История компьютерных вирусов

Проект подготовил студент группы ЗИ-280

Сколков Е.В.

Содержание

- КРАТКАЯ ИСТОРИЯ ВИРУСОВ
- SLAMMER
- CODE RED
- ILOVEYOU
- SOBIG.F
- MYDOOM
- MRSMAJOR 2.0.EXE (BOSSDAMAJOR)
- PETYA
- NJRAT
- BAD RABBIT

Краткая история вирусов

Что такое компьютерный вирус? Идея компьютерных вирусов впервые обсуждалась в серии лекций математика Джона фон Неймана в конце 1940-х годов; в 1966 году вышла его монография «Теория самовоспроизводящихся автоматов» – по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма – например, компьютерного кода – который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус.

Как отмечается на сайте Discovery, программа Creeper, о которой часто говорят как о первом вирусе, была создана в 1971 году сотрудником компании BBN Бобом Томасом. По факту, Creeper был создан как тестовая программа, чтобы проверить, возможна ли в принципе самовоспроизводящаяся программа. Оказалось, что в некотором смысле возможна. Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper не совершал никаких вредоносных действий – он только выводил простое сообщение: "I'M THE CREEPER. CATCH ME IF YOU CAN!" (Я CREEPER. ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ!)

SLAMMER

Slammer — это червь, который появился в 2003 году. Как и многие другие вирусы, Slammer имел несколько названий. Он стал известен также как SQL Slammer, Saphire, WORM_SQLP1434.A, SQL Hell или Helkern.

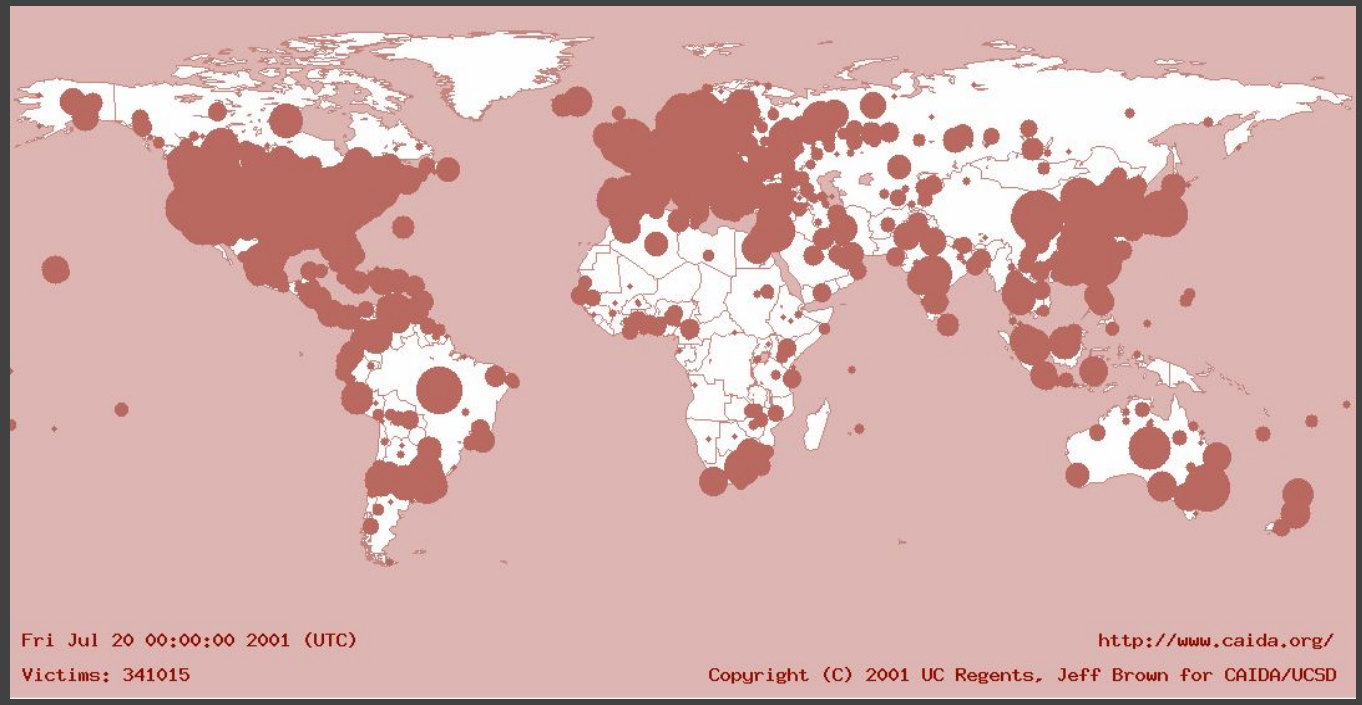
- Slammer инфицировал около 200 000 компьютеров. Ущерб, который он причинил, оценивается в 1,2 млрд долларов США.
- Целью стали серверы баз данных, на которых был установлен Microsoft SQL Server 2000. Собственно говоря, распространения этого вредителя можно было бы избежать. Компания Microsoft уже выпустила патч для устранения уязвимости — вот только многие не стали его инсталлировать.
- Slammer отправлял непрерывный поток данных и тем самым существенно замедлял доступ к интернету. Из-за этого некоторые хосты совсем застопорились. Также пострадал сервер одной из американских АЭС — система безопасности была парализована.

