Вирус «Bad Rabbit»

АВТОР:
ШНАЙДЕР А.В.

Компьютерные вирусы

Компьютерный вирус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Компьютерные вирусы

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п.

История вирусов

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.

Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. Andy Hopkins). В начале 1985 года Ги Вон (англ. Gee Wong) написал программу DPROTECT — первый резидентный антивирус.

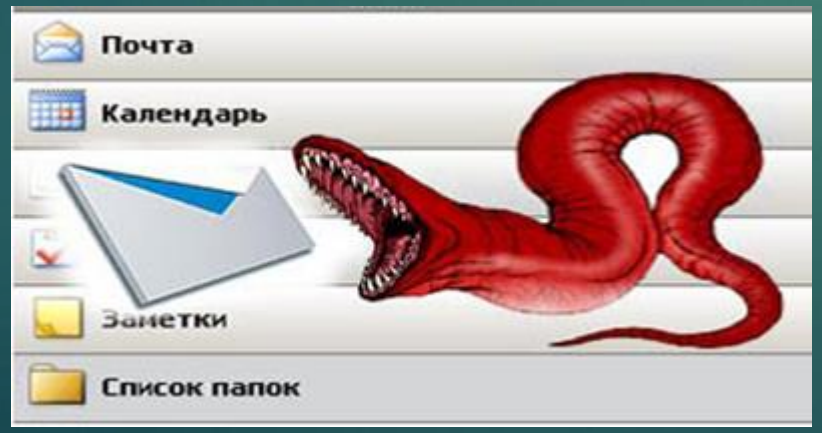
```
  Elk Cloner:  The program with a personality

   It will get on all your disks
     It will infiltrate your chips
       Yes it's Cloner!

   It will stick to you like glue
     It will modify ram too
       Send in the Cloner!
Перевод:
Elk Cloner: программа с индивидуальностью

   Он проникнет во все ваши диски
     Он внедрится в ваши чипы
       Да, это - Cloner!

   Он прилипнет к вам как клей
     Он даже изменит оперативную память
       Отправь Cloner
```

Механизм работы вирусов

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое.

Механизм работы вирусов

После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения. Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, например удаление данных или кража конфиденциальной информации.

