

Как хантят IT-специалистов в даркнете

Переход на
темную сторону

Ключевые результаты

Мы публикуем результаты исследования теневой биржи труда, основанного на информации из различных киберкриминальных ресурсов даркнета

Для исследования было отобрано 155 форумов в даркнете, в которых присутствовали обсуждения тем поиска и предложения работы за период с января 2020 года по июнь 2022 года. В анализе участвовали только те объявления, в которых содержалась информация о продолжительной или постоянной работе.

В нашем исследовании мы расскажем об особенностях такого трудоустройства, условиях работы, требованиях по отбору соискателей, уровне зарплат и разберем специфику наиболее востребованных IT-профессий в даркнете.



Более 800

объявлений было проанализировано

- Резюме — 26%
- Вакансии — 74%



1300-4000\$

медианные зарплаты IT-специалистов



Март 2020

пик по количеству опубликованных объявлений



Основной работодатель

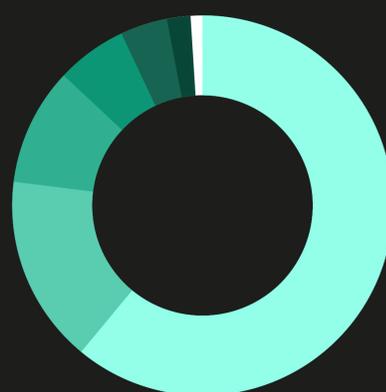
Команды хакеров и APT-группировки, которые ищут людей, способных заниматься разработкой вредоносного кода и его распространением, создавать и поддерживать IT-инфраструктуру и прочее.

Самые высокооплачиваемые специалисты

Разработчики возглавили список самых оплачиваемых профессий среди IT-специалистов в даркнете: их заработная плата может достигать 20 000 USD в месяц. В то же время **самая высокая медианная зарплата** (4000 USD) — в объявлениях о поиске специалистов по реверс-инжинирингу.

Самые востребованные специалисты

Чаще других в даркнете ищут **разработчиков** — 61% объявлений.



- Разработчики — 61%
- Атакующие — 16%
- Дизайнеры — 10%
- Администраторы — 6%
- Реверс-инженеры — 4%
- Аналитики — 2%
- Тестировщики — 1%



Теневая биржа труда

Даркнет — это общее название для различных ресурсов и площадок, которые объединяют людей, готовых к противозаконной работе или работе в юридически серых зонах. На теневых форумах можно встретить самые разные предложения: о нелегальной продаже и покупке украденных данных, об оказании услуг по написанию вредоносных программ и взлому различных сервисов, о поиске единомышленников для реализации атак на различные компании и многое другое.

Киберпреступному бизнесу, как и любому другому, необходимы работники. Сотрудников для участия в кибератаках и иной преступной деятельности ищут там же, где ведут бизнес, в даркнете. Работодатели на теневом рынке чаще всего предлагают соискателям серые и черные схемы заработка, однако можно встретить и предложения, предусматривающие официальную, белую работу, не противоречащую законам страны.

Черную работу предлагают, например, хакерские группировки. Чтобы проникнуть в инфраструктуру организации, похитить конфиденциальные данные или пошифровать систему для дальнейшего шантажа, злоумышленникам нужен свой штат специалистов, владеющих определенными навыками.

Схема координации в команде атакующих

Даркнет

- Общение внутри команды
- Общение с заказчиками
- Поиск исполнителей, инструментов, данных
- Продажа данных, инструментов, доступов

← Менеджер →

Координация действий в команде

АРТ-группировка

Атакующий

Первичная компрометация инфраструктуры и развитие атаки

Разработчик

Создание вредоносного ПО и инструментов

Реверс-инженер

Обратная разработка инструментов и создание своих на их основе

Аналитик

Сбор информации для подготовки атаки и обработка украденных данных

Дизайнер

Создание поддельных сайтов и писем для фишинга

Тестировщик

Отладка вредоносного ПО и проверка обхода средств защиты

Администратор

Настройка и поддержка IT-инфраструктуры группировки, а также управление взломанными сетями

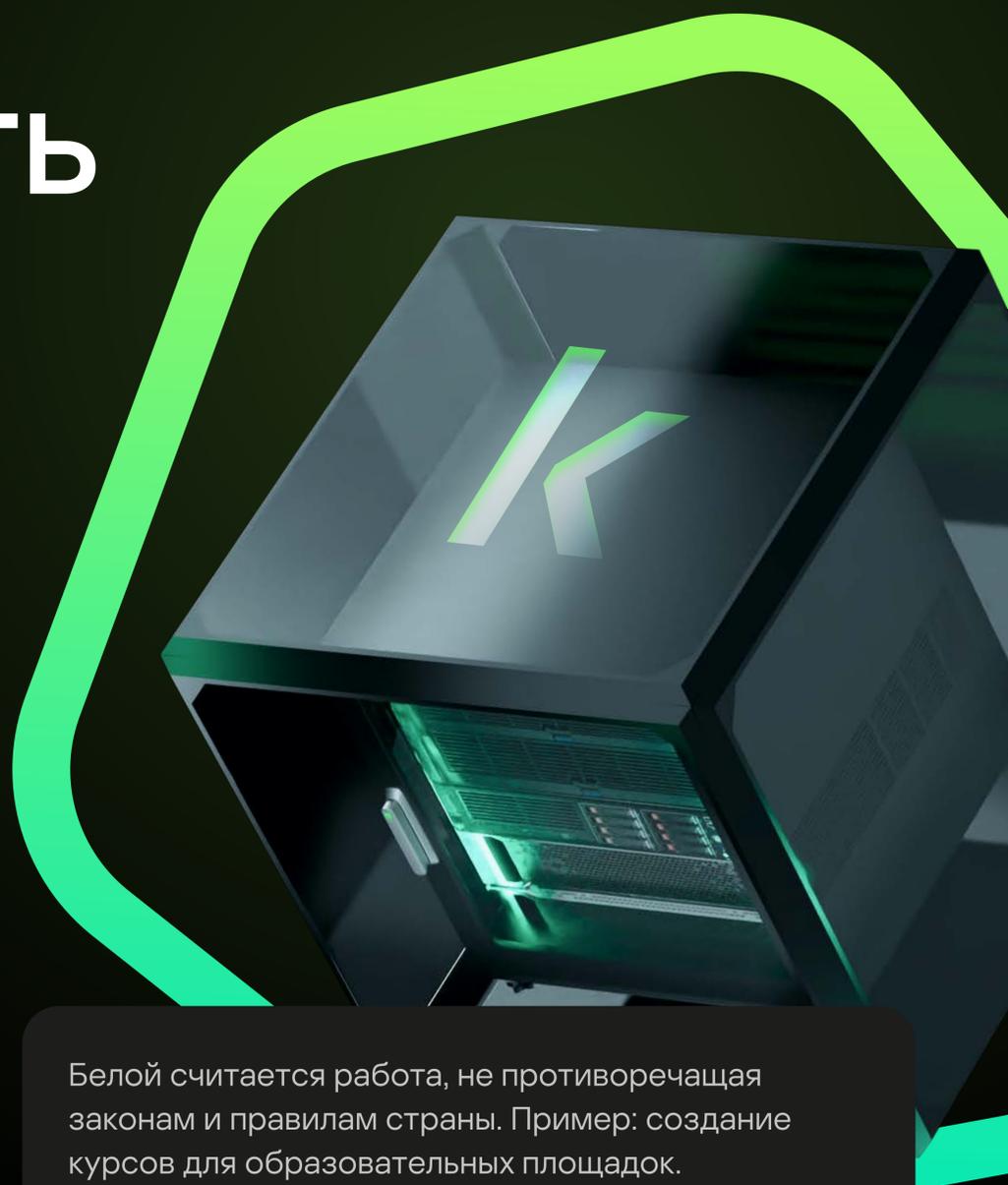


Незаконная деятельность

Причин поиска работы на теневых ресурсах может быть несколько. Среди них — отсутствие некоторых обязательных требований к соискателям, таких как наличие высшего образования, военного билета, отсутствие судимости и т. д. Основное требование, которое можно встретить в объявлениях, чтобы кандидат достиг совершеннолетнего возраста. Вакансии на теневом рынке интересуют фрилансеров и удаленщиков, поскольку не предполагают необходимости посещать офис и позволяют быть «цифровым кочевником» — работать из любой точки земного шара. Также кандидатов привлекает высокий уровень свободы, который предлагают в даркнете: нет ограничений по количеству отпускных дней, графику работы, внешнему виду и т. д., есть возможность самостоятельно выбирать задачи и сферу применения своих навыков.

