ИЮНЬ 2020
GROUP-IB.RU

GROUP-IB

Fxmsp

“Невидимый бог сети”*

* - «Вы станете невидимым богом сети», эта фраза была указана в рекламном посте автора Lampeduza, продвигающего услуги Fxmsp по взлому корпоративных сетей и продаже доступа к ним.

ПРОФАЙЛ

НИК	**Fxmsp**
СПЕЦИАЛИЗАЦИЯ	**ПРОДАЖА ДОСТУПОВ В КОРПОРАТИВНЫЕ СЕТИ**
КОЛИЧЕСТВО ЖЕРТВ	**БОЛЕЕ 135 КОМПАНИЙ**
ГЕОГРАФИЯ ДЕЯТЕЛЬНОСТИ	**44 СТРАНЫ**
ПЕРИОД АКТИВНОСТИ	**> 3 ЛЕТ**
СУММАРНЫЙ ЗАРАБОТОК	**КАК МИНИМУМ 1,5 млн. долл**

СОДЕРЖАНИЕ

*Раздел доступен только в полной версии отчета.

ВВЕДЕНИЕ

В октябре 2017 года на самом известном русскоязычном андеграундном форуме exploit[.]in появилось объявление о продаже доступа к корпоративным сетям ряда компаний – редкой для того времени услуги в андеграунде. 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.

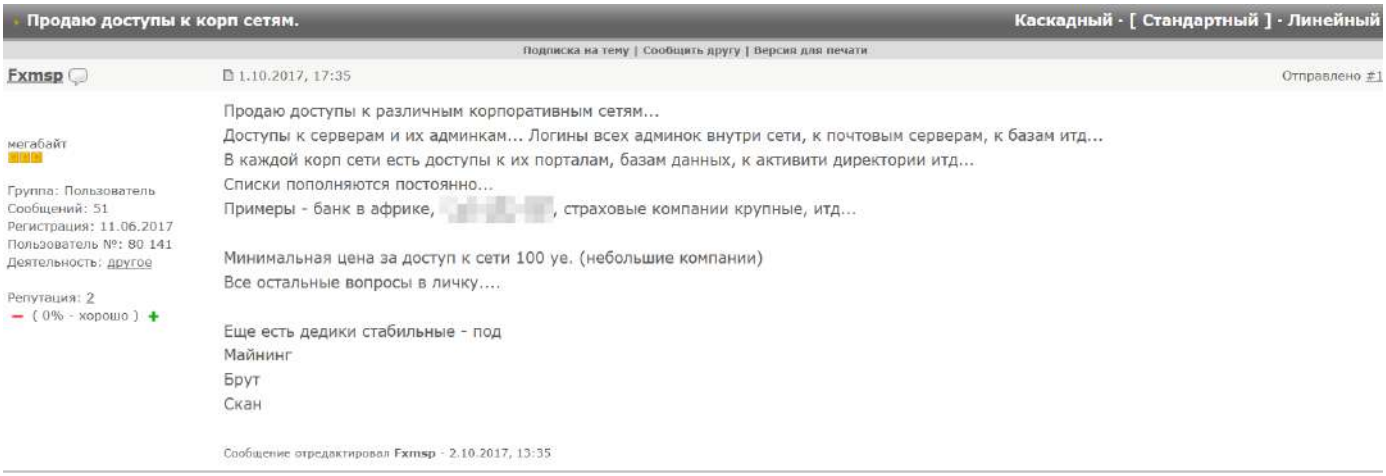


Рис.1 — Октябрь, 2017. Скриншот сообщения о старте продаж доступов к корпоративным сетям

1 октября 2017 года - “день рождения” Fxmsp, как одного из самых известных продавцов доступа к корпоративным сетям на андеграундных форумах. Но известным на весь мир это имя стало в мае 2019 года, благодаря новости о получении доступа в защищенные сети трех ведущих антивирусных компаний[1] . Fxmsp скопировал из внутренних сетей вендоров различные фрагменты кода антивирусных продуктов, модули аналитики, документацию по разработке и др. Этот лот, как сообщалось в СМИ, 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, не знающего, как монетизировать свои навыки взлома, стать одним из главных игроков русскоязычного андеграунда – со своим пулом постоянных клиентов и даже менеджером по продажам.

К моменту появления скандальной новости о взломе трех антивирусных вендоров, Fxmsp фактически закончил свою “публичную” деятельность. 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. В связи с этим командой **Group-IB Threat Intelligence & Attribution** было принято решение о подготовке данного отчета, передачи его расширенной версии международным правоохранительным органам и обнародовании имею-щихся материалов об инструментах и тактике Fxmsp.

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

КЛЮЧЕВЫЕ ВЫВОДЫ

РАСКРЫТИЕ ОСНОВНЫХ ЭТАПОВ ДЕЯТЕЛЬНОСТИ

Специалисты Group-IB Threat Intelligence & Attribution изучали преступную деятельность Fxmsp с момента его регистрации на первом андеграундном форуме в сентябре 2016 года до фактического прекращения его активности в конце 2019 года. Путь Fxmsp по продаже доступов к корпора-тивным сетям можно разделить на 3 этапа. Они представлены в таблице ниже:

октябрь 2017 - 31 июля 2018
Заработок: $268 800

1 РАЗГОН

Все доступы продаются лично Fxmsp, основная активность ведется на хакерском форуме exploit[.]in

июль - октябрь 2018
Заработок: $1 100 800

2 ПАРТНЕРСТВО Fxmsp И Lampeduza

Fxmsp находит сообщника и передает функции менеджера по продажам пользователю с ником Lampeduza. Lampeduza занимается продвижением, контактами и реализацией доступов в скомпрометиро-ванные Fxmsp компании.Этап заканчивается блоки-ровкой сообщников на форуме exploit[.]in

март 2019 - сентябрь 2019
Заработок: $124 100

3 СКРЫТАЯ УГРОЗА

Lampeduza восстанавливает продажу доступов на других форумах. Их сотрудничество с Fxmsp продолжается до осени 2019 года.

ХАРАКТЕРИСТИКА ЖЕРТВ: ГЕОГРАФИЯ И ИНДУСТРИИ

Чуть более чем за 3 года Fxmsp удалось получить доступ к корпоративным сетям компаний в более чем 44 странах. По подсчетам исследователей команды Group-IB Threat Intelligence & Attribution, прибыль Fxmsp за все время его активности могла составлять как минимум **1,5 млн долларов.** Эта сумма не учитывает продаж в привате, а также порядка 20% лотов по компаниям, доступ к которым он предлагал, но цену не указывал.

Fxmsp не специализировался на компрометации определенных компаний, среди его жертв были как крупные банки и международные сети отелей, так и маленькие школьные сайты.

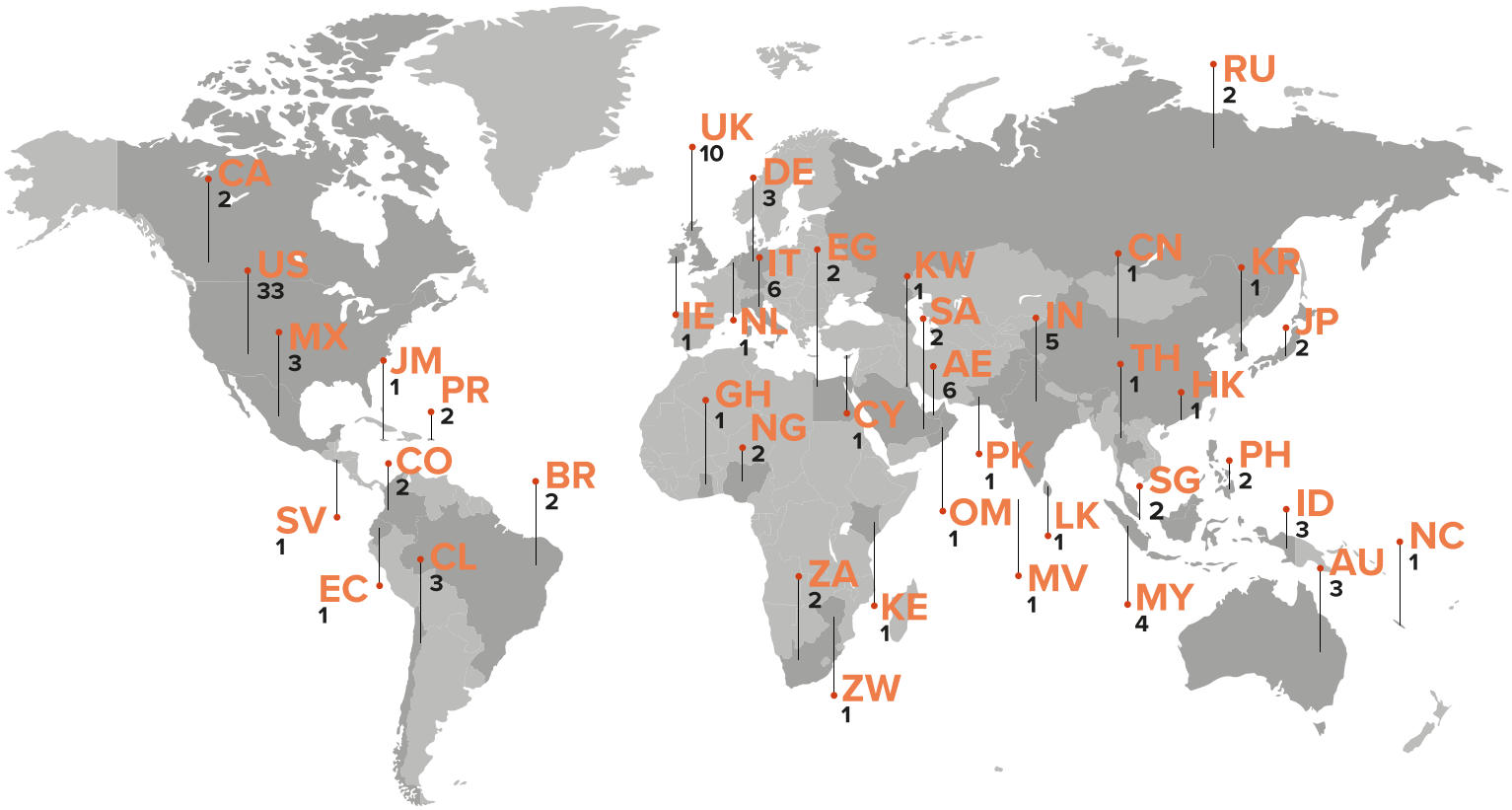


*Рис. 2— География расположения жертв Fxmsp**

*На карте не учтены международные компании со многими регионами присутствия (5), а также компании, доступ к которым Fxmsp предлагал без указания географии (8).

Рис. 3 — Распределение жертв Fxmsp по индустриям

Как видно на Рис.3, основная масса его жертв – это компании из сферы легкой промышленности, занятые мелким производством предметов массового потребления. На втором месте - провайдеры IT-сервисов. Замыкают тройку организации розничной торговли. Интересно, что порядка 9% составляли сети, принадлежащие государственным компаниям.

Между тем, среди атакованных Fxmsp компаний была и “крупная рыба”: так, 4 из них входят в рейтинг “Global 500 | Fortune” за 2019 год.

ТАЙМЛАЙН АКТИВНОСТИ НА АНДЕГРАУНДНЫХ РЕСУРСАХ

Пик активности Fxmsp пришелся на период с октября 2017 по сентябрь 2019. За это время он анонсировал продажу доступа к корпоративным сетям 135 компаний. Ниже представлен таймлайн публикаций постов о продаже доступов на андеграундных ресурсах:

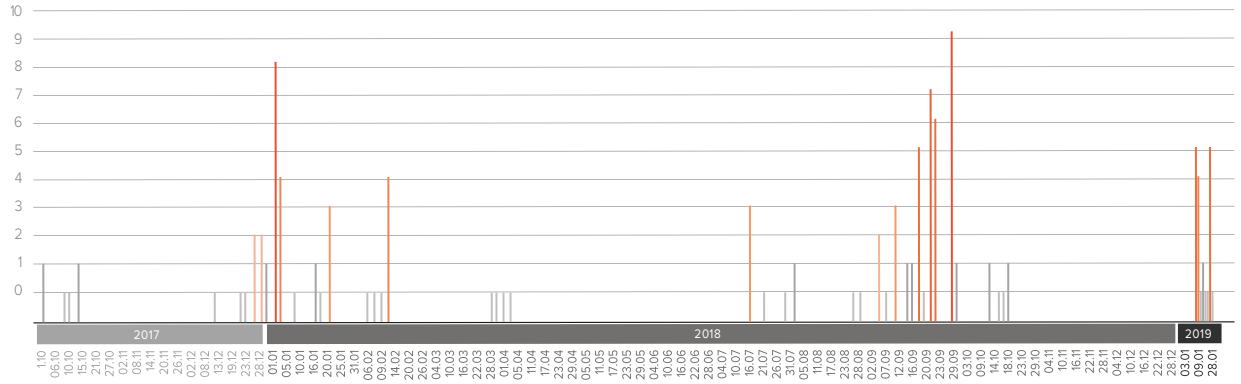


Рис. 4 –Таймлайн публикаций постов на даркнет-форумах о продаже доступов к скомпрометированным сетям компаний

ТАКТИКА И ИНСТРУМЕНТЫ

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. Тем не менее он успешно получал доступы к сетям крупных компаний. Ниже приведены основные этапы “пробива” и его движения по сети.

1. Сканирование определенного диапазона IP-адресов. Это достаточно известный и простой подход – для сканирования могут использоваться IP-адреса города или страны на наличие определенных открытых портов. Исходя из некоторых постов, которые оставил злоумышленник на специализированных даркнет-форумах, для этих целей он использовал широко распространенное программное обеспечения **Masscan**, а также более продвинутые сканеры. Основной целью этого этапа обычно являлись открытые **RDP (Remote Desktop Protocol)** порты, а именно 3389. Именно этот порт был целевым для Fxmsp, так как он используется для обеспечения удаленного доступа к серверам и рабочим станциям MS Windows.

2. 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 обычно 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.

3. 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.

4. Обеспечение персистентности. После получения доступа к целевой машине злоумышленник, как правило, 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 использовал полезную нагрузку **Meterpreter**. Об этом свидетельствует тот факт, что в 2017 году он интересовался работой с Metasploit PRO. Fxmsp отдельно отмечал, что при установке бэкдоров, он назначает очень большой интервал соединений с CnC – раз в 15 дней.

5. Исследование сети. После закрепления на отдельной машине следующей целью является получение доступа к контроллеру домена. Предположительно, он искал аккаунты с административными правами, что позволяло легко получить доступ к искомым данным. Затем злоумышленник извлекал дампы всех учетных записей и пытался их расшифровать. Нам известно, что для дешифровки он использовал, в том числе, **Windows Password Recovery**. Это ПО позволяет автоматизированно загружать базы пользователей из SAM или ntds.dit и обладает функцией дешифровки хэшированных паролей.

6. Инфицирование бэкапов. Так же 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.

7. Монетизация. На основном этапе своей деятельности Fxmsp продавал полученные доступы на андеграундных форумах, сначала сам, потом с помощью сообщника **Lampeduza**. На более ранних этапах своей работы он устанавливал на серверы вредоносное ПО для майнинга криптовалюты.

В течение всего времени активности Fxmsp специалисты Group-IB наблюдали за его развитием, анализируя десятки постов в андеграунде. Данные, полученные в ходе исследования, позволили выявить инструменты, которые он использовал для компрометации компаний, определить – с большой степенью точности – число его жертв, а также установить предполагаемую личность киберпреступника. Как и всегда, в конце данного отчета мы приводим **рекомендации**, которые позволят защитить компании от атак, подобных тем, что проводил и, возможно, проводит Fxmsp и подобные ему злоумышленники.

ПЕРВЫЕ ШАГИ В АНДЕРГРАУНДЕ

В сентябре 2016 года пользователь под ником Fxmsp впервые регистрируется на известном в те времена хакерском форуме fuckav[.]ru (hxxps://fuckav[.]ru/member.php?u=36898).

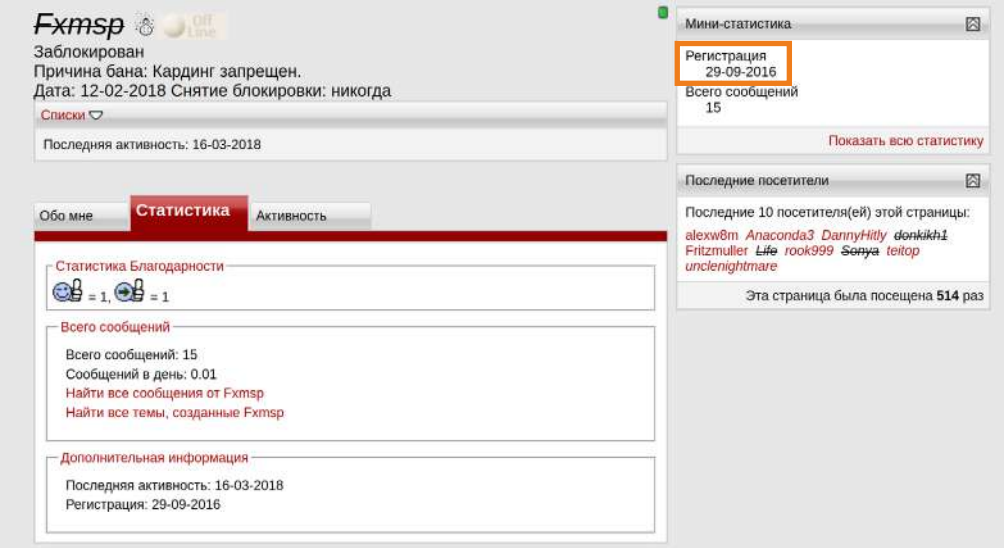


Рис. 5 — Сентябрь, 2016. Скриншот первого аккаунта пользователя «Fxmsp» на форуме fuckav[.]ru

По данным Group-IB Threat Intelligence & Attribution, на протяжении почти двух месяцев, с сентября 2016 года, Fxmsp не проявляет активности. Вероятнее всего, он изучал статьи, изредка оставляя комментарии к постам других пользователей форума, набираясь опыта и пытаясь найти еди-номышленников.

Скорее всего, на тот момент Fxmsp уже имел успешный опыт взлома корпоративных сетей. Однако он не знал, как монетизировать полученные доступы и выбирал наиболее простой путь. Вместо продажи, собственно, доступов он решает использовать ресурсы скомпрометированных компаний для майнинга криптовалюты: 11 ноября 2016 года злоумышленник пишет свой первый пост о поиске программы-майнера криптовалют с функциями самораспространения и персистентности (hxxps://fuckav[.]ru/showthread.php?t=30798).

