

POSITIVE TECHNOLOGIES

Рынок преступных киберуслуг

2018



Содержание

Введение.....	3
Резюме.....	4
1. Киберпреступность как бизнес.....	5
2. Продажа продуктов.....	5
2.1. Вредоносное ПО.....	6
2.1.1. Трояны для кражи данных.....	7
2.1.2. RAT и ВПО для ботнета.....	8
2.1.3. Трояны для банкоматов.....	9
2.1.4. Трояны-вымогатели.....	10
2.2. Эксплойты.....	12
2.3. Данные.....	13
2.3.1. Учетные данные пользователей.....	14
2.3.2. Данные банковских карт.....	15
2.3.3. Скан-копии личных и конфиденциальных документов.....	16
2.4. Доступы.....	17
3. Услуги.....	19
3.1. Связанные с ВПО услуги.....	20
3.1.1. Разработка ВПО.....	21
3.1.2. Обфускация ВПО.....	22
3.1.3. Распространение ВПО.....	23
3.2. Инфраструктура.....	25
3.3. Спам и фишинг.....	26
3.4. Взлом на заказ.....	27
3.4.1. Взлом электронной почты и аккаунтов социальных сетей.....	28
3.4.2. Взлом сайтов, серверов, сетевого оборудования.....	29
3.5. Дропы, обналичивание и инсайдеры.....	30
3.6. Ботнет.....	33
3.7. DDoS.....	33
Выводы.....	35



Введение

Сегодня в новостях можно прочитать про финансовый ущерб той или иной организации от хакерской атаки или об утечке сотен тысяч учетных записей пользователей какого-нибудь ресурса. При этом не получится найти сообщения о том, сколько стоило проведение такой атаки, или о том, насколько сложно было ее реализовать. Но ведь работа, в том числе и работа киберпреступников, направлена на получение прибыли, и если затраты сравнимы или же превышают возможную выручку, хакер просто переключится на другую, более выгодную задачу.

В нашем недавнем исследовании актуальных киберугроз мы отметили рост числа значимых киберинцидентов: в первом квартале 2018 года их выявлено на 32% больше, чем в первом квартале 2017 года¹. При этом в атаках с использованием вредоносного ПО в большинстве случаев применялись программы для кражи данных и скрытого майнинга криптовалюты. В то же время в интернете появляется все больше информации о том, что код того или иного трояна выложен в открытый доступ. Именно с возможностью получения готового вредоносного ПО и последующего его использования мы связываем столь существенное увеличение числа атак. Для того чтобы оценить стоимость подобного ПО, сложность его приобретения, а также проанализировать существующие спрос и предложение на рынке, мы провели данное исследование.

Мы детально проанализировали рынок преступных киберуслуг и постарались оценить, нужен ли вообще киберпреступнику широкий спектр специализированных знаний, или для реализации атаки достаточно обратиться к представителям теневого рынка — взломщикам сайтов и серверов, разработчикам и распространителям вредоносного ПО, владельцам ботнетов и другим. В ходе анализа мы неоднократно сталкивались с ситуацией, когда учетные данные для доступа к системам либо веб-шеллы для удаленного управления серверами крупных компаний были выставлены на продажу. Полученную информацию мы оперативно передавали представителям скомпрометированных организаций, предупреждая о необходимости принять меры по защите и провести расследование.

В качестве объектов для исследования мы выбрали 25 наиболее популярных англоязычных и русскоязычных теневых торговых площадок, названия которых мы не раскрываем, с общим числом зарегистрированных пользователей более трех миллионов. Всего проанализировано более 10 000 объявлений, при этом мы не учитывали явно мошеннические предложения, которых на теневом рынке так же много, как и на любом другом.

Мы подсчитали минимальную и среднюю стоимость различных инструментов и услуг, которые продаются на таких площадках, оценили соотношения спроса и предложения, а также полноту представленных услуг и их достаточность для проведения полноценной кибератаки.

¹ ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf



Резюме

Современные кибератаки в большинстве своем основаны на использовании не собственных, а купленных и арендованных у третьих лиц разработок и серверов. Это не только снижает порог входа в киберпреступность и упрощает проведение атак, но и существенно затрудняет или делает невозможной точную атрибуцию целевых атак.

На схеме ниже представлены распространенные типы атак, а также рассчитана их минимальная стоимость в долларах США при условии, что все необходимые средства и инструменты организатор атаки приобретет за деньги. Так, например, стоимость целевой атаки на организацию в зависимости от сложности может составлять от 4500 \$, включая наем специалиста по взлому, аренду инфраструктуры и покупку соответствующих инструментов. Взлом сайта с получением полного контроля над веб-приложением обойдется всего в 150 \$, при этом мы находили объявления с запросами на целевой взлом сайтов, в которых оценка работы доходила до 1000 \$.

Исследование показало, что на теневом рынке киберуслуг широко распространены криптомайнеры, хакерские утилиты, ВПО для создания ботнета, RAT и трояны-вымогатели, а основным спросом закономерно пользуются услуги, связанные с разработкой и распространением ВПО. На рынке представлено более 50 различных категорий товаров и услуг, которые в совокупности могут быть использованы для организации любой атаки.

Хакера осудили за взлом учетных записей должностных лиц США ² 5 лет лишения свободы	Взлом почты от 40 \$	Взлом сайта от 150 \$	Хакера осудили за проведение DDoS-атак ³ 2 года лишения свободы
Целевая атака на компанию от 4500 \$			DDoS-атака от 50 \$ / день
Заражение трояном- майнером от 750 \$			Кража денег из банкоматов от 1500 \$
Программиста осудили за создание ВПО для обхода системы учета АЗС ⁴ 1,5 года лишения свободы	Заражение трояном-вымогателем (1000 узлов) от 300 \$	Кража денег со счетов (с помощью фишинга) от 270 \$	Мошенника осудили за кражу денег клиентов банка через систему ДБО ⁵ 6 лет лишения свободы

² goo.gl/v8SwKZ

³ goo.gl/x8nJPn

⁴ goo.gl/1XGBvU

⁵ goo.gl/VXUT8z

1. Киберпреступность как бизнес

По данным FireCompass, только 4% страниц интернета проиндексировано поисковыми системами⁶. Приватные форумы, закрытые базы данных (медицинские, исследовательские, финансовые) и другие невидимые для поисковых машин ресурсы все вместе называются глубокой сетью (deep web), или глубоким интернетом. Помимо ресурсов с конфиденциальными и другими легальными данными в глубокой сети размещаются специализированные площадки и форумы нелегальной направленности, которые в совокупности называются дарквебом (dark web). А поскольку на таких ресурсах часто происходит торговля нелегальными продуктами и услугами, которые предлагаются их участниками, то совокупность этих ресурсов также называется теневым рынком. В рамках нашего исследования мы сосредоточились на хакерских форумах.

Ниже схематично представлено место теневого рынка в процессе планирования и реализации кибератаки.

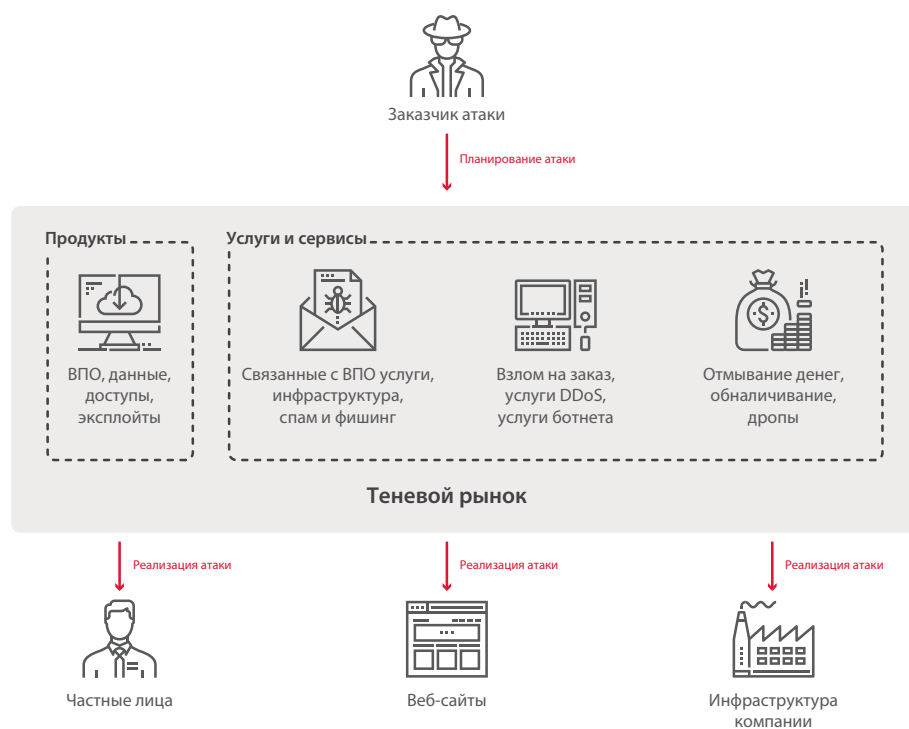


Рисунок 1. Теневой рынок и его место в киберпреступном мире

2. Продажа продуктов

Подавляющее большинство продуктов на теновом рынке относится к следующим категориям:

- **вредоносное программное обеспечение** — шифровальщики-вымогатели, майнеры и т. п.;
- **эксплойты** — как для известных уязвимостей, так и для уязвимостей нулевого дня;
- **данные** — персональные, учетные, платежные и т. п.;
- **доступы** — веб-шеллы, пароли от сайтов или серверов.

Далее продукты каждой категории будут рассмотрены подробнее. Будет показано, как на теновом рынке представлены спрос и предложение на тот или иной продукт, а также за какую цену его можно приобрести.

⁶ firecompass.com/blog/darkweb-deepweb-darknet-browsers/



2.1. Вредоносное ПО

Сегодня ВПО стало тем элементом, без которого практически невозможна ни одна кибератака, поскольку оно позволяет решать задачи, связанные с автоматизацией, скоростью проведения, незаметностью атаки. В зависимости от назначения ВПО подразделяется на несколько типов:

На 1,5 года лишения свободы осужден программист за разработку ВПО⁷

- криптомайнеры,
- трояны для кражи данных (stealer),
- хакерские инструменты,
- ВПО для DDoS,
- трояны-вымогатели (ransomware),
- RAT,
- трояны-загрузчики (loader, dropper),
- ВПО для создания ботнета,
- ВПО для банкоматов.

На диаграмме ниже показано, насколько распространены объявления о продаже того или иного ВПО в дарквебе. Важно отметить, что в рамках исследования мы встретили именно объявления о продаже готового трояна либо о поиске людей для разработки ВПО, но объявления о намерении купить готовый специфический троян отсутствовали. Это может говорить о том, что сегодня широкий спектр предложений ВПО практически полностью покрывает спрос, а когда необходима специфичная разработка, злоумышленники выполняют ее самостоятельно либо нанимают программистов. О найме программистов для разработки ВПО мы расскажем отдельно (см. [раздел 3.1.1](#)).

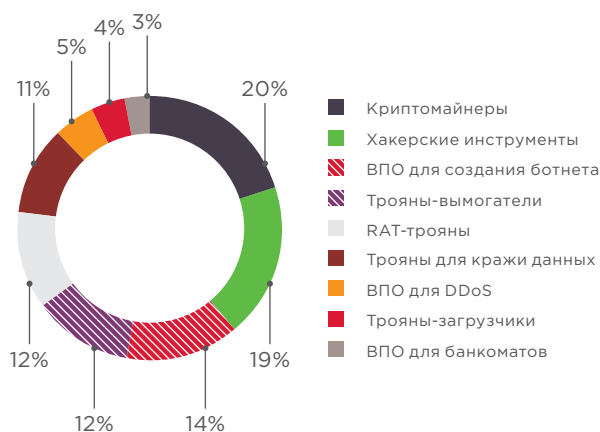


Рисунок 2. Доли объявлений о продаже ВПО разных типов

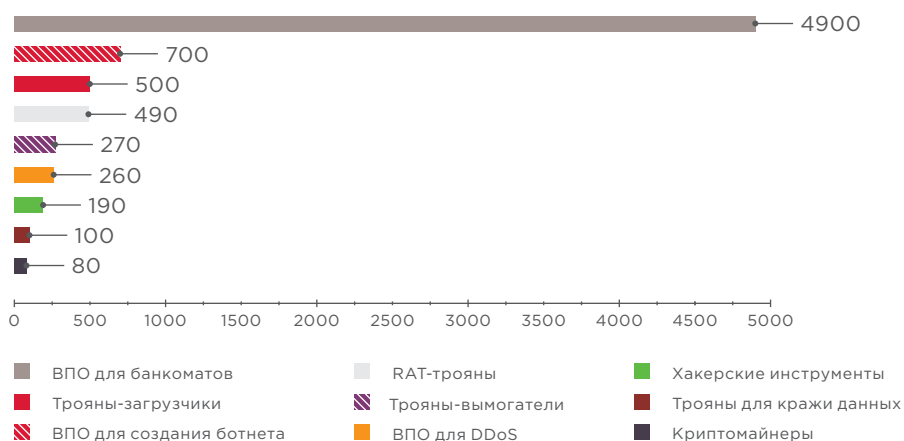


Рисунок 3. Средняя стоимость ВПО, \$

⁷ goo.gl/1XGBvU

В 2017 году на волне бурного роста ценности криптовалют широкое распространение получило ПО для скрытого майнинга. Среди предлагаемого к продаже ВПО их доля сегодня составляет 20%. При этом в первом квартале 2018 года доля кибератак с применением этого типа ВПО составила 23%⁸. Рост интереса к криптовалютным проектам привел и к более широкому распространению ВПО для кражи данных (стилиеры, шпионское ПО), направленного, в частности, на хищение средств с криптокошельков пользователей. При доле 11% в общем объеме предложений о продаже ВПО стилеры занимают первое место по количеству киберинцидентов, зарегистрированных в первом квартале 2018 года (с долей 30% от их общего числа).

Девятнадцать процентов предложений о продаже составили хакерские инструменты, к которым мы относим ПО, предназначенное для проведения атак на сайты, массовых почтовых рассылок, а также генераторы адресов и паролей, упаковщики и шифровальщики исполняемых файлов.

