения собственных финансовых амбиций.

Важным фактором ценообразования и скорости продажи доступа является уровень доступа: чем он выше, тем дороже будет предложение. Ниже представлен пример темы о продаже доступа с правами администратора домена к итальянской фармацевтической компании.

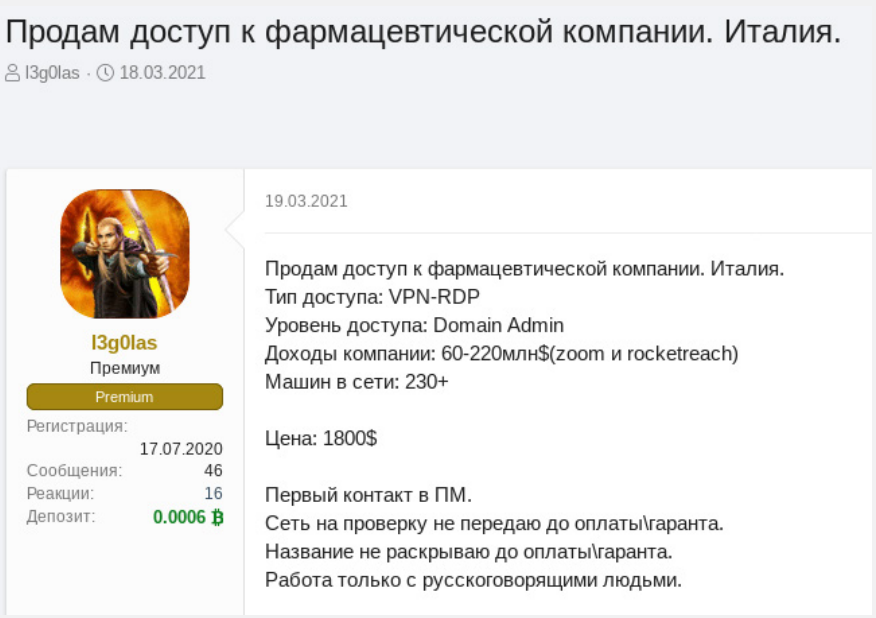


Рис. 19. Объявление о продаже доступа к итальянской фармацевтической компании

Уровень доступа с правами администратора домена предоставляет все имеющиеся привилегии: злоумышленник получает доступ ко всей информации в сети и может управлять другими учетными записями. Наличие этих двух слов (Domain Admin) в объявлении означает для злоумышленника, планирующего приобрести этот доступ, что у него не возникнет трудностей с кражей информации из сети или запуском

ВПО, и от цели его отделяет лишь стоимость доступа, которая с большой долей вероятности окупится.

Иногда злоумышленники прямо указывают компанию, к которой продают доступ. На скриншоте ниже тема о продаже доступа к медицинской организации из ОАЭ.

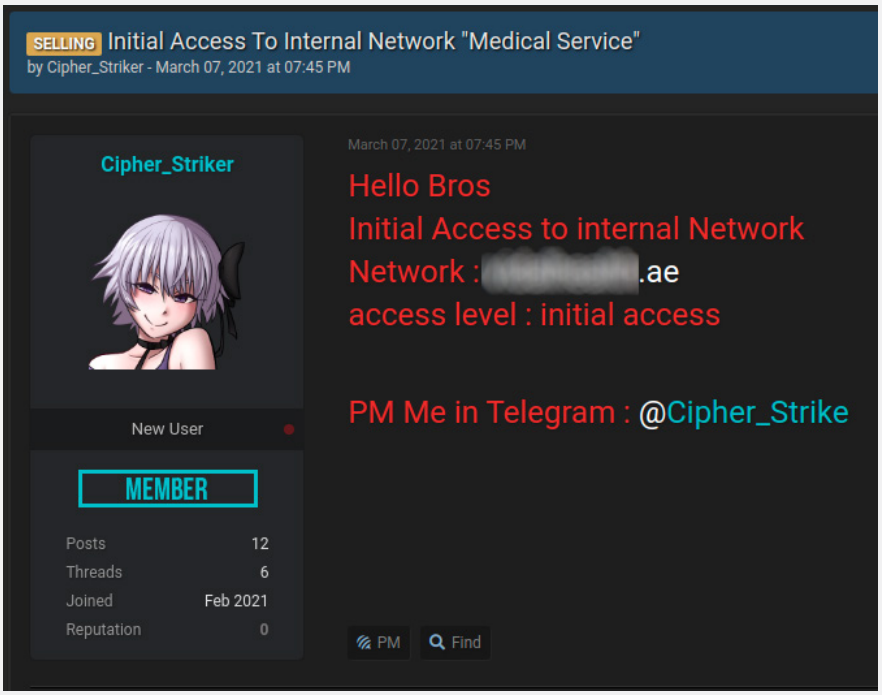


Рис. 20. Объявление о продаже доступа к медицинской организации из ОАЭ

Однако такой подход к публикации объявлений опасен для злоумышленников тем, что исследователи безопасности оповестят компанию-жертву о продаже доступа к ней, в результате чего он будет закрыт. Поэтому большинство продавцов предпочитает указывать ключевую информацию о скомпрометированной компании (годовой доход, тип доступа, страну, индустрию) без указания бренда.

В некоторых случаях продавцы доступов приводят описание с официальных сайтов или операторов баз данных для бизнес-клиентов.

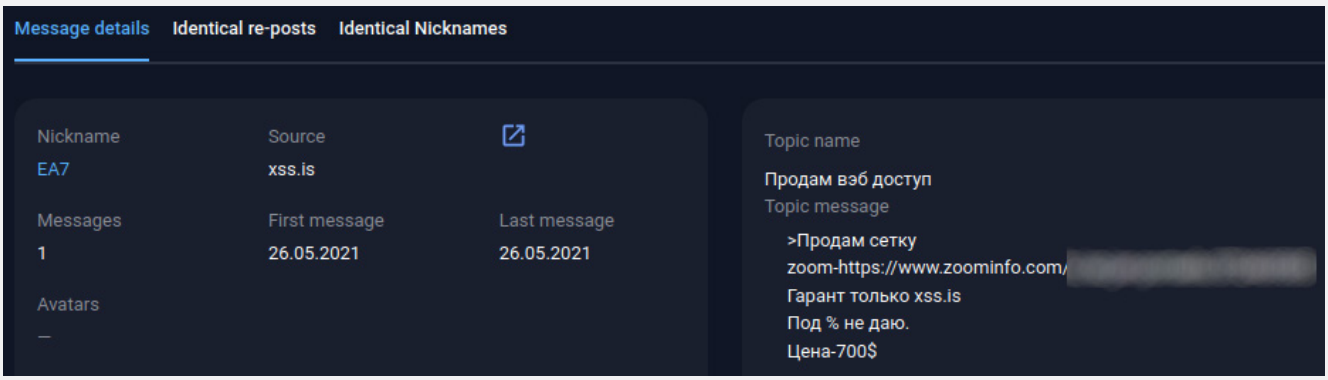


Рис. 21. Объявление о продаже доступа к медицинской организации из Бельгии

Zoominfo предоставляет информацию о компаниях из своей базы данных. Как показано на скриншоте ниже, все важные характеристики для принятия решения о покупке доступа указаны на сайте.

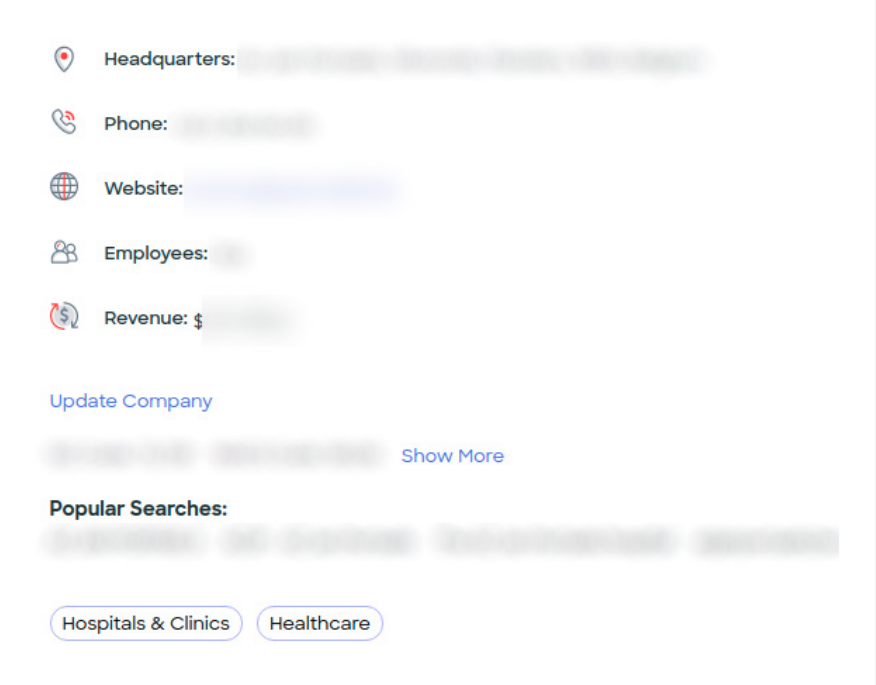


Рис. 22. Пример информации о компании на сайте zoominfo.com

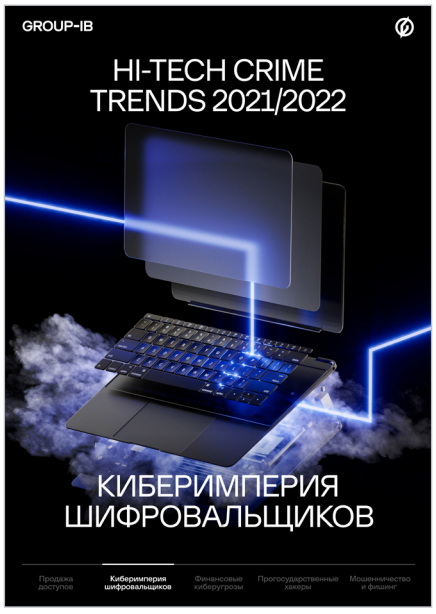
С начала 2020 года существенно выросло количество партнерских программ операторов различных программ-шифровальщиков. Причиной роста послужила пандемия, в результате которой многие компании были вынуждены изменить свою инфраструктуру для организации удаленной работы сотрудников. Подробное описание текущих трендов программ-вымогателей можно найти в нашем отчете «**Киберимперия шифровальщиков**».

Во многих случаях развертывание программ-вымогателей начинается с установки соединения по RDP со скомпрометированным сервером. После чего атакующие продвигаются по сети к одному из контроллеров домена. Публично доступные RDP-серверы являются наиболее частой мишенью для многих операторов программ-вымогателей, что в свою очередь увеличивает интерес к продажам RDP-доступов к корпоративным сетям.

RDP-доступ к серверам — не единственная точка входа, в отношении которой операторы шифровальщиков применяют брутфорс-атаку. Этот способ используется также в отношении VPN-сервисов, если не была внедрена мультифакторная аутентификация.

Рост популярности программ-шифровальщиков повлек за собой рост количества продавцов доступов к корпоративным сетям. Это привело к отсутствию необходимости у операторов вымогателей или участников партнерских программ самим искать уязвимости в инфраструктуре компании, поскольку они могли просто приобрести доступ к интересующей сети у третьих лиц. Нередко подобные объявления о скупке доступов к сети можно встретить на андеграундных форумах.

Киберимперия шифровальщиков



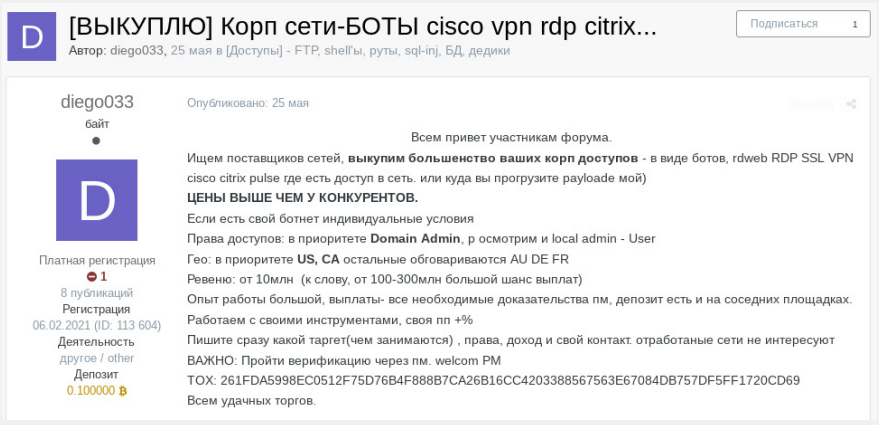
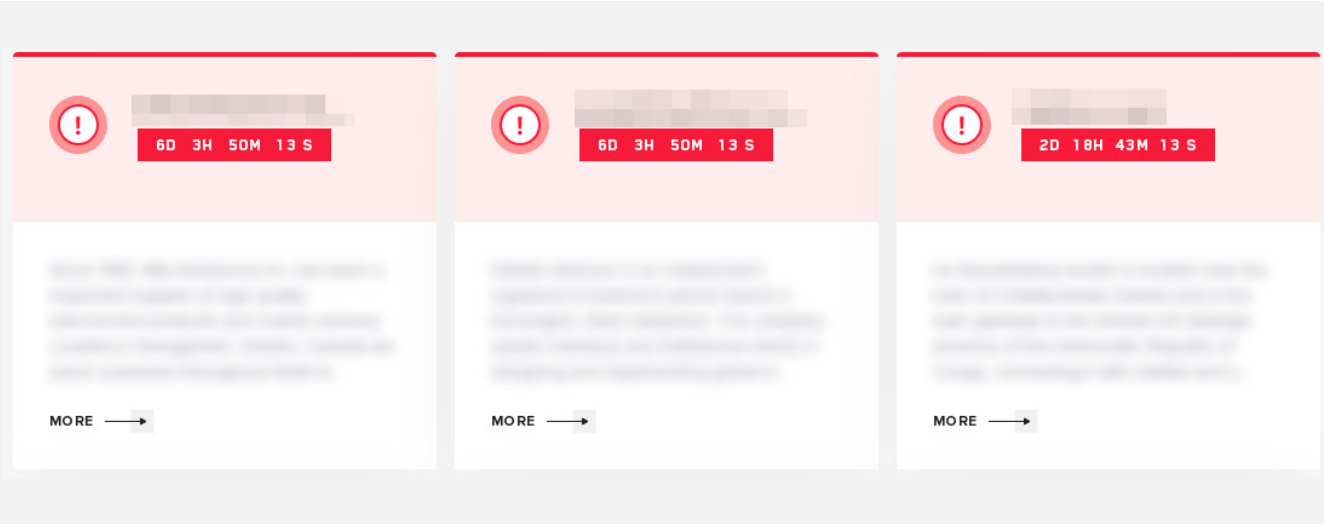


Рис. 23. Объявление о скупке доступов на форуме Exploit

Основная цель операторов программ-вымогателей — получение выкупа за расшифровку данных. Поэтому, помимо непосредственного шифрования данных, главной целью становилось уничтожение резервных копий критически важных данных, чтобы лишить жертву возможности восстановить их. С учетом этого факта, большинство программ-вымогателей обладает возможностями отключения или удаления функций восстановления системы.

В качестве методов “устрашения” компаний-жертв многие операторы вирусов-шифровальщиков создали собственные DLS-сайты, на которых они периодически публикуют скомпрометированные данные атакованных компаний.