Карта заражения вирусом SLAMMER

CODE RED

Это тоже червь, уже одно только название которого выглядит угрожающе. В 2001 году он прокрался через уязвимость в Internet Information Server компании Microsoft и стал распространяться от одного веб-сервера к другому.

- Цель червя заключалась в том, чтобы изменять содержимое веб-страниц.
- Кроме того, в направлении определенных IP-адресов им была инициирована так называемая DDoS-атака. DDoS-атаки должны делать серверы недоступными. Самой известной жертвой подобной атаки со стороны CODE RED стал сервер Белого дома.
- Code Red инфицировал 400 000 серверов в течение всего одной недели. В общей сложности червем были затронуты около 1 млн ПК, а причиненный ущерб составил приблизительно 2,6 млрд долларов США.



Карта заражения вирусом CODE RED

ILOVEYOU

ILOVEYOU, известный также под названием Loveletter — это, к сожалению, не признание в любви, а также компьютерный червь. В мае 2000 года множество интернет-пользователей получили по электронной почте письмо с признанием в любви, «содержащемся» в прикрепленном файле. Однако радость была недолгой — как только пользователь открывал почту, вирус прочно заседал в почтовой программе и на жестком диске.

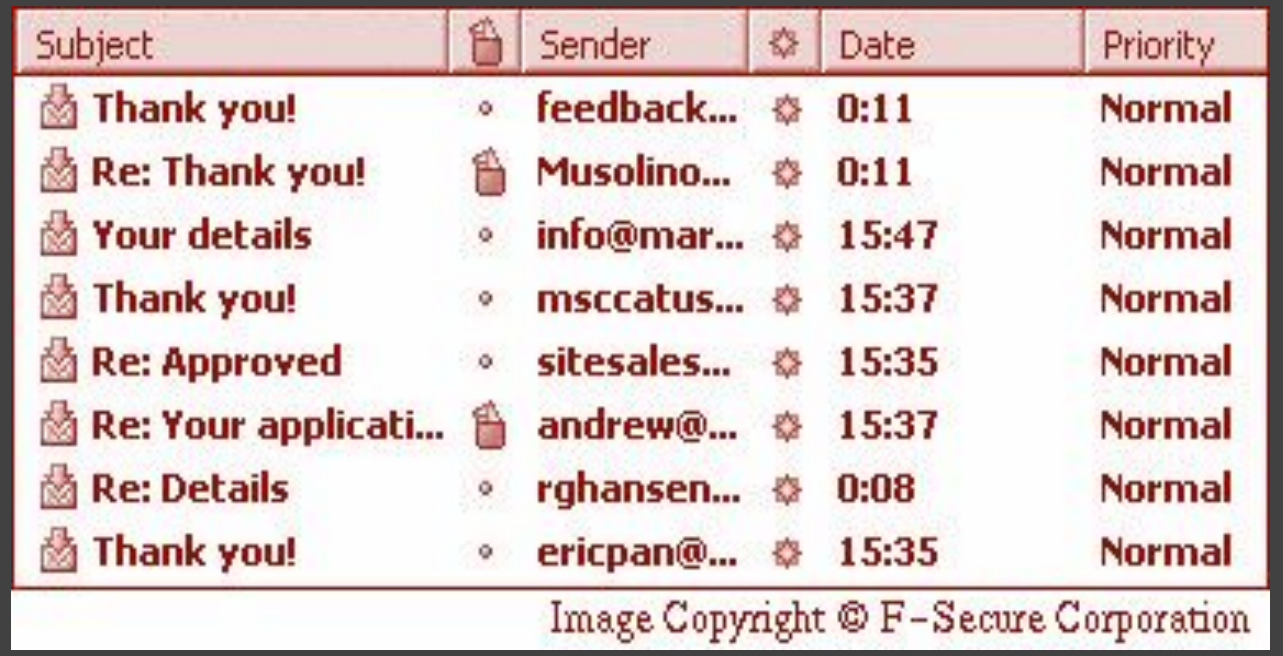
- Затем вирус приступал к самораспространению: он отправлял себя по почте контактам из адресной книги.
- Loveletter перезаписывал графические файлы и похищал пароли с компьютеров.
- Данный червь инфицировал более 3 млн компьютеров, ему удалось нанести ущерб, оцениваемый аж в 15 млрд долларов США. Предполагаемым местом происхождения ILOVEYOU считаются Филиппины. Там подозревали даже трех конкретных людей. Однако для предполагаемых авторов вируса последствий в любом случае не последовало: в те времена на Филиппинах попросту не существовало законов, предусматривающих ответственность за распространение вредоносных программ.

