kaspersky

Вирусы-вымогатели (ransomware):

И снова здравствуйте!...

"Количество":

1994

1 КВ*/ЧАС

2006

1 КВ/МИН

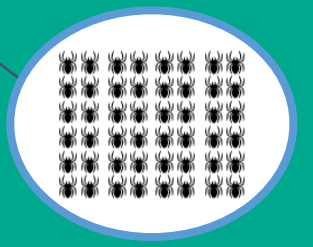
2011

1 КВ/СЕК

2019

4+ КВ/СЕК

(346000/СУТКИ)



* - КОМПЬЮТЕРНЫЙ ВИРУС

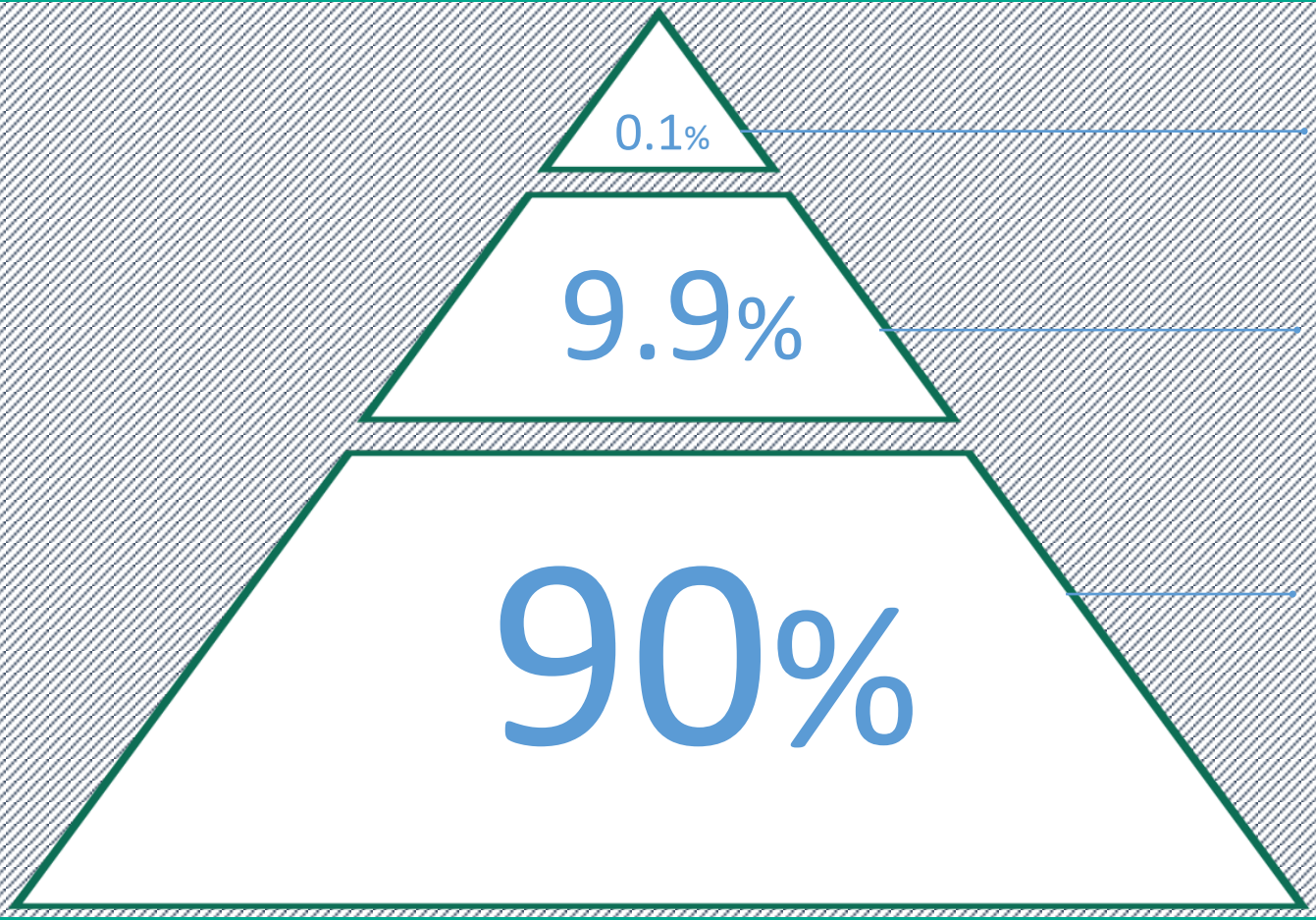
Рынок преступных киберуслуг: спрос втрое превышает предложение