Рис. 24. DLS-сайт операторов вируса-шифровальщика Lockbit

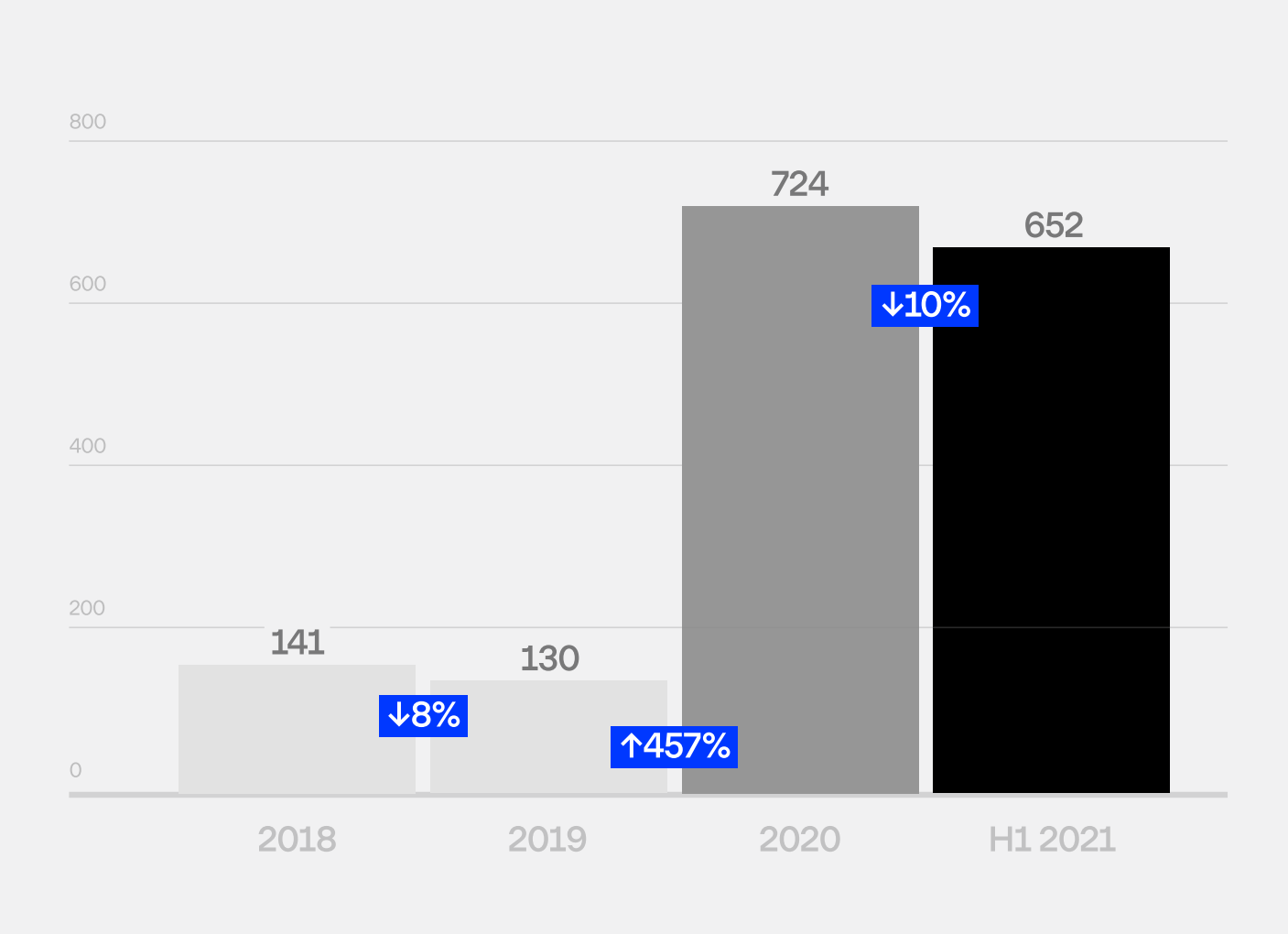


Поскольку у каждой группы, управляющей программой-шифровальщиком, может быть несколько партнеров, то тактика, техники и процедуры разных злоумышленников, использующих одни и те же шифровальщики, могут отличаться. Специалистами Group-IB было проведено подробное исследование вирусов-шифровальщиков “Программы-вымогатели 2020/2021”, опубликованное в марте 2021 года. В нем приводится разбор основных техник и тактик, а также рекомендации по предотвращению угроз от вирусов-шифровальщиков.

Таким образом, партнерские программы шифровальщиков сформировали спрос на доступы к корпоративным сетям, тем самым создав мотивацию для брокеров первоначальных доступов и дальше развивать свою деятельность.

Всего за период с начала 2018 года до середины 2021 года на продажу было выставлено 1 647 доступов. Из них большая часть — 1099 доступов — предлагалась за последний год (H2 2020 — H1 2021). Ниже представлена статистика количества продаваемых доступов начиная с 2018 года.

Рис. 25. График продажи доступов

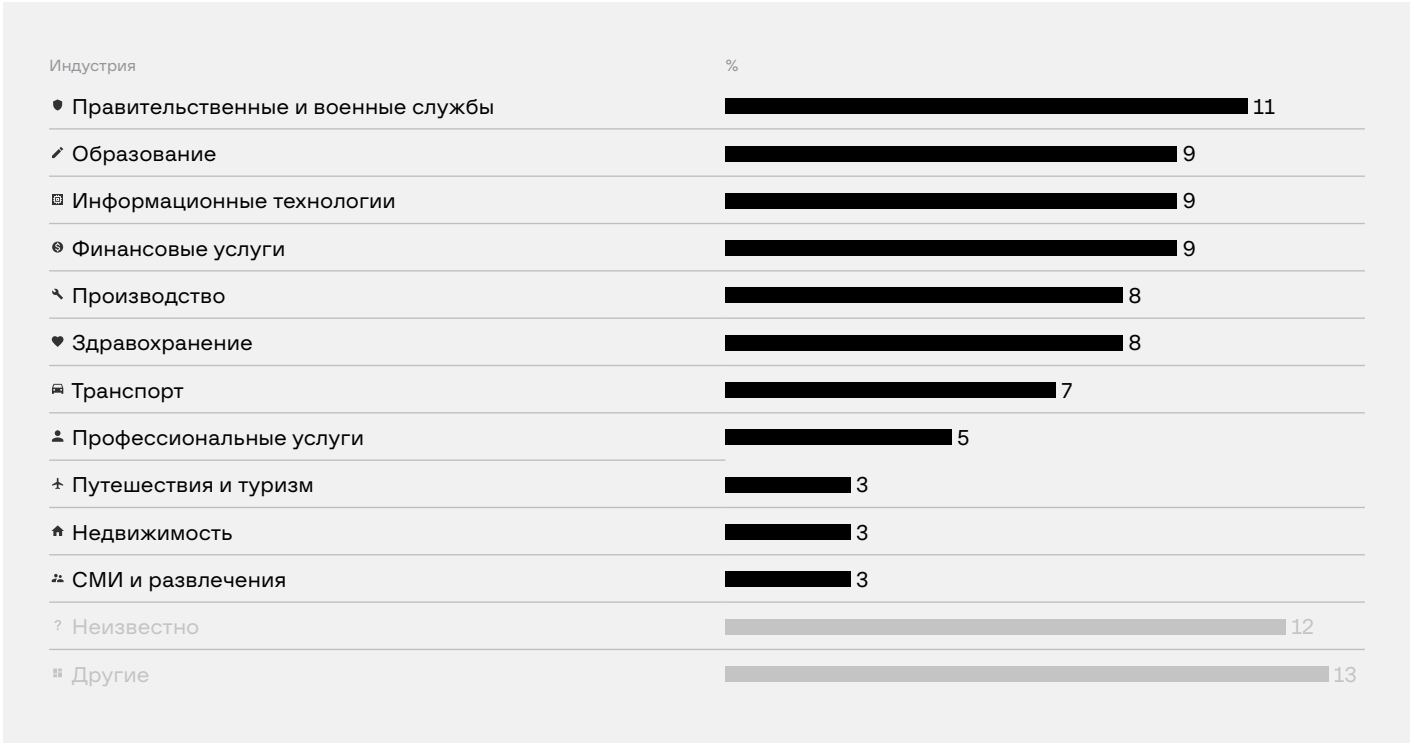


Снижение доли предложений Fxmsp и еще не достигшая уверенного роста популярность рынка доступов незначительно сократили количество продаж в 2019 году (130 доступов) по сравнению с 2018 годом (141 доступ). Однако уже через год количество объявлений о продаже доступов увеличилось в 5,5 раз (724 доступа за 2020 год). За первое полугодие 2021 года на форумах было предложено немногим меньше — 652 доступа.

Данный раздел содержит анализ рынка первичных доступов к корпоративным сетям компаний, обнаруженных на киберпреступных форумах за последние 2 года.

С момента возникновения рынка доступов среди всех известных отраслей не осталось практически ни одной, доступ к которой не продавался бы на черном рынке.

Ниже приведена статистика по отраслям компаний, к которым продавались доступы в период со 2-й половины 2019 по 1-ую половину 2020 года.



Продавцы доступов указывают минимальное количество данных в объявлениях с целью заинтересовать покупателей, но при этом скрыть определяющую информацию о жертве. Зачастую публикуется только информация о выручке компании и стране, в которой она находится. Отрасль работы компании обычно не указывается или описывается так, что можно определить лишь, является ли она государственной или коммерческой. По этой причине категория “Неизвестно” в сравнении с другими составляет 12%. Такая же цифра характерна для категории “Другое” — это общее количество доступов к компаниям других отраслей, не представленных на диаграмме, каждая из которых в отдельности составляет не более 2% от общего количества доступов, продаваемых за период H2 2019 — H1 2020. Примеры таких отраслей — компании, занимающиеся благотворительностью, спортивные и игровые организации.

Всего за это время на продажу было выставлено 362 доступа, а самыми продаваемыми были доступы к государственным и военным службам.

Спустя год ситуация значительно изменилась: общее количество доступов, выставленных на продажу со 2-ой половины 2020 по 1-ую половину 2021 года, составило 1099, что почти в 3 раза больше, чем за предыдущий период.

Ниже представлена статистика по отраслям компаний, к которым продавались доступы в период со 2-й половины 2020 по 1-ую половину 2021 года.

Индустрия	%
Производство	9
Образование	9
Финансовые услуги	9
Торговля	7
Здравохранение	7
Профессиональные услуги	6
Информационные технологии	5
Правительственные и военные службы	5
Транспорт	5
Природные ресурсы	5
Недвижимость	4
Неизвестно	11
Другие	18

Лидерами среди самых продаваемых доступов стали отрасли производства, образования и финансовых услуг, сместив доступы к сетям государственных и военных служб на 4 место. Стоит отметить, что ввиду увеличения общего количества продаваемых доступов, снижение процентного соотношения для отрасли не говорит о снижении продаваемых к ней доступов — их число также увеличилось.

О том, что до сих пор злоумышленники не осознавали весь спектр возможных жертв, говорит значительно увеличившееся число затронутых областей: если год назад в даркнете можно было найти доступы к компаниям 20 отраслей, то на сегодняшний момент их уже 35.

Ситуация изменилась и в отношении атакованных стран. На диаграмме ниже представлена статистика по странам, в которых зарегистрированы компании, доступы к которым продавались в период H2 2019 — H1 2020.

Страна	%
США	33
Франция	5
Великобритания	5
Италия	4
Канада	3
Австралия	2
Китай	2
Другие	23
Неизвестно	23

США лидировали по количеству компаний, подвергшихся атакам. Однако немалый процент продаваемых на тот момент доступов невозможно отнести ни к одной из стран. Большой процент доступов, для которых неизвестно местоположение жертвы, обусловлен наличием объявлений, в которых злоумышленники предоставляют ограниченные сведения. Ниже представлен пример подобного объявления.

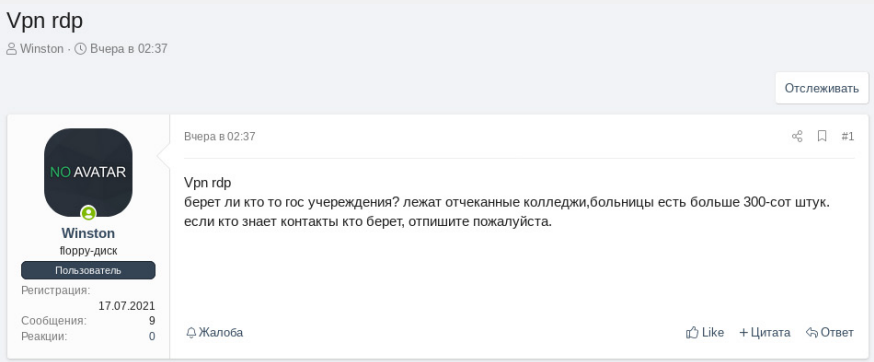


Рис. 26. Объявление о продаже доступов к различным учреждениям

Учесть информацию из такого описания в статистике сложно, но можно предположить, что это небольшие организации с невысоким доходом. Так как первичные доступы к крупным организациям продаются обычно отдельно и за большую цену.

Ниже представлена аналогичная статистика за период H2 2020 — H1 2021.

Страна	%
США	30
Франция	5
Великобритания	4
Австралия	4
Италия	3
Индия	3
Канада	3
Другие	30
Неизвестно	18

Спустя год США по-прежнему сохранили свою лидирующую позицию, и хотя их доля стала меньше, увеличение общего количества доступов не говорит о положительной динамике для США и других стран в целом.

Примечательно, что лоты с продажей доступов к компаниям в Индии стали одними из самых продаваемых стран, обойдя Китай на несколько позиций.

Увеличилось также само количество стран, доступом к компаниям которых можно было завладеть: 68 стран было атаковано за период H2 2020 — H1 2021 вместо 42 стран годом ранее.

Растет и количество злоумышленников, активно продающих доступы в корпоративные сети. За H2 2019 — H1 2020 специалистами Group-IB было обнаружено 86 продавцов, а за последний год (H2 2020 — H1 2021) их количество насчитывает 262, что в 3 раза больше, чем за предыдущий период. Из них 229 — это новые брокеры.

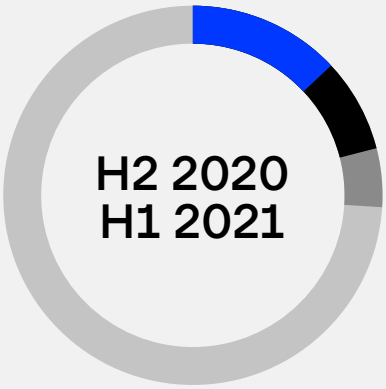
Ниже представлена статистика по злоумышленникам, опубликовавшим объявления о продаже доступов в период со 2-й половины 2019 по 1-ую половину 2020 года.

Название	%
network	15
nanash	12
SHERIFF	6
Streetskip	5
B.Wanted	4
bc.monster	4
wazawaka (AKA m1x)	4
cryzaa	3
ellis.J.douglas	3
vasyldn	3
TrueFighter	2
Lannister	2
Другие	37

Лидерами рынка на тот период являлись продавцы с никнеймами network и Nanash, предложившие более четверти всех продаваемых доступов.

Ниже представлена статистика за текущий отчетный период. Количество злоумышленников, делающих единичные предложения на рынке доступов, значительно увеличилось, что говорит о росте желающих подзаработать в этой сфере.

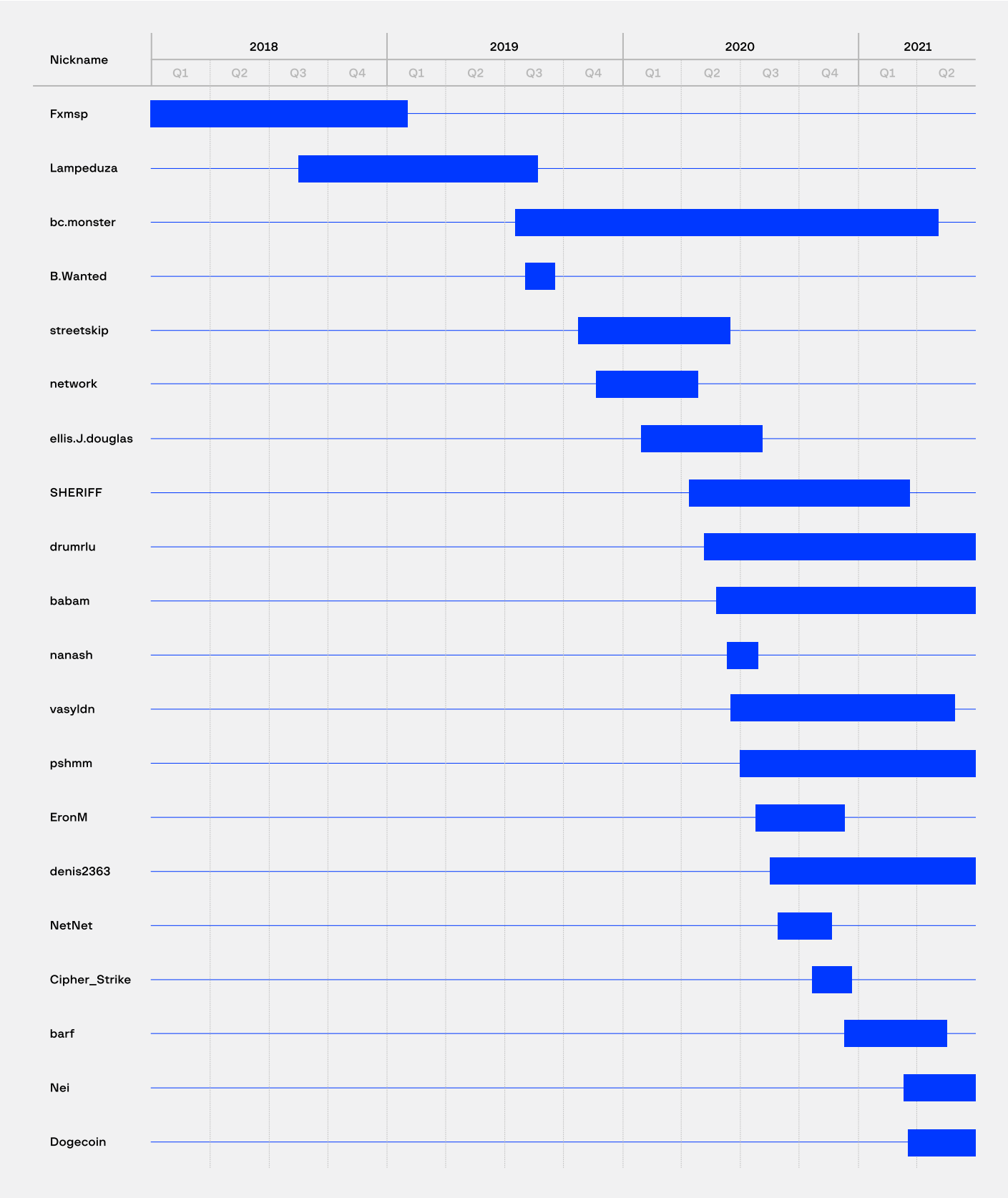
Название	%
barf	13
pshmm	8
nei	5
vasyldn	4
DogeCoin	4
drumrlu	4
babam	3
denis2363	3
NetNet	2
EronM	2
Другие	52



Заметим, что два года подряд среди лидеров по продажам доступов оставался только один злоумышленник — с псевдонимом vasyldn.