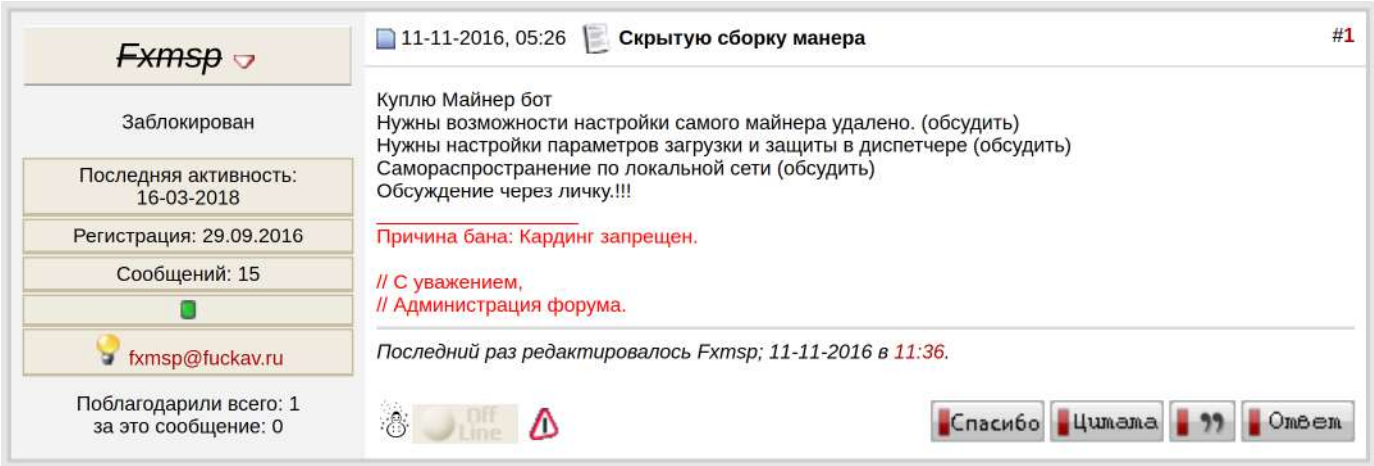


Рис. 6 — Ноябрь, 2016. Скриншот сообщения о поиске вредоносного ПО майнера криптовалют

На свой вопрос Fxmsp получает грубый ответ от другого, на тот момент более известного пользователя с ником **frec**, который просит его переходить к делу, а не задавать глупые вопросы. Это стандартная практика для андеграунда – люди, которые сидят на подобных форумах, не любят отвечать на вопросы новичков и обучать потенциальных конкурентов.

Вскоре Fxmsp начинает тестировать известный банковский троян **Atmos**, который на тот момент распространялся в паблике.

Atmos – это вариант вредоносной программы Citadel, основанной на трояне Zeus. Вредоносная программа используется для компрометации банковских данных с помощью модуля формграббера и веб-инжектов (поддерживаются инжекты под Zeus). Бот также может перехватывать данные карт в GET и POST-запросах и осуществлять автозаливы. Кроме того, троян обладает модулем VNC, обеспечивающим удаленный доступ к компьютеру жертвы. Троян может использовать кейлоггер/видеологгер и модуль для хищения файлов с машины жертвы. Кроме этого, троян обладает множеством других дополнительных функциональных возможностей. В июне 2016 года исходные коды данного трояна были опубликованы в публичном доступе.

Обычно, когда хакер только начинает делать первые шаги в мире киберпреступности, он не задумывается о том, что оставляет цифровой след, который в будущем может привести к раскрытию его личности. Так произошло и с Fxmsp. Он указал в своих контактных данных на форуме jabber-аккаунт - **fxmsp@fuckav[.]ru**. Опытные злоумышленники стараются никогда не публиковать свои контактные данные и предоставляют их только после контакта через личные сообщения на форумах.

В конце ноября того же года Fxmsp опубликовал свой последний пост перед долгим перерывом. Публикация была посвящена поиску вредоносного ПО для заражения сетей, как и ранее – с функциями самораспространения и персистентности.

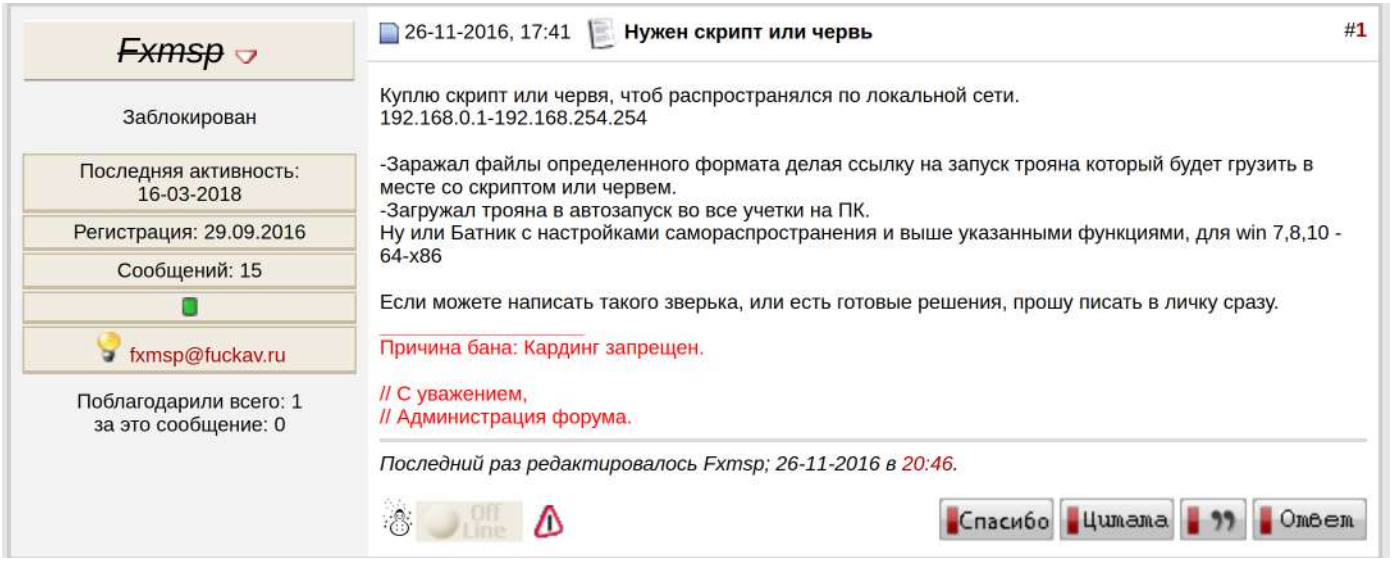


Рис. 7 – Ноябрь, 2016. Скриншот сообщения о поиске вредоносного ПО с функцией самораспространения

Его сообщение никто не прокомментировал: вероятно, он понял, что искать майнеры на публичных форумах бесполезно.
На протяжении полугода злоумышленник не проявлял активности на форумах, по всей видимости продолжая атаковать корпоративные сети. Следующее сообщение пользователя с ником Fxmsp появилось лишь в мае 2017 года. В своем посте он сообщал, что получил частичный доступ к крупной сети, которая разделена на три административные зоны. Также Fxmsp удалось получить RDP доступ на часть устройств.

Рис. 8 — Май, 2017. Скриншот сообщения о получении частичного доступа к крупной сети

Fxmsp понимал, что брутить все 6 000 серверов – бессмысленно, поэтому вновь обратился за помощью к пользователям андеграундного форума. Его основной целью было получение доступа к учётным записям администраторов домена. В ответ ему порекомендовали обратиться на форум exploit[.]in, где он потенциально мог найти специалистов, имеющих нужные мощности для взлома хэшей, которые хранятся в SAM (Security Account Manager).

Любопытно, что уже в тот же день, 11 мая 2017, пять часов спустя, после появления первого поста, Fxmsp сообщил о том, что его проблема решена.

Рис. 9 — Май, 2017. Скриншот сообщения о получении частичного доступа к крупной сети

В ходе дальнейшего исследования было выявлено, что данное сообщение было отредактировано. Системы Group-IB Threat Intelligence & Attribution позволяют мониторить все сообщения в анде-граунде в режиме реального времени и получать доступ как к оригинальным постам, так и к отредактированным со всей историей правок. Таким образом удалось выявить один из ин-струментов, который использовался злоумышленником для совершения атак на корпоратив-ные сети - Windows Password Recovery. Он позволяет автоматизировано загружать базы поль-зователей из SAM или ntds.dit и обладает функцией дешифровки хэшированных паролей. По словам самого Fxmsp, с помощью последней версии программы ему удалось расшифровать пароли от 90% аккаунтов.

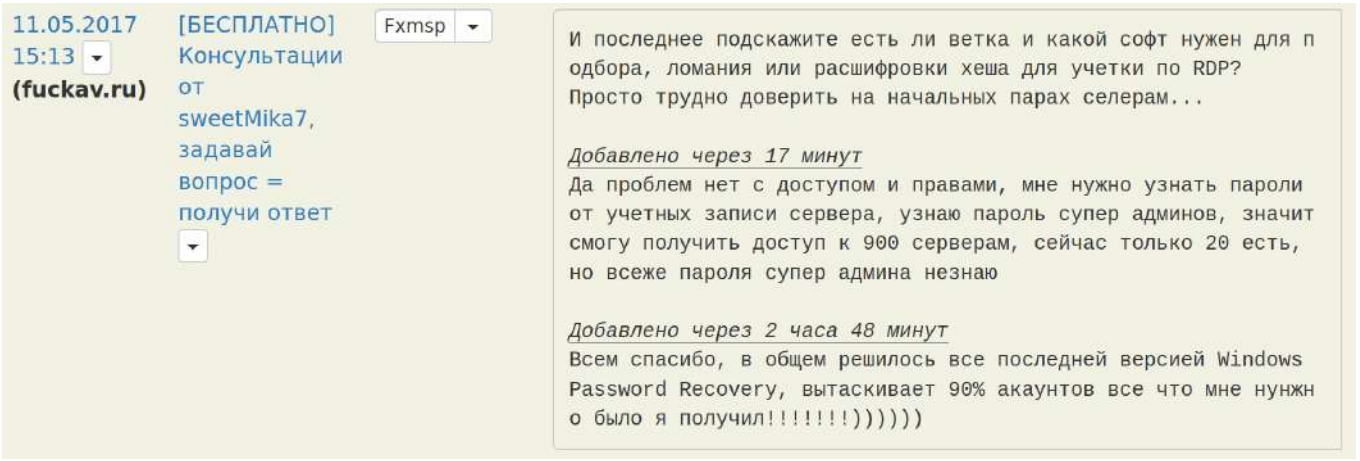


Рис. 10 — Май, 2017. Скриншот сообщения с описанием того, как злоумышленнику удалось получить пароли от аккаунтов

В июне 2017 года злоумышленник решил попробовать новые способы компрометации сетей и начал работать с известной программой для проведения пентестов Metasploit PRO. Fxmsp оставил сообщение на том же форуме, что ищет людей, которые готовы помочь ему с этим ПО или присоединиться к его команде на постоянной основе:

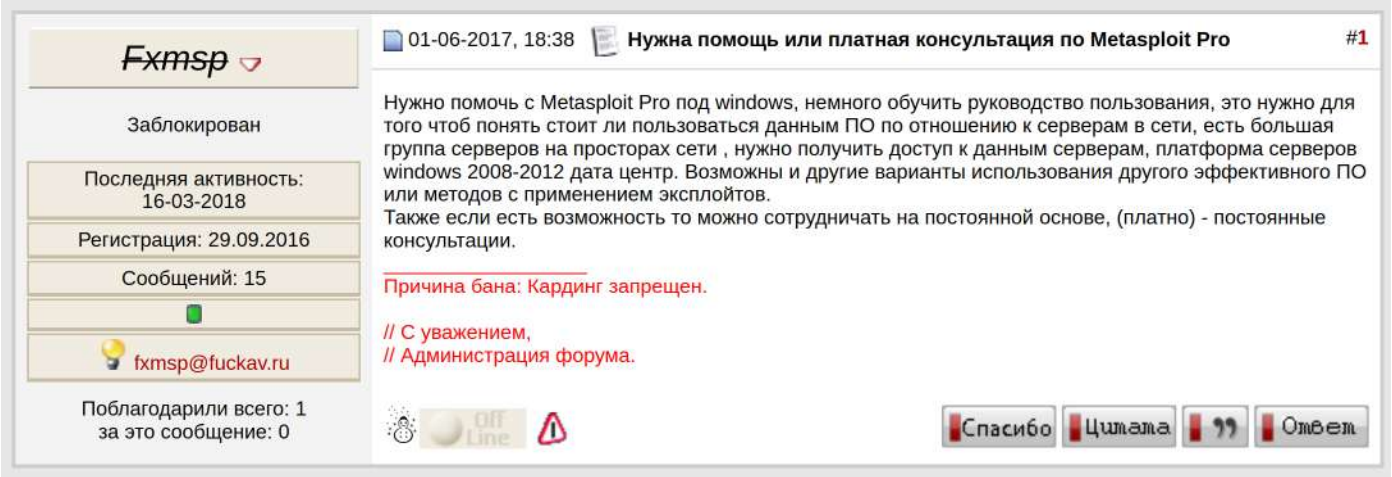


Рис. 11 — Июнь, 2017. Скриншот сообщения с поиском помощи по Metasploit PRO

Активность злоумышленника даже на одном андеграундном форуме позволяет получить общее понимание о его интересах и целях. Также мы видим контактные данные, которые тот использовал в начале своей деятельности:

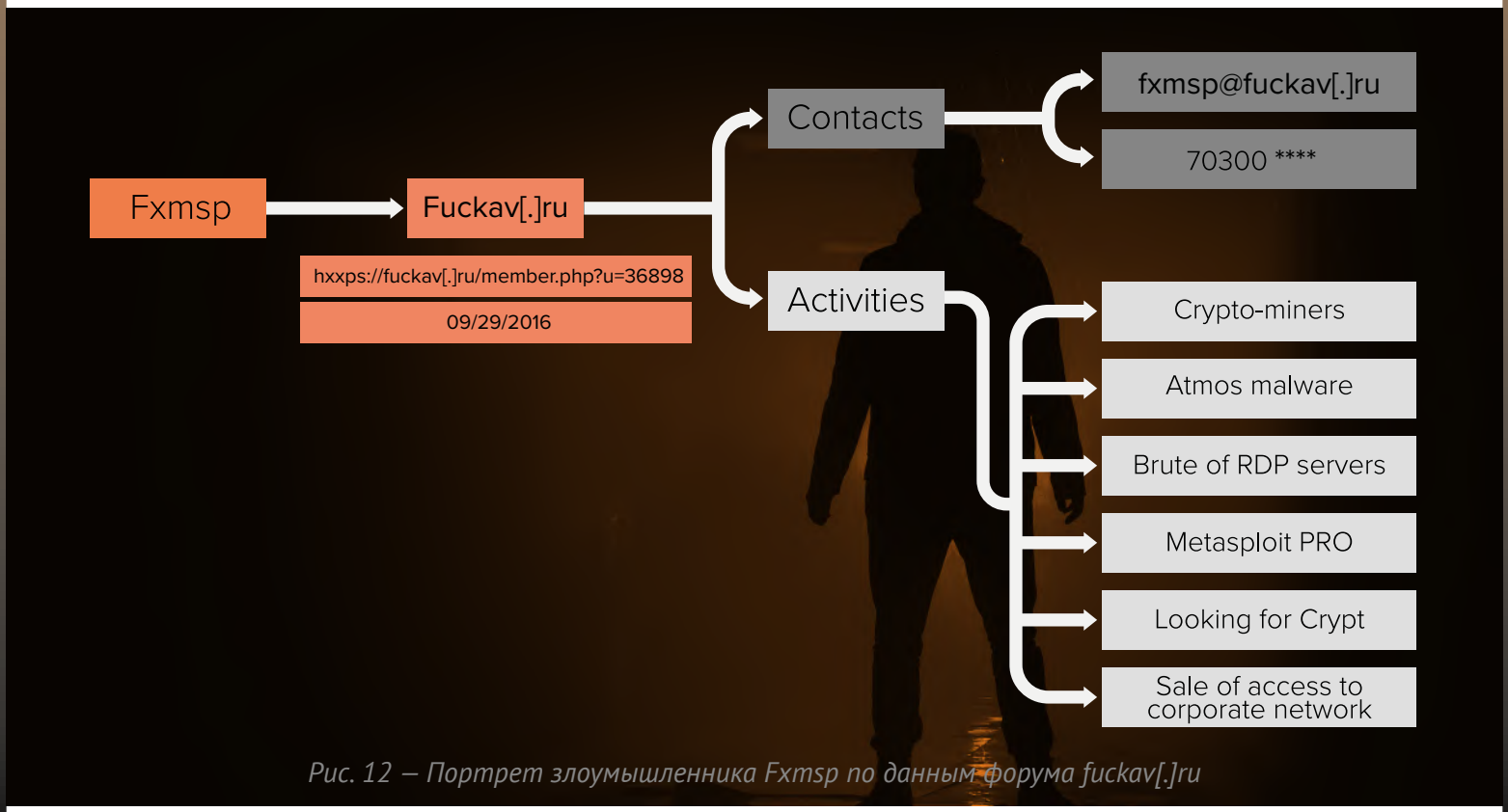
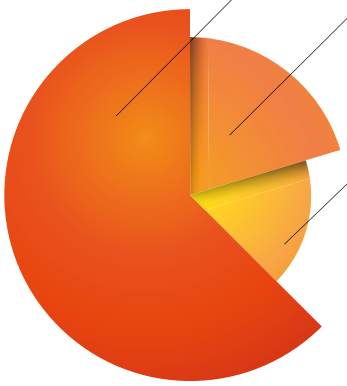


Рис. 12 — Портрет злоумышленника Fxmsp по данным форума fuckav[.]ru

Также в ходе исследования активности Fxmsp на форуме fuckav[.]ru удалось выявить инструменты, которые он использовал для закрепления в системе:



1 этап

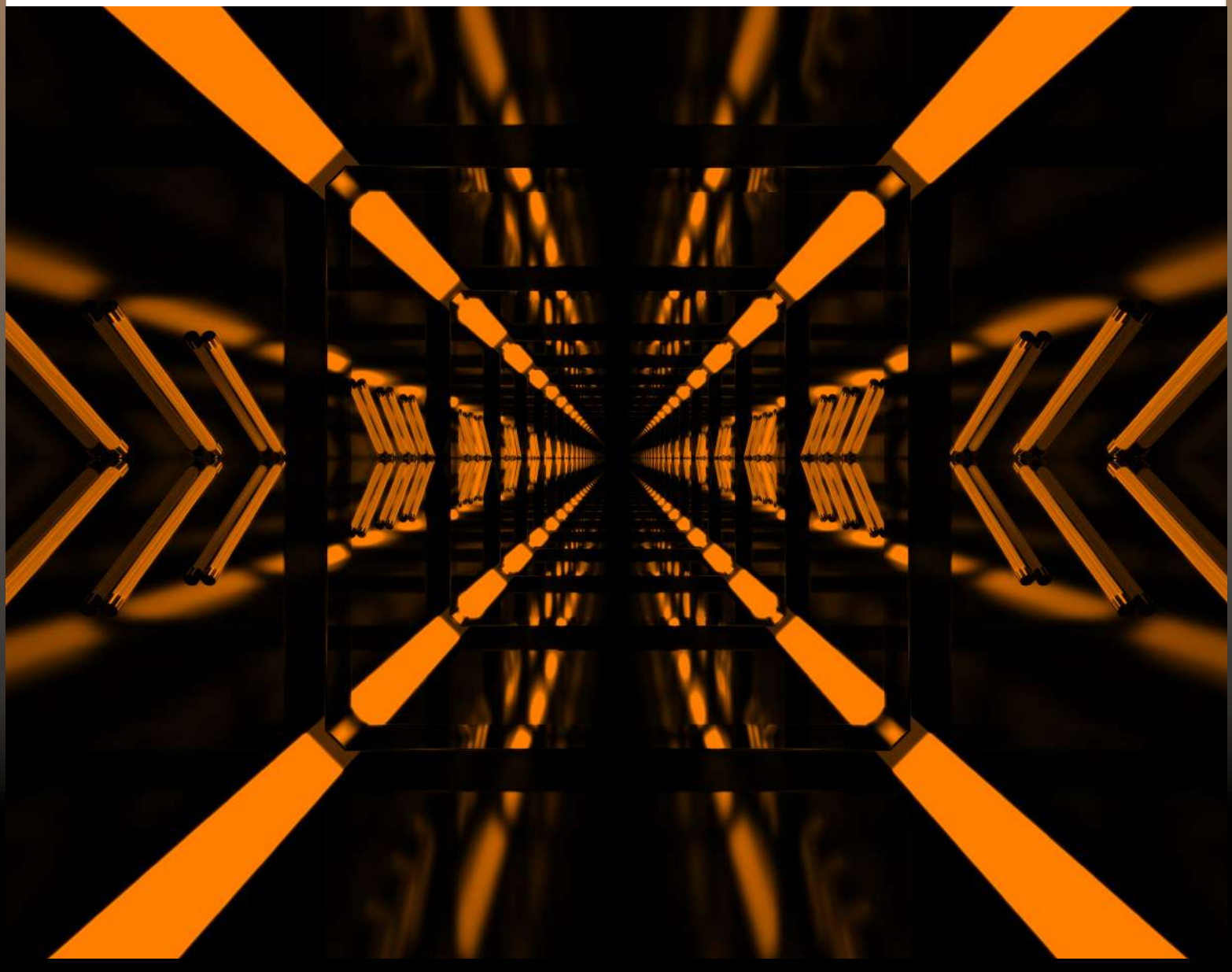
После попадания в сеть жертвы для закрепления Fxmsp использует бэкдоры с таймером, которые инициируют соединение с CnC с большим интервалом - раз в 15 дней, это затрудняет его обнаружение анализаторами трафика.

2 этап

После этого он получает доступ к контроллеру домена и извлекает дампы всех учетных записей. Затем расшифровывает хэши паролей, тем самым получая все критичные доступы в сети.

3 этап

Затем злоумышленник закладывает в backup серверы свои бэкдоры с таймерами. Таким образом, даже если жертва заметит подозрительную активность в системе, то скорее всего, произойдет смена паролей и откат к бэкапу, который уже скомпрометирован.



РАСШИРЕНИЕ АКТИВНОСТИ: ВЫХОД НА НОВЫЕ АНДЕГРАУНДНЫЕ ПЛОЩАДКИ

В начале июня 2017 года наблюдается снижение активности пользователя Fxmsp на форуме fuckav[.]ru. Вместе с тем эксперты Group-IB зафиксировали массовую регистрацию пользователей с таким же никнеймом на других хакерских площадках:

6 июня

аккаунт с именем Fxmsp появился на околохакерском форуме **proxy-base[.]com**

hxxp://proxy-base[.]com/members/fxmsp/

8 июня

аккаунт с именем Fxmsp был зарегистрирован на площадке **lolzteam[.]net**

hxxps://lolzteam[.]net/members/125112/

11 июня

аккаунт с именем Fxmsp был создан на форуме **exploit[.]in**

hxxps://forum.exploit[.]in/index.php?showuser=80141

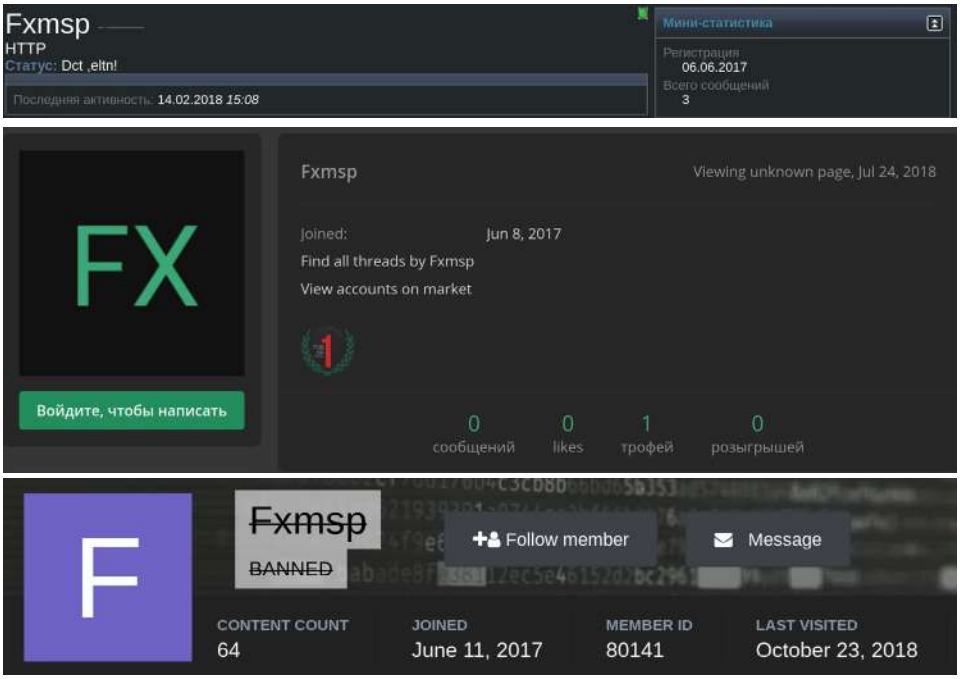


Рис. 13 — Июнь, 2017. Аккаунты пользователя Fxmsp на других андеграундных форумах

На следующий день после регистрации на форуме proxy-base[.]com злоумышленник оставил еще одно сообщение, в котором рассказал, что у него есть доступ к огромной сети из 1,5 млн устройств. В ходе дальнейшего сканирования сети на доступные RDP ему удалось найти 230 000 устройств с открытым портом 3389.

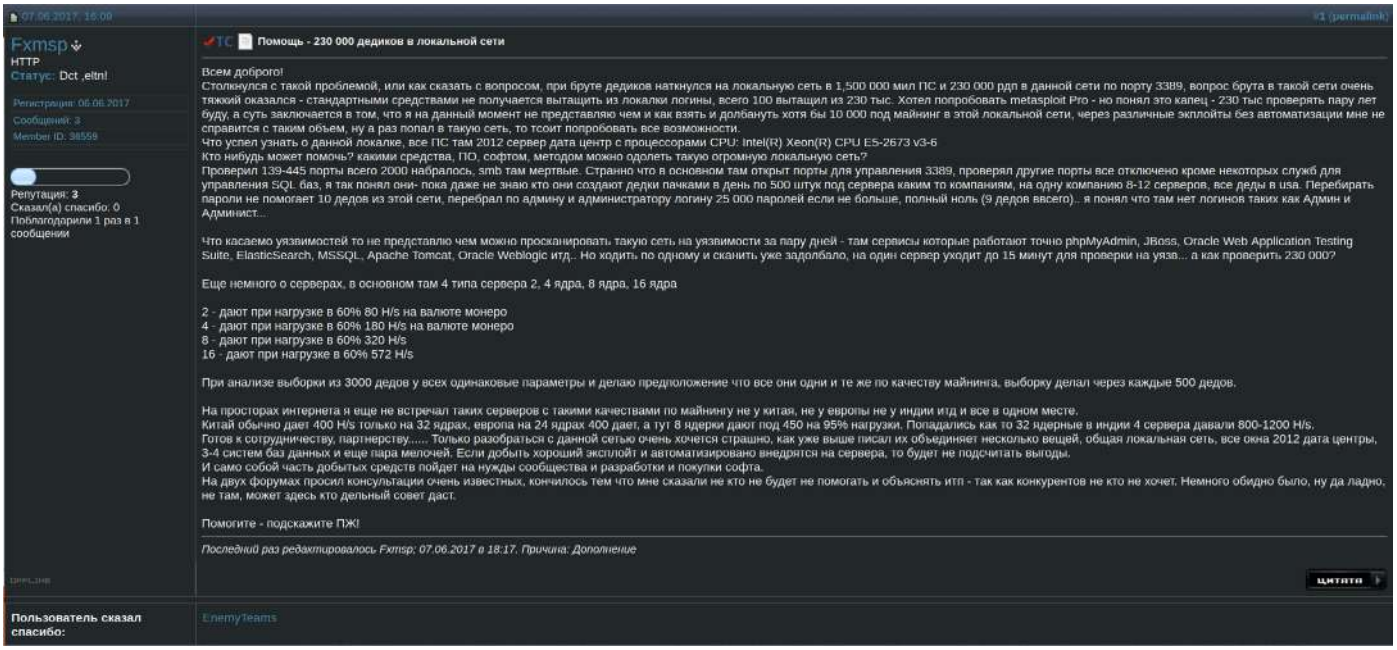


Рис. 14 — Июнь, 2017. Скриншот сообщения о поиске помощи с получением доступа к крупной сети

Стоит обратить внимание на смятение Fxmsp: имея доступ в скомпрометированную компанию, он не собирался продавать его или использовать чувствительную информацию в сети для дальнейшей перепродажи. Его целью был всего лишь майнинг криптовалюты Monero, для чего он планировал использовать серверные мощности жертвы.
Сообщиков долго искать не пришлось. Два пользователя - с никами **zunbah и Kibergyry** - выразили готовность помочь злоумышленнику.

Обратим внимание на еще одно сообщение из того же топика: в ноябре 2017 пользователя Fxmsp спросили о том, получила ли вышеупомянутая история какое-то развитие, и Fxmsp ответил: ему удалось через систему DNS узнать, кому именно принадлежат данные серверы. Затем он начал проверять их на определенные уязвимости, что помогло ему получить доступ к некоторым из серверов, а далее с помощью скомпрометированных паролей и к остальным.

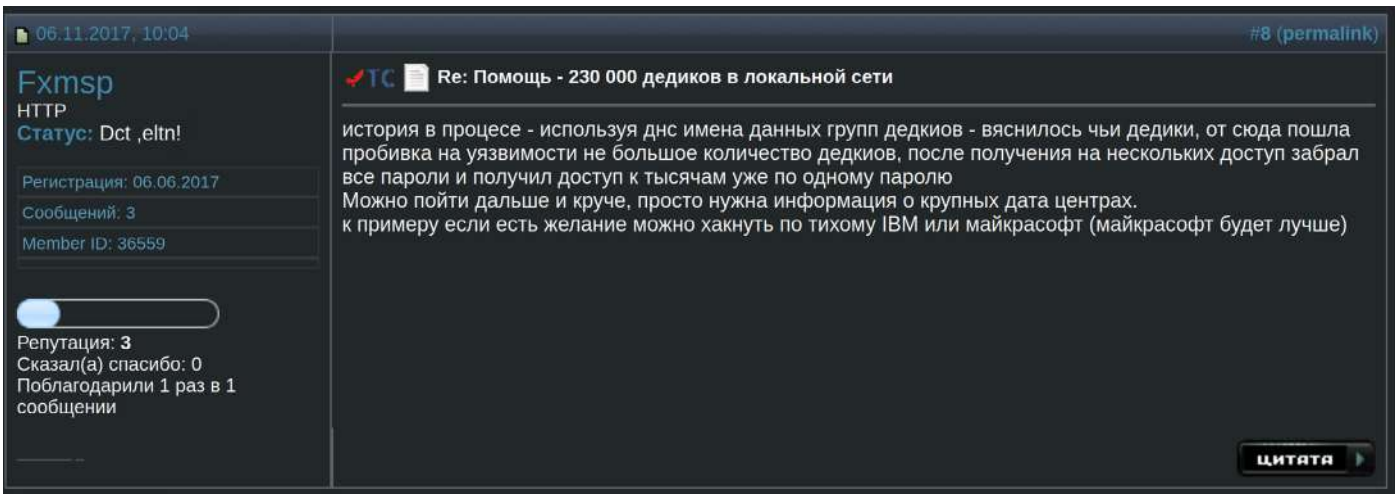


Рис. 15 — Ноябрь. 2017. Скриншот сообщения о возможности взлома сетей IBM и Microsoft

Быстро найдя решение и, видимо, поверив в свой успех, Fxmsp начинает хвастать и говорить о потенциальном взломе IBM или Microsoft.

EXPLOIT[.]IN И ПЕРВЫЕ ОБЪЯВЛЕНИЯ О ПРОДАЖЕ ДОСТУПА К СКОМПРОМЕТИРОВАННЫМ СЕТЯМ

Как говорилось выше, в июне 2017 злоумышленник регистрирует свой основной аккаунт на форуме exploit[.]in, где он в дальнейшем перепрофилирует свою деятельность и начинает продавать доступ к скомпрометированным сетям компаний.