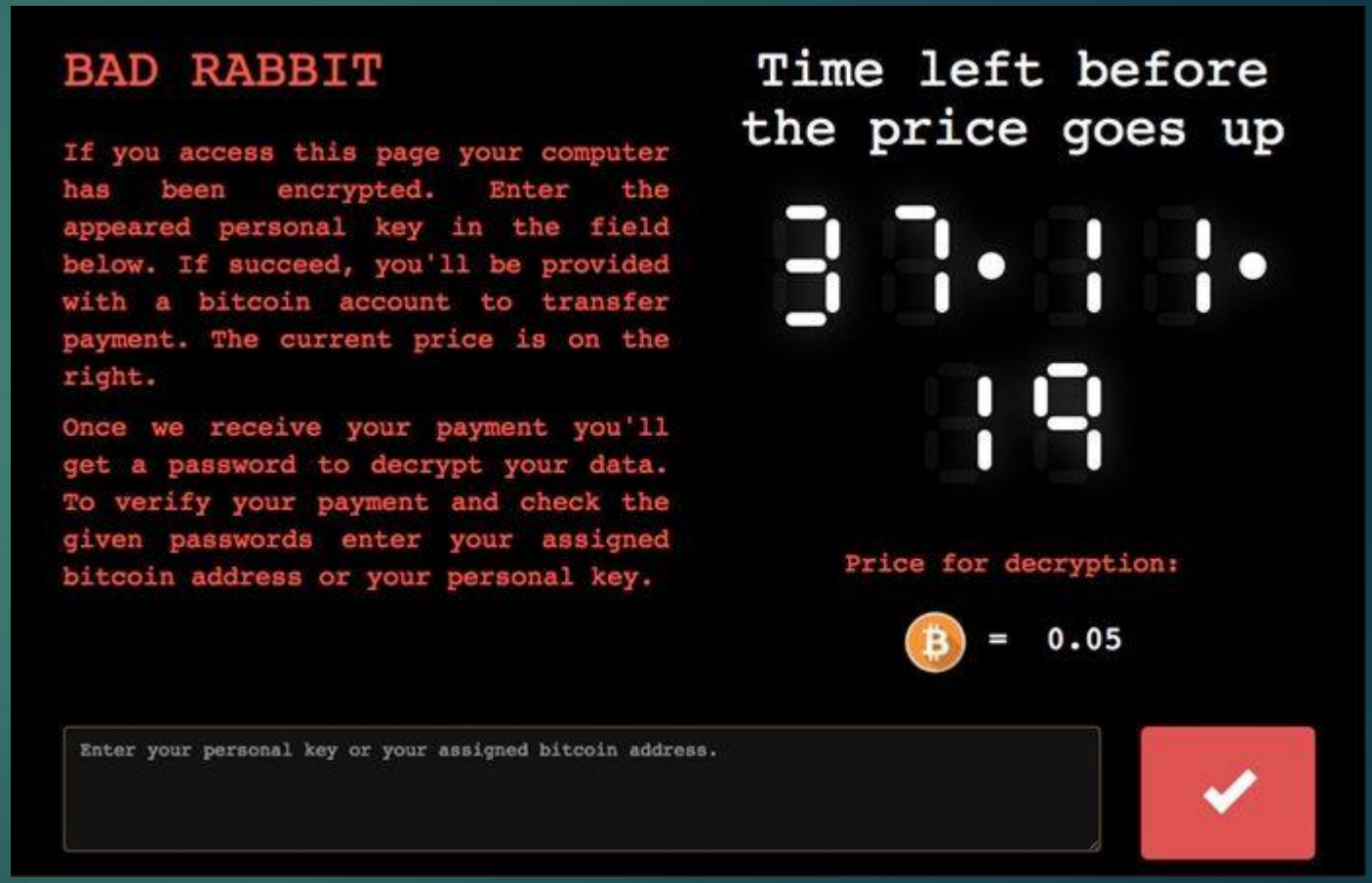


Способы распространения

- Дискеты
- Флэш-накопители
- Электронная почта
- Сообщения с ссылками
- Веб-страницы
- Интернет и локальные сети