Эксперты исследовали более 10 000 предложений теневого рынка киберуслуг:

- взлом сайта с получением полного контроля над веб-приложением - 150 $
- целевая атака - 4500 $
- ВПО для банкоматов - 1500 $
- DDoS-атака мощностью 270 Гбит/с в течение суток - 50 $

Где: DarkNet

"Качество":



кибероружие

APT (организованная киберпреступность)

"традиционная" киберпреступность (майнерство, бот-неты, вымогательство etc)

Кто (или что):

- **Блокировщики**: прописываются в автозагрузке и при перезапуске поражённого компьютера перехватывают управление, требуя ввод пароля, который предоставляется после уплаты выкупа.

Впервые зафиксированы в мае 2005 года

- **Шифровальщики**: осуществляют шифрование файлов в системе.

Впервые зафиксированы ровно через год – в мае 2006. Являются результатом «эволюции» блокировщиков, для которых может потребоваться эскалация привилегий, чего часто не требуется для манипуляций с файлами.

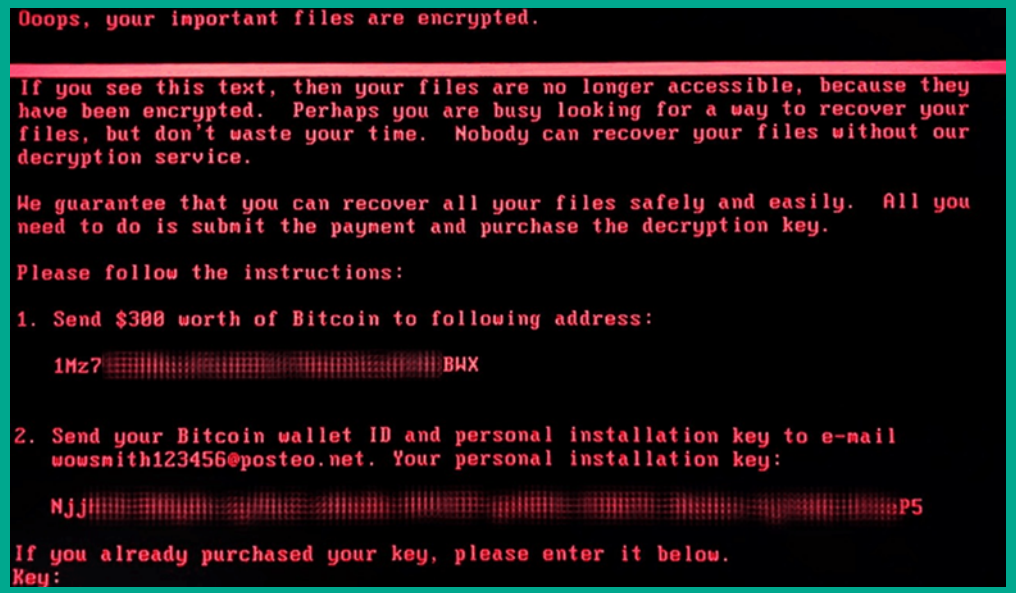
Как (через что):

- **Фишинг, спам etc**
- **Уязвимости (прежде всего – в сетевых службах)**
- **Цепочки поставки**
- **Комбинирование**

К 2013 году применение вирусов-вымогателей выросло в серьёзный «бизнес»:
только с 15 октября по 18 декабря операторам шифровальщика CryptoLocker удалось собрать около 27 миллионов долларов США (в биткойнах)

ExPetr (Petya, PetrWrap, NotPetya)