Во многом мотивацией к поиску работы на теневых ресурсах становится ожидание легкого заработка и высокой финансовой выгоды, однако в большинстве случаев оно расходится с реальностью. Далеко не всегда предлагаемые в даркнете оклады оказываются значительно выше тех, которые можно получить на белом рынке, к тому же заработок зависит от опыта, способностей и готовности вкладываться в работу. Тем не менее нередко бывает так, что уровень текущей заработной платы не устраивает сотрудника и он покидает свое официальное место работы в пользу теневого рынка без смены специализации. Изменения на рынке труда, сокращения рабочих мест и зарплат также побуждают к поиску работы на киберпреступных ресурсах.

Еще одна причина поиска работы в даркнете — **неосведомленность либо недостаточно серьезное отношение к последствиям**. Между тем сотрудничество с подпольными командами, и тем более киберпреступными группировками, несет серьезные риски участников могут раскрыть и привлечь к ответственности, не говоря уже о том, что им могут попросту не заплатить за выполненную работу.



Белой считается работа, не противоречащая законам и правилам страны. Пример: создание курсов для образовательных площадок.

Работа по серым схемам уже граничит с нелегальностью, а иногда и нарушает закон. Примером серой работы может стать получение прибыли от продажи сомнительных препаратов на мошеннических сайтах.

Работа «по-черному» запрещена законом и чаще всего связана с криминалом. Против специалиста, работающего по таким схемам, могут возбудить уголовное дело и в случае поимки лишит его свободы. К черной работе относятся различные мошеннические схемы, взломы сайтов, социальных сетей или IT-инфраструктуры компаний.

Пример объявления о поиске работы

Ищу работу

Ищу работу, чрн, бел, сер. РФ

 cocerbulit 10 сен 2022



Статистика рынка труда в даркнете

Для анализа биржи рынка труда в даркнете с января 2020 года по июнь 2022 года была собрана статистика всех сообщений с упоминаниями работы, опубликованных на 155 форумах в даркнете. Отбор сообщений для анализа проводился на основе разделов, посвященных любой работе, не только IT-профессиям. Всего за анализируемый период на теневых форумах было размещено порядка 200 тысяч объявлений, связанных с работой. **Наибольшее количество сообщений было опубликовано в 2020 году (46% от общего числа).** Пик активности пришелся на март 2020 года, что, предположительно, может быть связано с резким сокращением уровня дохода части населения из-за пандемии.

Особенно заметное влияние на рынок пандемия оказала в странах СНГ.

Так, в марте 2020 года из-за кризиса часть жителей этого региона потеряла привычный доход, ушла на вынужденные выходные или вовсе осталась без работы, что впоследствии привело к росту безработицы.

Некоторые соискатели, отчаявшись найти белую работу со стабильным заработком, начали искать ее на различных теневых форумах, что привело к резкому увеличению количества резюме в даркнете. В результате в марте 2022 года наблюдались самые высокие показатели среди объявлений — 6% от общего числа объявлений.

Резюме соискателя, оказавшегося в затруднительной ситуации

Ищу онлайн работу

Парень больше 25 лет, не употребляю, спорт на уме. Сложилось так что сижу на карантине без денег,кто может предложить что-то стоящее, готов посотрудничать.

zann 22 окт 2020

Теги из объявления, предлагающего работу во время кризиса

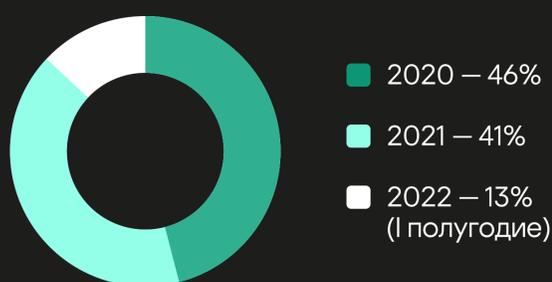
где взять денег в кризис где заработать денег в пандемию