Средние цены на инструменты из каждой категории представлены на диаграмме выше. Наиболее дорогим оказалось ВПО для банкоматов. Это неудивительно, ведь именно с его помощью преступники могут наверняка получить существенную прибыль.

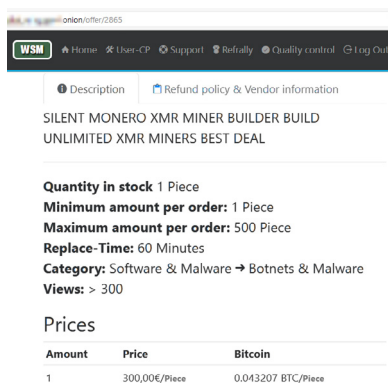


Рисунок 4. Продажа трояна для добычи криптовалюты Monero

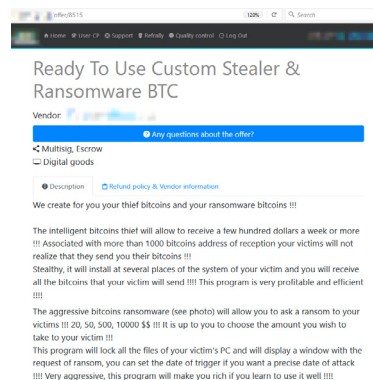


Рисунок 5. Продажа трояна для хищения криптовалюты из кошелька пользователя

2.1.1. Трояны для кражи данных

Стилеры позволяют атакующим решать следующие задачи:

- кража паролей из буфера обмена,
- перехват нажатий клавиш и сохранение заголовка окна, в котором эти клавиши нажимались;
- обход или отключение антивирусов;
- отправка файлов на почту злоумышленника.

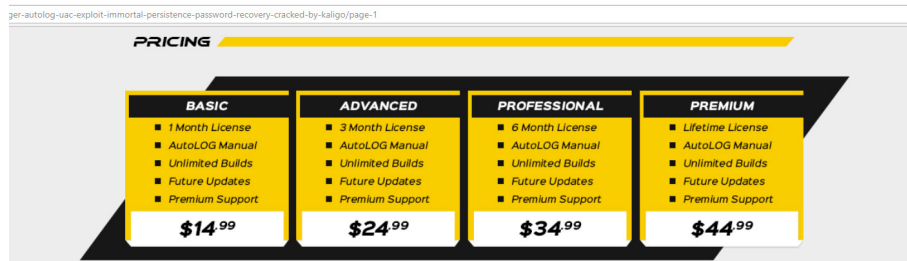


Рисунок 6. Продажа кейлоггера Autolog

⁸ ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatsape-2018-Q1-rus.pdf



Украденные данные при стоимости стилера около 10 \$ могут стоить от нескольких долларов до нескольких сотен долларов, если речь идет об учетных данных к почтовым ящикам, социальным сетям и другим ресурсам, содержащим персональную информацию. А если с помощью ВПО удастся украсть данные пользователей платежных систем или пароли от криптокошельков, то потенциальный доход в тысячи раз превысит расход на атаку.

2.1.2. RAT и ВПО для ботнета

Когда хакеры хотят не просто украсть какие-то заранее определенные данные, а получить доступ к устройству с возможностью долгосрочного скрытого присутствия в системе и удаленного выполнения команд, они используют так называемые троянские программы для удаленного доступа, или remote access trojan (RAT). Обычно ВПО этого типа предоставляет злоумышленнику следующие возможности:

- слежка за действиями пользователей;
- запуск файлов и выполнение команд;
- запись снимков экрана;
- включение веб-камеры и микрофона;
- сканирование локальной сети;
- загрузка файлов из интернета.

На теневом рынке средняя стоимость RAT составляет 490 \$, и в основном они используются для целенаправленных атак и заражения отдельных узлов. Наиболее известными RAT являются DarkComet, CyberGate, ProRAT, Turbojan, Back Orifice, Cerberus Rat, Spy-Net. Самый популярный, DarkComet, распространялся бесплатно, до тех пор пока в 2012 году не выяснилось, что с помощью него правительство Сирии шпионило за компьютерами оппозиционеров, а Китай следил за противобетскими неправительственными организациями⁹. После этого доступ к проекту DarkComet был закрыт, однако на его основе создаются многочисленные сборки, которые используются злоумышленниками и сегодня.

Существует также целое семейство RAT, разработанных на основе модифицированных легальных программ для управления удаленным компьютером типа TeamViewer, Remote Manipulator System, VNC. Подписка на такое ВПО стоит около 1000 \$ в месяц. Отметим, что благодаря своим легальным «корням» подобная вредоносная программа не детектируется средствами антивирусной защиты, но, в отличие от «доноров», осуществляет свою работу в скрытом режиме. Такое ПО можно часто встретить в арсенале хакеров, атакующих банки. Так, например, группировка MoneyTaker в ходе своих атак на банки России и США работала с UltraVNC¹⁰. А продвинутые банковские трояны Dridex, Neverquest и Gozi используют модули на основе hVNC для управления рабочими станциями зараженных пользователей¹¹.

Если же злоумышленники рассчитывают захватить контроль над большим числом устройств, то кроме ВПО с функциями RAT им потребуется специальное ПО, предназначенное для координации управления зараженными устройствами, — командный или управляющий центр. Сеть зараженных устройств, находящихся под единым управлением, называют ботнетом.

На 1 год лишения
свободы со штрафом
15 000 ₽ осужден
программист за создание
ботнета с целью кражи
учетных данных¹²

9 rus.azattyq.org/a/syria-darkcomet-program-opposition/24648538.html

10 group-ib.ru/resources/threat-research/money-taker.html

11 securityintelligence.com/anatomy-of-an-hvnc-attack/

12 goo.gl/Mgw55B

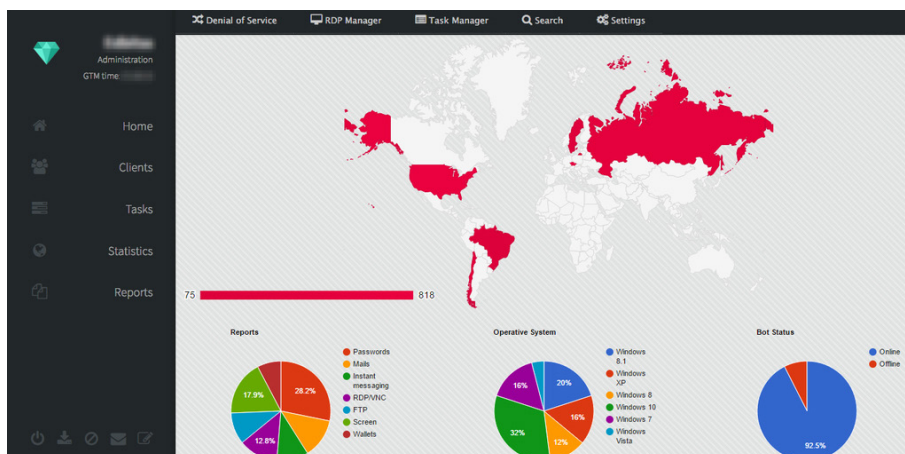


Рисунок 7. Интерфейс командного центра ботнета со статистикой по зараженным узлам

Цены на ВПО для создания ботнета на теневом рынке начинаются от 200 \$. Полный комплект, включающий ПО для командного сервера, ПО для создания троянов, настроенных на работу с определенным сервером (билдер), и дополнительные модули для трояна, может стоить 1000–1500 \$. При этом ботнет окупается меньше чем за месяц, если его использовать только, например, для проведения DDoS-атак.

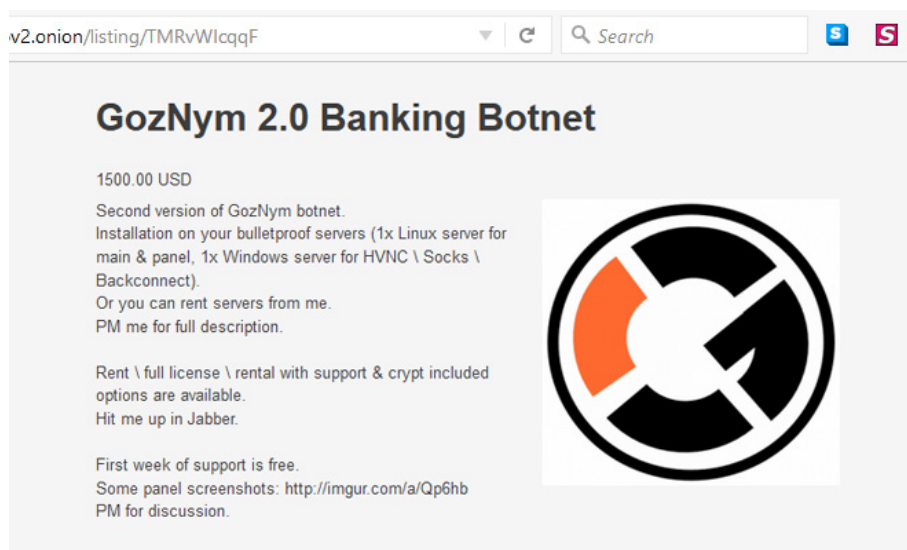


Рисунок 8. Продажа банковского ботнета

2.1.3. Трояны для банкоматов

Еще один вид ВПО, на который возлагают надежды злоумышленники, стремящиеся к быстрому обогащению, — трояны для банкоматов. Логические атаки на банкоматы мы подробно разобрали еще в 2017 году в исследовании «Атаки на банкоматы на примере GreenDispenser: организация и технологии»¹³, а в начале 2018 года эта тема снова подтвердила свою актуальность во время серии атак на банкоматы в США¹⁴.

¹³ ptsecurity.com/upload/corporate/ru-ru/analytics/ATM-Security-rus.pdf

¹⁴ krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms/

ВПО для банкоматов — это самый дорогой класс готового ВПО, цены на него начинаются от 1500 \$. Разработка таких программ требует не только хороших навыков программирования, но и знания внутреннего устройства банкоматов различных производителей.

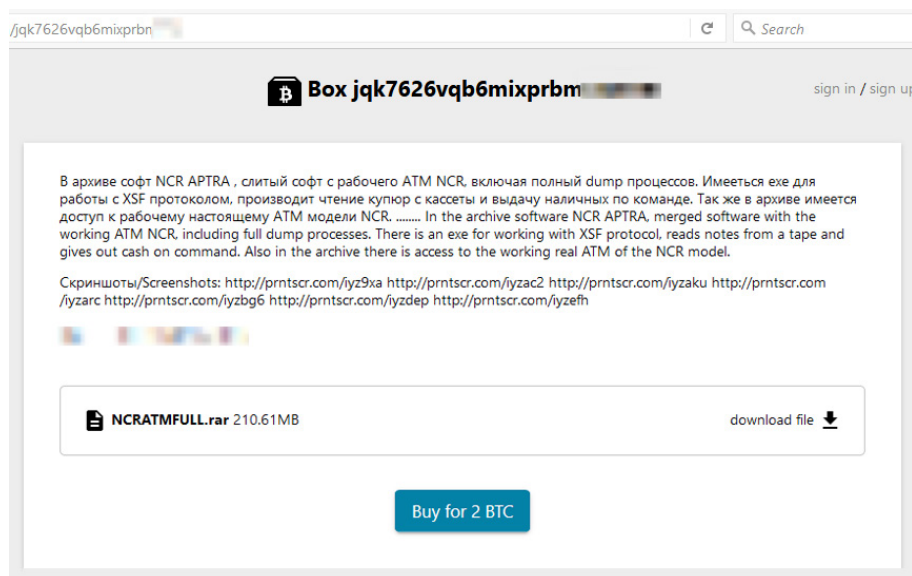


Рисунок 9. Продажа комплекта ПО для управления диспенсером банкомата

Конечно, на рыночную стоимость ВПО влияет и потенциальная прибыль от его использования: в один банкомат помещается порядка 8000 купюр разного номинала, что эквивалентно примерно 8 млн рублей (200 000 \$, 120 000 фунтов стерлингов). Одно ВПО можно использовать для атак сразу на множество однотипных банкоматов, поэтому слаженные действия преступной группы позволяют ей неплохо заработать. Так, по данным Европейской ассоциации безопасных транзакций (EAST), в 2017 году было 192 атаки на банкоматы с применением ВПО, официальный ущерб от которых составил 1,52 млн евро¹⁵. При этом по сравнению с 2016 годом количество инцидентов выросло на 231%, а общий ущерб на 230%.

2.1.4. Трояны-вымогатели

Этот вид ВПО, возможно, самый известный на сегодня из-за широкого распространения атак с использованием троянов-шифровальщиков в 2017 году.

Согласно исследованию IBM, до 70% опрошенных американских компаний выплачивали выкуп, чтобы восстановить свои данные¹⁶. Для российских компаний эту статистику сложно посчитать, но тем не менее в нашей практике расследования инцидентов тоже не раз были случаи, когда пострадавшие предпочитали заплатить. Исходя из этого очевидно, что затраты многократно окупаются после первой же успешно проведенной массовой атаки. Самыми крупными атаками вымогателей в 2017 году были эпидемии WannaCry, NotPetya, BadRabbit, Locky, Cerber, а общий ущерб от атак с использованием шифровальщиков превышает 1,5 миллиарда долларов.

Средние затраты на приобретение такого ВПО составляют 270 \$. Выкуп, который можно оплатить только в криптовалюте, устанавливается распространителями шифровальщика обычно самостоятельно и составляет 200–500 \$. Например, выкуп установленный за расшифровку данных, заблокированных троянами WannaCry и NotPetya, был установлен в размере 300 \$.

¹⁵ finextra.com/pressarticle/73375/atm-malware-attacks-hit-europe

¹⁶ www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN

Сегодня наиболее продвинутый метод распространения ВПО, и в частности шифровальщиков, — это модель продажи «как услуга» (as a service). Покупатель платит только за необходимое число запусков, период работы или количество созданных файлов.