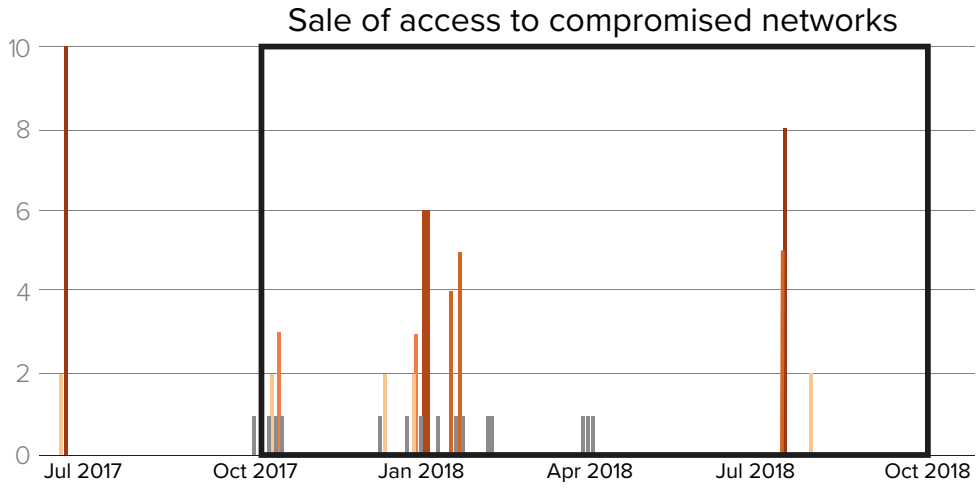


Рис. 16 — Активность злоумышленника на форуме exploit[.]in

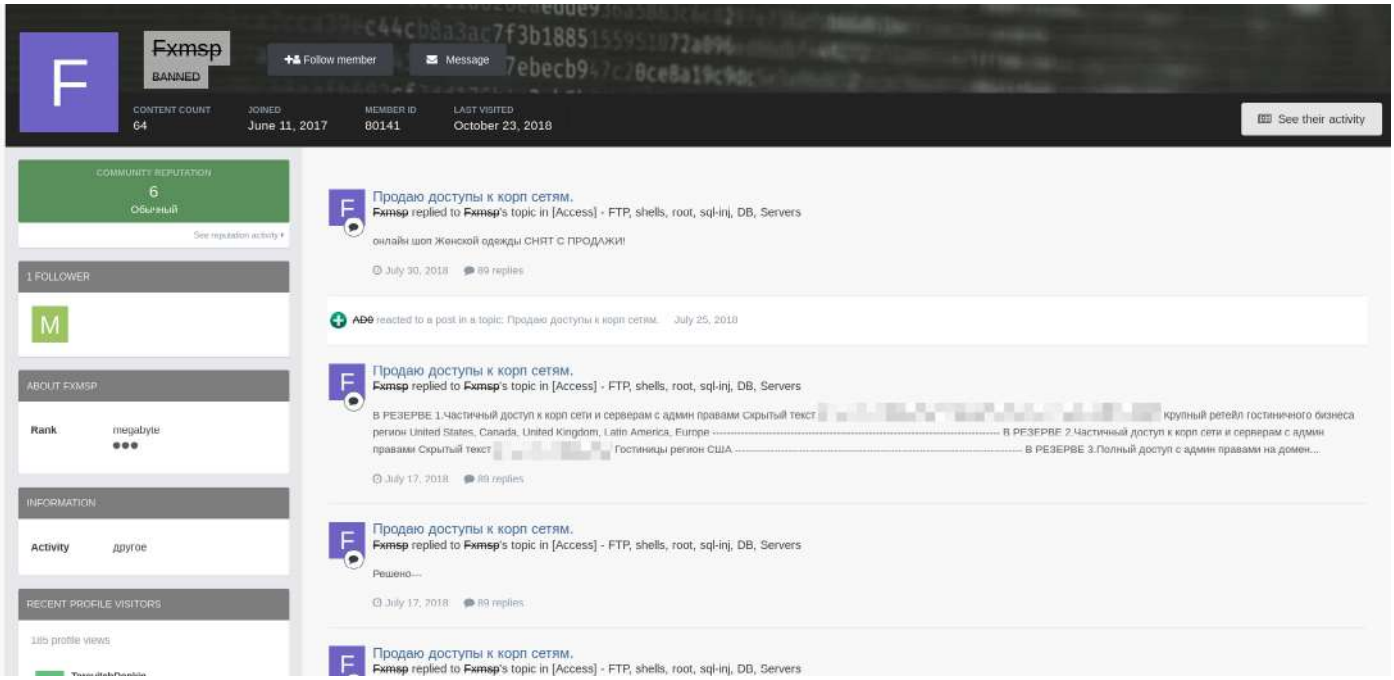
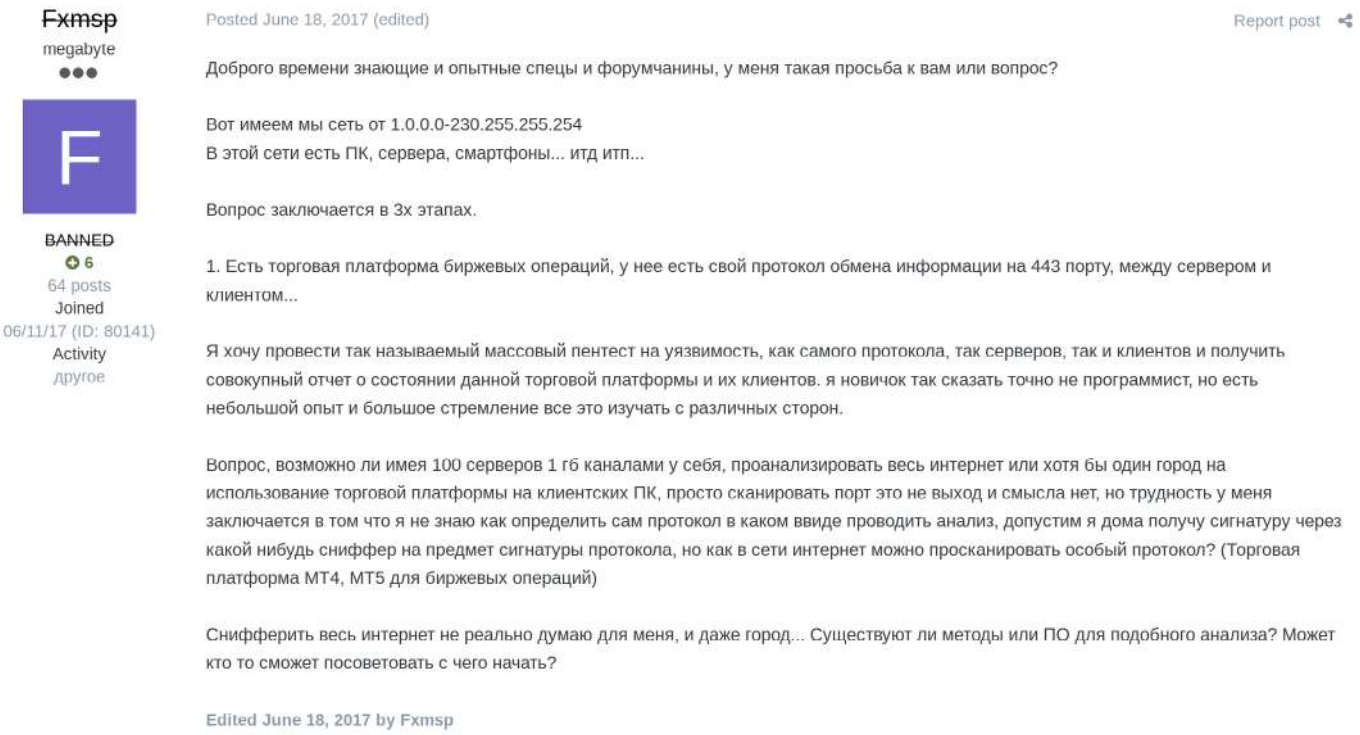


Рис. 17 — Скриншот аккаунта на форуме exploit[.]in. Аккаунт был зарегистрирован 11 июня 2017

Скорее всего, изначально Fxmsp регистрировался на форуме для других целей. Его интересовал лишь один вопрос: можно ли просканировать большую сеть торговой платформы биржевых операций на наличие уязвимостей. Пользователи рекомендовали ему посылать на порты определенные запросы и анализировать ответы сервера, чтобы идентифицировать машины с уязвимостями.



Fxmsp
megabyte
●●●
F
BANNED
6
64 posts
Joined
06/11/17 (ID: 80141)
Activity
другое

Posted June 18, 2017 (edited) Report post

Доброго времени знающие и опытные спецы и форумчанины, у меня такая просьба к вам или вопрос?

Вот имеем мы сеть от 1.0.0.0-230.255.255.254
В этой сети есть ПК, сервера, смартфоны... итд итп...

Вопрос заключается в 3х этапах.

1. Есть торговая платформа биржевых операций, у нее есть свой протокол обмена информации на 443 порту, между сервером и клиентом...

Я хочу провести так называемый массовый пентест на уязвимость, как самого протокола, так серверов, так и клиентов и получить совокупный отчет о состоянии данной торговой платформы и их клиентов. я новичок так сказать точно не программист, но есть небольшой опыт и большое стремление все это изучать с различных сторон.

Вопрос, возможно ли имея 100 серверов 1 гб каналами у себя, проанализировать весь интернет или хотя бы один город на использование торговой платформы на клиентских ПК, просто сканировать порт это не выход и смысла нет, но трудность у меня заключается в том что я не знаю как определить сам протокол в каком ввиде проводить анализ, допустим я дома получу сигнатуру через какой нибудь сниффер на предмет сигнатуры протокола, но как в сети интернет можно просканировать особый протокол? (Торговая платформа MT4, MT5 для биржевых операций)

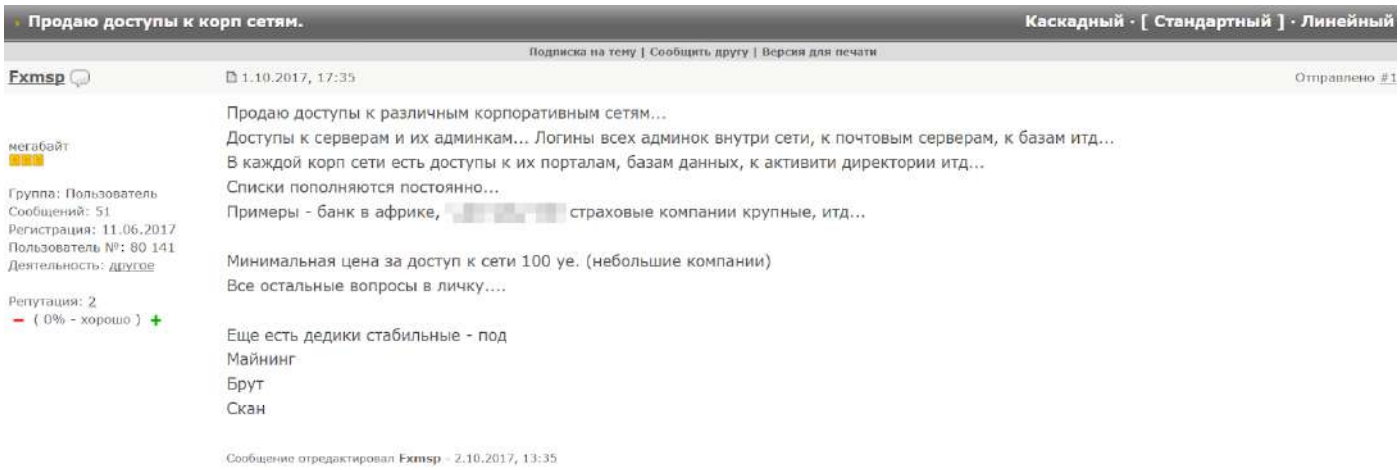
Сниффферить весь интернет не реально думаю для меня, и даже город... Существуют ли методы или ПО для подобного анализа? Может кто то сможет посоветовать с чего начать?

Edited June 18, 2017 by Fxmsp

Рис. 18 — Июнь, 2017. Скриншот сообщения о помощи со сканированием сетей

Последнее сообщение на эту тему датируется 16 июня 2017, после чего злоумышленник приостановил активность на форумах на три месяца.

1 октября 2017 года Fxmsp публикует свое первое сообщение о продаже доступа к корпоративным сетям. Изначально злоумышленник пытался продать доступ в сети компаний без указания их названий. Также пост не содержал контактной информации.



Продаю доступы к корп сетям. Каскадный · [Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

Fxmsp 1.10.2017, 17:35 Отправлено #1

мегабайт
●●●

Группа: Пользователь
Сообщений: 51
Регистрация: 11.06.2017
Пользователь №: 80 141
Деятельность: другое

Репутация: 2
− (0% - хорошо) +

Продаю доступы к различным корпоративным сетям...
Доступы к серверам и их админкам... Логины всех админок внутри сети, к почтовым серверам, к базам итд...
В каждой корп сети есть доступы к их порталам, базам данных, к активити директории итд...
Списки пополняются постоянно...
Примеры - банк в африке, [redacted] страховые компании крупные, итд...

Минимальная цена за доступ к сети 100 уе. (небольшие компании)
Все остальные вопросы в личку....

Еще есть дедики стабильные - под
Майнинг
Брут
Скан

Сообщение отредактировал Fxmsp - 2.10.2017, 13:35

Рис. 19 — Октябрь, 2017. Скриншот объявления о продаже доступов к корпоративным сетям (изначальная версия)

Позже это объявление было отредактировано: в нем появился Jabber-аккаунт злоумышленника fxmsp541@exploit[.]im, но по-прежнему не были указаны названия скомпрометированных компаний.

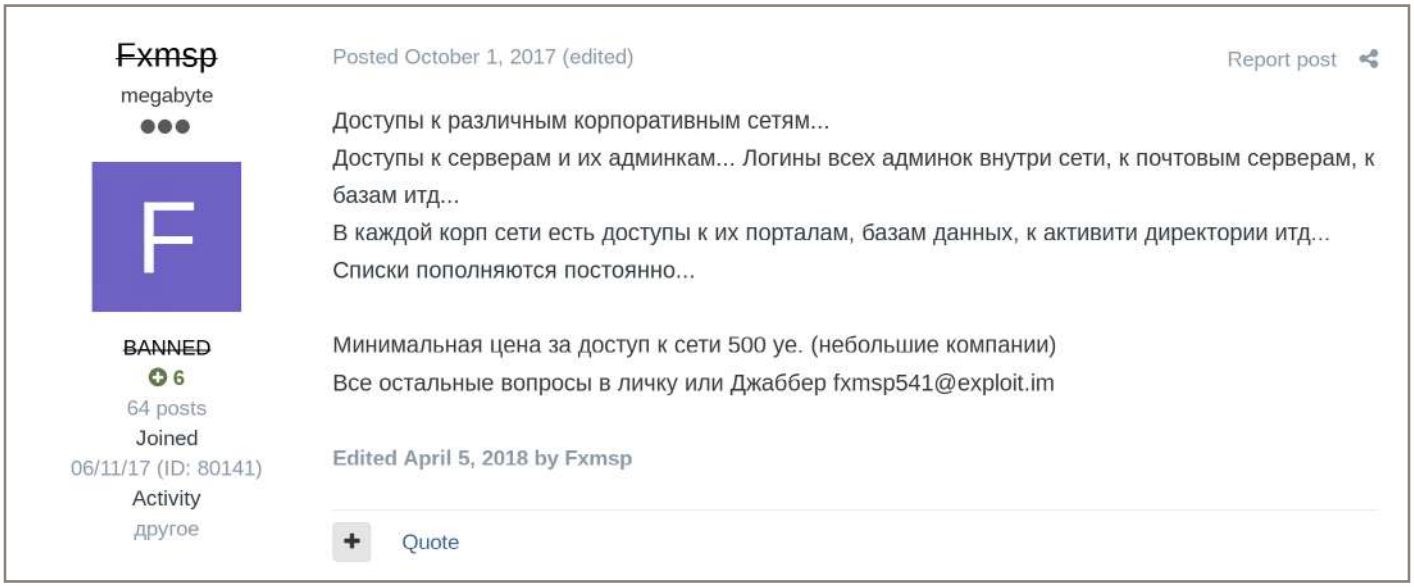


Рис. 20 — Октябрь, 2017. Скриншот объявления о продаже доступа к корпоративным сетям (отредактированная версия)

Уже через неделю после публикации первого объявления Fxmsp понимает, что без указания жертв крайне сложно найти покупателей в андеграунд-коммьюнити. Он решает раскрыть название банка. Его первой жертвой в финансовом секторе, о которой злоумышленник сообщил на форумах, оказался коммерческий банк в Нигерии.

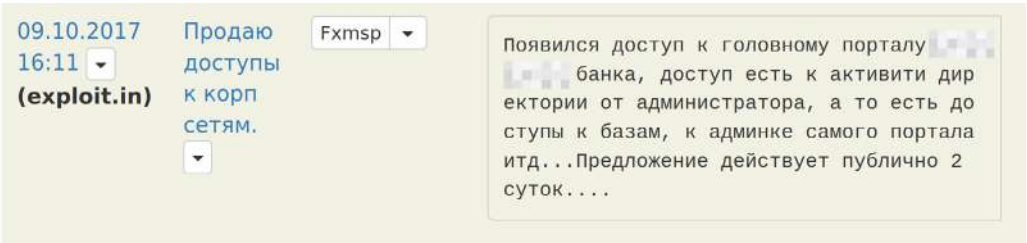


Рис. 21 — Октябрь, 2017. Скриншот объявления о продаже доступа к банку (изначальная версия)

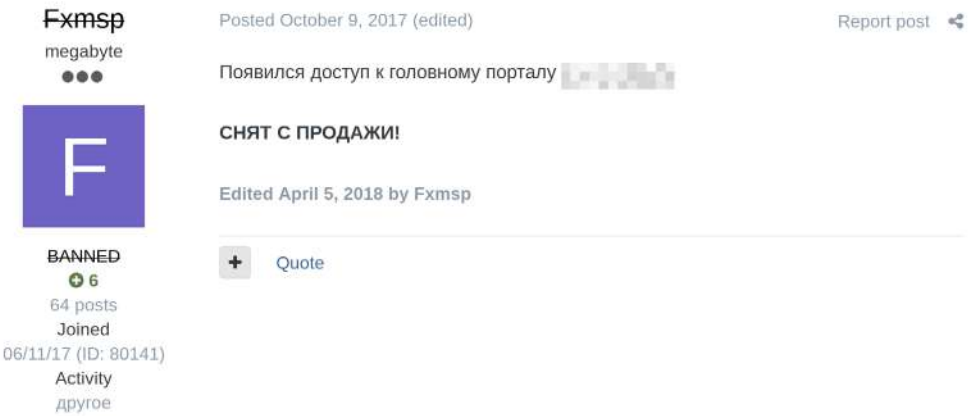


Рис. 22 — Октябрь, 2017. Скриншот объявления о продаже доступа к банку (отредактированная версия)

Также Fxmsp впервые указывает другой свой Jabber-аккаунт uwerty5411@exploit[.]im. Это было сделано 14 октября 2017.

В дальнейшем именно эта публикация помогла установить его реальную личность.

Рис. 23 – Октябрь, 2017. Первое упоминание Jabber-аккаунта Fxmsp на андеграундных форумах

Заметим, что в качестве даты рождения пользователя в Jabber-аккаунте указано **5 декабря**. Также видно, что злоумышленник использует ОС Windows 10.

10 октября 2017 года Fxmsp сообщил, что у него появился доступ к группе отелей премиального класса с локациями в Доминикане, Европе, Кубе, Панаме, США и в других странах. По его словам, этот лот позволяет проводить прямое отслеживание посетителей номеров отеля, дает доступ к серверам службы безопасности, Active Directory, базам данных, а также панели управления кредитными картами. Fxmsp предлагает доступы к 4-10 контроллерам домена, 600 серверам и 1000 рабочих станций. Управление контроллерами домена и Active Directory автор предоставлял с правами администратора. Кроме того, он также предоставил карту отелей по странам:

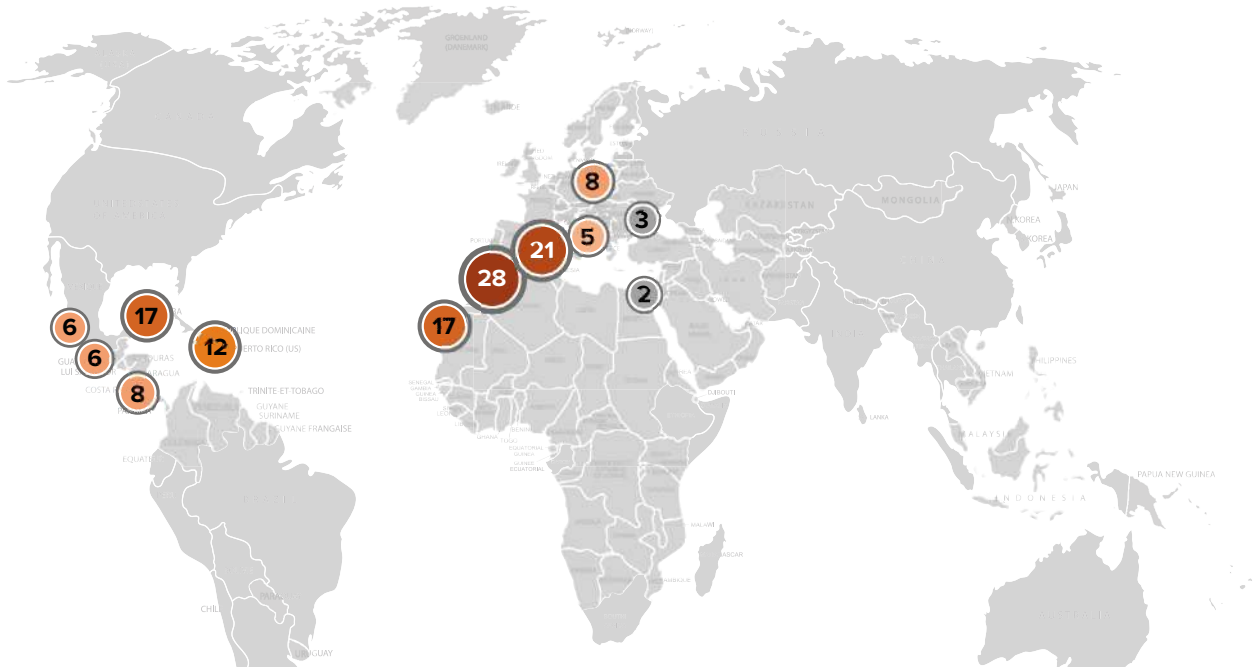


Рис. 24 – Один из самых известных кейсов Fxmsp: продажа доступов к сети группы отелей в США, Европе, Африке и др.

12 декабря 2017 года автор заявил, что у него есть доступ к африканскому банку с капитализацией в $20 миллиардов. По его словам, данный лот предоставляет полную информацию об учетных записях, паролях, базах данных, аккаунтах, банковских картах, депозитных счетах и бухгалтерских документах.