заработок во время коронавируса работа пандемия

работа в кризис коронавирус последние новости

DoomGuy969 4 апр 2020

Распределение объявлений по дате публикации

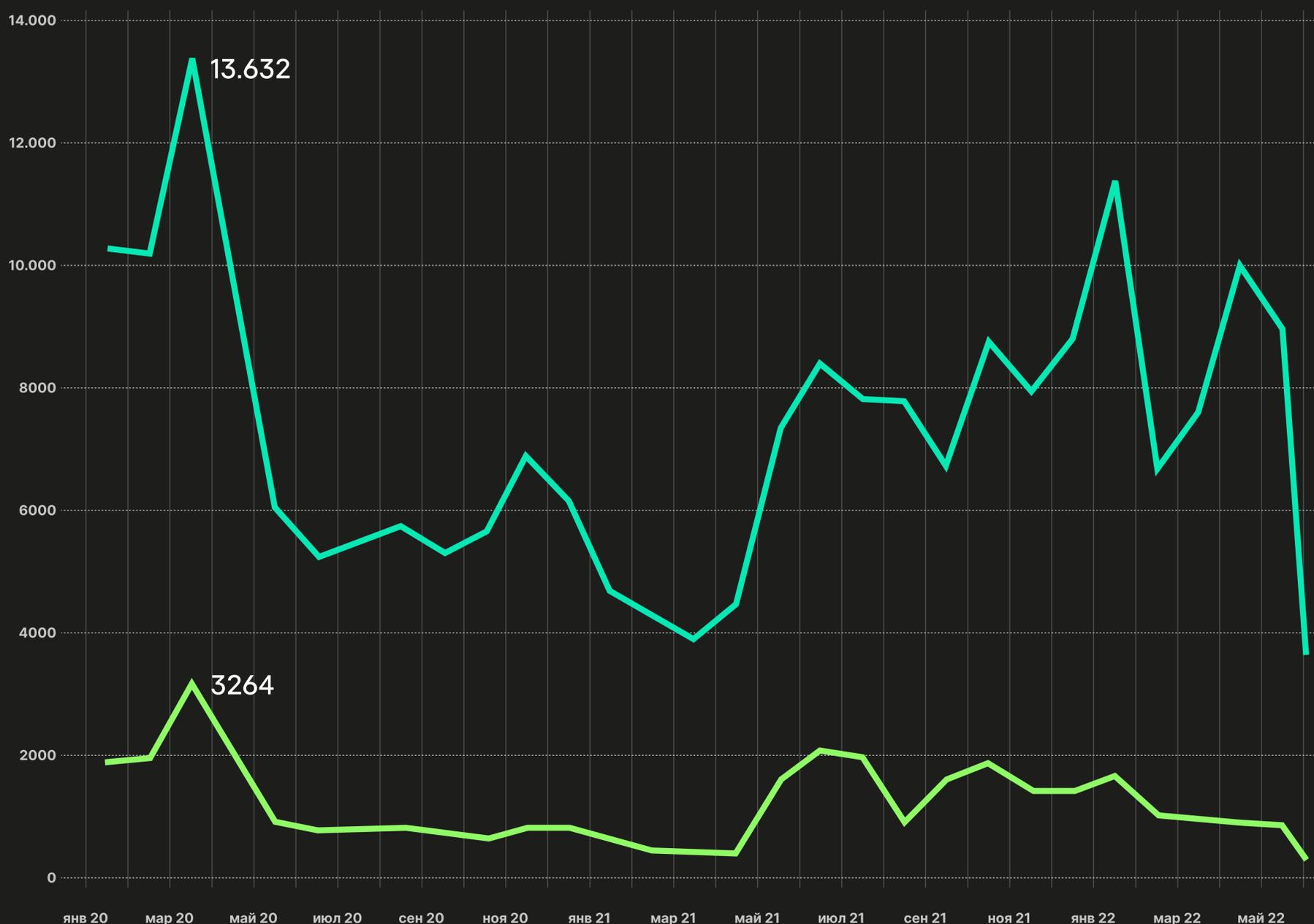


Статистика публикации объявлений



Динамика количества публикаций в тематических разделах даркнет-форумов за период 2020-2022 гг.

■ Всего сообщений ■ Поиск работы



Сообщений о поиске работы значительно меньше, чем самих вакансий. Так, из всех найденных объявлений только 17% были связаны с поиском работы.

Заинтересованные в работе пользователи чаще откликаются на вакансии, уже опубликованные работодателями, чем сами пишут объявления.

Согласно опубликованным на теневых форумах резюме, соискатели ищут работу в разных сферах и претендуют на должности, обязанности которых могут варьироваться, от ведения телеграм-каналов, до компрометации инфраструктуры различных компаний. В рамках данного исследования мы рассматривали объявления, связанные непосредственно с IT-сферой. Мы проанализировали 867 объявлений, отобранных по ключевым словам, из которых 638 — это сообщения о поиске работников (вакансии), а 229 — это сообщения о поиске работы (резюме).



Условия отбора

Методы отбора IT-специалистов на теневом рынке во многом совпадают с методами отбора в легитимных компаниях. Работодатели точно так же заинтересованы в высококвалифицированных кадрах и поэтому пытаются отобрать наиболее сильных кандидатов.

В объявлениях нередко упоминаются тестовые задания, в том числе оплачиваемые; также можно встретить упоминания собеседований, испытательных сроков и прочих схем отбора.

Так, в одном из объявлений приводилась подробная схема отбора потенциальных сотрудников. Соискатель работы должен был пройти несколько этапов проверки, в том числе тестовые задания, связанные с шифрованием исполняемых вредоносных файлов и обходом средств защиты, и испытательный срок.

Из особенностей найма сотрудников в даркнет-пространстве можно также выделить требования об отсутствии зависимостей, в том числе алкогольной и наркотической.



Условия отбора из объявлений в даркнете

Тестовые задания — 82%

Наличие резюме/портфолио — 37%

Собеседования — 26%

Испытательные сроки — 2%

Для статистики процент высчитывался от общего числа объявлений, в которых явно указывались условия отбора.

Пример схемы отбора работников

Требуется криптощик DLL/EXE файлов ...

Схема отбора кандидатов следующая:

1. Даем Вам на крипт нашу тестовую дллку. Крипт должен быть FUD на скантайм и максимум 3 детекта незначительных AV на рантайме.
2. Если пункт 1 пройден, даем Вам на крипт боевой файл. Крипт должен быть FUD на скантайм, и продержаться чистым в течении 24 часов (без прогруза).
3. Если пункт 2 пройден, работаем с Вами в течении испытательного срока (2 недели), с оплатой \$40 за крипт. С понедельника по пятницу до 13.00 по мск у нас должен быть работающий FUD dll/exe.
4. Если испытательный срок пройден, Вы регулярно были на связи, стабильно делали чистки, и показали себя как добросовестный и компетентный специалист, берем Вас на постоянную работу, с оплатой \$800-\$1500 в неделю

tomp 21 дек 2021



Вакансия с тестовым заданием

Требуется Программист C++ ...

Если Вас заинтересовала эта вакансия, вышлите свое резюме в пм - если ваша кандидатура нас заинтересует - мы вышлем оплачиваемое (20т.р.в бтц по курсу) тестовое задание.

IT_Work 10 июн 2021



Вакансия с требованиями об отсутствии вредных привычек

Ищется вебкодер в крупный проект ...

Умение работать в команде, хороший онлайн, отсутствие проблем с алкогольной и нарко зависимостью.

winhost 11 ноя 2021



Условия труда

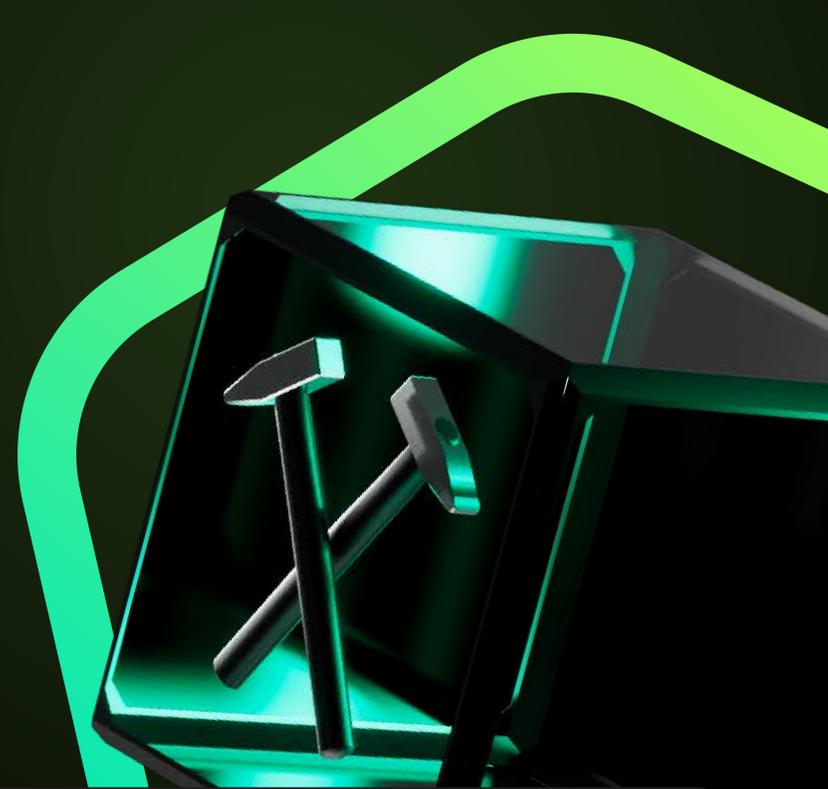
Работодатели даркнета используют разные способы привлечения внимания кандидатов, предлагая им различные выгодные условия. В основном специалистам обещают удаленную работу (45%), полную занятость (34%) и гибкий график (33%).

Наиболее комфортные условия, в том числе возможности карьерного роста и поощрительные бонусные планы, предлагают киберпреступные группировки, чтобы завлечь к себе наиболее квалифицированных работников.

Такие группировки могут также оценивать производительность сотрудников, как это делали Conti. По результатам оценки работник может получить премию либо финансовый штраф из-за неэффективности работы. Более того, у некоторых подпольных «организаций» существуют целые реферальные программы для сотрудников, которые предоставляют бонусы тем, кто смог успешно привлечь других к работе.

Как и на белом рынке, работодатели предлагают разные виды занятости: полная, неполная занятость и стажировки, сотрудничество, партнерство, прием в команду.