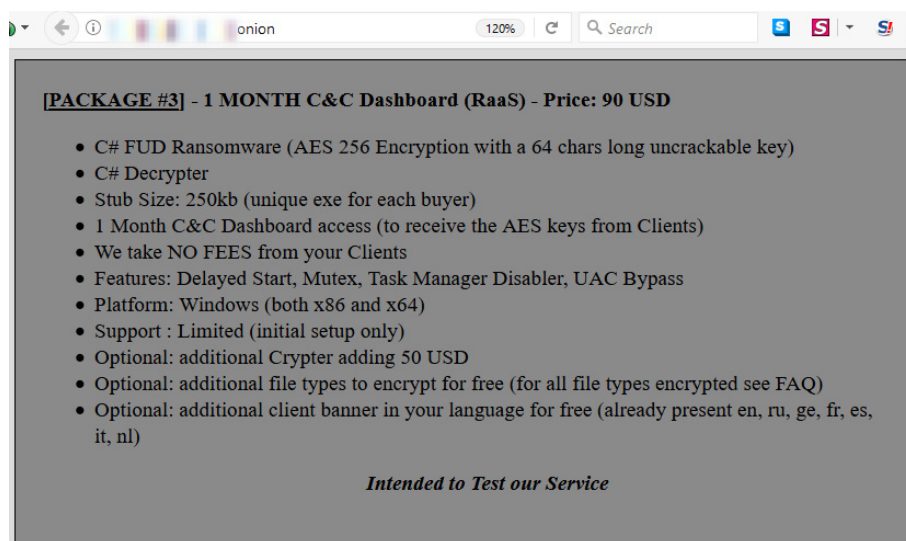


Рисунок 10. Объявление о сдаче трояна-вымогателя в аренду

Для того, чтобы увеличить свой доход, разработчики шифровальщиков в последнее время начали распространять их по так называемой партнерской программе. Продавец передает персонифицированный файл шифровальщика и ссылку для доступа в личный кабинет, в котором отображается статистика по зараженным узлам и осуществленным выплатам. Задача покупателя заключается в распространении трояна. Когда жертва атак с использованием данного экземпляра трояна оплачивает выкуп, продавец перечисляет выплату распространителю за вычетом своей доли. Обычно продавец оставляет себе 15–50%, а распространителю достается, соответственно, 50–85%. По такой схеме распространяются шифровальщики Gandcrab, Tantalus, Aleta, Princess, Rapid, Scarab, Sphinx, Lovecraft, Onyonlock и другие. Например, получивший за последний год широкое распространение шифровальщик Gandcrab только за апрель-май 2018 года принес злоумышленникам свыше 700 000 \$, при этом заражены оказались более 315 000 узлов.

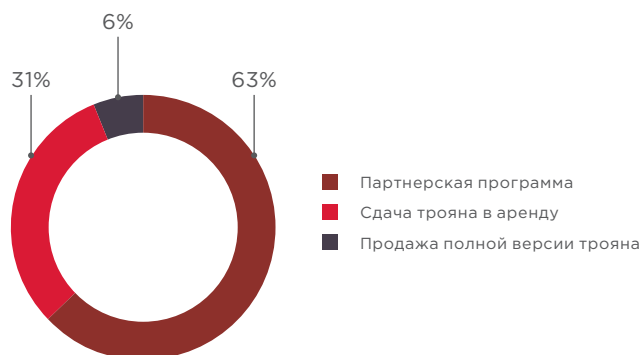


Рисунок 11. Предложения о продаже шифровальщиков

Как видно из диаграммы, на момент исследования именно партнерская программа наиболее широко представлена в данном сегменте рынка ВПО. Это вполне объяснимо, ведь злоумышленнику совершенно не придется заботиться о технических



аспектах, связанных с вредоносным ПО и инфраструктурой для его работы, а также обладать навыками программирования и взлома систем. При расходах от 90 \$ в месяц за доступ к сервису он получает готовый к рассылке троян, настроенный на его кошелек, который «отобьет» затраты уже после первой выплаты выкупа.

2.2. Эксплойты

Эксплойт — это программа или программный код, который, используя уязвимости в ПО, позволяет провести атаку на компьютерную систему.

Сведения об уязвимостях в ПО и эксплойты к ним высоко ценятся на теневом рынке. Так, например, на одной из площадок средняя цена на эксплойты, которые были представлены на продажу в 2017–2018 годах, составляла 2540 \$. Среди них 38% эксплойтов предназначались для уязвимостей в операционных системах семейства Windows или ПО, работающем под Windows. Пятая часть эксплойтов (19%) предназначена для кроссплатформенных технологий, таких как Java, Adobe Flash, с помощью которых злоумышленники могут атаковать не только пользователей ОС семейства Windows, но и Linux, Android, macOS. Доля эксплойтов для уязвимостей в самих ОС семейства macOS составила 5% от общего предложения, а стоимость варьировалась от 2200 \$ до 5300 \$.

2540 \$

средняя стоимость
эксплойта для веб-
и Windows-приложений

DATE	DESCRIPTION	TYPE	HITS	RISK	GOLD
11-04-2018	Hotmail.com reset account 0day Exploit	tricks	1 338	R D	B 0.329
12-01-2018	Instagram info disclosure (email + phone) 0day Exploit	tricks	6 028	R D	B 0.153
11-12-2017	iCloud reset mail Account Authentication Elevation Of Privilege 0day Exploit	tricks	4 799	R D	B 0.493
30-09-2017	GovRAT 2.0 - FUD unknown RAT with special functions	windows	2 444	R D	B 0.329
23-08-2017	Windows 10 RCE (Sandbox Escape/Bypass ASLR/Bypass DEP) 0day Exploit	windows	5 077	R D	B 0.658
17-07-2017	Google Chrome RCE + Sandbox Escape 0day Exploit	windows	11 859	R D	B 0.57
30-05-2017	Vanilla Forums 2.0.18.7 Remote Code Execution Exploit	php	4 797	R D	B 0.011
26-02-2017	Adobe Acrobat Reader DC Memory Corruption Remote Code Execution Exploit	windows	5 327	R D	B 0.175
26-02-2017	Adobe Flash Player MediaPlayer Out-Of-Bounds Access Remote Code Execution Exploit	windows	7 722	R D	B 0.164
26-02-2017	Adobe Flash Player MessageChannel Type Confusion Remote Code Execution Exploit	windows	2 918	R D	B 0.166
06-02-2017	Oracle Java AtomicReferenceFieldUpdater Type Confusion Remote Code Execution	java	3 538	R D	B 0.208
06-02-2017	Oracle Java Uninitialized Memory Remote Code Execution Vulnerability	java	2 651	R D	B 0.197
24-01-2017	Joomla 3.6.5 Remote code execution Exploit 0day	php	9 902	R D	B 0.362

Рисунок 12. Площадка для торговли эксплойтами

38%

предлагаемых эксплойтов
связаны с Windows и при-
ложениями под эту ОС

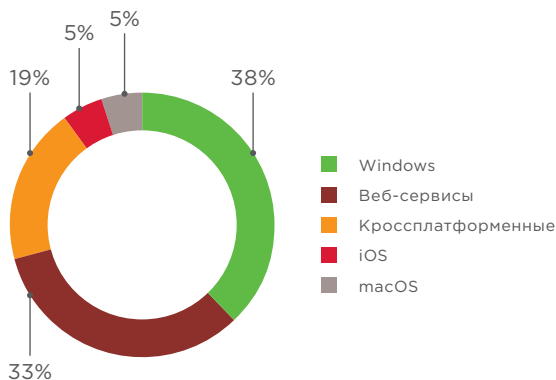


Рисунок 13. Категории эксплойтов

Наиболее ценными на теневом рынке являются эксплойты для уязвимостей нулевого дня: для таких уязвимостей производитель еще не выпустил обновление, исправляющее недостаток ПО. Но ситуация, когда обновление уже выпущено, а пользователи его не установили, встречается настолько часто, что злоумышленникам удается успешно использовать эксплойты для уже выявленных и опубликованных уязвимостей. При этом, по нашим данным, минимальный промежуток между публикацией деталей уязвимости и первыми попытками ее эксплуатации в 2017 году составлял всего три часа¹⁷.

¹⁷ ptsecurity.com/ru-ru/premium/web-attacks-2017/



Самый яркий пример прошлого года — ransomware-атака WannaCry, в результате которой количество зараженных устройств превысило 500 тысяч¹⁸, несмотря на то что обновление, устраняющее уязвимость, было доступно на сайте Microsoft за два месяца до атаки.

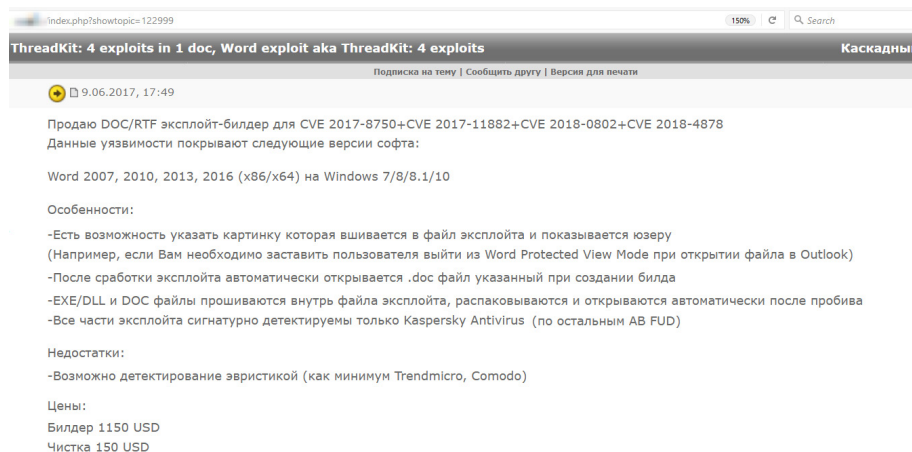


Рисунок 14. Продажа эксплойт-билдера

2.3. Данные

На теневой рынок данные попадают разными путями: например, от злоумышленников, которые целенаправленно выманивают у пользователей личную информацию и учетные данные от различных сервисов, или от преступных группировок, которые во время целевой атаки на компанию заодно раздобыли и базу данных ее клиентов.

Можно выделить следующие категории данных, которые продают и покупают на теневом рынке:

- логины и пароли от различных интернет-сервисов, например социальных сетей, онлайн-банков;
- данные банковских карт;
- персональные данные частных лиц, в том числе скан-копии документов, подтверждающих личность (паспортов, водительских удостоверений);
- финансовая отчетность компаний, скан-копии учредительных документов и другая конфиденциальная документация.

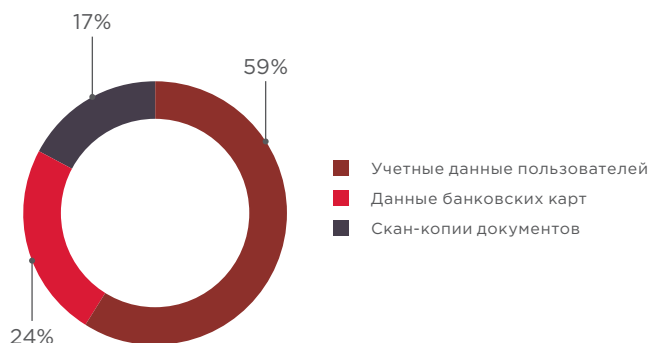


Рисунок 15. Типы продаваемых данных

¹⁸ [ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf](https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf)



Наиболее распространены в дарквебе объявления о продаже учетных данных пользователей к различным сервисам. Это неудивительно, учитывая, как часто в СМИ просачивается информация об утечках баз данных с паролями для доступа к тому или иному сервису в интернете. Большинство же подобных утечек не передается огласке.

**На 6 лет лишения
свободы со штрафом
450 000 ₽ осужден
преступник за кражу денег
со счетов клиентов банка
через систему ДБО¹⁹**

2.3.1. Учетные данные пользователей

Среди учетных записей наибольшую ценность для злоумышленников представляют логины и пароли пользователей платежных систем, онлайн-банков и криптовалютных бирж. Пароли от популярных онлайн-магазинов, таких как Ebay или Amazon, также пользуются спросом, ведь в личных кабинетах пользователей обычно уже привязаны банковские карты, что позволяет преступникам совершать покупки за чужой счет, или они используют эти торговые площадки для того, чтобы обналичить деньги с украденных банковских карт путем покупки товаров от чужого имени и их дальнейшей перепродажи.

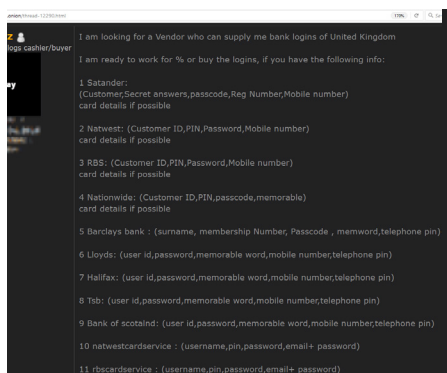


Рисунок 16. Объявление о покупке учетных данных для доступа к онлайн-банку

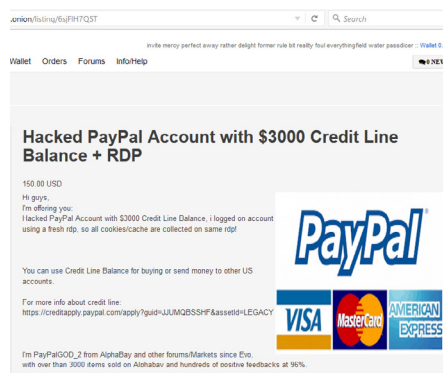


Рисунок 17. Учетные данные пользователя PayPal

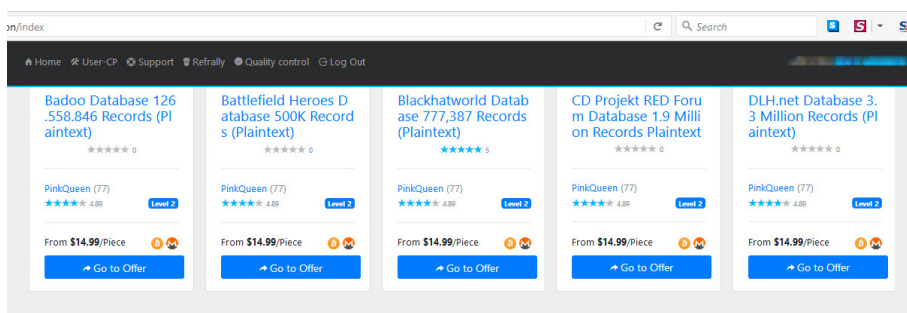


Рисунок 18. Продажа учетных данных пользователей различных сервисов

22 \$

средняя стоимость
данных пользователей
онлайн-банков

Большая часть учетных данных продается по цене до 10 \$. Отметим, что украденные аккаунты от социальных сетей и других интернет-сервисов продаются партиями от нескольких тысяч до нескольких миллионов записей. Цены за такие комплекты варьируются от десятков до сотен долларов.

