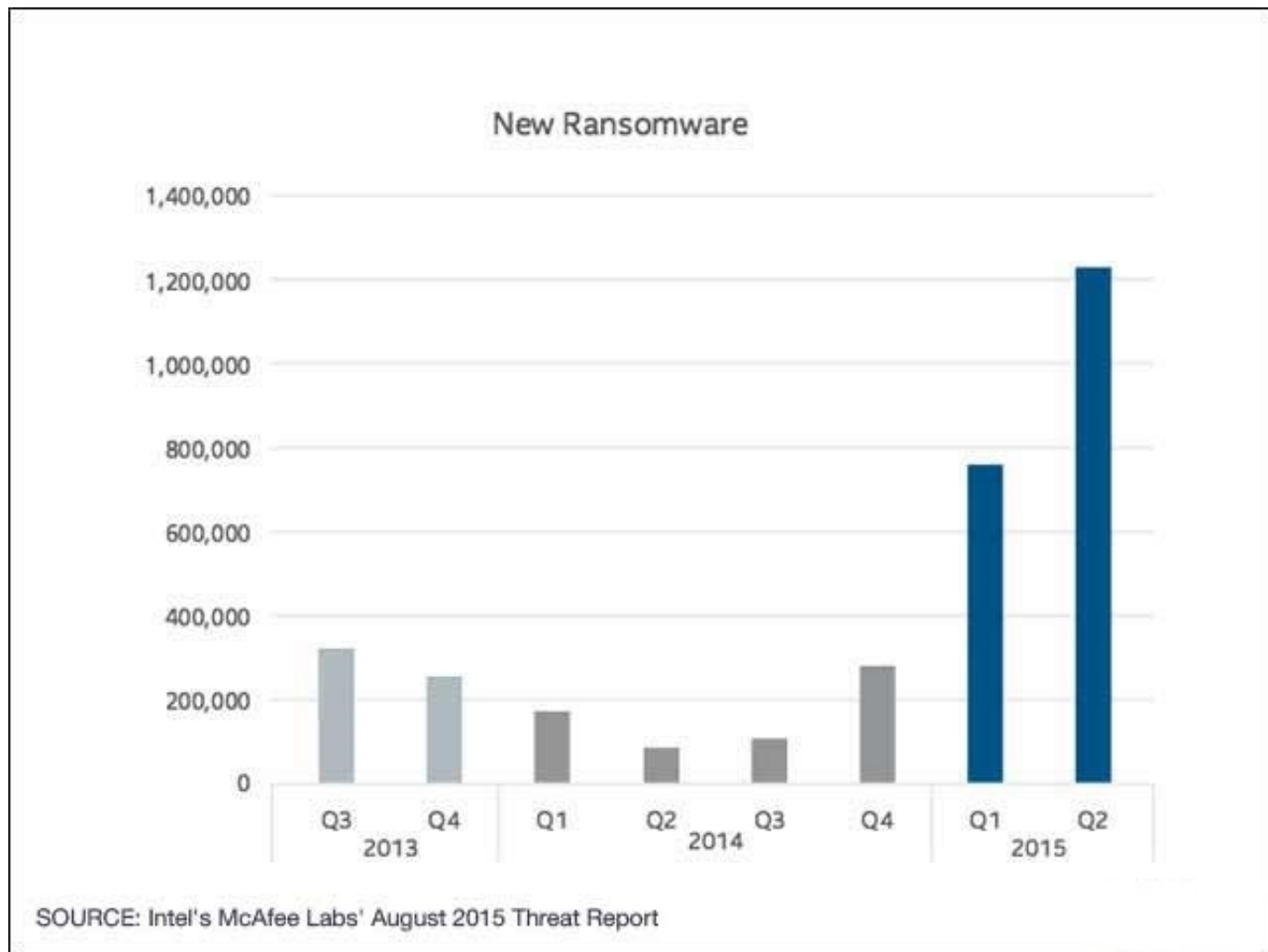


9 Февраля, 2016

## Готовимся к нашествию "криптолокеров"

### [Headlight Security](#)

Вирусы-шифровальщики обещают стать главной проблемой года. Об этом предупреждают и в [IBMX-Force](#), и в [Paloalto](#), и в [TrendMicro](#), а исследователи [Intel McAfee](#) не только в ужасе хватаются за голову, но и приводят статистику роста активности так называемых «ransomware» в первых двух кварталах 2015 года.