Основное отличие даркнета от белого рынка труда — отсутствие оформления по трудовому кодексу. При этом в даркнете все же встречаются объявления, связанные с наймом сотрудников на официальную работу. Например, мы обнаружили несколько объявлений о поиске программиста в известный российский банк, в условиях которых упоминалось официальное трудоустройство и ДМС.

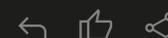


Объявление об официальном трудоустройстве

Java-разработчик на удалённую работу в современный российский Банк

Условия: • Работа в крупном российском банке из ТОП-50 • Официальное трудоустройство • ДМС (с 1-го месяца работы) • График работы 5/2, удаленная работа • Зарплата: разработчик на удалённую работу в Самаре – 125 000 ₺ gross + 10% годовой бонус / в офисе в Пензе 115 000 ₺ gross +10% годовой бонус • Работа в команде профессионалов в доброжелательной атмосфере • Амбициозные задачи и проекты, возможность повлиять на результат технологического

anonymus 6 июн 2020



В случае даркнета удаленная работа является скорее необходимостью, а не выгодным предложением, поскольку в киберпреступном мире важную роль играет анонимность.

Условия труда из вакансии в даркнете

Вакансия "ПРОГРАММИСТ C++ с навыками реверс-инженеринга"

Условия: Мы предлагаем Вам своевременную зарплату. Уровень зарплаты определяется по итогам тестового задания и собеседования (от \$2000 и выше); Работа полностью УДАЛЕННАЯ, 5 дней в неделю, СБ и ВС выходные; Оплачиваемый отпуск; БЕЗ оформления по ТК; У нас в условиях есть постоянный рост; на каждый успех вы получаете постоянную прибавку плюс мгновенный бонус

anonymus 11 июн 2021



Статистика условий труда из объявлений в даркнете

Удаленная работа — 45%

Полная занятость — 34%

Гибкий график — 33%

Стабильная и своевременная ЗП — 10%

Оплачиваемые отпуска и больничные — 8%

Дружный коллектив — 8%

Фиксированный график — 8%



Заработные платы

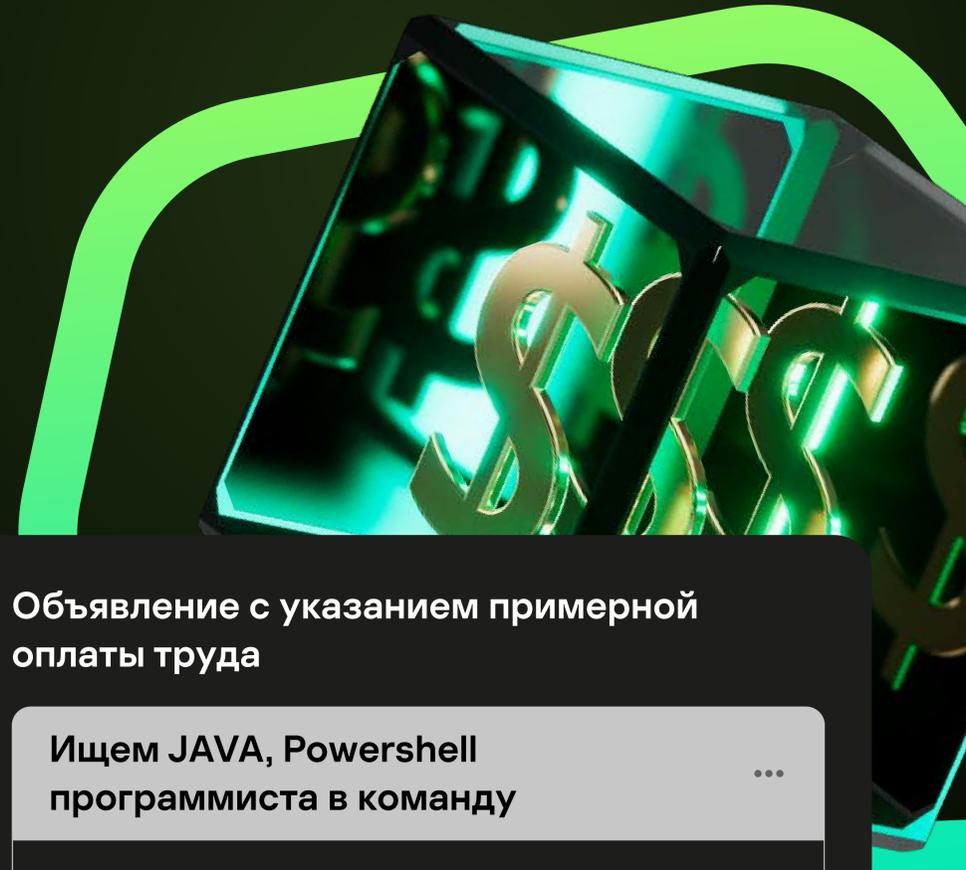
Мы проанализировали более 160 IT-вакансий, в которых явно указывались размеры компенсаций. При рассмотрении полученной статистики важно понимать, что в объявлениях указывается приблизительный оклад. Часто работодатели пишут либо диапазоны зарплат, либо их начальные уровни.

Со временем зарплата может расти в зависимости от приложенных усилий, вклада в работу сотрудника, его роста как специалиста и в целом от того, насколько развился сам «бизнес», в котором он принимает участие. В объявлениях зарплаты, как правило, указываются в долларах, однако на практике работу часто оплачивают в криптовалюте.

На момент исследования самой высокооплачиваемой профессией являются разработчики, максимальный оклад которых мог достигать 20 000 USD в месяц. Однако у них же наблюдалась и самая маленькая стартовая зарплата, которая составляла всего 200 USD.

Помимо разработчиков выделились также реверс-инженеры, у которых наблюдалась самая высокая медианная оплата труда — 4000 USD.

Встречаются вакансии, обещающие специалистам оклад намного выше приведенных цифр, но достигаться он будет, как правило, за счет различных бонусов и процентов, пришедших от удачно реализованных проектов вроде получения прибыли путем шантажа скомпрометированной организации.

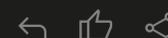


Объявление с указанием примерной оплаты труда

Ищем JAVA, Powershell программиста в команду

Ищем в команду профессионалов программистов на Java, Powershell (другие языки приветствуются)
Предлагаем заработную плату от 3k\$ до 5k\$ + бонусы от заработка