Стоит отметить, что злоумышленник также пытался продавать доступы по России: 30 декабря 2017 года он опубликовал сообщение о продаже доступа через Radmin к банкомату и базе данных таможни в двух разных городах России. Скриншот данного сообщения остался в системе Group-IB Threat Intelligence & Attribution:

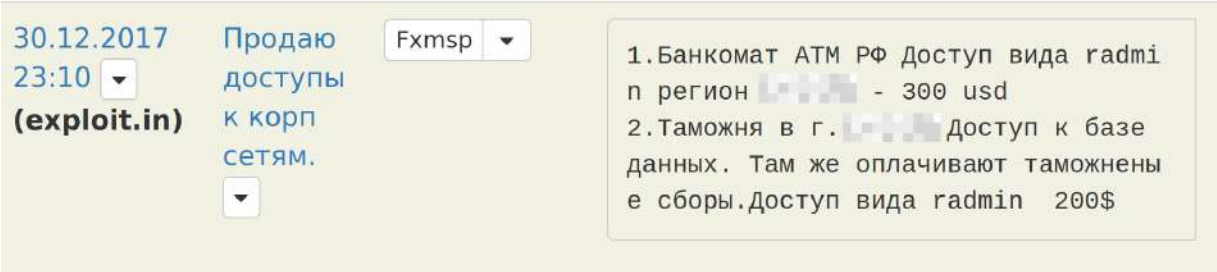


Рис. 25 – Декабрь, 2017. Скриншот из внутренней системы мониторинга даркнет-форумов Group-IB о продаже доступов к банкоматам в РФ

Затем, 2 января, он написал, что доступ к данным базам снят с продажи, что обычно означает, что продавец нашел покупателя. Однако вскоре после этого он изменил сообщение и указал, что не работает по СНГ.

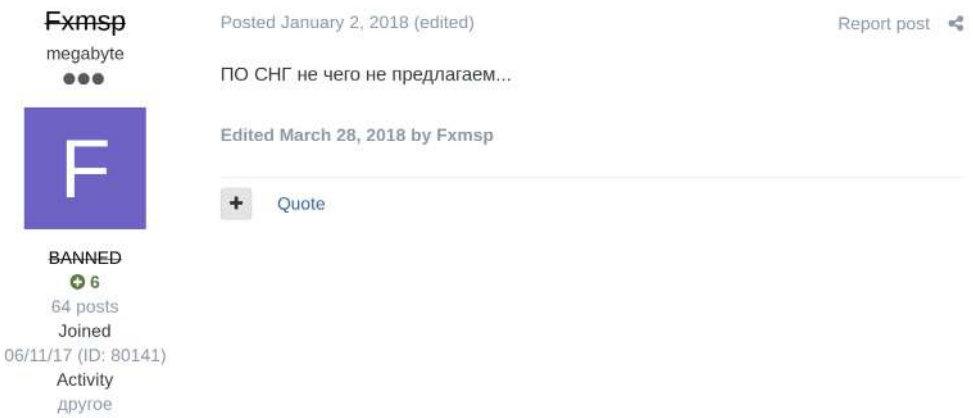


Рис. 26 – Скриншот измененного сообщения, где автор заявляет, что не работает по СНГ

У злоумышленников из России есть негласное правило не работать “по РУ”, то есть по странам СНГ. Это объясняется страхом угодить за решетку. “Работа” вне России снижает риски: уголовное дело будет заведено в стране-жертве, следовательно шансы быть пойманными и экстрадированными у злоумышленников минимальны, особенно если выбирать жертв в странах, где отсутствуют или крайне слабы дипломатические связи.

В результате пользователь Fxmsp был заблокирован на форуме за нарушение правила с работой по РУ-зоне. Урок был выучен: он удалил все предложения, связанные с Россией, после чего блокировка была снята.

3 января 2018 года автор вновь разместил объявление о продаже доступа к сети компании, которая предоставляет услуги по строительству и управлению отелями премиум класса в США. Он снова, по традиции, предоставил карту расположения скомпрометированных отелей:

Рис. 27 – Новый кейс по продаже доступов к сетям отелей. Расположение скомпрометированных объектов.

17 января 2018 злоумышленник назвал точное число своих покупателей на тот момент — по его словам, их было 18 человек. Ему пришлось “раскрыть карты” в ответ на упреки пользователей форума о том, что Fxmsp в действительности не обладал заявленными доступами.

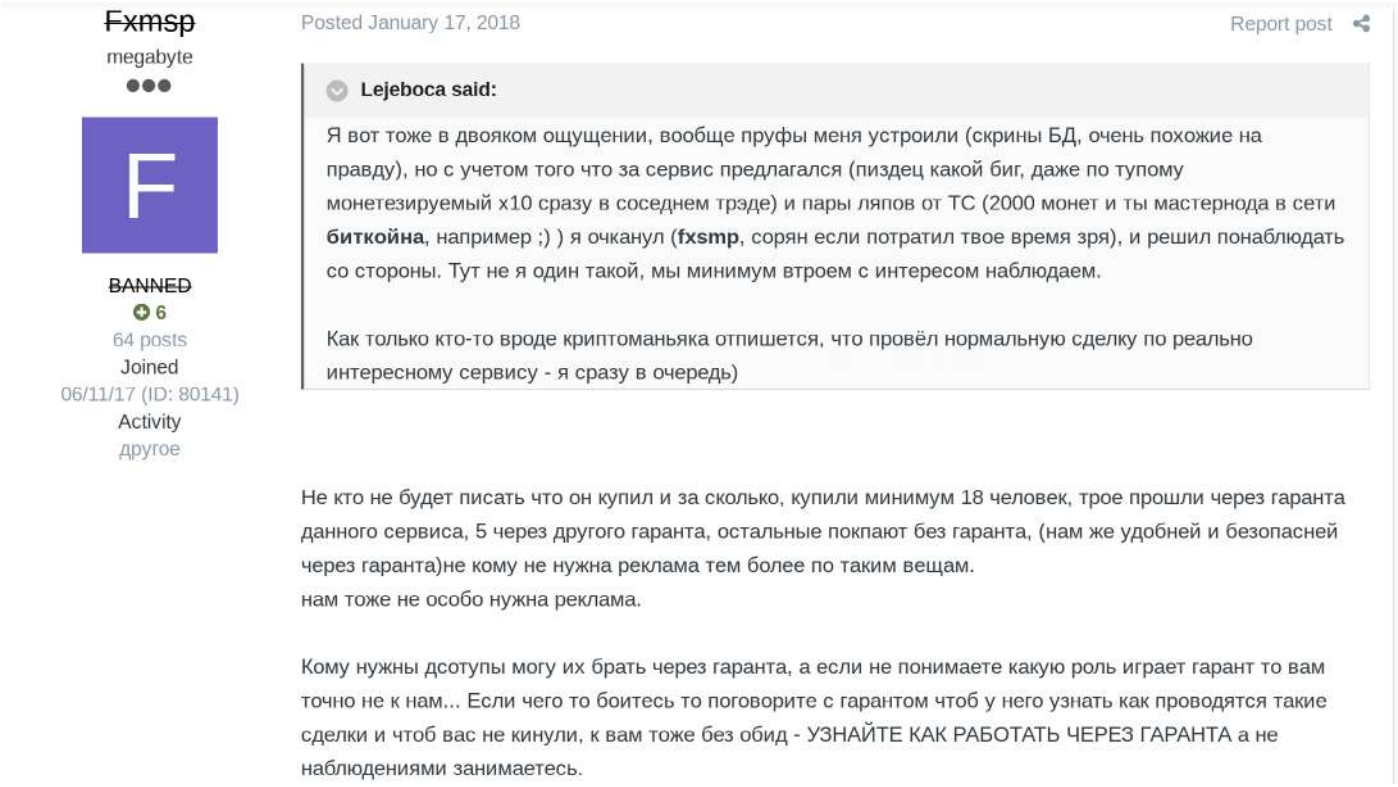


Рис. 28 – Скриншот поста, в котором злоумышленник сообщает о количестве текущих клиентов

6 февраля 2018 года автор объявления начал продавать доступ к сети индийской компании и её подразделениям. По словам автора, компания имеет прямой доступ к своим клиентам и серверам их партнеров, куда входят несколько банков и СМИ. В качестве примера таких партнеров и клиентов он указал 8 различных организаций, как минимум 2 - финансовые.

За время своей активности на форуме exploit[.]in, с начала октября 2017 года по 31 июля 2018 года Fxmsp выставил на продажу доступ к 51-й компании из 21-й страны. Злоумышленник указывал цену только в 30% случаев. К этому моменту за 9 месяцев активности суммарно цена всех опубликованных доступов (без учета возможных продаж в привате) составила **$268 800**.

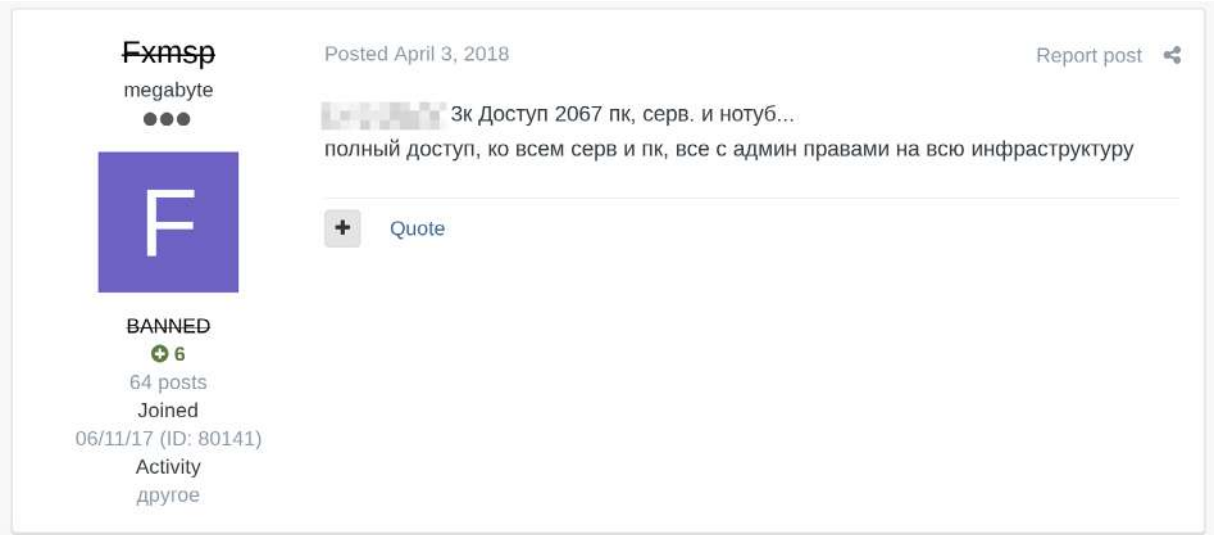
После публикации сообщения о продаже доступа к одной индонезийской компании в апреле 2018 злоумышленник приостановил свою активность на форумах до середины июля, когда он опубликовал свой дополнительный аккаунт Jabber – fxmsp541@exploit[.]im. В этом же месяце он запостил объявление о продаже доступа к сетям еще пяти компаний и прекратил свою активность полностью, передав функции менеджера по продажам уже упоминавшемуся в этом отчете пользователю с ником **Lampeduza**.

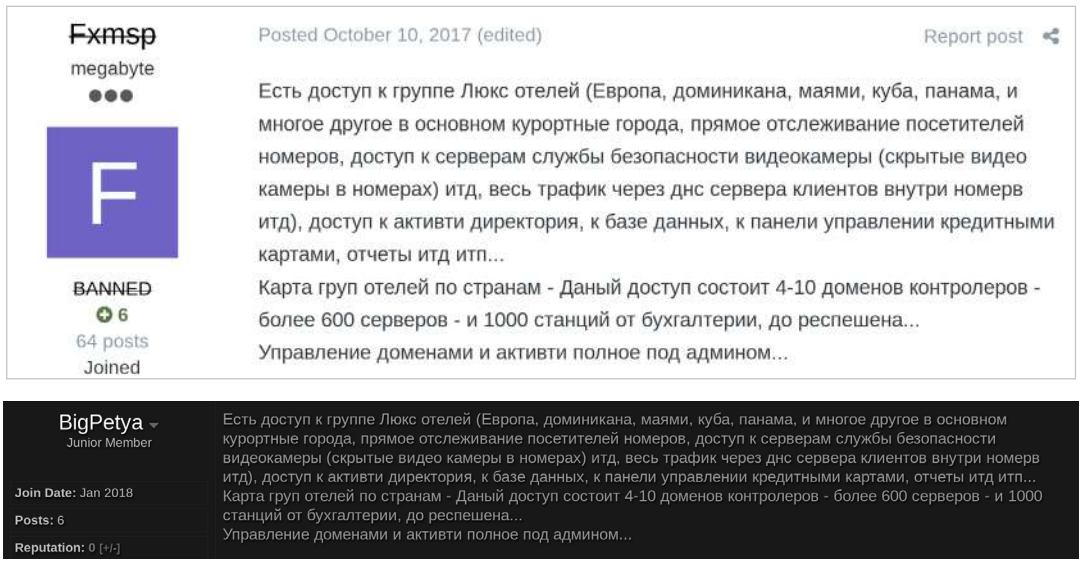
ЭПИЗОД I. СОТРУДНИЧЕСТВО С LAMPEDUZA

Пользователь с ником **Lampeduza** зарегистрировался на форуме exploit[.]in 10 апреля 2018 года (hxxps://exploitinqx4sjro[.]onion/profile/86842-lampeduza/). Lampeduza использует различные псевдонимы на разных андеграундных площадках, что затрудняет его отслеживание.

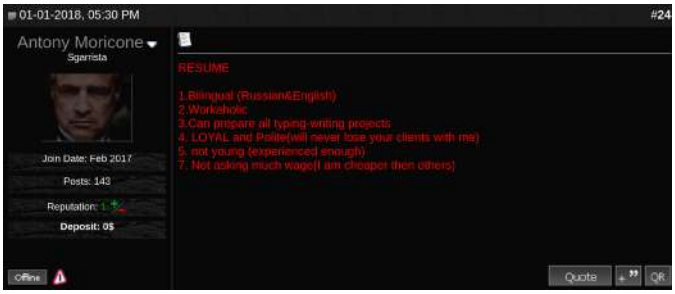
Однако специалистам Group-IB удалось выяснить и другие его ники, среди них: **Antony Moricone**, **BigPetya**, **Fivelife**, **Nikolay**, **tor.ter**, **andropov**, **Gromyko**. До начала сотрудничества с Fxmsp Lampeduza занимался продажей дампов банковских карт (данных, хранящихся на магнитной ленте карты), логинов и паролей от аккаунтов Facebook, а также интересовался взломом аккаунтов Snapchat. В качестве контактных данных он указывал Jabber-аккаунт — zeusl1fe@exploit[.]im

Связь между пользователями Lampeduza и Fxmsp удалось установить, в том числе, благодаря тому, что они оставляли почти полностью одинаковые посты регулярно, в одно и то же время на разных форумах. Ниже примеры одинаковых постов о продаже доступов к одним и тем же компаниям:





Впервые факт сотрудничества между Fxmsp и Lampeduza был зафиксирован в начале 2018 года. Lampeduza публикует сообщение о поиске работы на форуме Omerta 1 января:



В том же месяце на этом и других форумах начинают появляться сообщения от Lampeduza о продаже доступов к тем же компаниям, о которых говорил Fxmsp ранее. Была также зафиксирована продажа доступов к 5 компаниям, которые не были указаны на форуме exploit[.]in.

В конце июня 2018 года Lampeduza вновь опубликовал сообщение, что ищет работу. Это могло быть связано с тем, что ни Fxmsp, ни Lampeduza не выставили на продажу ни одного доступа с апреля по июнь 2018 года.

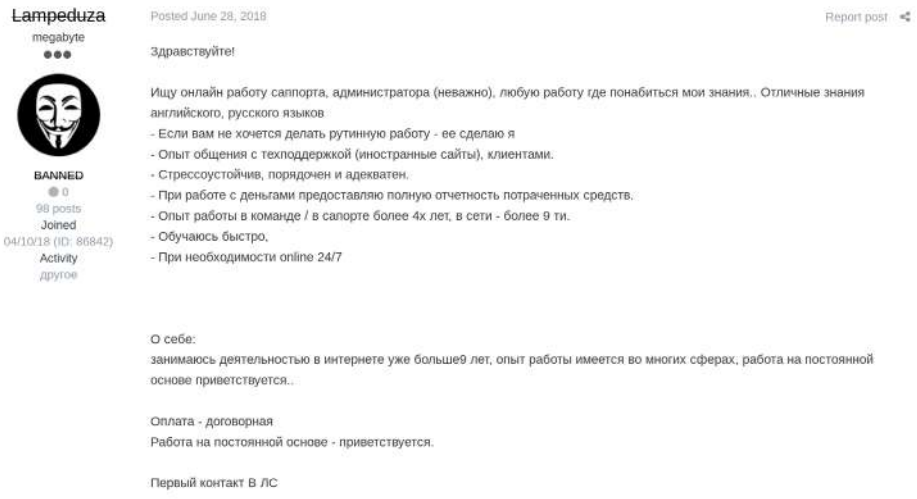


Рис. 29 – Скриншот сообщения пользователя Lampeduza о поиске работы

В июле 2018 Lampeduza и Fxmsp возобновили сотрудничество: 16 июля 2018 года на андеграундном форуме — en.wt1[.]la — появляется сообщение о продаже доступа к корпоративной сети многонационального оператора розничной франшизы. Исходя из анализа брендов, жертвой оказалась компания компания из ОАЭ, о продаже доступа к которой Fxmsp объявил на форуме exploit[.]in в феврале 2018. Сообщение было опубликовано пользователем под псевдонимом **Fivelife**, у которого в контактных данных был указан Jabber-аккаунт — zeusl1fe@exploit[.]im, который Lampeduza публиковал на форуме exploit[.]in

