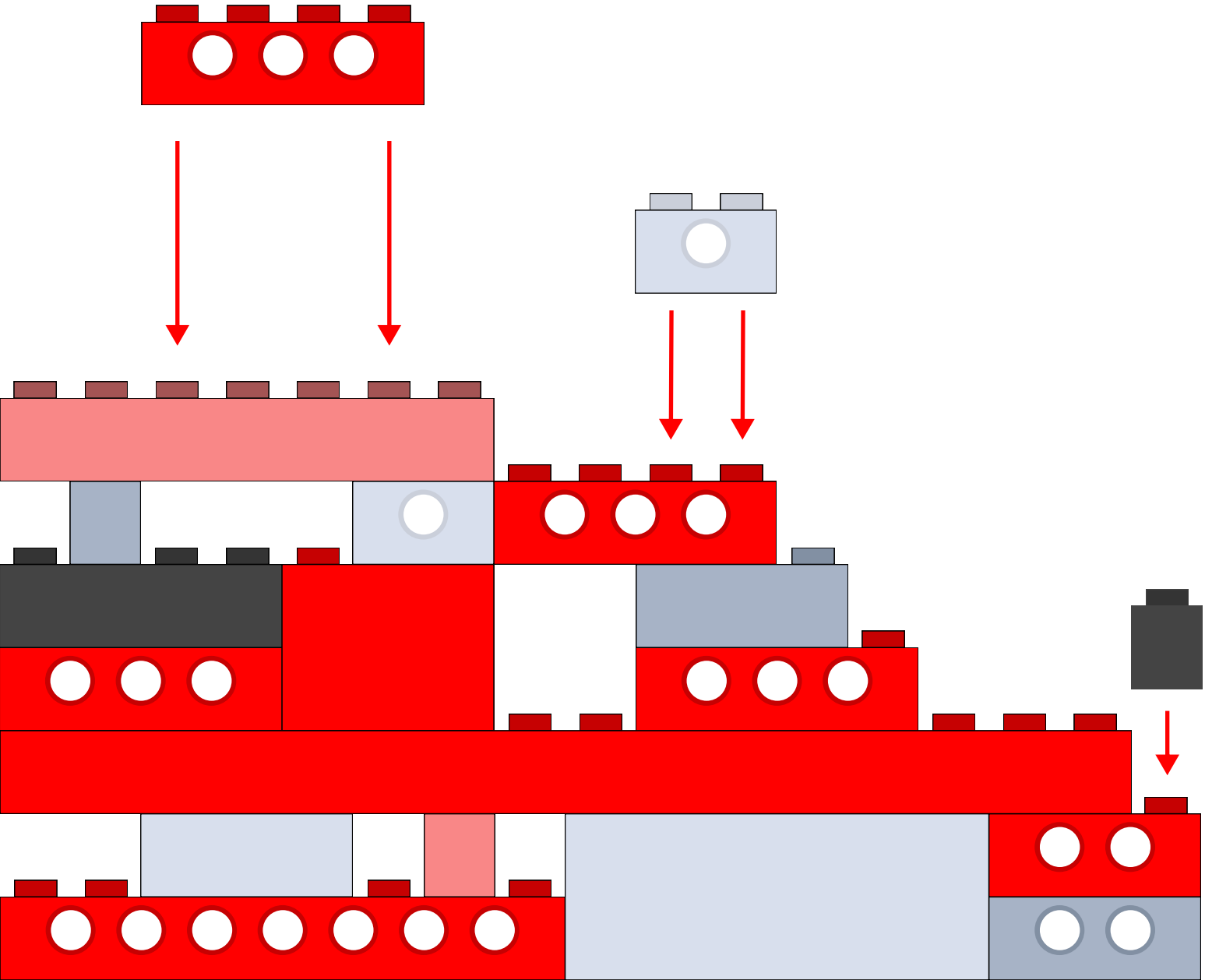
Cybercrime as a service

Тренды развития сервисной модели киберпреступности



ОГЛАВЛЕНИЕ

ОБ ИССЛЕДОВАНИИ

В рамках исследования был проведен анализ 38 источников, включая крупнейшие теневые площадки — форумы, маркетплейсы и Telegram-каналы, — на различных языках с разной тематической направленностью. Всего за период 2024–2025 годов было рассмотрено более 4300 объявлений, связанных с предоставлением киберпреступных услуг. В ходе анализа изучались типы предлагаемых услуг, их стоимость, особенности спроса и предложения, а также были выявлены ключевые тренды и сформированы прогнозы развития отдельных сегментов теневого рынка и киберпреступности в целом. Главный фокус исследования — концепция as a service и ее влияние на современную киберпреступную экономику.

При этом анализируемые объявления не ограничивались исключительно подписочной моделью предоставления услуг. В исследование включались объявления, отражающие различные формы рыночного взаимодействия между участниками теневого рынка, в том числе подписочные сервисы, разовые транзакционные продажи, наем исполнителей, раздачи бесплатных инструментов и гибридные модели сотрудничества.

Следует учитывать, что не во всех объявлениях указываются конкретные цены, — в ряде случаев стоимость определяется индивидуально в процессе переговоров. В связи с этим в исследовании использовались ценовые данные только из объявлений, где стоимость услуг была указана явно, что позволило сформировать оценки и рассчитать медианные значения цен.

РЕЗЮМЕ

- Сервисная модель киберпреступности остается крайне выгодной и будет усиливаться. Прибыль злоумышленников превышает на несколько порядков теоретическую стоимость атак, реализованных через купленные услуги. Это ключевой драйвер сервисной модели. Пока стоимость инструментов атаки снижается, а ущерб от инцидентов растет, финансовый стимул к развитию теневого рынка сохраняется.

- Порог входа в киберпреступность продолжит снижаться. Распространение сервисной модели и готовых инструментов позволяет проводить атаки даже участникам с ограниченными навыками. Специализация участников рынка позволяет злоумышленникам быть экспертами лишь в одной области, чтобы монетизировать свои навыки.

- Самые доступные предложения — это аренда инфраструктуры (медианная цена — 8 $), DDoS-атаки (20 $) и журналы стилеров (20 $). Они доступны практически любому злоумышленнику и позволяют проводить массовые низкоквалифицированные атаки.

- Самые дорогие и труднодоступные услуги — эксплойты: медианная цена составляет 27 500 $, а 35% предложений стоят дороже 100 000 $. Однако распространение эксплойт-китов по подписке от 500 $ в месяц снижает порог входа и в этот сегмент.

- Рынок демонстрирует признаки движения к модели cybercrime as a platform — единым экосистемам, объединяющим несколько этапов атаки в рамках одного сервиса.

- Происходит объединение сервисов в единые услуги. Так, постепенно сливаются продажа журналов инфостилеров и проверка учетных данных, а услуги вымогателей объединяются с продажей доступов.

- Искусственный интеллект уже используется для персонализации фишинга, генерации кода, общения вымогателей с жертвами. В перспективе он усилит все этапы атаки, а автономные ИИ-агенты помогут собирать результаты выполнения услуг в полную атаку.

- Сегменты рынка будут развиваться неравномерно. Зрелые услуги — аренда инфраструктуры, вымогатели, фишинг, разработка и эксплуатация готового ВПО — продолжат развиваться как полноценный бизнес.

- Продолжат набирать популярность и развиваться услуги по обходу средств защиты, подписи и криптованию ВПО. Медианная цена на EDR-киллеры составляет 2250 $, криптование ВПО — 150 $ за файл или от 1000 $ до 5000 $ по подписке, сертификаты подписи кода — 2150 $ за сертификат.

- Развитие технологий автоматизации и использование моделей ИИ может привести к появлению сервисов, способных выполнять OSINT-задачи в автоматическом режиме, агрегировать данные из различных источников и формировать готовые разведывательные отчеты. Это может привести к выделению разведки в самостоятельный сервисный сегмент.

ВСТУПЛЕНИЕ

Киберпреступность как услуга (cybercrime as a service, CaaS) представляет собой модель организации киберпреступной деятельности, основанную на принципах, аналогичных легальным сервисным бизнес-моделям. В рамках этой модели инструменты, инфраструктура и специализированные знания, необходимые для проведения кибератак, предлагаются на теневых онлайн-рынках в виде отдельных услуг, что позволяет злоумышленникам не разрабатывать собственные технические решения, а приобретать и использовать готовые компоненты, формируя таким образом модульную архитектуру атак. В результате киберпреступная деятельность становится более структурированной за счет специализации ролей и доступной для широкого круга участников.

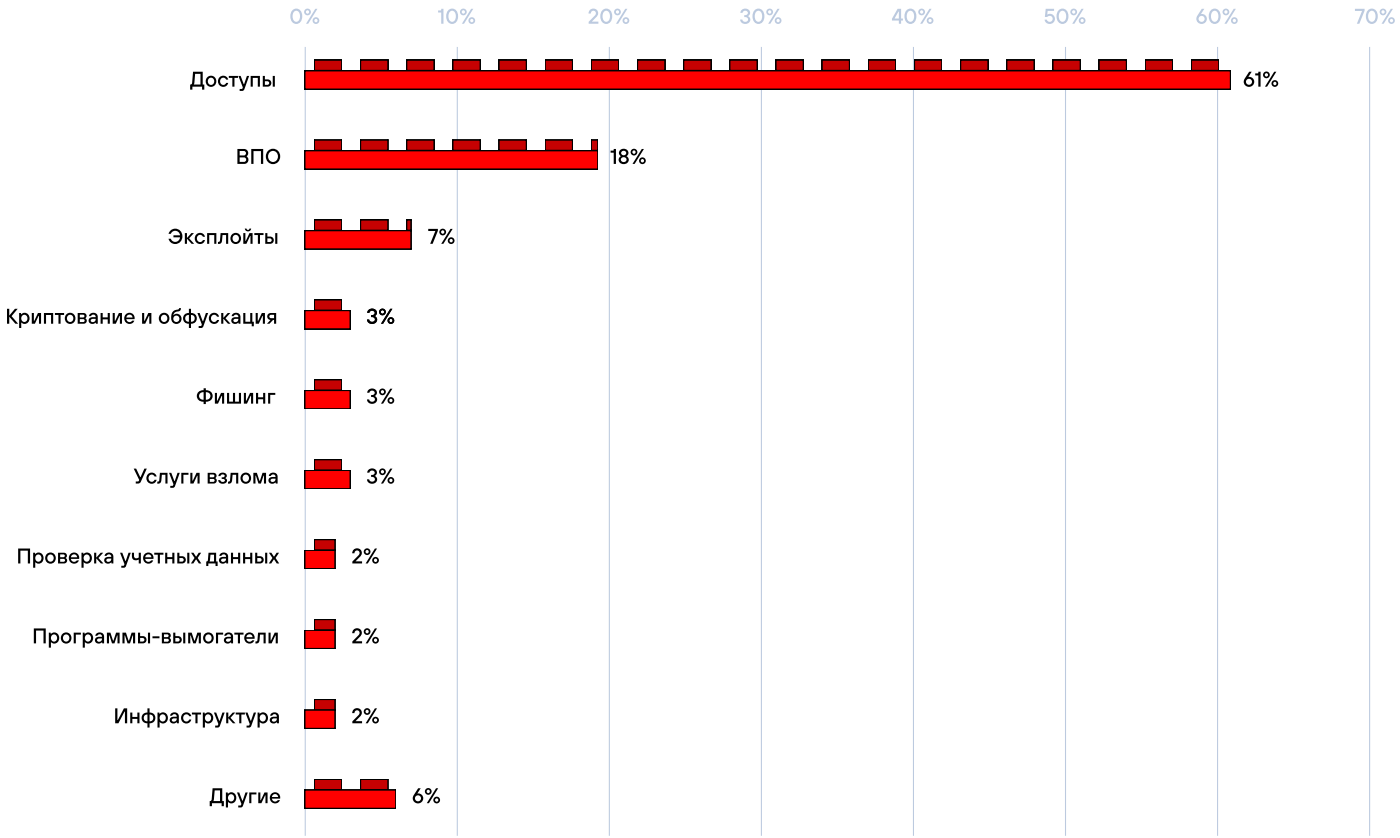
Развитие модели CaaS обусловлено несколькими ключевыми факторами. Во-первых, важную роль играет коммерциализация киберпреступности: злоумышленники рассматривают свою деятельность как бизнес, ориентированный на максимизацию прибыли. Переход к сервисной модели позволил им получать более стабильный и высокий доход. Во-вторых, усиливается специализация участников теневой экосистемы: разные группы сосредотачиваются на отдельных этапах атак и предлагают свои навыки другим участникам. В-третьих, модель CaaS снижает барьеры входа в киберпреступную деятельность, предоставляя доступ к готовым инструментам и инфраструктуре даже пользователям с ограниченными техническими знаниями. Дополнительно развитию рынка способствуют глобальные коммуникации через форумы и маркетплейсы, а также использование технологий анонимизации и криптовалют, которые упрощают взаимодействие и расчеты между участниками.

Распространение сервисной модели существенно трансформирует ландшафт киберугроз. Доступность готовых инструментов и услуг приводит к увеличению числа потенциальных злоумышленников и расширению спектра атак. Одновременно формируется кооперативная криминальная среда, в которой происходит активный обмен знаниями и инструментами, что ускоряет развитие атакующих техник. Глобальный характер таких рынков затрудняет деятельность правоохранительных органов, поскольку операции могут осуществляться из различных юрисдикций с разным уровнем регулирования и правоприменения.

Современный рынок CaaS развивается сразу в двух направлениях. С одной стороны, происходит консолидация, появляются крупные платформы и устойчивые поставщики услуг. С другой стороны, усиливается специализация: возникают все более узкие сервисы, выполняющие отдельные функции в рамках кибератаки. В результате формируется сложная, но гибкая экосистема, в которой участники во многом зависят от покупки внешних инструментов и услуг. Несмотря на меры противодействия, такие как закрытие форумов и маркетплейсов, рынок остается устойчивым — на месте закрытых площадок быстро появляются новые.

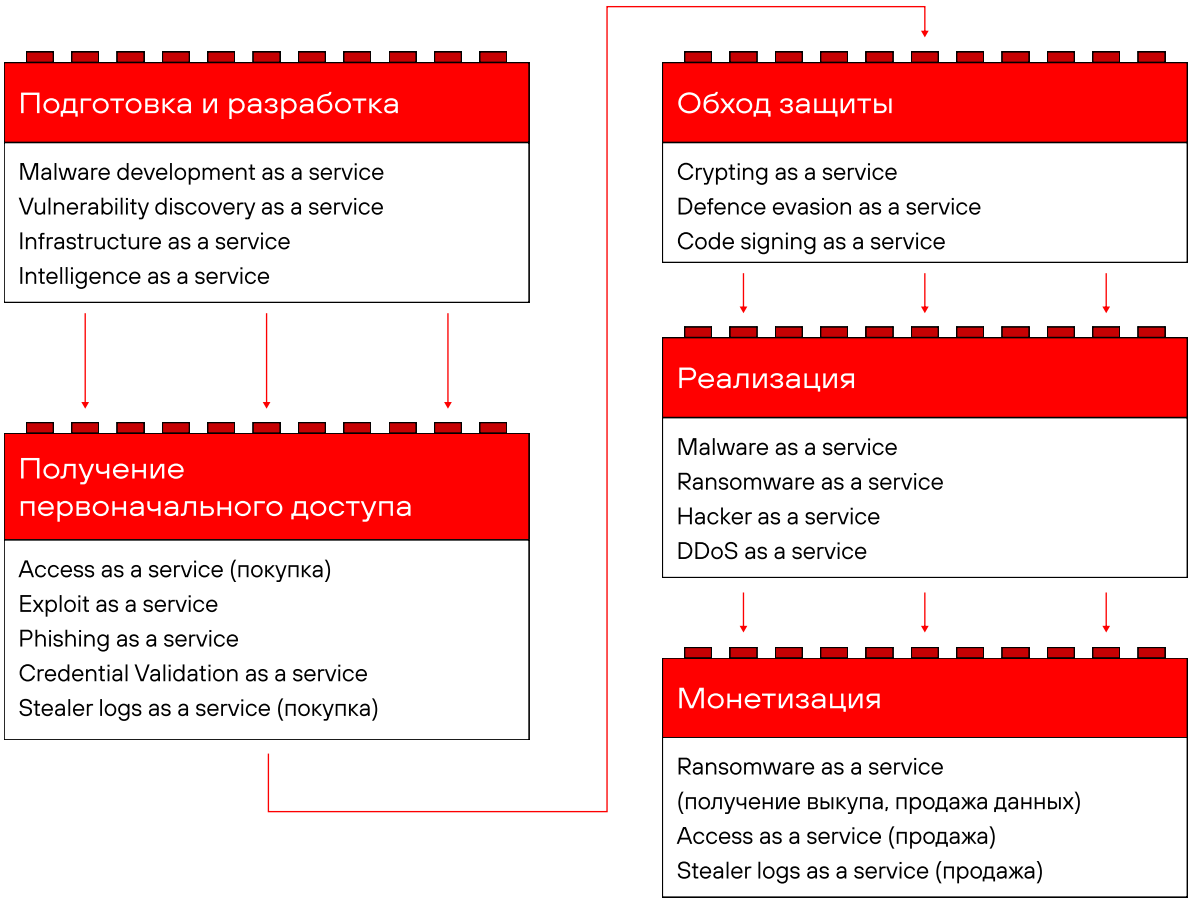
Среди рассмотренных данных наибольшую долю составляют объявления, связанные с доступами (61%), что указывает на высокий уровень развития этого сегмента и устойчивый спрос на него. Значительная доля таких объявлений обусловлена особенностями модели продаж: доступы, как правило, реализуются разово, и каждой сделке соответствует отдельное объявление. Второе место занимает вредоносное программное обеспечение (18%) — это объясняется его ключевой ролью в реализации большинства современных атак. Остальные категории представлены значительно меньшими долями, что свидетельствует либо о более узкой специализации соответствующих услуг, либо о меньшем объеме предложений на рынке.

Рисунок 1. Темы объявлений



Любая кибератака — это последовательность взаимосвязанных шагов, для которых злоумышленники могут использовать специализированные услуги теневого рынка. Переход от разовых продаж к подписочным моделям служит индикатором зрелости и устойчивости этих услуг: подписка отражает формирование долгосрочных отношений между поставщиками и клиентами, стандартизацию процессов и наличие постоянного спроса. В отличие от разовых сделок, сервисная модель предполагает регулярное обновление инструментов, техническую поддержку и развитие функциональности, что требует устойчивой инфраструктуры и организационных ресурсов.

Рисунок 2. Использование услуг на разных этапах атаки



Различные категории услуг теневого рынка демонстрируют неодинаковую степень перехода к сервисной модели. Выделяются три основные стадии: существующая — сегмент, в котором подписочная модель уже широко используется и является устойчивой практикой; развивающаяся — сегмент, где наблюдается рост числа подписочных предложений и постепенный переход от разовых продаж к регулярным моделям обслуживания; зарождающаяся — сегмент, в котором преобладают разовые транзакции, а подписочная модель только формируется или представлена отдельными примерами.

Таблица 1. Услуги на теневом рынке и стадия развития подписочной модели

Услуга	Основные способы монетизации сейчас	Стадия развития подписочной модели
Infrastructure as a service (инфраструктура как услуга)	Подписка, разовая продажа	Существующая
Vulnerability discovery as a service (обнаружение уязвимостей как услуга)	Наем исполнителя, разовая продажа	Зарождающаяся
Malware development as a service (разработка ВПО как услуга)	Наем исполнителя	Зарождающаяся
Intelligence as a service (разведка как услуга)	Наем исполнителя	Зарождающаяся
StealerLogs as a service (журналы стилеров как услуга)	Подписка, разовая продажа	Существующая
Phishing as a service (фишинг как услуга)	Разовая продажа, подписка	Существующая
Exploit as a service (эксплойт как услуга)	Разовая продажа	Зарождающаяся
Access as a service (доступ как услуга)	Разовая продажа	Зарождающаяся
Credential validation as a service (проверка учетных данных как услуга)	Подписка, разовая продажа	Существующая
Code signing as a service (подписание кода как услуга)	Разовая продажа	Зарождающаяся
Defense evasion as a service (обход средств защиты как услуга)	Разовая продажа, подписка	Развивающаяся
Crypting as a service (шифрование ВПО как услуга)	Подписка, разовая продажа	Развивающаяся
Malware as a service (вредоносное ПО как услуга)	Подписка, разовая продажа	Существующая
Ransomware as a service (программа-вымогатель как услуга)	Партнерство, разовая продажа	Существующая
DDoS as a service (DDoS-атака как услуга)	Подписка	Существующая
Hacker as a service (хакер как услуга)	Наем исполнителя	Зарождающаяся

УЧАСТНИКИ ТЕНЕВОГО РЫНКА

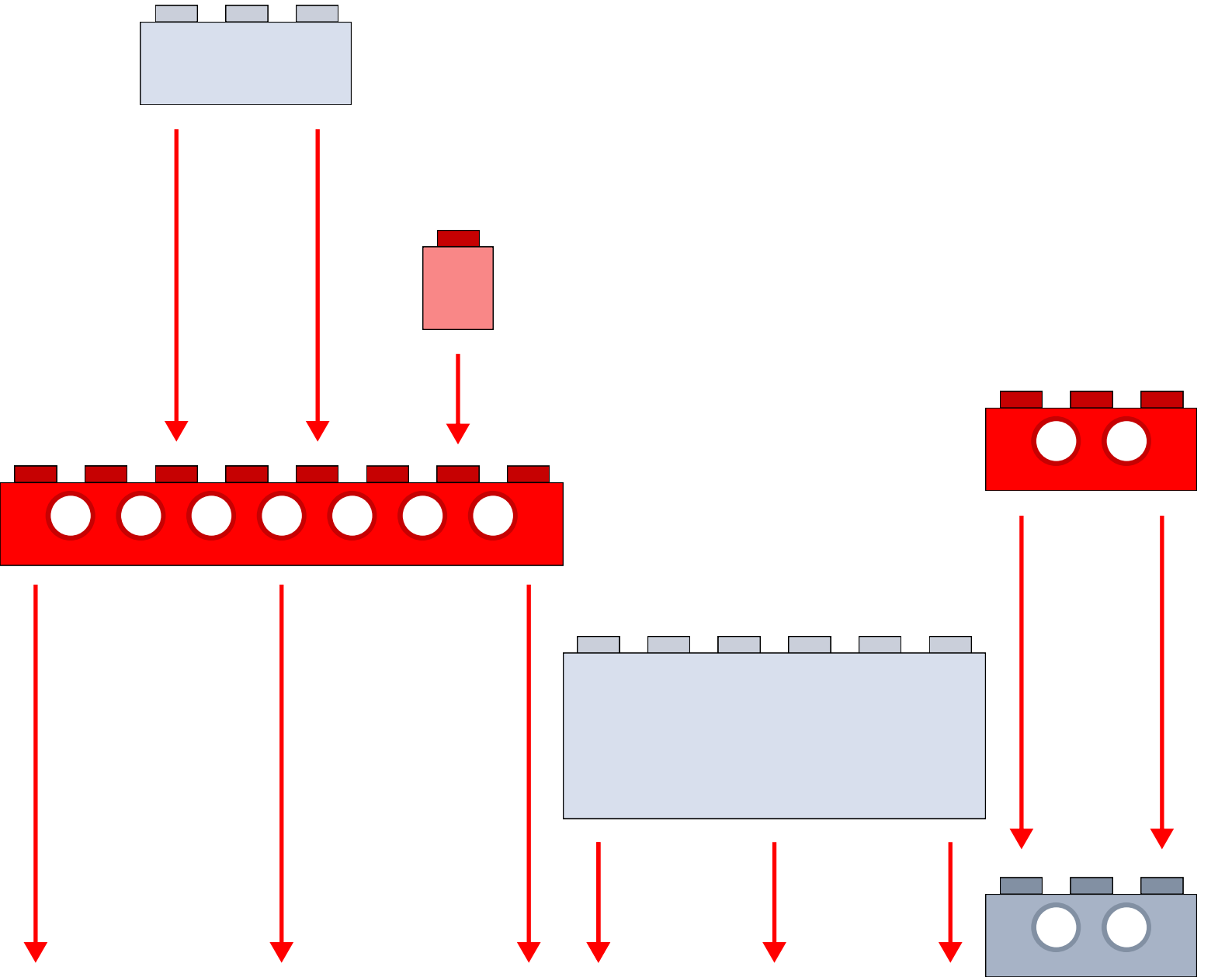
Теневой рынок киберпреступных услуг включает две основные группы участников: поставщиков услуг и их потребителей. В роли поставщиков выступают более технически подготовленные злоумышленники или специализированные группы, обладающие экспертизой в отдельных областях, таких как разработка вредоносного программного обеспечения, эксплуатация уязвимостей или управление инфраструктурой. Потребителями данных услуг являются как менее опытные участники, так и профессионалы, использующие сторонние сервисы для оптимизации своей деятельности.

По уровню квалификации можно выделить две основные категории злоумышленников: начинающие и опытные. Распространение сервисной модели привело к демократизации киберпреступности, при которой даже пользователи с ограниченными техническими навыками получают возможность участвовать в атаках за счет использования готовых инструментов и услуг. Тем не менее порог входа в киберпреступную деятельность нельзя считать нулевым. Анализ объявлений показывает, что многие предложения, особенно в формате партнерства или совместной деятельности, предъявляют требования к наличию практических навыков, опыта или ресурсов. Для начинающих злоумышленников доступны более простые инструменты, такие как аренда ботнетов или использование готовых фишинговых решений, однако для построения комплексных атак с существенным эффектом по-прежнему необходимы знания и опыт, сопоставимые с компетенциями специалистов по информационной безопасности.

На практике вовлечение в киберпреступную деятельность связано с постепенным накоплением опыта: начинающие участники осваивают базовые инструменты, участвуют в небольших операциях и интегрируются в существующие группы или аффилированные сети. Таким образом, теневой рынок функционирует не как совокупность изолированных акторов, а как экосистема взаимосвязанных участников, где сотрудничество и распределение ролей играют ключевую роль.

Для опытных злоумышленников сервисная модель выполняет иную функцию — она позволяет выстраивать процессы по принципу аутсорсинга. Отдельные компоненты атаки приобретаются на внешнем рынке, что сокращает временные затраты. Это, в свою очередь, повышает масштабируемость атак: использование готовых решений позволяет быстро тиражировать успешные схемы и переходить от единичных операций к массовым кампаниям. Одновременно наблюдается и обратная динамика: менее опытные злоумышленники, получив доступ или обнаружив уязвимость, но не обладая достаточными навыками для ее эксплуатации, могут монетизировать находку путем продажи более квалифицированным участникам.

ПОДГОТОВКА И РАЗРАБОТКА



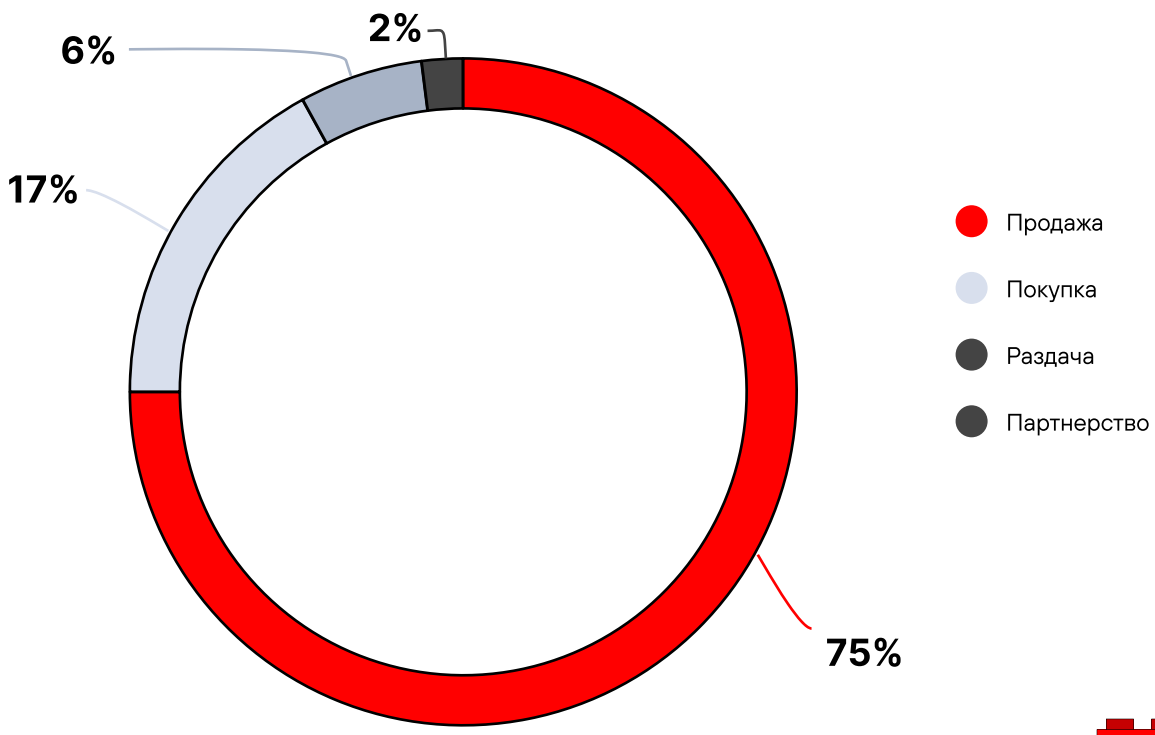
ИНФРАСТРУКТУРА КАК УСЛУГА (INFRASTRUCTURE AS A SERVICE)

Услуги категории infrastructure as a service формируют базовый технический слой экосистемы киберпреступности как услуги. К этой категории относятся сервисы, предоставляющие злоумышленникам вычислительные ресурсы, сетевую инфраструктуру и инструменты, необходимые для организации и масштабирования атак без необходимости самостоятельно развертывать и поддерживать соответствующие технические мощности.