Примечательно, что за H2 2019 — H1 2020 network выложил на продажу 54 доступа, став лидером среди продавцов, а год спустя это место занял barf, но уже со 145 доступами.

На диаграмме ниже представлена хронология активности основных продавцов доступов с 2018 по 1-ю половину 2021 года.



Объем рынка продажи доступов в скомпрометированные сети

H2 2018 — H1 2019
$1 609 930
МИР

H2 2019 — H1 2020
$6 189 388
МИР

H2 2020 — H1 2021
$7 165 387
МИР

В прошлом отчете **Hi-Tech Crime Trends 2020/2021**, доступном на сайте Group-IB, аналитики Threat Intelligence оценили общий объем рынка продаваемых на даркнет-форумах доступов к корпоративным сетям компаний. В отчете был сделан вывод о том, что масштабы рынка увеличиваются ежегодно, однако “пик пришелся на 2020 год”. Новый анализируемый период (H2 2020 — H1 2021), по количеству предложений на рынке почти в 3 раза превысил пиковую отметку прошлого периода. Общий размер рынка в текущем периоде (H2 2020 — H1 2021) специалисты компании оценили в **$7 165 387**, что на 16% больше, чем за прошлый период (H2 2019 — H1 2020), когда рынок составлял **$6 189 388**.

Специалистами Group-IB также была проанализирована статистика по регионам. Однако еще раз подчеркнем, что не для всех компаний удалось определить страну, поэтому реальное количество жертв для каждого региона может отличаться.

Как можно заметить ниже, наибольший объем рынка составили доступы, принадлежащие странам **APAC**. За период H2 2020 — H1 2021 общая стоимость доступов составила **$3 307 210** что почти в 6 раз больше, чем за прошлый год. Наибольшее количество доступов среди стран APAC за этот период принадлежит **Австралии — 36%** от общего количества. Далее следует **Индия — 23%** и **Китай — 14%**.

Hi-Tech Crime Trends 2020/2021

H2 2020 — H1 2021 ОБЪЕМ РЫНКА
APAC
$3 307 210

Страны	Количество доступов, %
Австралия	36
Индия	23
Китай	14
Тайланд	8
Сингапур	4
Япония	4
Филиппины	2
Тайвань	2
Южная Корея	2
Другие	3

H2 2019 — H1 2020 ОБЪЕМ РЫНКА
APAC
$453 497

H2 2018 — H1 2019 ОБЪЕМ РЫНКА
APAC
$223 050

Второе место по объему на рынке составили доступы, относящиеся к странам **Америки — $1 377 552**, однако это почти в 2 раза меньше, чем было за H2 2019 — H1 2020, когда рынок составил более 3 миллионов долларов. Стоит отметить, что основную часть среди стран Америки составили доступы из **США — 76%** от общего количества объявлений.

H2 2020 — H1 2021 ОБЪЕМ РЫНКА АМЕРИКА

$1 377 552

Страны	Количество доступов, %
США	76
Канада	7
Бразилия	6
Мексика	3
Аргентина	2
Колумбия	2
Другие	4

H2 2019 — H1 2020 ОБЪЕМ РЫНКА АМЕРИКА

$3 300 601

H2 2018 — H1 2019 ОБЪЕМ РЫНКА АМЕРИКА

$647 400

Для **европейских** стран пик пришелся на прошлый период и составил **$753 598**, что на 25% больше, чем за H2 2020 — H1 2021 (**$590 095**). Лидирующие позиции в данном регионе занимают страны **Франция** и **Великобритания**, набравшие **20%** и **18%** от общего количества. Третье место заняла **Италия — 13%**, остальные страны составляют не более 10% от общего числа доступов.

H2 2020 — H1 2021 ОБЪЕМ РЫНКА ЕВРОПА

$590 095

Страны	Количество доступов, %
Франция	20
Великобритания	18
Италия	13
Испания	10
Германия	9
Нидерланды	5
Португалия	4
Швейцария	3
Бельгия	3
Швеция	3
Другие	12

H2 2019 — H1 2020 ОБЪЕМ РЫНКА ЕВРОПА

$753 598

H2 2018 — H1 2019 ОБЪЕМ РЫНКА ЕВРОПА

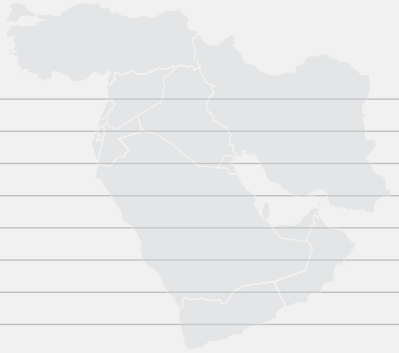
$408 700

Для стран **Ближнего Востока** напротив, рынок увеличился в 1,5 раза за отчетный период, по сравнению с прошлым годом. Безусловным лидером в данном регионе являются **ОАЭ**, набравшие **24%** от общего количества доступов. Далее идут **Турция** и **Израиль** — **14%** и **13%** соответственно; **Саудовская Аравия** и **Иран** — **12%** от всех доступов в регионе.

H2 2020 — H1 2021 ОБЪЕМ РЫНКА

СРЕДНЯЯ АЗИЯ

$247 836



Страны	Количество доступов, %
ОАЭ	24
Израиль	14
Турция	13
Саудовская Аравия	12
Иран	12
Кувейт	11
Египет	5
Катар	5
Другие	4

H2 2019 — H1 2020 ОБЪЕМ РЫНКА
СРЕДНЯЯ АЗИЯ

$180 538

H2 2018 — H1 2019 ОБЪЕМ РЫНКА
СРЕДНЯЯ АЗИЯ

$101 100

Среди стран **Африки** наблюдается спад интересов, по сравнению с предыдущим годом рынок упал до **$120 290**. В данном регионе за H2 2020 — H1 2021 лидирующую позицию заняли сразу две страны — **ЮАР, Египет**, процент которых составил **практически половину** от общего числа доступов в Африке. Также **23%** составили страны, где был указана принадлежность в Африке, но не была явно указана страна. Процент каждой из оставшихся стран составил не более **6%**.

H2 2020 — H1 2021 ОБЪЕМ РЫНКА

АФРИКА

$120 290

Страны	Количество доступов, %
Южная Африка	24
Египет	23
Гаана	6
Алжир	6
Нигерия	6
Сьерра-Леоне	6
Ливия	6
Другие	23

H2 2019 — H1 2020 ОБЪЕМ РЫНКА
АФРИКА

$135 188

H2 2018 — H1 2019 ОБЪЕМ РЫНКА
АФРИКА

$167 500

По странам **СНГ** пик рынка приходится на H2 2019 — H1 2020 и составил **$142 058**, в то время как за H2 2020 — H1 2021 рынок составляет **$48 239**, что почти в 3 раза меньше. Основной рынок за H2 2020 — H1 2021 составили доступы из России — **76%** от общего количества доступов. Стоит отметить, что большинство обнаруженных брокеров — русскоязычные, и они предпочитают избегать жертв в регионе СНГ, что делает его наименее атакуемым из всех представленных регионов

H2 2020 — H1 2021 ОБЪЕМ РЫНКА СНГ

$48 239

Страны	Количество доступов, %
Россия	76
Азербайджан	12
Армения	12

H2 2019 — H1 2020 ОБЪЕМ РЫНКА СНГ

$142 058

H2 2018 — H1 2019 ОБЪЕМ РЫНКА СНГ

$8 250

Отметим, что с появлением тенденции сокрытия ряда данных в объявлениях, включая стоимость лота, оценить общий объем рынка достаточно сложно. Кроме того, сделки часто происходят «в привате». Однако технологии Group-IB по исследованию таких ресурсов, в том числе с учетом удаленных записей и скрытой злоумышленниками информации, позволяют специалистам Group-IB измерять динамику и масштабы продаж такого “товара” в даркнете.

АНТИРЕЙТИНГ: ТОП-10 ПРОДАВЦОВ ДОСТУПОВ

08

В данном разделе подробно рассматривается деятельность 10 продавцов, предложивших наибольшее количество первичных доступов на продажу за отчетный период.

Nanash

Активность	**июнь 2020 — июль 2020**
Количество жертв	**> 40**
Георграфия атак	**11 стран**
Предположительный доход	**USD 5 000 000**

Nanash зарегистрировался на андеграундном форуме RaidForums 10 июня 2020 года и в тот же день создал тему о продаже, в которой предложил доступы к корпоративным сетям более **40 компаний** и правительственных организаций по всему миру. Последняя активность данного пользователя была отмечена в июле 2020 года. Nanash в своем первом сообщении в теме опубликовал краткое описание компаний и организаций, к которым он якобы имел доступы.

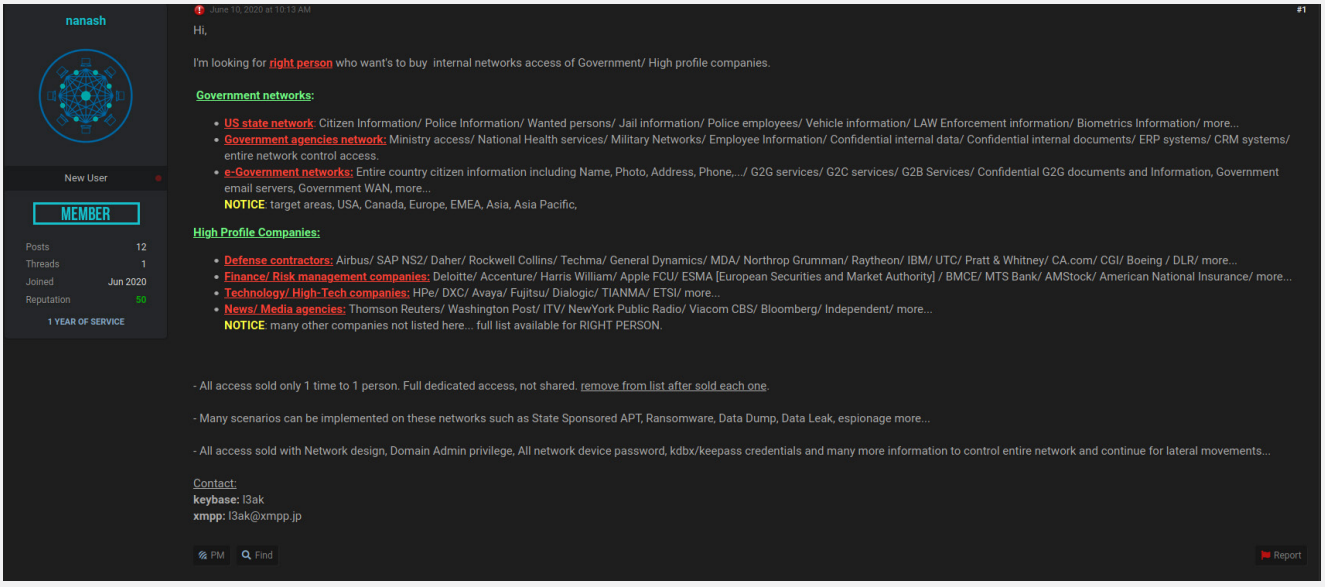


Рис. 27. Первое объявление пользователя Nanash на Raidforums

Из текста сообщения злоумышленника можно сделать вывод о том, что он имел доступы к государственным службам **Северной Америки, Европы, Ближнего Востока, Африки и Азиатско-Тихоокеанского региона**, однако он воздерживался от публикации точных наименований большинства из них. Помимо жертв в лице правительственных организаций, Nanash также упомянул такие компании, как **Northrop Grumman, Airbus, Raytheon, Boeing, Deloitte, Accenture, HPE, Thomson Reuters и Washington Post**.

Nanash вызвал неоднозначную реакцию у участников форума: одни из них проявили заинтересованность в том , что предложил Nanash, другие отнеслись с недоверием к новому пользователю. Однако исследователями Group-IB было установлено, что злоумышленник получил доступ как минимум к 2 компаниям, подтверждением этому служат предоставленные им скриншоты и записи предварительных просмотров службы директорий LDAP в реальном времени.

После общения в теме на форуме с разными пользователями Nanash указал цену в **11 BTC (100 тысяч долларов)** за каждый доступ. Он также отметил, что продажа должна была происходить “в одни руки”, причем он также указал, что предоставит полный список жертв лишь доверенному пользователю. По словам злоумышленника, первоначально покупатель должен был заплатить 5 BTC в качестве подтверждения сделки, после чего он должен был отправить оставшуюся сумму, чтобы получить полные данные.

По нашим оценкам, исходя из полного списка доступов и с учетом базовой цены за доступ, он потенциально мог бы заработать **не менее 5 миллионов долларов** с их продажи.

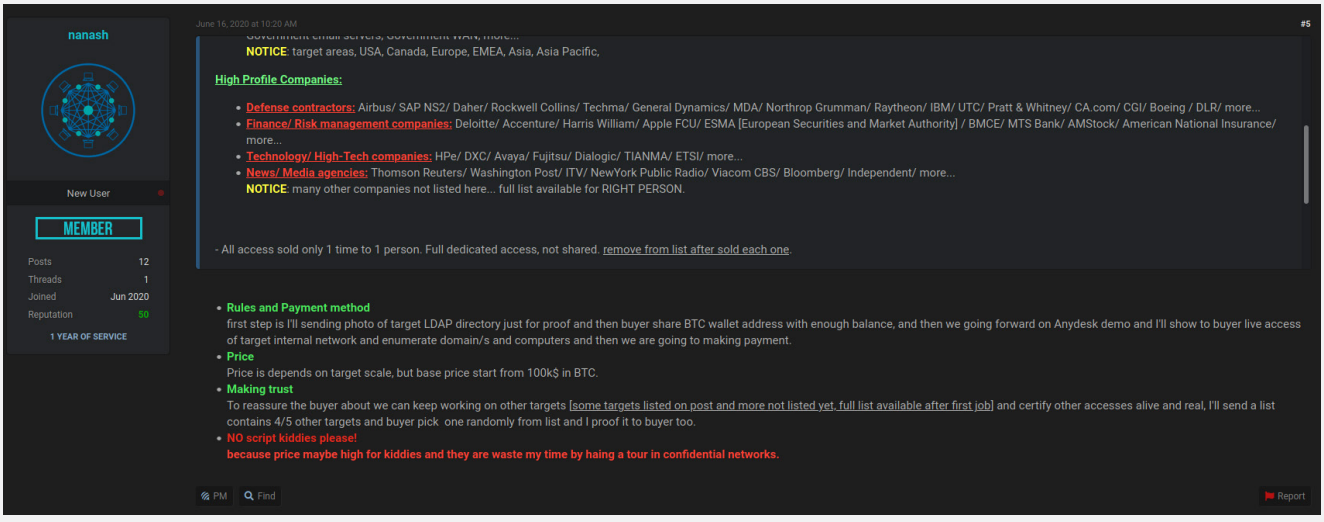


Рис. 28. Комментарий Nanash о стоимости доступов

Что случилось с Nanash после публикации этого объявления — остается загадкой. До сих пор неизвестно, сколько доступов к корпоративным сетям он смог продать, если он действительно их имел. После этого он перестал публиковать сообщения на форуме.

Спустя пару месяцев после того, как Nanash был замечен на Raidforums, исследователи **ClearSkySec** опубликовали свое исследование кампании вируса-шифровальщика Pay2Key, проводимой иранской APT-группой, известным как Fox Kitten. Они также связали одного пользователя под псевдонимом **kharpedar** с **Fox Kitten**, судя по опубликованным им сообщениям на андеграундных форумах. В своем отчете

ClearSkySec обнаружили, что этот пользователь также продавал доступ к компаниям, похожим по описанию на те, что выкладывал на продажу Nanash, выражая в них интерес к турецким организациям и незаинтересованность в правительстве Индии.

Ниже представлена статистика по странам и индустриям, к которым относятся жертвы Nanash.