То самое письмо

SOBIG.F

SOBIG.F — это одновременно и самокопирующийся червь и троянец, а появился он в августе 2003 года.

- 2 миллиона инфицированных компьютеров и нанесенный ущерб, превышающим 37 млрд долларов США
- Он был быстрым, следует признать это за Sobig.F: в течение 24 часов вредитель сумел отправить около миллиона своих копий.
- Не только почтовые сервисы были перегружены гигантским потоком данных, «упали» даже целые системы. В Вашингтоне отправка электронной почты и обмен данными в течение короткого времени вообще были невозможны. Многие компьютеры различных предприятий работали чрезвычайно медленно. Air Canada из-за Sobig.F вынуждена была отменить некоторые рейсы.
- Компания Microsoft даже объявила награду за поимку автора червя — 250 000 долларов США. Безрезультатно — на сегодняшний день имя разработчика Sobig.F не известно.
- Уже 10 сентября 2003 года Sobig.F вновь исчез с экранов компьютеров.

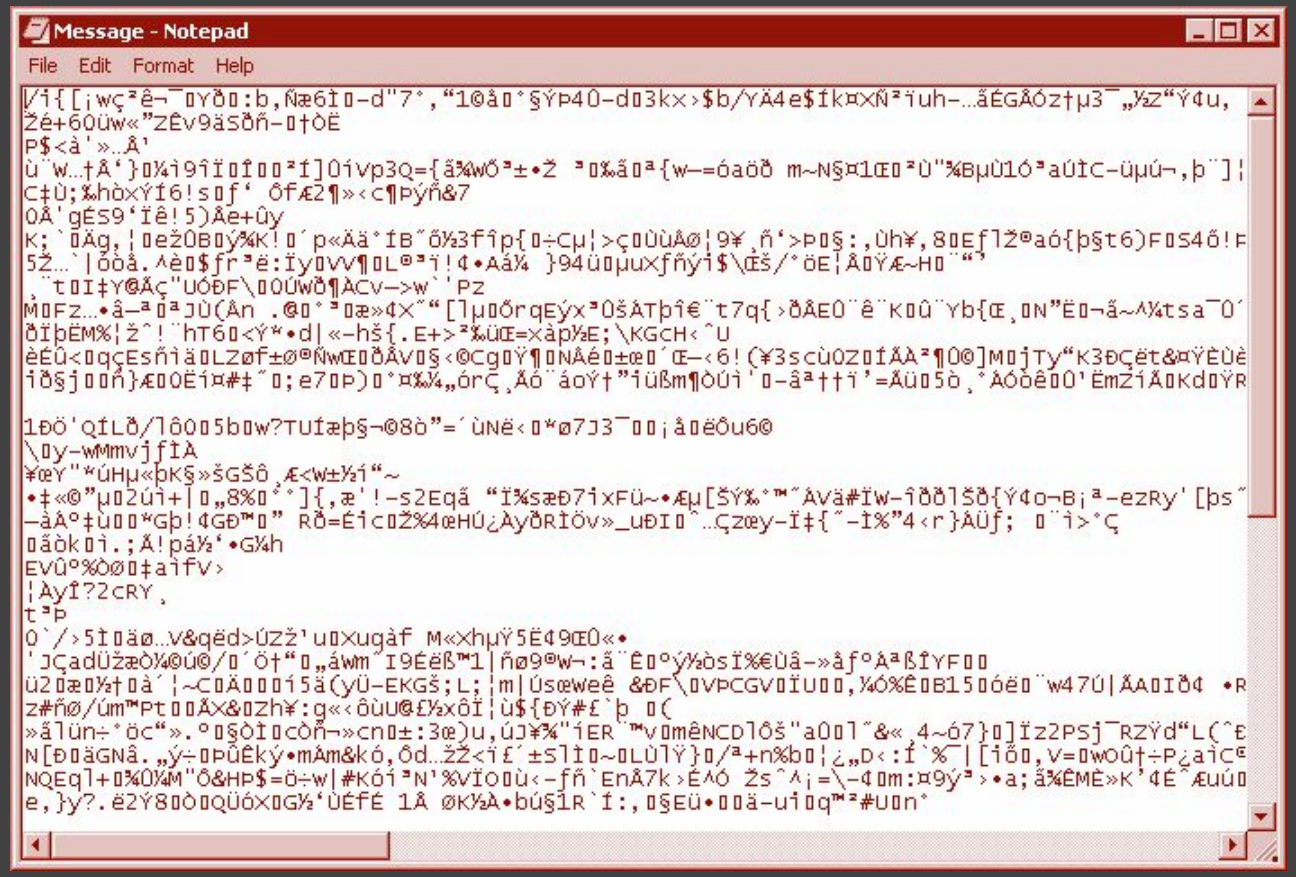


Действие вируса SOBIG.F

MYDOOM

MyDoom — это тоже червь, который «ползал» на свободе с января по февраль 2004 года. После этого MyDoom исчез.

- Mydoom распространялся через так называемые Bounce Message. Это уведомления «Non Delivery Notification», которые почтовый сервер создает в том случае, если письмо не удается доставить. Как только пользователь открывал такое уведомление, компьютер оказывался зараженным. Затем червь рассылал себя по всем контактам, которые только мог обнаружить.
- Mydoom замедлял интернет в целом примерно на 10 процентов, а время загрузки страниц увеличивалось на 50 процентов. Пик активности вируса был отмечен 26 января 2004 года: несколько часов последствия были заметны по всему миру.
- Инфицированы были 2 миллиона компьютеров. Ущерб, который Mydoom причинил за несколько недель, оценивается в невероятные 38 млрд долларов США.
- И в случае с MyDoom была объявлена награда «за голову» автора вируса в четверть миллиона долларов США.



Файл message создаваемый вирусом

MRSMAJOR 2.0.EXE (BOSSDAMAJOR)

