Учимся бороться с шифровальщиками

Владимир Безмалый

В последнее время произошел резкий рост количества атак вредоносов-шифровальщиков. Причем надо отметить, что этот рост наблюдается практически для всех операционных систем. В силу массовости устройств на базе операционных систем Windows и Android мы будем говорить исключительно о них. Для начала немного статистики (см. рисунок).

В 2016 году шифровальщиками было атаковано 1 445 434 пользователей. Каждые 100 дней программы-вымогатели делают своих создателей богаче на 30 млн долл. (согласно отчету Dell SecureWorks). Количество новых модификаций таких программ выросло в 11 раз. Число атак на компании увеличилось в три раза: если раньше атаки проводились в среднем каждые две минуты, то теперь уже каждые 40 секунд. Интенсивность атак на индивидуальных пользователей удвоилась: атаки проводились в среднем раз в 20 секунд в начале периода и раз в 10 секунд — в конце.

Однако если раньше атакам в основном подвергались компьютеры с операционными системами Microsoft, то сегодня ситуация изменилась. В сети опубликован исходный код одного из самых популярных семейств программ для вымогательства для устройств с операционной системой Android — Slocker, число новых вариантов которого за последние полгода возросло в шесть раз (код опубликован на портале GitHub). Код троянца разместил некто под псевдонимом fs0 c1 ety, призвавший пользователей ресурса внести

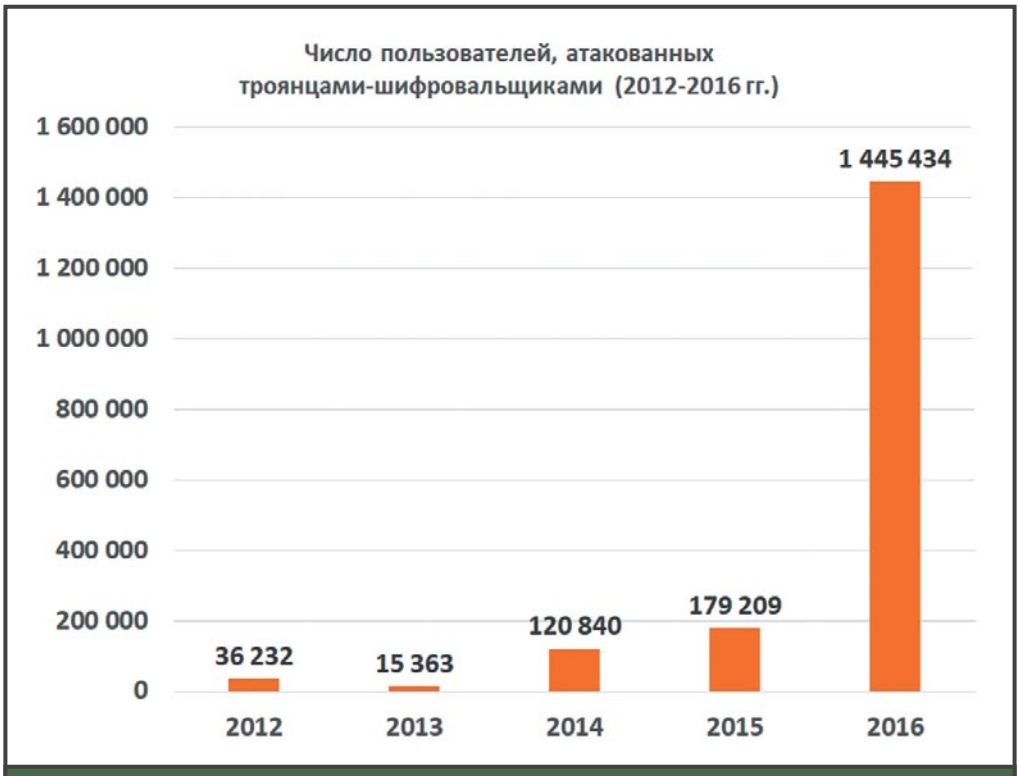
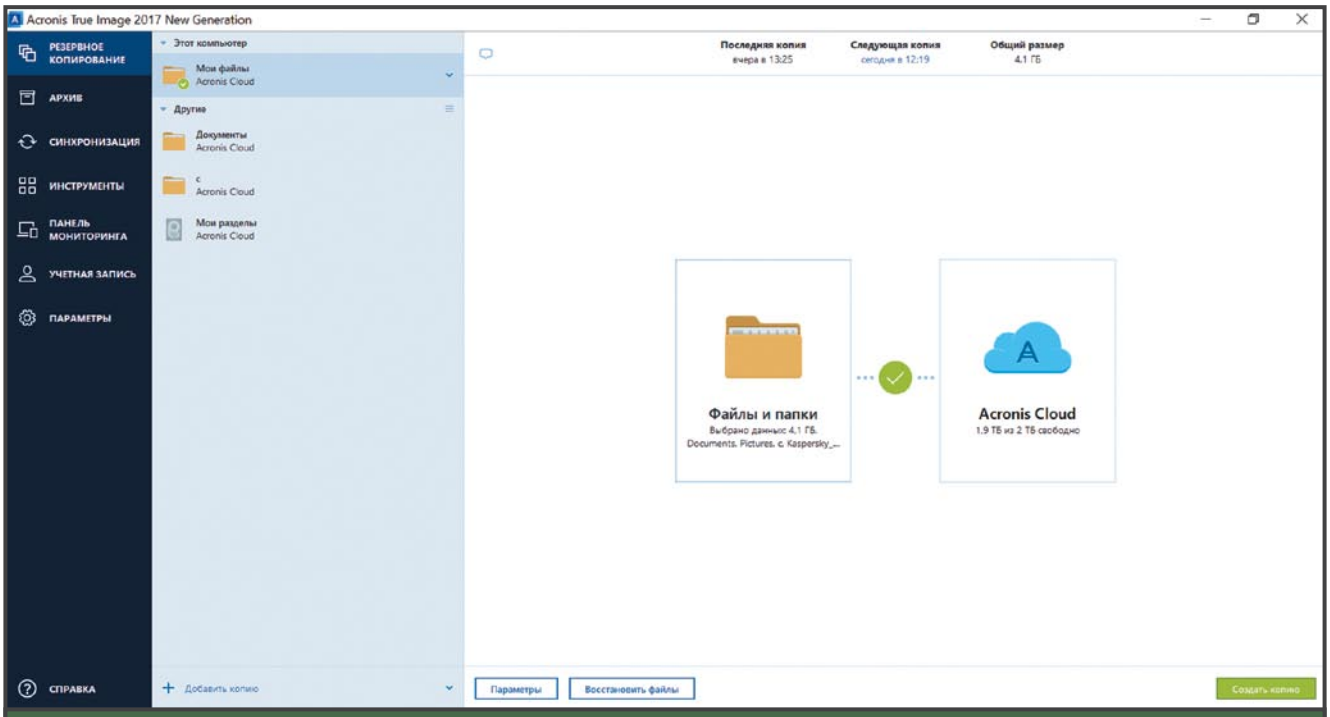