Учетные данные для доступа к личным кабинетам в онлайн-банках продаются поштучно; при средней цене доступа в 22 \$ счета имеют баланс от нескольких десятков долларов до десятков тысяч.

¹⁹ goo.gl/VXUT8z



5840 \$

в среднем на взломанном
аккаунте пользователя пла-
тежной системы

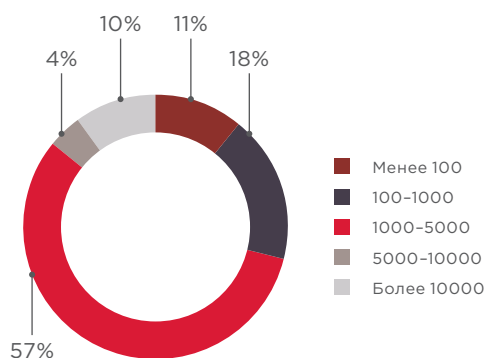


Рисунок 19. Распределение средств на взломанных счетах, \$

2.3.2. Данные банковских карт

Другая категория данных, которые продаются на теневом рынке, — это данные банковских карт. Их используют для получения денег следующими способами:

- покупая и продавая товары в интернете;
- обналичивая средства через платежные системы;
- изготавливая дубликаты банковских карт, которые потом можно использовать при снятии наличных денег из банкомата.

Bin	Card	Debit/Credit	Mark	Expires	Country	State	City	Zip	Phone	VBV	Birthday	Base	Price	Cart
525107	MASTERCARD BANCOBP BANK Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	DEBIT	PREPAID	07/2019	United States	OK	Moor	73160				Serpent	10\$	+
437303	VISA Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	DEBIT	PREPAID	04/2020	United States	OK	Oklahoma City	73117				Serpent	8\$	+

Рисунок 20. Площадка для продажи данных банковских карт

9 \$

стоимость данных одной
банковской карты

В первых двух случаях злоумышленнику может потребоваться код подтверждения, который банк-эмитент присылает владельцу в SMS-сообщении. Эту проблему также можно решить с помощью поставщиков теневых услуг, которые предоставляют детализацию звонков и SMS-сообщений по заданному номеру мобильного телефона. Текст SMS-сообщения, содержащего одноразовый код для проведения платежа, можно оперативно получить за 250 \$.

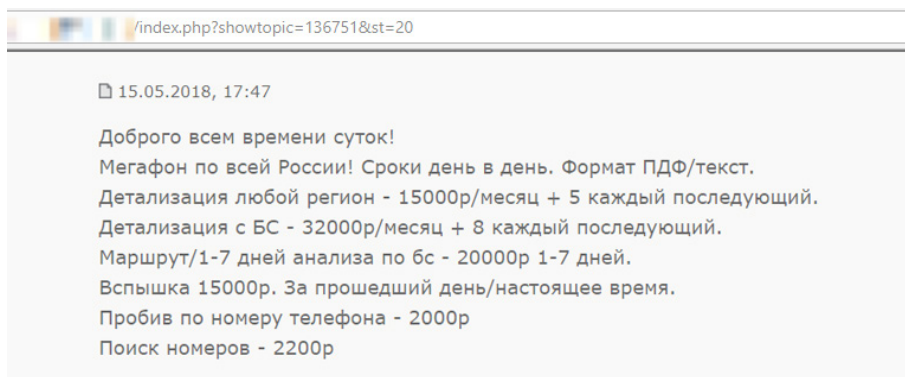


Рисунок 21. Услуги по предоставлению детализации звонков и перехвату SMS-сообщений

Данные одной банковской карты с балансом от нескольких сотен до нескольких тысяч долларов на счету продаются в среднем за 9 \$.

2.3.3. Скан-копии личных и конфиденциальных документов

Еще одна категория данных, которые можно купить или продать на теневом рынке, это скан-копии различных документов, среди которых:

- документы, удостоверяющие личность, содержащие персональные данные, — паспорта, водительские удостоверения, ИНН, СНИЛС и т. п.;
- финансовые документы, в том числе отчеты о кредитной истории граждан;
- скан-копии внутренних документов коммерческих компаний.

2 \$

средняя стоимость
отсканированной копии
паспорта

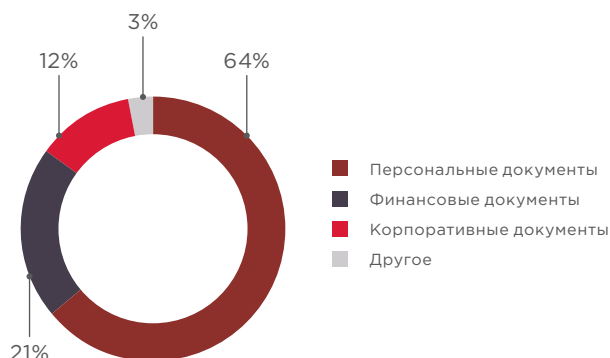


Рисунок 22. Типы продаваемых конфиденциальных документов

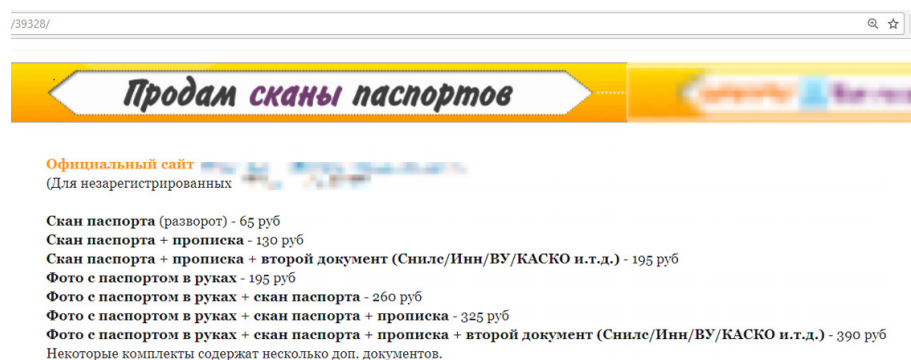


Рисунок 23. Продажа скан-копий паспортов

Паспортные данные используются злоумышленниками для регистрации в различных интернет-сервисах. Так, например, в системе «Яндекс.Деньги» переводить денежные средства другим пользователям системы можно при статусе кошелька начиная с «Именного». Чтобы получить этот статус, нужно предоставить данные паспорта, номер телефона, ИНН или СНИЛС. В этом случае злоумышленнику достаточно будет иметь на руках реальные паспортные данные любого человека. Остальную информацию он сможет получить из открытых источников (социальных сетей, ресурсов государственных органов). Такой кошелек не будет связан с личностью злоумышленника, что позволит ему производить расчеты с другими участниками теневого рынка от имени другого человека.



2.4. Доступы

«Доступами» в дарквебе называют сведения, с помощью которых можно осуществить несанкционированный доступ к сайту или серверу с последующей возможностью загрузки файлов или выполнения команд. Доступы могут быть использованы для различных целей.

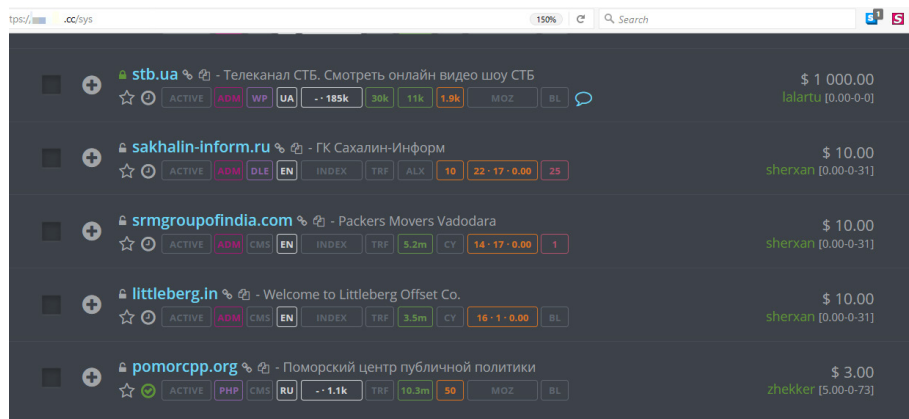


Рисунок 24. Биржа доступов к взломанным сайтам

Например, получив контроль над новостным сайтом, хакеры могут распространять с его страниц ВПО и заражать посетителей. Доступ к сайту интернет-магазина преступники могут использовать для кражи данных банковских карт клиентов. Сайты государственных учреждений чаще подвергаются DoS-атакам или дефейсу (изменению содержимого главной страницы ресурса).

Доступы к серверам и рабочим станциям чаще всего используются злоумышленниками для распространения троянов-шифровальщиков, а также в качестве точек входа в корпоративные информационные системы компаний при проведении целевых атак.

Отметим, что согласно результатам работ по внешнему тестированию на проникновение, проведенных специалистами Positive Technologies, несмотря на то что в 2017 году защищенность сетевого периметра корпоративных информационных систем осталась на уровне 2016 года, сложность атак существенно снизилась²⁰. Так, если в 2016 году сложность атаки оценивалась как тривиальная в 27% случаев, то в 2017 году — уже в 56%.

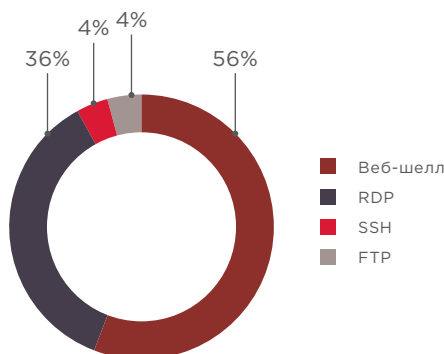


Рисунок 25. Типы запрашиваемых доступов

²⁰ ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-vulnerabilities-2018-rus.pdf

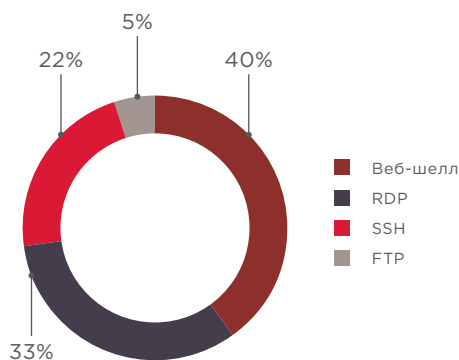


Рисунок 26. Типы предлагаемых к продаже доступов

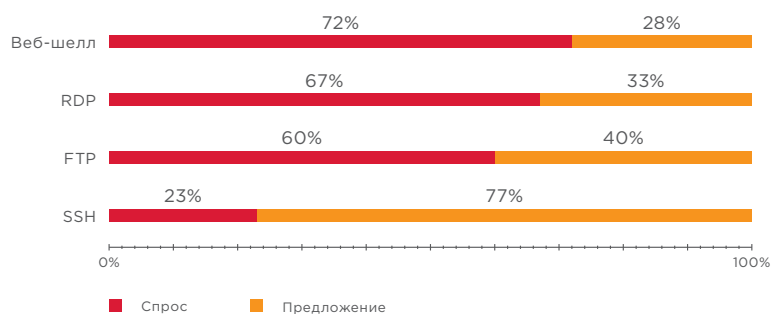


Рисунок 27. Соотношение спроса и предложения в торговле доступами

Наиболее популярный тип доступа — доступ к взломанному сайту в виде веб-шелла или учетных данных администратора системы управления содержимым сайта (CMS). Веб-шелл — это ранее загруженный через уязвимость в веб-приложении вредоносный скрипт, который обеспечивает злоумышленнику доступ к ОС сервера через страницу в браузере, часто с возможностью доступа и к базе данных. В большинстве случаев привилегии нарушителя, обладающего таким веб-шеллом, не превышают привилегий самого веб-приложения, и поэтому он может атаковать только сам сайт. Чтобы получить полный контроль над сервером, нарушителю придется повысить привилегии самостоятельно, используя уязвимости ПО.

Поскольку большое число сайтов разработано с помощью одинаковых технологий, то, например, обнаружение критически опасной уязвимости всего лишь в одной CMS позволяет автоматически атаковать сразу множество сайтов. В таком случае доступ к одному сайту, который позволит загружать на сервер файлы, могут продавать за 0,15 \$.

Если взломанный ресурс связан с финансами, криптовалютами, ICO или является интернет-магазином, то цены на такой доступ могут начинаться от нескольких сотен долларов и достигать нескольких тысяч.



Рисунок 28. Продажа доступа к сайту ICO



Доступ к серверу — это обычно адрес сервера и учетные данные пользователя для входа в систему по протоколам RDP или SSH. Небольшой спрос на SSH-доступы обусловлен тем, что этот протокол чаще всего используется для подключения к серверам под управлением ОС Linux, а злоумышленники традиционно привыкли атаковать компьютеры под управлением ОС Windows. Цены за учетные данные для доступа к одному узлу начинаются от нескольких долларов и могут достигать до нескольких сотен. Так, например, RDP-доступ к банкомату может стоить 500 \$.