Страна	%
США	57
Франция	10
Великобритания	5
Германия	5
Россия	2
Япония	2
Китай	2
Другие	10
Неизвестно	7

Индустрия	%
Правительственные и военные службы	18
СМИ и развлечения	15
Информационные технологии	15
Наука и инженерия	13
Финансовые услуги	13
Транспорт	5
Профессиональные услуги	5
Производство	5
Аппаратное обеспечение	5
Недвижимость	3
Неизвестно	3

ATT&CK Matrix for Enterprise (Nanash)

TACTICS	TECHNIQUES	DETAILS
Discovery	Account Discovery: Domain Account (T1087.002)	Злоумышленник предоставил скриншот LDAP с информацией о пользователях домена в корпоративной сети
	Permission Groups Discovery: Domain Groups (T1069.002)	Злоумышленник предоставил скриншот LDAP с информацией о доменах корпоративной сети

Vasyldn

Активность	**июнь 2020 — май 2021**
Количество жертв	**> 50**
Георграфия атак	**14 стран**
Предположительный доход	**USD 360 000**

15 июня 2020 года пользователь с псевдонимом vasyldn зарегистрировался на форуме Exploit. Сразу после этого он создал тему о продаже доступов к Active Directory корпоративных и правительственных организаций. Это событие стало началом его кампании по продаже доступов более чем в 50 организаций, расположенных в 14 разных странах. Последний раз vasyldn опубликовал объявление в мае 2021 года, после этого активности замечено не было.

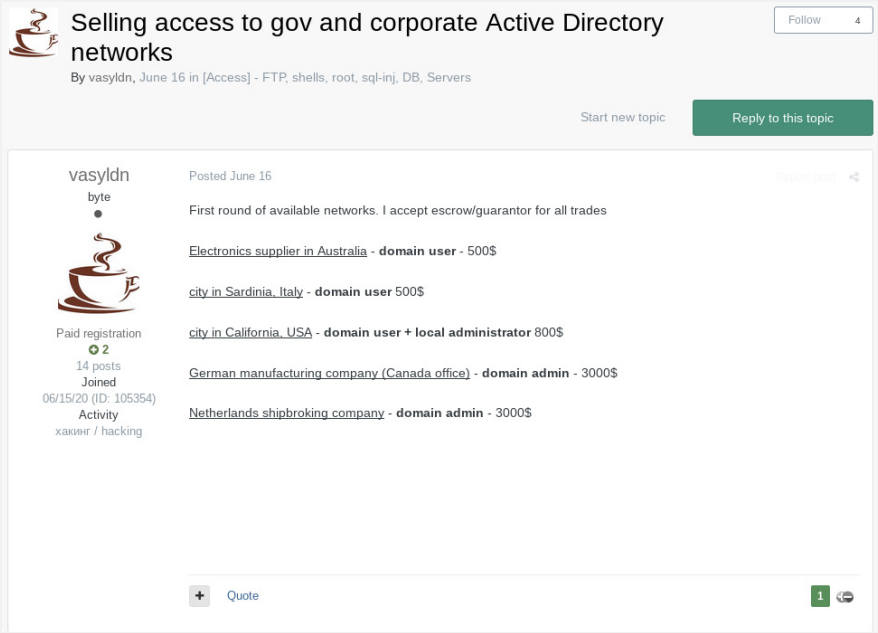


Рис. 29. Первое объявление пользователя vasyldn

В своем первом объявлении он выложил на продажу доступ к Active Directory 5 различных организаций в **США, Италии, Канаде, Австралии и Нидерландах**. Среди них: поставщик электроники в Австралии, судовой брокер в Нидерландах, производственное предприятие в Германии и объекты инфраструктуры неизвестных городов Сардинии и Калифорнии.

Vasyldn активно выкладывал в своей теме доступы на продажу вплоть до октября 2020 года. За это время им были скомпрометированы 23 компании, некоторые из которых были проданы вскоре после публикации объявления. После полугодичного перерыва vasyldn вновь возобновил свои продажи. Начиная с марта 2021 года, он опубликовал еще примерно 30 объявлений.

В частности, в его объявлениях были указаны 6 компаний из различных штатов США, в том числе крупный американский банк с доходом в миллиард долларов.

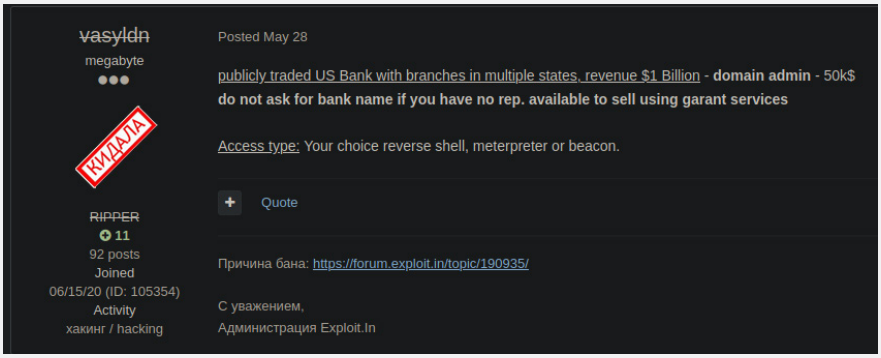


Рис. 30. Объявление vasyldn о продаже доступа к банку

Доподлинно неизвестно, как именно vasyldn получал доступ к корпоративным сетям. Однако мы знаем, что он использовал действующие учетные записи администратора домена для получения первоначального доступа.

Проанализировав активность злоумышленника, мы поняли, что vasyldn использовал Cobalt Strike для закрепления в сети, а также альтернативные методы аутентификации, такие как pass-the-ticket и golden tickets, для дальнейших перемещений по сети. Также в одном из сообщений атакующий явно указал, что использовал программу-вымогатель внутри неизвестной сети.

Как видно из диаграммы ниже, vasyldn в основном атаковал компании, расположенные на территории США, Великобритании и Канады.

Атаковал vasyldn преимущественно финансовые организации и государственные учреждения. Также злоумышленник продавал доступ к организациям, работающим в юридическом, производственном, строительном, транспортном и образовательном секторах.

Страна	%
США	53
Великобритания	10
Канада	7
Израиль	7
Мексика	6
Италия	3
Швейцария	3
Другие	12

Индустрия	%
Правительственные и военные службы	26
Финансовые услуги	20
Юридические услуги	16
Производство	10
Недвижимость	8
Транспорт	7
Образование	5
Другие	8

ATT&CK Matrix for Enterprise (vasyldn)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	Злоумышленник использовал RDP, VPN, SSH для доступа к корпоративным сетям
Execution	Command and Scripting Interpreter (T1059)	Злоумышленник указывал, что может предоставить доступы через Meterpreter, реверс-шелл
Credential access	Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001)	Злоумышленник указал в объявлении, что продает доступ с Kerberos golden Ticket (krbtgt) хэшем
Discovery	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы
Command and Control	Ingress Tool Transfer (T1105)	Злоумышленник мог использовать Meterpreter или CSB для установки RAT на машину жертвы
Impact	Data Encrypted for Impact (T1486)	Злоумышленник использовал вирус-шифровальщик

Drumrlu

Активность	**май 2020 — настоящее время**
Количество жертв	**50**
Георграфия атак	**22 страны**
Предположительный доход	**USD 180 000**

Drumrlu, также известный как 3lv4n, предположительно турецкий брокер первоначальных доступов и поставщик баз данных, впервые появился на форумах в мае 2020 года. Свою деятельность он начал с продажи базы данных, содержащей личную информацию 500 тысяч граждан Саудовской Аравии.

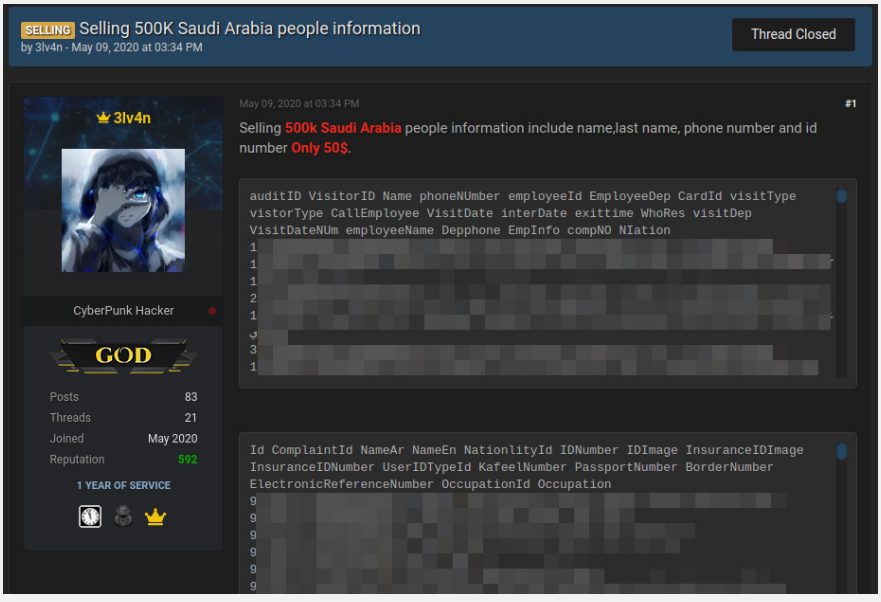


Рис. 31. Объявление Drumrlu о продаже базы данных

Помимо деятельности по продаже данных, Drumrlu обсуждал различные уязвимости с другими пользователями, например, он предложил кому-то изучить CVE-2018-14847, критическую уязвимость WinBox, позволяющую читать и записывать произвольные файлы из-за уязвимости обхода каталогов в интерфейсе для компрометации интернет-провайдера. Он также пытался продать эксплойт для CVE-2020-0688, уязвимости удаленного выполнения кода на серверах Exchange.

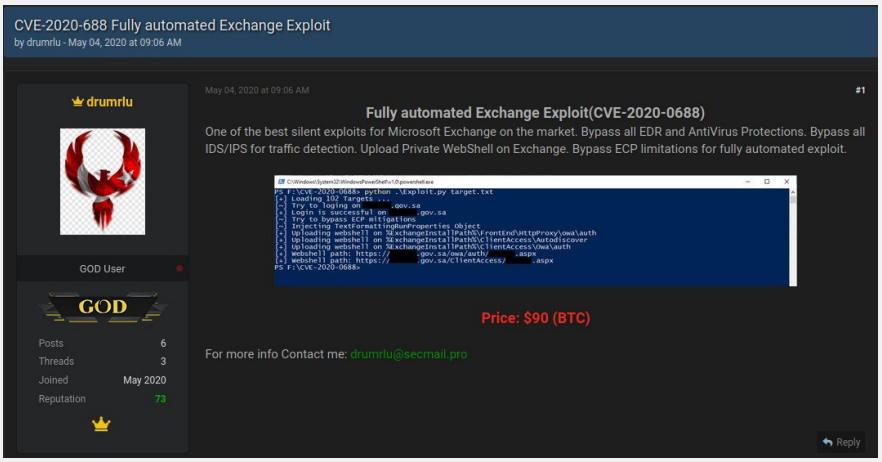


Рис. 32. Объявление Drumrlu о продаже эксплойта

Drumrlu, вероятно, также сотрудничал с Nosophoros, разработчиком вымогателя Thanos — несколько раз они хвалили работу друг друга.

Рис. 33. Комментарии Nosophoros о сотрудничестве с Drumrlu

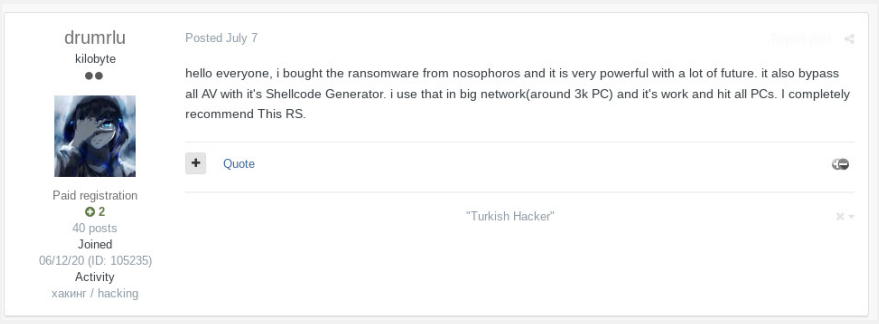


Рис. 34. Комментарий Drumrlu о сотрудничестве с Nosophoros

Использование Drumrlu программ-вымогателей также подтверждается заявлением команды исследователей **Intel 471** о том, что он предположительно работал на правительство Ирана. Согласно их отчету через несколько месяцев после написания комментария выше в нескольких организациях была развернута программа-вымогатель. Результаты показывают, что TTPs Drumrlu аналогичны TTPs MuddyWater, APT-организации, работающей на то же правительство.

Drumrlu получает данные различными способами. Мы смогли идентифицировать несколько из них на основе его сообщений, в которых он говорит, что получил данные напрямую из сети взломанной организации или с помощью вредоносной программы. В первых темах о продаже Drumrlu в основном предлагал доступ к серверам ESXi и AD. Судя по ценам, установленным злоумышленником, он мог заработать **около 180 000 долларов**.

Как видно на диаграмме ниже, наибольшее количество жертв Drumrlu находится в Соединенных Штатах Америки, Объединенных Арабских Эмиратах и Саудовской Аравии.

Большую часть жертв составляли компании в сфере информационных технологий, финансовых услуг и правительственные организации.

Страна	%
США	20
ЮАЭ	8
Саудовская Араваия	8
Италия	6
Таиланд	6
Иордания	4
Индия	4
Канада	4
Турция	2
Китай	2
Неизвестно	12
Другие	22

Индустрия	%
Информационные технологии	18
Финансовые услуги	18
Правительственные и военные службы	12
Энергия	10
Природные ресурсы	6
Здравохранение	4
Торговля и шоппинг	4
Образование	4
Телекоммуникации	4
Транспорт	4
Другие	16

ATT&CK Matrix for Enterprise (vasyldn)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	Злоумышленник использовал учетные записи VPN, Citrix для доступа в сеть
	Exploit Public-Facing Application (T1190)	Злоумышленник продавал эксплоит для CVE-2020-0688 в Microsoft Exchange
Execution	Command and Scripting Interpreter: Visual Basic (T1059.005)	Злоумышленник использовал вредоносные Office-документы с макросами
Persistence	Server Software Component: Web Shell (T1505.003)	Злоумышленник продавал Web Shell
Credential Access	OS Credential Dumping: NTDS (T1003.003)	Злоумышленник продавал NTDS файл
Discovery	Account Discovery: Domain Account (T1087.002)	Злоумышленник предоставил скриншот LDAP с информацией о пользователях домена в корпоративной сети
Impact	Data Encrypted for Impact (T1486)	Злоумышленник оставлял отзыв о Thanos Ransomware

denis2363

Активность	**август 2020 — настоящее время**
Количество жертв	**> 50**
Георграфия атак	**4 страны**
Предположительный доход	**USD 160 000**

denis2363 начал свою деятельность на форуме Exploit 3 ноября 2015 года и в настоящее время является активным продавцом доступов.

9 августа 2020 года denis2363 опубликовал первое объявление о продаже доступа к компании, занимающейся разработкой игр, установив цену в $25000. Позже в этот же день он снизил цену доступа до **5000 долларов**, а 26 августа оставил в теме о продаже комментарий, что доступ продан.