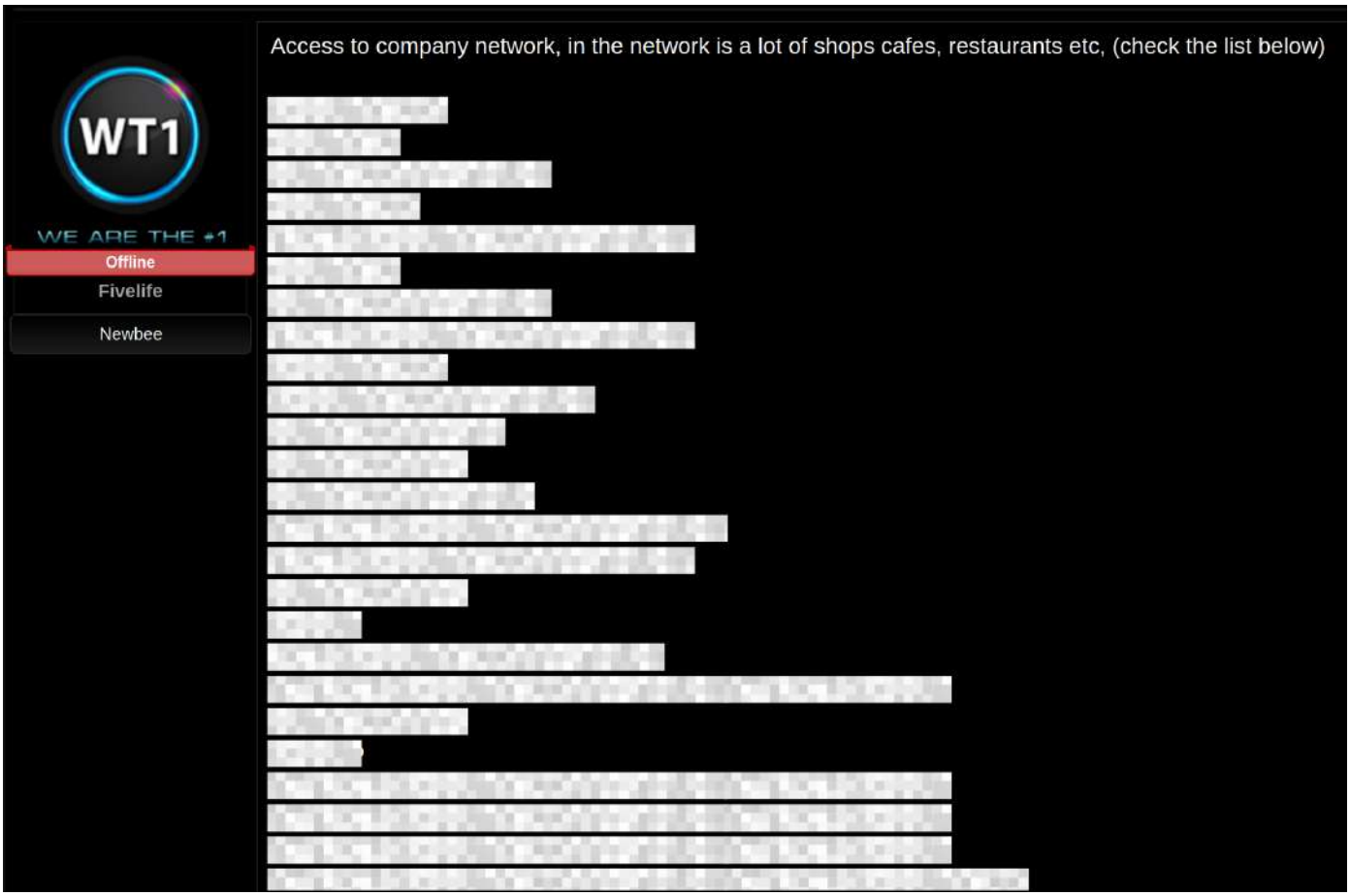


Рис. 30 – Скриншот сообщения со списком доступов на форуме wt1[.]la

Также Lampeduza возобновляет продажи на форуме Omerta под псевдонимом **Antony Moricone**. На сегодня все сообщения, оставленные на форуме пользователем, содержат одинаковый текст — “del”, то есть они удалены. Однако система Group-IB Threat Intelligence & Attribution зафиксировала оригиналы постов.

Рис. 31 – Июль, 2018. Восстановленное с помощью системы Group-IB Threat Intelligence сообщение о продаже доступов на форуме Omerta от пользователя Lampeduza

Такое же сообщение было опубликовано пользователем Fxmsp на форуме exploit[.]in в тот же день:

Рис. 32 – Июль, 2018. Сообщение о продаже доступов на форуме exploit[.]in от пользователя Fxmsp

С конца августа 2018 года Lampeduza прекращает всю предыдущую активность на форумах и фокусируется на продаже доступов к корпоративным сетям.

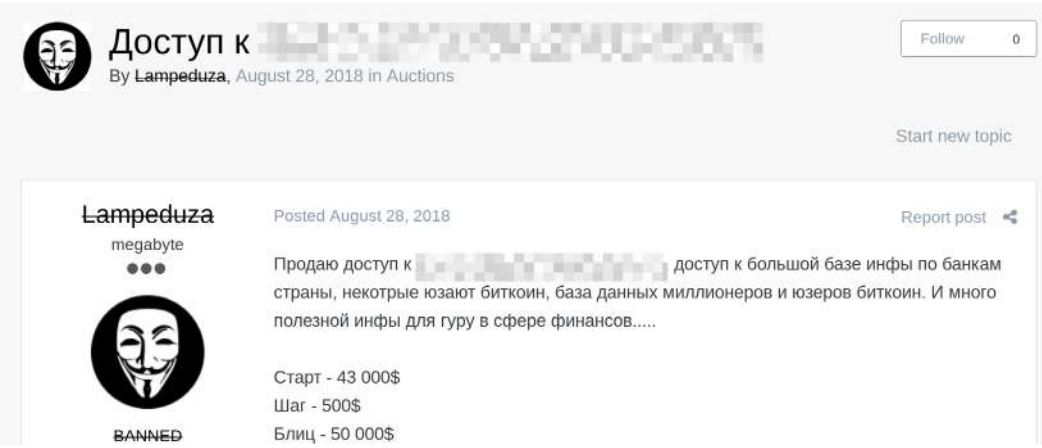


Рис. 33 – Август, 2018. Продажа доступа к госорганизации в Африке

С 20 сентября 2018 Lampeduza начинает дифференцировать целевую аудиторию и скрывать названия скомпрометированных компаний для пользователей, которые разместили менее 50 сообщений:

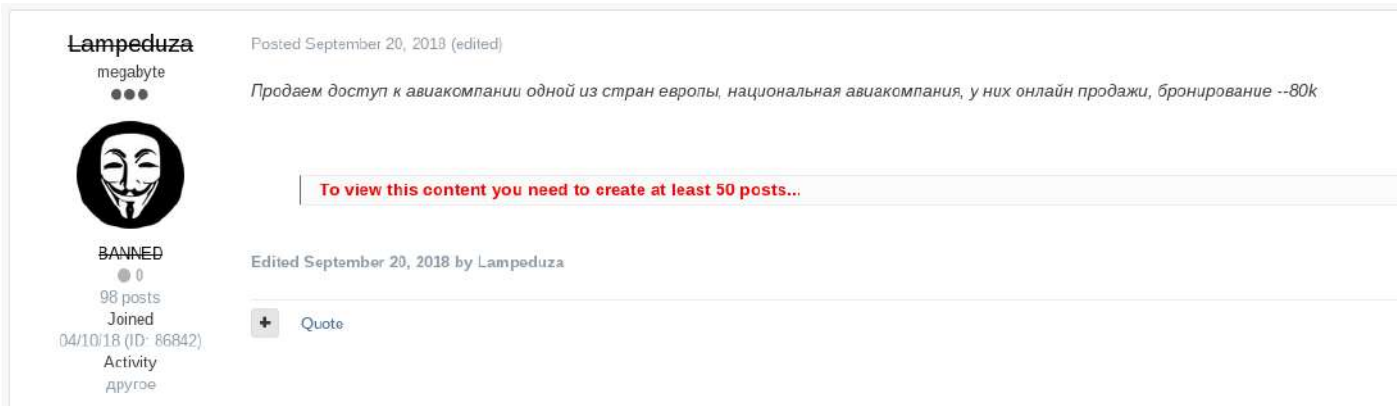


Рис. 34 – Сентябрь, 2018. Ограничение на просмотр контента

Однако специалистам Group-IB Threat Intelligence & Attribution удалось получить информацию о скомпроме-тированных организациях:

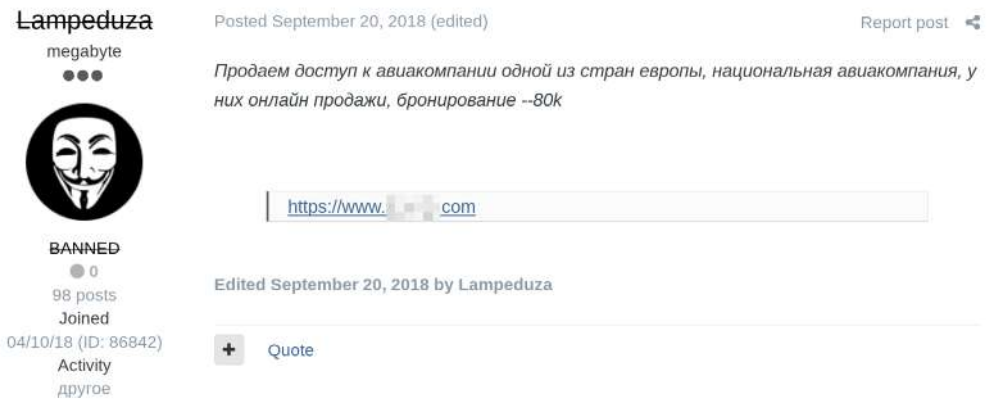


Рис. 35 – Информация, скрытая за хайдом

26 сентября 2018 года Lampeduza опубликовал пост о том, продажу каких услуг он осуществляет, подробно описывая преимущества доступа в скомпрометированные сети. Рекламируя предоставляемые услуги, Lampeduza пишет: **“...У вас будет полный доступ ко всей сети компании. Вы станете НЕВИДИМЫМ БОГОМ СЕТИ”.**

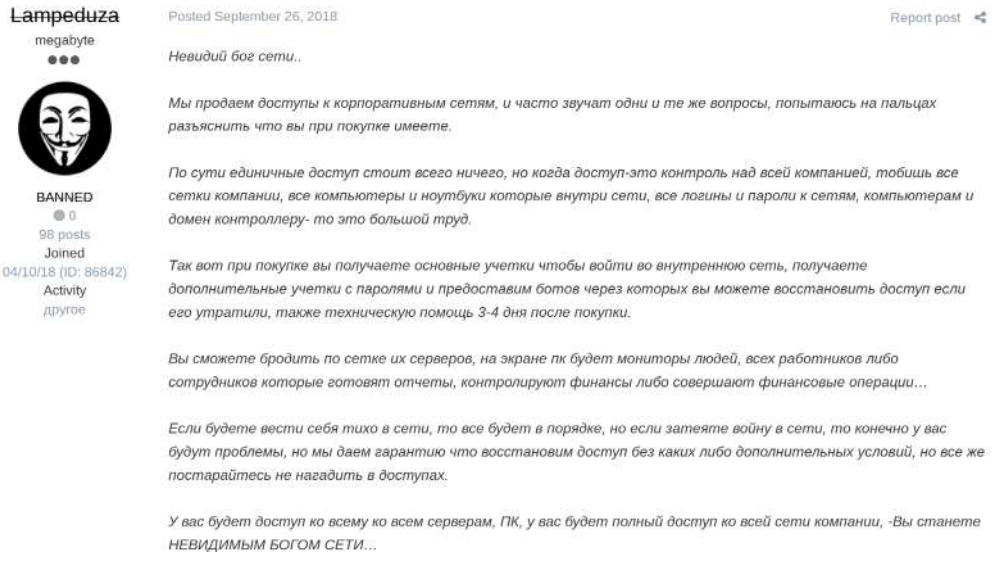


Рис. 36 – Сентябрь, 2018. Скриншот сообщения с подробным описанием того, как сообщники продают доступы

В своем сообщении Lampeduza отмечает, что потерянный доступ может быть восстановлен за счет оставленных в сети бэкдоров – инструментарий, используемый Fxmsp.

Основная активность Lampeduza приходится на конец августа-ноябрь 2018 года, то есть после того, как Fxmsp передал обязанности по продаже данному злоумышленнику, до его блокировки на форуме exploit[.]in. За этот промежуток времени на форуме были опубликованы доступы к 62 новым компаниям. Суммарная стоимость всех продаваемых доступов к этому моменту составила $1 100 800.

В конце октября 2018 года деятельность Fxmsp и Lampeduza оказывается под угрозой. Выясняется, что они пытались продавать доступ к одной и той же сети разным людям. Такое запрещено на форуме без согласия покупателя. В итоге пользователь с ником **g0rx** создал специальный топик на форуме, в котором он описал сложившуюся ситуацию. Подобные топики представляют собой разрешение споров между пользователями андеграунд-сообщества, когда покупатель и продавец вступают в конфликтную ситуацию, а для разрешения необходима помощь третьей стороны, в качестве которой обычно выступает администрация форума.

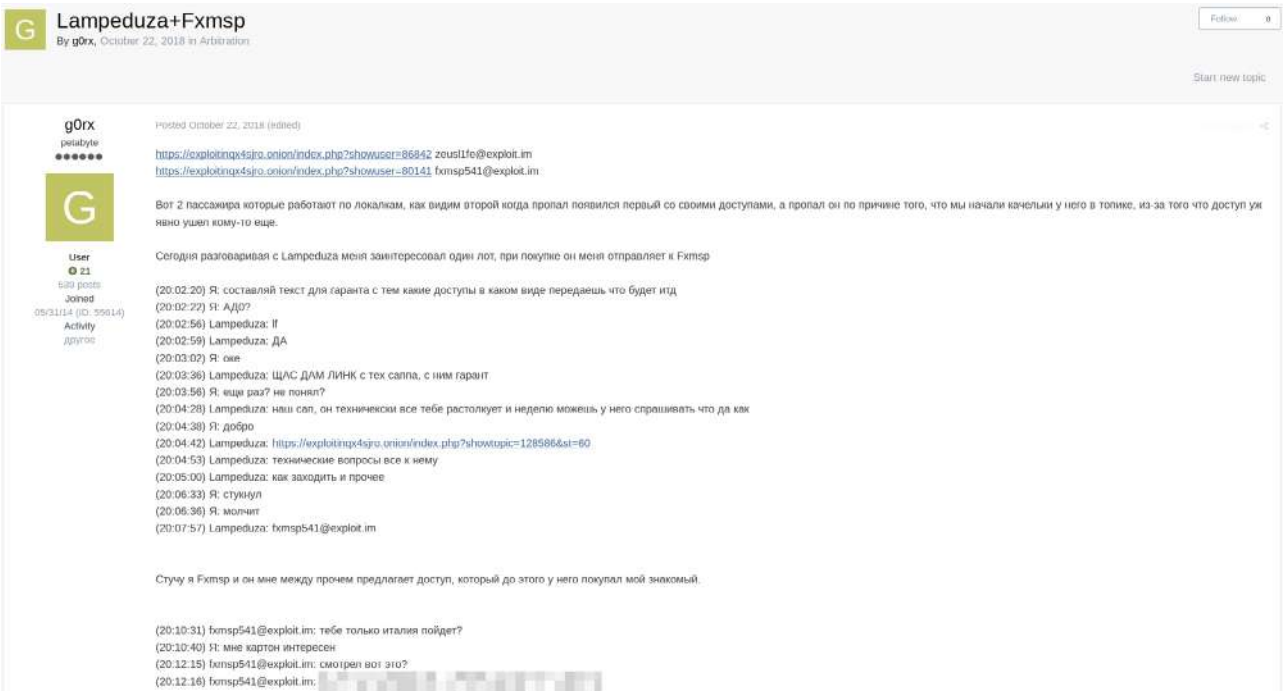


Рис. 37 – Скриншот блэка на данную преступную группу

Пользователь g0rx заявил, что его знакомый с псевдонимом **mimikatz** купил доступ к компании из ОАЭ у Fxmsp, однако потом в сети были обнаружены криптомайнеры. Как мы упоминали выше в главе “Первые шаги в андеграунде”, в начале своей деятельности Fxmsp действительно устанавливал майнеры в скомпрометированных инфраструктурах. Более того, Fxmsp предложил g0rx также купить доступ к данной компании.

Lampeduza в свою защиту заявил, что прекращает сотрудничество с Fxmsp и приостанавливает продажу доступа к скомпрометированным сетям. В итоге 24 октября оба пользователя получают бан 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. Сообщники возобновляют работу на форумах в середине марта 2019. Сразу на нескольких андеграундных площадках появились новые сообщения о продаже доступа.

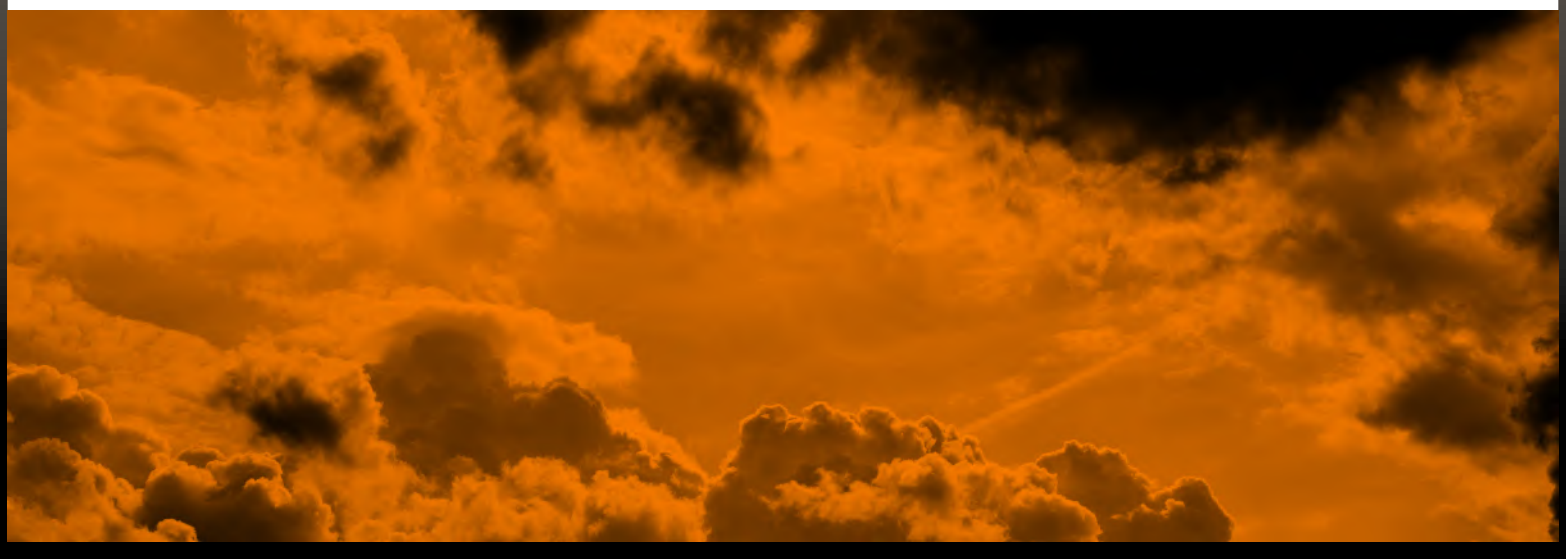
Пример одного из таких объявлений представлен на рисунке ниже:

Рис. 38 – Скриншот нового объявления о продаже доступов

Стоит также отметить объявление от 21 марта 2019 года, где автор утверждает, что теперь он продает доступ к корпоративным сетям именно для загрузки в компании майнеров криптовалюты:

Рис. 39 – Скриншот нового объявления о продаже доступа

А теперь вернемся к началу отчета: публичная кульминация деятельности Fxmsp пришлась на апрель 2019. По данным некой компании AdvIntel, они получили от Fxmsp информацию о том, что ему удалось скомпрометировать сети трех крупных антивирусных вендоров. По словам злоумышленника, он смог также выгрузить из сети исходные коды антивирусных агентов, модули аналитики и плагины безопасности для браузеров. Цена исходного кода и доступа в сеть составляла $300 000. По словам компании, злоумышленнику удалось получить доступ к компаниям Symantec, Trend Micro и McAfee. Однако все компании, кроме Trend Micro (выпустила официальное заявление по данной теме https://www[.]cbronline[.]com/news/trend-micro-symantec-fxmsp), не подтвердили факт доступа.