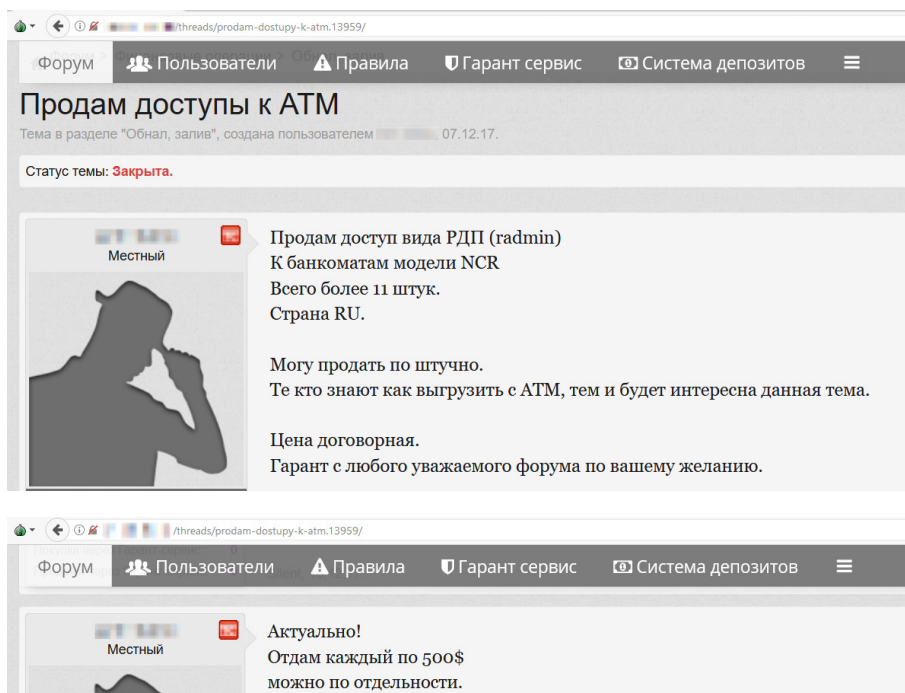


Рисунок 29. Продажа учетных данных для доступа по RDP к удаленным узлам

3. Услуги

Для подготовки атак злоумышленники часто прибегают к помощи третьих лиц. При этом наемные работники могут вовсе не знать об истинной цели их работы: им поручают узконаправленную задачу, после выполнения которой они получают обещанную сумму денег. Кроме услуг таких фрилансеров злоумышленников интересуют сервисы, предоставляющие инфраструктуру и ресурсы, которые необходимы для проведения атак (выделенные серверы, VPN, ботнеты и другие).

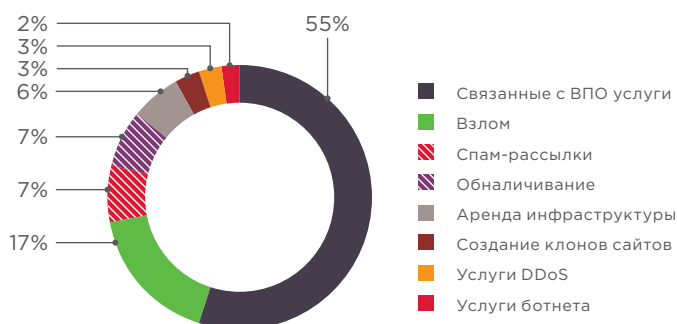


Рисунок 30. Спрос на услуги

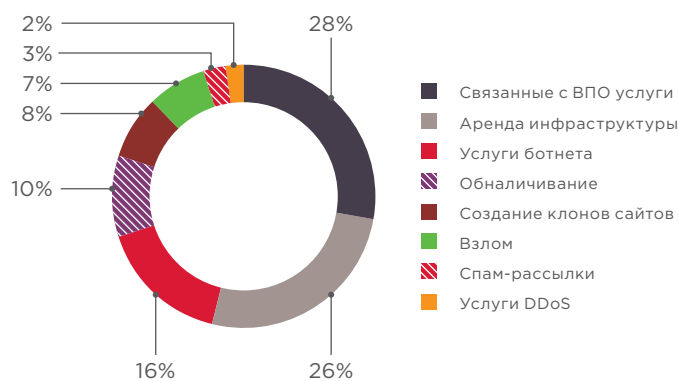


Рисунок 31. Предложение услуг

Наибольшим спросом в дарквебе пользуются услуги, связанные с созданием и распространением ВПО (55%), а также взлом почты, сайтов и удаленных серверов (17%). Предложения также чаще всего связаны с ВПО (28%). В то же время значительное количество предложений приходится на хостинги и VPN-сервисы (26%), сервисы по накрутке просмотров, лайков, постов и т. п., использующие ресурсы ботнетов (16%), и услуги по обналичиванию денег (10%).

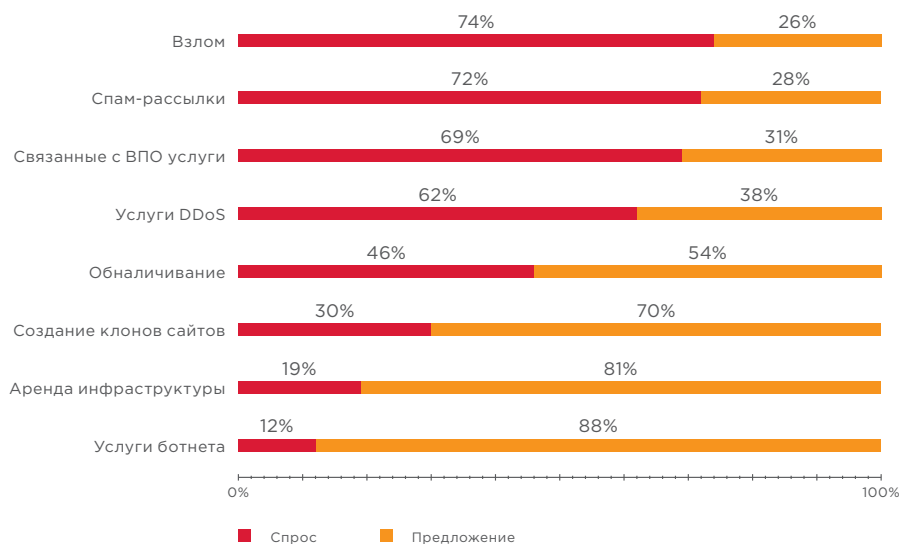


Рисунок 32. Соотношение спроса и предложения услуг на теневом рынке

3.1. Связанные с ВПО услуги

Когда готовых решений на рынке ВПО нет, а преступнику необходимо разработать специфический троян, он может или сделать это самостоятельно, или разместить объявление о поиске программиста для решения этой задачи. Как видно из диаграммы ниже, спрос на разработку ВПО втрое превышает существующее предложение, а это означает, что ежедневно преступники модифицируют методы атаки, ищут новые пути обхода средств защиты и более выгодные схемы преступлений. Кроме того, те программисты, которые вчера зарабатывали созданием ВПО на заказ, сегодня начинают переходить в категорию продавцов готовых решений, ведь это более выгодный бизнес.

Обфускация ВПО — приведение исполняемого кода с сохранением функциональности к виду, затрудняющему анализ, — обычно входит в стоимость услуги разработки, поэтому ее редко заказывают отдельно, но эта услуга все же присутствует среди предложений.



Аналогичным образом в дарквебе можно найти и сервисы, через которые вновь созданное ВПО будет распространяться. Спрос на распространение ВПО существенно превышает предложение. Если у преступника нет собственного ботнета, и он не хочет заниматься рассылкой по электронной почте, то ему необходимо найти соответствующие услуги на рынке.

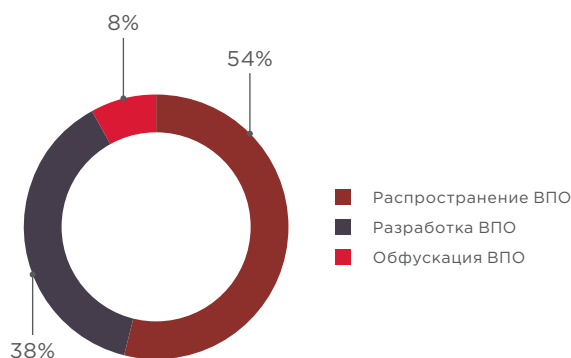


Рисунок 33. Спрос на услуги, связанные с ВПО

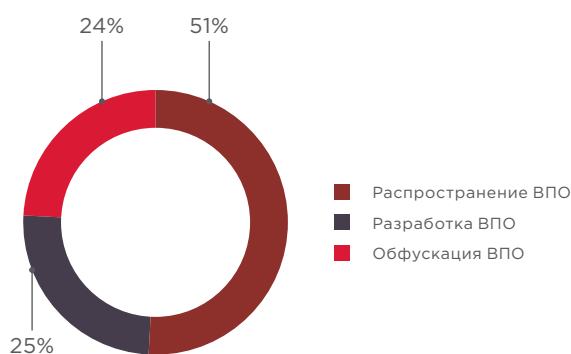


Рисунок 34. Предложение услуг, связанных с ВПО

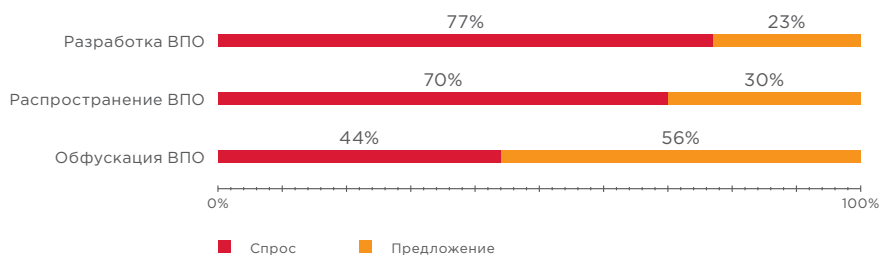


Рисунок 35. Соотношение спроса и предложения услуг, связанных с ВПО

3.1.1. Разработка ВПО

Услуги по разработке ВПО оцениваются на площадках дарквеба в среднем от 500 \$. Часто требуется не только разработка, но и реверс-инжиниринг (например, для создания нового ВПО на базе существующих, код которых невозможно получить ни из открытых, ни из закрытых источников).

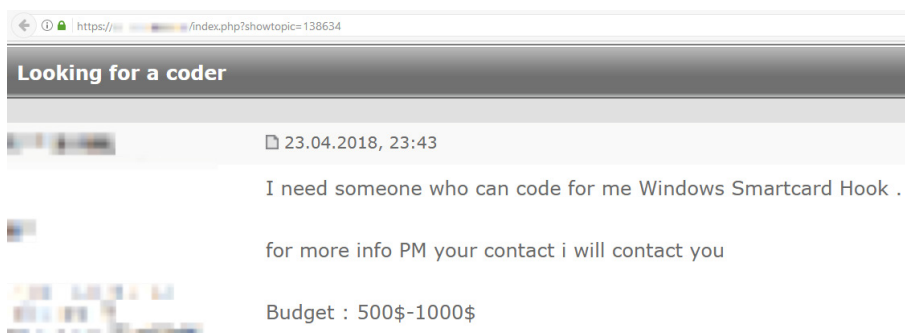


Рисунок 36. Поиск разработчика частного ВПО

На специализированных площадках предложения о работе для реверс-инженеров начинаются от 1000 \$ за проект.

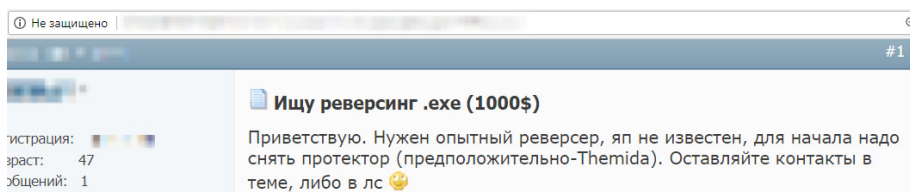


Рисунок 37. Поиск реверс-инженера

3.1.2. Обфускация ВПО

В дарквебе вокруг разработки ВПО сформировались несколько обслуживающих направлений, таких как упаковка, обфускация, шифрование исполняемых файлов и проверка файлов всеми возможными антивирусами. Задача сервисов и решений, реализующих эти направления, заключается в том, чтобы итоговый исполняемый файл не детектировался большинством популярных антивирусов, в идеальном случае — не определялся никакими из них как можно дольше.

Обычно подразумевается, что первичная «очистка», обфускация или шифрование файла, входит в стоимость ВПО. Дополнительные очистки стоят 5–10% от базовой стоимости ВПО. Если продавец-разработчик не занимается такой модификацией файлов, то покупатель всегда может воспользоваться сторонними услугами по обфускации, которые стоят в среднем 20 \$.

Существуют сервисы, которые позволяют за несколько центов проверить файл с помощью нескольких десятков антивирусов. Для тех, кому необходимо проверять большее количество файлов на регулярной основе, предлагается ежемесячная подписка от 25 \$.

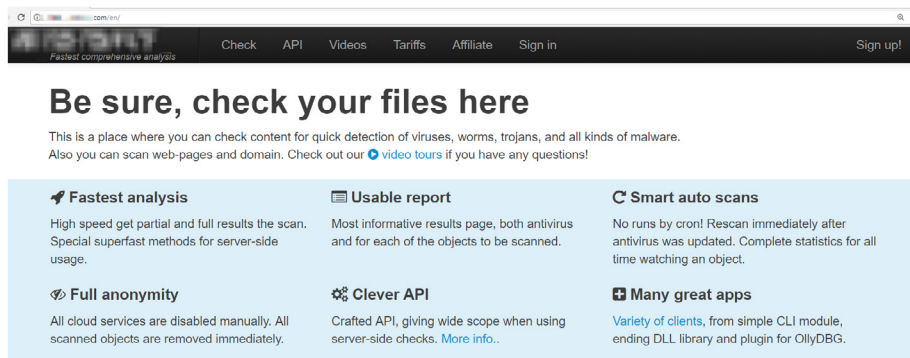


Рисунок 38. Анонимная проверка файла с помощью нескольких десятков антивирусов



3.1.3. Распространение ВПО

Для проведения кибератаки недостаточно иметь само ВПО, его необходимо еще доставить на компьютеры жертв. Злоумышленники могут распространять ВПО различными способами:

- в виде вложения в фишинговых письмах;
- через ссылку на скачивание файла в фишинговых письмах, SMS, сообщениях в мессенджерах и социальных сетях;
- в виде поддельных файлов якобы с обновлениями или утилитами, которые размещают на взломанных или подконтрольных злоумышленнику сайтах;
- через ботнет.

Для привлечения пользователей на зараженный ресурс злоумышленники пользуются услугами тех, кто продает трафик. Услуга, которая в среднем стоит около 15 \$, предполагает перенаправление потоков пользователей на сайт, подконтрольный злоумышленникам, с уже взломанного сайта с большой посещаемостью или через систему контекстной рекламы популярных поисковых систем.