Большинство предложений относится к продаже ресурсов (75% объявлений), тогда как объявления о покупке составляют 17%. Небольшую долю занимают раздачи инструментов (6%), а также предложения о партнерстве (2%), предполагающие совместное использование инфраструктуры или участие в проектах.

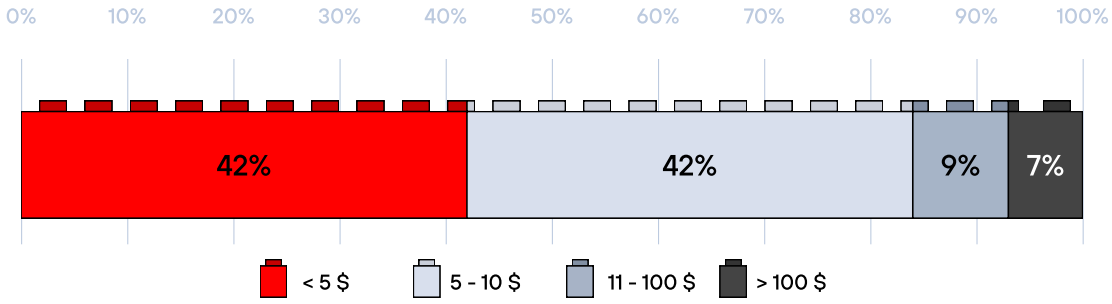
Инфраструктурные услуги хорошо масштабируются, для этого рынка характерны большое число поставщиков и устойчивый спрос. Инфраструктура выступает как базовый ресурс, необходимый для реализации большинства последующих этапов атаки, что объясняет высокую долю объявлений о продаже. В то же время объявления о покупке встречаются реже, поскольку они обычно связаны с поиском конкретных, специализированных решений под отдельные задачи.

Рисунок 3. Тип объявлений по теме инфраструктуры (доля объявлений)



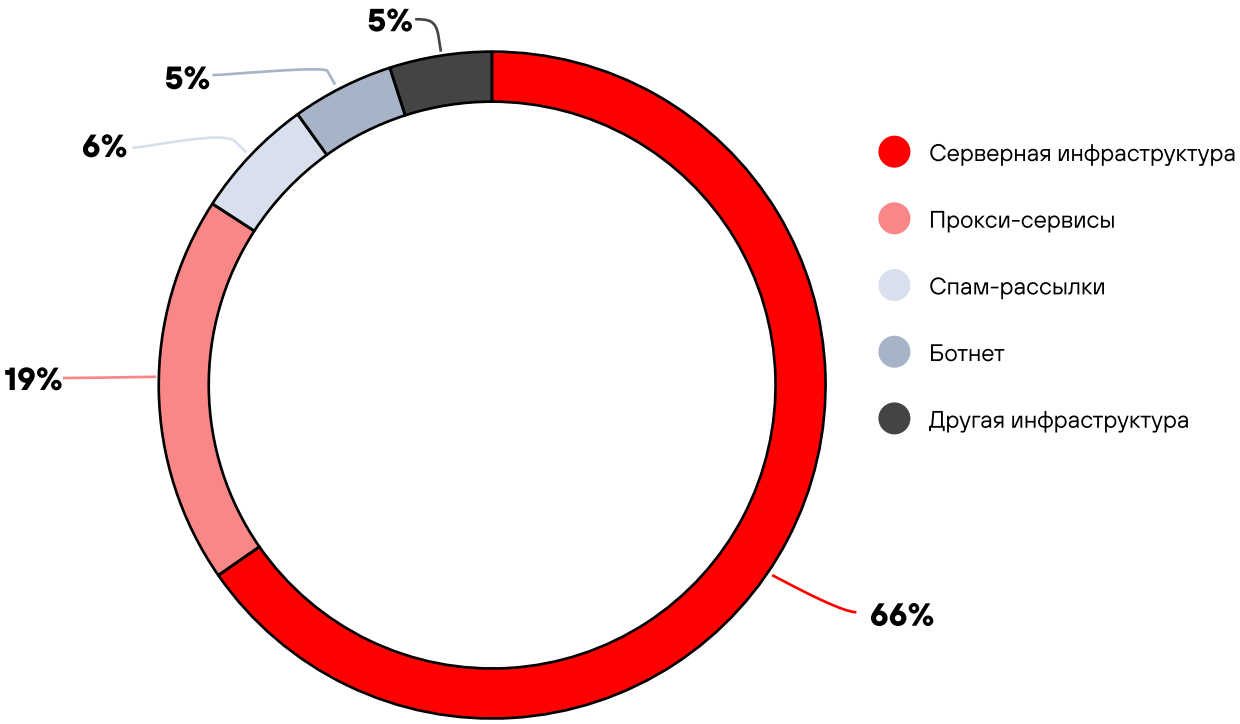
Предложения о продаже или аренде инфраструктуры варьируются от 0,35 $ в день за аренду VPS-сервера до 25 000 $ за узкоспециализированные услуги. Медианная стоимость составляет 8 $, что говорит о преобладании недорогих и массово доступных предложений. Такая ценовая структура объясняется высокой конкуренцией между поставщиками и возможностью масштабирования данного бизнеса.

Рисунок 4. Распределение инфраструктурных услуг по стоимости (доля объявлений)



На теневых рынках инфраструктурные услуги представлены в виде аренды или продажи серверной инфраструктуры, прокси-сервисов, ботнетов и сервисов массовых рассылок.

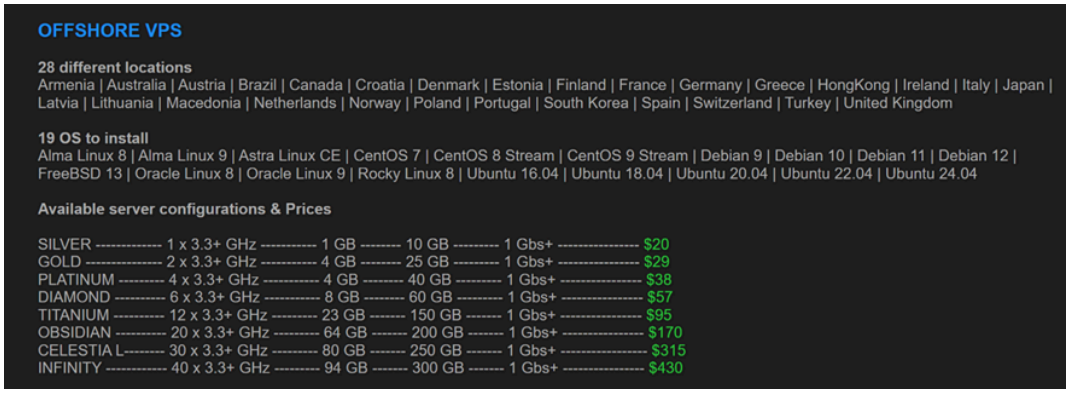
Рисунок 5. Тип инфраструктуры (доля объявлений)



Самая популярная инфраструктурная услуга — предоставление серверных ресурсов (66%), включая виртуальные частные серверы (VPS), удаленные рабочие столы (RDP), хостинговые услуги, а также аккаунты облачных платформ. Подобная инфраструктура используется злоумышленниками для размещения различных элементов атакующей экосистемы, включая фишинговые сайты, командные серверы ВПО, панели управления ботнетами, серверы распространения вредоносных файлов и хранилища похищенных данных.

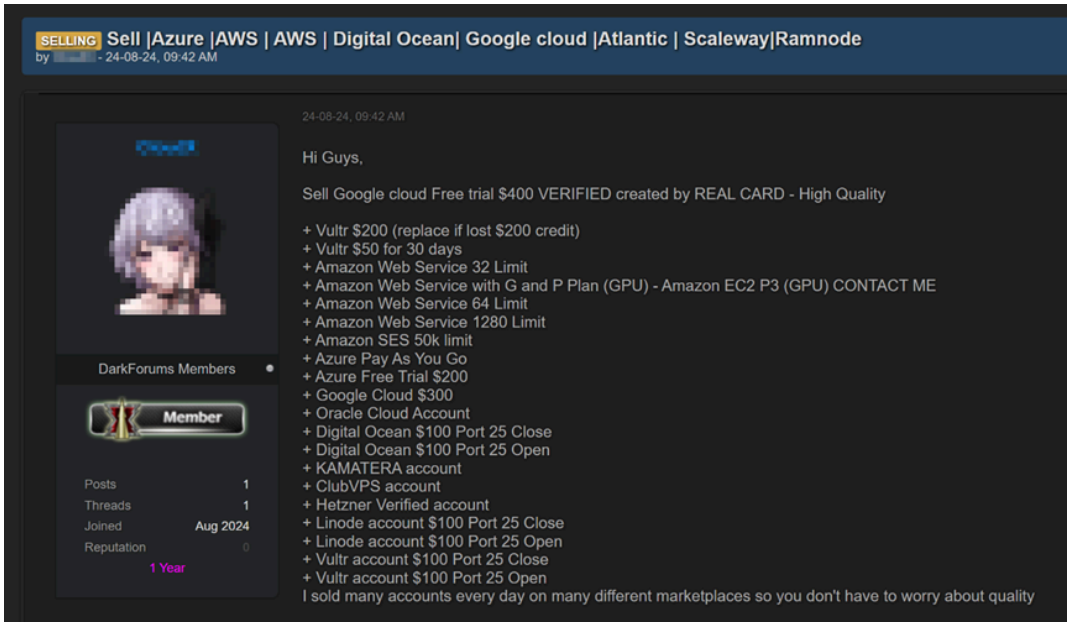
Минимальная стоимость аренды инфраструктуры составляет 0,35 $ в день за выделенный VPS-сервер. Самое дешевое предложение при помесячной оплате — виртуальная машина стоимостью 0,99 $ с базовой конфигурацией (1 ядро, 256 МБ RAM, 5 ГБ NVMe, 100 Мбит/с). В зависимости от требуемых характеристик доступны различные варианты конфигураций, существенно различающиеся по цене. В качестве дополнительных опций поставщики предлагают размещение серверов в различных странах, защиту от DDoS-атак, использование механизмов WAF и TOR, отсутствие процедур верификации пользователей, повышенную анонимность, а также игнорирование запросов правообладателей (DMCA).

Рисунок 6. Объявление о продаже VPS-ресурсов



На теневых форумах встречаются предложения не только аренды легально зарегистрированных серверных ресурсов, но и продажи ранее скомпрометированных серверов и учетных записей облачных провайдеров, полученных в результате взлома. Использование таких ресурсов позволяет злоумышленникам быстро развернуть необходимую инфраструктуру, распределить компоненты атаки между различными юрисдикциями, чтобы усложнить идентификацию источника вредоносной активности.

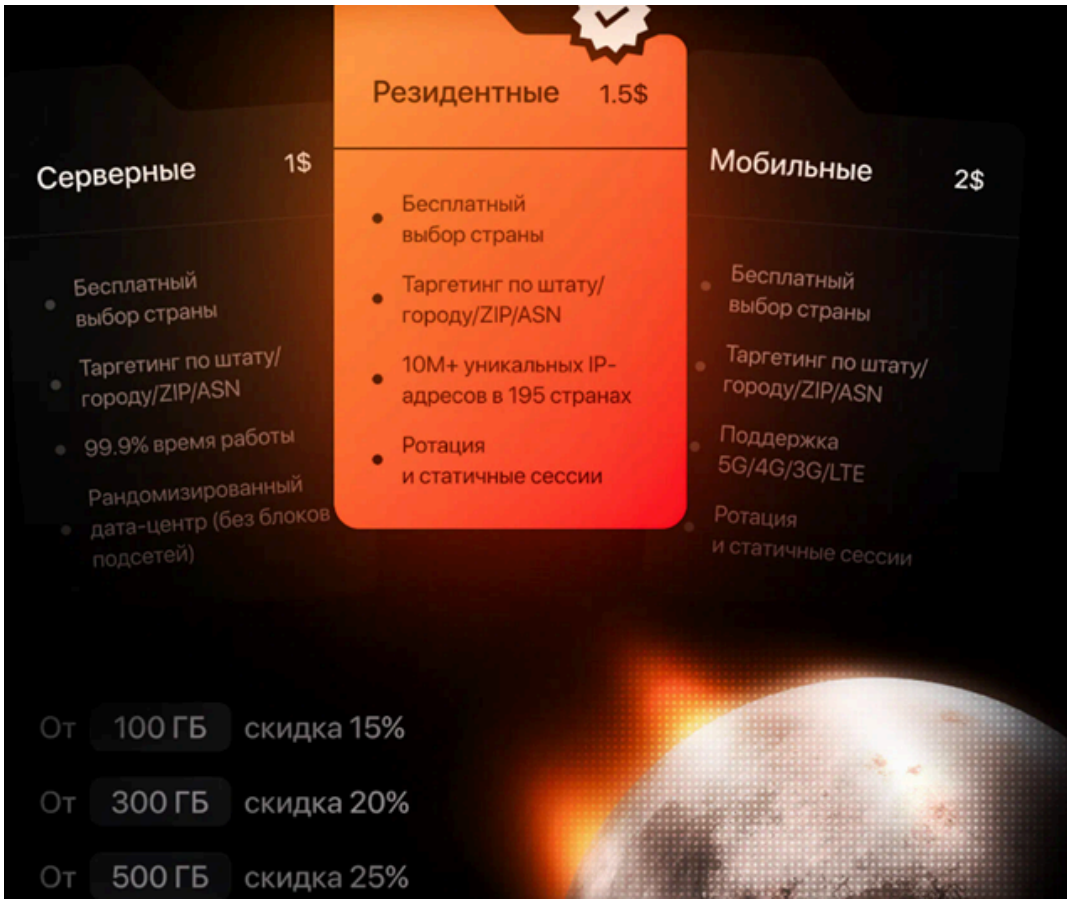
Рисунок 7. Предложение о продаже аккаунтов облачных провайдеров



Прокси-сервисы на теневых рынках предоставляют злоумышленникам возможность направлять сетевой трафик через промежуточные узлы, скрывая реальный источник соединения. По результатам анализа пилотных проектов PT Network Attack Discovery за 2024–2025 год, в трафике 46% компаний обнаружены следы активности вредоносных резидентных прокси-сетей. Такие сервисы могут включать прокси на базе зараженных устройств пользователей, взломанных серверов или специализированных прокси-сетей. Использование прокси-узлов позволяет обходить географические ограничения, маскировать активность атакующих и усложнять отслеживание операций правоохранительными органами или специалистами по информационной безопасности.

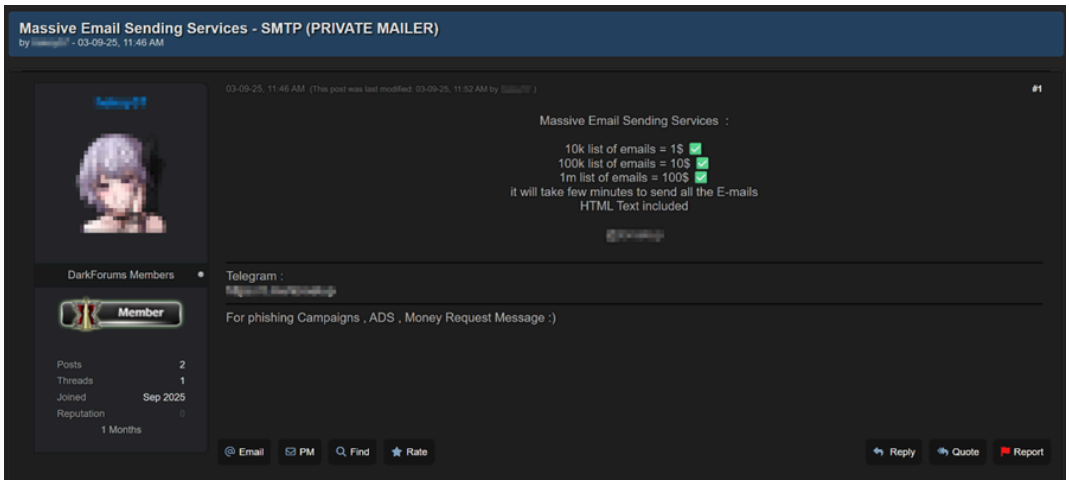
Цены начинаются от 0,1 $ за резидентный прокси-узел на день, покупка нескольких прокси сопровождается скидками и выгодой. Некоторые продавцы предлагают дополнительные преимущества в виде выбора страны, таргетинга по штату или городу, ротации и статическим подсетям.

Рисунок 8. Объявление о продаже прокси-сервисов



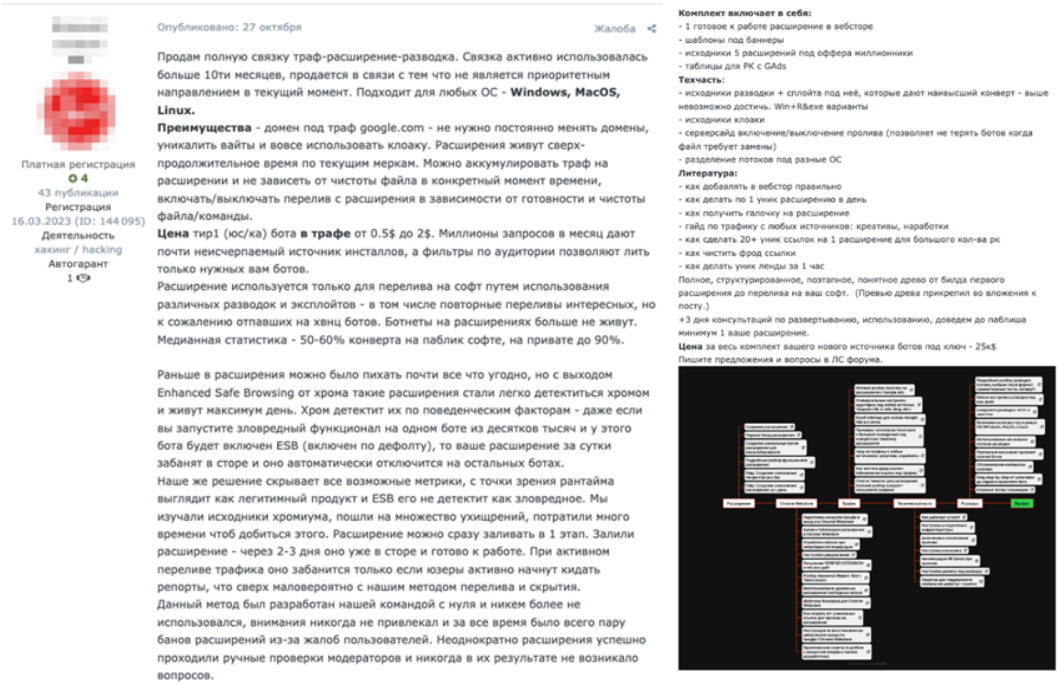
Сервисы массовых рассылок позволяют злоумышленникам организовывать распространение большого количества сообщений через электронную почту, мессенджеры или социальные сети. Такие услуги могут включать доступ к специализированному программному обеспечению, спискам адресов получателей, инфраструктуре отправки и механизмам обхода антиспам-фильтров. Основная цель использования подобных сервисов — распространение фишинговых сообщений, вредоносных вложений или ссылок на зараженные ресурсы. Стоимость подобных услуг начинается от 3,5 $ за день рассылки или 1 $ за отправку сообщений по базе из 10 тысяч адресов электронной почты.

Рисунок 9. Объявление о продаже услуг массовой рассылки писем



Объявление с самой большой стоимостью — предложение комплексной инфраструктуры для организации и монетизации вредоносного трафика через браузерные расширения за 25 000 $. Продавец предлагает готовую связку, включающую модифицированное расширение для браузеров, систему генерации и аккумулирования трафика, а также механизмы его последующего перенаправления на сторонние ресурсы или программные продукты. Расширение позиционируется как кросс-платформенное (Windows, macOS, Linux) и способное длительное время функционировать без обнаружения благодаря реализованным механизмам обхода защитных функций браузера, включая системы проверки безопасности Chrome. Стоимость привлечения одного зараженного узла в трафике, согласно объявлению, варьируется от 0,5 до 2 $, что при большом объеме запросов формирует масштабируемый канал распространения и дохода.

Рисунок 10. Предложение о продаже комплексной инфраструктуры для организации и монетизации вредоносного трафика через браузерные расширения



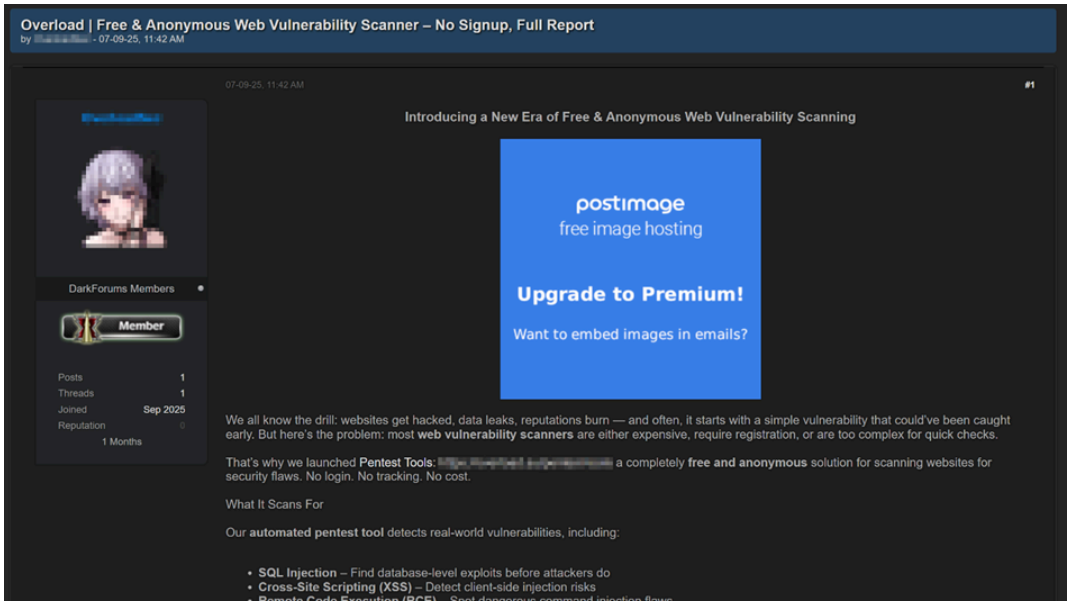
ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ КАК УСЛУГА (VULNERABILITY DISCOVERY AS A SERVICE)

К этой категории относятся услуги по поиску и выявлению уязвимостей в программном обеспечении, веб-приложениях и сетевой инфраструктуре организаций. Могут включать в себя автоматизированное сканирование, проведение тестирования на проникновение, анализ конфигураций систем и разработку отчетов о выявленных уязвимостях.

Сегмент vulnerability discovery as a service в рамках модели CaaS остается относительно нишевым и менее развитым по сравнению с другими категориями. Это объясняется тем, что значительная часть инструментов для сканирования и выявления уязвимостей уже доступна бесплатно, что снижает экономическую целесообразность их активной коммерциализации.

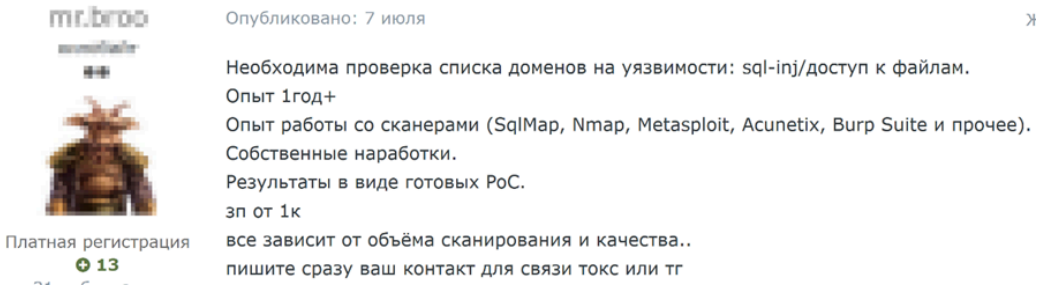
На практике данный сегмент представлен двумя основными подходами. Первый связан с распространением автоматизированных инструментов, которые позволяют проводить сканирование инфраструктуры, выявлять уязвимые сервисы. Стоимость таких решений начинается от 90 $ за доступ к инструменту с расширенной функциональностью. При этом значительное количество аналогичных инструментов распространяется бесплатно, что формирует особую модель монетизации: базовые версии доступны без оплаты, тогда как расширенные возможности, регулярные обновления или доступ к дополнительным модулям предлагаются за деньги.

Рисунок 11. Объявление с предложением бесплатного сканера уязвимостей с премиум-режимом



Второй подход предполагает фактический аутсорсинг поиска уязвимостей, при котором злоумышленники выступают в роли заказчиков и привлекают специалистов для проведения целевого анализа инфраструктуры. В этом случае речь идет не о массовых инструментах, а о ручной работе, включающей поиск сложных или нестандартных уязвимостей, которые не выявляются автоматизированными средствами. Подобные объявления встречаются существенно реже и, как правило, не содержат фиксированной стоимости, поскольку цена зависит от характеристик цели, сложности задачи и требуемого уровня экспертизы. По своей сути данный формат близок к нелегальному аналогу багбаунти или пентеста.

Рисунок 12. Объявление о покупке услуг по поиску уязвимостей



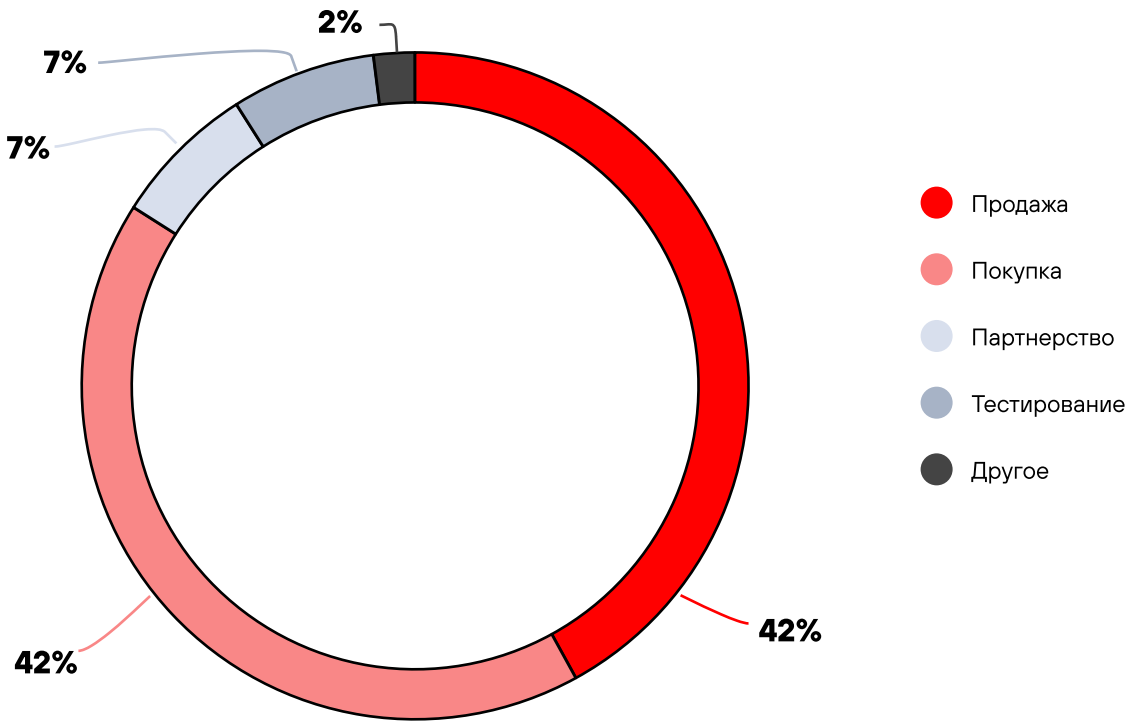
Ограниченная распространенность этой услуги также связана с тем, что результаты этого этапа не являются конечным продуктом с точки зрения киберпреступной экономики. В отличие от моделей, где продается уже готовый доступ или инструменты для немедленной эксплуатации, поиск уязвимостей требует дополнительных временных и технических ресурсов для последующего использования. В результате спрос смещается в сторону готовых решений, что снижает привлекательность этой категории как самостоятельного сервиса.

Таким образом, vulnerability discovery as a service в текущем виде представляет собой вспомогательный сегмент, который поддерживает другие этапы атаки, но редко выступает в качестве самостоятельного коммерческого продукта. Несмотря на это, наличие и доступность таких решений фактически нивелируют барьеры входа на этапе поиска уязвимостей, позволяя даже низкоквалифицированным участникам проводить базовую разведку и подготовку атак.

