FXMSP «НЕВИДИМЫЙ БОГ СЕТИ»[1]

Один из самых известных продавцов доступа к корпоративным сетях

ROOT LEVEL RESOURCES

44
государства, пострадавших от нападений

135
атакованных компаний

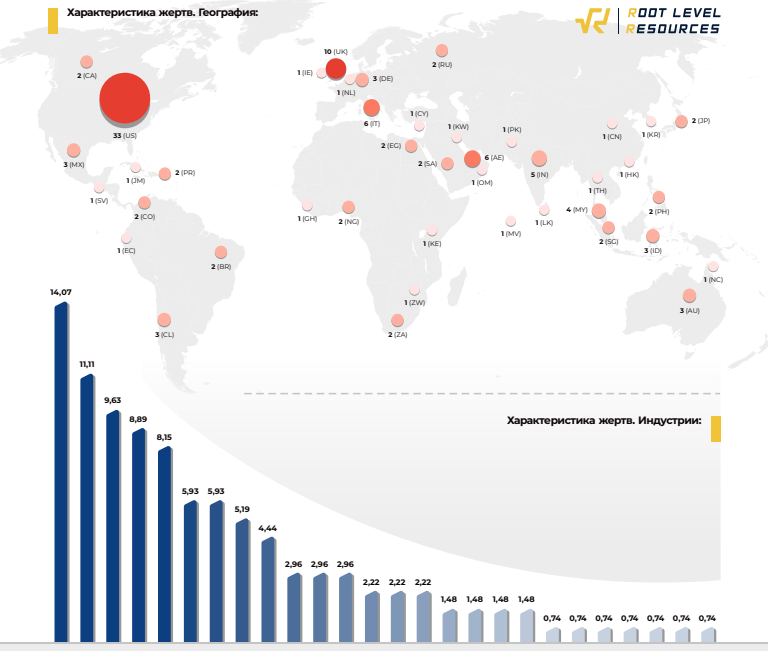
$1 500 000+
минимальная оценка выручки от продаж[2]

Более 3 лет
активности на андеграундных форумах

01 октября 2017 года - "день рождения" Fxmsp. В этого день, 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.

Но известным на весь мир это имя стало в мае 2019 года, благодаря новости о получении доступа в защищенные сети трех ведущих антивирусных компаний.[3] Fxmsp скопировали из внутренних сетей вендоров различные фрагменты кода антивирусных продуктов, модули аналитики, документацию по разработке и др. Этот лот был выставлен за $300 000. Fxmsp писал о том, что это была целенаправленная акция. Ему понадобилось чуть больше трех лет, чтобы из рядового пользователя хакерского форума, незнающего, как монетизировать свои навыки взлома, стать одним из главных игроков русскоязычного андеграунда – со своим пулом постоянных клиентов и даже менеджером по продажам.

Характеристика жертв. География:



Характеристика жертв. Индустрии:

Интересно, что порядка 9% составляли сети, принадлежащие государственным компаниям. Между тем, среди атакованных Fxmsp компаний был и "крупный улов": так, 4 из "пойманных на крючок" входят в рейтинг "Global 500|Fortune" за 2019 год.

Тактики и нструменты

ROOT LEVEL RESOURCES

В отличие от большинства атакующих, Fxmsp не использует стандартные фишинговые рассылки для проникновения в сеть и не изучает жертву перед атакой, что исключает таргетированный характер его действий и указывает на массовость. Ниже приведены основные этапы "удара" и его движения по сети.

Сканирование определенного диапазона IP-адресов

Это достаточно известный и простой подход – для сканирования используются IP-адреса города или страны на наличие определенных открытых портов. Для этих целей он использует широко распространённое программное обеспечения Masscan, а также более продвинутые сканеры. Основной целью этого этапа обычно являются открытые RDP[4] порты, а именно 3389. Именно этот порт является целевым для Fxmsp, так как он используется для обеспечения удаленного доступа к серверам и рабочим станциям MS Windows.

Подготовка к атаке

После сканирования диапазона IP-адресов и выделения потенциальных жертв с открытыми RDP портами злоумышленнику необходимо уменьшить количество входных данных для брута. Для этих целей используется ПО с наименованием RDP Recognizer. На большинстве удаленных серверов под управлением Windows существует возможность увидеть экран авторизации со списком всех учетных записей на сервере. С помощью OCR любой RDP Recognizer пытается распознать логины всех учетных записей на сервере. В случае успеха злоумышленнику остается подобрать методом брутфорса только пароли.