Рисунок. Количество пользователей, атакованных шифровальщиками за последние годы



Экран 1. Главное окно Acronis True Image 2017

свой вклад в его разработку и предоставить отчеты о найденных в нем уязвимых местах.

SLocker (или Simple Locker) представляет собой программу для вымогательства, шифрующую файлы на мобильном устройстве и блокирующую его экран. Для связи с C&C-сервером используется сеть Tor. Что можно предпринять для борьбы с ним и профилактики? На самом деле рекомендации будут стандартными для обеих рассматриваемых операционных систем.

1. Используйте последнюю версию операционной системы.
2. Регулярно устанавливайте обновления.
3. Используйте и регулярно обновляйте антивирусное программное обеспечение, причем обращайте внимание на то, какие именно программы вы используете. На мой взгляд, они должны лидировать в независимых тестах и показывать хорошие результаты при обнаружении вирусов.
4. Не работайте с правами учетной записи локального администратора.
5. Не работайте на устройстве с измененной прошивкой, то есть рутованном.
6. И последняя, самая главная рекомендация: ДЕЛАЙТЕ РЕЗЕРВНЫЕ КОПИИ!

Советы для Windows

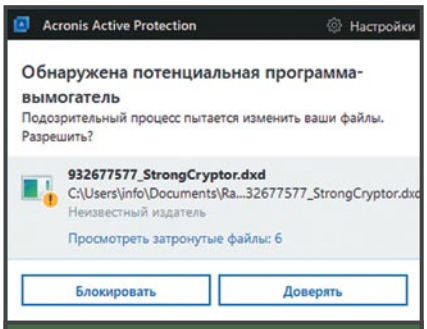
Многообразие операционных систем Windows, представленных сегодня на рынке, включает версии XP, 7, 8.1 и 10. Тем не менее количество домашних компьютеров под управлением Windows XP остается достаточно высоким. Что можно посоветовать пользователям этой операционной системы? Только посочувствовать. Им просто следует понять, что пора двигаться вперед. Нельзя требовать безопасности от операционной системы, не сопровождаемой производителем. Их безопасность — это только их проблема.

Что же касается версий 7, 8.1 и 10, то здесь необходимо вспомнить, что в данных операционных системах вы сможете задействовать как встроенные средства резервного копирования, так и программы резервного копирования от независимых производителей. Единственное, о чем необходимо помнить, — внешний носитель для резервного копирования должен подключаться только на время создания резервной копии. Это позволит вам избежать ситуации, когда одновременно будет зашифрован как основной, так и резервный носитель.