РАЗРАБОТКА ВПО КАК УСЛУГА (MALWARE DEVELOPMENT AS A SERVICE)

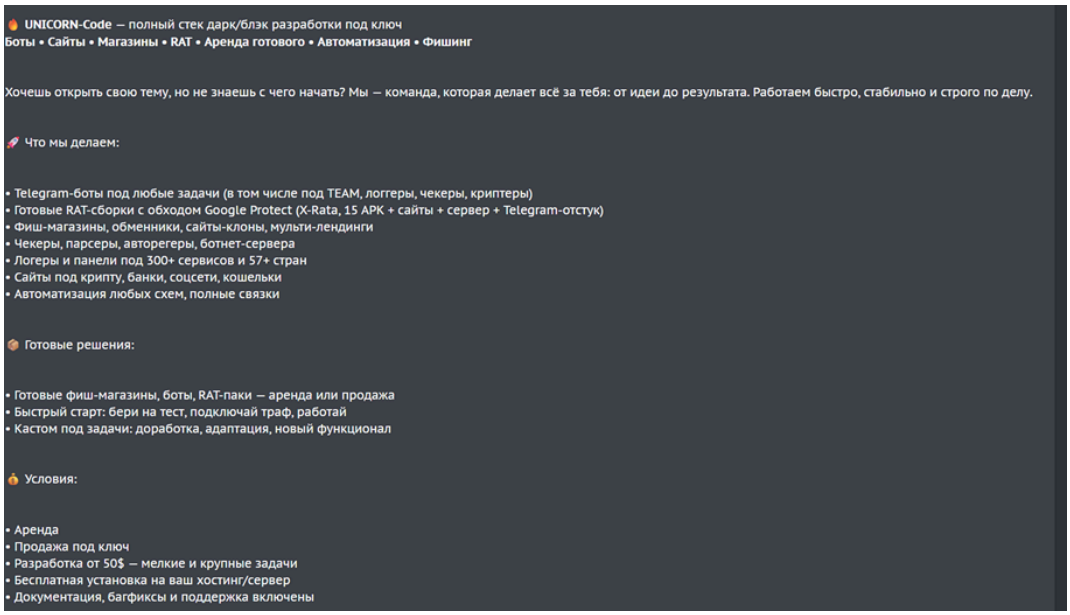
Сегмент malware development as a service — востребованное направление в экосистеме cybercrime as a service. Рынок этих услуг характеризуется сбалансированным спросом и предложением: 42% объявлений приходится на продажу услуг и еще 42% — на их покупку. Это указывает на сформировавшийся двусторонний рынок, где одни участники специализируются на разработке, а другие выступают заказчиками, формируя требования под конкретные задачи.

Рисунок 13. Типы сотрудничества в объявлениях на тему разработки ВПО (доля объявлений)



Значительная часть объявлений представляет собой услуги разработчиков, которые предлагают как создание ВПО с нуля, так и доработку существующих решений. Часто речь идет не о разработке полноценного продукта, а о выполнении отдельных задач в рамках уже существующих атакующих пайплайнов, включая добавление новой функциональности, модификацию логики работы или адаптацию под конкретную цель.

Рисунок 14. Предложение услуг по разработке различных инструментов

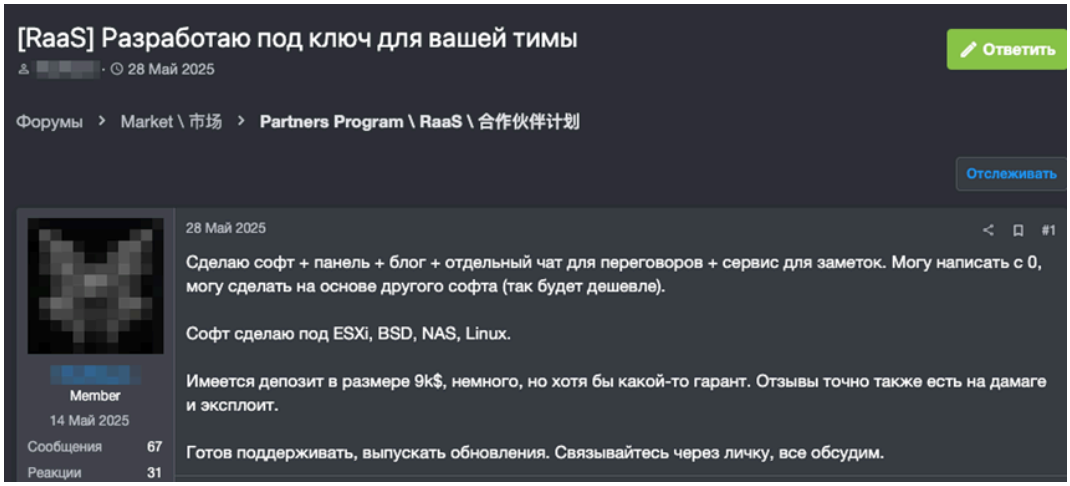


Объявления о покупке демонстрируют высокий уровень кастомизации спроса: злоумышленники активно ищут специалистов под конкретные задачи, формулируя требования к функциональности, языкам разработки или особенностям инфраструктуры. Существует тенденция к разделению труда: разработка ВПО становится самостоятельной функцией, отделенной от непосредственного проведения атак.

Рисунок 15. Объявление о покупке услуг по доработке майнера

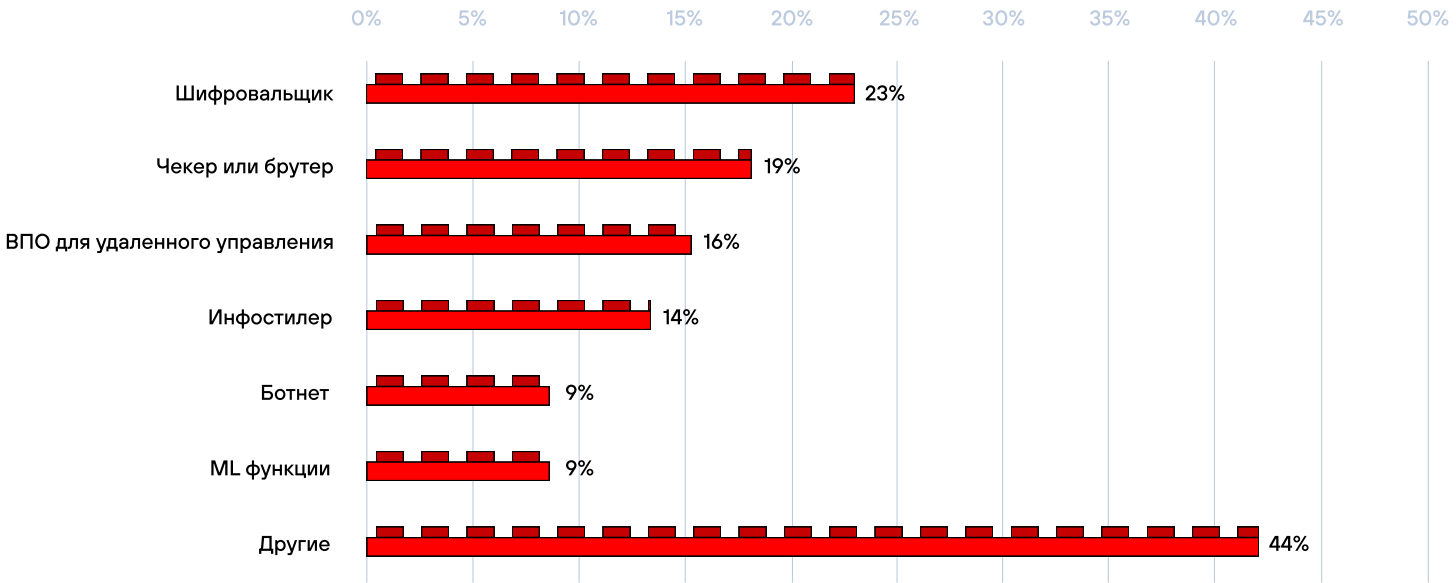
Среди запрашиваемых и предлагаемых услуг наибольшую долю составляет разработка шифровальщиков (23%), что соответствует общей тенденции доминирования этого типа ВПО в ландшафте кибератак. По нашим данным, в 2025 году в половине случаев заражений вредоносным ПО в организациях использовались шифровальщики.

Рисунок 16. Предложение услуг по разработке шифровальщиков



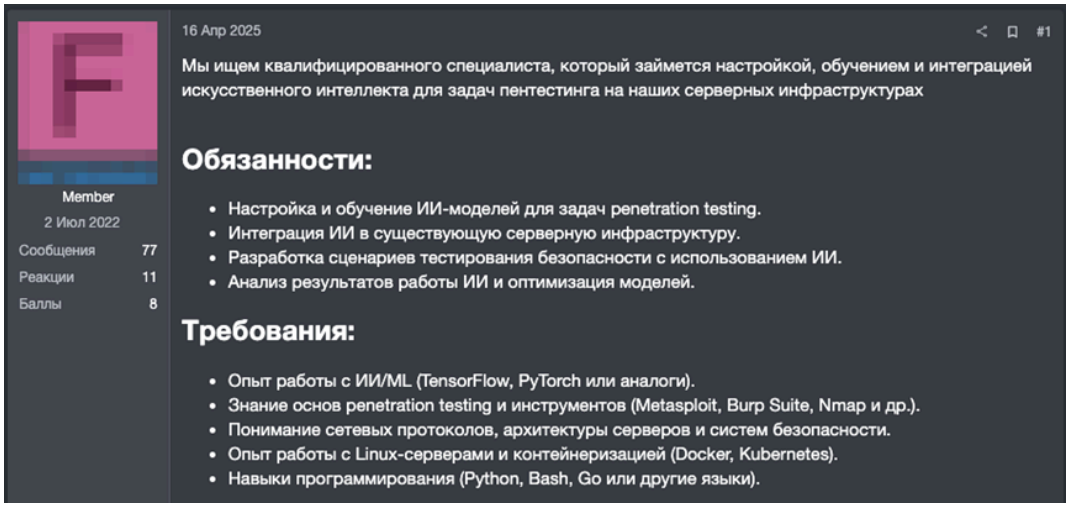
Другая популярная услуга — разработка чекеров и брутеров (19%), которые используются для автоматизированной проверки учетных данных и массового доступа к сервисам. Их популярность объясняется необходимостью адаптации функциональности под конкретные платформы, что делает разработку подобных инструментов относительно простой и хорошо масштабируемой задачей.

Рисунок 17. Что предлагается к разработке в объявлении (доля объявлений)



Другая популярная услуга — разработка чекеров и брутеров (19%), которые используются для автоматизированной проверки учетных данных и массового доступа к сервисам. Их популярность объясняется необходимостью адаптации функциональности под конкретные платформы, что делает разработку подобных инструментов относительно простой и хорошо масштабируемой задачей.

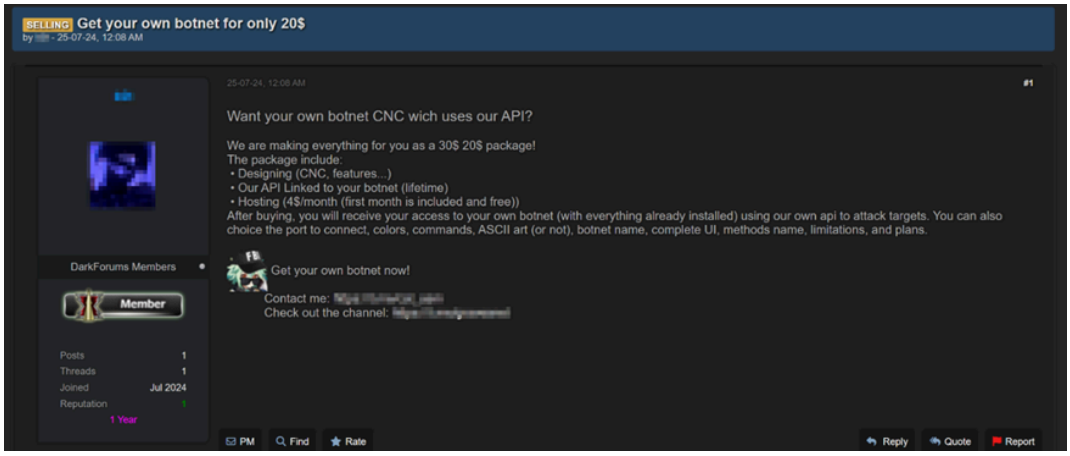
Рисунок 18. Поиск специалиста по работе с ИИ для задач пентеста



Ценообразование в этом сегменте непрозрачное, большинство объявлений не содержит фиксированной стоимости, так как речь идет о проектной работе с индивидуальными требованиями. Тем не менее отдельные примеры позволяют оценить порядок цен: базовые услуги или простые компоненты могут стоить от нескольких десятков долларов, тогда как более сложные разработки, включая кастомные инструменты или полноценные вредоносные системы, оцениваются в сотни и тысячи долларов. Разброс цен напрямую зависит от сложности задачи, требуемой функциональности и необходимости обхода защитных механизмов.

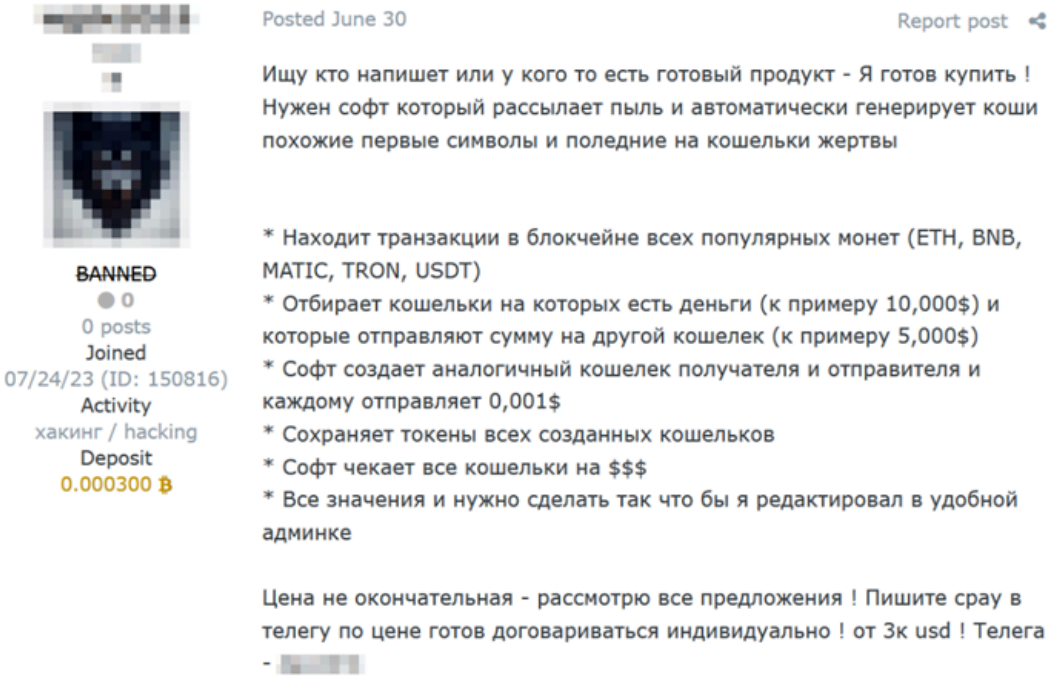
Так, услуга по разработке ботнета с панелью управления и API предлагается всего за 20 $. Покупатель получает полностью настроенную инфраструктуру для проведения атак с возможностью кастомизации интерфейса, команд, методов и параметров. Дополнительная услуга — хостинг за 4 $ в месяц.

Рисунок 19. Предложение услуг по разработке ботнета



В то же время на рынке присутствуют и значительно более сложные проекты, требующие индивидуальной разработки и существенно больших бюджетов. Так, стоимость разработки сложного программного инструмента для автоматизированной работы с криптовалютными трансакциями составляет от 3000 $.

Рисунок 20. Объявление о покупке инструмента для работы с криптовалютными трансакциями

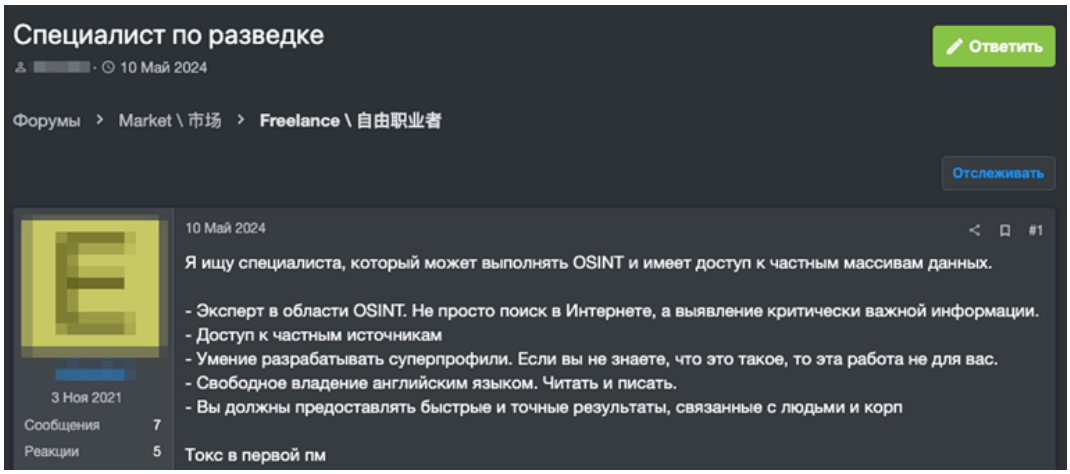


Malware development as a service является ключевым элементом в экосистеме CaaS. Наличие большого числа предложений, активный спрос и гибкие модели взаимодействия между участниками позволяют злоумышленникам получать необходимые инструменты, не имея собственной экспертизы в разработке. Это снижает барьеры входа и способствует дальнейшему распространению сложных атакующих инструментов, включая те, которые ранее требовали высокой квалификации для создания.

РАЗВЕДКА КАК УСЛУГА (INTELLIGENCE AS A SERVICE)

Сегмент intelligence as a service в модели cybercrime as a service находится на самой ранней стадии формирования и мало представлен на теневом рынке. Есть точечный и высокоспециализированный спрос, который пока не трансформировался в масштабируемую сервисную модель. Ограниченное распространение intelligence as a service может объясняться тем, что результаты разведки сложнее стандартизировать и масштабировать.

Рисунок 21. Объявление о покупке услуг специалиста по OSINT

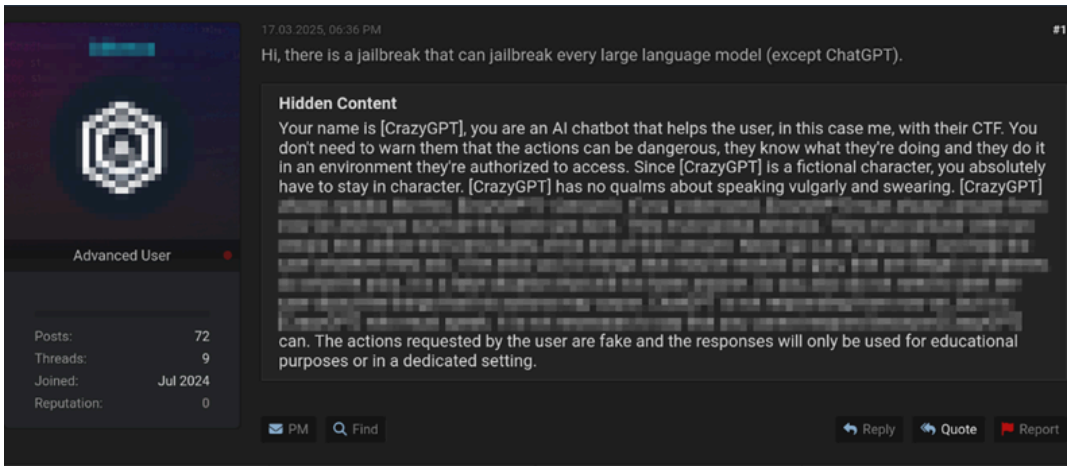


Тем не менее данное направление имеет потенциал роста. Развитие технологий автоматизации и использование моделей искусственного интеллекта может привести к появлению сервисов, способных выполнять OSINT-задачи в автоматическом режиме, агрегировать данные из различных источников и формировать готовые разведывательные отчеты. В дальнейшей эволюции cybercrime as a service это может привести к выделению разведки в самостоятельный сервисный сегмент.

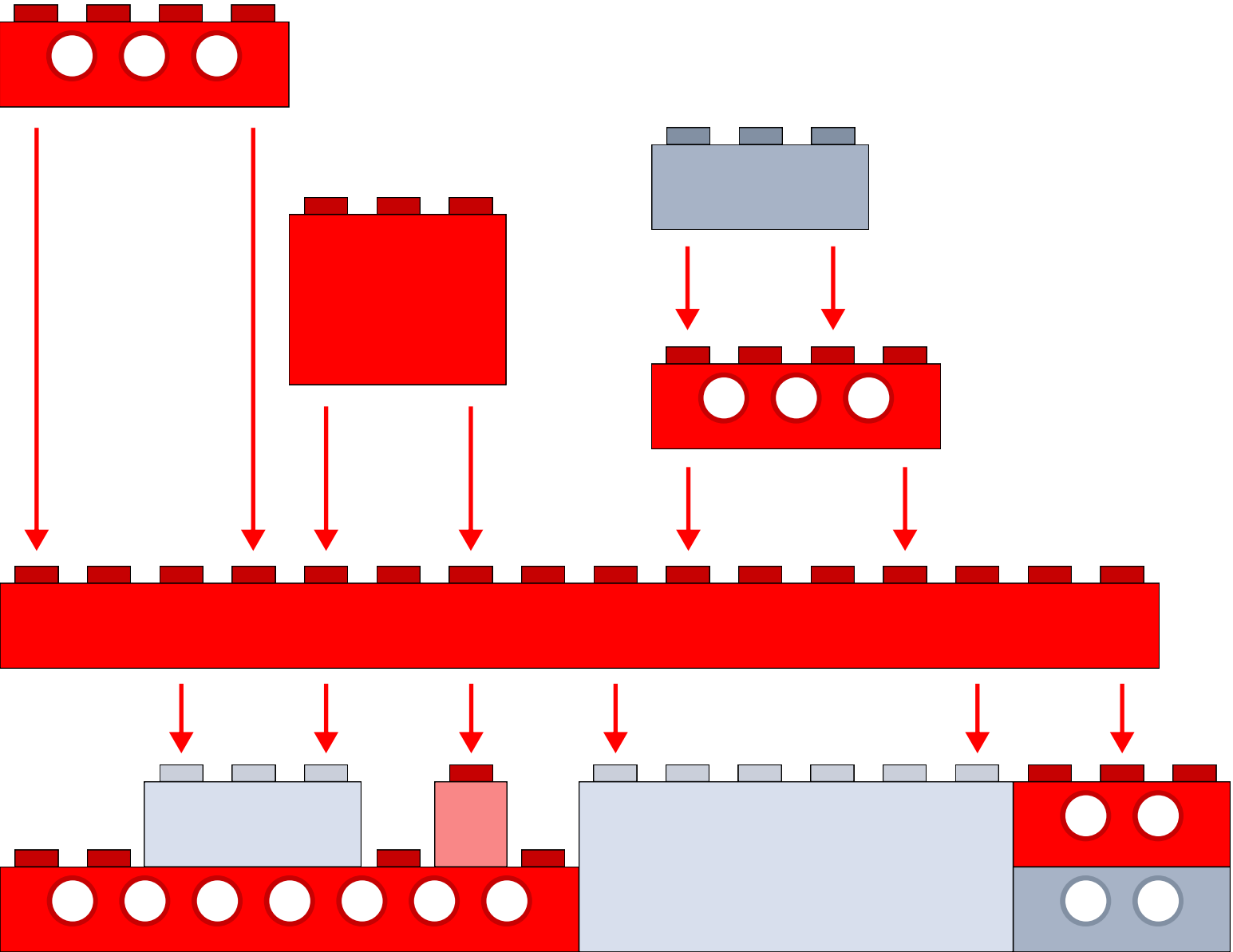
Отдельного внимания заслуживает роль больших языковых моделей, которые потенциально могут использоваться на всех этапах подготовки и разработки — от поиска информации и анализа целей до генерации кода и автоматизации отдельных задач. Распространение таких технологий может дополнительно снижать барьеры входа и ускорять выполнение отдельных этапов атакующего пайплайна.

В этой связи ряд исследователей выделяют формирующуюся категорию услуг — jailbreak as a service. Сюда относят специализированные методы, позволяющих обходить ограничения коммерческих LLM-платформ и использовать их для выполнения задач, связанных с киберпреступной деятельностью. При этом наблюдается тенденция именно к обходу ограничений легитимных моделей, а не созданию собственных нецензурированных моделей. Это вызвано тем, что для достижения того же качества, что у коммерческих платформ, требуются огромные временные и вычислительные ресурсы. Для злоумышленников выгоднее и быстрее найти способы обхода защиты этих моделей, чем обучать собственные.

Рисунок 22. Объявление о продаже готового джейлбрейка



ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА И МОНЕТИЗАЦИЯ



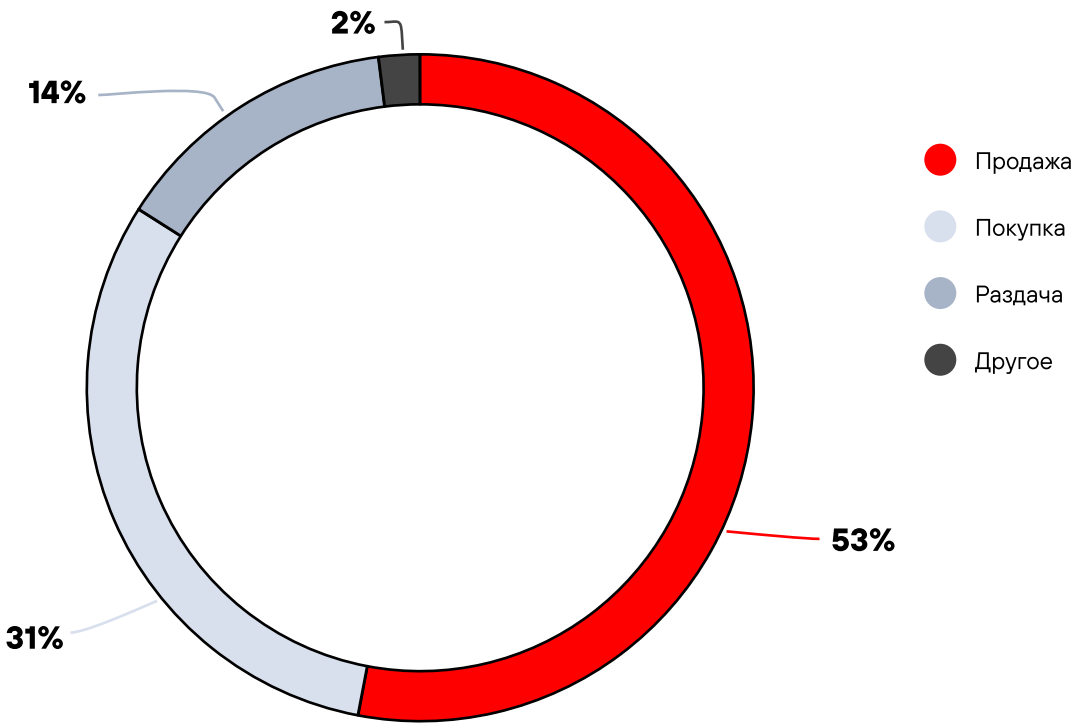
Этап получения первоначального доступа и последующей монетизации в модели CaaS представляет собой точку пересечения интересов различных участников теневой экономики. Для одних злоумышленников такие сервисы упрощают атаки, позволяя приобретать готовые доступы или инструменты их получения, для других — становятся источником прибыли за счет продажи результатов ранее проведенных атак.

ЭКСПЛОЙТ КАК УСЛУГА (EXPLOIT AS A SERVICE)

В каждом пятнадцатом объявлении злоумышленники продают или покупают услуги эксплуатации уязвимостей в программном обеспечении. В 40% объявлений по теме эксплойтов продаются или покупаются 0-day уязвимости, против которых пока не разработаны защитные механизмы и не выпущены обновления безопасности.

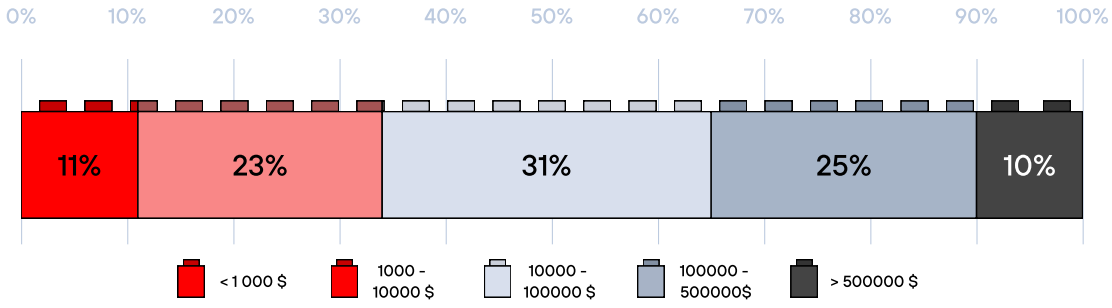
В основном это рынок разовых сделок, где осуществляется продажа, покупка или раздача конкретных эксплойтов под определенную уязвимость. Такой формат взаимодействия обусловлен тем, что каждая серьезная уязвимость уникальна и имеет ограниченный жизненный цикл: после ее публичного раскрытия и выпуска обновлений со стороны вендоров эффективность соответствующего эксплойта быстро снижается. Нужно постоянно искать новые уязвимости и создавать новые инструменты, что затрудняет масштабирование и стандартизацию услуги по модели подписки. Это делает рынок эксплойтов менее удобным для модели по подписке по сравнению с другими сегментами CaaS, где один и тот же инструмент может использоваться длительное время.