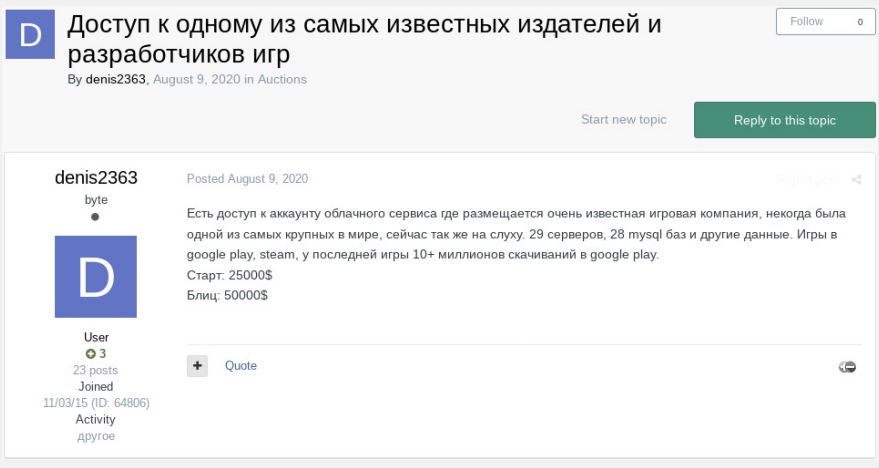
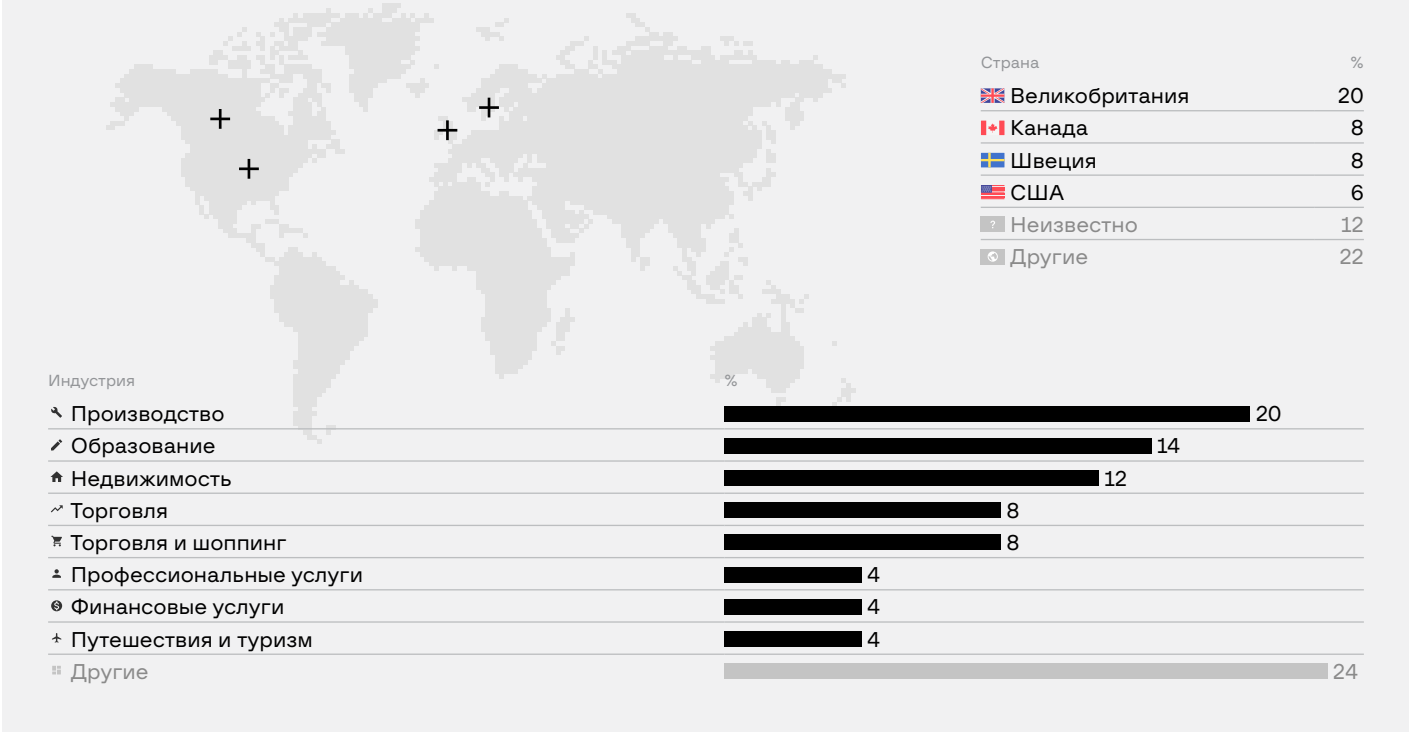


Рис. 35. Объявление denis2363 о продаже доступа

Мы проанализировали публичную активность denis2363 и пришли к выводу, что в ходе некоторых атак он эксплуатировал уязвимости BlueKeep, EternalBlue, PrintNightmare, а уязвимые хосты находил путем сканирования публичных IP-адресов, в том числе через **Shodan**.

Жертвы denis2363 есть в многих сферах, но наибольшее количество пришлось на области производства, образования и недвижимости.

Подавляющее большинство компаний, скомпрометированных denis2363, расположены в США.



ATT&CK Matrix for Enterprise (denis2363)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.001)	Злоумышленник сканировал IP-адреса на наличие уязвимых сервисов
Initial Access	Exploit Public-Facing Application (T1190)	Злоумышленник эксплуатировал уязвимости в Citrix, FortiGate для получения доступа
	External Remote Services (T1133)	Злоумышленник использовал учетные записи VPN, Citrix для доступа в сеть
	Valid Accounts: Domain Accounts (T1078.002)	Злоумышленник использовал скомпрометированные доменные учетные записи для доступа в сеть
	Valid Accounts: Local Accounts (T1078.003)	Злоумышленник использовал скомпрометированные локальные учетные записи для доступа в сеть
Persistence	Create Account: Local Account (T1136.001)	Злоумышленник упоминал создание учетной записи локального администратора для закрепления в сети
	Hijack Execution Flow: DLL Side-Loading (T1574.002)	Злоумышленник использовал DLL Side-Loading при эксплуатации уязвимости PrintNightmare

TACTICS	TECHNIQUES	DETAILS
Discovery	Network Share Discovery (T1135)	Злоумышленник использовал общие папки для эксплуатации уязвимости PrintNightmare
	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы
Lateral Movement	Exploitation of Remote Services (T1210)	Злоумышленник использовал уязвимости BlueKeep и EternalBlue для продвижения по сети

Pshmm

Активность	**июль 2020 — настоящее время**
Количество жертв	**> 85**
Георграфия атак	**19 стран**
Предположительный доход	**USD 300 000**

Англоговорящий злоумышленник под псевдонимом **pshmm** был впервые замечен на форумах в начале 2020 года, его активность прослеживается и в октябре 2021 года.

Нелегальный бизнес pshmm начался с продажи доступа к контроллеру домена медицинской компании, расположенной в Соединенных Штатах.

Рис. 36. Первое объявление pshmm о продаже доступа к контроллеру домена

На следующий день после регистрации на Exploit pshmm создал специализированную тему, в которой он в дальнейшем выкладывал доступы на продажу. Всего им было выставлено на продажу более чем 85 компаний, относящихся к 19 отраслям и 19 странам.

Несмотря на то, что pshmm начал свою деятельность с продажи доступа к контроллерам домена, в которые он предположительно проник через RDP, он также указывал, что получал доступ к скомпрометированным сетями через корпоративное ПО для обеспечения удалённого мониторинга и управления (RMM).

Известно, что одной из используемых точек входа в сеть для pshmm был Zoho ManageEngine Desktop Central — ПО для централизованного управления настольными ПК и мобильными устройствами в локальной сети. При помощи данного ПО возможно выполнение удаленных операций, которыми в основном пользуются IT-специалисты: развертывание стороннего ПО, настройка политик и, что наиболее важно, запуск настраиваемых сценариев.

В программе Desktop Central в январе 2020 года была обнаружена RCE-уязвимость, которая была исправлена лишь двумя месяцами позже. Эта уязвимость позволяет атакующему выполнить набор произвольных команд с привилегиями SYSTEM без аутентификации. Исследователи безопасности отмечали, что данная уязвимость активно эксплуатировалась даже после того, как в марте 2020 года был выпущен официальный патч. Вполне вероятно, что pshmm мог эксплуатировать эту уязвимость.

Как показано на рисунке ниже, в приоритете pshmm, как и у большинства исследованных нами продавцов доступа, были Соединенные Штаты Америки, на долю которых приходится 42% всех его жертв.

Если посмотреть на распределение по индустриям, то можно заметить, что pshmm в основном был сосредоточен на отрасли здравоохранения, куда входят больницы и медицинские организации, доступ к которым он продавал. Далее следуют отрасли производства и финансовых услуг. Очевидно, что у pshmm не было четкой последовательности атак на организации. Судя по его активности, он не выделял какую-то конкретную страну или индустрию для массовых атак, а нацеливался на всех, с кого можно было получить прибыль.

Страна	%
США	42
Канада	7
Бразилия	6
Китай	6
Франция	3
Великобритания	3
Италия	3
Индия	3
Австралия	3
Неизвестно	7
Другие	17

Индустрия	%
Здравоохранение	17
Производство	10
Финансовые услуги	9
Образование	8
Правительственные и военные службы	8
Еда и напитки	7
Транспорт	6
Торговля и шоппинг	5
Информационные технологии	5
Природные ресурсы	5
Неизвестно	1
Другие	19

Что касается прибыли, то с учетом всех указанных в объявлениях цен, этот злоумышленник потенциально мог заработать более 300 000 долларов США. Основываясь на обновлениях о том, что доступ был кому-то продан, можно сказать, что pshmm гарантированно заработал порядка 65 000 долларов США.

ATT&CK Matrix for Enterprise (pshmm)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning (T1595)	Атакующий сканировал устройства с открытыми RDP-сервисами
Initial access	External Remote Services (T1133)	Злоумышленник использовал учетные записи RDP, VPN для доступа в сеть
	Valid Accounts: Domain Accounts (T1078.002)	Злоумышленник использовал скомпрометированные доменные учетные записи для доступа в сеть
	Valid Accounts: Local Accounts (T1078.003)	Злоумышленник использовал скомпрометированные локальные учетные записи для доступа в сеть
Credential access	Brute Force (T1110)	Атакующий использовал технику перебора для получения доступа к RDP-аккаунтам
Discovery	Remote System Discovery (T1018)	Злоумышленник проводил сканирование для поиска контроллеров домена и удаленных служб в целевой среде
	File and Directory Discovery (T1083)	Злоумышленник указал на наличие конкретных файлов на файловом сервере жертвы
	Network Share Discovery (T1135)	Злоумышленник указал на наличие конкретных файлов на файловом сервере жертвы
	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы
Credential access	Email Collection: Remote Email Collection (T1114.002)	Злоумышленник продавал доступы к компании, включая доступы к серверам Exchange.
	Data from Network Shared Drive (T1039)	Злоумышленник выставлял на продажу данные, полученные с файлового сервера

SHERIFF

Активность	**апрель 2020 — март 2021**
Количество жертв	**> 30**
Георграфия атак	**5 стран**
Предположительный доход	**USD 837 800**

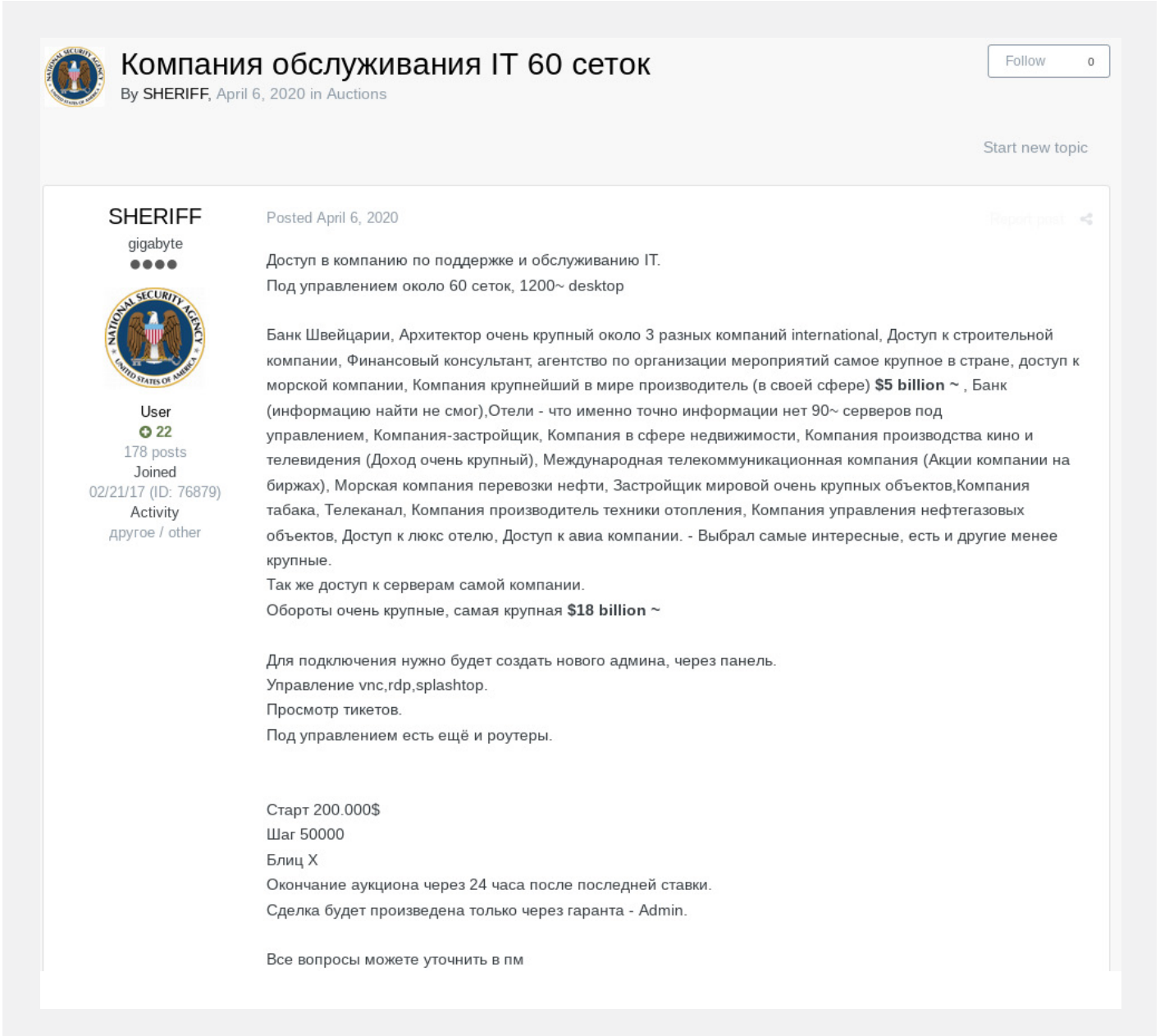
Еще один брокер первоначального доступа в корпоративные сети — пользователь с псевдонимом SHERIFF — известный русскоязычный злоумышленник, специализирующийся на финансовых организациях. Его деятельность началась на андеграундном форуме Exploit в 2017 году. Последняя активность этого продавца на форумах была отмечена в марте 2021 года.

Изначально SHERIFF занимался деятельностью, связанной с кардингом, продавая дампы банковских карт, базы данных, подарочные карты вплоть до 2019 года.

С начала 2019 года SHERIFF перешел к получению доступов к уязвимым веб-сайтам при помощи таких инструментов, как SIB-служба, X-MapAdmin и OWASP ZAP. Затем злоумышленник начал продавать доступы к административным панелям и базам данных жертв. Отметим, что почти все сайты представляли из себя онлайн-магазины в США. Кроме этого, в 2020 году он активно эксплуатировал RCE-уязвимости, связанные с протоколом Citrix RDP.

В апреле 2020 года SHERIFF выставил на продажу доступ к крупной IT-компании (возможно, MSP). Согласно объявлению у этой компании имеются клиенты в областях архитектуры, строительства, финансового консалтинга, морского и авиационного секторов, а также несколько банков, один из которых находится в Швейцарии.

Рис. 37. Первое объявление SHERIFF о продаже доступа



Компания обслуживания IT 60 сеток

By SHERIFF, April 6, 2020 in Auctions

Follow 0

Start new topic

SHERIFF
gigabyte
User
22
178 posts
Joined
02/21/17 (ID: 76879)
Activity
другое / other

Posted April 6, 2020

Доступ в компанию по поддержке и обслуживанию IT.
Под управлением около 60 сеток, 1200~ desktop

Банк Швейцарии, Архитектор очень крупный около 3 разных компаний international, Доступ к строительной компании, Финансовый консультант, агентство по организации мероприятий самое крупное в стране, доступ к морской компании, Компания крупнейший в мире производитель (в своей сфере) **$5 billion ~** , Банк (информацию найти не смог),Отели - что именно точно информации нет 90~ серверов под управлением, Компания-застройщик, Компания в сфере недвижимости, Компания производства кино и телевидения (Доход очень крупный), Международная телекоммуникационная компания (Акции компании на биржах), Морская компания перевозки нефти, Застройщик мировой очень крупных объектов,Компания табака, Телеканал, Компания производитель техники отопления, Компания управления нефтегазовых объектов, Доступ к люкс отелю, Доступ к авиа компании. - Выбрал самые интересные, есть и другие менее крупные.
Так же доступ к серверам самой компании.
Обороты очень крупные, самая крупная **$18 billion ~**

Для подключения нужно будет создать нового админа, через панель.
Управление vnc,rdp,splashtop.
Просмотр тикетов.
Под управлением есть ещё и роутеры.

Старт 200.000$
Шаг 50000
Блиц X
Окончание аукциона через 24 часа после последней ставки.
Сделка будет произведена только через гаранта - Admin.

Все вопросы можете уточнить в пм

В этом же месяце был опубликован еще один пост, в котором SHERIFF выложил на продажу 20 доступов к серверам компаний. Поскольку описание схоже с тем, что было в предыдущем посте, мы можем предположить, что злоумышленник получил доступ к сетям клиентов вышеупомянутой IT-компании. Также неизвестно, были ли проданы какие-либо из этих доступов.