ЭПИЗОД II. СКРЫТАЯ УГРОЗА

С мая 2019 Lampeduza заявляет, что больше не работает с Fxmsp. В одной из переписок он также указывает, что никак не связан с утечкой исходных кодов антивирусных компаний. Повышенное внимание СМИ к Fxmsp, как писал сообщник, якобы стало причиной остановки их сотрудничества. Отметим, что к тому времени Lampeduza предоставлял информацию о скомпрометированных компаниях только постоянным клиентам. Вскоре он ненадолго пропал с форумов, однако, вероятнее всего, продолжил свою работу в привате и по-прежнему продавал “товар” Fxmsp.

Новый “публичный” лот появился спустя несколько месяцев, 19 сентября 2019 года: Lampeduza сообщил, что готов продать доступ к очередной корпоративной сети одной немецкой компании:

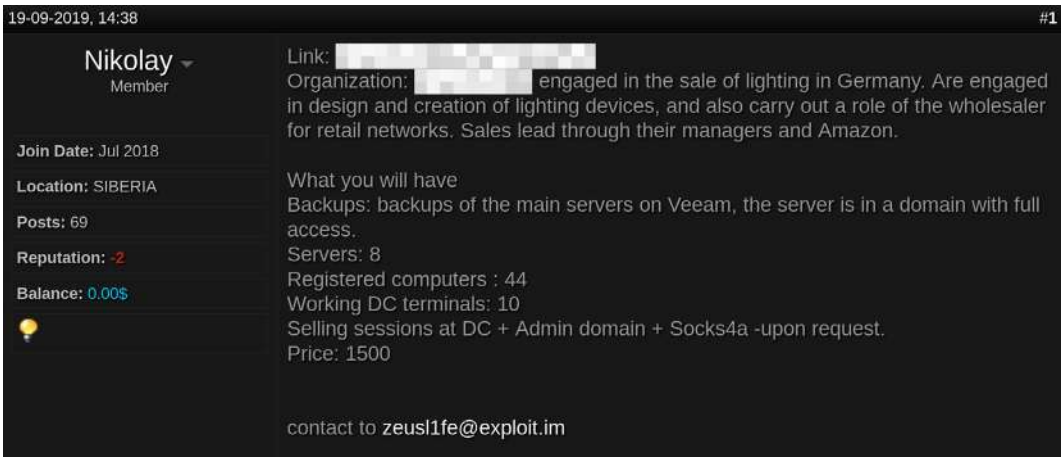


Рис. 40 – Сентябрь, 2019. Скриншот нового объявления о продаже доступа

Оценка заработка Fxmsp в этот период затруднительна, поскольку за все время активности в 2019 году на продажу “в паблик” было выставлено только 22 доступа к корпоративным сетям различных компаний. Суммарная стоимость предлагаемых услуг на тот момент составила $124 100.

Таким образом, несмотря на бан на форуме exploit[.]in, в период с мая по сентябрь 2019 года преступная группа продолжала свою работу, а Lampeduza, несмотря на все заявления, по-прежнему продавал доступ к скомпрометированным Fxmsp корпоративным сетям.

НА ФИНИШНОЙ ПРЯМОЙ: ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ Fxmsp

Прекращение сотрудничества между Lampeduza и Fxmsp приходится на декабрь 2019 года. Используя свой псевдоним Antony Moricone, 3 декабря 2019 года Lampeduza публикует на том же форуме Omerta объявление о поиске работы менеджера по андеграунд продажам, как когда-то публиковал перед началом работы с Fxmsp:

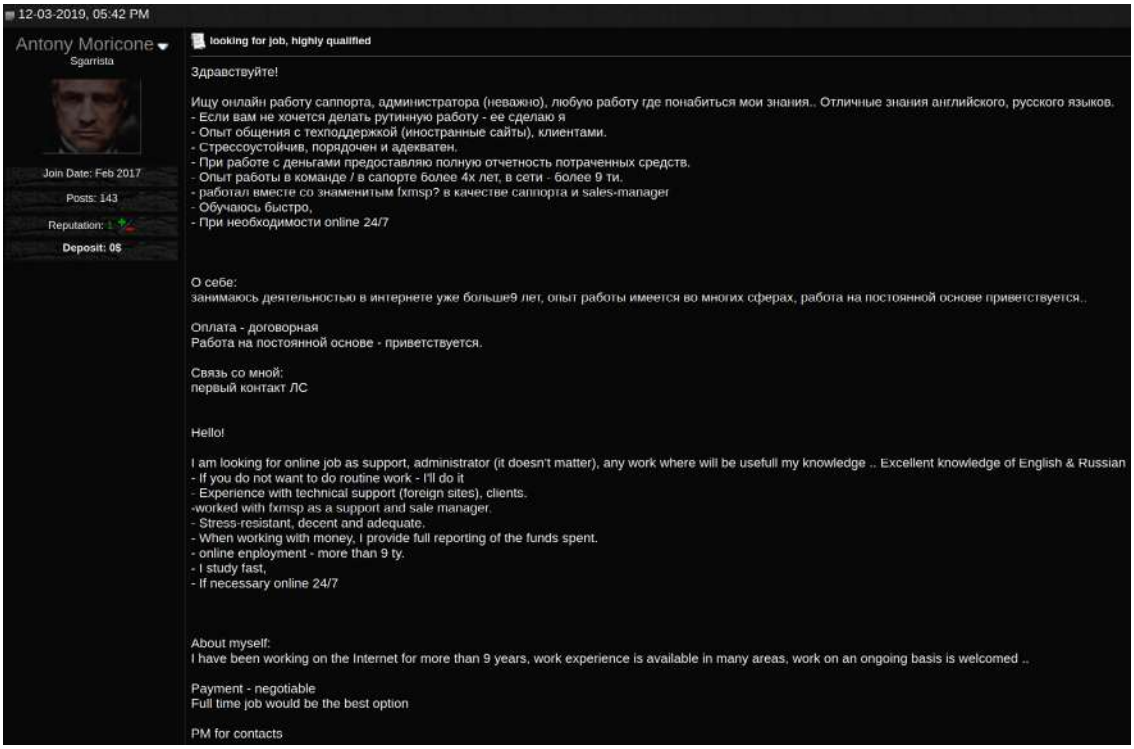


Рис. 41 – Март, 2019. Скриншот о поиске работы Lampeduza

Lampeduza подтвердил пользователям форума, что Fxmsp закончил свою работу 17 декабря 2019.

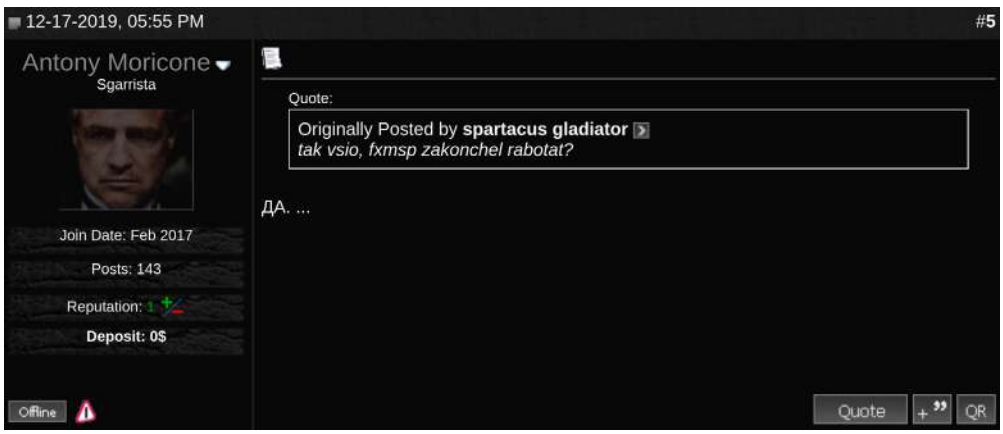


Рис. 42 – Декабрь, 2019. Lampeduza заявил, что Fxmsp закончил свою работу

ПРЕДПОЛОЖИТЕЛЬНАЯ ЛИЧНОСТЬ Fxmsp: ЭТАПЫ ДЕАНОНА

Изначально Fxmsp использовал для связи Jabber-аккаунт **uwerty5411@exploit[.]im**. Стоит отметить, что это совсем не похоже на его стандартный ник, мы обратили внимание на это расхождение и запомнили данный псевдоним на будущее. Обычно преступник использовал уникальный никнейм Fxmsp – он и стал отправной точкой для установления реальной личности продавца доступов.

Исходя из того, что псевдоним является достаточно редким, была найдена почта на сервисе m***[.]ru - **Fxmsp@m***[.]ru**. Злоумышленник нигде не указывал данную почту, это могло быть совпадением, однако мы решили проверить, использовался ли данный адрес для регистрации каких-либо аккаунтов на андеграунд-форумах. И нашли пересечения с аккаунтами злоумышленника. Было выявлено, что эта почта использовалась для регистрации на форумах exploit[.]in, fuckav[.]ru, proxy-base[.]com и lolzteam[.]net

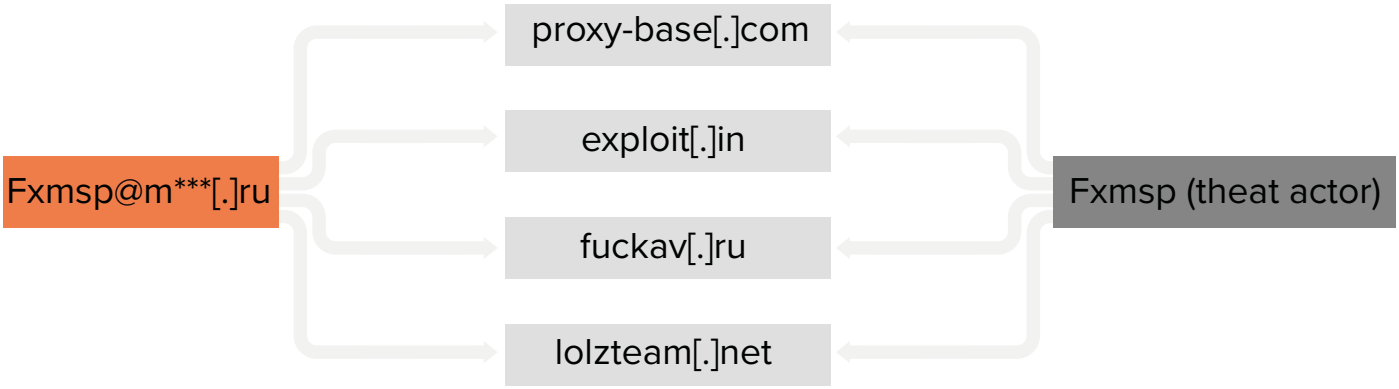


*Рис. 43 – Соотнесение аккаунта на m***.ru с регистрацией Fxmsp на форумах*

Для почты Fxmsp@m***[.]ru в качестве резервной была указана почта **fxmsp@b***[.]ru**. Последняя также привязана к первой; при привязке было указано, что никнейм у почты на m***[.]ru начинается именно с заглавной буквы. Эта мелочь является достаточно важным фактором, так как на всех форумах злоумышленник указывает свой никнейм именно с заглавной буквы.

Таким образом, было найдено еще одно косвенное подтверждением того, что оригинальная почта связана именно с тем псевдонимом, который использовался на андеграунд-форумах.
К почте Fxmsp@m***[.]ru также привязаны два аккаунта в сети Skype:

- **msgp*** (Mich*** Ko***)**
- **wcypr*** (An*** Ayt***)**

Помимо этого, email Fxmsp@m***[.]ru был использован для регистрации домена gov360[.]info

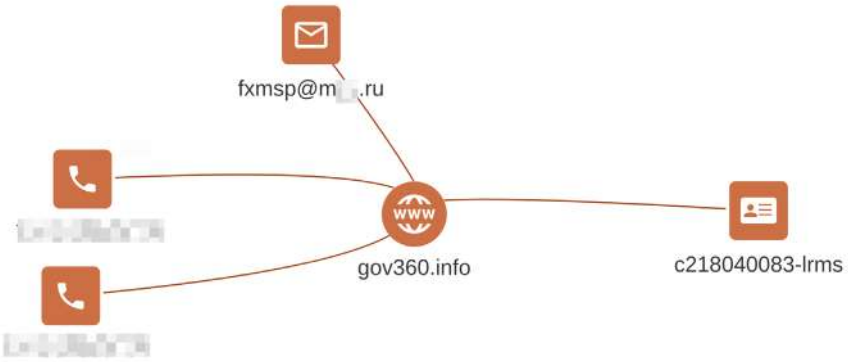


*Рис. 44 – Скриншот из систем Group-IB, показывающий связь между различными аккаунтами и доменным именем, зарегистрированным с использованием учетки Fxmsp@m***[.]ru*

В поле «Org» в WHOIS данных был указан некий “**andej a turchin**”.

Org	andej a turchin hosting telesystems jsc
Address	
City	almata moscow
Zipcode	050000 115093

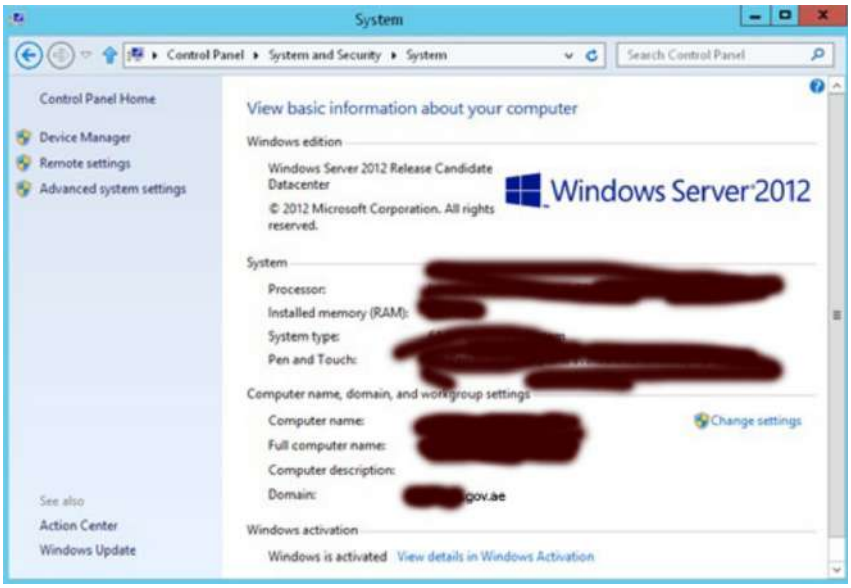
Стоит отметить, что в WHOIS данных почта также указана с заглавной буквы:

```
Registrant Fax Ext:
Registrant Email: Fxmsp@m .ru
```

Здесь же был указан номер телефона **+77783168*****. Согласно DEF-коду оператора, номер телефона принадлежит компании Kcell/Activ, Казахстан.

Отталкиваясь от Jabber-аккаунта злоумышленника, мы нашли очень похожий по стилистике аккаунт (с него велась аналогичная активность), который был зарегистрирован на форуме proxy-base[.]com (hxxp://proxy-base[.]com/members/uwert/). Мы упоминали его ранее, теперь поясним, почему мы считаем, что он также принадлежит злоумышленнику.

Во-первых, владелец этого аккаунта использует никнейм частично похожий на Jabber-аккаунт злоумышленника. Этого фактора мало: “uwerty” - это всего лишь распространенная комбинация как qwerty, но с одной заменой. Во-вторых, активность пользователя на данном форуме. И этот фактор значительно сильнее. Он интересовался брутом RDP серверов и просил помощи у пользователя под ником **Montano** (hxxp://proxy-base[.]com/members/montano/). Затем выяснилось, что тот не смог выполнить просьбу и “нарисовал” скрины об успешном взломе, куда вставил нужный домен, который запрашивал злоумышленник. Тут начинается самое интересное: переписка была опубликована с 14 по 16 февраля 2018 года. Здесь же был приложен “нарисованный” скриншот:



На снимке отчетливо виден домен первого уровня **gov[.]ae**. Напомним, что за месяц до описываемых событий, злоумышленник Fxmsp продавал доступ к скомпрометированным сетям в ОАЭ.

В ходе дальнейшего исследования, используя основной Jabber-аккаунт Fxmsp и выявленный второй аккаунт на форуме proxy-base[.]com, мы проверили почту uwert@m***[.]ru, оказалось, что она использовалась для регистрации 4 доменов:

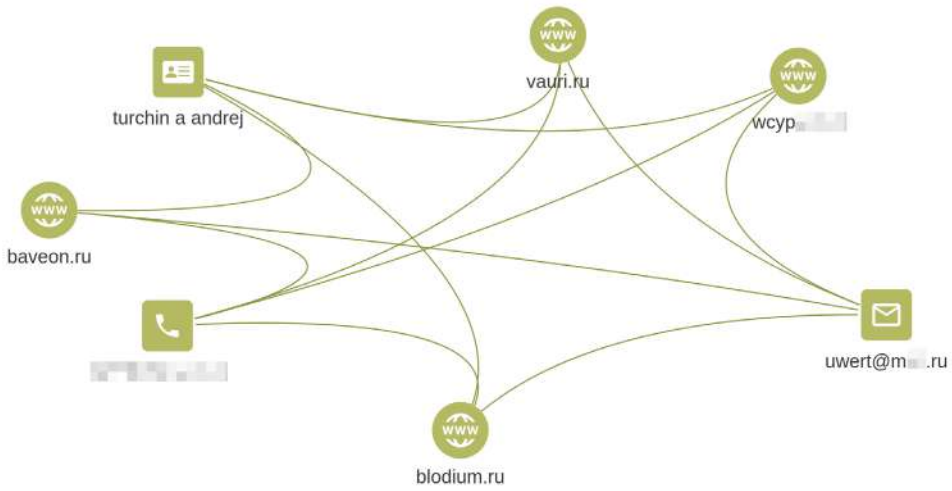


*Рис. 45 – Проверка связей между различными аккаунтами, установка доменов, зарегистрированных с использованием uwert@m***[.]ru*

Как видно, название домена **wcypr***.ru** пересекается с ником пользователя **wcypr*** (An*** Ayt***)** в Skype, который был зарегистрирован на адрес Fxmsp@m***[.]ru

В качестве имени указан тот же “**turchin a andrej**”.