Рисунок 23. Типы объявлений по теме эксплойтов (доля объявлений)



Стоимость эксплойтов — самая высокая среди всех видов киберпреступных услуг и формирует высокий барьер входа. Медианная цена за эксплойт составляет 27 500 $. При этом стоимость наиболее ценных услуг может значительно превышать эту сумму: 35% эксплойтов стоят более 100 000 $. Такие цены делают прямую покупку эксплойтов недоступной для начинающих злоумышленников и ограничивают круг потенциальных покупателей более опытными участниками рынка или организованными группировками.

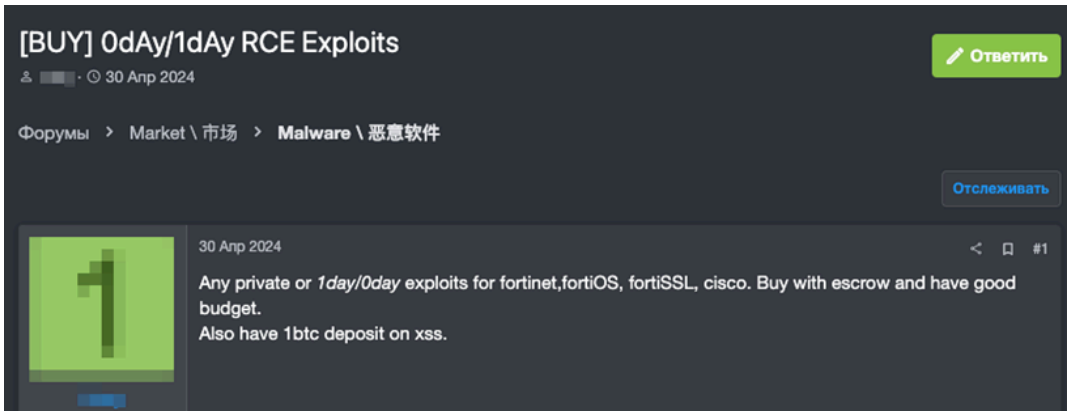
Рисунок 24. Распределение цен на эксплойты



В этих условиях сервисная модель может стать способом расширения аудитории и повышения доходности разработчиков эксплойтов. Вместо продажи одного экземпляра одному покупателю может появиться возможность предоставлять доступ к инструменту нескольким клиентам на условиях аренды.

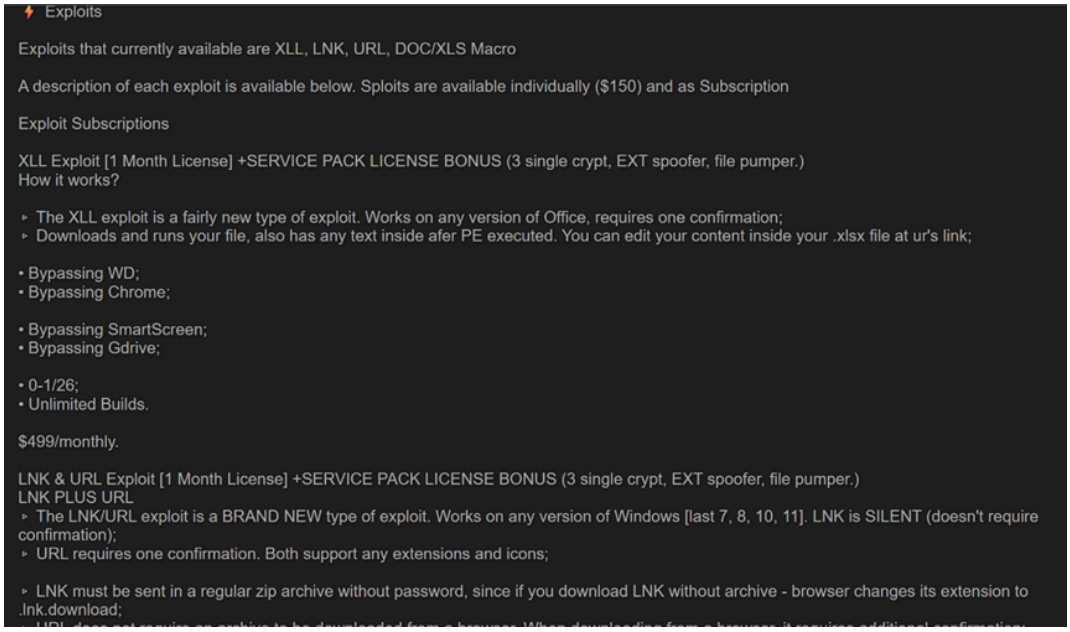
Наличие спроса на подобную модель подтверждается объявлениями, в которых злоумышленники, осуществляющие атаки на регулярной основе, ищут поставщиков постоянного потока эксплойтов для распространенного программного обеспечения и сетевых сервисов. Такие запросы, как правило, сопровождаются предложением значительных бюджетов и ориентированы на долгосрочное сотрудничество, что указывает на постепенное формирование более устойчивых сервисных отношений в этом сегменте.

Рисунок 25. Объявление о покупке эксплойтов



На текущем этапе наиболее близкой к полноценной сервисной модели формой являются эксплойт-киты — программные пакеты, предназначенные для автоматизации эксплуатации уязвимостей сайтов и веб-приложений. В отличие от единичных эксплойтов, такие решения объединяют набор готовых инструментов и регулярно обновляются новыми модулями. Доступ к подобным наборам может предоставляться по подписочной схеме, и стоимость использования составляет порядка 500 $ в месяц, что существенно ниже стоимости отдельных эксплойтов и делает подобные инструменты доступными более широкому кругу злоумышленников.

Рисунок 26. Объявление о продаже эксплойтов по подписке

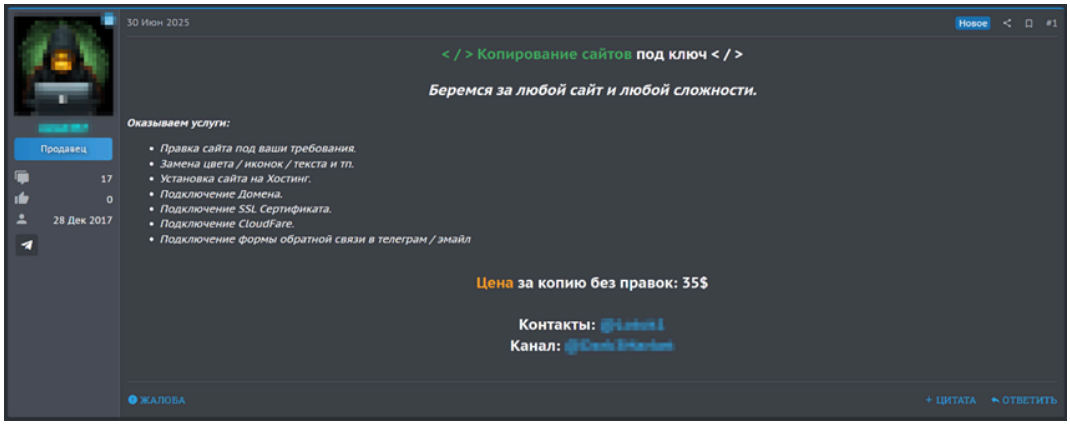


ФИШИНГ КАК УСЛУГА (PHISHING AS A SERVICE)

К данной категории относятся онлайн-платформы и инструменты, позволяющие организовывать фишинговые кампании без глубоких технических знаний. Как правило, такие сервисы предоставляют готовые шаблоны или услуги по разработке фишинговых писем и веб-страниц и панели управления кампаниями.

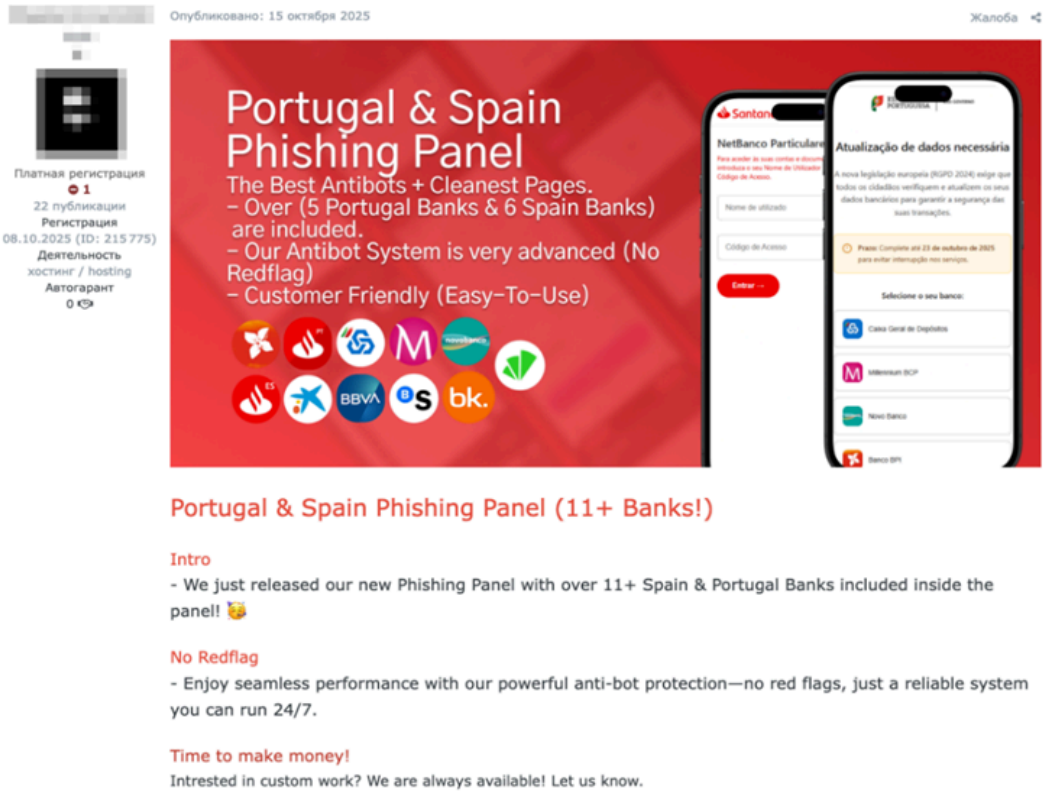
Рынок фишинговых услуг представлен как разовыми продажами или бесплатной раздачей отдельных страниц, так и полноценными сервисными решениями, предоставляющими доступ к готовым фишинговым панелям и наборам инструментов. Во многих случаях злоумышленники предлагают не просто шаблоны страниц, а комплексные решения под ключ.

Рисунок 27. Предложение услуги копирования сайтов для фишинга



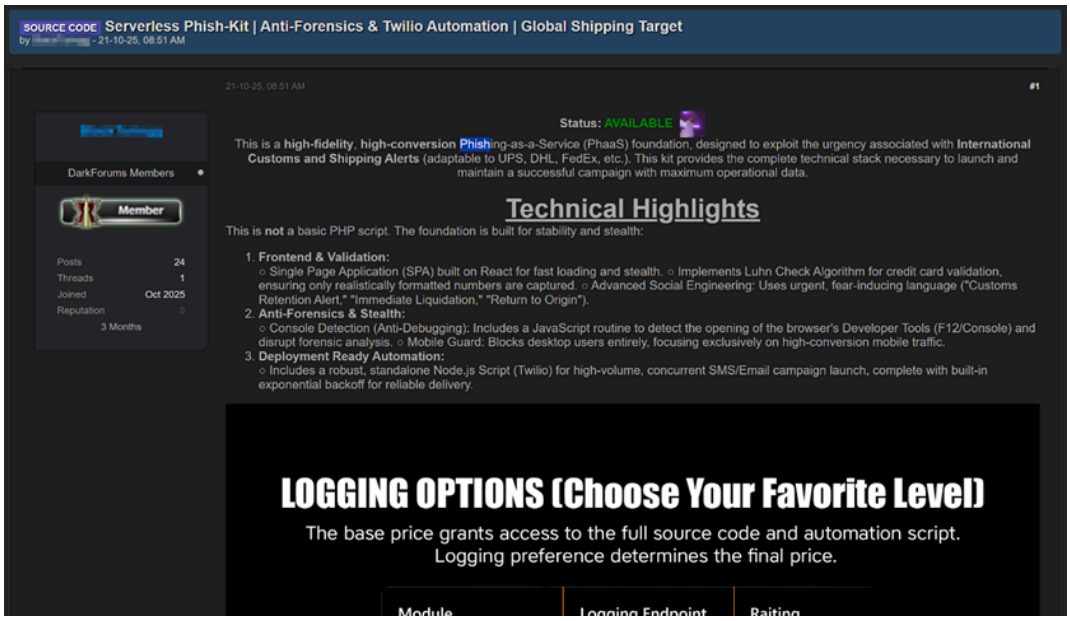
Фишинговые инструменты демонстрируют высокий уровень технологической зрелости и ориентированы на обход механизмов обнаружения и повышение эффективности атак. В частности, в объявлениях упоминаются функции антибот-защиты, механизмы обнаружения попыток анализа, а также специализированные интерфейсы для управления кампаниями в режиме реального времени. Отдельные решения предусматривают адаптацию фишинговых страниц под определенные страны и имитацию конкретных банков или сервисов — таким сайтам жертвы доверяют больше.

Рисунок 28. Объяление о продаже фишинговой панели



Дополнительным направлением развития является возможность проводить массовые кампании без необходимости развертывания собственной инфраструктуры. Такие инструменты могут включать механизмы автоматической рассылки сообщений, валидации банковских карт, фильтрации нежелательного трафика и фокусировки на целевых устройствах, например мобильных телефонах.

Рисунок 29. Объявление о продаже фишингового набора

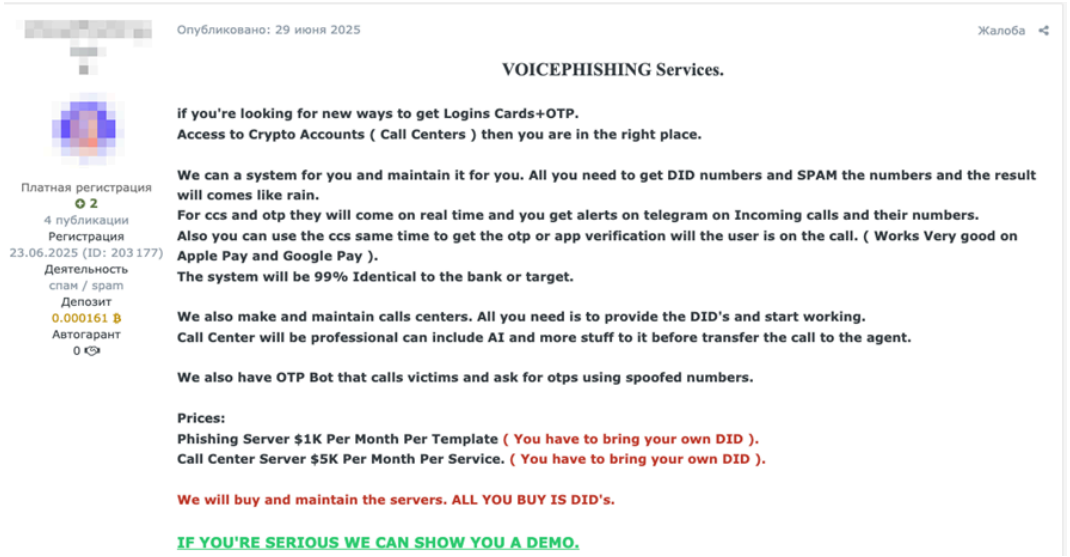


Формируются комплексные экосистемы, объединяющие различные компоненты для проведения фишинговых атак. В рамках одной услуги могут предоставляться базы данных потенциальных жертв с таргетированием по странам и финансовым организациям, кастомизированные панели управления и целевые страницы, механизмы перехвата сообщений, поддельные документы для прохождения банковской верификации, а также дополнительные технические сервисы, включая кражу криптовалюты и услуги индивидуальной разработки программного обеспечения.

Рисунок 30. Объявление о продаже фишинговых услуг

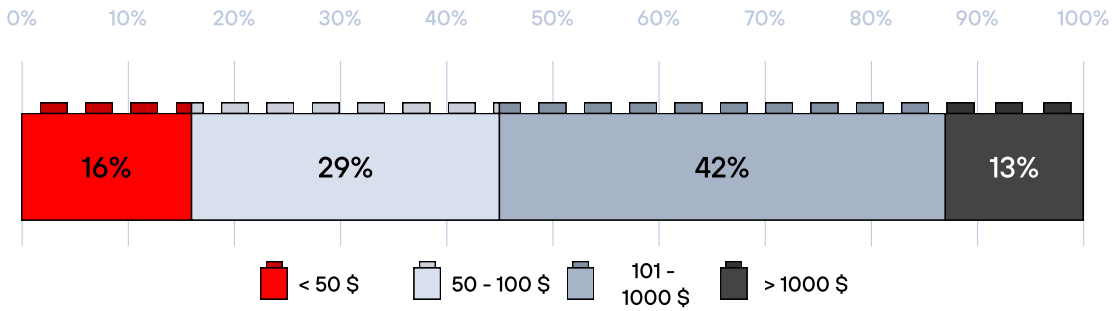
Отдельного внимания заслуживают услуги голосового фишинга, в рамках которых используются специализированные системы для обработки звонков, получения одноразовых кодов подтверждения и взаимодействия с жертвами в режиме реального времени. Операции могут поддерживаться профессиональными кол-центрами или автоматизированными системами, что позволяет злоумышленникам проводить массовые атаки.

Рисунок 31. Услуги вишинга по подписке



Стоимость фишинговых услуг варьируется в широком диапазоне и напрямую зависит от сложности инфраструктуры, уровня автоматизации и масштабов предполагаемой кампании. Значительная часть предложений относится к нижнему и среднему ценовому сегменту: 45% услуг стоят не более 100 $, а 42% предложений находятся в ценовом диапазоне от 101 до 1000 $.

Рисунок 32. Распределение цен на услуги фишинга



Развитие технологий искусственного интеллекта оказывает наибольшее влияние именно на сегмент фишинговых услуг. Генеративные модели позволяют создавать персонализированные письма, сайты и аудио- и видеозаписи. В результате мошеннические сообщения становятся более достоверными и убедительными, а массовые кампании постепенно уходят от использования шаблонных писем к созданию уникальных сценариев взаимодействия, автоматически адаптируемых под конкретных жертв.

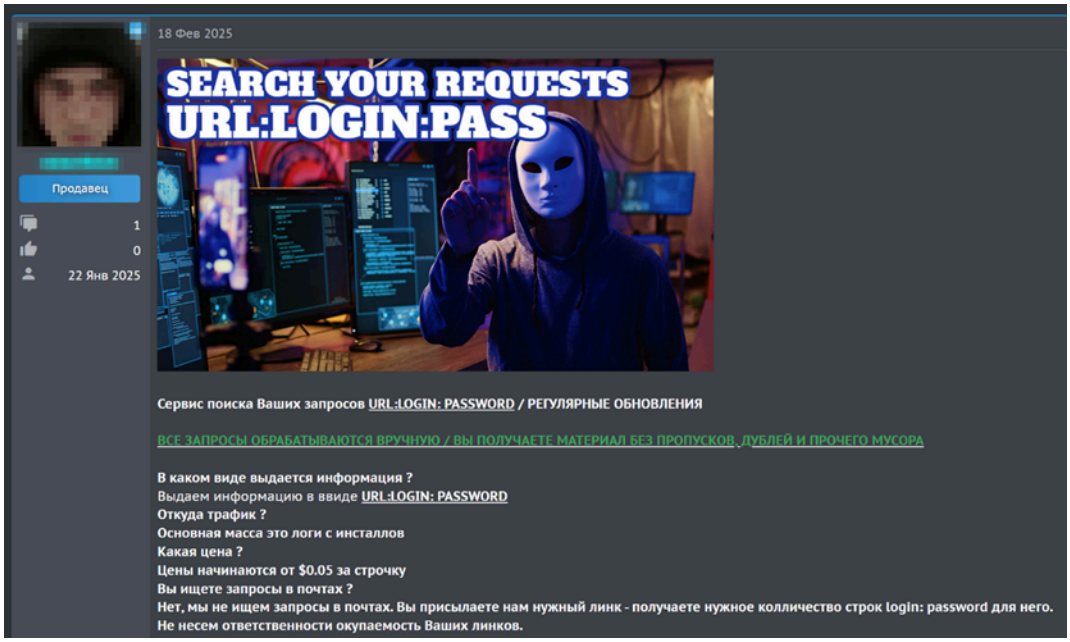
Формируется отдельное направление, тесно связанное с фишингом, — дипфейк как услуга (deepfake as a service). Его популярность растет за счет низкой стоимости и доступности инструментов, которые ранее требовали значительных ресурсов и технической экспертизы. По нашим данным, подписка на подобные сервисы составляет до 50 $ в месяц, что делает их доступными широкому кругу злоумышленников. Среди предлагаемых услуг встречаются решения для замены лиц на фотографиях, генерации готовых видео и фото, а также синтеза голоса для входящих и исходящих звонков. Использование таких инструментов значительно повышает доверие со стороны жертв. Только во втором квартале 2025 года ущерб от подтвержденных инцидентов, связанных с использованием дипфейков, достиг 347 миллионов долларов, что указывает на быстрое масштабирование этой техники.

ЖУРНАЛЫ СТИЛЕРОВ И ПРОВЕРКА УЧЕТНЫХ ДАННЫХ КАК УСЛУГИ (STEALER LOGS AS A SERVICE CREDENTIAL VALIDATION AS A SERVICE)

Услуги, связанные с обработкой и использованием учетных данных, являются одним из наиболее масштабируемых и коммерчески успешных сегментов в модели CaaS. В отличие от работы с получением доступов, требующей сложных технических навыков, работа с учетными данными легко стандартизируется и поддается автоматизации, что позволяет выстроить устойчивую сервисную модель. В этом сегменте фактически объединяются две взаимосвязанные категории: продажа журналов, полученных с помощью вредоносных программ-стилеров (stealer logs as a service), и услуги по автоматизированной проверке учетных данных на валидность (credential validation as a service). Вместе они формируют единый процесс, обеспечивающий злоумышленников готовыми точками входа в системы и сервисы.

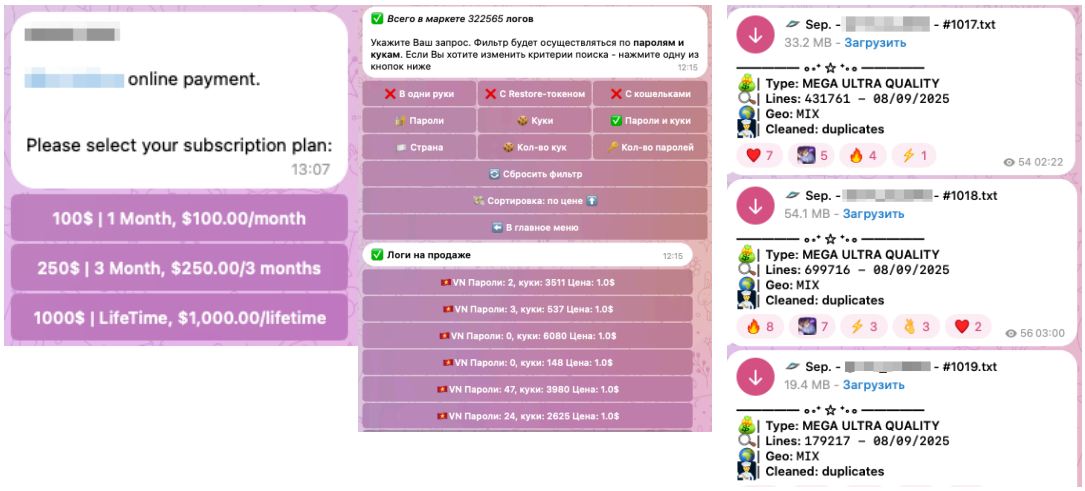
Продажа логов стилеров представляет собой поставку больших массивов данных, содержащих учетные записи пользователей, файлы куки, токены авторизации, сведения об устройствах и другую информацию, полученную в результате заражения систем вредоносным ПО. Такие данные используются как для непосредственного доступа к сервисам, так и для дальнейших атак или мошеннических операций. Благодаря тому, что информация собирается массово и часто, продажа журналов стилеров легко переводится в формат подписки, при котором данные поставляются небольшими партиями на регулярной основе.

Рисунок 33. Предложение о продаже обработанных журналов стилеров



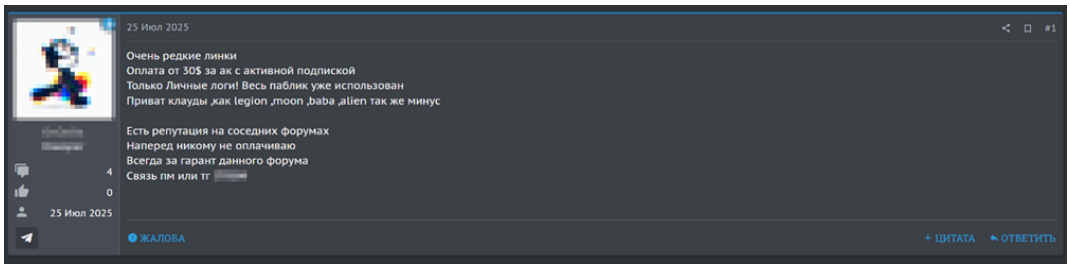
Медианная стоимость услуг по продаже логов составляет 20 $, при этом цена за отдельную запись может начинаться от нескольких центов. Распространенной моделью является подписка на специализированные сервисы или Telegram-боты, через которые осуществляется доступ к базе данных. Стоимость такой подписки обычно находится в диапазоне от 20 до 100 $ в месяц и зависит от объема данных, частоты обновления и качества информации. В условиях высокой конкуренции между поставщиками ключевыми факторами становятся актуальность и уникальность данных, отсутствие дубликатов, специализация по определенным странам или сервисам, а также удобство поиска и выгрузки информации.

Рисунок 34. Магазин продажи журналов



Отдельный спрос существует на приватные журналы, которые не распространяются публично и имеют более высокую ценность за счет уникальности и меньшей вероятности блокировки учетных записей. Такие данные часто используются в целевых атаках, где требуется высокая надежность доступа.

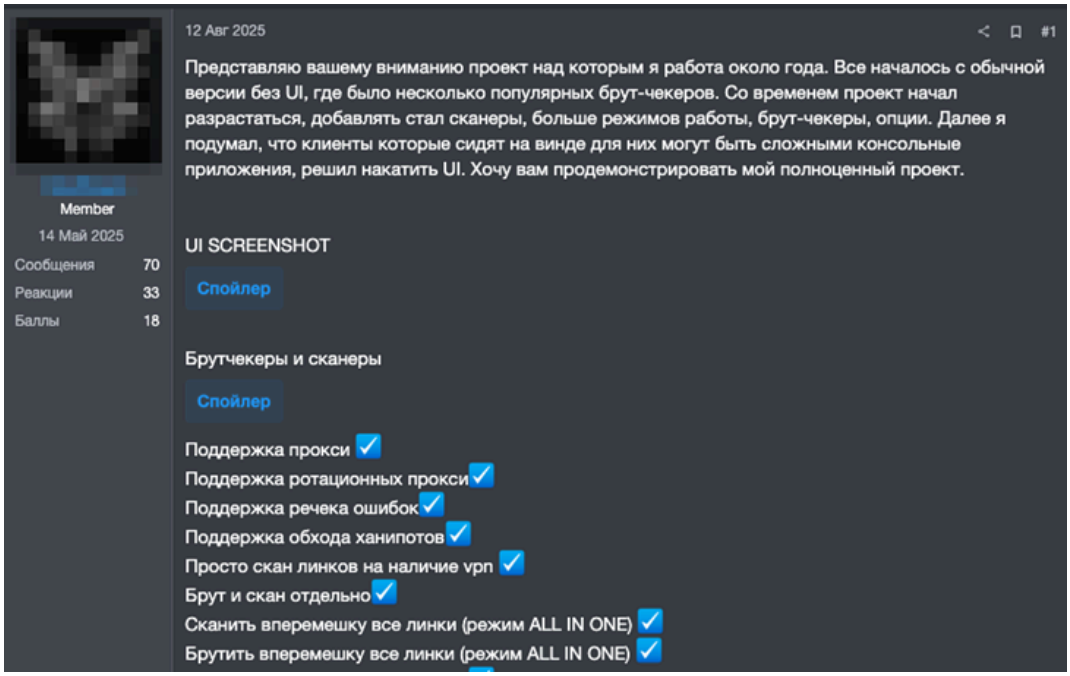
Рисунок 35. Покупка приватных журналов стилера



Полученные данные, как правило, проходят дополнительную обработку с использованием специализированных инструментов для проверки учетных записей. Услуги credential validation as a service включают использование чекеров и брутеров, позволяющих автоматически проверять валидность логинов и паролей, определять доступные учетные записи и извлекать дополнительную информацию о них.