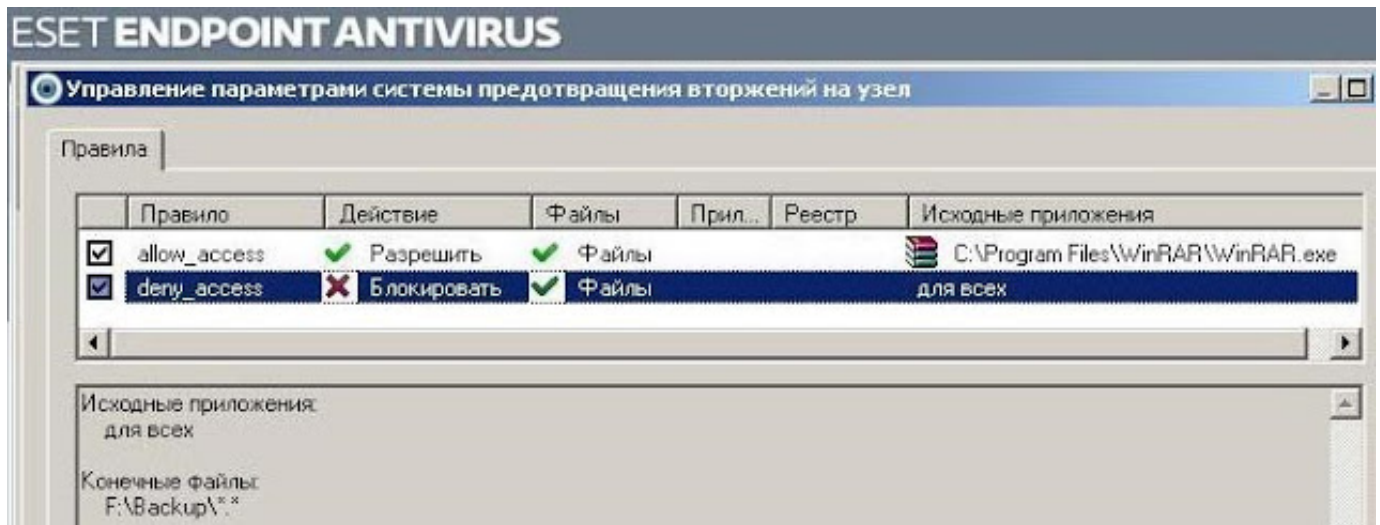
Как известно, программы-вымогатели проникают на компьютер пользователя, шифруют файлы (doc, docx, xls,xlsx, jpeg, pdf) и требуют выкуп за отправку ключа (от \$200 до \$5000). Сейчас различные версии этой заразы атакуют не только ПК, но и сайты, а также смартфоны. Большинство антивирусов со значительным опозданием реагируют на новые версии шифровальщиков, поэтому для защиты файлов требуются дополнительные превентивные меры.

Что предпринять в первую очередь?