monochrome76 6 авг 2021



Объявление с вакансией на темном форуме, предлагающее завышенный оклад

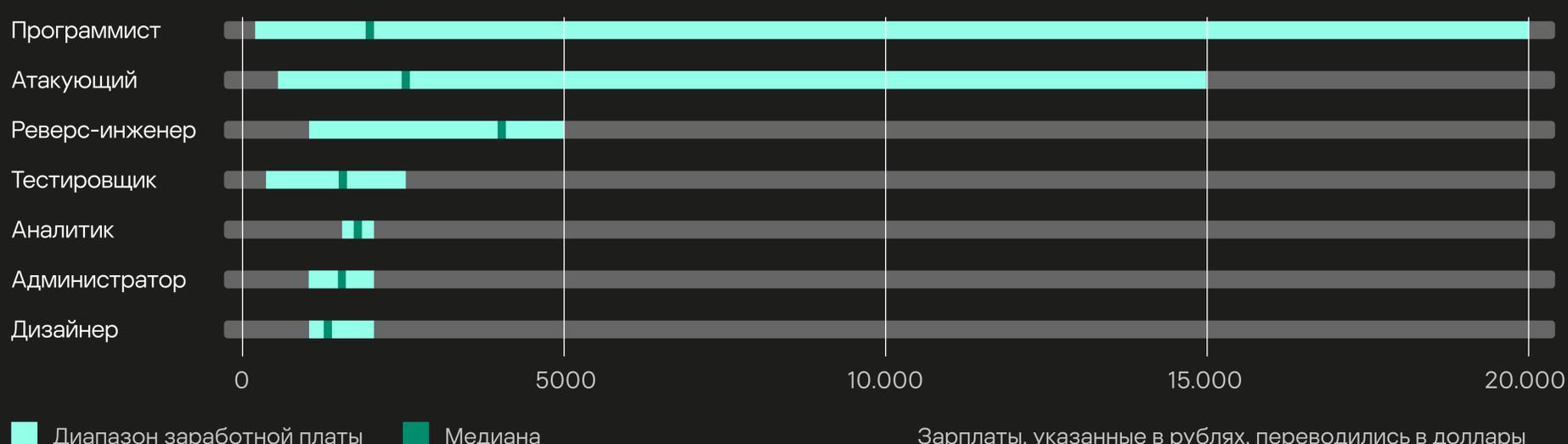
Ищем пентестера XXE, XSS, SQL

В команду ищем человека, который знает ххе, хss, sql атаки как свои 5 пальцев для пентеста своих сайтов на уязвимости. (белая работа) Зп до 100k\$ в месяц
Детали в пм

ZelleCashOut 26 апр 2020



Диапазоны заработных плат IT-специалистов из объявлений в даркнете, \$



Зарплаты, указанные в рублях, переводились в доллары по курсу, соответствующему началу исследования — 75



Стоит сказать, что не все вакансии вошли в статистику по заработным платам, так как среди них могут быть подозрительные, а порой и вовсе мошеннические предложения работы.

Так, в одном из доступных в даркнете объявлений о поиске «пентестера сайтов» обещали платить вплоть до 100 000 долларов в месяц. Интересно то, что в описании вакансии говорится о «белой работе».

Помимо стандартного месячного и иных видов оклада (почасового, ежедневного, еженедельного) существуют также и другие способы оплаты труда, которые либо сами по себе являются основными, либо добавляются к основным.

В частности, встречается проектная работа со сдельной заработной платой, выплачиваемой по факту выполнения работы. Это может быть оплата за взломанный сайт, разработанную фишинговую страницу.

В качестве дополнительной оплаты труда работодатели нередко обещают к фиксированному окладу различные проценты, зависящие от результата работы. К примеру, «пентестеру» обещают оклад 10 000 USD в месяц, а также процент от прибыли за скомпрометированные сети различных организаций, продажи доступов, конфиденциальных данных, шантажа и т. д.

Нередко точно такому же эксперту могут предлагать и вовсе работать только на процентном окладе.

Иногда попадаются вакансии, в которых в принципе нет никакой оплаты труда. Работодатели либо предлагают работать за идею, либо обещают возможность получения процентов или прибыли в будущем.

Пример вакансии с окладом и процентами за работу

Ищем WIN пентестера

Ищем WIN пентестера в команду.

- Опыт работы с Cobalt Strike, MSF и т.п.
- Ответственный подход к работе
- Без вредных привычек

ЗП от 10к\$ в мес. + %.Пишите в ЛС.

LEO-001 1 дек 2021



Пример вакансии с отсутствием оплаты труда

Набор кодеров/дизайнеров

Набираю команду для создания, тестирования и продвижения софта. Сам софт представляет из себя комплекс ботов на разные социальные сети с free лицензией, и другими платными функциями.

Требования:

- Быть готовым работать на бесплатной основе до выстрела проекта
- Иметь хоть какие-то знания в сфере web или дизайна (будет плюсом знание web яп - таких как php, python, js и прочие)

Сукер11 2 июн 2020



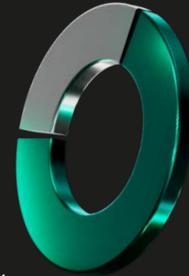
Программист



Программисты являются самыми востребованными IT-специалистами в даркнете — 61% от всех найденных IT-вакансий.

Всего сообщений

553



Резюме — 30%
Вакансии — 70%

Специальности

Веб-разработчики — 60%
Разработчики десктоп-приложений — 34%
Мобильные разработчики — 6%
Разработчики игр — 3%

Наиболее востребованным направлением считается веб-разработка — на нее приходится 60% объявлений. Веб-программисты занимаются созданием различных веб-продуктов, самыми популярными из которых считаются фишинговые страницы и веб-сайты.

Еще один востребованный разработчик в даркнете — вирусписатель. В его задачи может входить разработка вредоносного ПО (троянцы, шифровальщики, стиллеры, бэкдоры, ботнеты и прочее) и в целом разработка и модификация инструментов для проведения атак.

Отбор в команду осуществляется по тому, насколько кандидат соответствует требованиям работодателя составленным в вакансии требованиям. Часто такие вакансии могут быть похожи или вовсе совпадать с вакансиями с белого рынка труда.

Среди требований основными считается опыт разработки и знание языков программирования. Анализ показал, что самым востребованным среди работодателей языком является PHP — он встречался в 20% вакансий. В тройку также вошли языки JavaScript и C++.

Пример объявления о поиске Java-программиста

Работа Java-программист уровня middle-senior

Требования:

Хорошее знание Java (SE); Хорошее знание ООП; Понимание принципов создания многопоточных приложений; Английский язык на уровне чтения технической документации

Будет плюсом: Опыт работы с сокетами; Опыт работы с JNI, JNA; Опыт работы с PHP, MySQL, Git; Базовые знания C/C++

EgorData 29 июл 2021

Топ 5 требуемых языков программирования

PHP — 20%

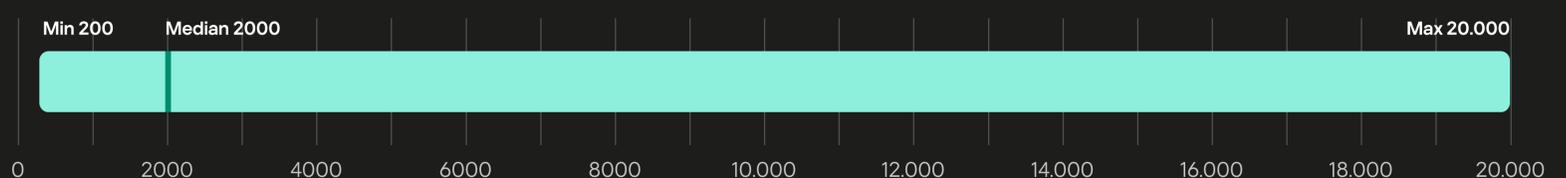
JavaScript — 20%

C++ — 19%

Python — 14%

CSS — 10%

Зарботные платы, \$



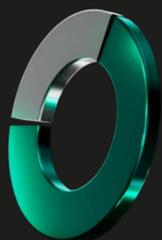
Специалист по проведению атак

Вакансии для специалистов по проведению атак составляют 16% от общего количества предложений.

Всего сообщений

150

- Резюме — 30%
- Вакансии — 70%



Специальности

- Сетевые атаки — 48%
- Атаки на веб-приложения — 21%
- Атаки на мобильные устройства — 5%

Стоит заметить, что, в отличие от прочих профессий, работа «взломщиком» в даркнете сильно отличается от ближайшего легального аналога — специалиста по тестированию на проникновение.

Большинство обнаруженных вакансий в даркнете связано с наймом специалистов для компрометации инфраструктур организаций. Часто целью такого взлома является заражение программами-шифровальщиками, похищение данных или непосредственная кража денег со счетов.

Кроме того, существуют группировки, не занимающиеся развитием атаки, а продающие доступ к скомпрометированным системам другим злоумышленникам. Также атакующих нередко нанимают для проведения взломов веб- и мобильных приложений.