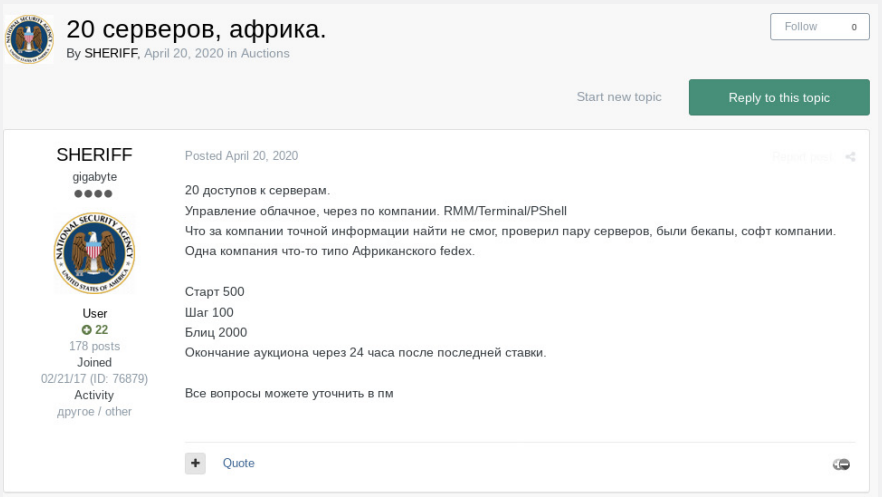


Рис. 38. Объявление SHERIFF о продаже доступов к серверам

В августе 2019 года SHERIFF создал тему на форуме, в которой попросил других пользователей посоветовать способы монетизировать данные с инвестиционного веб-сайта, который содержал коды сортировки, IBAN, BIC и SWIFT. Спустя 2 дня он выставил эти данные на продажу **за 35 000 долларов США**.

Еще одно свидетельство сосредоточенности SHERIFF на финансовой индустрии — одна из его жертв, производитель POS-терминалов. Согласно сообщению от 16 сентября 2019 года этот производитель обслуживает крупные корпорации США, колледжи и отели. Кроме того, автор заявил, что злоумышленники могут изменить клиентский IP-порт платежных терминалов в административной панели жертвы для перехвата данных.

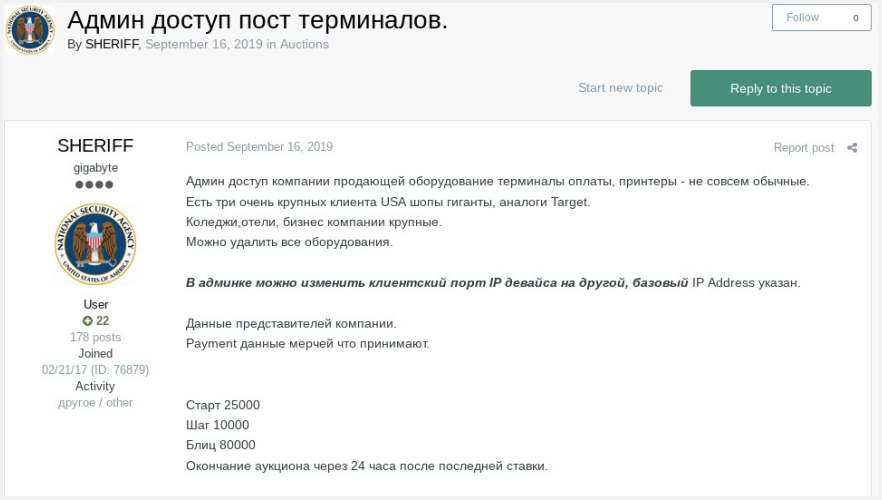


Рис. 39. Объявление SHERIFF о продаже доступа

SHERIFF активно занимался поиском партнеров для сотрудничества на андеграундных форумах. Помимо этого, он также пытался приобрести на аукционе данные, полученные со стилеров, у других пользователей. Например, он принимал участие в аукционе по продаже «логов» (скомпрометированных данных), полученных при помощи вредоносного ПО AZORult stealer.

Одной из самых примечательных активностей SHERIFF было партнерство с представителями хакерской группировки **REvil**. Они неоднократно приобретали у SHERIFF доступы, используя псевдонимы **UNKN** и **unknown**, которые, как известно, принадлежат участникам группы REvil, использующих одноименный вирус-шифровальщик для кибератак.

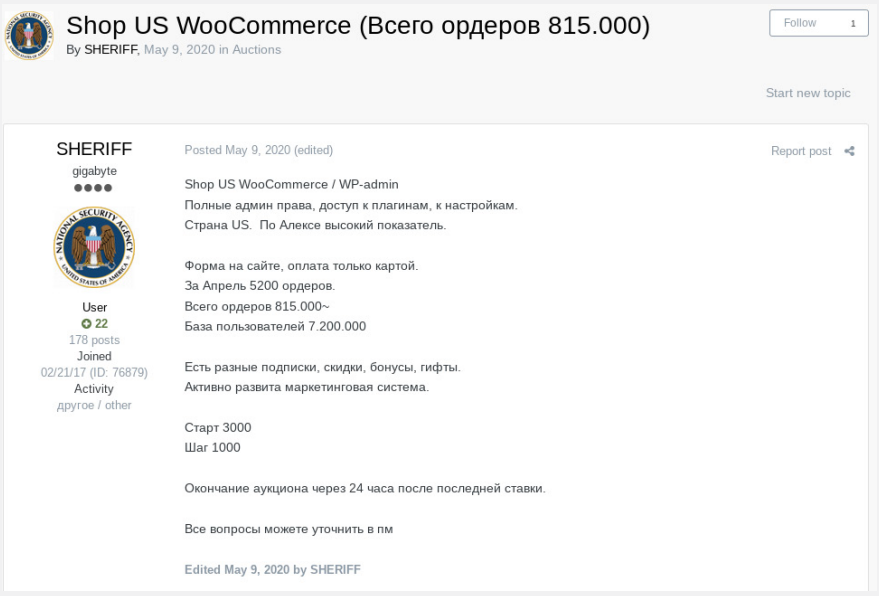


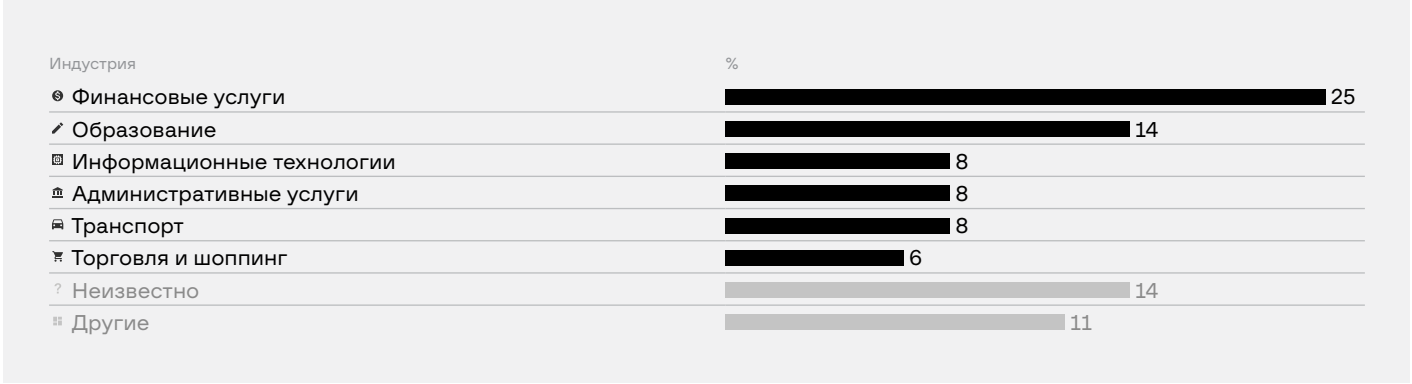
Рис. 40. Скриншот темы SHERIFF на форуме Exploit

Рис. 41. Комментарий участника группы REvil в теме SHERIFF

За 2020-2021 годы SHERIFF выставил на продажу 33 доступа к корпоративным сетям. Однако нельзя точно сказать, сколько ему удалось заработать на них, так как в большинстве его тем нет комментариев о продаже. По нашим подсчетам он мог бы заработать не менее 837 800 долларов за счет продаж всех своих доступов.

SHERIFF редко указывал, к какой стране относятся его жертвы, поэтому нельзя точно определить, какие именно страны он атаковал. Из той информации, что он указывал в объявлениях можно сделать вывод о том, что он был нацелен на компании, расположенные в странах Азии и США, реже встречались жертвы из Европейских стран, Австралии и Канады.

Распределение по атакованным SHERIFF индустриям представлено на диаграмме ниже.



Выделить наиболее атакуемые злоумышленником страны не представляется возможным, он не указывал детальной информации по продаваемым доступам.

ATT&CK Matrix for Enterprise (SHERIFF)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.002)	Злоумышленник сканировал веб-сайты на наличие уязвимостей (при помощи X-MapAdmin)
Initial access	External Remote Services (T1133)	Злоумышленник занимался продажей Citrix, RDP доступов
	Valid Accounts (T1078)	Злоумышленник использовал скомпрометированные аккаунты для получения доступа к удаленным службам и сайтам
Credential access	Brute Force (T1110)	Злоумышленник занимался продажей аккаунтов, полученных в результате брутфорс атаки
Discovery	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы
Command and Control	Remote Access Software (T1219)	Злоумышленник использовал скрытый TeamViewer

Nei (aka Rakuda)

Активность	**март 2021 - настоящее время**
Количество жертв	**55**
Георграфия атак	**7 стран**
Предположительный доход	**USD 24 000 — 36 000**

Nei, также известный как **Rakuda** и **Asatru**, является злоумышленником, специализирующимся на продаже доступа через VPN-RDP. Данный пользователь активно ведет свою деятельность на форумах Exploit и XSS с марта 2021 года. Последняя его активность наблюдалась в октябре 2021 года.

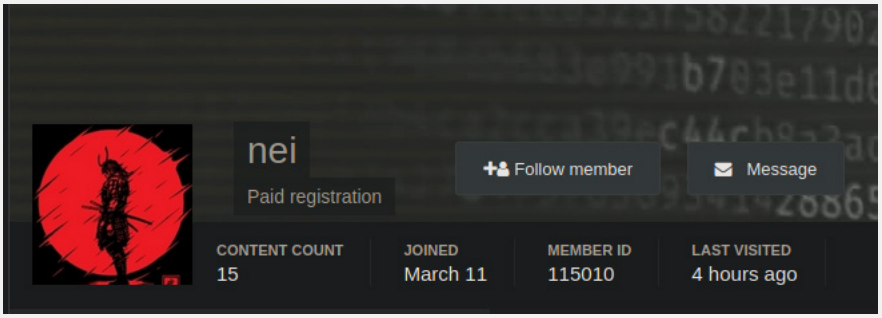


Рис. 42. Профиль nei на форуме Exploit

Помимо продажи доступов на форуме Exploit Nei также активно участвует в обсуждениях с другими киберпреступниками на форуме XSS. Например, он оставлял советы по обходу антифрод-систем и по проведению атак на веб-сайты.

В своих темах Nei указал, что 42 из 55 выставленных им на продажу доступов уже проданы. Несмотря на то, что стоимость доступов у него ниже, чем у других брокеров, его доходы по нашим подсчетам составили **от 24 000 до 36 000 долларов**.

Точно неизвестно, какие именно методы использовал Nei для получения доступа к корпоративным сетям организаций. Однако известно, что он использовал такие инструменты, как Masscan, для выявления новых жертв в крупном объеме. Это в свою очередь показывает, что злоумышленник активно занимается поиском открытых RDP и VPN-серверов по всему миру.

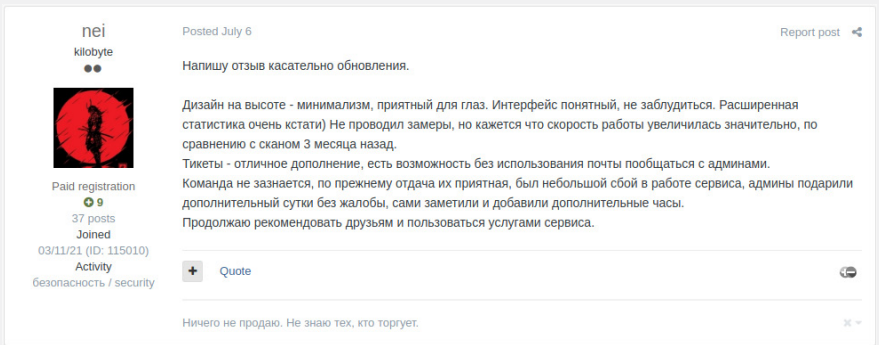


Рис. 43. Комментарий nei в теме с обсуждением обновлений для Masscan

Зарегистрировавшись на форуме XSS, он неоднократно интересовался продажей новых вредоносных программ-стилеров, в том числе участвовал в обсуждениях Raccoon Stealer.

Ниже представлена статистика по индустриям, атакованным данным злоумышленником. Лидирующие позиции занимают организации здравоохранения, сферы услуг и производственные предприятия. К ним также относится и категория Other, в которую вошли компании, отрасль которых не установлена.

При анализе распределения жертв по странам, становится ясно, что Nei в основном нацеливался на компании, расположенные в Соединенных Штатах и Франции, что составляет половину его жертв.

Страна	%
США	30
Франция	18
Испания	9
Великобритания	9
Канада	5
Чили	5
Италия	5
Неизвестно	19

Индустрия	%
Здравоохранение	12
Профессиональные услуги	12
Производство	12
Путешествия и туризм	9
Торговля и шоппинг	7
Правительственные и военные службы	7
Природные ресурсы	5
Еда и напитки	5
Юридические услуги	5
Транспорт	4
СМИ и развлечения	4
Энергия	4
Другие	14

ATT&CK Matrix for Enterprise (Nei)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Scanning IP Blocks (T1595.001)	Злоумышленник использовал Masscan для поиска открытых портов
Initial access	Exploit Public-Facing Application (T1190)	Злоумышленник занимался поиском уязвимостей в сайтах на WordPress
	External Remote Services (T1133)	Атакующий использовал RDP, VPN для доступа к корпоративным сетям
Execution	User Execution: Malicious File (T1204.002)	Злоумышленник использовал вредоносное ПО для получения скомпрометированных учетных записей пользователей

TACTICS	TECHNIQUES	DETAILS
Credential access	OS Credential Dumping (T1003)	Злоумышленник использовал вредоносное ПО для получения скомпрометированных учетных записей пользователей
Discovery	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы

network

Активность	**ноябрь 2019 — май 2020**
Количество жертв	**54**
Георграфия атак	**17 стран**
Предположительный доход	**USD 400 000**

Пользователь под псевдонимом **network** был еще одним брокером первичного доступа, работавшим на форуме Exploit в период с ноября 2019 года по май 2020 года.

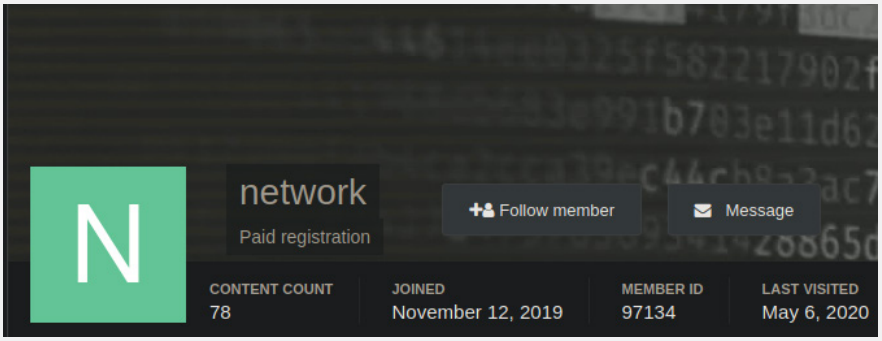
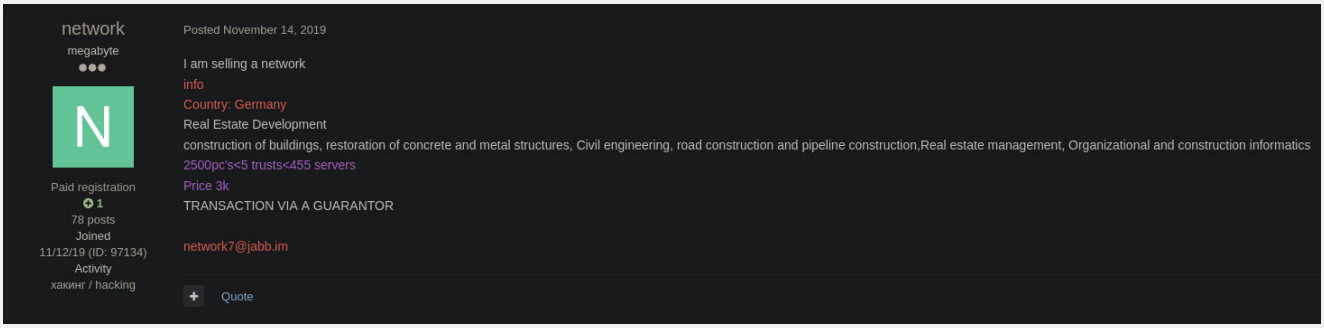


Рис. 44. Профиль network на форуме Exploit

Свой первый доступ network выложил на продажу всего через два дня после регистрации на форуме — 14 ноября 2019 года. В объявлении он продавал доступ к сети немецкой компании по недвижимости за 3000 долларов США.