### Делайте бэкапы

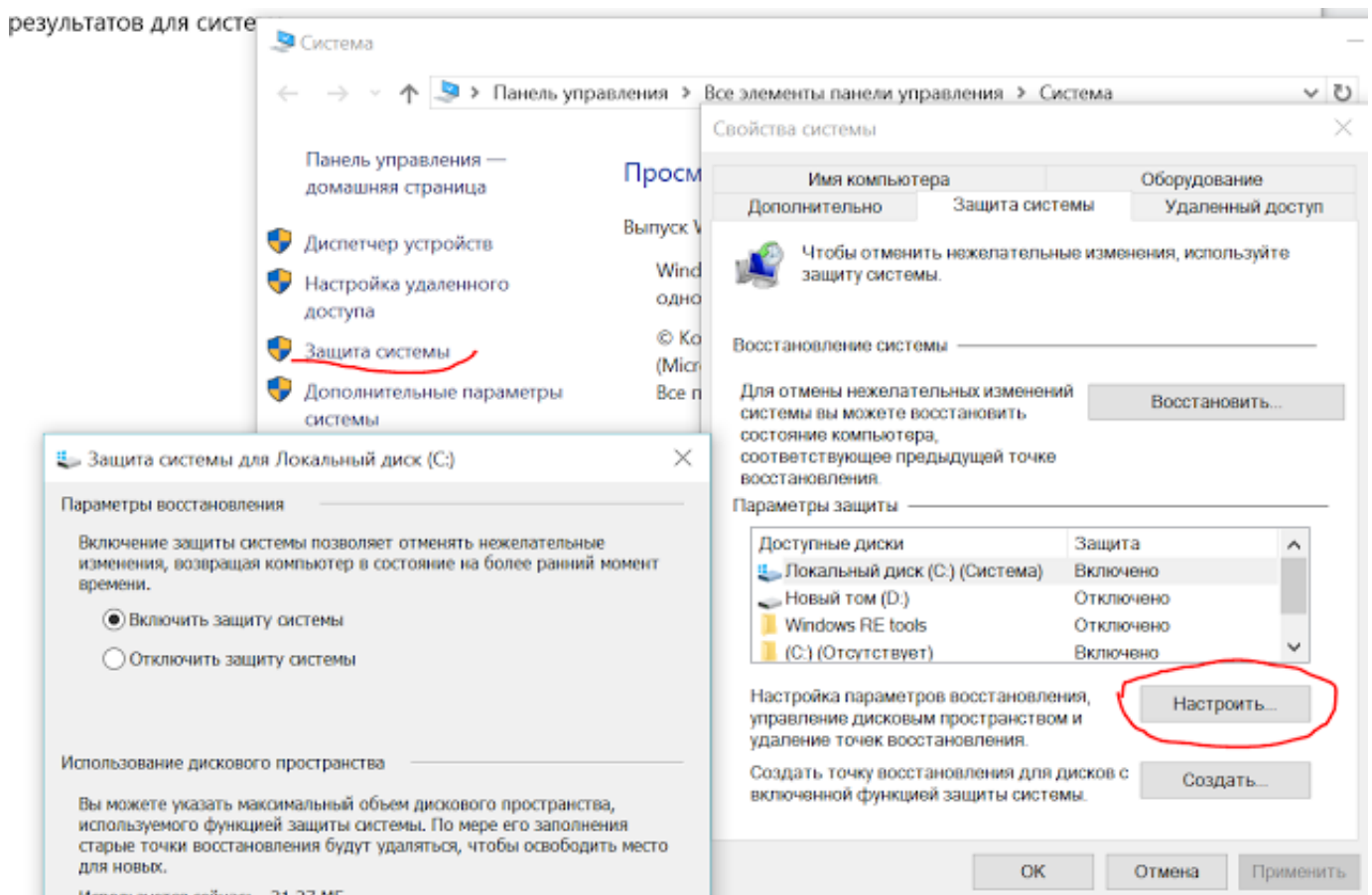
Резервное копирование – основной способ защиты файлов от модификации. Однако некоторые «криптолокеры» запросто шифруют данные и на сетевых папках. Для домашних пользователей рекомендуется защищать резервные папки с помощью локальных систем

предотвращения вторжений (Host Intrusion Prevention System, HIPS), которые встроены в некоторые антивирусы ( [ESETEndpointSecurity](#) , Kaspersky Internet Security, Kaspersky Endpoint Security). В данном случае одно правило должно запрещать для выбранной папки запись и удаление, а второе – разрешать эти действия программе, которая делает бэкап.