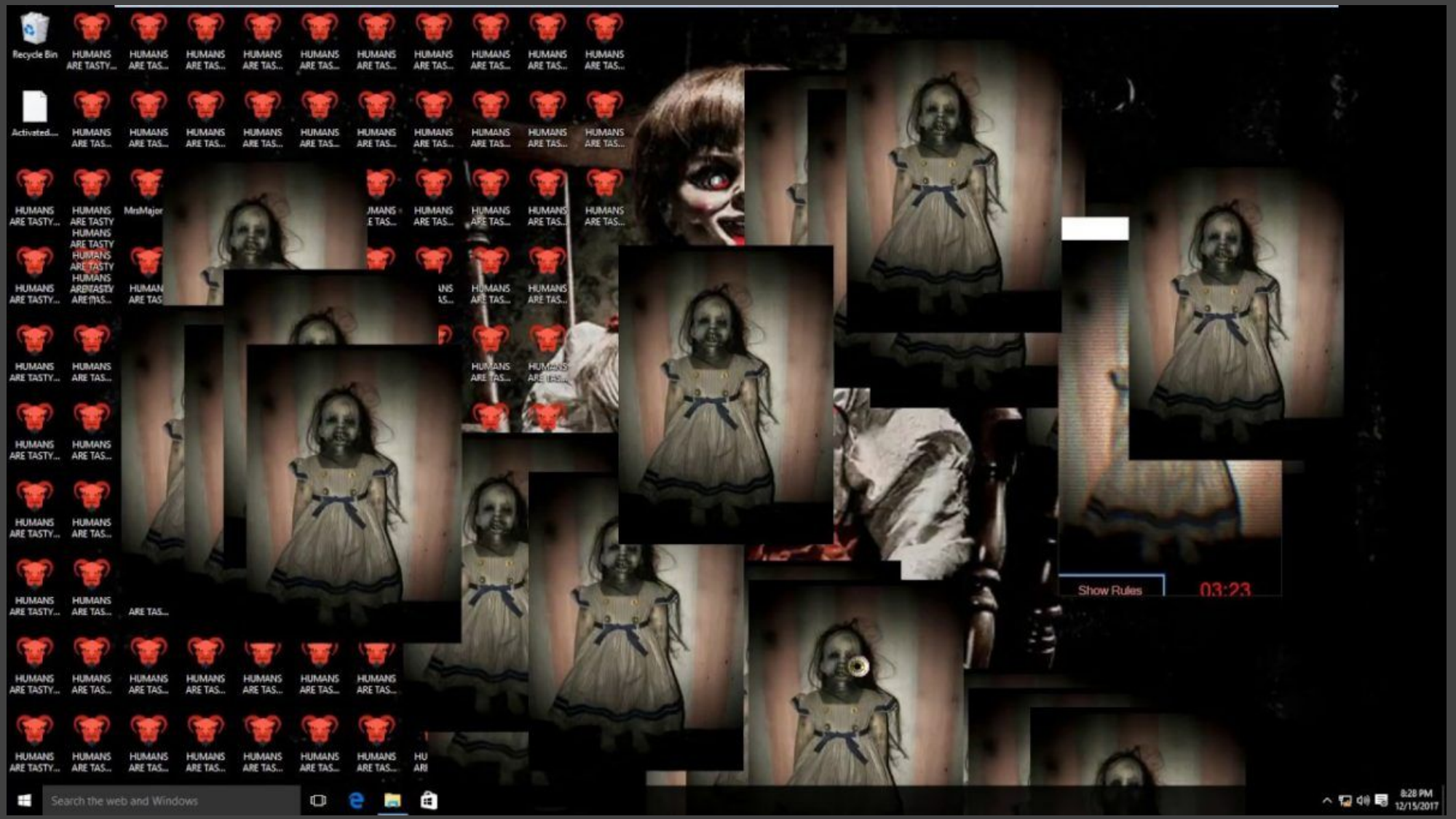
После запуска фон рабочего стола становится чёрным, а сам рабочий стол забивается файлами с названием «HUMANS ARE TASTY». После появляется окно с изображением госпожи Майор, 5-минутным таймером и кнопкой «Показать правила», и начинает играть напряжённая музыка. Также курсор заменяется на глазное яблоко.

Правила:

- *Если время на таймере вируса закончится, компьютер больше не включится.*
- *Если вы попытаетесь завершить процесс, компьютер получит непоправимый урон.*
- *Не удалять никаких файлов вируса.*
- *Удалить все антивирусы, т.к. они могут удалить вирус.*
- *Не запускать диспетчер задач, командную строку, Sethc.*
- *Не запускать компьютер в безопасном режиме.*
- *Не удалять ключи через msconfig и т.д.*
- *Иначе ваш компьютер не сможет больше запуститься.*

При запуске диспетчера задач на экране последовательно высветятся 4 слова «THERE IS NO ESCAPE».