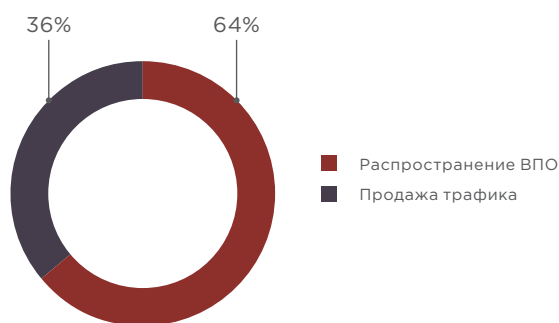


Рисунок 39. Спрос на услуги по распространению



Рисунок 40. Предложение услуг по распространению



Рисунок 41. Соотношение спроса и предложения услуг по распространению ВПО

Владельцы ботнетов предлагают в качестве услуги загрузку сторонних файлов на контролируемые устройства с последующим их запуском. Так, за 50 \$ можно загрузить файл на 1000 случайных узлов, а за сумму около 400 \$ можно выбрать географическое расположение этих узлов. Такими сервисами пользуются группировки, которые атакуют компании определенной сферы деятельности. Например, если готовится атака на банки, у владельца ботнета запрашивают список IP-адресов зараженных устройств и выбирают узлы, относящиеся к финансовым организациям и их контрагентам.

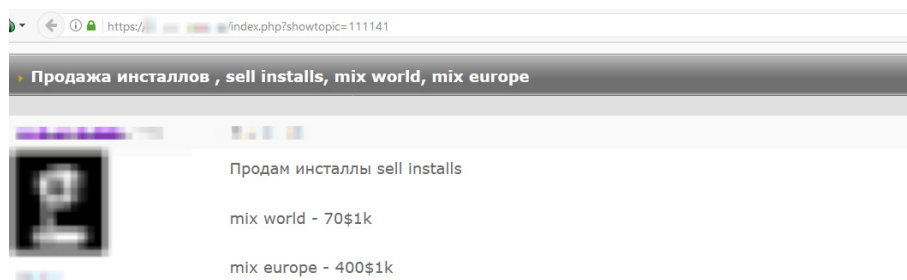


Рисунок 42. Услуги ботнета по загрузке и установке ВПО на ботов

Для успешной фишинговой атаки преступнику часто необходимо создать сайт, который он будет использовать либо для распространения ВПО, либо для кражи учетных и платежных данных пользователей. Создание простой копии сайта на теневом рынке обойдется в 50–150 \$, тогда как продвинутый вариант с формами аутентификации, проверяющими вводимые данные и перенаправляющими пользователя после атаки на оригинальный сайт (чтобы не вызывать подозрений), будет стоить свыше 200 \$. При этом, согласно оценке осведомленности сотрудников в вопросах ИБ, которую проводили наши специалисты, в 27% случаев злоумышленники достигают успеха, рассылая фишинговые письма со ссылками на веб-ресурс с запросом учетных данных²¹.

Наиболее актуальный пример: в 2017 году получил распространение метод атаки на ICO с помощью клонирования официального сайта проекта одновременно с массовой рассылкой фишинговых писем. Пользователи заходили на такой ресурс и перечисляли криптовалюту на указанные ложные адреса кошельков. Тем самым, вместо вложения средств в проект, потенциальные инвесторы спонсировали преступников. Таким был проект BeeToken ICO в начале 2018 года, в ходе которого злоумышленникам удалось украсть более 1 000 000 \$ в криптовалюте Ethereum²².

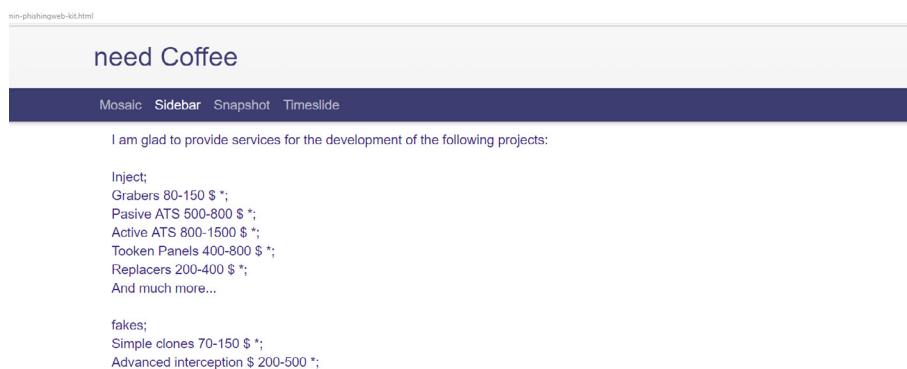


Рисунок 43. Стоимость услуг по разработке фишингового сайта

21 ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf
22 medium.com/@MikeBacina/buzz-off-ico-phishing-scams-44b8e5620211



3.2. Инфраструктура

В интернете широко представлены легальные коммерческие провайдеры VPN-сервисов, регистраторы доменов и хостинг-провайдеры. Услуги таких провайдеров злоумышленники могут купить за относительно небольшие деньги, регистрируясь по чужим паспортным данным.

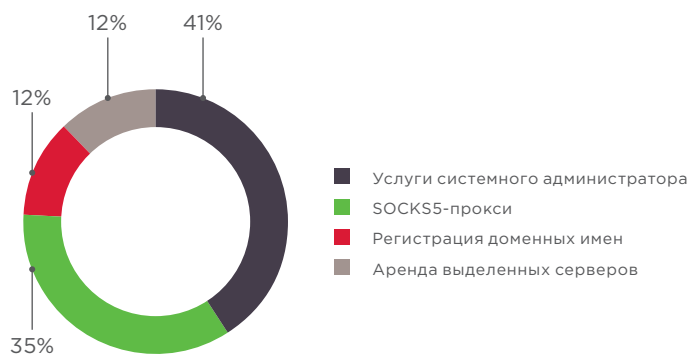


Рисунок 44. Типы запрашиваемых услуг, связанных с инфраструктурой

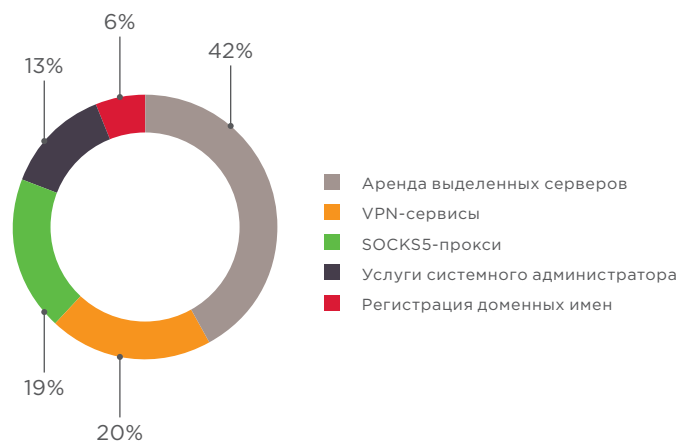


Рисунок 45. Типы предлагаемых услуг, связанных с инфраструктурой

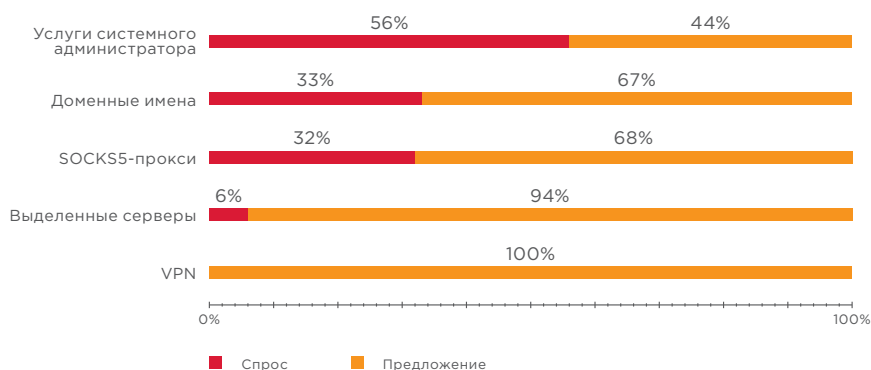


Рисунок 46. Соотношение спроса и предложения услуг, связанных с инфраструктурой

При проведении кибератак злоумышленники используют как легальные, так и нелегальные VPN-сервисы для обеспечения своей анонимности. Основным критерий, по которому киберпреступники выбирают сервис, — отсутствие системы учета пользователей сервиса, то есть фактическое отсутствие записей, позволяющих восстановить соответствие между IP-адресом и конкретным пользователем.



Цена на коммерческие VPN-сервисы начинается от 5 \$ в месяц, если не брать в расчет сезонные скидки и прочее. Однако некоторые пользователи отдадут предпочтение более дорогим сервисам, стоимость которых составляет от 15 \$ в месяц, рассчитывая на их надежность. Такие сервисы легальны и открыто размещаются в интернете, тем не менее их реклама может присутствовать и на форумах в дарк-вебе, где одни преступники оставляют отзывы об опыте использования тех или иных VPN-сервисов, что подталкивает других преступников к такому же выбору.

Аналогично обстоит дело с арендой выделенных серверов, которые используются злоумышленниками в качестве командных центров для вредоносного ПО, хостинга сайтов или промежуточных узлов, с которых осуществляется атака. Владельцы сдают такие серверы в аренду на темных форумах по ценам от 80 \$ в месяц.

Помимо аренды хостинга для создания фишингового сайта злоумышленнику необходимо доменное имя, которое можно получить за 3–10 \$, воспользовавшись услугами регистратора. Обычно при покупке домена регистратор проверяет паспортные данные пользователя, который обращается с такой заявкой. Однако, как мы отмечали выше, покупка скана паспорта не составляет для злоумышленника большой проблемы.

Некоторые сервисы принимают оплату за регистрацию домена в криптовалюте — при том, что криптокошелек создается за пару минут и не содержит информации о владельце, что также позволяет сохранять анонимность. Такие сервисы объяснимо пользуются заметным спросом.

3.3. Спам и фишинг

Сегодня практически не осталось пользователей интернета, которые не сталкивались с фишингом или спам-рассылками.

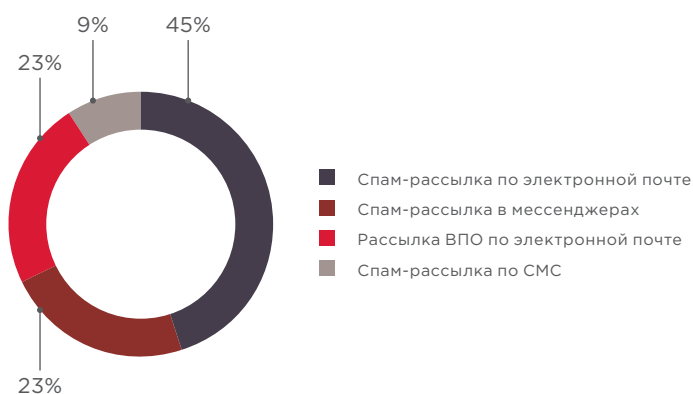


Рисунок 47. Спрос на услуги по рассылкам

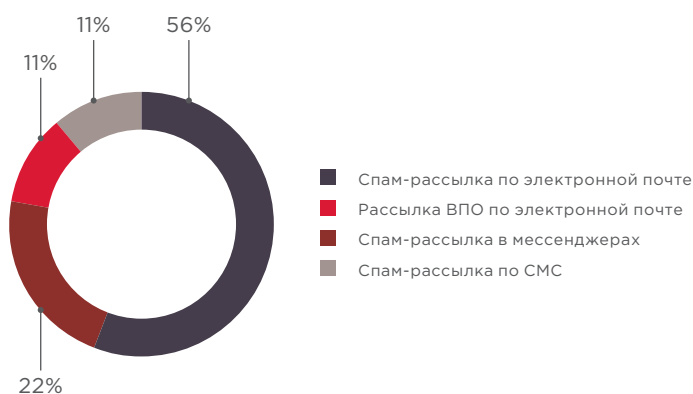


Рисунок 48. Предложение услуг по рассылкам



Рисунок 49. Соотношение спроса и предложения услуг по рассылкам

Чтобы расширить число потенциальных жертв, преступники нередко пользуются предложениями по проведению массовых почтовых рассылок, которые можно встретить на специализированных форумах. Сегодня меньше чем за 1 \$ можно отправить письмо с необходимым текстом и вложенным файлом сразу на 1000 случайных адресов. Разумеется, существуют сервисы, предлагающие рассылки с учетом определенной тематики, которая может быть интересна определенной группе пользователей. Это настоящий бизнес, ведь в результате заражения компьютеров с помощью трояна-вымогателя выплата выкупа даже одной жертвой многократно окупает расходы на рассылку.

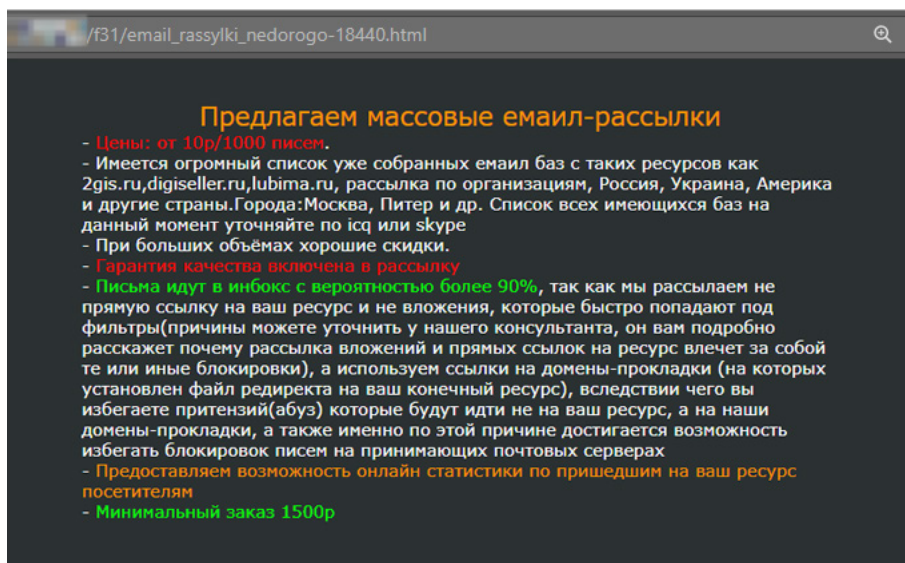


Рисунок 50. Предложение о массовых рассылках электронных писем

3.4. Взлом на заказ

Хакеры в сознании широкой публики ассоциируются с теми, кто взламывает серверы госучреждений и крупных компаний. В реальности большая часть запросов о взломе в дарквебе имеет отношение к поиску уязвимостей на сайтах (36%) и получению паролей от электронной почты (32%). При этом специалиста, который сможет провести атаку на удаленный сервер, ищут всего 23% посетителей теневых площадок. Среди предлагаемых услуг лидируют взлом учетных записей социальных сетей и электронной почты (по 33%). С одной стороны, это связано с желанием одних людей получить доступ к переписке других, а с другой, эти «взломы» меньше других требуют от атакующего каких-либо технических навыков.