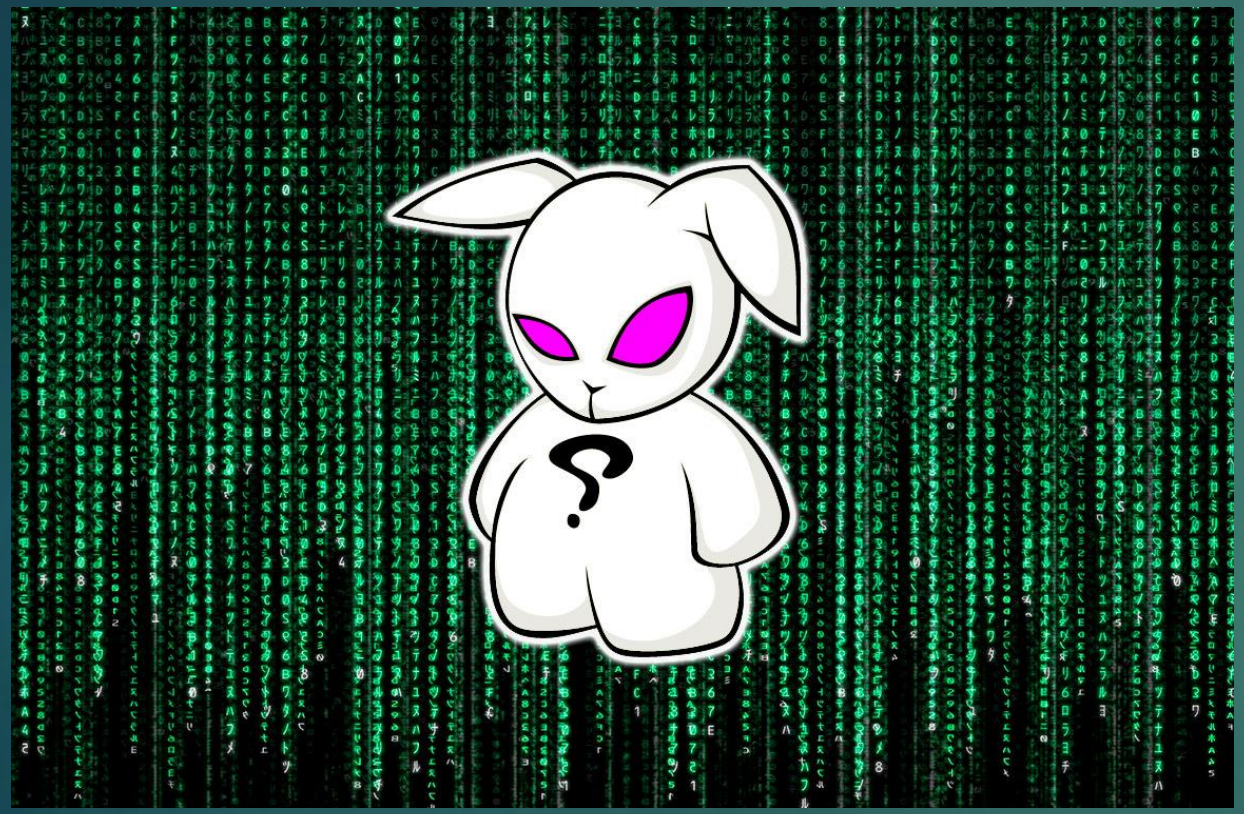
Вирус Bad Rabbit

Bad Rabbit (рус. «Плохой кролик») — вирус-шифровальщик, разработанный для ОС семейства Windows и обнаруженный 24 октября 2017 года. По предположениям аналитиков, программа имеет сходство отдельных фрагментов с вирусом NotPetya.