Рис. 45. Скриншот первого сообщения о продаже доступа



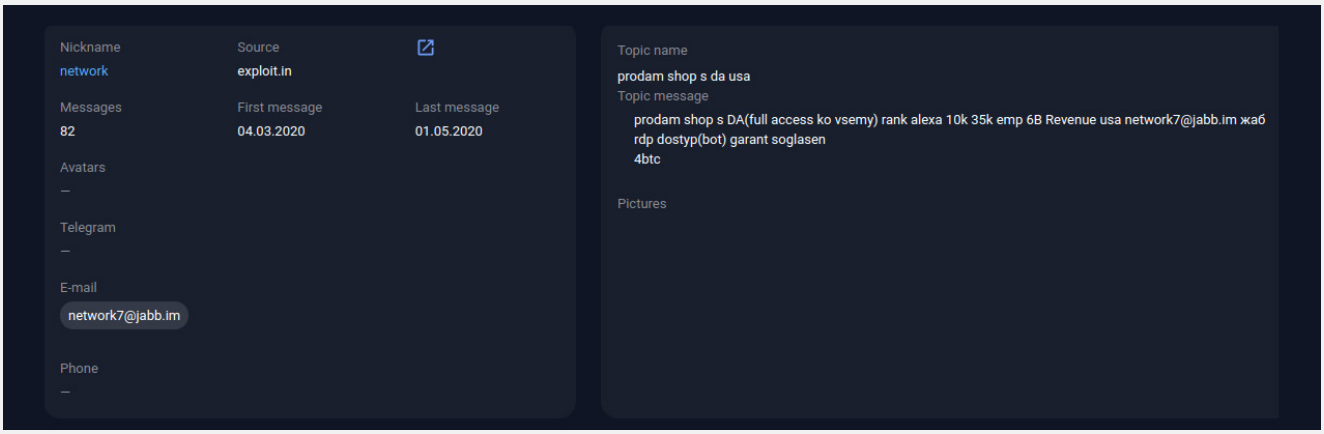
Можно подчеркнуть, что продавец стабильно постил объявления о продаже доступов небольшими партиями от 3 до 4 в день. Обычно на продажу выставлялись доступы двух видов: учетные записи администратора домена и «сеансовый» доступ, что наталкивает на мысль об использовании им Cobalt Strike или Armitage для получения данных.

После года почти постоянной активности 1 мая network резко прекратил свою деятельность и перестал публиковать сообщения. Его последней продажей был доступ к интернет-магазину в США с доходом в 6 миллиардов долларов, который впоследствии был удален с форума.

Network, в отличие от других брокеров, не указывал в темах, был ли продан доступ или нет, при этом периодически удалял свои объявления на форуме. Это может значить, что доступ был продан или стал недоступен.

Однако несмотря на то, что эти сообщения уже удалены автором, они все еще доступны на нашей платформе Group-IB Threat Intelligence & Attribution. С её помощью мы можем точно узнать, сколько именно доступов в сети компаний было выставлено на продажу данным злоумышленником. Также с помощью нашей системы нам удалось восстановить, сообщение о продаже вышеупомянутой компании в США. Скриншот сообщения представлен ниже.

Рис. 46. Сообщение network в системе Threat Intelligence & Attribution



Как мы уже отметили выше, network редко сообщал о продаже доступа. Поэтому нельзя точно установить его доход с продажи доступов. Однако основываясь лишь на указанных им ценах, мы можем примерно оценить общую стоимость продаваемых им доступов. Она составила **более чем 400 000 долларов США**.

Несмотря на то, что карьера Network была недолгой (по крайней мере, под этим псевдонимом), он успел получить доступы в более чем 50 компаний, расположенных в 17 странах.

Ниже представлено распределение жертв, атакованных злоумышленником, по странам. При анализе статистики становится видно, что главной мишенью network являлись Соединенные Штаты, вслед за которыми явно можно выделить Великобританию и остальную Европу. Стоит указать на то, что многие доступы нельзя было отнести ни к одной из стран, поэтому они были отнесены к категории «Unknown». Данная категория, в свою очередь также составляет большую часть от общего количества объявлений — 21%.

Приоритетными целями network были организации здравоохранения, производственные предприятия, компании по разработке ПО и компании из сферы туризма.

Страна	%
США	34
Европа	21
Великобритания	9
Индия	5
Америка	5
Неизвестно	24
Другие	5

Индустрия	%
Здравоохранение	15
Производство	15
Информационные технологии	13
Путешествия и туризм	9
Финансовые услуги	9
Транспорт	7
Правительственные и военные службы	7
Образование	7
Неизвестно	5
Другие	9

ATT&CK Matrix for Enterprise (Network)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	Атакующий использовал учетные записи RDP для доступа в сети
Discovery	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы

barf

Активность	**декабрь 2020 — май 2021**
Количество жертв	**145**
Георграфия атак	**9 стран**
Предположительный доход	**USD 49 000**

Активность данного пользователя на андеграундных форумах началась в 2017 году и наблюдалась вплоть до мая 2021 года. Начиная с 2018 года, злоумышленник начал создавать объявления о продаже RDP-серверов на других андеграундных форумах под псевдонимом **barf**.

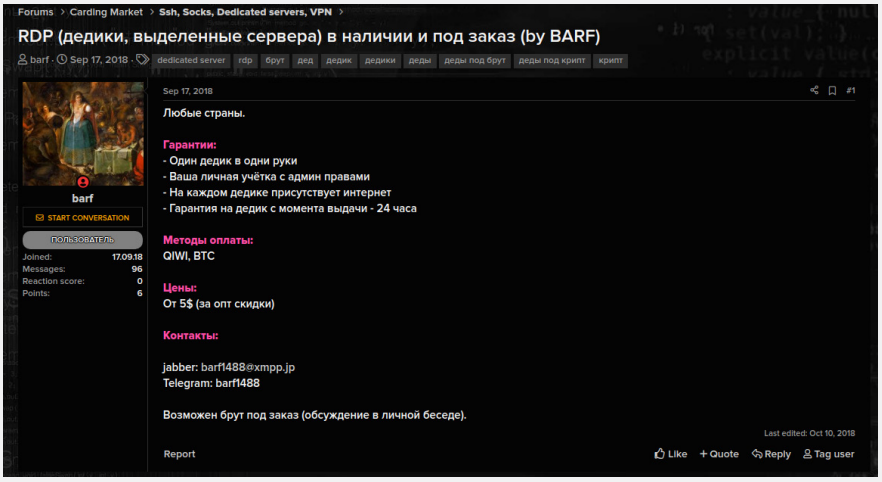


Рис. 47. Пример темы пользователя barf о продаже выделенных серверов в 2018 году

В январе 2019 года, barf выставил на продажу подписку для вредоносного ПО для брутфорса SSH, RDP и VNC-доступов, созданного пользователем z668. По словам злоумышленника, он какое-то время использовал данное ПО для своих целей, однако затем сменил род деятельности.

Можно сказать, что основная деятельность этого злоумышленника по продаже доступов в корпоративные сети началась в июле 2020 года, когда он создал учетную запись с псевдонимом barf на популярном андеграундном форуме Exploit. Именно на этом форуме были опубликованы все его объявления о продажах доступов.

После регистрации barf создал тему о поиске разработчика, способного написать ПО для брутфорса RDP и проверки на наличие доступа с правами администратора, версии ОС и другой информации.

Свою первую тему о продаже доступа в сеть он создал на форуме Exploit в декабре 2020 года. В ней он предлагал доступ в корпоративную сеть компании, расположенной в США, занимающейся благотворительностью.

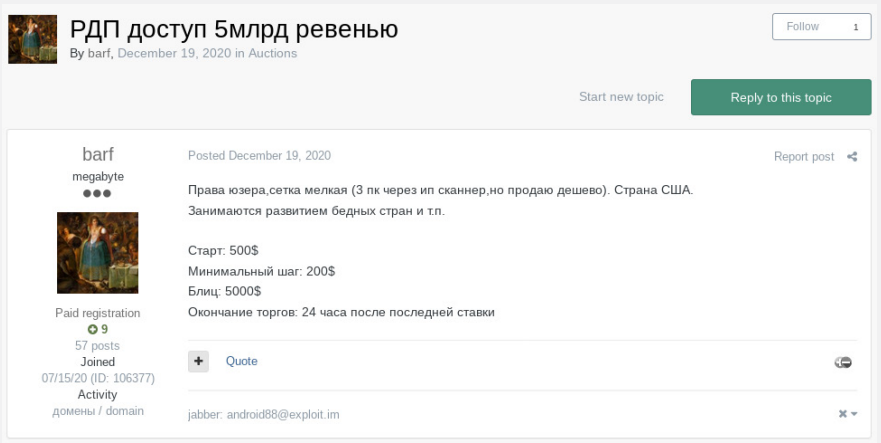


Рис. 48. Первая тема barf о продаже доступа в сеть

В отличие от большинства продавцов доступов в своих объявлениях barf часто указывал первые два октета IP-адресов жертв, что наводит на мысль об использовании IP-сканера.

Исходя из активности на форумах, он специализируется на продаже доступов в корпоративные сети только через RDP.

За период со 2-й половины 2020 по 1-ую половину 2021 года barf являлся одним из наиболее активных продавцов доступов к корпоративным сетям.

За все время активности на форуме Exploit barf выложил на продажу 145 RDP-доступов. Как видно из диаграммы ниже, большинство из его жертв располагаются в США, далее идут Великобритания и Австралия. Одинаковое процентное соотношение с доступами из США имеют доступы из категории “Other”: эта категория включает в себя общее количество доступов к компаниям из других стран, не представленных на диаграмме, каждая из которых в отдельности составляет не более 2% от общего количества выставленных на продажу данным злоумышленником доступов.

Страна	%
США	22
Великобритания	11
Австралия	10
Франция	9
Бразилия	7
Италия	7
Испания	6
Германия	3
Швеция	3
Другие	22

Индустрия	%
Торговля и шоппинг	19
Производство	16
Профессиональные услуги	12
Транспорт	7
Еда и напитки	6
Информационные технологии	6
Путешествия и туризм	6
Недвижимость	5
Наука и инженерия	4
Природные ресурсы	3
Административные услуги	2
Здравохранение	2
Программное обеспечение	2
Другие	10

Мы заметили, что его излюбленными жертвами являются торговые и производственные компании, а также компании из сферы услуг. Однако сложно утверждать, что данный злоумышленник был заинтересован в какой-то определенной сфере, учитывая массовый характер его объявлений.

Минимальная стоимость доступа составляла 10 долларов, максимальная — $5000. По нашим подсчетам, за все время активности с декабря 2020 года, он потенциально мог заработать порядка 49 000 долларов на продаже RDP-доступов к корпоративным сетям.

Ниже в таблице указаны TTPs, предположительно используемые злоумышленником barf.

ATT&CK Matrix for Enterprise (barf)

Tactics	Techniques	Details
Reconnaissance	Active Scanning (T1595)	Атакующий сканировал устройства с открытыми RDP-сервисами
Initial access	External Remote Services (T1133)	Атакующий использовал учетные записи RDP для доступа в сети
Credential access	Brute Force (T1110)	Пользователь использовал вредоносное ПО для брутфорса RDP
	Brute Force: Credential Stuffing (T1110.004)	Злоумышленник предположительно использовал скомпрометированные ранее учетные записи для брутфорс-атаки, чтобы получить доступы к корпоративным сетям
Discovery	Network Service Scanning (T1046)	Злоумышленник получил информацию об установленном на хосте жертвы ПО Drake Software
	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы

babam

Активность	**май 2020 — сентябрь 2021**
Количество жертв	**37**
География атак	**15 стран**
Предположительный доход	**USD 25 000**

Одним из популярных брокеров первичного доступа в сеть является злоумышленник под псевдонимом babam. Впервые пользователь был замечен на форуме Exploit 23 января 2015 года. Последний раз злоумышленник был активен 28 сентября 2021 года. После этого его аккаунт на форуме был забанен.

Хотя деятельность данного злоумышленника на андеграундных форумах продолжалась с 2015 года, его первое объявление о продаже первичного доступа в корпоративную сеть было опубликовано 11 мая 2020 года. Автор продавал доступ Citrix XenApp к алжирской телекоммуникационной компании.

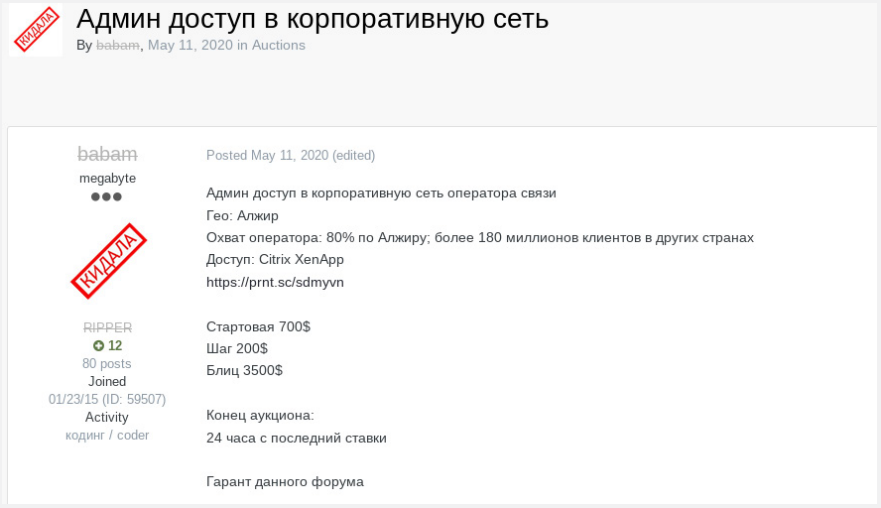


Рис. 49. Первое сообщение о продаже первичного доступа к корпоративной сети на форуме Exploit

В марте 2021 года злоумышленник упомянул, что использовал утилиту Mimikatz для извлечения информации из дампа сеанса.

26 июня 2021 года злоумышленник babam создал тему на Exploit о продаже доступа Citrix к сети крупного банка с доходом в 30 миллиардов долларов. Пользователь упомянул, что этот банк находится в Великобритании и США.

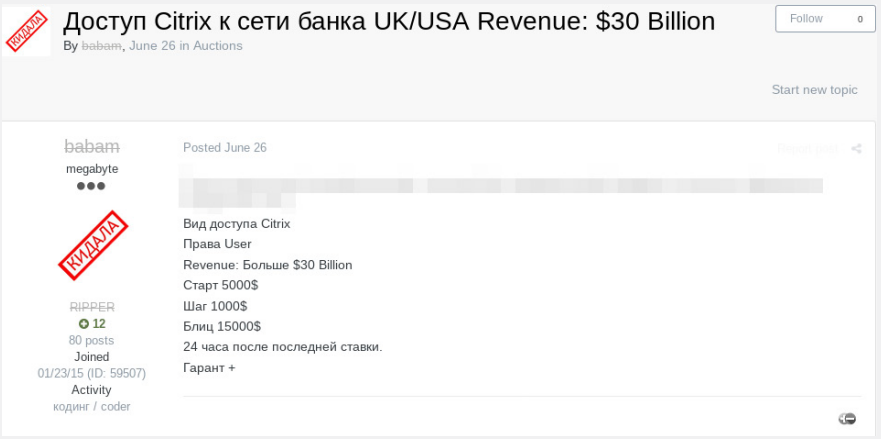


Рис. 50. Объявление о продаже Citrix доступа к корпоративной сети крупного банка

Данная жертва была одной из самых крупных из тех, к которым злоумышленник предоставлял доступы. 28 июня 2021 года продавец сообщил о продаже доступа.

По нашим данным, злоумышленник вероятнее всего использовал инструмент для брутфорса RDP, созданный пользователем z668. В июне 2017 года и в октябре 2020 babam изъявлял желание о покупке данного инструмента в соответствующих темах. Основываясь на этом факте, мы предполагаем, что babam сканирует уязвимые порты RDP и перебирает их при помощи этого или аналогичного ПО.

Специалисты Group-IB обнаружили, что babam выставил на продажу всего 37 объявлений на андеграундных форумах о продаже первичных доступов к корпоративным сетям. По нашим подсчетам общая стоимость доступов составила от 25 000 долларов.

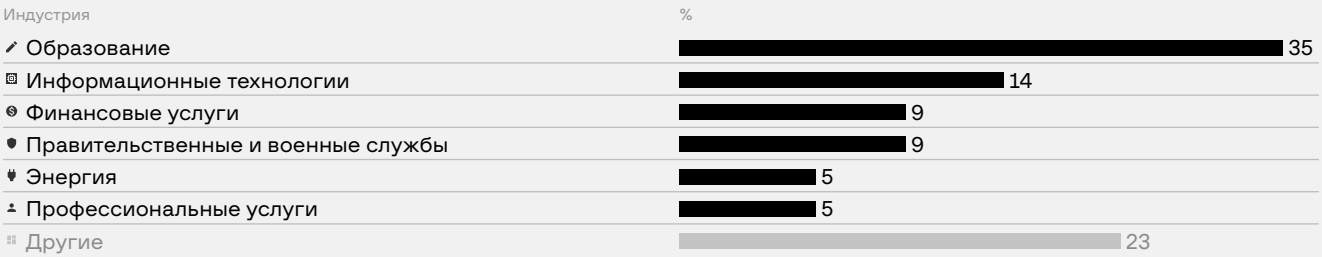
Среди них были доступы Citrix, RD Web, RDP, VPN и Cisco VPN — типы доступов с правами администратора или пользователя.