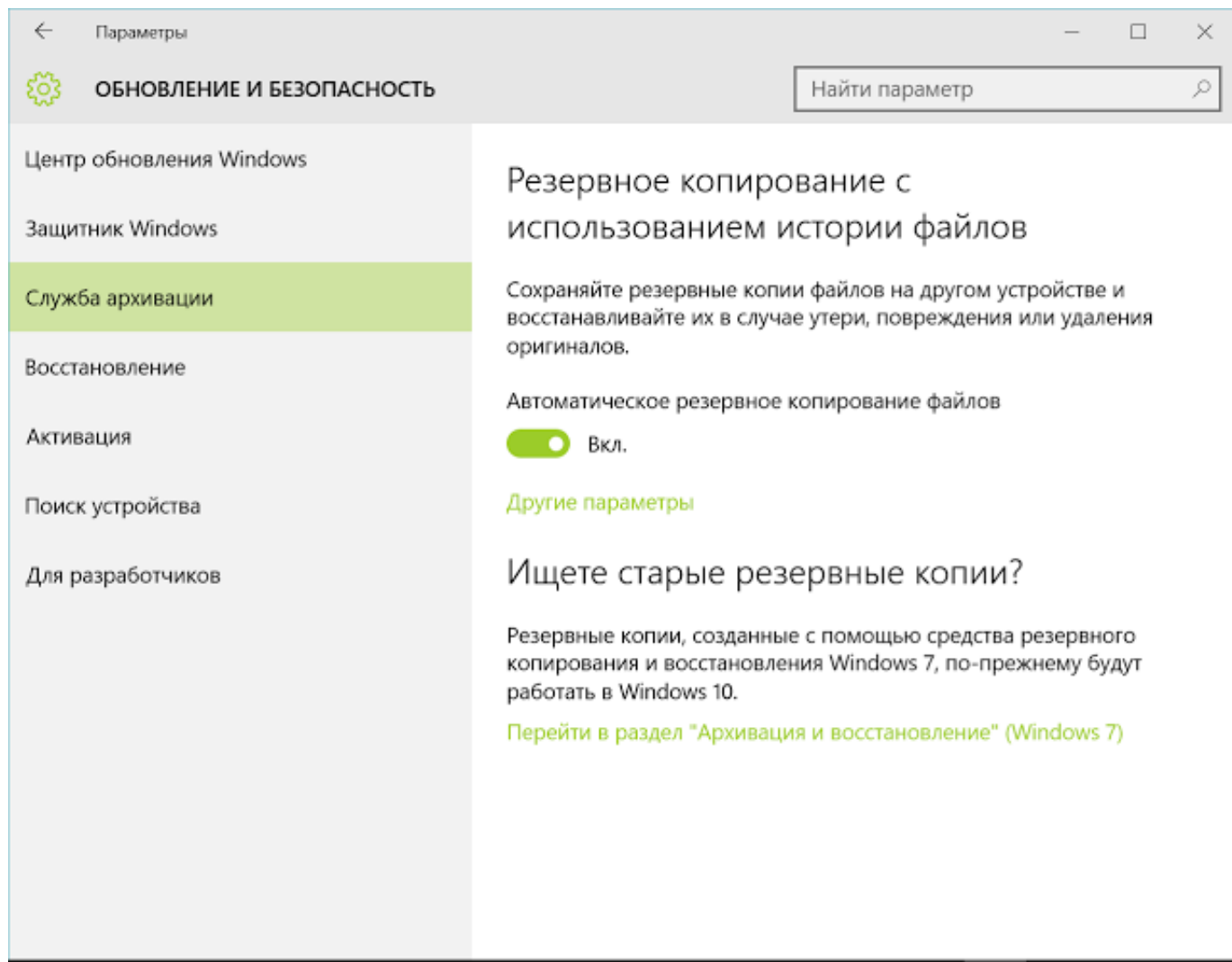
Можно доверить хранение резервных копий таким онлайн решениям, как Google Drive, Dropbox, Flickr, а чтобы зашифрованные зловредом файлы не затерли свои старые версии ( [один](#) из случаев), стоит дублировать данные с помощью решений «cloud-to-cloud backup», например Backupify или Spanning.

Кроме того, включите защиту системы в Windows, так как по умолчанию эта функция, как правило, отключена.