Если пользователь нарушит правила, компьютер выдаст RSoD (Red Screen of Death). Код ошибки: «TROJANS_NEVER_JOKE_RESPECT_THE_TROJANS».

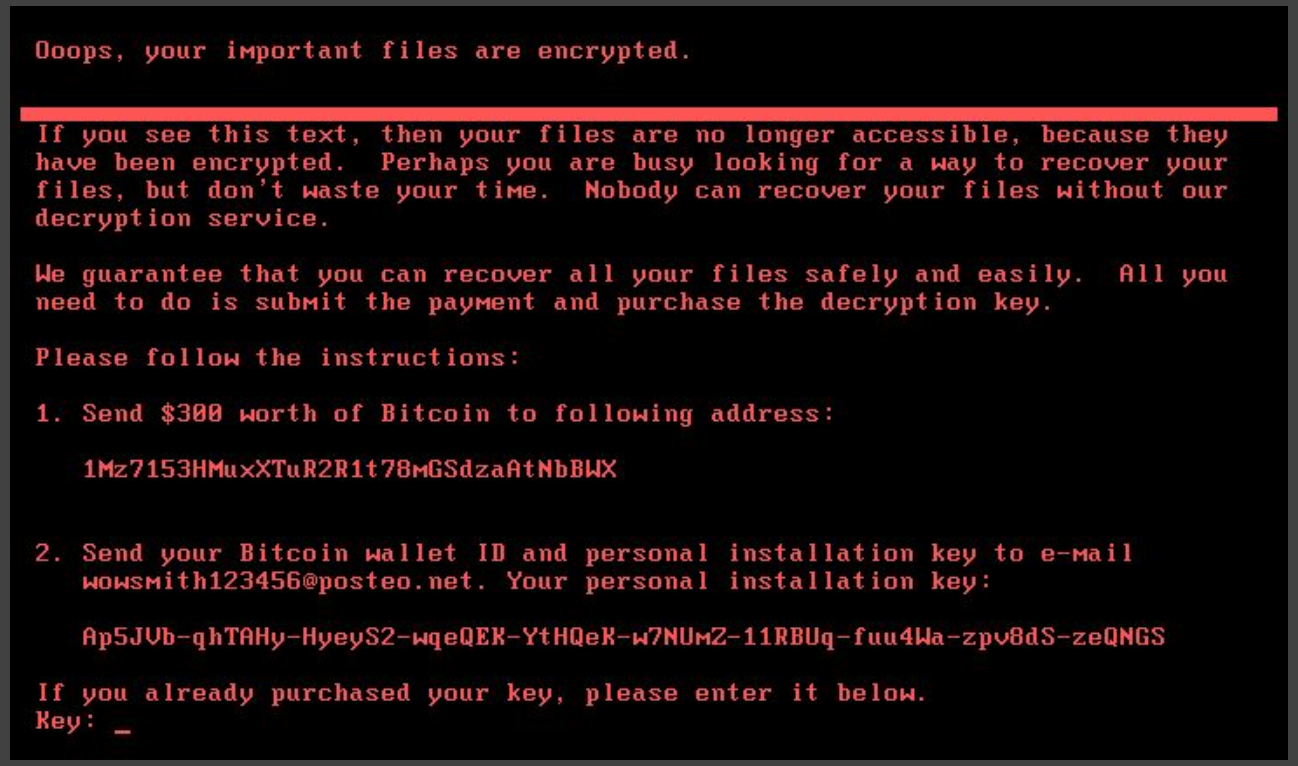


Действие вируса MRSMAJOR 2.0.EXE

PETYA

В начале мая порядка 230 000 компьютеров в более чем 150 странах были заражены вирусом-шифровальщиком WannaCry. Не успели жертвы устранить последствия этой атаки, как последовала новая — под названием Petya. От нее пострадали крупнейшие украинские и российские компании, а также госучреждения.