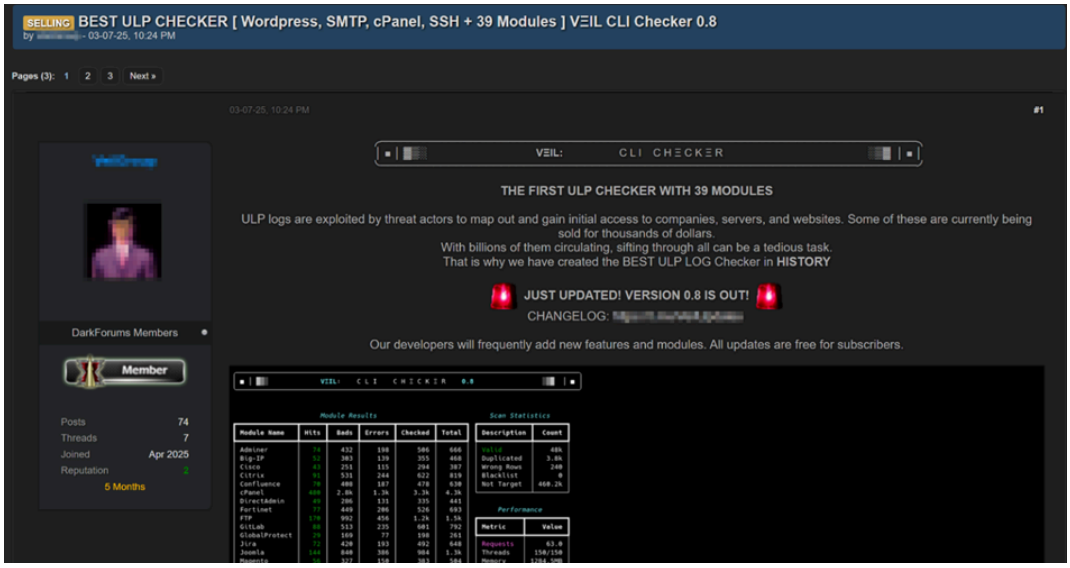
Стоимость таких инструментов при покупке может достигать десятков тысяч долларов. Так, примерно столько стоят специализированные сканеры и брутчекеры корпоративных сервисов.

Рисунок 36. Продажа брутчекера



При этом более распространенной моделью является подписка, стоимость которой обычно находится в диапазоне от 100 до 1000 $ в месяц. Регулярные обновления программного обеспечения позволяют поддерживать актуальность инструментов и повышать их эффективность. Так, стоимость чекера, содержащего 39 модулей и получающего постоянные обновления, составляет 125 $, 200 $, 275 $ за 1, 2, 3 месяца соответственно.

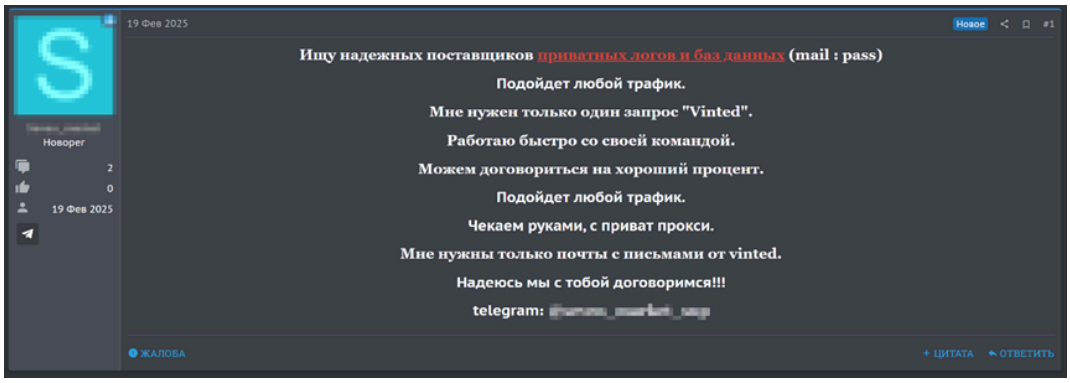
Рисунок 37. Продажа чекера



Совместное использование логов и инструментов проверки формирует автоматизированный пайплайн получения доступа, в котором каждый этап может быть реализован как отдельная услуга. В рамках такого процесса сначала происходит массовый сбор данных, затем их фильтрация и проверка, после чего валидные учетные записи передаются для дальнейшего использования или продажи. Подобная цепочка операций позволяет существенно ускорить проведение атак и минимизировать участие человека.

При этом в условиях широкого распространения автоматизированных инструментов наблюдается парадоксальный рост ценности ручной обработки данных. Автоматизированные системы могут создавать заметный сетевой шум и повышать вероятность обнаружения атак, тогда как аккуратная ручная проверка учетных записей позволяет снизить риск блокировки и продлить срок использования доступа. В результате ручная проверка и эксплуатация учетных записей становятся более дорогими и востребованными, особенно в рамках целевых атак.

Рисунок 38. Покупка приватных логов с ручной их проверкой

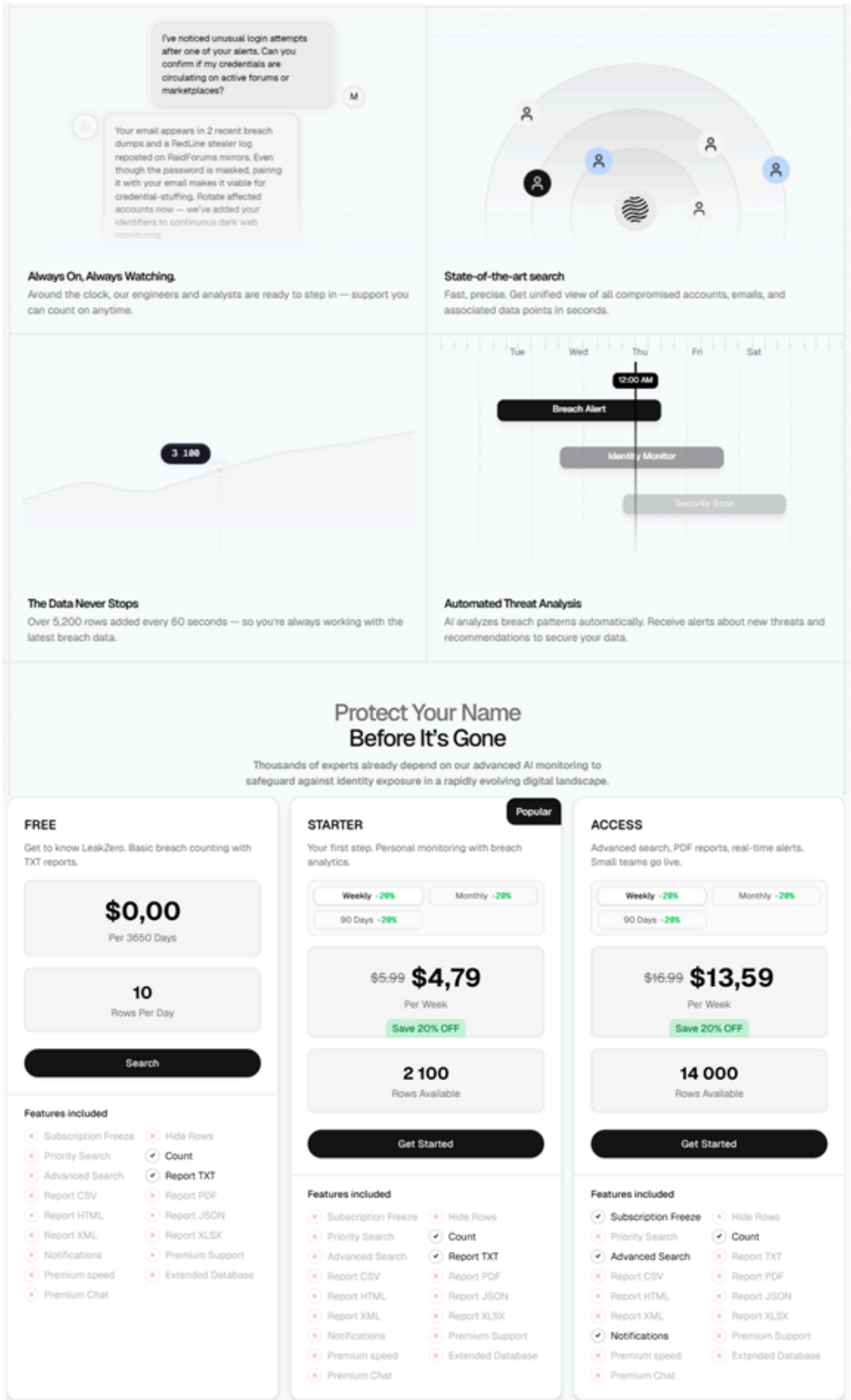


Часто такие услуги предоставляются в формате партнерства, где исполнитель получает процент от прибыли, полученной в результате использования доступа.

Рисунок 39. Предложение о партнерстве с поставщиком журналов

Дополнительным направлением развития этого сегмента становится внедрение технологий искусственного интеллекта в процессы обработки данных. Появляются сервисы, заявляющие об использовании алгоритмов искусственного интеллекта для анализа журналов, поиска релевантных учетных записей и повышения качества предоставляемых данных. При этом стоимость таких решений остается сопоставимой с традиционными, что способствует их быстрому распространению.

Рисунок 40. Магазин продажи логов



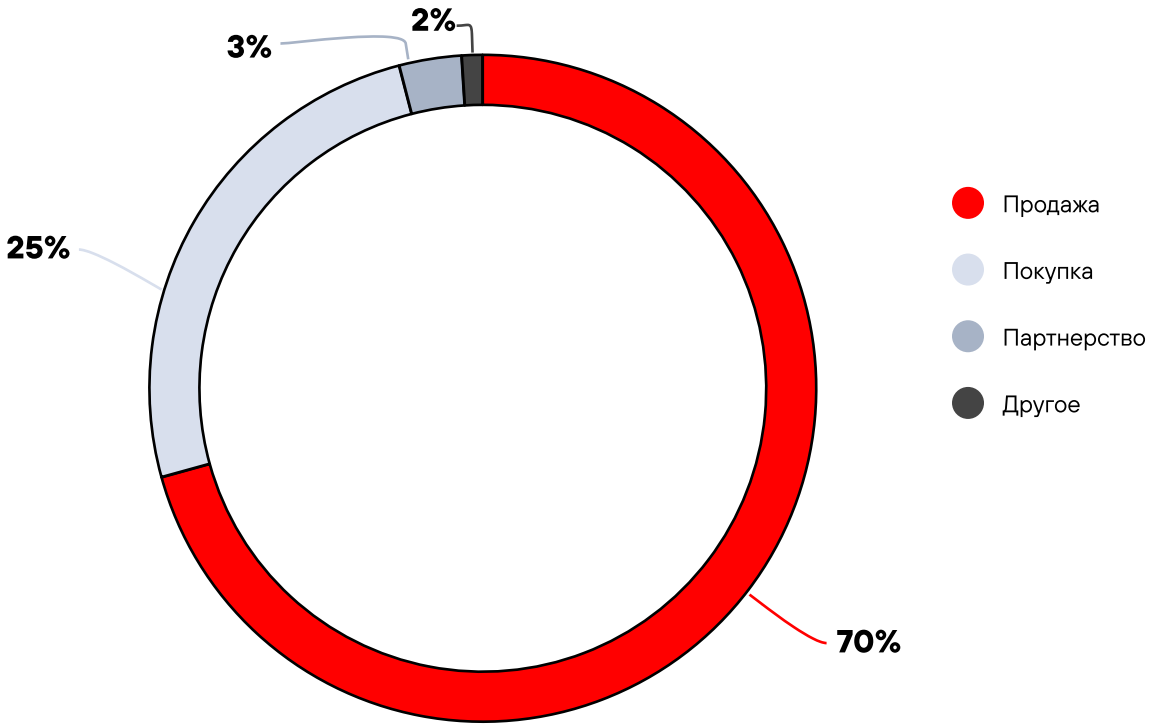
ДОСТУП КАК УСЛУГА (ACCESS AS A SERVICE)

Услуги по продаже доступа к ранее скомпрометированным системам и сетям организаций — самые распространенные на теневом рынке. Им соответствует наибольшая доля объявлений на теневом рынке (61%). Этот сегмент является одним из ключевых элементов экономики киберпреступности, поскольку именно доступ к инфраструктуре организации — самая удобная стартовая точка атаки.

Продажа доступов к корпоративным сетям представляет собой устойчивый и прибыльный бизнес, в котором сформировалась отдельная роль — брокеры первоначального доступа (initial access brokers, IAB). Они специализируются исключительно на получении и последующей продаже доступов, не участвуя непосредственно в реализации атак. Наличие такой роли позволяет вовлекать в рынок менее опытных злоумышленников. Даже если атакующий не способен довести атаку до конца, он может монетизировать полученный доступ, продав его более квалифицированным участникам.

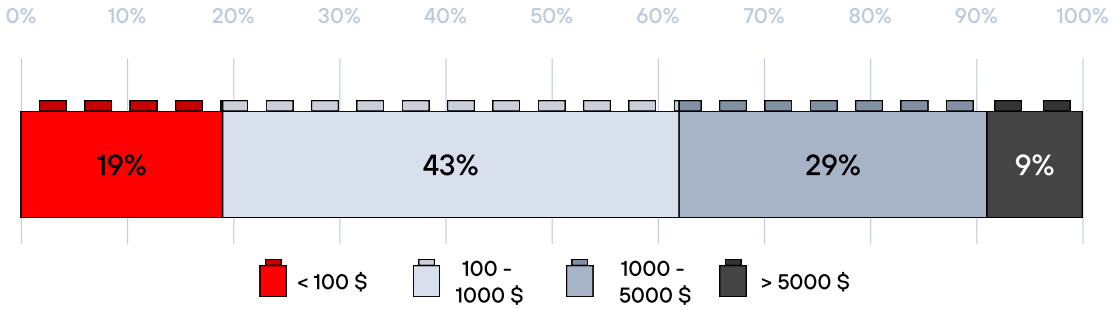
Подавляющее большинство предложений на рынке связано с продажей доступов (70% объявлений по теме доступов). Еще четверть объявлений приходится на поиск доступов для покупки. Несмотря на широкое распространение услуги, доступы в основном продаются разово, часто — одному покупателю. Подписочная модель монетизации практически не встречается на рынке, что объясняется тем, что каждый доступ уникален по своим характеристикам: уровню привилегий, отрасли организации, географии и степени защищенности инфраструктуры. В результате стандартизация услуги и ее перевод в регулярную подписку затруднены, а основными форматами взаимодействия остаются разовые продажи и партнерские соглашения.

Рисунок 41. Типы объявлений по теме доступов



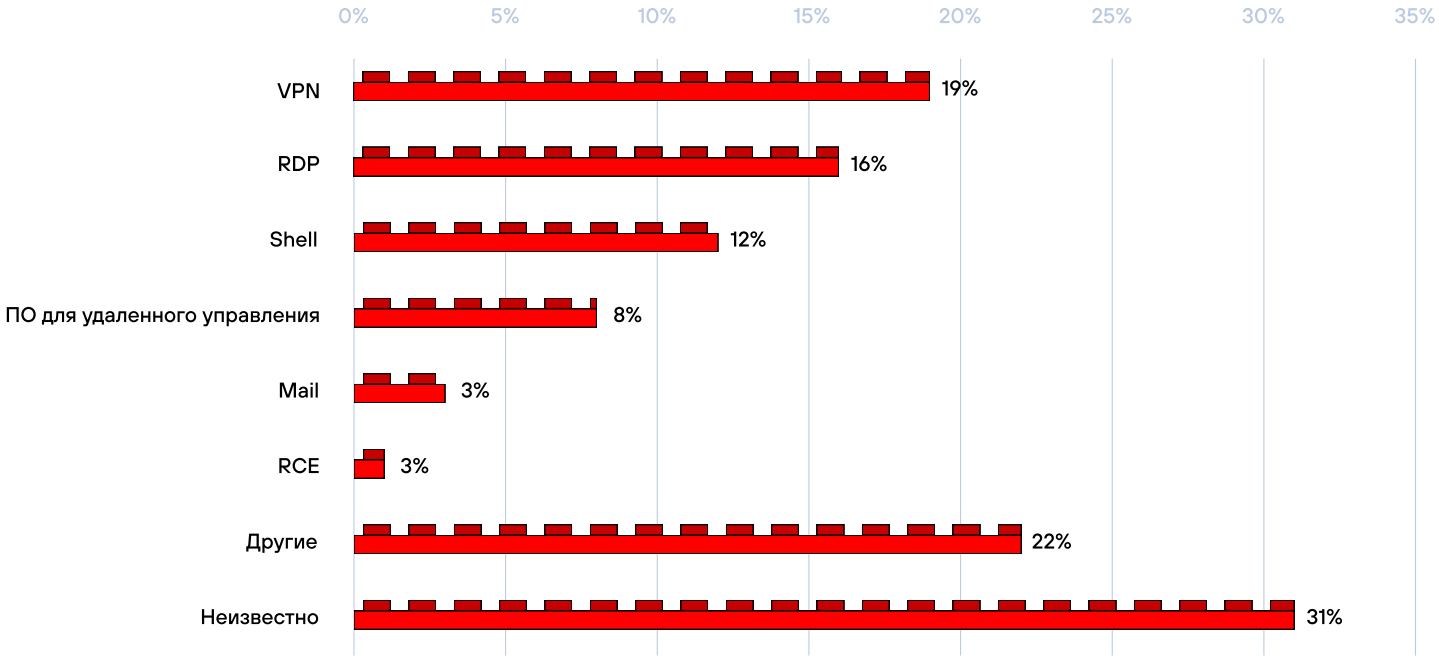
Медианная стоимость доступа составляет 600 $, однако фактический диапазон цен значительно варьируется. Наиболее распространенная категория — доступы стоимостью от 100 до 1000 $, что делает их доступными для широкого круга злоумышленников. Более дорогие предложения связаны с доступами высокого уровня, крупными организациями или наличием административных прав, тогда как дешевые варианты обычно предполагают ограниченные привилегии или меньшую ценность инфраструктуры.

Рисунок 42. Распределение цен на доступы



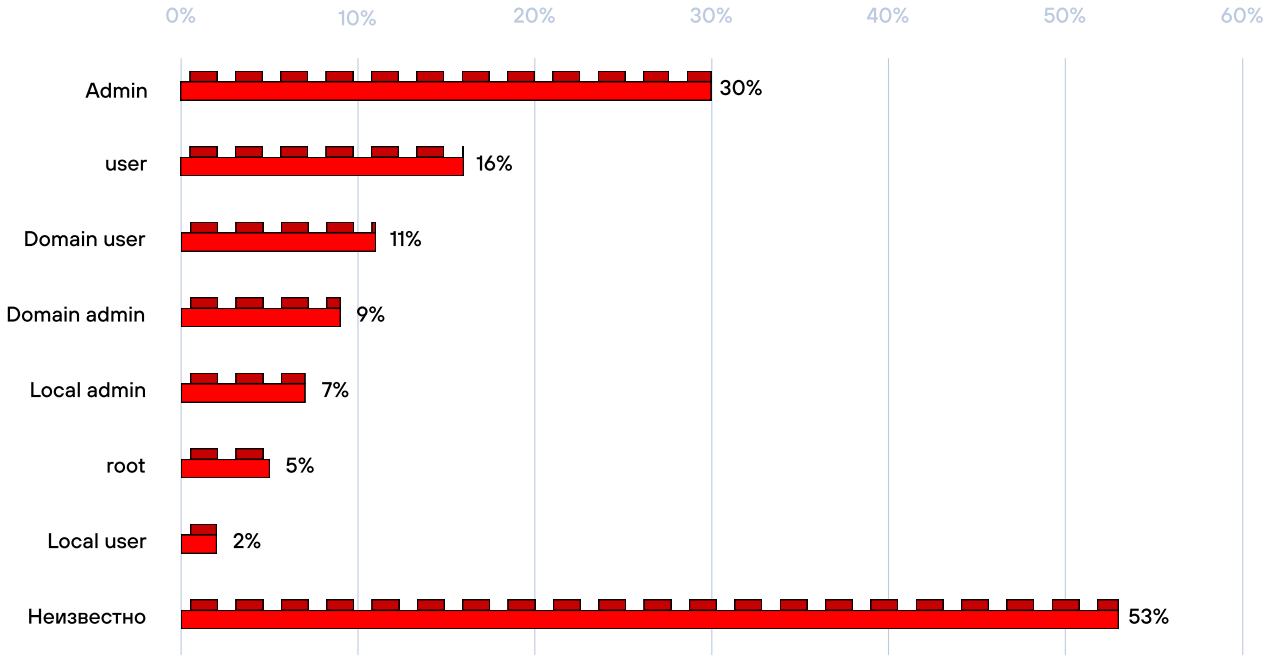
Наиболее распространенные типы доступов — VPN (19%) и RDP (16%), за которыми следуют доступы к командным оболочкам Shell (12%) и различному ПО для удаленного управления (8%).

Рисунок 43. Типы доступа



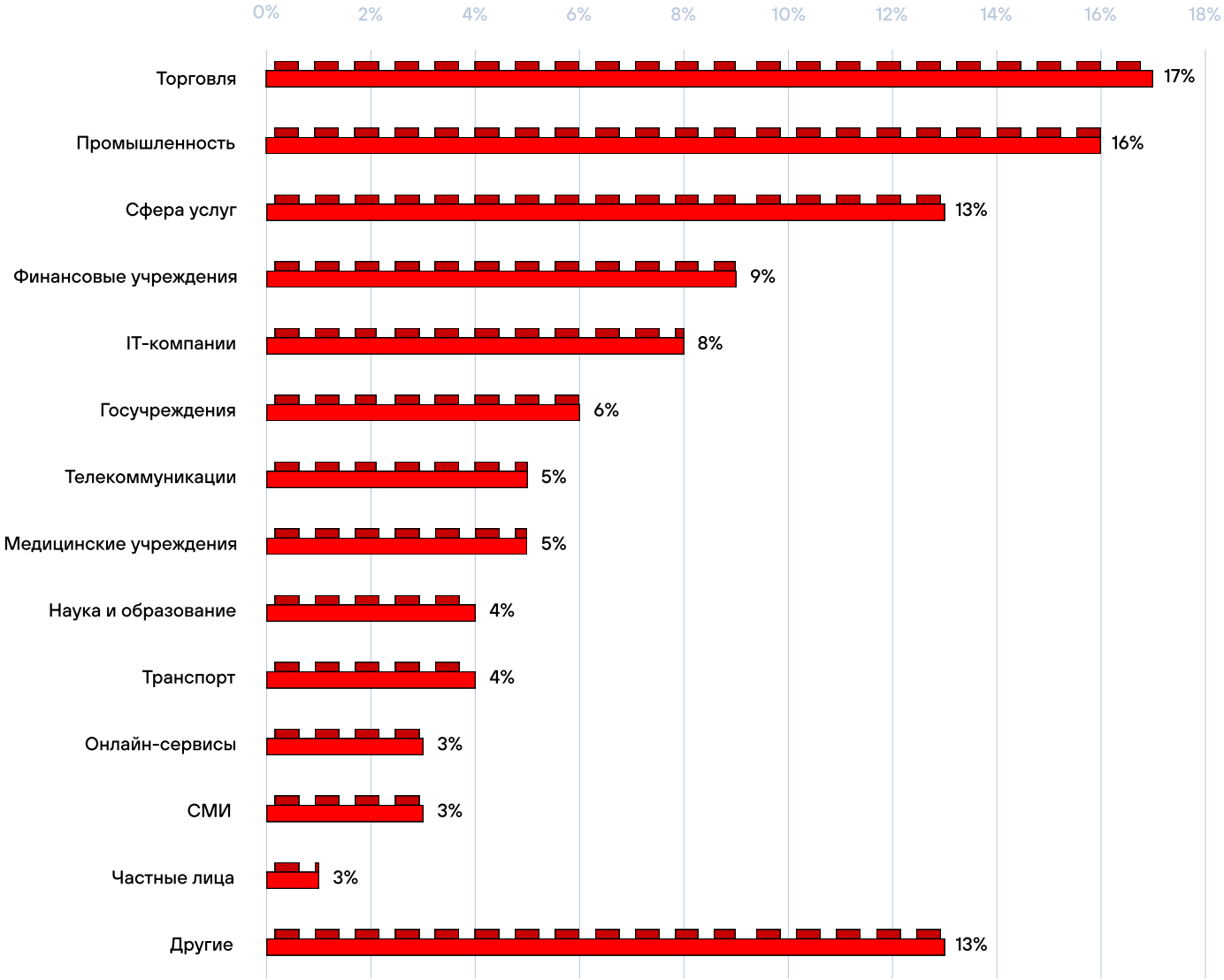
Важным фактором, влияющим на стоимость и привлекательность доступа, является уровень привилегий: значительная часть предложений связана с административными правами (30%).

Рисунок 44. Права в объявлениях с доступами



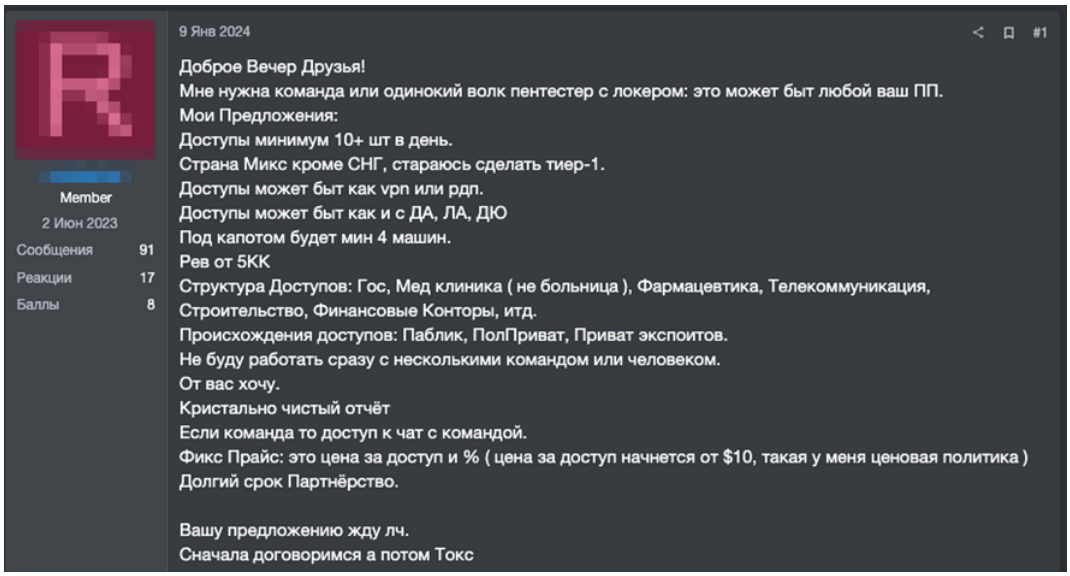
Наиболее часто в объявлениях фигурируют организации из сфер торговли (17%), промышленности (16%) и услуг (13%), что отражает их широкое присутствие на рынке и потенциальную финансовую ценность. При этом доступы к финансовым учреждениям (9%) и государственным организациям (6%) могут стоить значительно дороже из-за повышенного уровня чувствительности данных и возможных последствий компрометации.