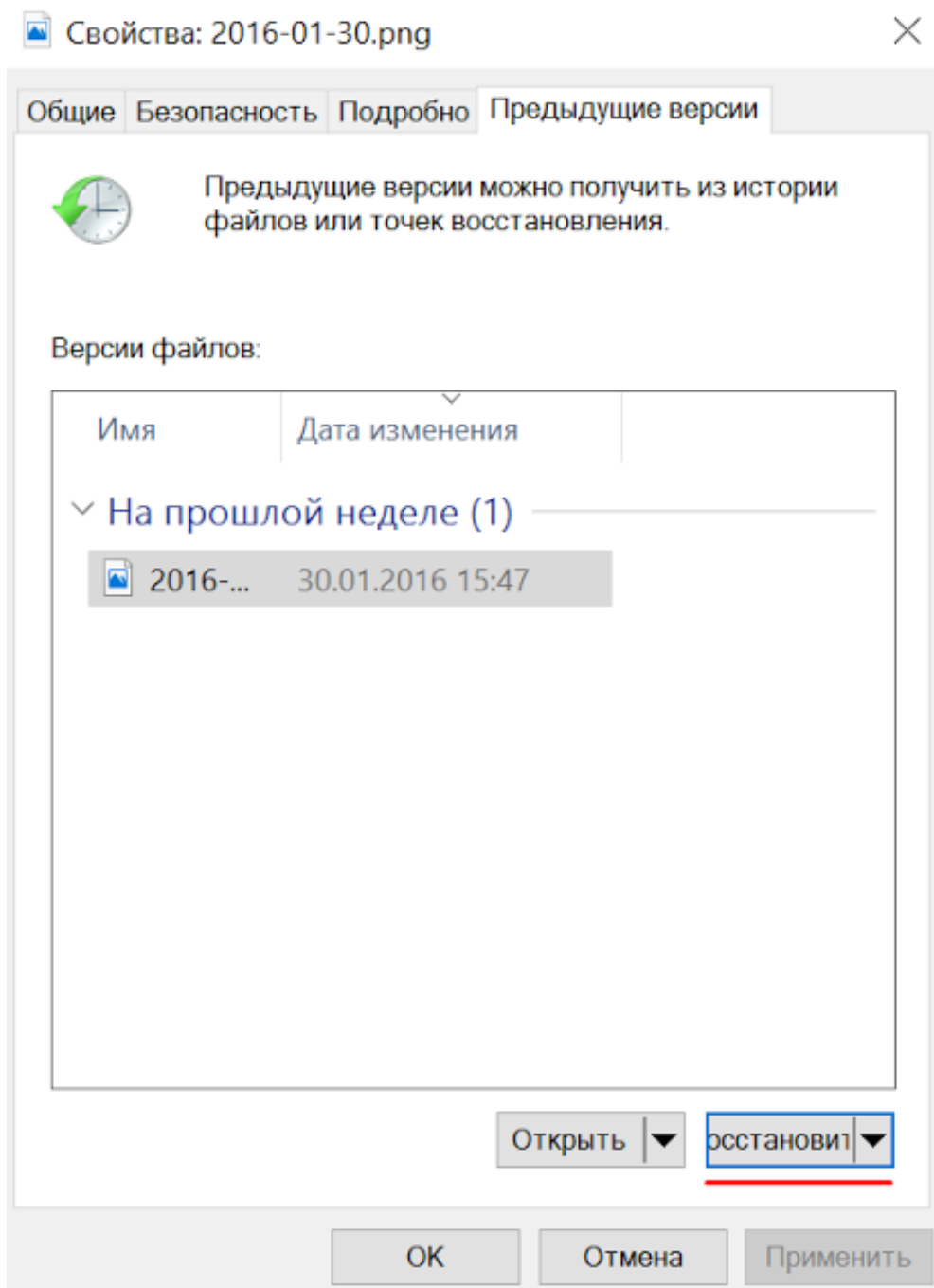


## Активируйте «историю файлов»

Для сохранения системой предыдущих версий файлов в случае Windows 10 наберите в поиске «Параметры», выберите пункт «Обновление и безопасность», далее – «Служба архивации», – «Резервное копирование использованием истории файлов». Можно не архивировать все подряд, меню «Другие параметры» позволяет выбрать конкретные папки, в которых лежат ваши важные файлы.




Наведите правой кнопкой мыши на файл, для которого включена история файлов, и выберете закладку «Предыдущие версии». Теперь его можно восстановить.






## Запретите открытие исполняемых файлов

Самый популярный способ попадания «криптолокера» на компьютер – открытие пользователем исполняемого файла, который замаскирован под офисный документ (.doc, .xls, .pdf).

Тексты писем выглядят весьма убедительно: *«Пожалуйста, сообщите, сколько еще ожидать оплату за услуги, оказанные в позапрошлом месяце? Мы еще три недели назад высылали Вам оригиналы счетов на оплату»*.

**Счета и акты приема** [andreyippe@front.ru](mailto:andreyippe@front.ru) [<mailto:andreyippe@front.ru>]

Отправлено: Пт 14.08.2015 10:39

Кому:  Простаков Илья Евгеньевич Сообщение  АКТ\_ООО-SoftCom.zip (2 Кбайт)

День добрый,

Прошу изучить и передать на подписание акты приема-передачи по контракту от 21.08.2015 года, а также оплатить соответствующие счета (сканы документации во вложении).

К слову, по нашей информации за Вашей компанией числится небольшая недоплата за прошлый месяц. Проверьте, пожалуйста, еще и предыдущий платеж.

Надеемся на дальнейшее сотрудничество..

---

С Ув.,

И.С. Сокур

зам главбуха Общества с ограниченной ответственностью "Софт - Ком"

В первую очередь необходимо включить «отображать расширение зарегистрированных типов файлов» и объяснить своим домочадцам или сотрудникам, что файлы с расширениями .exe, .js, .com, .pif, .cmd, .scr, .bat не могут быть офисными документами.

Например, один из самых распространенных «криптолокеров» Vault имеет расширение .js и является программой на языке Java Script. Чтобы случайно не открыть подобный зловред, можно воспользоваться наиболее примитивным способом – создать текстовый файл, изменить ему расширение на .js, а затем правой клавишей мыши назначить текстовый файл для постоянного открытия .js. В браузере Java Script естественно продолжит работать.

