Системы
Информационной
Безопасности

Cybercrime intelligence

разведка кибер-преступлений, аналитика
теневого рынка информации.

Теневой рынок

Системы Информационной Безопасности

- Ежедневно в теневом информационном пространстве украденные данные и деньги переходят из рук в руки.

- На различных Darkweb-ресурсах, биржах, рынках и форумах продаются и покупаются ежедневно сотни баз данных, содержащих персональные данные, дампы кредитных карт, паспорта, банковские платежные аккаунты и даже пакеты «бесплатных» миль ведущих авиакомпаний или скидок на проживание в крупных сетях отелей.

- Общий ущерб бизнесу от деятельности на теневом рынке информации оценить сложно, однако по данным различных исследований за последние годы он доходит до сотен миллиардов долларов в год.

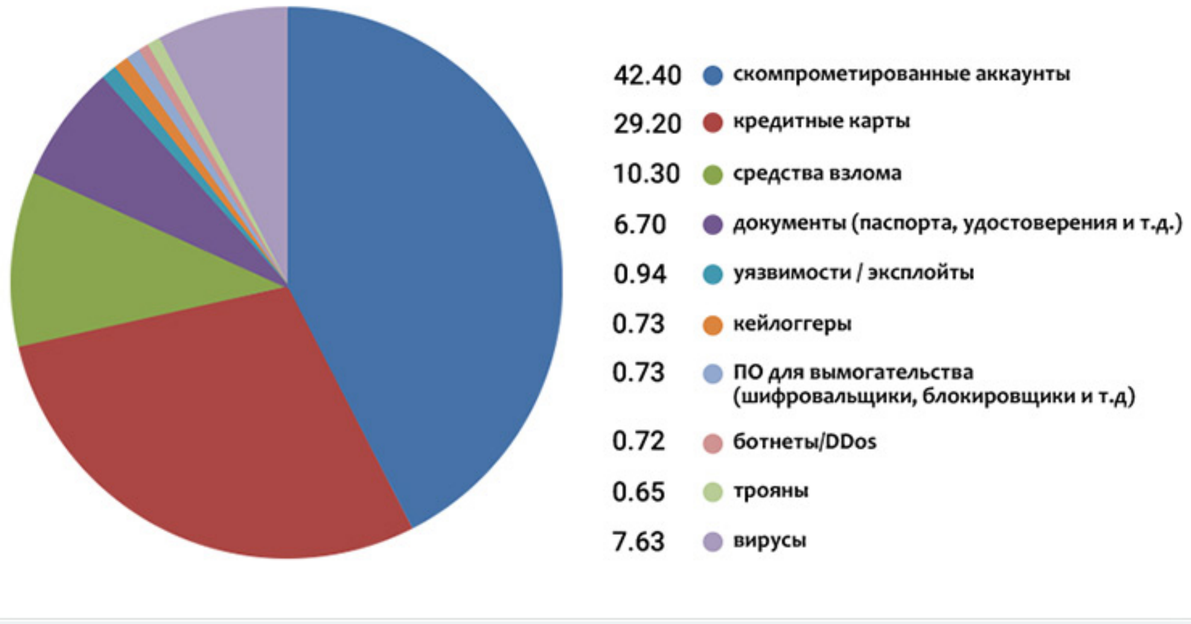
Теневой рынок статистика

Системы Информационной Безопасности

- Ассортимент дарк-веба
- типы торгуемых данных
- цены на услуги/данные

Средние предложения различных типов программного обеспечения (в $)

Предложения на теневом рынке



BANKING & ONLINE PAYMENT ACCOUNTS CREDENTIALS	
ACCOUNTS (U.S.) BANK OF AMERICA, JPMORGAN CHASE, WELLS FARGO...	
Balance $2.000 - $5.000	$100 - $400
Balance $12.000 - $15.000	$600 - $1.000
Balance $20.000 +	$1.000 +
ACCOUNTS (UK) LLOYDS, BANK, BARCLAYS, HSBC...	
Balance 3.000 - 6.000 GBP	$150 - $600
Balance 10.000 - 16.000 GBP	$600 - $1.000
Balance 20.000 GBP+	$800 - $1.500
ATM CARDS WITH BALANCES AND PIN	
Balance $2.000 - $8.000	$100 - $500

CREDIT CARD DATA		
VISA / mastercard.	U.S.	$7 - $10
	UK	$15 - $25
	Canada	$15 - $25
	Australia	$25 - $27
	EU (Italy, Spain, France, Germany, Denmark, Sweden, Ireland)	$15 - $30

* Агрегированные данные за 2018 год из собственных исследований и публичных источников

Теневой рынок
– почему опасно?

Системы Информационной Безопасности

- Прямые финансовые потери при компрометации сервисов, кража активов и отток клиентов.

- Репутационные потери, сопутствующая громким утечкам «шумиха» в СМИ. Внеплановые проверки и повышенное внимание регуляторов, риски отзыва лицензий на ведение деятельности.

- Реакция на события «пост-фактум», часто о крупных утечках компании узнают от клиентов, партнеров, из публичных новостей или от профильных регуляторов.

Системы
Информационной
Безопасности

Наше решение
– что исследуем?

- Открытые и приватные источники информации по активности на теневом рынке информации.

- Собственная уникальная информационная база (поиск по закрытым участкам, в виде группировок, сервисов, магазинов, частных лиц и группировок). Референсный охват составляет более 1 миллиона участников теневых сообществ из различных сфер.

- Почты, корпоративные аккаунты, логи ботнетов, различные базы, архивы старых тем и переписок, маяки прошедших периодов. Архивные данные позволяют восстановить полную картину событий от подготовки до атаки.

Системы
Информационной
Безопасности

Наше решение
– как работает?

- Выявление и анализ текущих активностей на теневом рынке, связанных с заказчиком.

- Анализ маркеров состояния рынка, общего фона угроз, применимых к Заказчику.

- Оцениваются и анализируются общие показатели по компании, что позволяет оценивать влияние тех или иных действий со стороны компании на теневые сообщества.

- Прогнозирование последствий тех или иных действий и их влияние на фрод-сообщество.

- Уменьшение общего фона опасности для компаний за счет создания собственного информационного фона, который постепенно снижает активности атакующих групп.

Наше решение
– что дает?

Системы Информационной Безопасности

- Обнаружение скрытых угроз Вашему бизнесу, которые невозможно выявить другими методами.
- Возможность снизить ущерб по уже случившимся утечкам данных и превентивно отреагировать на компрометацию сервисов.
- Предотвращение потерь от внешних целевых атак на сервисы и инфраструктуру. Возможность адекватно подготовиться к вопросам клиентов, отреагировать на претензии по безопасности к компании от регуляторов и СМИ.
- Консультации, семинары и лекционные курсы по любым вопросам, связанным с черным рынком и теневыми сообществами.
- Создание и раскрутка виртуалов на заказ под любые нужды.

Системы
Информационной
Безопасности

Наше решение
– с чего начать?

- Подписать NDA.
- Выбрать вариант: демо или полноценное исследование.
- Подготовить стартовые данные для поиска:
  - доменные имена;
  - ip-адреса;
  - список лиц (ФИО, аккаунты в соц. сетях, почта, телефоны).
- Прислать данные нам на почту.

Системы
Информационной
Безопасности

Как с нами связаться?

+7 495 766-05-38
info@is-systems.org