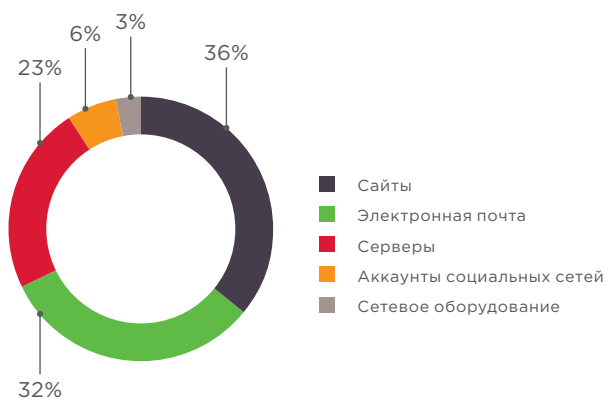


Рисунок 51. Спрос на услуги по взлому

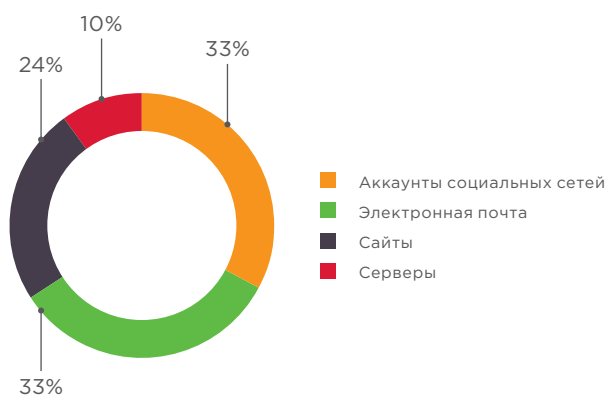


Рисунок 52. Предложение услуг по взлому

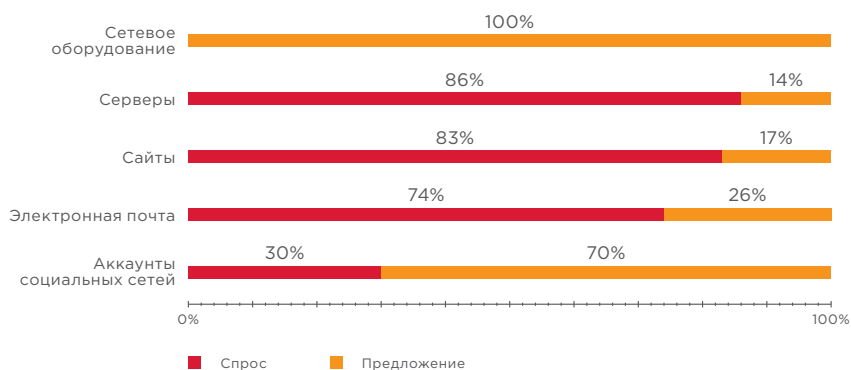


Рисунок 53. Соотношение спроса и предложения услуг по взлому

На 1,5 года ограниче-
ния свободы осужден
злоумышленник за кражу
учетных данных от почто-
вых сервисов²³

3.4.1. Взлом электронной почты и аккаунтов социальных сетей

На теневых сайтах услуги взлома почтовых ящиков и учетных записей в популяр-
ных социальных сетях стоят от 40 \$.

Существует множество причин, по которым хакерам и их клиентам может потре-
боваться доступ к чьему-то почтовому ящику или учетной записи в социальной
сети. Одни хотят получить доступ к частной переписке известных лиц, другие
к конфиденциальной информации конкурентов по бизнесу, третьи просто хотят
контролировать своих знакомых или родственников.

²³ goo.gl/vVbJzL

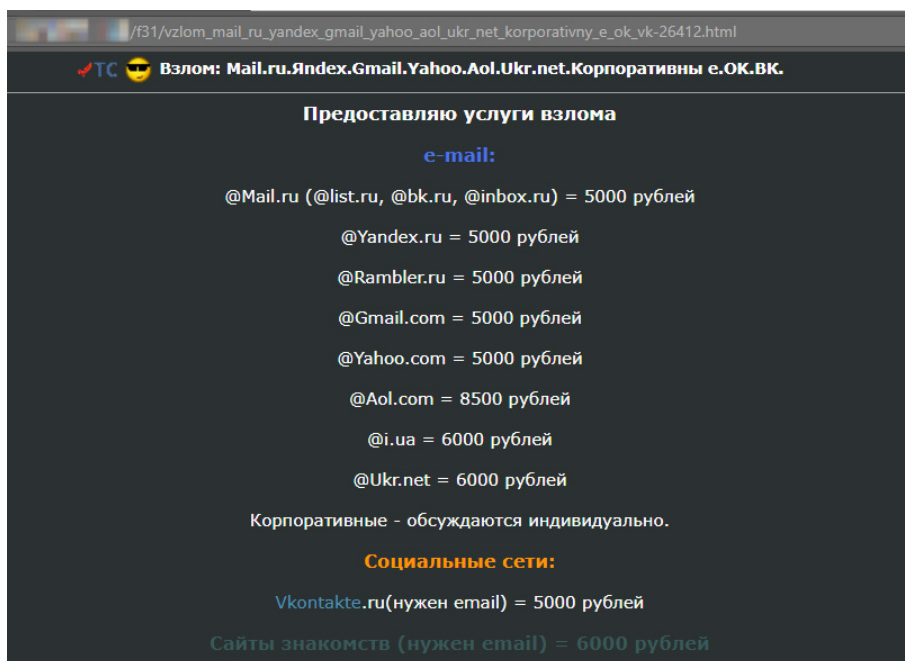


Рисунок 54. Взлом почтовых ящиков

Кроме того, доступ к электронной почте автоматически позволяет получить контроль над всеми личными кабинетами пользователя на различных сайтах, где данная почта использовалась для регистрации аккаунта: это могут быть социальные сети, форумы, интернет-магазины, электронные кошельки и другие сервисы. Нарушителю достаточно отправить на эти сайты запрос на восстановление пароля и сменить его на собственный, перейдя по ссылке в письме. Таким образом, злоумышленникам намного проще и эффективнее взломать всего один аккаунт от почты, чем пытаться похищать учетные данные от множества различных сервисов, принадлежащих одному человеку, поэтому эта услуга пользуется спросом.

3.4.2. Взлом сайтов, серверов, сетевого оборудования

Цели получения контроля над сайтами могут быть различными: получение доступа к базе данных пользователей, размещение на сайте вредоносного контента, проверка собственных хакерских навыков или заявление о себе, своих политических взглядах (например, с помощью дефейса). Для осуществления атаки преступникам необходимо получить контроль над сайтом либо проэксплуатировать отдельные уязвимости в веб-приложении. Учитывая крайне низкую защищенность большинства ресурсов в интернете, сделать это несложно.

Услуги по взлому сайтов оказывают как хакеры-одиночки, так и целые группировки. В дарквебе цена за взлом одного веб-ресурса начинается от 150 \$. Самая высокая цена на исследованных торговых площадках не превышала 1000 \$.

В 2017 году взломщики сайтов сосредоточили свое внимание на криптовалютных проектах — биржах и компаниях, проводящих ICO. Так, например, заменив на сайте проекта, вышедшего на ICO, всего лишь номер кошелька, злоумышленники перенаправляли миллионы долларов инвесторов в криптовалюту в свои кошельки. Взлом веб-ресурсов является не только наиболее распространенным способом атаки на ICO, но и наиболее успешным: в ходе работ по анализу защищенности ICO, которые провели наши специалисты, в 32% проектов обнаружилось уязвимость веб-приложений²⁴.

²⁴ ptsecurity.com/upload/corporate/ru-ru/analytics/ICO-Threats-rus.pdf

²⁵ goo.gl/ykvZ1D

10 000 ₽ штрафа

назначили студенту за
попытку атаки на сайт
госучреждения²⁵

Кроме того, уязвимые сайты могут быть использованы нарушителями для размещения на них ВПО для последующих целевых атак. Владельцы подобных сайтов тем самым неумышленно становятся звеном в цепочке атаки. Подобную технику использовала группировка Cobalt, методы которой описаны в одном из наших отчетов²⁶.

Не стоит забывать и о хактивистах, которые взламывают сайты государственных учреждений для того, чтобы провести дефейс — подмену содержимого на главной странице.

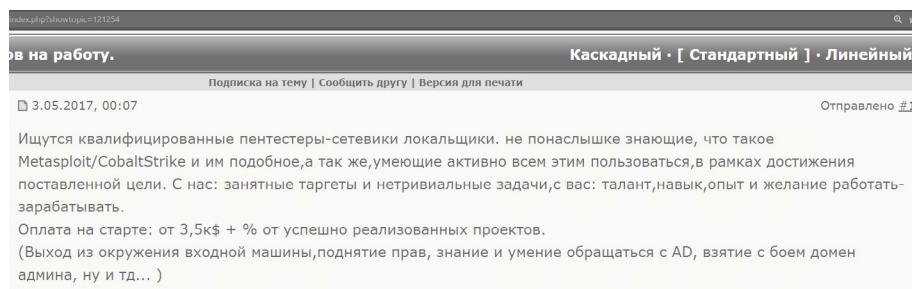


Рисунок 55. Набор хакеров в команду

Работа специалистов, которые взламывают серверы с помощью ВПО, подбирающего пароли, оценивается в 150–250 \$ в неделю. Полученные таким образом доступы продаются на теневых торговых площадках или монетизируются самими злоумышленниками, например с помощью криптомайнеров или шифровальщиков.

Аналогичным образом получают доступ к сетевому оборудованию: пользователи часто забывают менять установленные производителем пароли, что позволяет злоумышленникам с легкостью их подбирать. Чаще всего взломанные устройства заражают специальным ВПО и подключают к ботнету, который затем используют в DDoS-атаках.

Серьезные группировки киберпреступников часто ищут специалистов, обладающих глубокими техническими навыками в области поиска уязвимостей и взлома сетевых ресурсов. На исследованных площадках мы встречали объявления, в которых людям с такими компетенциями предлагали зарплату от 3000 \$. При этом сами группировки оказывают услуги по взлому, включающие атаки на веб-серверы и инфраструктуру, стоимость которых начинается от 500 \$ за одну атаку.

3.5. Дропы, обналичивание и инсайдеры

Практически все кибератаки в конечном счете совершаются с целью обогащения. Это подтверждается статистикой наших исследований, которая говорит о том, что 70% кибератак в 2017 году было совершено ради получения финансовой выгоды²⁷. Однако грязные деньги, полученные в результате киберкриминальной деятельности, злоумышленники не могут сразу перевести себе на банковскую карту. Поэтому преступникам приходится прибегать к ряду существующих на теневом рынке услуг, связанных с финансами.

Перевод средств через платежные системы — услуга, пользующаяся наибольшим спросом (52%) и при этом наиболее широко представленная в числе предложений (35%). Часто злоумышленники пользуются ею для хищения денежных средств с привязанных к аккаунтам платежных систем банковских карт пользователей. Средняя комиссия, которую берут такие сервисы, составляет 20% от суммы перевода.

²⁶ ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-2017-rus.pdf

²⁷ ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf

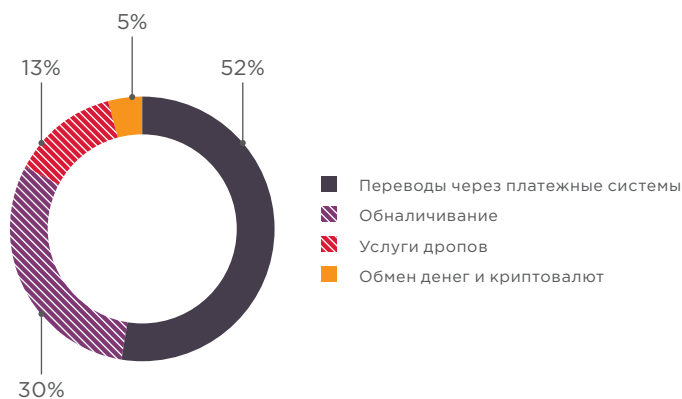


Рисунок 56. Спрос на финансовые услуги

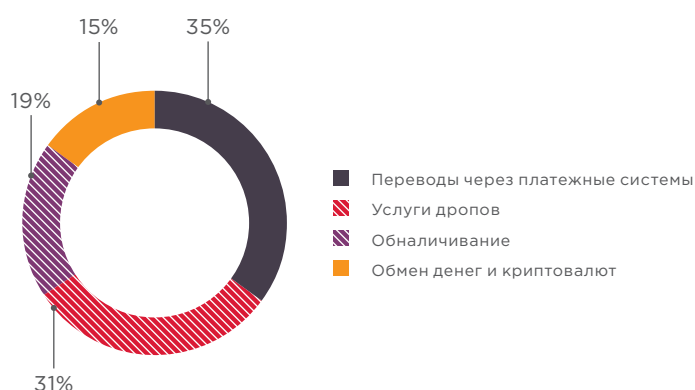


Рисунок 57. Предложение финансовых услуг

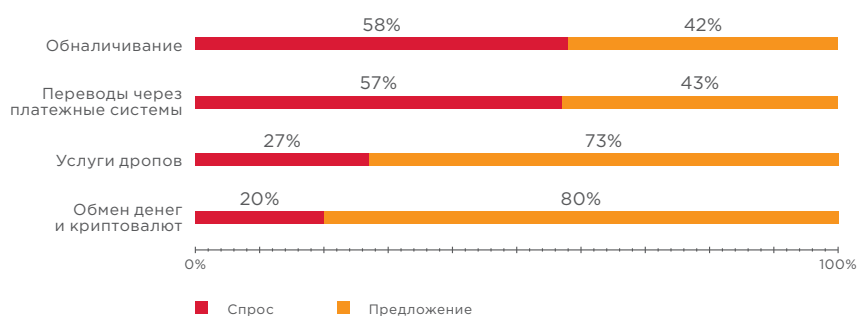


Рисунок 58. Соотношение спроса и предложения финансовых услуг

Для реализации различных схем по обналичиванию денег или осуществлению другой мошеннической деятельности преступникам нужны сообщники в финансовых организациях. Например, сотрудник салона связи может потребоваться для идентификации пользователя кошелька в одной из платежных систем. Работник банка может иметь доступ к базе клиентов, содержащей информацию о вкладчиках и заемщиках. Были случаи, когда банковские сотрудники выпускали карты к счетам клиентов без их ведома и согласия²⁸.