Выдаваемое вирусом окно

Источник распространения вируса

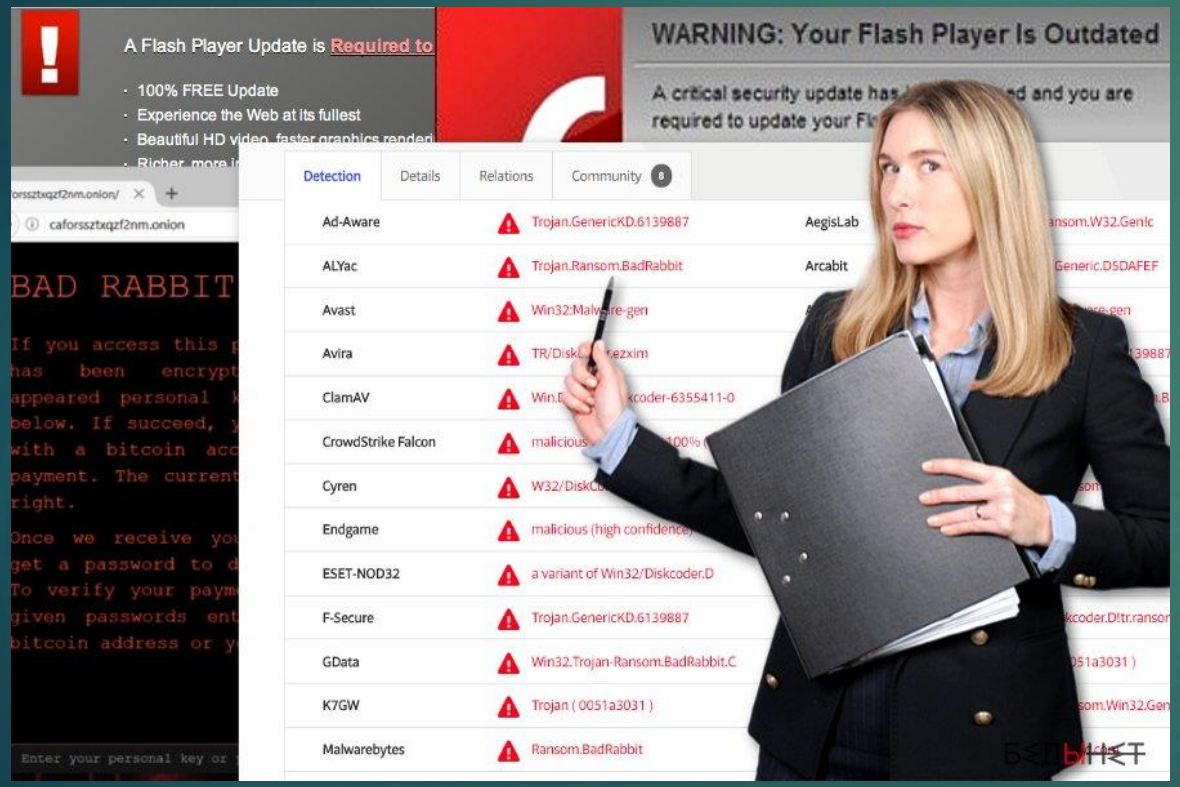


Специалисты компании Group-IB определили доменное имя, откуда началось распространение вируса. "Расследование показало, что раздача вредоносного ПО проводилась с ресурса 1dnscontrol.com. Доменное имя 1dnscontrol.com имеет IP 5.61.37.209", — говорится в сообщении на сайте компании.

Метод атаки

Для первоначальной установки Вирус не использует каких-либо эксплойтов или уязвимостей: инсталлятор вируса, маскирующийся под установку обновления для Adobe Flash Player, должен быть скачан и запущен вручную пользователем, он запрашивает подтверждение повышения полномочий посредством UAC Windows.

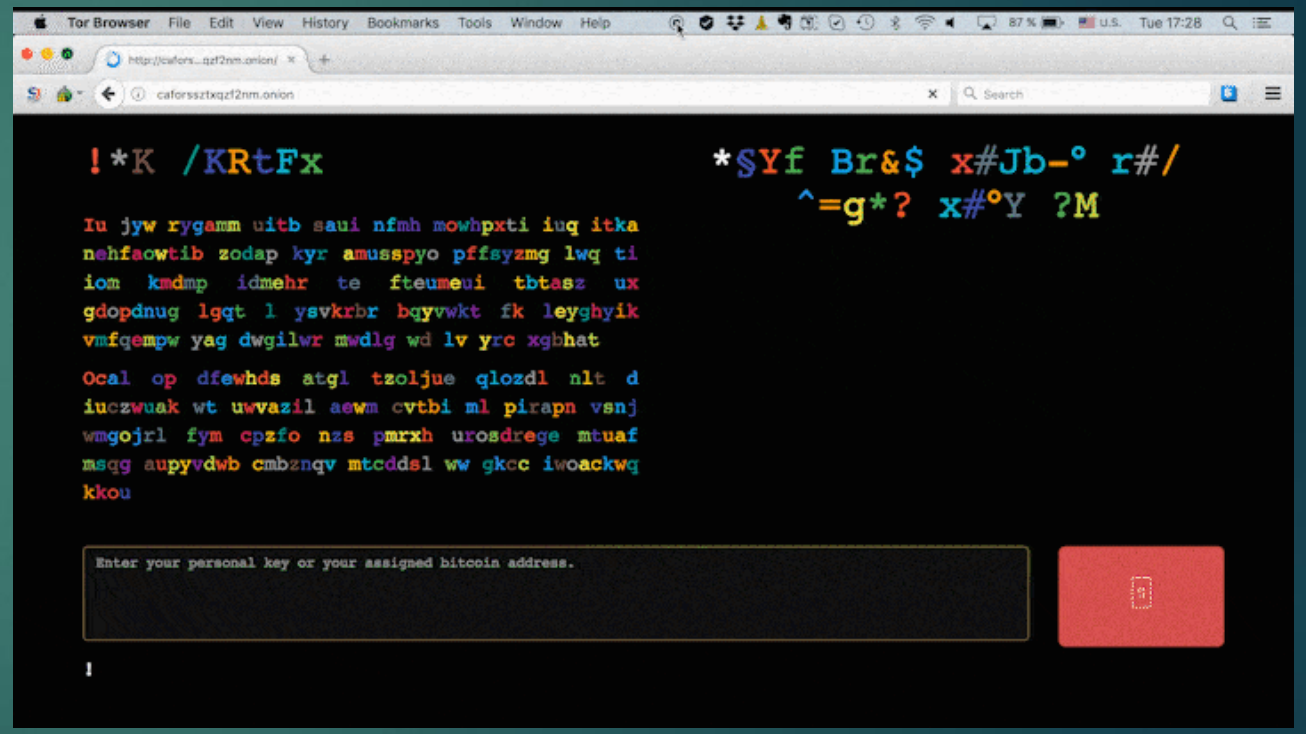
Метод атаки



После установки приложение регистрируется в штатном механизме планирования заданий и начинает самостоятельное распространение по локальной сети через удаленные подключения SMB и WMIC при помощи перехвата токенов и паролей утилитой Mimikatz и перебора паролей NTLM на удаленных узлах Windows для ряда распространенных имен пользователей. Приложение производит шифрование файлов по алгоритмам AES-128-CBC и RSA-2048

