Как бороться с вирусом Wana Decrypt0r 2.0

Кто вирус ещё не поймал, заблокируйте 445 порт TCP, скачайте сейчас обновление от Micro$oft (просмотрите, какие ОС могут быть атакованы, WinXP в этом списке нет). Обновите антивирус (бесплатный 360 Total Security подойдет).

Не работайте под аккаунтом администратора (а сами аккаунты администратора должны иметь пароль, притом стойкий, а не тот, что по умолчанию). Не запускайте файлы с множественными расширениями (например, файл devkivoserekupalis.torrent.exe — явно не надо запускать). Чтобы видеть расширения — включите в настройках вида папок показ скрытых расширений.

Бесплатный китайский антивирь 360 Total Security хорош среди прочего тем, что он САМ обновляет винду собственными средствами из собственного репозитория, в который складывает микрософтовские обновления после того, как их проверит на беспроблемность. Это работает даже если у вас ломанная винда с левым ключом. Чтобы обновиться вручную через него — зайдите в раздел «Инструменты», там выберите «Уязвимости» — и он сам выдаст список обновлений, которые у вас еще не стоят. Фича — обновления делятся на обновления безопасности (надо ставить обязательно) и на функциональные обновления (исправляют всякие ошибки, не влияющие на безопасность, и добавляют/меняют функционал компонентов — в общем, их можно не ставить, или ставить выборочно).

Кроме того, в 360 Total Security появился специальный «инструмент для дешифрования ПО-вымогателей». Хе-хе, он вам поможет вернуть файлы, если вы уже влипли. Спасибо китайским контрразведчикам — они спасают мир.

Для любителей дрочить руками вприсядку — вот способ восстановления зараженной машины, пригодный для Windows Vista, 7, 8, 8.1, 10, а также Windows Server 2008/2012/2016:

1. Скачайте патч MS17-010 для нужной Windows <https://technet.microsoft.com/>...

2. Отключитесь от интернета.

3. Откройте командную строку (cmd) от имени администратора.

3.1 Пуск => В поиске вбиваете cmd => Нажимаете правой кнопкой мыши => Запуск от имени администратора

4. Вписываете эту команду в командную строку:

netsh advfirewall firewall addrule dir=in action= blockprotocol=tcp localport=445 name=»Block\_TCP-445″

4.1 Нажимаете Enter => Должно показать OK.

5. Заходите в безопасный режим

5.1 Во время загрузки и появления окна BIOS-a нажмите F8, после чего в списке выберите «Безопасный режим»

6. Найдите и удалите папку вируса

6.1 Для этого нажмите на любой ярлык вируса правой кнопкой мыши, выберите «Расположение файла», и удалите корневую папку.

7. Перезагрузите компьютер.

8. Зайдите в обычный режим, и запустите устанавливаться патч MS17-010

8.1 Во время установки подключитесь к интернету.

Вот и всё. У моих друзей всё заработало.

ЗЫ. Не удаляйте зашифрованные файлы (т.е. с расширением .wncry) — декриптор вам их восстановит.

источник выше указан.