- Вирус-шифровальщик **без функции расшифровки**
- Начало эпидемии – июнь 2017 года
- Жертвы – корпоративные ("офисные") и банковские системы, АСУ ТП
- Распространялся через обновления (украинский офисный пакет M.E.Doc) и заражённые сайты
- Агрессивно использовал инструменты удалённого управления для захвата



ExPetr (продолжение):

- Украина: "чёрный вторник" 27.06.2017
  - ➢Были атакованы: Кабмин, Служба спецсвязи, Львовский горсовет, Киевска мэрия, телеканал "Интер" и др., всего – более 1000 сообщений об атаках
  - ➢Пострадали: аэропорт "Борисполь", ЧАЭС, Укртелеком, Укрпочта, Ощадбанк, Укрзализныця
  - ➢Потери – порядка 450 млн. долларов (оценочно)
- Транспортный гигант Maersk (около 300 млн долл. потерь)
- Merck (США, фармацевтика), «Роснефть» (в основном, её «дочка» «Башнефть»)

И снова здравствуйте! Ryuk

- Вирус-шифровальщик
- Декабрь 2019 года:
  - ➢Жертва – морской порт в США (какой - ???): 30 часов простоя
  - ➢Проник в результате фишинговой атаки, распространялся с использованием штатных средств администрирования, блокировал технологические и бизнес-процессы
  - ➢Ущерб – ??? (XYZ млн. долл.)
- Март 2020 года:
  - ➢ 10 больниц на территории США

И снова здравствуйте! Ragnar Locker

- Вирус-шифровальщик, проникает через RDP (но не только)
- Настройка на конкретную жертву, большой размер выкупа
- 14 апреля 2020 года была атакована компания Energias de Portugal (EDP):
  - ➢Зашифрованы данные
  - ➢Возможно, украдено более 10 Тб конфиденциальной информации
  - ➢Затребован выкуп – 10,9 млн. долл. (в биткойнах) с угрозой раскрытия украденных данных

И снова здравствуйте! Snake

- Вирус-шифровальщик, проникает через RDP (но не только)
- Настройка на конкретную жертву
- 8 июня 2020 года был атакован автопроизводитель Honda в Европе и Японии (пострадали службы поддержки клиентов и финансовые службы компании)

И снова здравствуйте! Netwalker

- Вирус-шифровальщик, проникает через RDP (но не только)
- В начале июня 2020 года был атакован Калифорнийский университет
- Заплачен выкуп – 1,14 млн.долл.

И снова здравствуйте! Digest (**существует мнение...**)

- 13 января: крупный производитель ткацких станков Picanol Group, зафиксировано серьезное нарушение в работе заводов в Бельгии, Румынии и Китае, 2300 сотрудников временно остались без работы
- 7-8 апреля: DESMI, датский производитель оборудования для судов и промышленности, на неделю были заблокированы электронная почта и элементы электронного документооборота. Возможна кража данных
- 7 мая: швейцарский производитель поездов Stadler, несколько компьютеров корпоративной сети были заражены, с них украдены данные, злоумышленники потребовали выкуп, угрожая их публикацией
- 14 мая: английская энергетическая компания Elexon – аналогичный случай

Что делать:

- Соблюдать **КИБЕРГИГИЕНУ** (**АКТИВНО РАБОТАТЬ С ПЕРСОНАЛОМ!!!**)
- Использовать антивирусное ПО и другие средства защиты информации
- Разработать и выполнять политику резервного копирования
- Разработать и выполнять политику обновлений для операционной системы и прикладного ПО
- По возможности ограничить использование RDP, сторонних утилит удаленного администрирования, а также круг лиц, их применяющих
- При появлении признаков атаки изолировать атакованные системы, принудительно сменить все пароли, которые могли быть скомпрометированы

kaspersky

Спасибо за внимание!

Вопросы?

Сатанин Дмитрий Николаевич
Office: +7 495 797 87 00 x5333 I Mobile: +7 916 939 61 62 I dmitry.satanin@kaspersky.com
АО "Лаборатория Касперского"
Москва, 125212
Ленинградское шоссе, д.39А, стр.3
+7 (495) 797-87-00
www.kaspersky.ru