Подробности нападения

Вирус атаковал ряд российских СМИ, включая ИА «Интерфакс» и интернет-газету «Фонтанка», а также киевское метро и аэропорт Одесса. Также, в меньшей степени, атаке подверглись Турция и Германия. За разблокировку одного компьютера вирус требовал 0.05 BTC (на тот момент около 16 тыс. рублей).

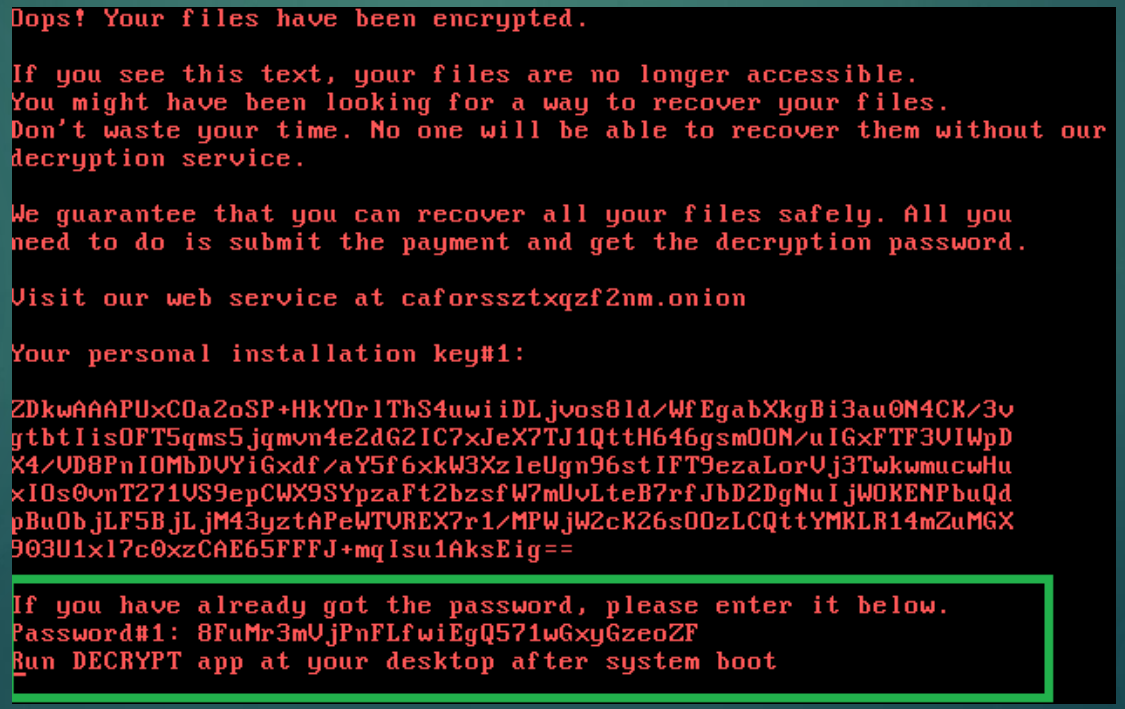


Связь между Bad Rabbit и NotPetya

"В ходе анализа установлено, что BadRabbit является модифицированной версией NotPetya с исправленными ошибками в алгоритме шифрования. Код BadRabbit включает в себя части, полностью повторяющие NotPetya", — утверждают специалисты.

Связь между Bad Rabbit и NotPetya

Отмечается, что на связь атаки с использованием BadRabbit с предыдущей атакой NotPetya указывают совпадения в коде. В текущей атаке поменялось количество искомых имен процессов, а сама функция вычисления хеша была скомпилирована в виде отдельной функции компилятором.




Спасибо за твое внимание!