Данная профессия подразумевает владение соответствующим инструментарием, таким как Cobalt Strike (встречалось в 71% вакансий, где указывались инструменты), Metasploit (67%), а также сканерами уязвимостей (14%), Mimikatz (10%), Empire (5%).

Пример объявления о поиске атакующего

Набираем пентестеров на работу

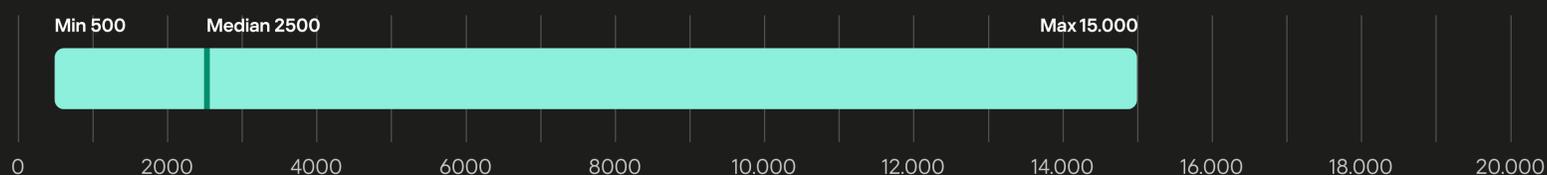
Ищутся квалифицированные пентестеры-сетевики локальщики. не понаслышке знающие, что такое Metasploit/CobaltStrike и им подобное, а так же, умеющие активно всем этим пользоваться, в рамках достижения поставленной цели. С нас: занятные таргеты и нетривиальные задачи, с вас: талант, навык, опыт и желание работать-зарабатывать. (Выход из окружения входной машины, поднятие прав, знание и умение обращаться с AD, взятие с боем домен админа, ну и тд...)

Mario 6 май 2020

Требования к кандидату

- Опыт работы — 20%
- Программы и фреймворки — 19%
- Атаки на Active Directory — 14%
- Навыки программирования — 13%
- Поиск веб-уязвимостей — 6%

Заработные платы, \$



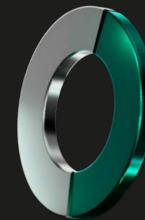
Дизайнер

Вакансии дизайнера составляют 10% от обнаруженных объявлений, опубликованных за анализируемый период.

Всего сообщений

115

■ Резюме — 55%
■ Вакансии — 45%



Специальности

Веб-дизайнер — 62%
UI/UX-дизайнер — 41%
Графический дизайнер — 17%

Основным направлением работы дизайнера в даркнете является разработка фишинговых веб-страниц. Это могут быть как обычные копии популярных ресурсов (социальные сети, банковские приложения, интернет-сервисы), так и страницы, создаваемые специально для целевых атак на организации. Также дизайнеры ответственны за создание скам-проектов и фишинговых электронных писем. Главная цель — сделать продукт таким образом, чтобы его было сложно отличить от настоящего, ведь чем больше они похожи, тем выше прибыль.

Веб-дизайнеры также могут привлекаться к разработке интерфейсов даркнет-форумов, административных панелей, маркетплейсов и т.д.

Главное требование для дизайнера — наличие портфолио с выполненными проектами и примерами работ. В требованиях часто указывается владение графическими программами (Photoshop, Illustrator, Adobe XD, Figma).

Пример объявления о поиске дизайнера

Открыты вакансии дизайн, отрисовка документов

Ведется набор в команду Diamond Service! Если ты хочешь иметь высокий стабильный доход, работать по гибкому графику, получать бесценный опыт от профессионалов своего дела. Тебе к нам! ВАКАНСИИ: - Дизайнер, веб-мастер (создавать аватарки, логотипы, стикеры, баннеры; оформлять торговые темы, каналы, группы; веб-дизайн сайтов; создание сайтов; моушн дизайн) Требования к кандидату: 1. Опыт работы в графических редакторах, front end; 2. Наличие портфолио, успешных кейсов; 3. Много свободного времени; 4. Стрессоустойчивость, коммуникабельность;

PerfectumSupport 22 дек 2021

Требования к кандидату

Наличие портфолио — 43%

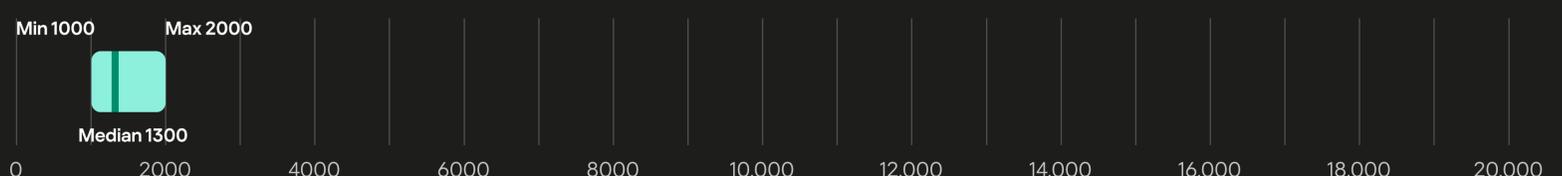
Графические редакторы — 38%

Знание стандартов — 38%

Основы веб-разработки — 6%

Опыт в сфере дизайна — 3%

Заработные платы, \$

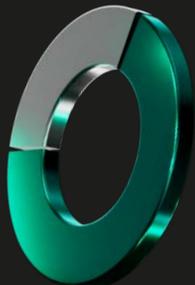


IT-администратор

За анализируемый период 6% обнаруженных вакансий были связаны с подбором администраторов.

Всего сообщений

52



Резюме — 31%
Вакансии — 69%

Специальности

Системный администратор — 53%

Веб-администратор — 11%

DevOps-инженер — 8%

NOC-администратор — 3%

Предположительно, невысокий спрос вызван тем, что часто обязанности по администрированию инфраструктуры берут на себя другие участники группировки. Кроме того, все больше киберпреступников и хакерских группировок активно используют облачные сервисы, обязанности по поддержке которых перекладываются уже на поставщика.

Работодатели могут явно указывать, в поисках какого именно администратора они находятся. Среди вакансий, более половины — это поиск системных администраторов. Реже нанимают DevOps-ов, веб и NOC администраторов.

Администраторы требуются для настройки и обеспечения необходимой поддержки инфраструктуры атакующих, а также для управления уже скомпрометированными сетями жертв. В задачи администратора может входить обслуживание серверов, установка панелей, покупка хостинга, создание прокси-серверов и т.д.

Администраторов могут привлекать для проведения «работ по компрометации инфраструктуры жертвы». Связано это с тем, что получение доступа и осуществление полной компрометации системы требует определенных знаний и навыков, которыми как раз обладают данные специалисты.