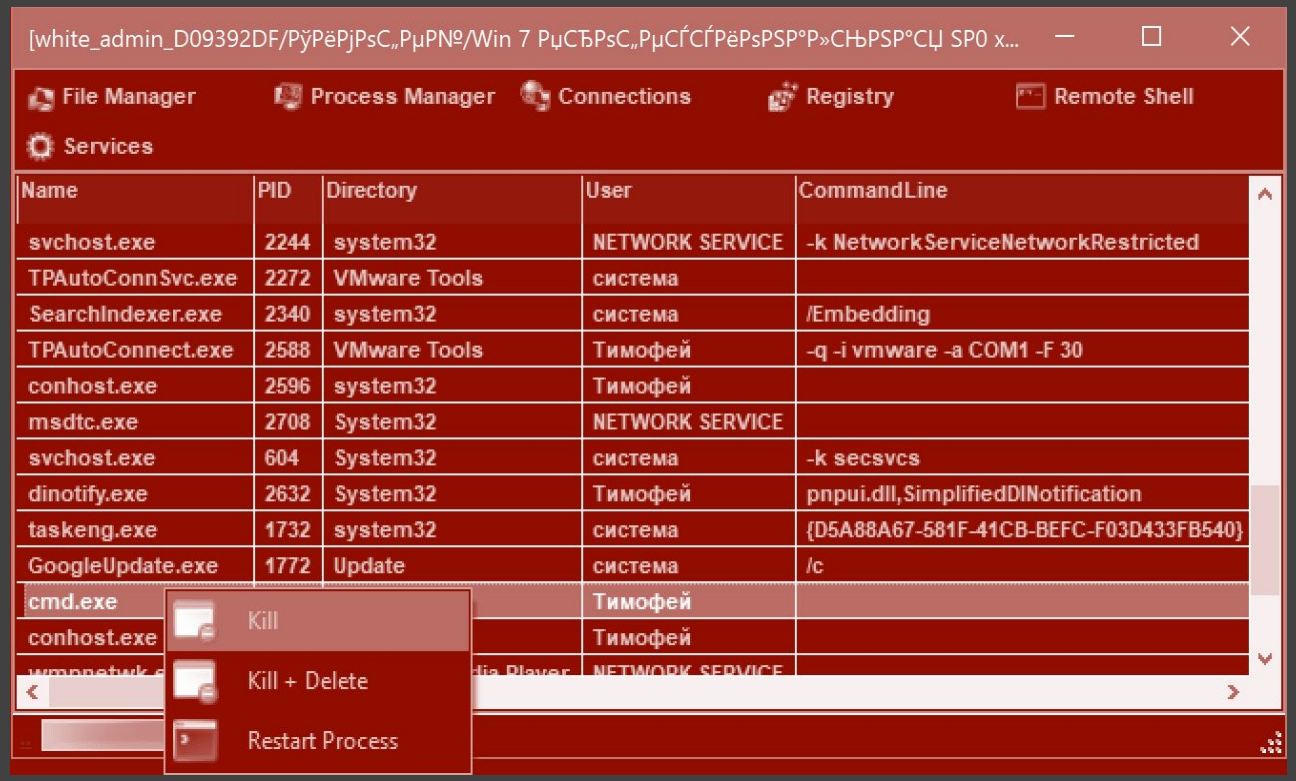
Попадая в компьютер, он скачивает из интернета шифровальщик и пытается поразить часть жесткого диска с данными, необходимыми для загрузки компьютера. Если ему это удается, то система выдает Blue Screen of Death («синий экран смерти»). После перезагрузки выходит сообщение о проверке жесткого диска с просьбой не отключать питание. Таким образом, вирус-шифровальщик выдает себя за системную программу по проверке диска, шифруя в это время файлы с определенными расширениями. В конце процесса появляется сообщение о блокировке компьютера и информация о том, как получить цифровой ключ для дешифровки данных. Вирус Petya требует выкупа, как правило, в биткоинах. Если у жертвы нет резервной копии файлов, она стоит перед выбором — заплатить сумму в размере $300 или потерять всю информацию.



Работа вируса PETYA

NJRAT

njRAT , также известный как **Bladabindi** , представляет собой троян для удаленного доступа, который позволяет владельцу программы управлять компьютером конечного пользователя. Впервые он был обнаружен в июне 2013 года, а некоторые варианты были прослежены до ноября 2012 года. Он был создан хакерской организацией из разных стран под названием Sparclyheason и часто использовался против целей на Ближнем Востоке. Он может распространяться через фишинг и зараженные диски.