Весьма гибкие возможности контроля файлов предоставляют средства AppLocker или SRP ([подробнее](#)) в Windows, но эти функции присутствуют только в Enterprise- и Ultimate-редакциях операционной системы.

## Установите Malwarebytes Anti-Ransomware

Это бесплатный инструмент пока еще находится на этапе [открытого бета-тестирования](#) и может удалить не только на программу-вымогатели (заявлена поддержка CryptoLocker, CryptoWall, CTBLocker), но, и например, Skype. Решение этой проблемы предложил пользователь ViP с ресурса [itc.ua](#).



ViP · 6 дней назад

Удаляет Skype.exe. Просто, не перезагружайтесь. Сразу идите в раздел Exclusions (3-я кнопка). Там Add Files и укажите Skype.exe, который лежит здесь: c:\Program Files (x86)\Skype\Phone\.

Из карантина восстановить не даст до перезагрузки. Перезагружаетесь и потом в Quarantine нажимаете Restore и он вернет файл и уже удалять не будет. Вот такое, пока, неудобство в Beta 2.

1 ^ | v · Ответить · Поделиться &gt;

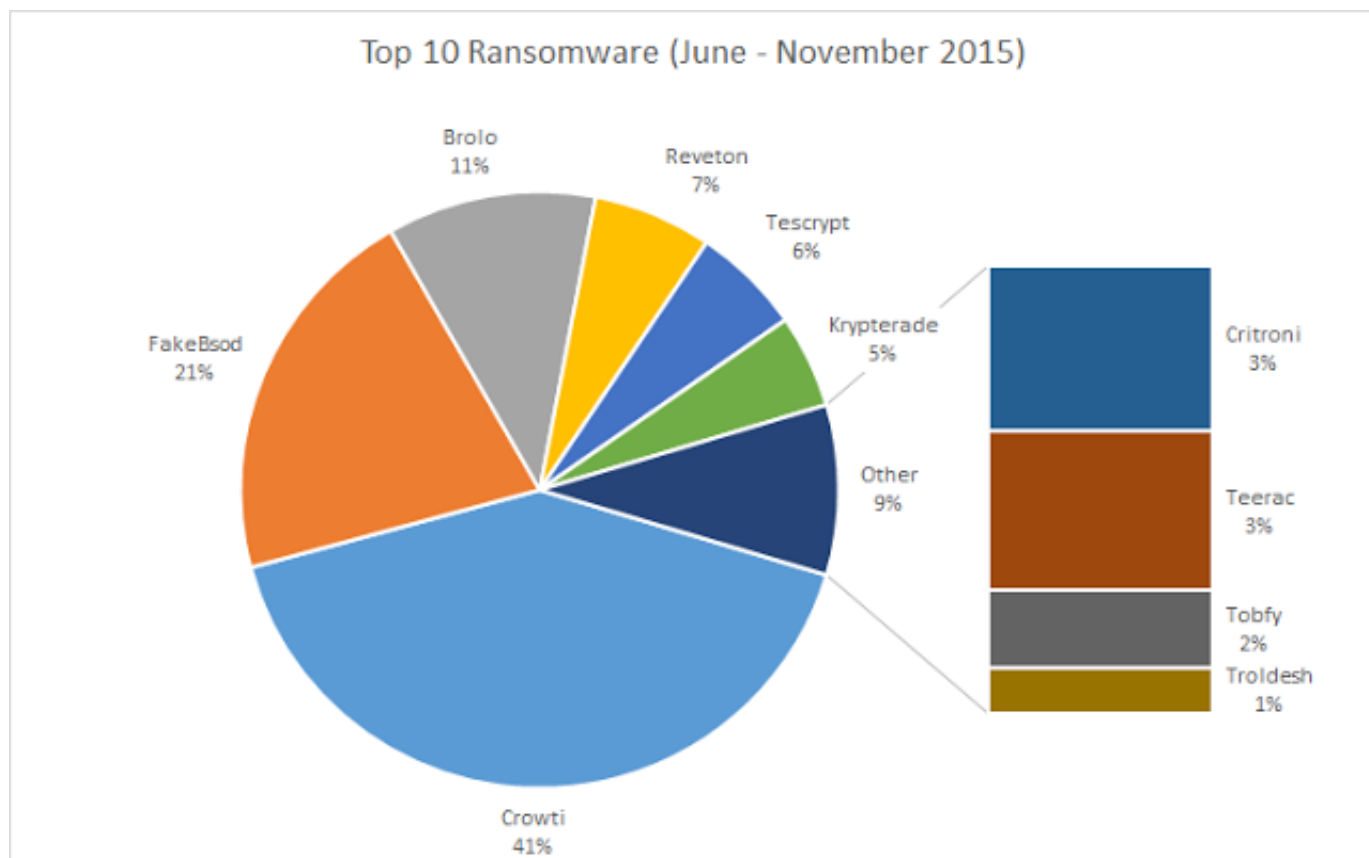
Аналогичную функциональность предлагает также [Bitdefender Anti-Ransomware](#).