Пример объявления о поиске IT-администратора

Требуются 2-3 Системных администратора

Требуются 2-3 Системных администратора. Мы гарантируем: Стабильную и своевременную оплату; Полную самостоятельность по задачам - "дружный коллектив" мешать вам не будет; Возможность реализации и повышение уровня. Условия: Удаленная работа, не менее 8 часов в сутки по будням; Linux, настройка, администрирование на высоком уровне; Маршрутизация пакетов, VPN, NAT, DNS, VLAN и т.п.; Виртуализация, знание на хорошем уровне любой из: XEN, VMWare, KVM; Умение работать с железом: сервера, коммутаторы, маршрутизаторы, сетевое оборудование и протоколы.

khano 25 окт 2020

Требования к кандидату

Операционные системы — 47%

Сети, протоколы и маршрутизация — 31%

Языки программирования — 28%

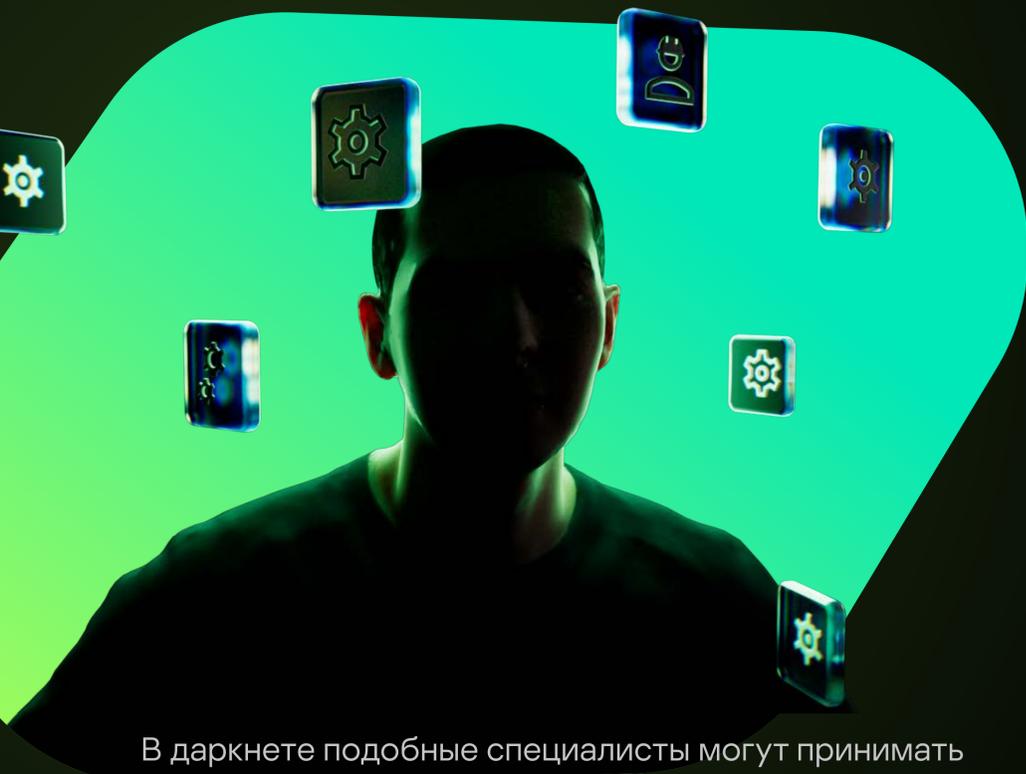
Виртуализация — 28%

ActiveDirectory, GPO — 22%

Зарботные платы, \$



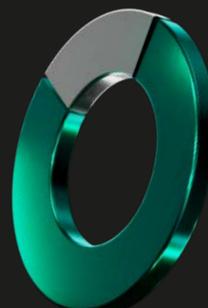
Реверс-инженер



В киберкриминальных сообществах с поиском реверс-инженеров связано 4% вакансий.

Всего сообщений

33



Резюме - 21%

Вакансии - 79%

Специальности

Анализ ПО – 31%

Анализ мобильных приложений – 31%

Анализ трафика – 15%

Анализ встраиваемых систем – 8%

В даркнете подобные специалисты могут принимать разовые заказы на поиск уязвимостей в каком-либо приложении или же самостоятельно продавать информацию об обнаруженных уязвимостях.

Основным направлением работы реверс-инженеров в команде можно считать поиск и эксплуатацию новых уязвимостей в широко используемом оборудовании или программном обеспечении. Также инженеры могут принимать участие в анализе защитных решений и отслеживании обновлений безопасности для поиска методов их обхода.

Навыки реверс-инженеров также бывают полезны, когда дело доходит до реверса и анализа чужих программ/инструментов с целью их модификации или разработки собственного продукта (в том числе вредоносной программы или инструмента для атак).

Среди требований для специалиста по реверс-инжинирингу чаще, чем в других профессиях, указывается необходимость наличия опыта работы. Возможно, это связано с тем, что задачи начинающего специалиста может выполнять программист, а отдельную роль выделяют только для высококвалифицированных специалистов.

Пример объявления о поиске реверс-инженера

Ищу несколько реверс-инженеров для постоянного сотрудничества

Ищу несколько реверс-инженеров для постоянного сотрудничества. Нужные навыки: - знание ассемблера x86/x64 - знание процессорной архитектуры x64 - владение отладчиками и дизассемблерами (IDA Pro, WinDbg, Radare) - владение инструментами фаззинга - понимание устройства современных ОС, в частности Windows - знание языка C - базовое знание скриптовых языков, используемых для автоматизации работы (Python, .bat, PowerShell)

khano 30 ноя 2020



Требования к кандидату

Опыт реверс-инжиниринга - 38%

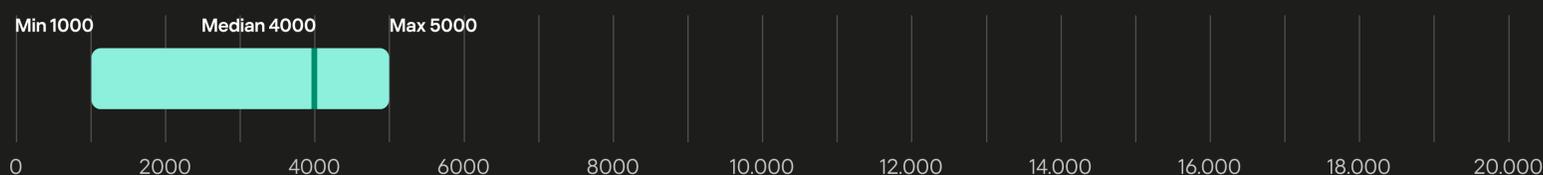
Языки программирования - 38%

Знание инструментов - 27%

Анализ протоколов/трафика - 27%

Архитектура ПК - 23%

Заработные платы, \$

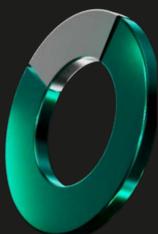


Аналитик

Вакансии для аналитиков довольно редко встречаются на даркнет-площадках. За анализируемый период они составили 2% от всех вакансий.

Всего сообщений

14



- Резюме — 22%
- Вакансии — 78%

Специальности

- Аналитик данных — 45%
- Бизнес-аналитик — 36%
- OSINT-аналитик — 9%



На этапе планирования атак группировки могут прибегать к помощи бизнес-аналитика, в обязанности которого входит сбор информации о потенциальных жертвах на основе информации из открытых источников. В частности, аналитик получает информацию об активах компании (в первую очередь финансовых). Кроме того, информация, предоставляемая аналитиком, может использоваться для разработки схемы атаки и оценки того, какой размер выкупа потом потребовать.

На заключительном же этапе атаки группировки могут привлекать к работе аналитика данных. Этому специалисту поручается извлечь интересующую киберпреступников информацию из больших массивов похищенных данных, часто неструктурированных.

Требования к будущим сотрудникам могут различаться в зависимости от специфики профессии. Чаще всего указываются владение английским языком (половина всех вакансий) и продвинутые навыки работы с ПК.