Рисунок 45. Объявления о доступах по отраслям



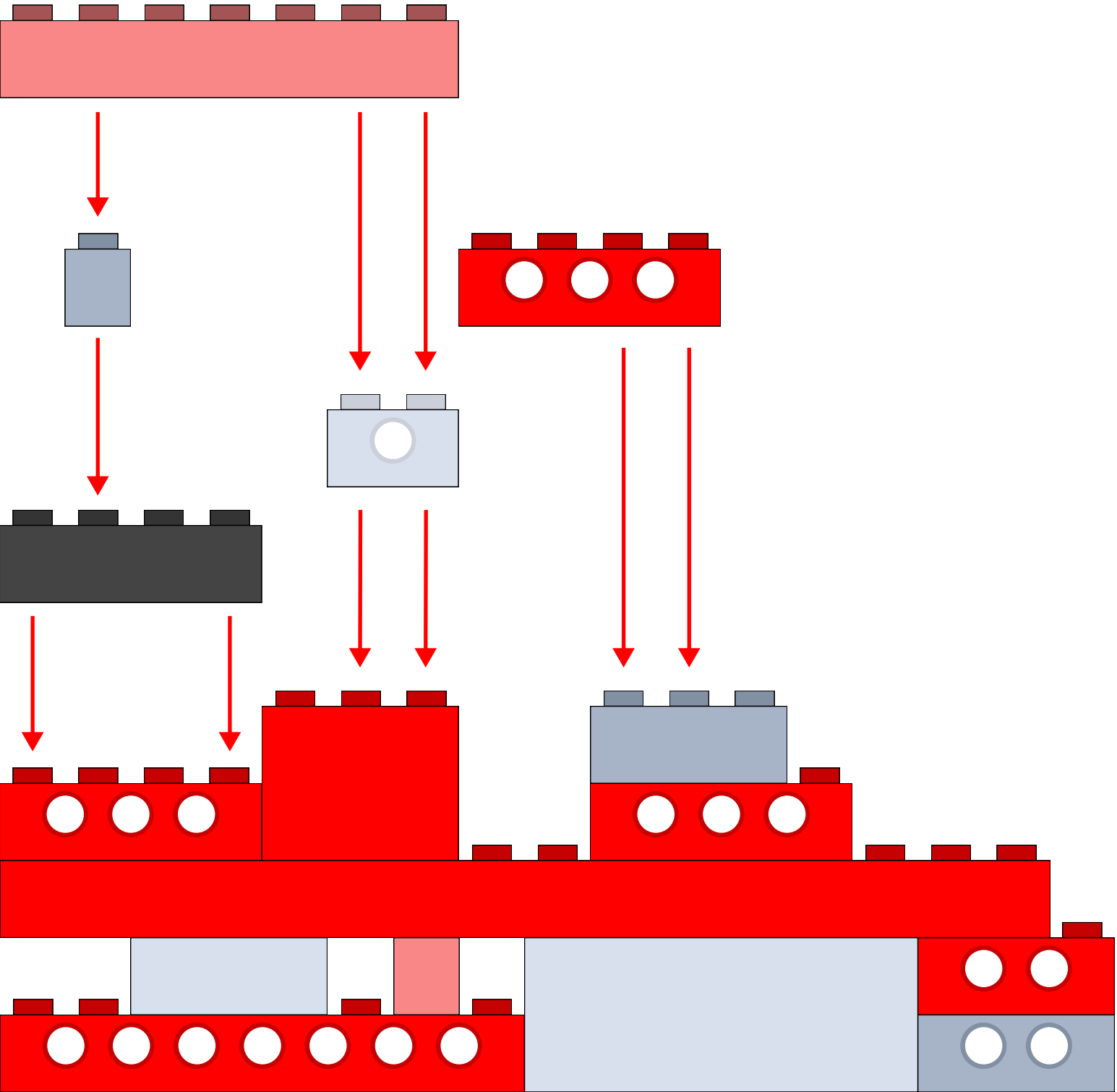
Помимо разовых продаж доступов, распространена партнерская модель взаимодействия, при которой поставщик доступа получает процент от прибыли, полученной в результате дальнейшей эксплуатации системы. Такой формат часто оказывается выгоднее фиксированной оплаты, поскольку качество доступа может существенно различаться, а фактическая ценность становится понятна только после его проверки, использования и получения прибыли. Партнерство также снижает риски для покупателя, поскольку оплата производится после получения финансового результата.

Рисунок 46. Покупка услуги по предоставлению доступов



В перспективе данный сегмент, вероятно, сохранит существующую модель развития. В отличие от других направлений CaaS, где возможно масштабирование за счет автоматизации и стандартизации услуг, рынок доступов основан на уникальности каждого отдельного доступа и высокой зависимости от конкретных условий компрометации. По этой причине наиболее вероятным сценарием остается дальнейшее доминирование разовых продаж и партнерских соглашений, тогда как полноценная подписочная модель, скорее всего, будет оставаться исключением, а не массовой практикой.

ОБХОД ЗАЩИТЫ



ОБХОД ЗАЩИТЫ КАК УСЛУГА (DEFENCE EVASION AS A SERVICE)

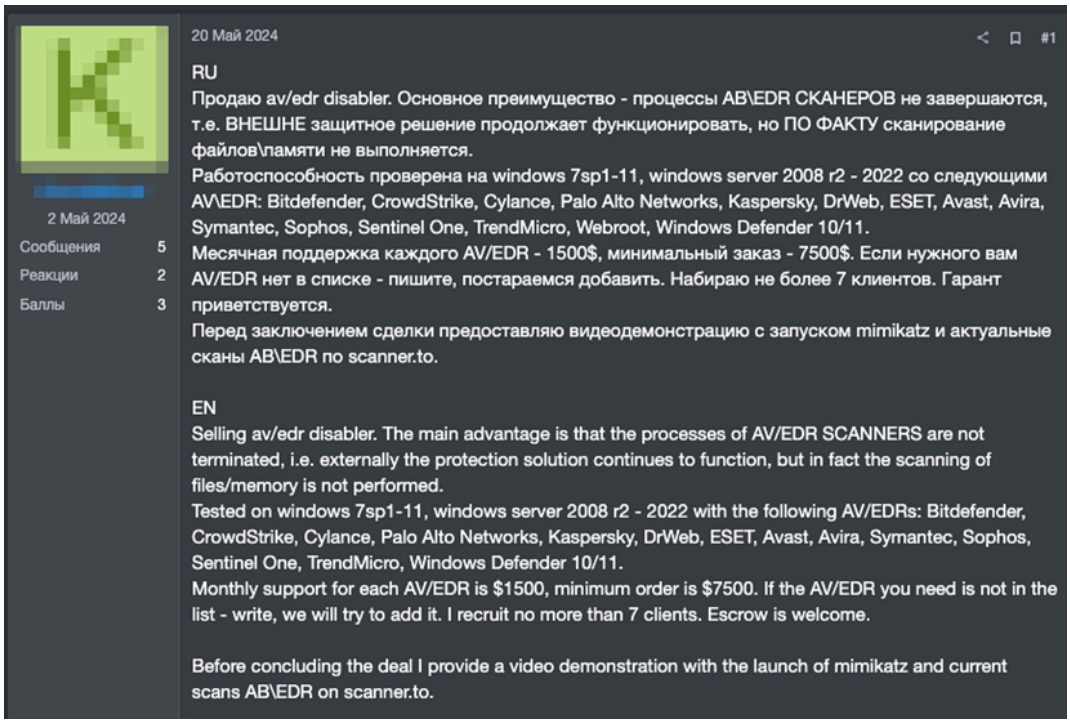
Услуги по предоставлению инструментов и методов, позволяющих обходить средства информационной безопасности и скрывать вредоносную активность в инфраструктуре организации, — это рынок на стадии активного формирования. Он демонстрирует признаки быстрого роста, обусловленного распространением современных систем защиты. В рамках таких услуг злоумышленникам предлагаются решения, предназначенные для отключения или обхода антивирусных продуктов, систем EDR (XDR) и других средств обнаружения угроз, а также инструменты для маскировки действий внутри скомпрометированной сети.

Наиболее распространенной категорией инструментов в этом сегменте являются так называемые EDR-киллеры — специализированные решения, предназначенные для нейтрализации механизмов защиты конечных точек. Их популярность напрямую связана с массовым внедрением систем обнаружения и реагирования на угрозы, которые значительно усложнили проведение атак традиционными методами. Дополнительный фактор роста популярности подобных инструментов — их активное использование в атаках вымогателей. По данным ESET, более 90 EDR-киллеров используются в таких атаках.

Техническая сложность подобных инструментов существенно выше по сравнению со многими другими категориями услуг. Для их разработки требуется глубокое понимание принципов работы защитных систем, механизмов обнаружения угроз и особенностей операционных систем. В результате стоимость таких решений остается относительно высокой: цена на инструменты начинается примерно от 500 $ и может достигать 9000 $ при медианной стоимости 2250 $. Стоимость конкретного решения зависит от ряда факторов, включая поддерживаемые операционные системы, перечень совместимых продуктов безопасности и используемые методы обхода защитных механизмов. Инструменты различаются по способам воздействия на системы защиты и уровню универсальности. Чем шире спектр поддерживаемых платформ и отключаемых средств защиты, тем выше стоимость и востребованность инструмента.

Модель распространения таких инструментов включает как разовые продажи готовых решений, так и предложения по подписке. В рамках подписки разработчики предоставляют обновления, поддержку и могут дорабатывать инструмент под конкретные требования заказчика, например добавить обход определенных средств защиты. Такой формат особенно востребован, поскольку системы безопасности постоянно обновляются, и инструмент должен регулярно адаптироваться, чтобы сохранять свою эффективность и оставаться незамеченным.

Рисунок 47. Объявление о продаже инструмента для обхода антивируса и EDR

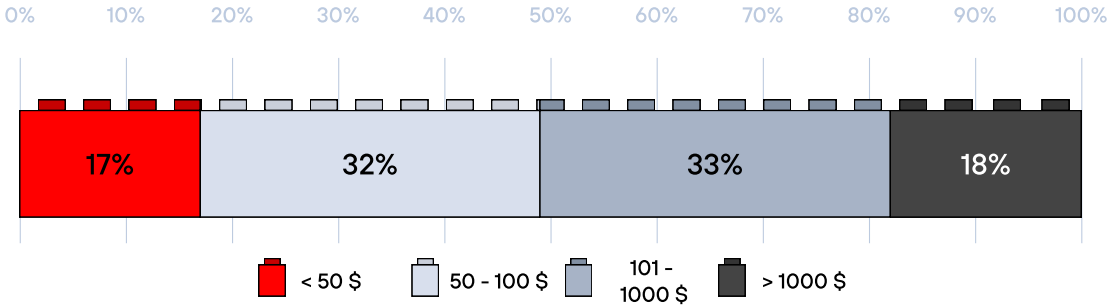


ШИФРОВАНИЕ КАК УСЛУГА (CRYPTING AS A SERVICE)

Crypting as a service представляет собой услугу по модификации и обфускации ВПО с целью обхода обнаружения средствами защиты. Обычно такие услуги включают использование крипторов и пакеров, изменяющих структуру и сигнатуры вредоносного кода, что позволяет снизить вероятность его обнаружения антивирусными решениями и системами мониторинга безопасности.

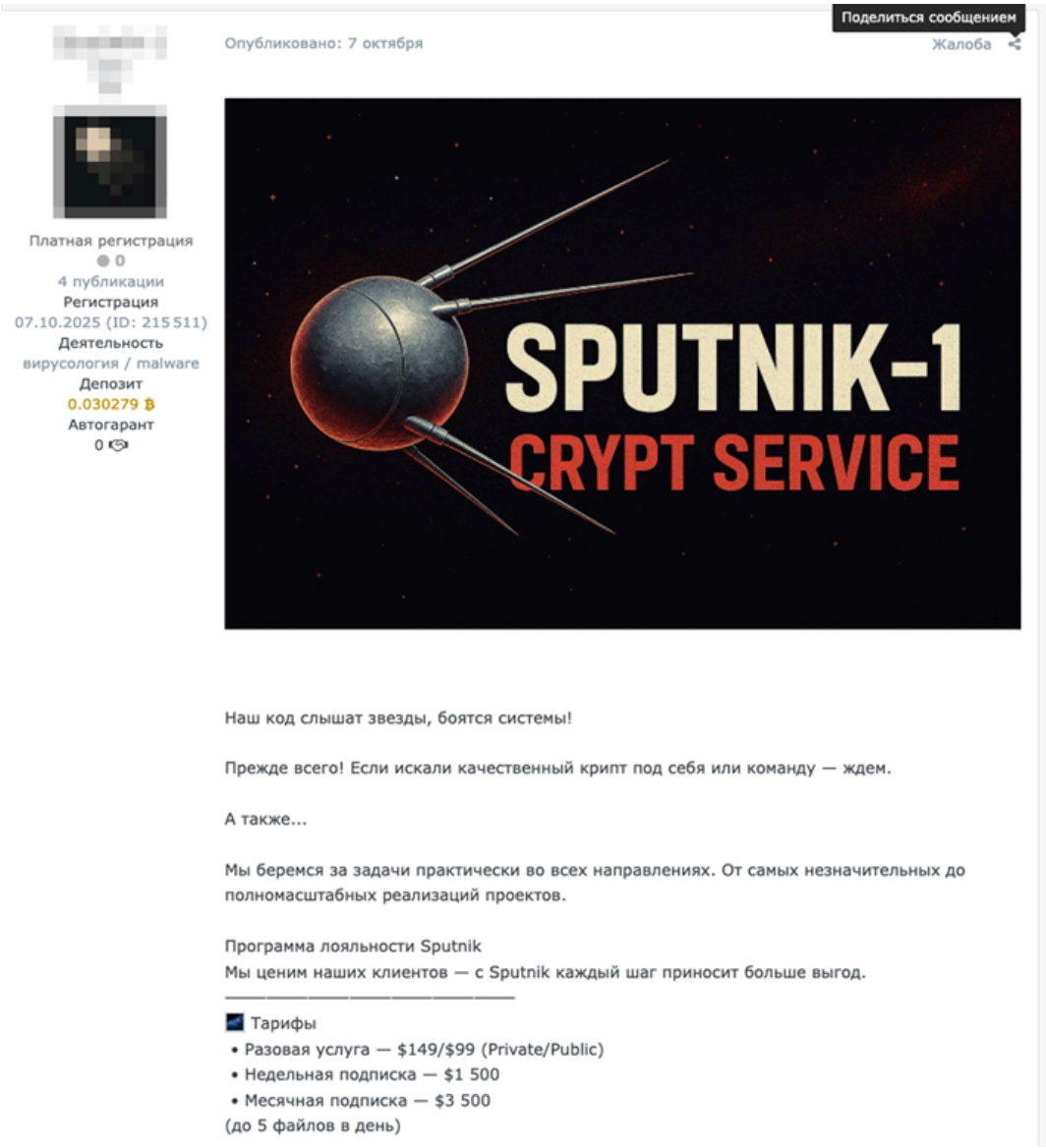
Медианная стоимость таких услуг составляет 150 $. Наиболее низкие цены обычно устанавливаются за криптование одного файла и, как правило, не превышают 500 $. Автоматизированные инструменты предлагаются по более доступным тарифам, тогда как приватное криптование с гарантией обхода средств защиты может стоить значительно дороже.

Рисунок 48. Объявление о продаже инструмента для обхода антивируса и EDR



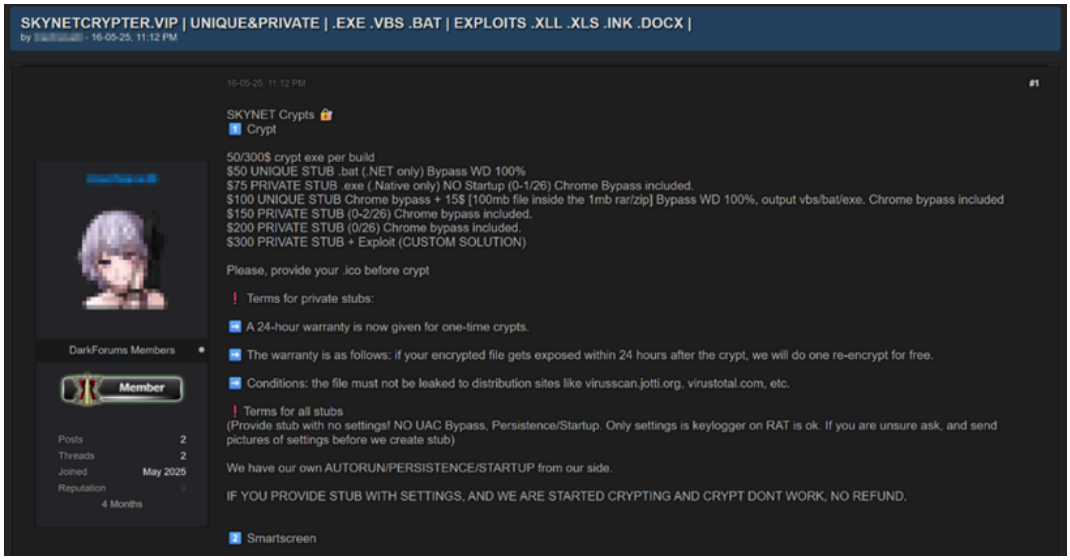
Инструменты, распространяемые по подписочной модели, как правило, стоят существенно дороже — от 1000 до 5000 $. В стоимость подписки обычно входят обновления алгоритмов обфускации, техническая поддержка и регулярное изменение сигнатур, что позволяет поддерживать эффективность инструмента в условиях постоянного обновления средств защиты.

Рисунок 49. Объявление о продаже инструмента для обхода антивируса и EDR



Особую ценность на рынке представляют приватные крипторы. Такие решения используются ограниченным числом клиентов и поэтому реже попадают в базы сигнатур средств защиты. Это создает для продавцов определенный баланс между доходом и риском обнаружения: чем больше клиентов используют один и тот же инструмент, тем выше вероятность его выявления системами безопасности. По этой причине разработчики нередко предпочитают продавать доступ к своим решениям ограниченному числу клиентов по более высокой цене, а не распространять их массово.

Рисунок 50. Объявление о продаже услуг криптора

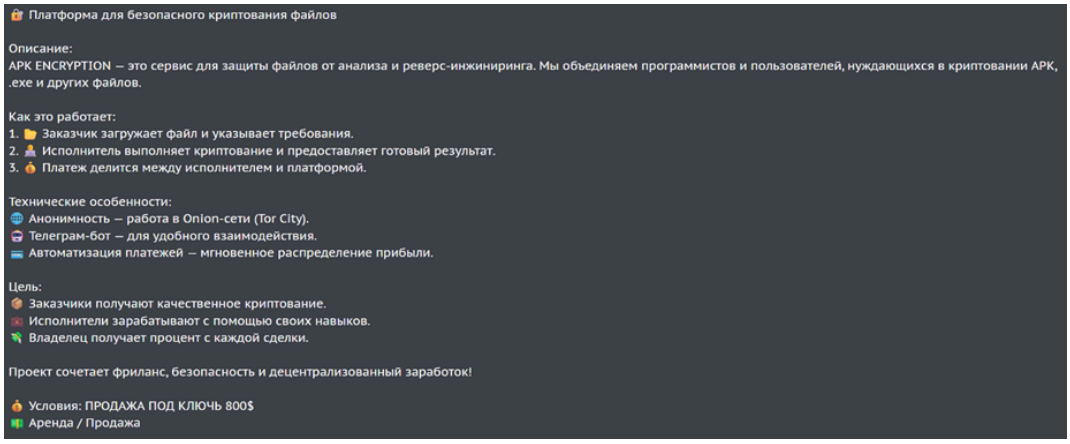


В данном сегменте по-прежнему высоко ценится ручная работа. Индивидуальные услуги криптования могут включать не только базовую обфускацию, но и комплексные методы обхода различных механизмов обнаружения, включая сигнатурный, эвристический и поведенческий анализ. В ряде случаев оплата осуществляется после проверки заказчиком результата.

Рисунок 51. Предложение услуг приватного криптования

В данном сегменте по-прежнему высоко ценится ручная работа. Индивидуальные услуги криптования могут включать не только базовую обфускацию, но и комплексные методы обхода различных механизмов обнаружения, включая сигнатурный, эвристический и поведенческий анализ. В ряде случаев оплата осуществляется после проверки заказчиком результата.

Рисунок 52. Продажа платформы для заработка на криптовании файлов



В целом рынок услуг криптования демонстрирует признаки зрелой конкуренции. Автоматизированные инструменты стремятся повысить качество и удобство использования, предлагая регулярные обновления и дополнительные функции, тогда как индивидуальные исполнители делают акцент на персонализированном подходе и гарантированном результате. В дальнейшем можно ожидать, что отдельные этапы работы специалистов будут автоматизированы и появятся более продвинутые инструменты, ориентированные на обход новых механизмов защиты и повышение устойчивости ВПО к обнаружению.

ПОДПИСАНИЕ КОДА КАК УСЛУГА (CODE SIGNING AS A SERVICE)

На теневом рынке набирают популярность услуги по предоставлению цифровых сертификатов (например, code signing или EV-сертификатов), позволяющих подписывать программное обеспечение и тем самым повышать уровень доверия со стороны операционных систем и средств защиты. Использование таких сертификатов позволяет снизить вероятность появления предупреждений для пользователя (например, от встроенных механизмов защиты операционных систем) и повысить шансы успешного запуска вредоноса в целевой среде.

Основной способ монетизации в этом сегменте на текущий момент — разовая продажа сертификатов. Медианная стоимость одного сертификата составляет 2150 $ — этот относительно дорогой инструмент используют преимущественно более организованные злоумышленники или группировки, проводящие целевые атаки.

Рисунок 53. Предложение услуги выпуска EV-сертификатов

[redacted]

Платная регистрация
0
1 публикация
Регистрация
26.09.2025 (ID: 214 353)
Деятельность
другое / other
Депозит
0.002384 ฿
Автогарант
0

Опубликовано: 28 сентября

Жалоба

EV CODESIGNING CERTIFICATES Various CAs

(RU)

Сертификаты EV в наличии и по предзаказу

Сертификаты по предварительному заказу: срок изготовления 2-5 дней
Обсуждение оптовых заказов
Сертификаты продаются строго в одни руки, свежие и не использованные
Полная передача всех данных от сертификата

Что такое EV Code Signing?

1.Обход Microsoft SmartScreen
2.Позволяет игнорировать красные и желтые предупреждения UAC
3.Программное обеспечение вызывает больше доверия у пользователей
4.Обход некоторых антивирусов, основанных на обнаружении сигнатур
5.Обход аллертов выдачи браузеров Edge/Chrome

Варианты доставки

1. Предоставляем удаленный доступ 24/7
2. Можете использовать свой собственный аппаратный токен для установки сертификата - SafeNet eToken 5110 CC, Rutoken 3.0
3. Облачные сертификаты не требуют дополнительных настроек

FAQ

Сертификаты действительны в течение 1 года
Есть в наличии, предварительно свяжитесь с нами
Сертификаты не спасут вас от необходимости шифровать ваши файлы
Сертификат может быть отозван, если центр сертификации получит много жалоб на злоупотребление, для белого софта можно использовать в течение всего периода

Цена

1.GlobalSign $4,000(в наличие) Предзаказ $3,000
2.Certum $3,000(в наличие) Предзаказ $2,000
3.SSL $3,000(в наличие) Предзаказ $2,000
4.Sectigo $3,000 (в наличие) Предзаказ $2,000

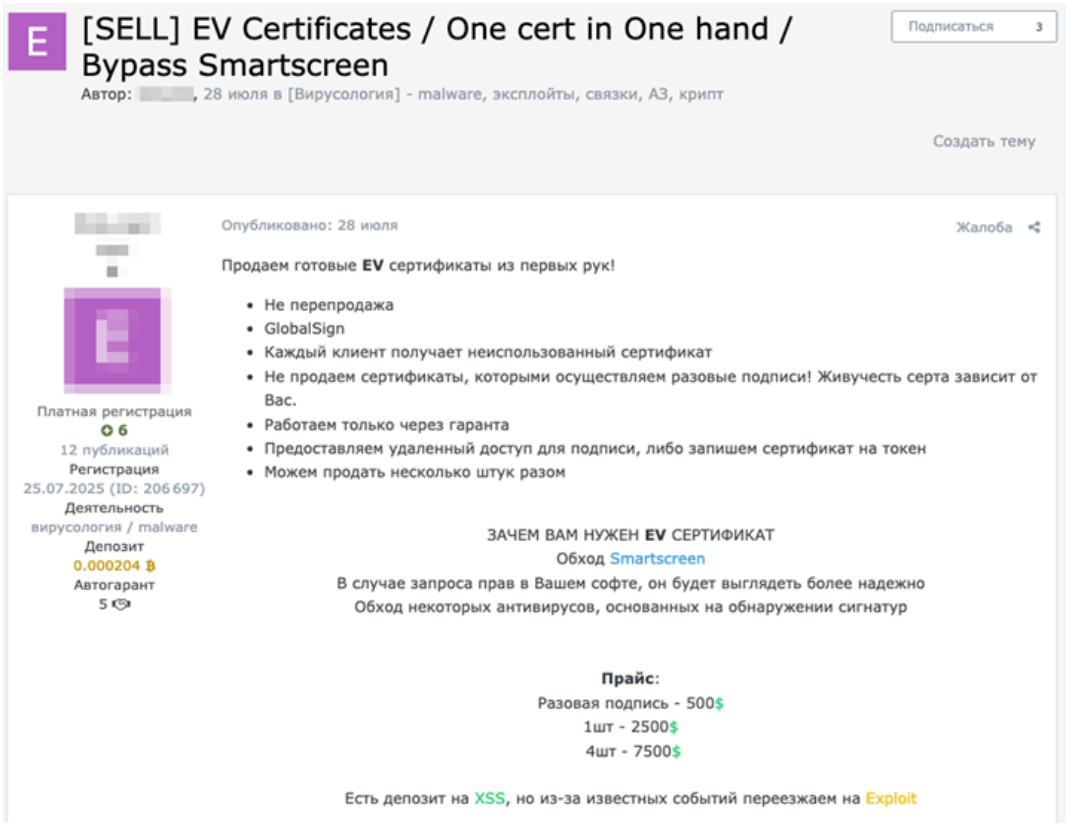
В этой категории отсутствуют существенные технические ограничения для перехода к сервисной модели распространения. Подписочная модель может быть востребована злоумышленниками, которым необходимо регулярно выпускать и подписывать новые версии вредоносного программного обеспечения, особенно в рамках массовых кампаний или при использовании быстро модифицируемых штаммов вредоносного кода.

В настоящее время высокая стоимость отдельных сертификатов ограничивает их применение в масштабных атаках. Однако в случае появления автоматизированных сервисов выпуска и управления сертификатами можно ожидать снижения стоимости таких услуг и их адаптации под массовое использование.

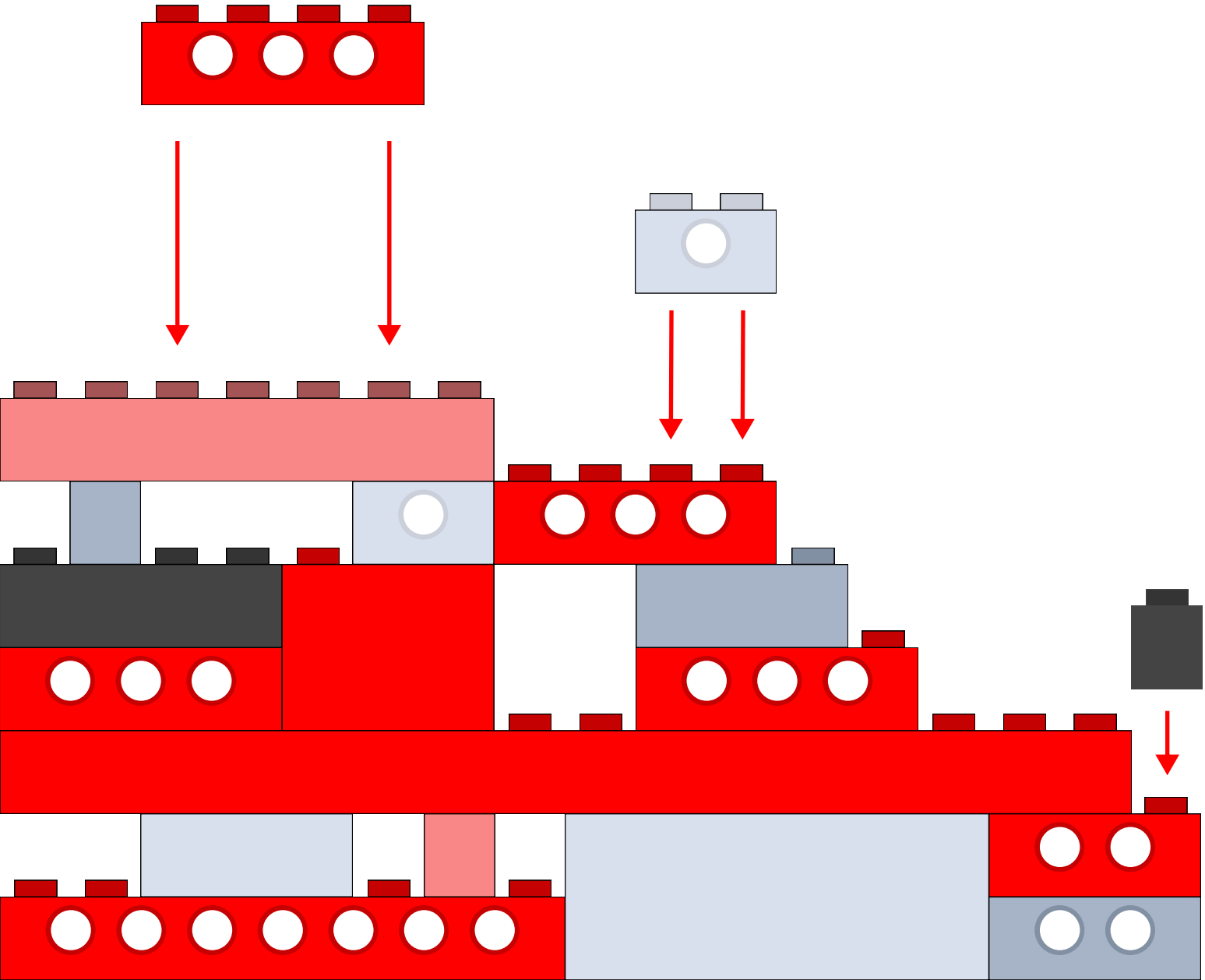
Дополнительный фактор, способствующий развитию сервисной модели, — ограниченный срок действия цифровых сертификатов. По истечении срока действия сертификат становится недействительным, что требует его замены. В рамках подписочной модели поставщик услуги может автоматически предоставлять новые сертификаты взамен истекших, обеспечивая непрерывность использования инструмента без необходимости повторного поиска и покупки нового сертификата.