## Обновляйте ПО

«Криптолокеры» приходят не только в письмах, но и посредством эксплойт-китов «drive by download», например, загружая вредоносный код через рекламные баннеры на Flash. Эта тенденция очень быстро набирает обороты, а значит надо устранять уязвимости с помощью

обновлений.

Посмотрим на статистику Microsoft.



Почти половина шифровальщиков относятся к семейству Crowti, так в Microsoft называют Cryptowall. Это наиболее рентабельный локер: согласно отчету отраслевого союза Cyber Threat Alliance (СТА), одна только версия Cryptowall 3.0 уже обошлось жертвам заражения в 325 млн. долл.

Шифровальщик Cryptowall (aka Crowti) для своей загрузки арендует эксплойт-киты Angler, Neutrino и Nuclear. Наборы эксплойтов нацелены на уязвимости в браузерах, Java, PDF, но самые распространённые уязвимости, применяемые в «китах», находятся во Flash.

Две единственные не-Flash уязвимости, которые используются в наборе Angler, это «дырки» в Microsoft Silverlight flaw (CVE-2015-1671) и в Microsoft Internet Explorer (CVE-2015-2419).

*Уязвимости Angler:*

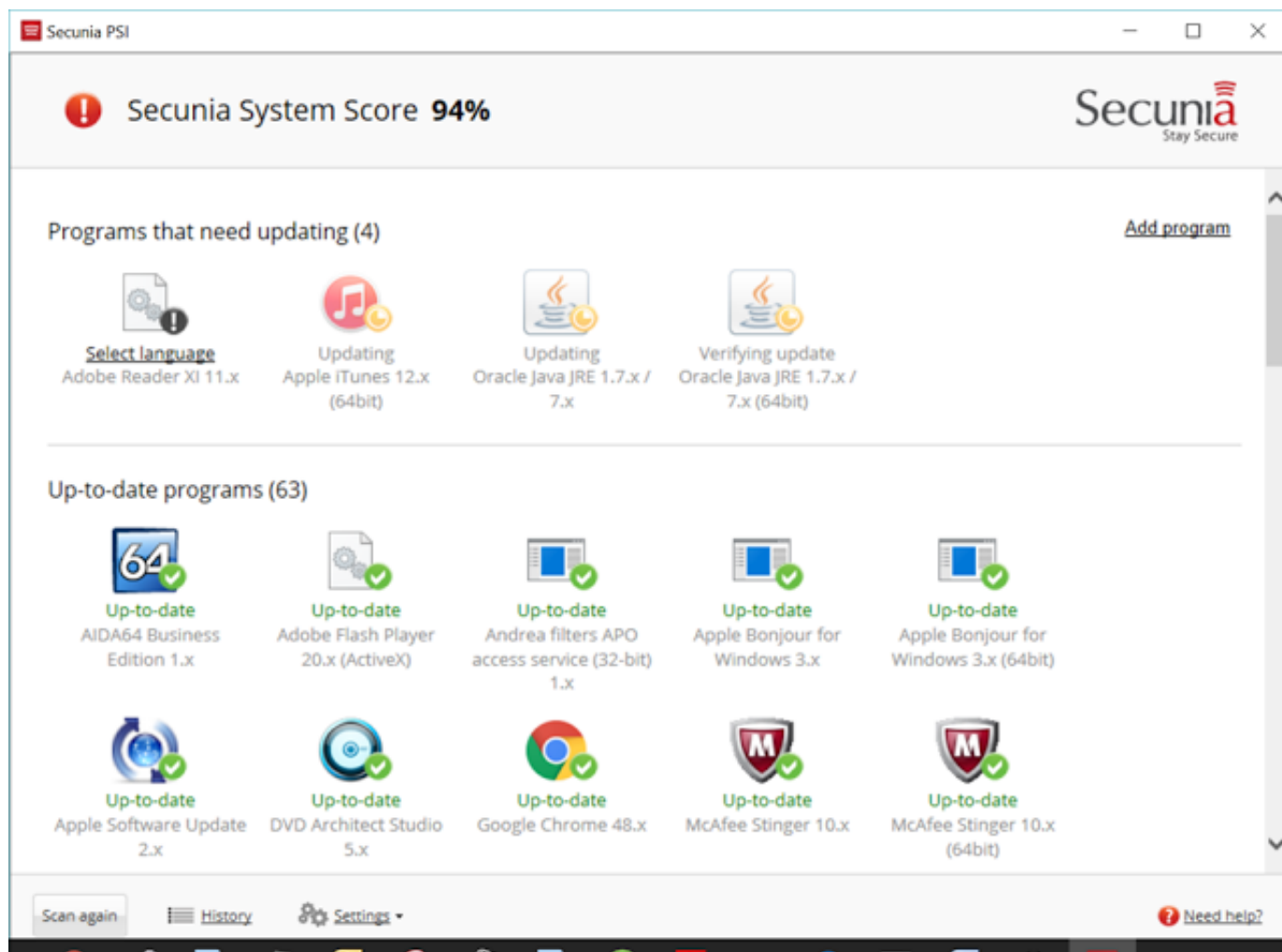
- CVE-2015-0310 (уязвимость Flash)
- CVE-2015-0311 (уязвимость Flash)
- CVE-2015-0313 (уязвимость Flash)
- CVE-2015-0336 (уязвимость Flash)
- CVE-2015-0359 (уязвимость Flash)
- CVE-2015-1671 (уязвимость в Microsoft Silverlight flaw)
- CVE-2015-2419 (уязвимость в Microsoft Internet Explorer)
- CVE-2015-3090 (уязвимость Flash)
- CVE-2015-3104 (уязвимость Flash)
- CVE-2015-3105 (уязвимость Flash)