Пример объявления о поиске аналитика данных

Неспешно ищущу аналитика данных

Мне требуется человек на процентном окладе. от 10 до 20 процентов от суммы выкупа процент зависит от того насколько была важна роль данных в этом процессе, в целом оно может быть и больше 20. Кто мне нужен: 1) Человек с депозитом минимум 15к USD 2) Человек который получает точку входа + ДА без лишних вопросов заходит туда 3) Не спаливаясь выкачивает ценное и уходит 4) У него нет морали (это делать можно это делать нельзя) 5) Должен уметь работать не только с EN датой ну и другими европейскими языками (легко можно использовать фотопереводчик) Первый контакт в ЛС

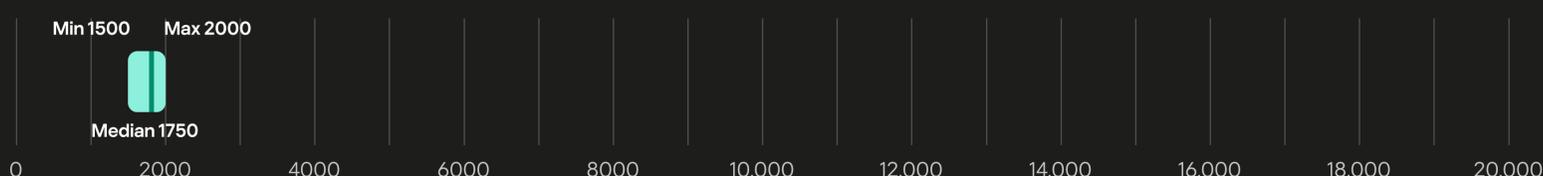
boriselcin 20 окт 2021



Требования к кандидату

- Английский язык — 50%
- Продвинутое владение ПК — 40%
- Аналитический склад ума — 20%
- Методы извлечения информации — 20%
- СУБД — 20%

Зарботные платы, \$

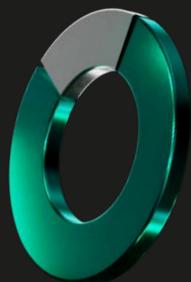


Тестировщик

В вакансиях специалисты по тестированию, так же как и аналитики, встречаются в даркнете достаточно редко — 1% вакансий.

Всего сообщений

10



Резюме — 20%
Вакансии — 80%

Специальности

Тестировщик ПО — 56%

Тестировщик веб-приложений — 22%

Тестировщик мобильных приложений — 11%

QA-инженер — 11%



В обязанности тестировщика в киберкриминальных сообществах чаще всего входит проверка вредоносных программ (троянцы, стиллеры, чекеры, брутеры) и инструментария для атак.

Также тестировщики могут заниматься тестированием и анализом веб-ресурсов (например, скам-сайтов — фишинговых страниц, имитирующих известные банковские веб-приложения) и мобильных приложений (например, троянских программ).

В задачи тестирования, помимо всего прочего, входит проверка возможности обхода методов обнаружения различными средствами защиты (antivirus detection).

Обязательное требование для любого тестировщика — умение устанавливать и настраивать тестовую среду на виртуальные машины с разными операционными системами (Windows, Linux, Android, iOS).

Пример объявления о поиске тестировщика-администратора

Нужны тестировщики ПО

Нужны тестировщики ПО, от вас знания как устанавливать различные операционные системы Windows/Linux на виртуальную машину.

Нужно просто запускать софт на разных операционных системах и предоставлять мне отчёт, за каждый отчёт получаете оплату.

Оплата договорная, зависит от вашей трудолюбивости и усидчивости.

TvoiDrug 24 сен 2021

Требования к кандидату

Виртуальные машины — 56%

Windows-администрирование — 22%

Уверенный пользователь ПК — 22%

Выявление проблем в ПО — 11%

Опыт работы с Unix — 11%

Зарботные платы, \$



Прочее IT

Как известно, IT-профессий гораздо больше, но из-за того, что некоторые из них попадались реже, они не вошли в общую статистику. Представителями IT-рынка в даркнете также являются разного рода инженеры и архитекторы, специалисты из техподдержки, авторы технических текстов, модераторы форумов и даже менеджеры и руководители целых проектов.

Как и в любом бизнесе, местным предпринимателям также нужны маркетологи, таргетологи, SMM-щики, линкбилдеры, копирайтеры и прочие специалисты для развития и продвижения своих проектов и продуктов. Стоит заметить, что подобные специалисты в ответе за повышение черных сайтов в поисковой выдаче.

На просторах даркнета встречались также объявления в области IT-образования, а именно вакансии на должность создателей образовательных программ и (или) преподавателя на известные в России курсы в области IT, репетиторов на зарубежных площадках.

И конечно, даже в даркнете не обходятся без HR-специалистов. Иногда роль по рекрутингу новых айтишников берет на себя руководитель, но если речь идет о команде с крупным доходом, то для этой роли в команду могут пригласить своего кадровика.

Пример объявления с предложением о работе руководителем проекта

Project Manager в теневой проект [мин. 1500\$, 10% от прибыли]

Об о мне и о работе: Мне нужен операционный директор / проджект менеджер с опытом в IT для масштабирования и поддержания работы проектов. Каких? Расскажу и покажу лично, заинтересовавшим меня кандидатам. Я не студент и не стартапер. У меня есть два функционирующих направления с операционной прибылью в 60.000 - 120.000\$ в месяц. Команда из 6 человек. Тезисно о проекте - создание несложных сайтов, ведение соц. сетей, отдел продаж, работа с платежами. Во всем этом ты должен хорошо разбираться и иметь возможность проконтролировать сотрудников/фрилансеров. Цвет - серый с уклоном в черный. Никакой работы по СНГ, оффлайну и ущербу гос. организациям.

LEO-001 1 дек 2021



Пример объявления с предложением о работе преподавателем

WEB-разработчик на C#

Образовательная платформа «***» ищет WEB-разработчика на C# уровня Senior или Teamlead для преподавания на курсах. Мы готовим мощную образовательную программу для обучения людей, желающих попасть в сферу IT. Ты можешь внести свой вклад в развитие web-разработки и присоединиться к нам в качестве автора занятий, лектора, дипломного руководителя или проверяющего домашние задания.

LEO-001 1 дек 2021



Выводы

Даркнет — это многофункциональная площадка, которая используется не только для проведения сделок между злоумышленниками и распространения противозаконной информации, но и для найма участников в те или иные команды или группировки.

Из данных, приведенных в этом отчете, видно, что **спрос на IT-специалистов на киберкриминальных ресурсах довольно высок**. При этом часто новые участники нанимаются как сотрудники с фиксированным окладом. Также интересно отметить, что для привлечения новых работников киберпреступные сообщества используют те же способы, что и легитимные организации, а сами объявления часто похожи на те, что публикуются на обычных рекрутинговых площадках.

Также, судя по проанализированным объявлениям, достаточно много людей готовы заниматься нелегальной или полулегальной деятельностью, несмотря на связанные с этим риски. В частности, многие начинают активно искать возможность дополнительного заработка на теневом рынке в кризисных ситуациях. Так, в марте 2020 года во время коронавирусной пандемии на теневых ресурсах резко возросло количество объявлений о поиске работы. Хотя можно было ожидать, что заработки в даркнете выше, чем в легитимных компаниях, **мы не выявили значительной разницы в медианном уровне зарплат IT-специалистов в киберкриминальной среде и на легальном рынке труда**.

Самыми востребованными специалистами оказались разработчики (с поиском программистов связан 61% всех объявлений). Это косвенно может говорить об усложнении процессов кибератак. Так, большую востребованность разработчиков можно связать с необходимостью настраивать и разрабатывать новые, более сложные инструменты.

Стоит отметить, что риски работы на темном рынке все еще превышают выгоды. Отсутствие оформления по трудовому кодексу снимает с работодателей всю ответственность. Соискателя могут обмануть с зарплатой, подставить или вовлечь в мошенническую схему.

Ну и конечно, не стоит забывать про уголовную ответственность, суды и лишение свободы за деятельность, противоречащую законодательству. Особенно высоки риски при работе с группировками, так как деанонимизация их участников — приоритетная задача для команд, занимающихся расследованием киберпреступлений. Поэтому рано или поздно группу могут раскрыть, а ее членам будет грозить тюремное заключение.

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

dfi@kaspersky.com