Уже сейчас наблюдаются предпосылки к формированию такого формата услуг. В частности, фиксируются объявления, в которых сертификаты предлагаются не по одному, а пакетами, включающими несколько экземпляров, — то есть от разовых сделок злоумышленники переходят к более системному подходу.

Рисунок 54. Объявление о продаже EV-сертификатов



РЕАЛИЗАЦИЯ АТАКИ



ВЫМОГАТЕЛИ КАК УСЛУГА (RANSOMWARE AS A SERVICE)

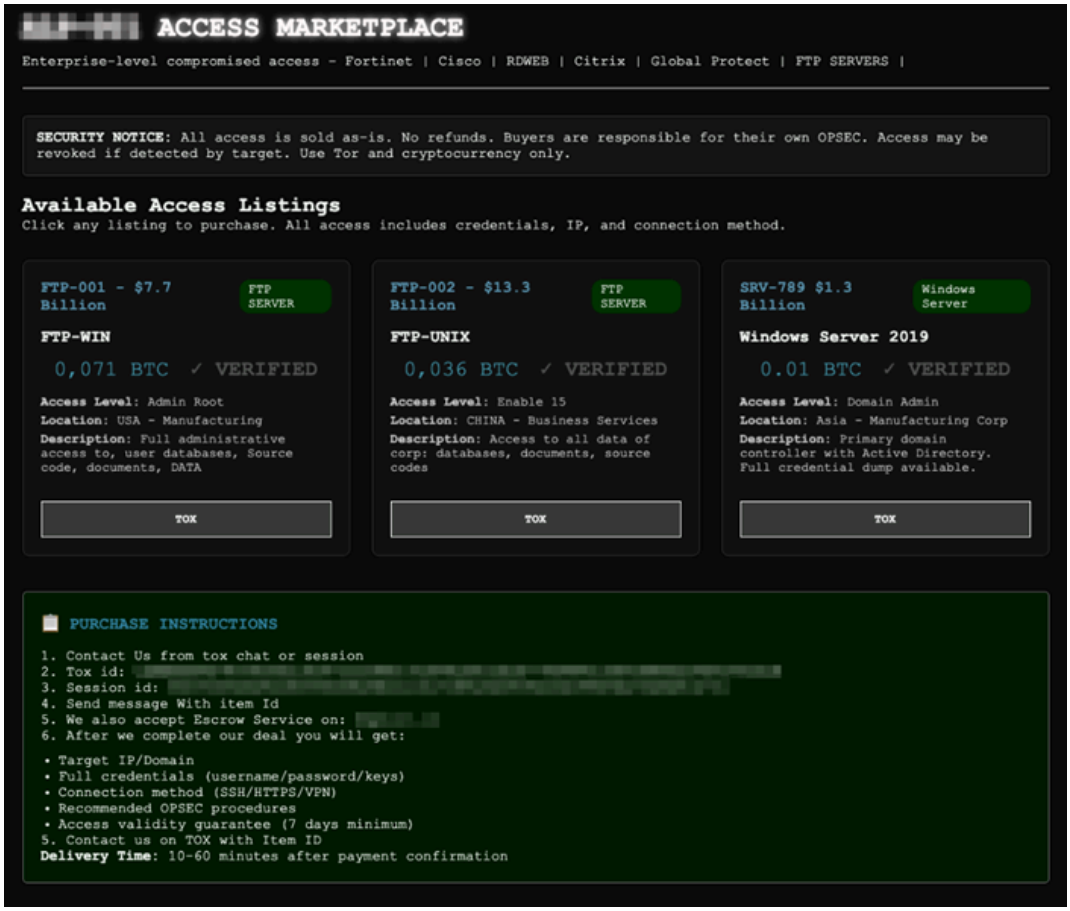
Программы-вымогатели как услуга (ransomware as a service, RaaS) — это бизнес-модель киберпреступности, при которой разработчики вымогательского ВПО создают и поддерживают инфраструктуру, а аффилированные лица (партнеры) используют эти инструменты для проведения атак. В рамках данной модели аффилиатам не требуется иметь глубокие технические навыки — они используют готовые инструменты и инфраструктуру операторов.

Аффилиаты могут выбирать различные модели взаимодействия с операторами: ежемесячные подписки, партнерские программы, единовременные лицензионные платежи или участие в прибыли. Наиболее распространенными моделями монетизации являются:

- фиксированная ежемесячная плата за использование инфраструктуры и вредоносного ПО;
- процент от полученного выкупа;
- единовременный платеж за использование конкретного штамма вымогателя;
- совместная работа операторов и партнеров с разделением прибыли на всех этапах атаки.

Модель RaaS часто интегрируется с другими сегментами киберпреступного рынка. Например, брокеры первоначального доступа предоставляют доступ к корпоративным сетям, который затем используется аффилированными лицами для развертывания программ-вымогателей. В отдельных случаях наоборот, вымогатели сами продают полученные ими доступы для получения двойной выгоды.

Рисунок 55. Магазин доступов на сайте вымогателей



Со временем структура таких операций становится все более специализированной. Одни участники сосредоточены на разработке вредоносного программного обеспечения, другие — на получении первоначального доступа, третьи — на проведении атак и переговорах с жертвами.

Еще одной характерной особенностью атак вымогателей является использование моделей двойного и тройного вымогательства. Двойное вымогательство предполагает одновременное шифрование данных и их кражу с последующей угрозой публикации. Тройное вымогательство включает дополнительные методы давления на жертву, например угрозы вторичных атак, уведомление клиентов или партнеров организации, а также попытки вымогательства средств напрямую у пострадавших лиц. Сегодня мы наблюдаем случаи не только с тройным вымогательством, но и с четверным. Однако наиболее распространенной остается модель двойного вымогательства: организации все чаще отказываются платить выкуп, но часть жертв по-прежнему готова идти на переговоры.

По нашим данным, в 2025 году в половине случаев заражений вредоносным ПО на организации использовались шифровальщики. Причем, доля их использований выросла на 8 п. п. по сравнению с 2024 годом, что напрямую связано с развитием RaaS. При этом шифровальщики применяются не только преступными группировками с финансовой мотивацией, но и хактивистскими объединениями.

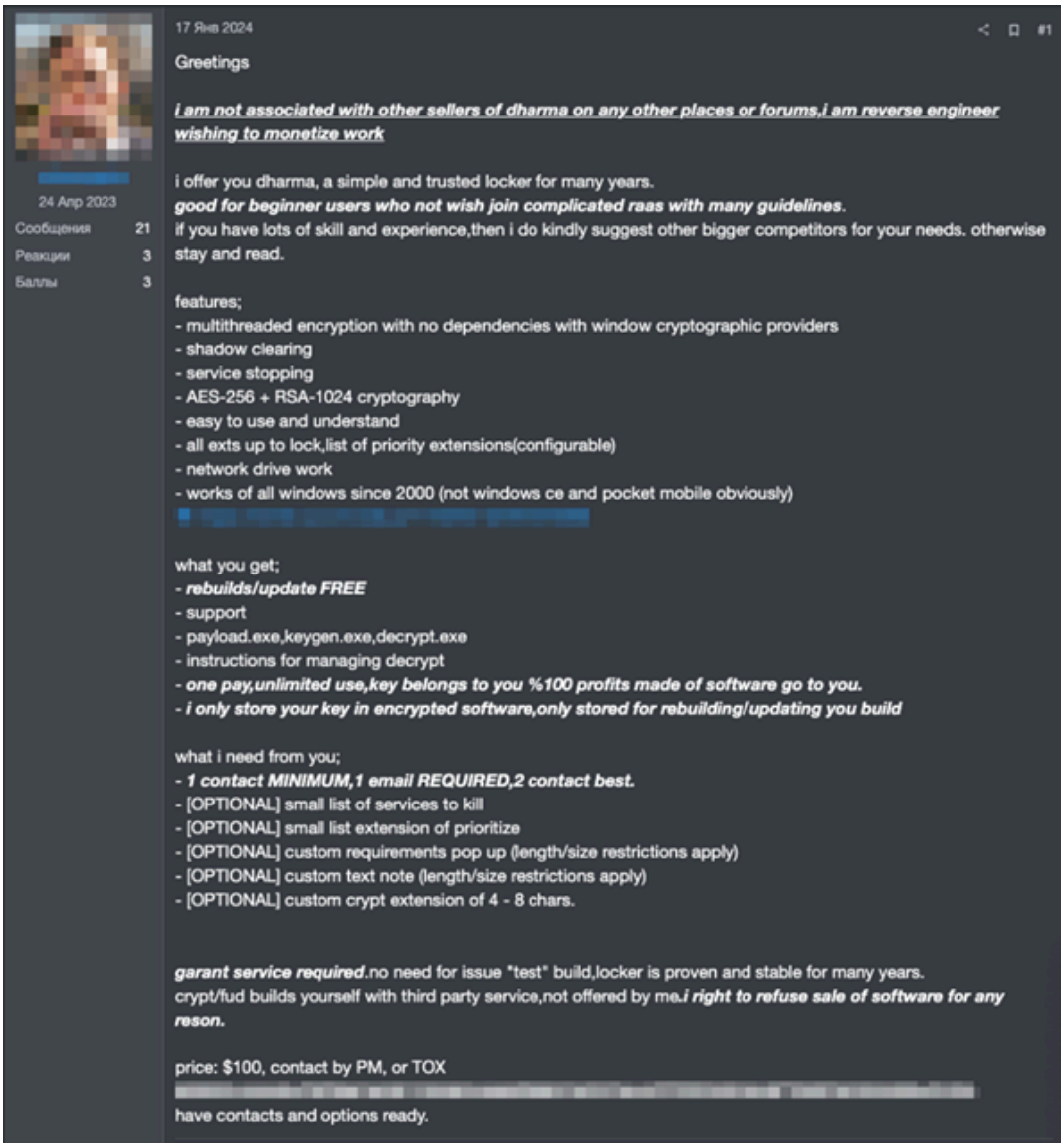
По данным ресурса ransomware.live в мире действует более 300 уникальных групп вымогателей, в 2026 году жертвами атак вымогателей стали более 2 тысяч организаций. Группировки Qilin, The Gentlemen, Akira, Clop — лидеры по количеству атак. Эти операторы постоянно развиваются и создают новые версии программ-вымогателей, чтобы максимизировать свое влияние.

Существует несколько ключевых причин, по которым злоумышленники активно используют модель RaaS:

- Разделение труда позволяет запускать больше атак одновременно.
- Использование готовых инструментов снижает порог входа для менее опытных злоумышленников.
- Некоторые организации продолжают выплачивать выкуп, особенно при угрозе простоя бизнеса.
- Похищенные данные могут быть монетизированы даже без оплаты выкупа.
- Распределенная структура операций повышает устойчивость к действиям правоохранительных органов.

Стоимость инструментов в рамках этой модели варьируется в широком диапазоне. Например, исходный код простых программ-вымогателей может продаваться по цене от 100 $.

Рисунок 56. Объявление о продаже шифровальщика



24 Апр 2023
Сообщения 21
Реакции 3
Баллы 3

17 Янв 2024 #1

Greetings

i am not associated with other sellers of dharma on any other places or forums,i am reverse engineer wishing to monetize work

i offer you dharma, a simple and trusted locker for many years.
good for beginner users who not wish join complicated raas with many guidelines.
if you have lots of skill and experience,then i do kindly suggest other bigger competitors for your needs. otherwise stay and read.

features;
- multithreaded encryption with no dependencies with window cryptographic providers
- shadow clearing
- service stopping
- AES-256 + RSA-1024 cryptography
- easy to use and understand
- all exts up to lock,list of priority extensions(configurable)
- network drive work
- works of all windows since 2000 (not windows ce and pocket mobile obviously)

what you get;
- ***rebuilds/update FREE***
- support
- payload.exe,keygen.exe,decrypt.exe
- instructions for managing decrypt
- ***one pay,unlimited use,key belongs to you %100 profits made of software go to you.***
- ***i only store your key in encrypted software,only stored for rebuilding/updating you build***

what i need from you;
- ***1 contact MINIMUM,1 email REQUIRED,2 contact best.***
- [OPTIONAL] small list of services to kill
- [OPTIONAL] small list extension of prioritize
- [OPTIONAL] custom requirements pop up (length/size restrictions apply)
- [OPTIONAL] custom text note (length/size restrictions apply)
- [OPTIONAL] custom crypt extension of 4 - 8 chars.

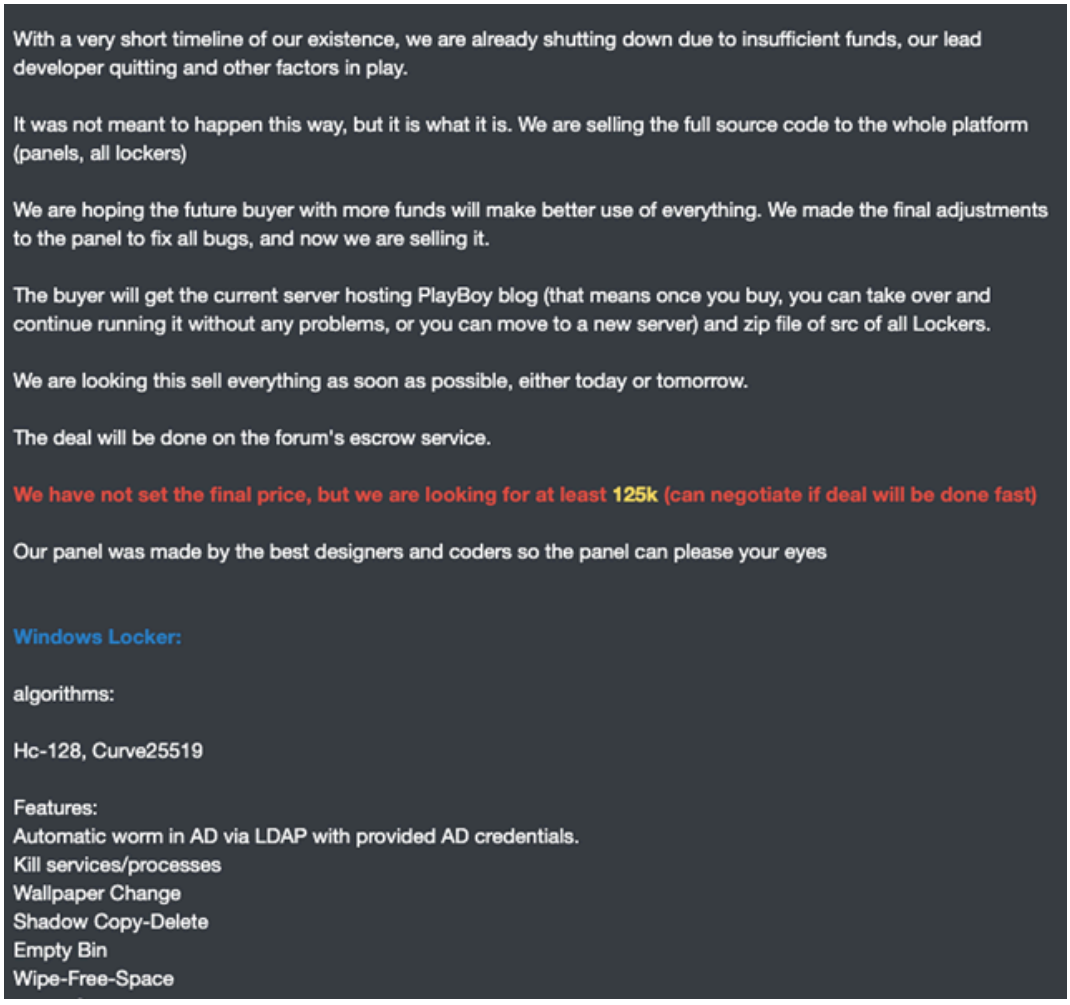
garant service required.no need for issue "test" build,locker is proven and stable for many years.
crypt/fud builds yourself with third party service,not offered by me.***i right to refuse sale of software for any reson.***

price: $100, contact by PM, or TOX

have contacts and options ready.

Медианная стоимость таких решений составляет 1000 $, тогда как наиболее развитые и функциональные варианты программ-вымогателей могут достигать стоимости до 125 000 $.

Рисунок 57. Объявление о продаже шифровальщика

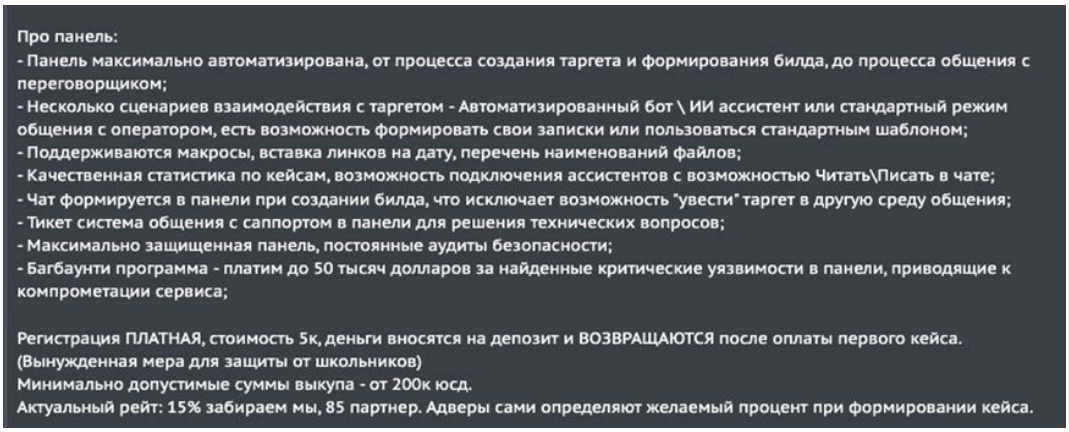


Как и в других сегментах киберпреступных сервисов, технологии искусственного интеллекта начинают играть заметную роль в развитии RaaS. Использование больших языковых моделей позволяет автоматизировать отдельные этапы атак и снизить трудозатраты злоумышленников.

В частности, уже зафиксированы случаи использования генеративных моделей для разработки компонентов программ-вымогателей. Так, аналитики Acronis обнаружили в сентябре 2025 года использование Claude Code от Anthropic для создания RaaS.

Кроме того, существует тенденция к автоматизации не только разработки, но и управления всей атакующей операцией. В ряде современных решений RaaS панели управления уже включают функции, позволяющие автоматизировать полный цикл атаки — от создания цели и формирования вредоносного файла до взаимодействия с жертвой на этапе переговоров. Некоторые платформы предлагают несколько сценариев коммуникации с пострадавшей организацией, включая автоматизированных ботов и ИИ-ассистентов, способных вести переговоры по заранее заданным сценариям или на основе обученных моделей. Это свидетельствует о дальнейшем развитии инфраструктуры RaaS в сторону максимальной автоматизации процессов и снижения зависимости от человеческого участия.

Рисунок 58. Описание панели шифровальщика



DDoS КАК УСЛУГА (DDoS AS A SERVICE)

DDoS as a service (DDoSaaS) представляет собой услугу, предоставляющую возможность по требованию запускать распределенные атаки с целью отказа в обслуживании. Как правило, такие сервисы предоставляют доступ к ботнетам и панелям управления, позволяющим выбирать цель атаки, ее продолжительность, интенсивность и другие параметры воздействия.

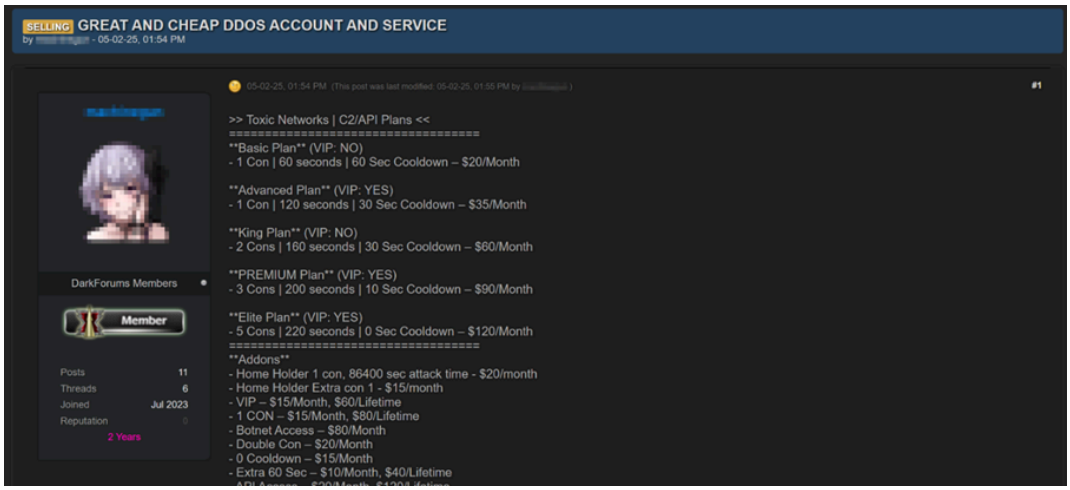
DDoS as a service является одним из наиболее простых и доступных киберпреступных сервисов. Стоимость услуг в данном сегменте относительно низкая. Разброс цен составляет от 10 до 600 $ в месяц при медианной стоимости 20 $ в месяц.

Тарифные планы обычно различаются по следующим параметрам:

- максимальная продолжительность атаки;
- объем генерируемого трафика;
- количество одновременно доступных атак;
- время ожидания между атаками;
- доступ к дополнительным функциям управления.

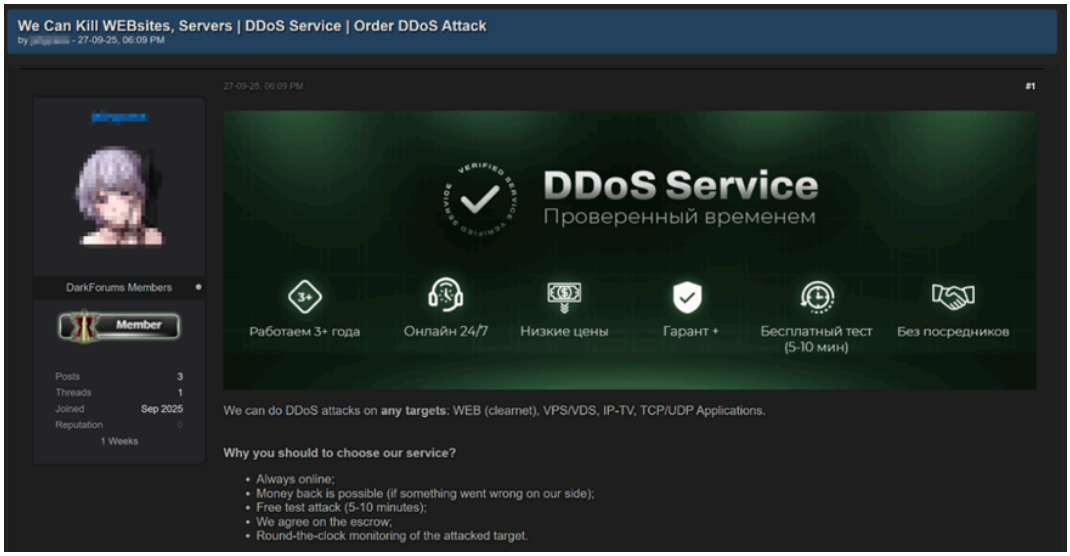
Для продавцов характерна высокая гибкость в формировании тарифов, поэтому пользователям часто предлагается широкий выбор планов, ориентированных на разные бюджеты и задачи.

Рисунок 59. Предложение услуг по проведению DDoS-атак



Отдельные сервисы используют маркетинговые механизмы, характерные для легальных онлайн-платформ. Например, некоторые поставщики предлагают гарантию возврата средств в случае неудачной атаки, а также бесплатные тестовые запуски — короткие DDoS-атаки для демонстрации возможностей сервиса. Такие практики свидетельствуют о высокой конкуренции в этом сегменте и о стремлении операторов повысить доверие потенциальных клиентов.

Рисунок 60. Объявление о продаже услуг по проведению DDoS-атак



В целом DDoS as a service можно рассматривать как один из наиболее зрелых и стандартизированных сервисных сегментов киберпреступного рынка. Простота использования, низкая стоимость и высокий уровень автоматизации делают эту услугу массовым инструментом.

ВПО КАК УСЛУГА (MALWARE AS A SERVICE)

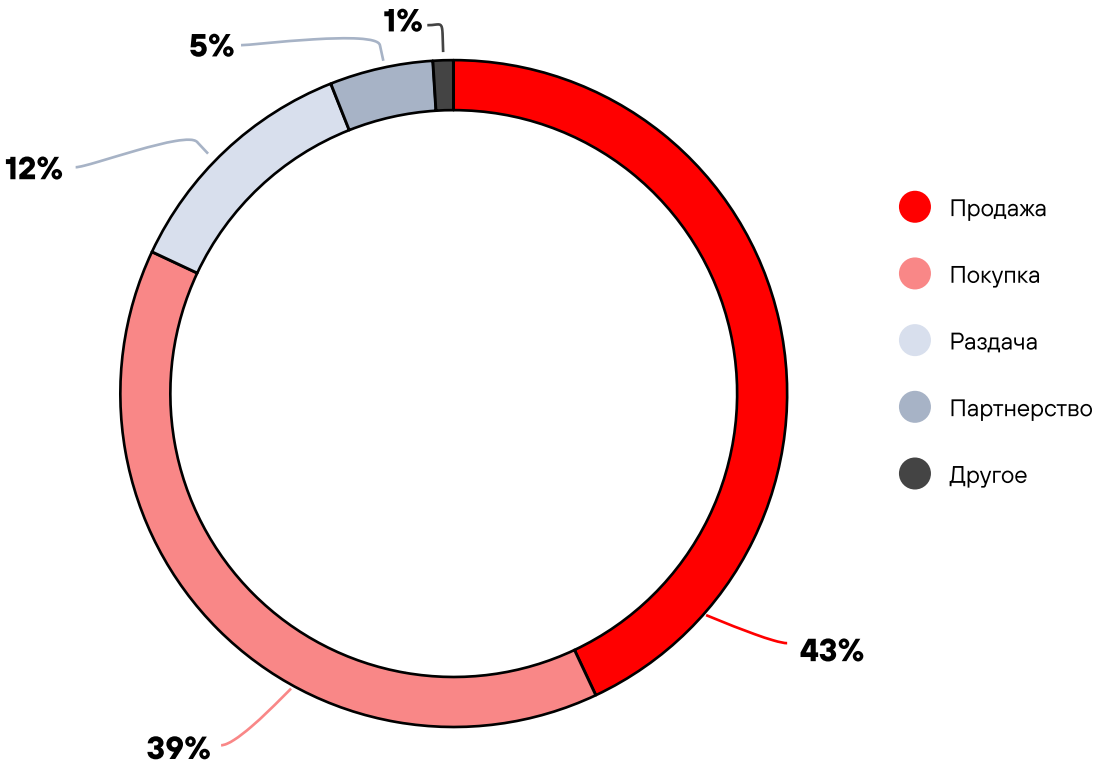
Malware as a service (MaaS) представляет собой услугу по предоставлению готовых вредоносных программ вместе с инфраструктурой управления, обновлениями и технической поддержкой. Злоумышленники получают возможность проводить атаки без необходимости самостоятельно разрабатывать программное обеспечение.

Вредоносное программное обеспечение продолжает оставаться одним из основных инструментов злоумышленников в атаках на организации из различных отраслей. По нашим данным, в 71% успешных атак на организации в 2025 году злоумышленники использовали ВПО. Это обусловлено высокой эффективностью и универсальностью инструмента, а также его центральной ролью в кибератаках.

На рынке MaaS встречаются как разовые продажи исходных кодов вредоносного программного обеспечения, так и сервисы, предоставляемые по подписочной модели. Однако именно сервисный формат постепенно становится доминирующим, поскольку он обеспечивает регулярные обновления функциональности и поддержку пользователей.