CVE-2015-3113 (уязвимость Flash)  
CVE-2015-5119 (уязвимость Flash)  
CVE-2015-5122 (уязвимость Flash)  
CVE-2015-5560 (уязвимость Flash)  
CVE-2015-7645 (уязвимость Flash)  
CVE-2015-8651 (уязвимость Flash)

Некоторые популярные наборы эксплойтов, такие как Nuclear, Teslacrypt и Sweet Orange, [содержат](#) достаточно древние уязвимости Java, Silverlight, Windows и Adobe PDF, поэтому проверять актуальность версий следует не только в случае Flash.

Как определить, что пора обновляться? Для контроля браузерных и системных обновлений хорошо подходят сканеры [Qualys BrowserCheck](#) (в виде плагина) и [Flexera Software Personal Software](#) (экс Secunia).



## Можно ли расшифровать

При отсутствии каких-либо резервных (или теневых) копий, вероятность восстановить файлы, зашифрованные современной программой-вымогателем, стремится к нулю. Тем не менее, специалисты крупных антивирусных компаний по мере возможности помогают в расшифровке файлов. В частности, осенью 2015 года «Лаборатория Касперского» и голландской полиции удалось извлечь все ключи дешифровки для файлов, пораженных вымогателем CoinVault, а полиция арестовала подозреваемых. На странице [www.noransom.kaspersky.com](http://www.noransom.kaspersky.com) выложены 14

031 ключ для программ CoinVault и Bitcryptor.

Полезные ссылки:

<http://forum.drweb.com/index.php?showtopic=320701>

[http://forum.esetnod32.ru/forum35/topic11845/?PAGEN\\_1=10](http://forum.esetnod32.ru/forum35/topic11845/?PAGEN_1=10)

<http://www.trendmicro.com/vinfo/us/security/definition/Ransomware>

<https://www.microsoft.com/security/portal/mmpe/shared/Ransomware.aspx>



**HEADLIGHT  
SECURITY**

## Headlight Security

Блог компании HeadLight Security.

- [2016](#)
  - [Февраль\(1\)](#)
    - 31 октября, 2014  
[Готовимся к нашествию "криптолокеров"](#)
  - [Январь\(2\)](#)
    - 31 октября, 2014  
[Отчет Cisco за 2015 год: зачем ломают сайты на WordPress и какие атаки](#)



[стали использовать чаще](#)

- 31 октября, 2014

[Немного о высокоточных атаках и АРТ](#)

- [2015](#)

^ Наверх