Если же вы захотите использовать в качестве носителя для резервной копии «облачное» хранилище, то можете выбрать как хранилище от Microsoft, так и хранилище от Google или воспользоваться программным обеспечением компании Acronis. Именно на нем я и остановлюсь, потому что сам использую продукт Acronis True Image 2017 (экран 1). Согласитесь, очень удобно, когда проактивный, активный и реактивный виды защиты сосредоточены в одном продукте. Таким образом, данное решение не только позволит вам создать резервные копии устройств в «облаке», но и предоставит уникальные технологии безопасности, включая активную защиту от шифровальщиков.

Acronis Active Protection

До появления вирусов-шифровальщиков, будем откровенны, не многие пользователи задумывались о резервном копировании. Технология Acronis Active Protection использует эвристические методы обнаружения



Экран 2. Зафиксирована активность сторонней программы

для мониторинга подозрительной активности с файловой системой в целом, а не только с файлами, для которых настроены задания резервного копирования. Защита работает постоянно, о чем свидетельствует значок в системном лотке на экране, который предоставляет доступ к настройкам.

Таким образом, резидентная утилита постоянно отслеживает сторонние приложения, которые пытаются зашифровать данные. Пользователь может сам как разрешить активность отдельных программ, так и отключить защиту определенных папок и файлов (экран 2). Более того, вы можете настроить автоматическое восстановление файлов, которые могли быть затронуты заблокированной операцией шифрования.

Функция Notary

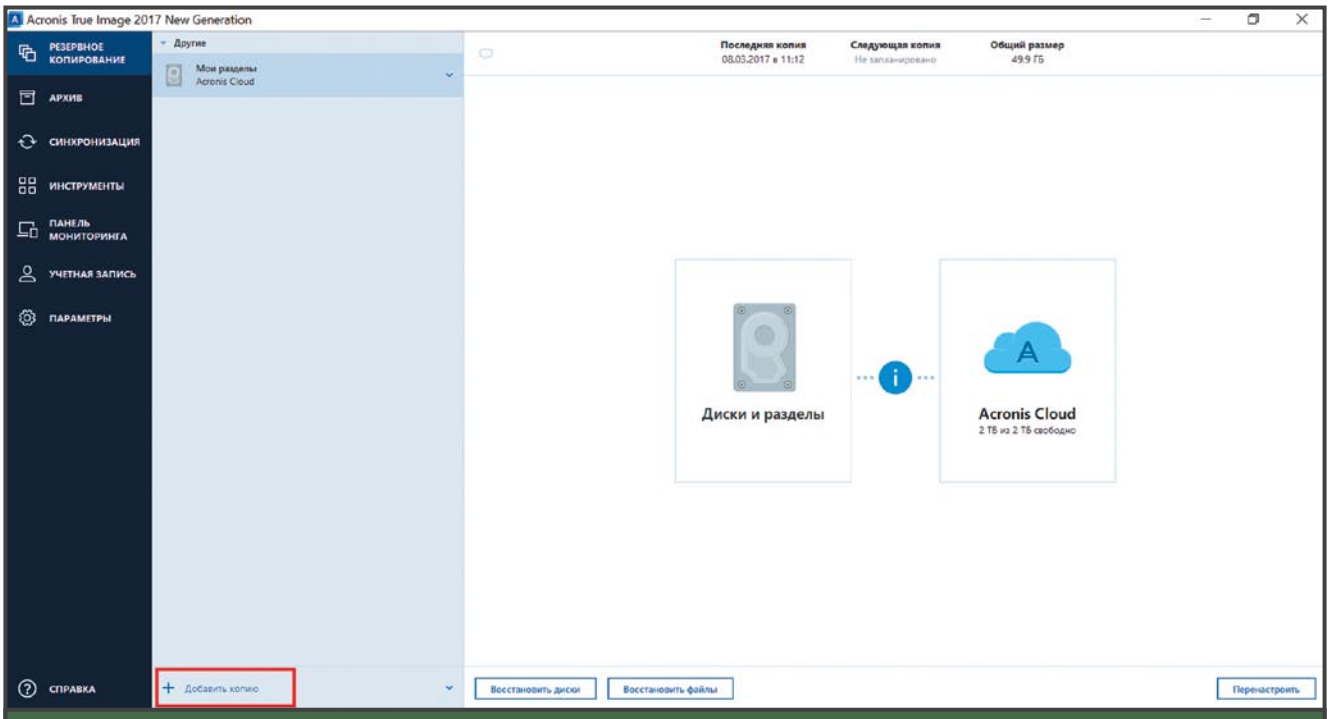
В качестве дополнительного подтверждения того, что файлы остались в таком же состоянии, как и при резервном копировании, Acronis предоставляет функцию Notary. Данная функция использует известную технологию цепочки блоков под названием «блокчейн», которая применяется в криптовалютах для обеспечения гарантии. Чтобы создать «заверенную» копию, нужно подготовить новое задание на резервное копирование и при выборе источника резервного копирования выбрать вариант «Файлы для заверения». Затем следует выбрать файлы и папки для обработки и в качестве места назначения указать локальное место или Acronis Cloud. Затем появится анимированное уведомление «Заверение».