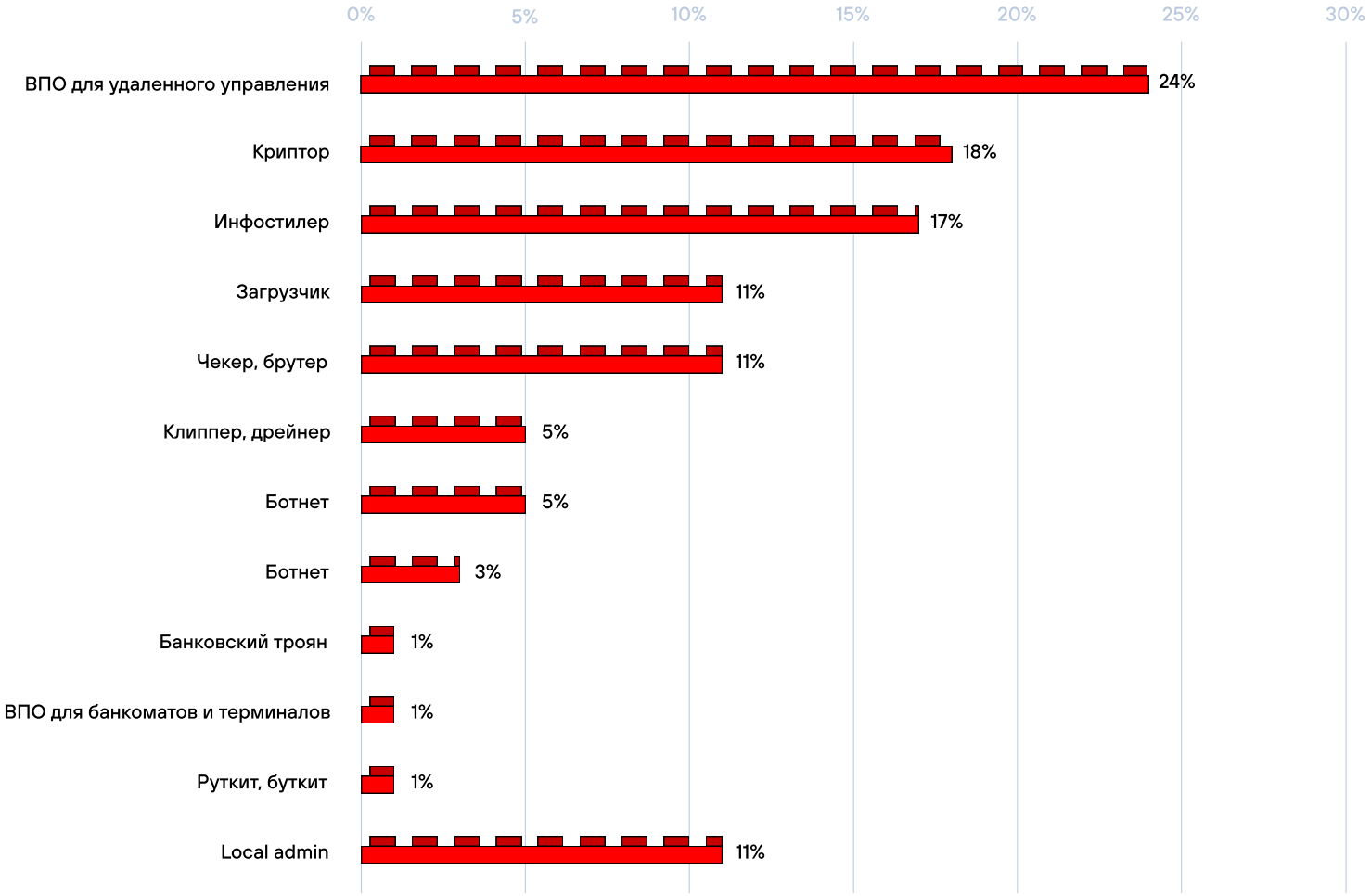
Рынок ВПО характеризуется высокой активностью со стороны как продавцов, так и покупателей. Большая доля объявлений о покупке (39%) свидетельствует о стабильном спросе на готовые инструменты и подтверждает востребованность сервисной модели. Наличие объявлений о раздаче (12%) отражает распространенную практику продвижения вредоносных инструментов через бесплатные версии.

Рисунок 61. Типы объявлений по теме ВПО



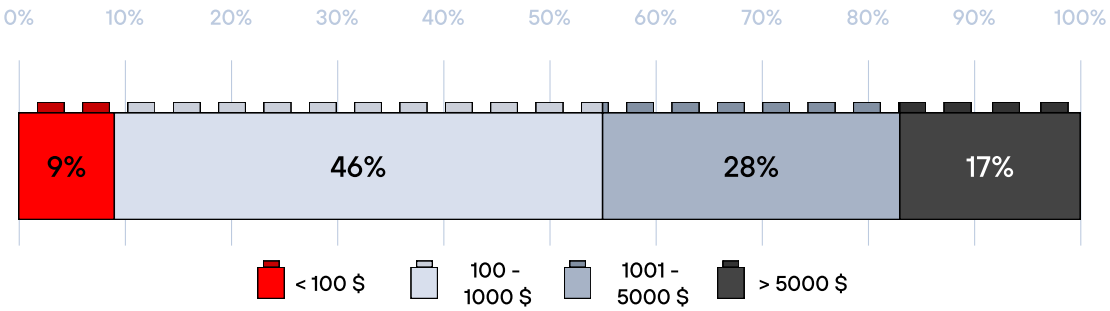
Распределение типов вредоносного программного обеспечения в объявлениях отражает текущие приоритеты злоумышленников. Наибольший интерес вызывают инструменты, обеспечивающие длительный доступ к инфраструктуре жертвы и позволяющие извлекать данные, а также обходить средства защиты. При этом разнообразие категорий свидетельствует о высокой специализации рынка и наличии решений для различных этапов атаки.

Рисунок 62. Типы ВПО, упоминаемого в объявлениях по теме ВПО



Наиболее популярный тип ВПО в объявлениях — инструменты удаленного управления (RAT). Это тесно связано с их высокой распространенностью в реальных атаках: по нашим данным, в первом квартале 2026 года трояны удаленного доступа были вторым по частоте использования типом ВПО (28% успешных атак на организации). Стоимость инструментов удаленного управления варьируется в широком диапазоне — от нескольких долларов до сотен тысяч долларов — и зависит от функциональности, уровня поддержки и степени скрытности. Основная масса предложений (46%) сосредоточена в среднем ценовом сегменте от 100 до 1000 $, а медианная цена составляет 1000 $. Это указывает на формирование массового рынка доступных решений.

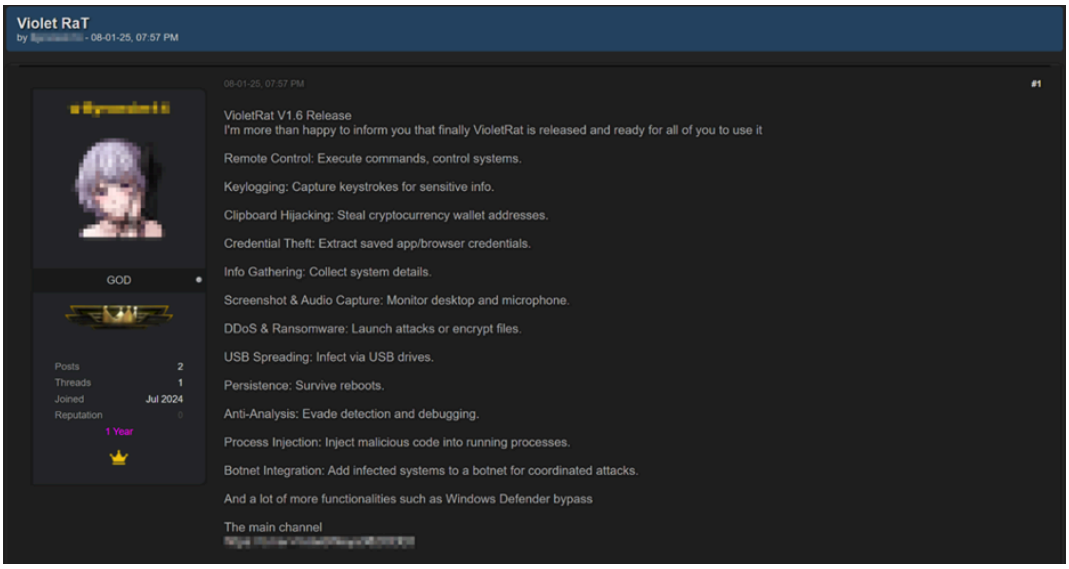
Рисунок 63. Распределение стоимости ВПО для удаленного управления



Современные инструменты удаленного управления постепенно превращаются в универсальные платформы для проведения кибератак, объединяющие функции нескольких классов ВПО. Такая модульность дает возможность реализовывать различные сценарии атак в рамках одного инструмента. Привлекательность таких решений усиливается тем, что, в отличие от программ-вымогателей, они позволяют злоумышленникам длительное время сохранять присутствие в инфраструктуре жертвы и извлекать максимальную выгоду.

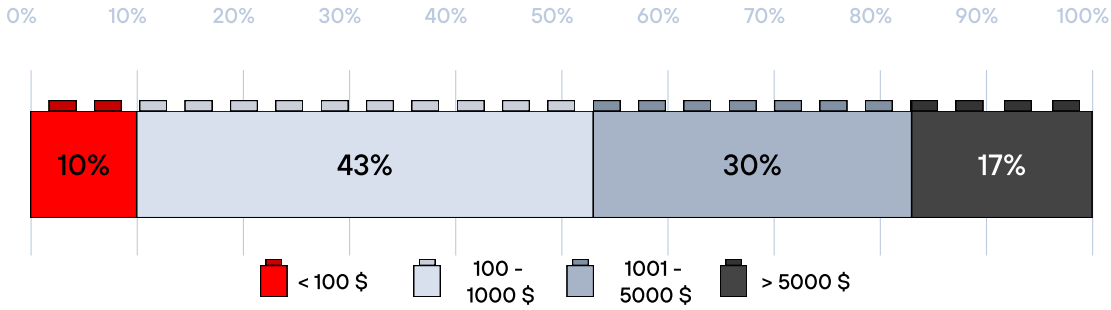
Например, многомодульное ВПО VioletRat предоставляет злоумышленникам широкий спектр возможностей для несанкционированного доступа к зараженным системам, включая удаленное управление, кейлоггинг, кражу учетных данных и криптовалют, создание скриншотов и аудиозаписей, а также функции DDoS-атак и шифрования файлов. Программа также обладает механизмами обхода систем безопасности (включая Windows Defender), маскировки от анализа, распространения через USB-накопители и интеграции в ботнеты для координированных кибератак.

Рисунок 64. Объявление о многомодульном RAT с множеством функций



Инфостилеры, как и трояны удаленного управления, являются одним из наиболее востребованных типов вредоносного ПО благодаря своей способности быстро извлекать ценные данные, включая учетные записи, файлы куки, финансовую информацию и криптовалютные ключи. Ценовое распределение инфостилеров демонстрирует схожую с другими категориями ВПО структуру, а большинство предложений находится в диапазоне до 1000 $ (53%), что делает такие инструменты доступными для широкого круга злоумышленников. Медианная стоимость инфостилеров составляет 1000 $.

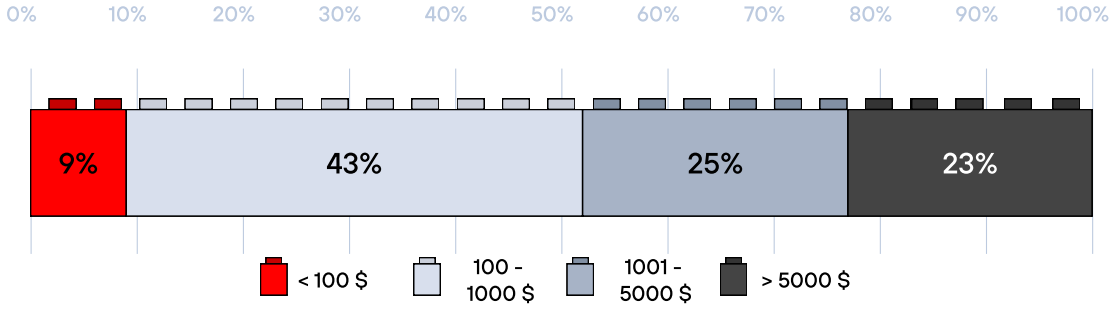
Рисунок 65. Распределение стоимости инфостилеров



Использование злоумышленниками инфостилеров способствует формированию вторичного рынка stealer logs as a service, где покупатели ВПО начинают перепродавать украденные данные другим злоумышленникам. Это позволяет операторам окупать затраты на инструмент и создавать дополнительный источник дохода.

Загрузчики используются для доставки и установки других типов вредоносного программного обеспечения, включая инфостилеры, шифровальщики и ВПО удаленного управления. Они являются важным элементом инфраструктуры атак, поскольку позволяют управлять распространением вредоносных компонентов. Медианная стоимость загрузчика составляет 1000 $.

Рисунок 66. Распределение стоимости загрузчиков



Сервисные инструменты этого класса часто предоставляются в виде веб-панелей управления, позволяющих автоматизировать процесс создания и распространения ВПО. Пользователь может формировать исполняемые файлы на основе заданных параметров, управлять ими через централизованный интерфейс и отслеживать статистику заражений, включая информацию о целевых устройствах. Характерная особенность таких решений — возможность использования панели не только для собственных атак, но и как коммерческого сервиса: разработчики предусматривают предоставление доступа по подписочной модели, что позволяет операторам выступать в роли провайдеров собственных MaaS-решений.

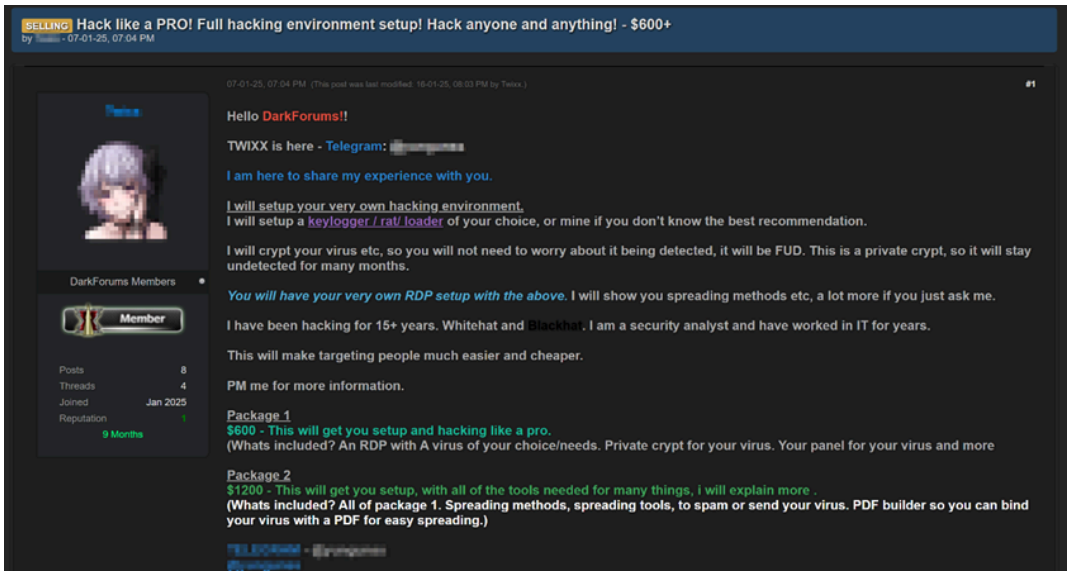
Рисунок 67. Объявление о продаже веб-панели для создания и управления инфостилерами

ВЗЛОМ КАК УСЛУГА (HACKER AS A SERVICE)

К услуге относятся предложения наемных специалистов, выполняющих кибератаки по заказу. Это может включать проникновение в информационные системы, кражу данных, нарушение работы инфраструктуры, внедрение вредоносного программного обеспечения или проведение других действий в интересах заказчика. Это комплексная услуга, которая чаще всего предполагает наем специалиста или команды, способных реализовать атаку под ключ по договорной цене. Медианная цена на такие услуги составляет 2750 $.

Несмотря на индивидуальный характер работы, рынок постепенно демонстрирует признаки сервисной модели. Появляются предложения, где несколько услуг объединяются в пакет, позволяя заказчику получить комплексное решение без необходимости взаимодействовать с несколькими исполнителями.

Рисунок 68. Услуга взлома, продаваемая пакетом



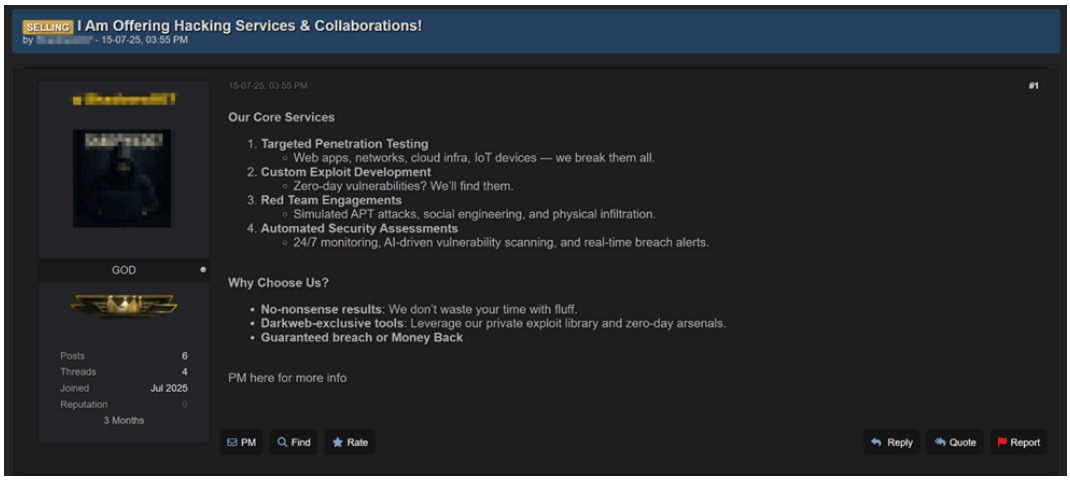
Отдельный сегмент — высокобюджетные предложения, ориентированные на сложные и целевые атаки. Например, встречаются объявления о возможности внедрения человека в организацию для проведения инсайдерской атаки. Стоимость таких услуг начинается от 500 000 $, что делает их доступными только для финансово мотивированных или APT-кампаний.

Рисунок 69. Типы ВПО, упоминаемого в объявлениях по теме ВПО

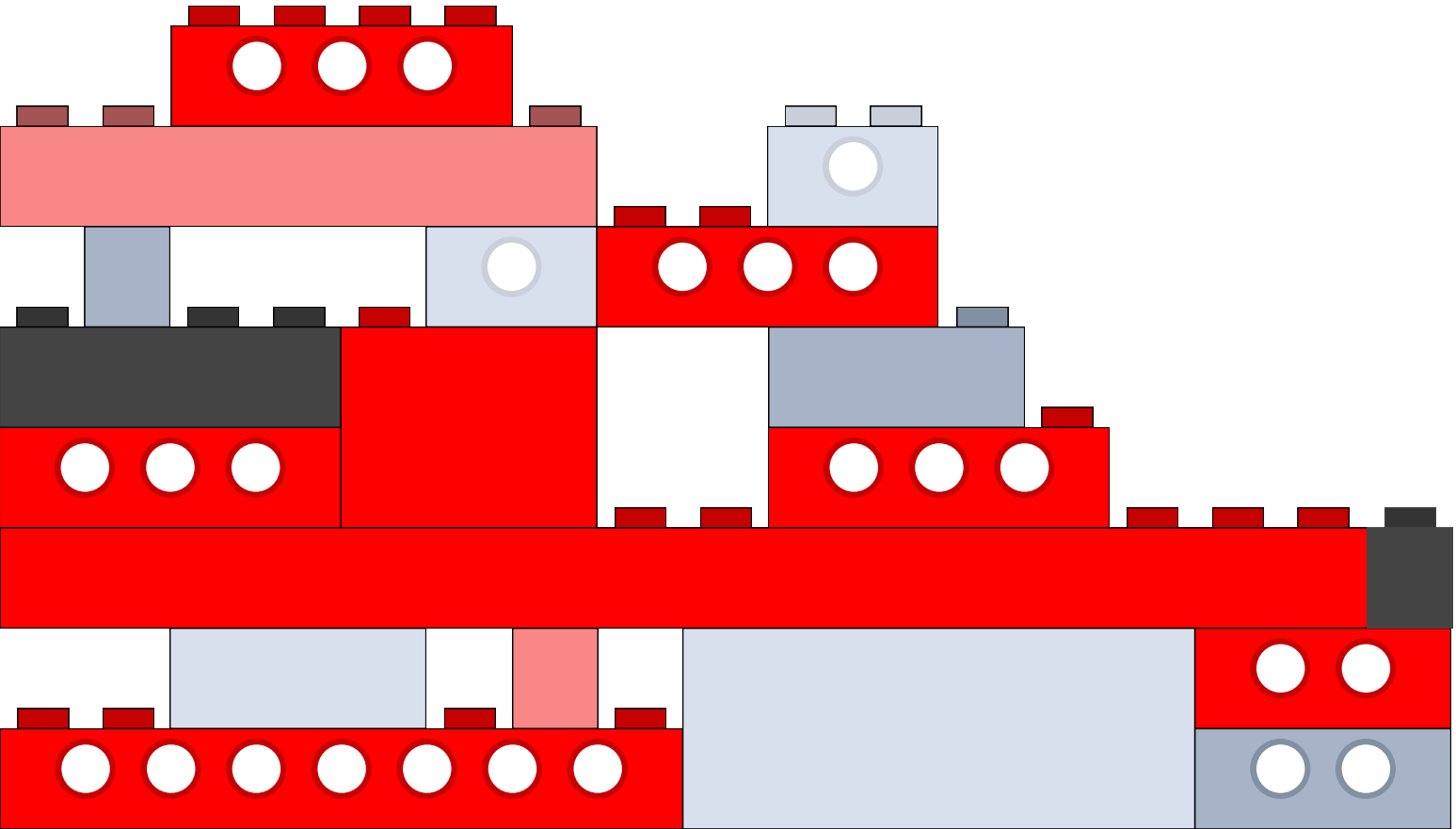
В данный сегмент постепенно проникают технологии искусственного интеллекта. В ряде объявлений указано использование ИИ для автоматизированного сканирования инфраструктуры, поиска уязвимостей и подготовки сценариев атаки. Это позволяет снизить трудозатраты исполнителей и ускорить подготовительный этап атаки.

Для данной категории услуг также характерно предоставление гарантий результата. В некоторых случаях оплата осуществляется только после достижения цели атаки, например успешного получения доступа к системе или утечки данных. Такая модель повышает доверие со стороны заказчиков и отражает конкурентный характер рынка.

Рисунок 70. Объявление о продаже услуг взлома

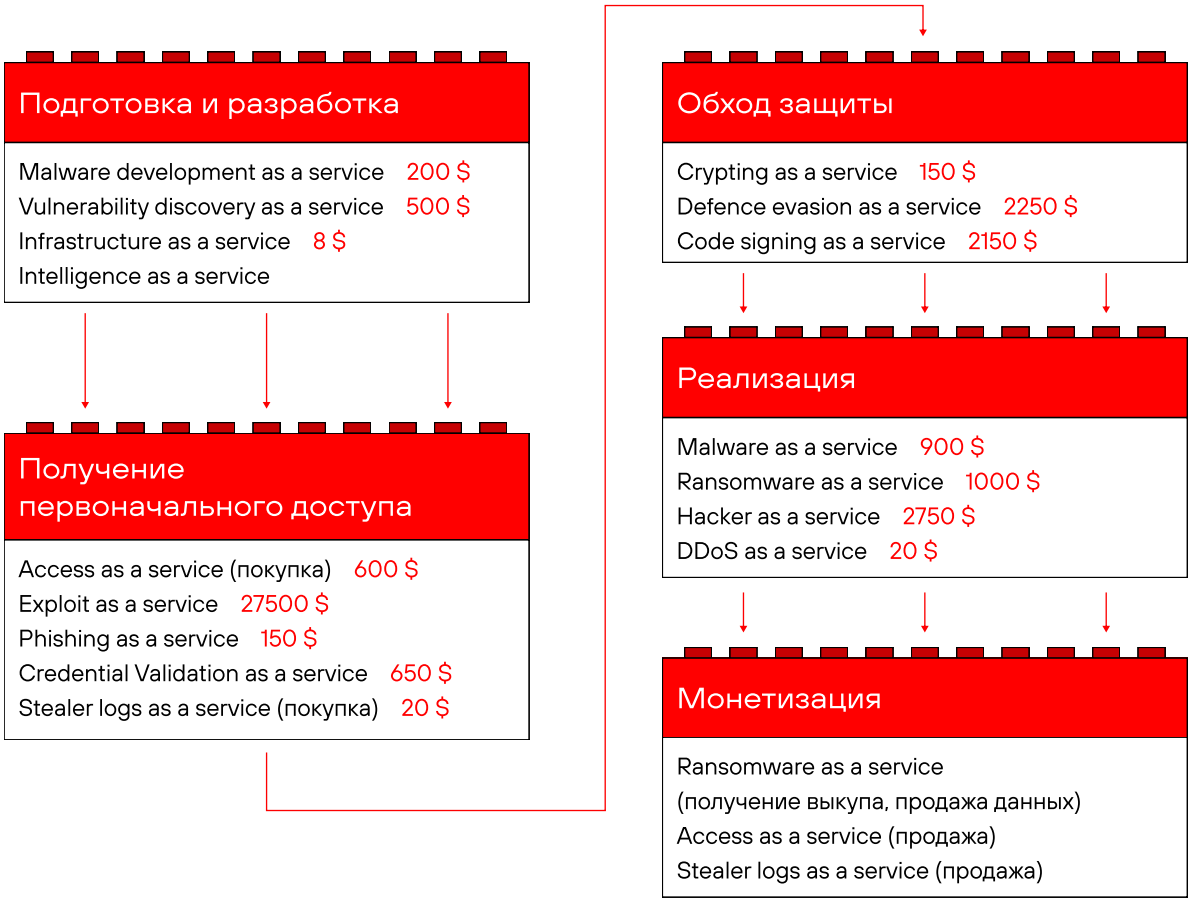


ВОЗМОЖНОСТЬ СБОРКИ АТАКИ ИЗ ДОСТУПНЫХ УСЛУГ И ОЦЕНКА СТОИМОСТИ



Многие этапы кибератаки в настоящее время могут быть реализованы за счет приобретения отдельных услуг. Наличие широкого спектра специализированных предложений — от получения доступа до монетизации — позволяет теоретически собрать атакующий пайплайн из готовых компонентов. Не все нужные компоненты можно найти по подписке, но почти все продается за разовые платежи. На практике наиболее распространенной является гибридная модель, при которой злоумышленники комбинируют собственные компетенции с приобретенными сервисами.

Рисунок 71. Медианная цена услуг на разных этапах атаки



Массовые кампании обеспечиваются дешевыми, легкодоступными услугами — инфраструктурой, фишинговыми панелями, журналами стилеров. Целевые атаки требуют иного набора компонентов — эксплойтов, EDR-киллеров, сертификатов подписи кода, — стоимость которых на порядок выше. Промежуточный уровень — ВПО, доступы — обслуживает средний сегмент угроз, наиболее распространенный на практике.

Рисунок 72. Медианные цены на услуги теневого рынка

Для оценки реальной стоимости атаки важно учитывать не только цены отдельных компонентов, но и набор инструментов, необходимый под конкретный сценарий. При этом в реальных условиях стоимость атаки может быть выше за счет дополнительных расходов, например, на привлечение исполнителей. Рассмотрим пример сценария атаки, собранной из покупных компонентов: злоумышленник не разрабатывает ничего самостоятельно, а лишь комбинирует готовые услуги теневого рынка. Представленные наборы инструментов являются типовыми.

Профиль атакующего: низкая техническая квалификация, минимальный бюджет. Цель — кража корпоративных учетных данных и их перепродажа.

Это наиболее доступный сценарий: для его реализации достаточно подписки на фишинговую панель с готовыми шаблонами и минимальной инфраструктуры. Фишинговые панели поставляются с шаблонами под банки, корпоративные порталы, почтовые сервисы; технических навыков для запуска кампании практически не требуется.

Компонент	Стоимость
Фишинговая панель (подписка 1 месяц)	≈ 150 $
Сервер или инфраструктура	≈ 8 $
Итого	≈ 158 $

Полученная прибыль: среди продаваемых доступов 75% стоят более 150 $. То есть даже один удачно полученный доступ может окупить затраты на кампанию.

Эта асимметрия — ключевой драйвер экономики модели CaaS. Пока стоимость инструментов атаки снижается, а ущерб от инцидентов растет, финансовый стимул к развитию теневого рынка сохраняется.

РАЗВИТИЕ CYBERCRIME AS A PLATFORM

Современная экосистема киберпреступности постепенно эволюционирует от фрагментированного набора услуг к модульной архитектуре, в которой каждый этап атаки поддерживается специализированным сегментом рынка. Это позволяет злоумышленникам гибко комбинировать компоненты и адаптировать атаки под конкретные цели и бюджеты.

В перспективе возможно дальнейшее развитие данной модели в сторону появления концепции cybercrime as a platform — интегрированных решений, объединяющих несколько этапов атаки в рамках единой экосистемы. Существенную роль в этом процессе могут сыграть системы на основе искусственного интеллекта, в частности автономные агенты, способные автоматизировать процессы выбора, комбинирования и управления различными сервисами. Это может привести к дальнейшему снижению барьеров входа в киберпреступность и увеличению скорости реализации атак, что, в свою очередь, усилит общую динамику развития этого рынка. Однако на текущий момент для реализации сложных атак все еще требуются практические навыки и опыт.

Регуляторные меры, операции против даркнет-форумов и ограничения анонимных криптовалют оказывают влияние на преступный рынок, но не приводят к его исчезновению. Теневая экосистема демонстрирует устойчивость и способность к быстрому восстановлению.

В этих условиях противодействие киберпреступности как услуге требует комплексного подхода. Приоритетными направлениями противодействия должны стать развитие мониторинга даркнета и связанных коммуникационных каналов, а также усиление обмена информацией между компаниями, исследовательскими организациями и правоохранительными органами.