Как показано на диаграмме ниже, основной акцент злоумышленник делал на доступы вида RD Web и Citrix. Реже доступ к его жертвам был получен через RDP.

Жертвы данного злоумышленника в основном находятся в США, а также в других странах Америки и Европе. Распределение всех обнаруженных доступов по странам показано на диаграмме ниже. Всего злоумышленником было атаковано 18 стран.

Судя по распределению жертв по индустриям, babam в основном был нацелен на образовательные учреждения, они составляют 35% от всех его жертв, далее идут IT-компании и финансовые организации.

Страна	%
США	23
Испания	13
Канада	10
Австралия	8
Франция	5
Нидерланды	5
Великобритания	6
Аргентина	5
Другие	26



ATT&CK Matrix for Enterprise (babam)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	Злоумышленник использовал учетные записи RDP, VPN, Citrix для доступа в сеть
	Valid Accounts: Domain Accounts (T1078.002)	Злоумышленник использовал скомпрометированные доменные учетные записи для доступа в сеть
	Valid Accounts: Local Accounts (T1078.003)	Злоумышленник использовал скомпрометированные локальные учетные записи для доступа в сеть
Credential access	OS Credential Dumping (T1003)	Злоумышленник использовал Mimikatz для извлечения информации из дампа сессии
	Brute Force (T1110)	Злоумышленник использовал вредоносное ПО для брутфорса RDP
Discovery	Account Discovery (T1087)	Пользователь указывал информацию о количестве хостов в сети жертвы

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

09

С увеличением числа продавцов первоначальных доступов, увеличилось и число используемых ими TTPs. Основываясь на информации о них, мы рекомендуем выполнять следующие действия:

1. **Настройка блокировки учетной записи.** Для получения доступа злоумышленники зачастую подбирают пароли для учетных записей. Число попыток аутентификации при брутфорс-атаке несравнимо превышает число попыток в случае, если пользователь ошибается при вводе пароля. Для предотвращения такого типа атак можно установить функцию блокировки учетной записи на определенное время, которая включится при превышении определенного числа неудачных попыток аутентификации.
2. **Проверка логинов и паролей в публичных утечках.** Часто в целях создания словарей для брута злоумышленники используют уже скомпрометированные данные из различных утечек — так называемые комбо-листы (набор из логина и пароля). Таким образом, превентивная проверка на утечку данных ваших сотрудников может существенно снизить вероятность успешной атаки. Проводить такие проверки позволяет система Group-IB Threat Intelligence & Attribution.
3. **Превентивные меры по выявлению утечек, выставленных на продажу в андеграунде.** Для оперативного реагирования на возможные утечки данных рекомендуется использовать системы класса Threat Intelligence, которые отслеживают любое появление данных по конкретной компании в даркнете, что позволит предпринять необходимые меры по обеспечению безопасности данных и выявить потенциальный канал утечки.
4. **Установка специализированного программного обеспечения для выявления аномалий на сервере.** Такое ПО позволяет выявить появление новых учетных записей, аномалий в трафике или попыток неправомерного доступа к каким-либо данным.
5. **Введение «белых списков» IP-адресов.** Стоит ограничить доступ к удаленным серверам только определенному списку IP-адресов. Если в компании есть сотрудники, работающие удаленно, то стоит настроить корпоративный VPN.
6. **Отключение или блокировка** невостребованных удаленных сервисов.
7. **Использование многофакторной аутентификации** для учетных записей удаленных сервисов. Это ограничивает возможности использования скомпрометированных учетных данных.

8. **Использование сложных уникальных паролей**.
9. **Использование минимальных привилегий** для учетных записей служб ограничивает права, получаемые процессом, уязвимость в котором может быть использована.
10. **Своевременное и регулярное обновление программного обеспечения**, которое позволяет закрывать обнаруженные уязвимости.
11. **Регулярное проведение анализа защищенности** и тестирования на проникновение, чтобы выявить «слабые места» в сети и возможные векторы атак.
12. **Проведение инвентаризации внешнего сетевого периметра**, правил межсетевого экранирования (Firewall) и правил трансляции сетевых адресов (NAT) для исключения ошибочно опубликованных сервисов.
13. **Запрет на публикацию в сети Интернет устройств**, которые могут быть легко скомпрометированы: видеонаблюдение, «умный дом», оргтехнику (принтеры, сканеры, МФУ), устройства хранения (типа NAS-серверов сегмента SOHO).
14. **Запрет на публикацию на внешнем сетевом периметре сервисов** непосредственного удаленного доступа для операционных систем (RDP, SSH, VNC, SMB/RPC и др.).
15. **Ограничение сетевого доступа** по задачам конкретной учетной записи (к примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети).
16. **Выставление поля вида «expires at»** для учетных записей и правил доступа на случай, если даст сбой процесс ручного отзыва удаленного доступа.
17. **Выявление признаков изначального доступа**, закрепления в системе, продвижения по сети. Хотя чаще всего техники атакующих достаточно примитивны, и их видно невооруженным глазом, с более сложными атаками может помочь регулярная проактивная охота за угрозами (threat hunting).
18. **Детектирование и регулярная дополнительная проверка** своей инфраструктуры на известные индикаторы компрометации.
19. **Запрет пользователям регистрироваться на сторонних сервисах** с использованием корпоративной почты, так как пользователи склонны использовать один пароль (или его модификации) на многих сервисах. При утечке паролей из одного сервиса злоумышленник может атаковать всю компанию.

Требования к средствам информационной безопасности:

20. **Детектирование следов использования** популярных пост-эксплуатационных фреймворков
21. **Обнаружение аномальной активности** в контексте использования легитимного программного обеспечения, установленного в организации. Например, запуск нетипичных процессов, создание файлов, модификации файловой системы или реестра, характерные для техник закрепления в системе и т.п.

ПРОГНОЗЫ РАЗВИТИЯ РЫНКА

10

За последний год количество предложений на рынке доступов выросло в 3 раза, в то время, как объем рынка вырос лишь на 14%. По нашим подсчетам такая ситуация была вызвана резким увеличением количества продавцов доступов на рынке (аналогично, в 3 раза за год), что повлекло за собой рост конкуренции. В условиях, когда злоумышленник не обладает навыками для закрепления в сети или при неправильном использовании доступа, он может быть быстро утерян. В таком случае злоумышленники могут стремиться как можно скорее продать доступ ниже рыночной стоимости. Часто для этого злоумышленники снижают цену до нескольких сотен долларов, что практически всегда гарантирует им продажу. Такая тенденция вероятно приведёт к снижению стоимости доступов в будущем, что сделает их еще более привлекательным товаром.

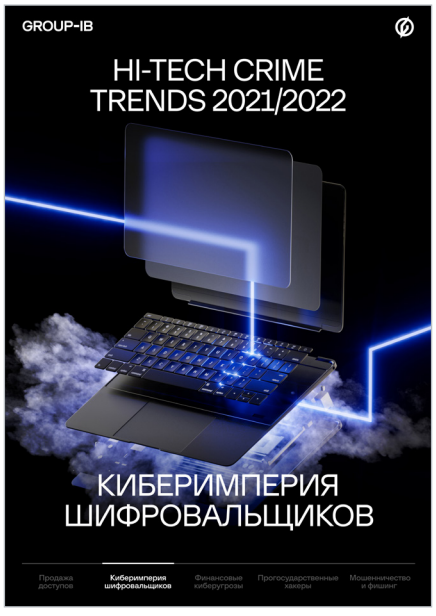
Подчеркнем, что на данный момент наблюдается прямая зависимость стоимости доступов от дохода компании: чем она выше, тем выше цена и тем более уязвимыми становятся крупные международные компании. Можно сказать, что если не принять меры по защите корпоративной сети, то конечном итоге это приведет к ее компрометации и потенциальному ущербу для бизнеса.

Стоит отметить, что популярность рынка продаж доступов во многом зависит от популярности программ-вымогателей. Специалисты Group-IB сделали вывод о том, что многие операторы шифровальщиков активно пользовались и, возможно, продолжают пользоваться услугами популярных брокеров первичного доступа, повышая спрос на них в андеграунде. Как показано в отчете «**Киберимперия шифровальщиков**» тренд на использование программ-вымогателей продолжит набирать популярность и, как следствие, приведет к увеличению атак на компании по всему миру.

На данный момент использование RaaS является основным способом монетизации доступов к корпоративным сетям. Повышение спроса на программы-вымогатели также продолжит способствовать появлению новых продавцов на рынке доступов и увеличению их общего количества.

С активным развитием рынка первоначальных доступов постепенно сформировалась единая концепция среди продавцов. Так появилось общее представление о ценообразовании доступа и популярности стран среди покупателей. Можно смело сказать, что злоумышленники останутся наиболее заинтересованы в получении доступов к компаниям из США, а также странам Ближнего Востока и APAC, в то время, как интерес к странам СНГ и Африки останется на низком уровне или пойдет на убыль.

Киберимперия шифровальщиков



Сокрытие части данных в объявлениях является ответной реакцией злоумышленников на работу исследователей, которые могут оповестить компанию о продаже доступа к ее сети. Так как рынок существует уже не один год, влиятельные продавцы доступов, скорее всего, уже имеют постоянных клиентов, которым могут предложить товар, минуя форум. Вполне вероятно, что скоро злоумышленники создадут отдельные закрытые ресурсы для продажи.

И последний прогноз: хотелось бы отметить появление новых точек входа в корпоративную сеть. Ими могут быть как новые решения для удаленного доступа или виртуализации, платформы для построения компьютерных сетей, облачные сервисы, так и продукты, уже представленные на рынке, в которых могут быть обнаружены уязвимости, позволяющие с легкостью заполучить доступ на устройствах с необновленным ПО, как это было в случае Citrix, FortiGate, Pulse Secure.

Так, например, в настоящее время компании все чаще переходят на единую авторизацию известного SSO-провайдера, поэтому можно сделать предположение, что она станет новым вектором атаки: злоумышленники будут получать доступ к приложениям и сервисам, которые доступны через данное решение.

Group-IB

— один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

Миссия Group-IB: Fight Against Cybercrime

Interpol и Europol

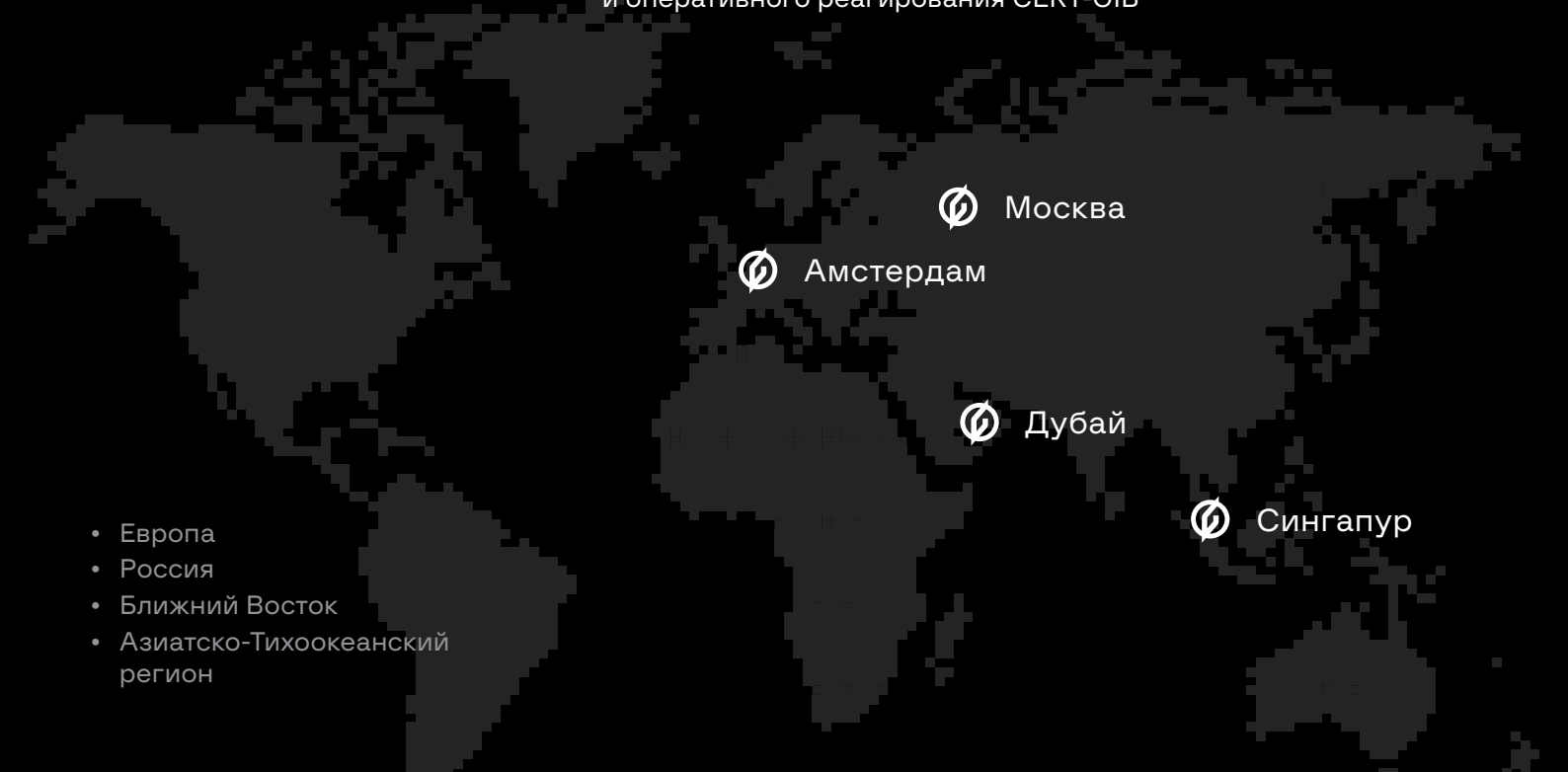
Group-IB — партнер и участник совместных расследований

Топ-10 в APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Реагирование и исследование киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



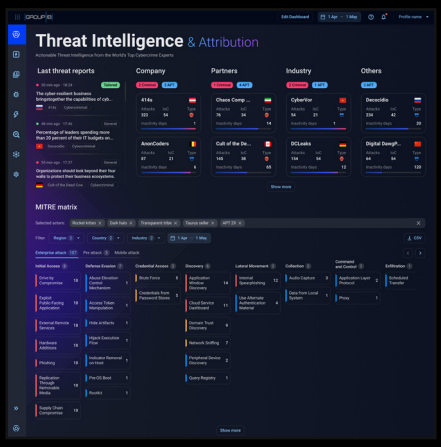
- Европа
- Россия
- Ближний Восток
- Азиатско-Тихоокеанский регион

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединяющую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества.

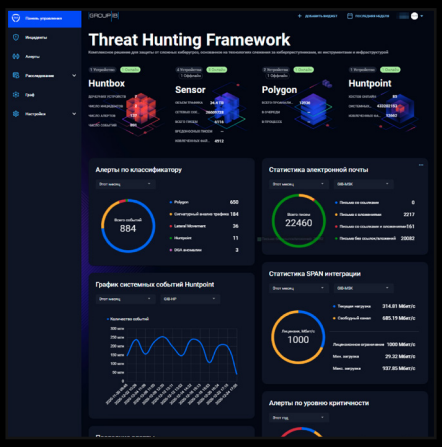
Решения Group-IB признаны мировыми агентствами

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN



Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры

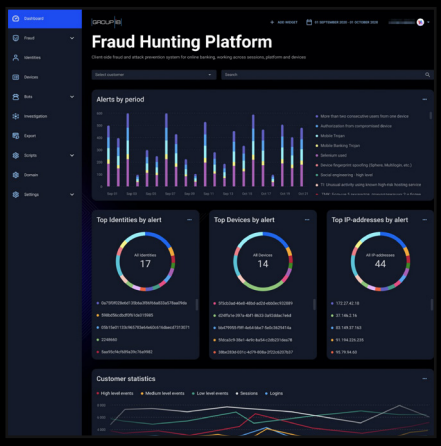


Threat Hunting Framework

Система защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта



Fraud Hunting Platform

Цифровая защита и противодействие мошенничеству в реальном времени

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

AssetZero

Мониторинг внешнего периметра с помощью данных киберразведки

Экспертиза Group-IB

600+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

В основе технологического лидерства компании, возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

Предотвращение

- Аудит безопасности
- Оценка безопасности
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Обучение

Реагирование

- Managed Incident reponse
- Managed detection and threat hunting

Расследование

- Компьютерная криминалистика
- Расследования
- Финансовые расследования
- eDiscovery

ПРЕДОТВРАЩАЕМ И ИССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru info@group-ib.com group-ib.ru/blog +7 495 984 3364