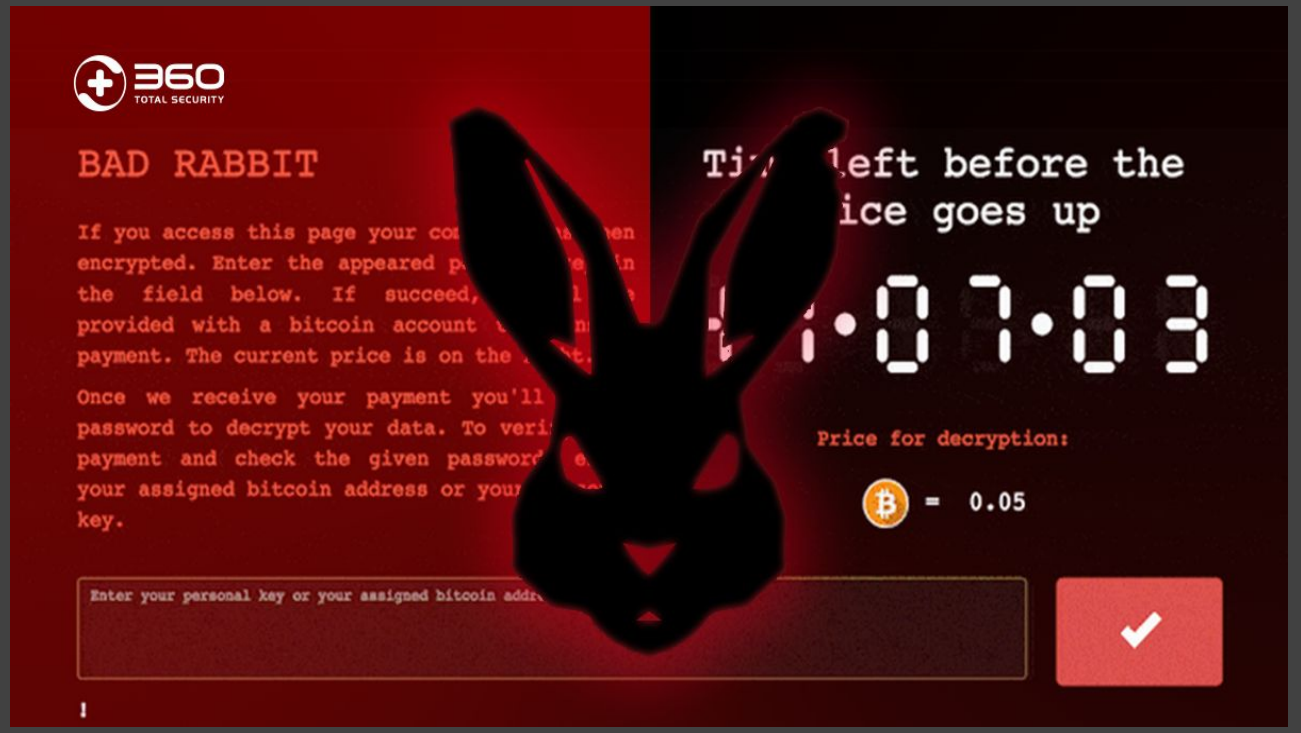


Интерфейс для использования NJRAT

BAD RABBIT

Bad Rabbit – это вирус, относящийся к шифрующим вирусам-вымогателям. Появился он совсем недавно и нацелен главным образом на компьютеры пользователей России и Украины, а также частично Германии и Турции.

После заражения BadRabbit создает в папке Windows файл infpub.dat, который создает остальные файлы программы: cscc.dat и dispci.exe, которые вносят свои изменения в настройки MBR диска пользователя и создают свои задачи подобно Планировщику задач. Эта вредоносная программа имеет свой персональный сайт для оплаты выкупа, пользуется сервисом шифрования DiskCryptor, шифрует методами RSA-2048 и AE, а также отслеживает все устройства, подключенные к данному компьютеру, пытаясь заразить и их тоже.



Работа вируса BAD RABBIT

СПАСИБО ЗА ВНИМАНИЕ