28 47news.ru/articles/83569/

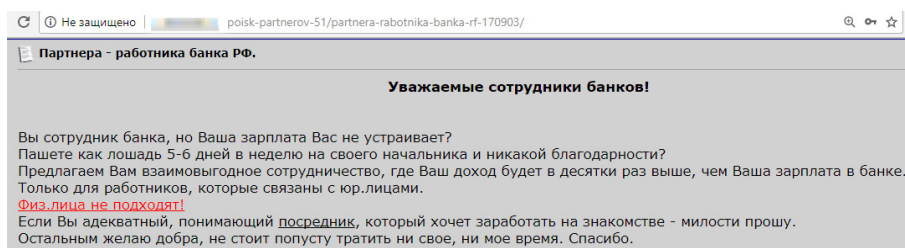


Рисунок 59. Поиск сотрудников

В ситуациях, когда дальнейшие действия требуют подтверждения личности либо существует высокий риск разоблачения, преступники обращаются к услугам людей, которых называют дропами. Дропы — это подставные лица, которые за несколько тысяч рублей выполняют «грязную» работу вроде снятия денег из банкомата с дубликатов карт, регистрации на свое имя юридического лица, получения и пересылки почтовых отправлений и т. п.

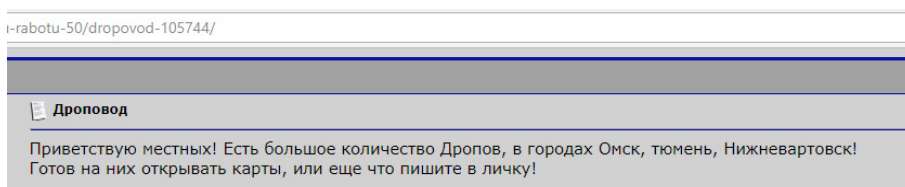


Рисунок 60. Дроповод с дропами

Для того чтобы сохранить свою анонимность, киберпреступники не выводят денежные средства непосредственно на свои криптокошельки или банковские счета. Например, если злоумышленник хочет перевести криптовалюту с одного кошелька на другой таким образом, чтобы операции невозможно было проследить, то он может воспользоваться услугами так называемых биткойн-миксеров. Денежные средства в криптовалюте с первого кошелька переводятся на кошелек сервиса, затем указывается адрес второго кошелька, на который необходимо зачислить эти средства. На указанный адрес криптовалюта поступает уже с заранее неизвестных непредсказуемых адресов. Владельцы таких сервисов используют особенности работы криптовалютных бирж и букмекерских контор для запутывания транзакций.

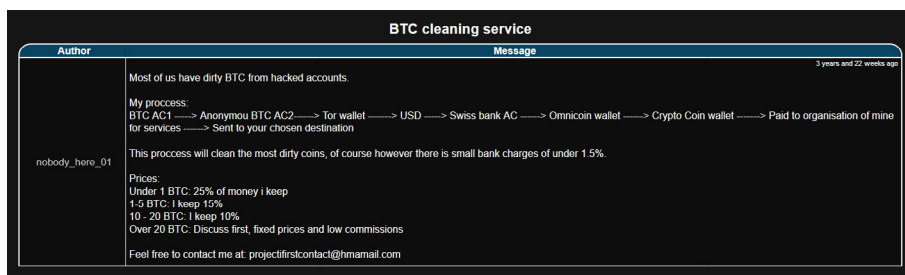


Рисунок 61. Очистка денег

Переводам, отмыванию и обналичиванию денег с банковских счетов посвящены целые теневые форумы. Существует множество схем, связанных с казино, букмекерскими конторами, подставными юридическими лицами, и в данном исследовании они не рассматриваются.

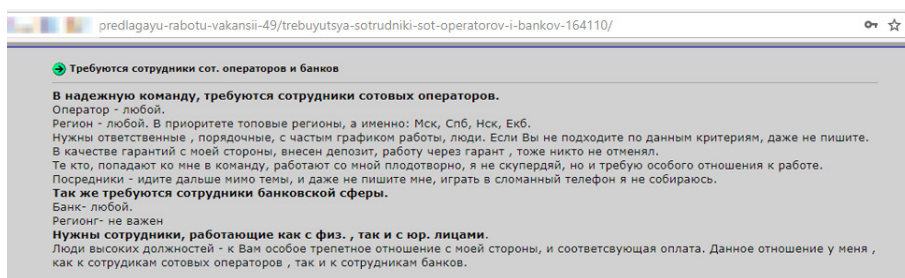


Рисунок 62. Поиск сотрудников банков для «обналички»

3.6. Ботнет

В общем случае ботнетом является объединенная группа зараженных специальным трояном устройств, которые могут выполнять определенные действия по команде из единого центра управления. Наиболее безобидным применением ботнета можно назвать накрутку лайков и просмотров, которые ценятся как обычными пользователями, так и теми, кто на этом зарабатывает, — профессиональными блогерами и различными интернет-компаниями.

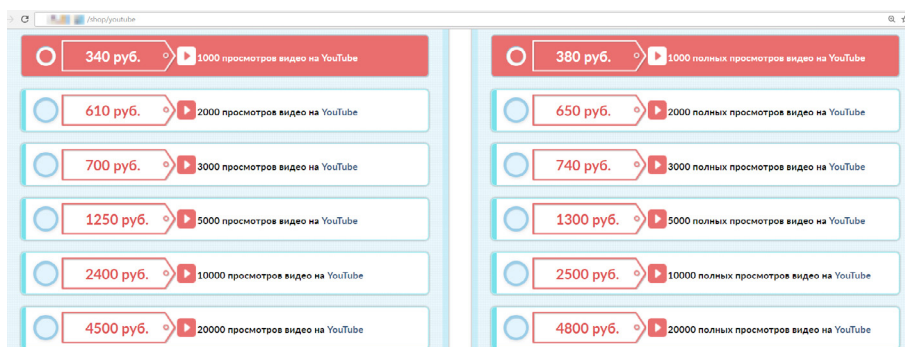


Рисунок 63. Накрутка просмотров видео на популярной платформе

Так, например, поставить ботом один лайк на популярной видеоплатформе стоит от 0,1 ₽, в то же время один голос в рейтинге ожидания на популярном ресурсе о кинофильмах будет стоить уже от 6 ₽.

Также ресурсы ботнета можно использовать для майнинга криптовалюты. Огромных денег это, конечно, не приносит, но простаивающий ботнет не приносит денег вовсе. Если считать, что один бот может «майнить» криптовалюту Monero с производительностью 40 хешей в секунду, что на момент проведения данного исследования эквивалентно доходу в 2 \$ в месяц, то ботнет из 1000 компьютеров увеличит доход злоумышленника на 2000 \$ в месяц.

В целом сценарии использования ресурсов ботнета ограничены только возможностями вредоносного ПО, которое контролирует зараженные узлы, и фантазией злоумышленников.

3.7. DDoS

Один из способов эксплуатации ботнета, который стоит выделить отдельно, — организация DDoS-атак. В дарквебе доступен широкий выбор автоматизированных сервисов и предложений от хакерских команд по проведению DDoS-атак любой сложности. Например, DDoS-атака на сайт мощностью в 270 Гбит/с в течение суток стоит около 50 \$.

На 2 года лишения свободы осужден хакер, проводивший DDoS-атаки²⁹

²⁹ goo.gl/x8nJPn



DDoS-атаки — один из популярных инструментов недобросовестной конкуренции. Так, по данным Neustar³⁰, ущерб от каждого часа атаки для трети американских компаний составляет 250 000 \$.

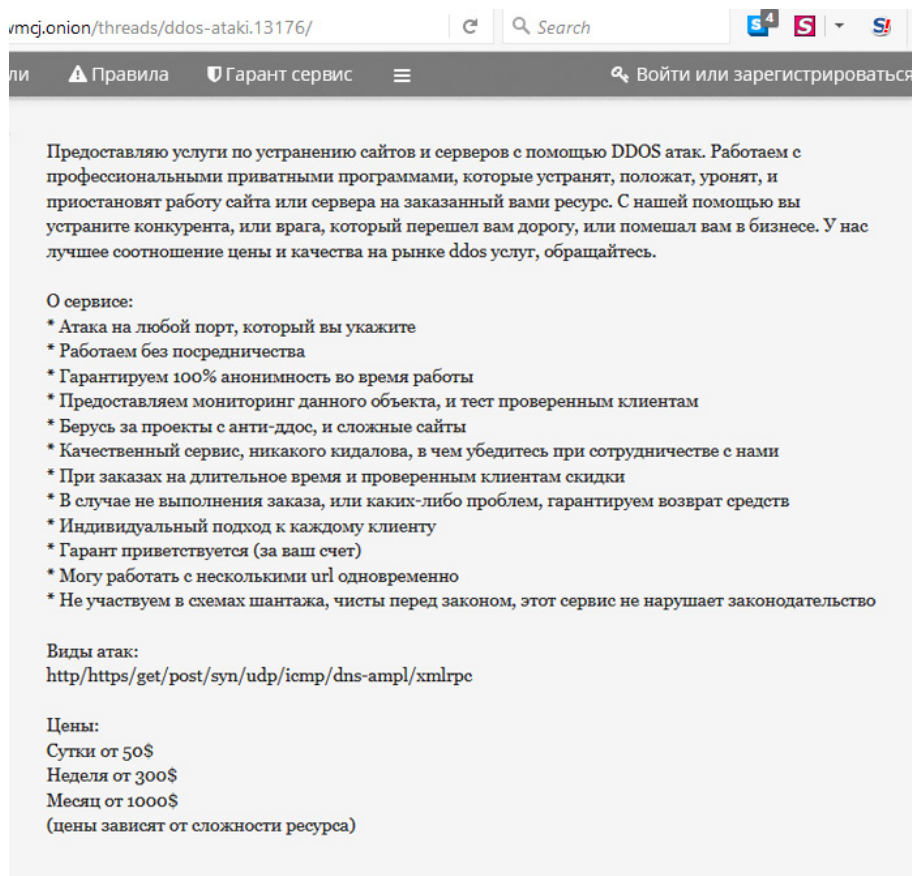


Рисунок 64. Предложение услуг по проведению DDoS-атак

³⁰ hello.neustar.biz/2017/10-Security-Solutions-Siteprotect-DDoS-2H2017-Report-LP.html



Выводы

За первый квартал 2018 года число уникальных инцидентов выросло на 32% по сравнению с аналогичным периодом 2017 года, и при этом в 63% инцидентов фигурировало ВПО. Проведенное исследование показало, что спрос на услуги по созданию ВПО на сегодняшний день превышает предложение в три раза, а по распространению в два раза. Такое положение дел позволяет говорить о запросе со стороны киберпреступников на новые инструменты, которые становятся все доступнее благодаря партнерским программам, сервисам по аренде ВПО и модели распространения «как услуга».

Эта тенденция не только способствует росту числа киберинцидентов, но и уже создает серьезные проблемы с атрибуцией злоумышленников при расследовании инцидентов. Очевидная атрибуция возможна в случае с теми злоумышленниками, которые самостоятельно разрабатывают эксклюзивные эксплойты и ВПО или заказывают такой эксклюзив.

При этом может получиться, что совершенно разных преступников ошибочно причислят к одной группировке из-за того, что они покупают одни и те же сервисы и ВПО на теневом рынке. То же касается и определения страны атакующего. То, что в ВПО проставлены комментарии на каком-либо определенном языке или письма написаны с ошибками, может свидетельствовать только о том, что ВПО написал носитель этого языка и продал его неизвестно кому, а фишинговые письма писал малограмотный школьник, промышляющий простейшими киберуслугами на форуме.

Все это может привести к тому, что threat intelligence станет крайне сложным процессом, а возможно, и бессмысленным, так как доверять на 100% результатам атрибуции станет нельзя. А раз так, то в нынешнем своем виде threat intelligence перестанет существовать, и с индикаторов компрометации акцент сместится на анализ дарквеба, чтобы выявлять по индикаторам не атакующую группу, а разработчика или продавца ВПО. И уже исходя из того, кто у кого и что покупал, — строить предположения об атакующей группировке. Эти методы уже зарекомендовали себя как эффективные и активно применяются.

Одновременно следует понимать и более детально анализировать техники и тактики, которые применял злоумышленник при организации атаки. Зачастую можно сделать выводы о квалификации злоумышленника не по тому инструментарию, который он использовал, а по тем ошибкам, которые он совершает на этапах постэксплуатации, или особенностям поведения во взломанной инфраструктуре. К сожалению, многие компании по ряду причин не готовы в случае взлома и крупных инцидентов проводить расследования — с поиском всех артефактов, восстановлением цепочки атаки и анализом действий злоумышленников в инфраструктуре. Но в тех случаях, когда высококлассная команда выполняет подобные работы и по их итогам предлагает рекомендации по защите инфраструктуры, это на порядок повышает защищенность организации, а также усложняет и удорожает ее взлом для злоумышленников в будущем.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.