Брутфорс-атака

На этом этапе злоумышленник использует различные программы для брутфорса на серверы жертвы. Атаки этого типа представляют собой попытки подбора пароля для RDP путем систематического перебора всех возможных вариантов, пока не будет найден верный. Может использоваться перебор как комбинаций символов, так и перебор по словарю популярных или скомпрометированных паролей.

Обеспечение персистентности

После получения доступа к целевой машине злоумышленник отключает антивирусное ПО и Firewall, а также создает дополнительные учетные записи для доступа. Далее идет закрепление в сети. Предположительно, для этой цели Fxmsp в качестве бэкдора на серверах использует полезную нагрузку Meterpreter. Стоит отметить, что при установке бэкдоров, Fxmsp назначает очень большой интервал соединений с CnC – раз в 15 дней.

Исследование сети

После закрепления на отдельной машине следующей целью является получение доступа к контроллеру домена. Предположительно, Fxmsp ищет аккаунты с административными правами, что позволяет легко получить доступ к искомым данным. Затем злоумышленник извлекает дампы всех учетных записей и пытается их расшифровать Известно, что для дешифровки, в том числе, используется Windows Password Recovery. Это ПО позволяет автоматизировано загружать базы пользователей из SAM или ntds.dit и обладает функцией дешифровки хэшированных паролей.

Инфицирование бэкапов

Также, как и с изначальным сервером, Fxmsp ставит бэкдоры с большим интервалом и на бэкапы. Таким образом, даже если жертва заметит подозрительную активность в системе, то скорее всего, произойдет смена паролей и откат к бэкапу, который уже скомпрометирован.

Монетизация

На основном этапе своей деятельности Fxmsp продает полученные доступы на андеграундных форумах. Вначале он делал это сам, потом с помощью сообщника Lampeduza. Изначально он устанавливал на серверы вредоносное ПО для майнинга криптовалюты.

Однако до сих пор наиболее плодовитый "продавец доступов" остается на свободе, представляя угрозу для компаний широкого диапазона отраслей независимо от того, в какой стране они находятся.

Для предотвращения подобных инцидентов помогут следующие действия:

Превентивные меры по выявлению утечек, выставленных на продажу в андеграунде

Для оперативного реагирования на возможные утечки данных рекомендуется использовать системы класса Threat Intelligence, которые в автоматизированном режиме отслеживают любое появление данных по конкретной компании в даркнете, что позволит предпринять все необходимые шаги по обеспечению безопасности данных, а также выявить потенциальный канал утечки.

Смена стандартного RDP порта 3389

Учитывая, что атаки обычно носят не таргетированный характер, злоумышленник обычно перебирает стандартные порты для поиска RDP. Данный порт можно отредактировать, поменяв на любой другой.

Проверка логинов и паролей в публичных утечках

Часто в целях создания словарей для брута злоумышленник использует уже скомпрометированные данные из различных утечек – так называемые комбо-листы.[5] Таким образом, превентивная проверка на наличие данных сотрудников в утечках может существенно снизить вероятность успешной атаки.

Установка специализированного ПО для выявления аномалий на сервере

Такое ПО позволяет выявить появление новых учетных записей, аномалий в трафике или попыток неправомерного доступа к каким-либо данным.

Введение "белых списков" IP-адресов

Стоит ограничить доступ к удаленным серверам только определенному списку IP адресов. Если многие сотрудники работают удаленно, то стоит настроить корпоративный VPN.

Отключение вывода информации о последнем авторизованном пользователе на сервере

Для этого необходимо изменить групповую политику в ActiveDirectory, установить параметр "Interactive logon: Do not display last user name" - на disabled.

Настройка блокировки учетной записи

Так как злоумышленнику обычно нужно подбирать огромное число паролей для получения доступа к RDP, можно установить функцию блокировки учетной записи на время, которая включится в случае определенного числа неудачных попыток.

1 – В 2018 году Lampeduza опубликовав пост о продаже доступа к взломанным корпоративным сетям подписав: «...У вас будет полный доступ ко всей сети компании. Вы станете невидимым богом сети.»

2 – Эта сумма не учитывает в себе продаж в приватe, а также порядка 20% лотов по компаниям, доступ к которым Fxmsp предлагал, но цену не указывал

3 – https://www.bleepingcomputer.com/news/security/fxmsp-chat-logs-reveal-the-hacked-antivirus-vendors-avs-respond/

4 – Remote Desktop Protocol

5 – Набор из логина и пароля