Status	registered, delegated, verified
Email	uwert@m[redacted].ru
Name	turchin a andrej

В своем Jabber-аккаунте uwerty5411@exploit[.]im он указал в качестве даты рождения **5 декабря**, а в качестве имени – набор символов **gdfsgfd**.

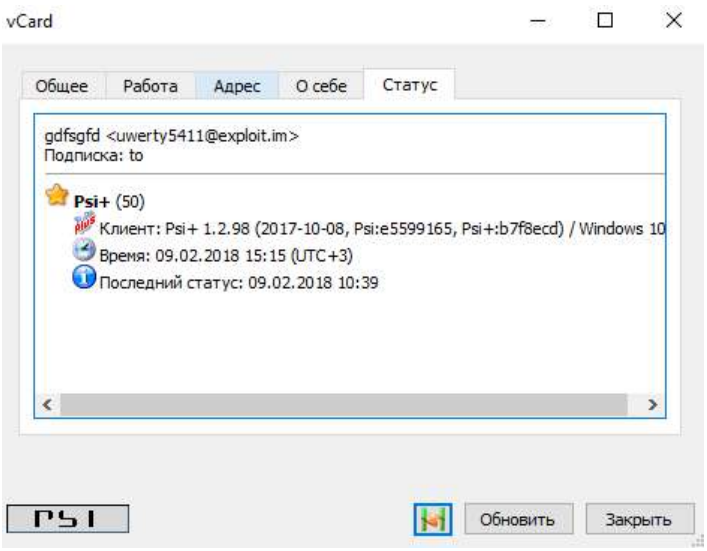
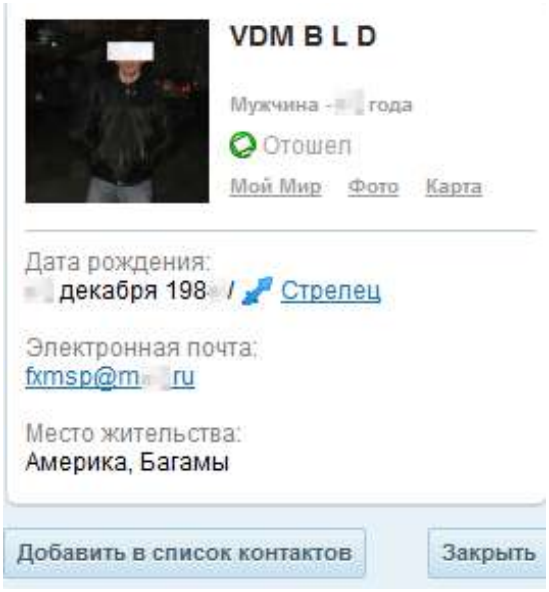
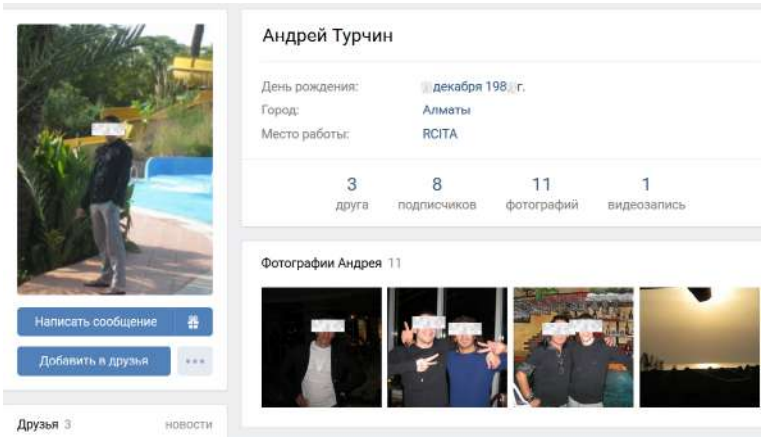


Рис. 46 – Скриншот информации из Jabber аккаунта – uwerty5411@exploit[.]im

В ходе изучения email адреса Fxmsp@m***[.]ru было выявлено, что к нему привязан аккаунт в социальной сети “Мой Мир”:



В социальной сети ВКонтакте был обнаружен аккаунт с именем “Андрей Турчин” (hxxps://vk[.]com/id***). Фотография из данного аккаунта совпадает с фотографией представленной в сети “Мой Мир”.



Мы выяснили, что данный аккаунт привязан к email-адресу **uwert@m***[.]com.**

Далее нами было обнаружено, что в 2008 году почта **uwert@m***[.]ru** использовалась для регистрации домена 2o2o[.]ru, где в качестве имени регистратора также был указан **Andrey A Turchin**:

с 2008.08.19 по 2008.12.26	domain:	2020.RU
	nserver:	ns1.agava.net.ru.
	nserver:	ns2.agava.net.ru.
	state:	REGISTERED, DELEGATED, UNVERIFIED
	person:	Andrey A Turchin
	phone:	**********
	e-mail:	uwert@m .ru
	registrar:	NAUNET-REG-RIPN
	created:	2008.07.13
	paid-till:	2009.07.13
с 2008.07.15 по 2008.08.18	domain:	2020.RU
	nserver:	dns1.naunet.ru.
	nserver:	dns2.naunet.ru.
	state:	REGISTERED, DELEGATED, UNVERIFIED
	person:	Andrey A Turchin
	phone:	**********
	e-mail:	uwert@m .ru
	registrar:	NAUNET-REG-RIPN
	created:	2008.07.13
	paid-till:	2009.07.13

Тут стоит отметить еще один почтовый адрес, который предположительно связан с Андреем А Турчиным – **boss@lb***[.]ru**. На данный email было зарегистрировано большое количество различных доменов. Система графового анализа Group-IB выдает следующее:

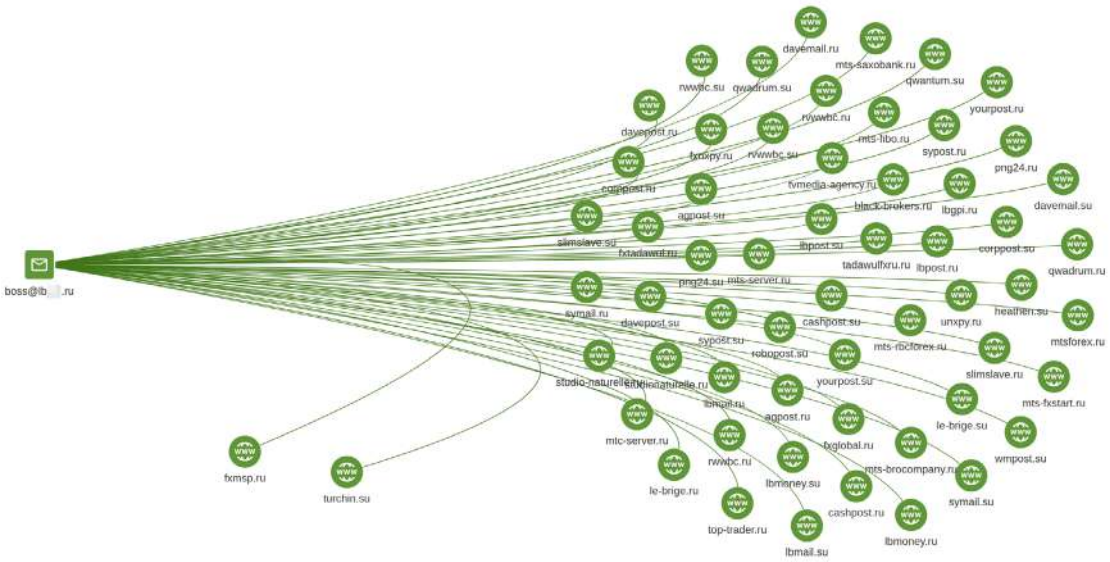
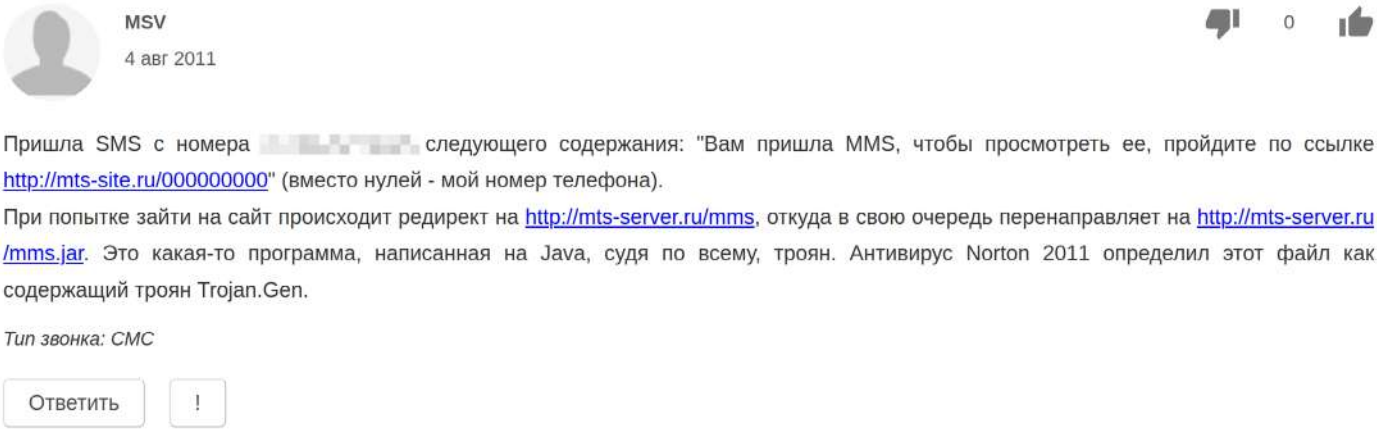


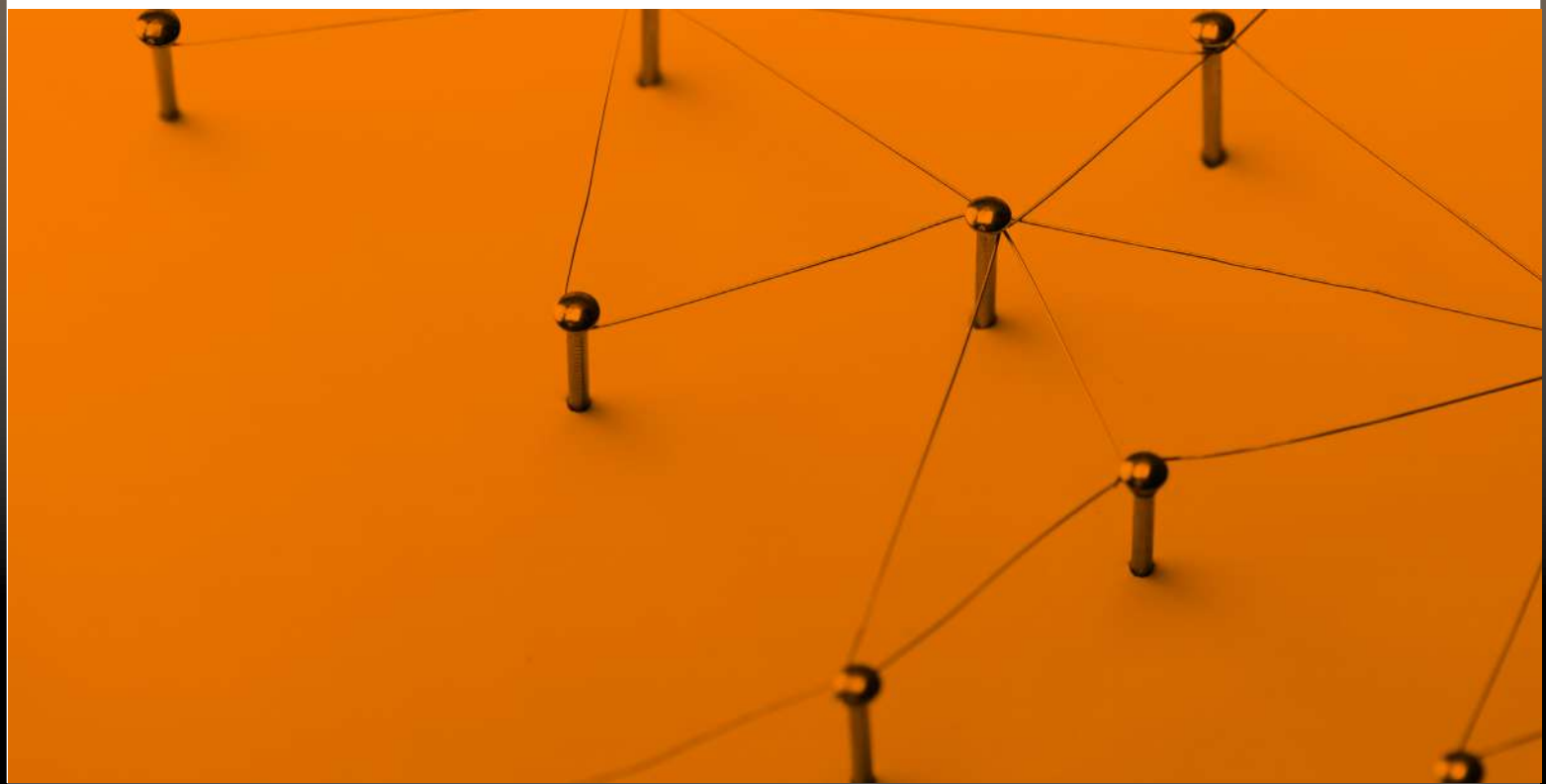
*Рис. 47 – Скриншот из интерфейса системы графового анализа Group-IB: связи почтового адреса boss@lb***[.]ru с зарегистрированными доменами*

Из более чем 60 доменов стоит отметить **turchin[.]ru** и **fxmsp[.]ru**. Наличие этих “говорящих” доменов еще раз подтверждает вышеизложенные связи. Большая часть из обнаруженных сайтов связана с торговлей на биржах (в особенности Forex), а также различными системами для автоматизации подобной торговли. Предположительно, они могли использоваться не только по прямому назначению, но и для распространения различного вредоносного ПО. Например, один из ресурсов, mts-server[.]ru, содержал вредоносный JAR-файл mts-server[.]ru/mms.jar (fc68d49bb0a0a9c35c19182760f5c274), который использовался для отправки платных СМС.

Согласно сообщениям пользователей, данный вредонос распространялся через СМС-рассылки:


MSV
4 авг 2011
0
Пришла SMS с номера [redacted] следующего содержания: "Вам пришла MMS, чтобы просмотреть ее, пройдите по ссылке http://mts-site.ru/000000000" (вместо нулей - мой номер телефона).
При попытке зайти на сайт происходит редирект на http://mts-server.ru/mms, откуда в свою очередь перенаправляет на http://mts-server.ru/mms.jar. Это какая-то программа, написанная на Java, судя по всему, троян. Антивирус Norton 2011 определил этот файл как содержащий троян Trojan.Gen.
Тип звонка: СМС
Ответить
!

Таким образом, Турчин Андрей А. (***.12.198***), проживающий в Казахстане, Алматы (согласно данным, указанным в социальных сетях, в регистрационных данных доменов и упомянутому нами ранее номеру телефона), предположительно является злоумышленником, который скрывается под псевдонимом Fxmsp. Это подтверждается фактами использования одних и тех же псевдонимов, а также общими интересами, связанными с биржевыми платформами.



GROUP-IB'S PROFILE: Fxmsp

NAME	Andrey A. Turchin
ACTIVITY	Compromises company networks and sells access to them
DOB	12/***/198***
PLACE OF RESIDENCE	Almaty, Kazakhstan
USERNAMES	Fxmsp, uwert, vidi, bosslb
ICQ	445436*** 703004***
ACCOUNTS ON UNDERGROUND FORUMS	https://lolzteam[.]net/members/125112/ http://proxy-base[.]com/members/fxmsp/ http://proxy-base[.]com/members/uwert/ https://forum.exploit[.]in/index.php?showuser=80141 https://fuckav[.]ru/member.php?u=36898
EMAIL ACCOUNTS	fxmsp@m***[.]ru uwert@m***[.]com uwert@m***[.]ru boss@lb***[.]ru
JABBER ACCOUNTS	uwerty5411@exploit[.]im fxmsp541@exploit[.]im

На момент подготовки к выпуску данного отчета, Fxmsp уже не вел публичной деятельности, однако, доподлинно неизвестно, продолжал ли он взламывать сети компаний и продавать доступы к ним. Учитывая этот риск, мы считаем необходимым дать универсальные рекомендации по способам защиты от атак, подобных тем, что проводил или проводит Fxmsp.

В разделе **“Ключевые выводы. Тактика и инструменты”** данного отчета мы указываем, что первоначальным вектором атаки Fxmsp являются открытые RDP порты. Соответственно, для предотвращения подобных инцидентов мы рекомендуем выполнить следующие шаги:

1. Смена стандартного RDP порта 3389. Учитывая, что атаки обычно носят не таргетированный характер, злоумышленники обычно перебирают стандартные порты для поиска RDP. Данный порт можно отредактировать, поменяв на любой другой.

2. Настройка блокировки учетной записи. Так как злоумышленникам 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.

3. 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 логин и пароль). Таким образом, превентивная проверка на наличие данных ваших сотрудников в утечках может существенно снизить вероятность успешной атаки.

4. 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.

5. 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.

6. 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.

7. Отключение вывода информации о последнем авторизованном пользователе на сервере. Для этого необходимо изменить групповую политику в Active Directory (GPO_name**\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**), установить параметр “Interactive logon: Do not display last user name” - на disabled.

GROUP IB

Preventing and investigating cybercrime since 2003.

www.group-ib.ru
info@group-ib.ru
www.group-ib.ru/blog
twitter.com/groupib
+7 495 984-33-64
linkedin.com/company/group-ib