После завершения процедуры создания резервной копии вы можете проверить файл и даже посмотреть его официальный сертификат, в котором в качестве правообладателя указан Acronis Notary. По утверждению специалистов Acronis, это неопровержимое доказательство, что файл не был изменен.

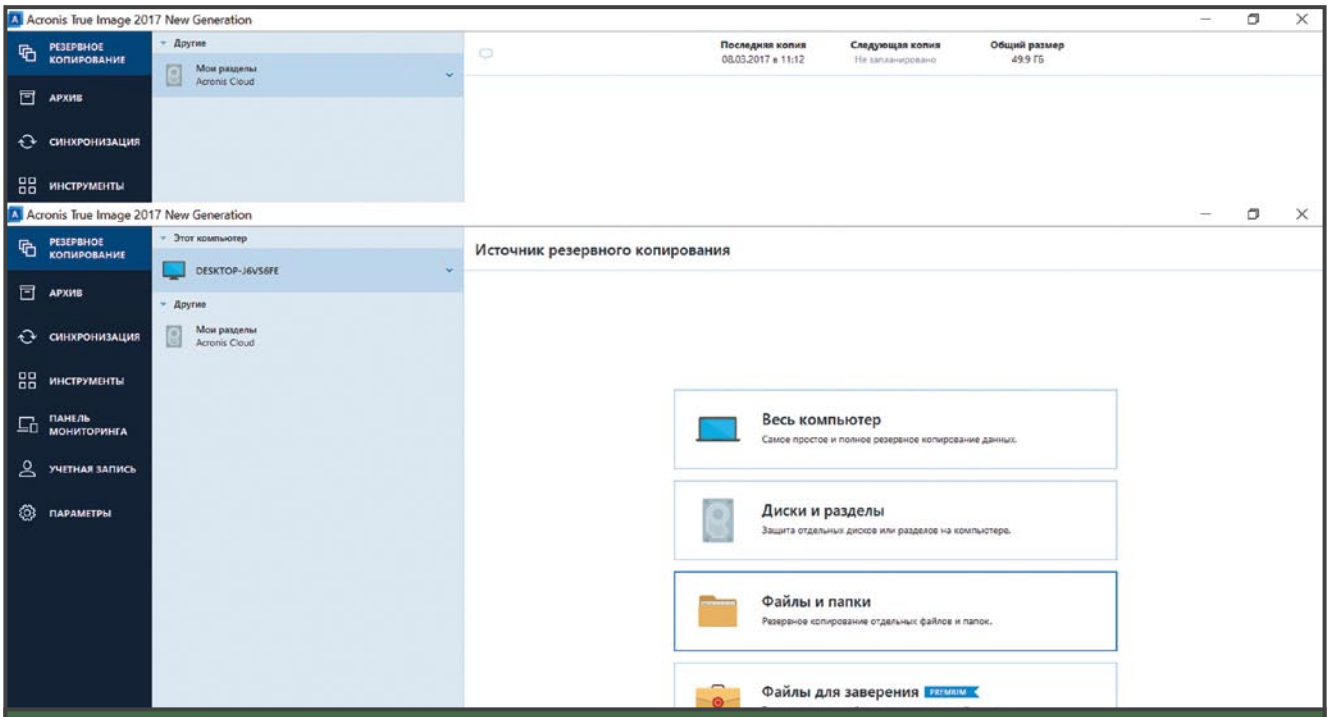
Итак, для создания резервной копии данных на компьютере вам необходимо установить и запустить программное обеспечение. В дальнейшем — определить, что именно вы хотите копировать. Я рекомендую делать на всякий случай три копии ваших наиболее важных файлов и компьютера в целом. Три копии на двух разных носителях, причем одна копия должна храниться вне вашего дома или офиса.

При использовании первой копии в случае неприятностей вам нужно будет заново установить все необходимое программное обеспечение, включая операционную систему, а затем восстановить свои данные. Очевидно, что в этом случае время создания резервной копии, как и время восстановления данных из нее, будет минимальным. Для такой копии я бы предложил «облачное» хранилище. Ведь неизвестно, насколько надежно ваше соединение с Интернетом. Выбираем в окне программы вариант «Добавить копию», как показано на экране 3.

Выбираем нужные файлы и папки (экран 4) и запускаем процесс



Экран 3. Создание копии



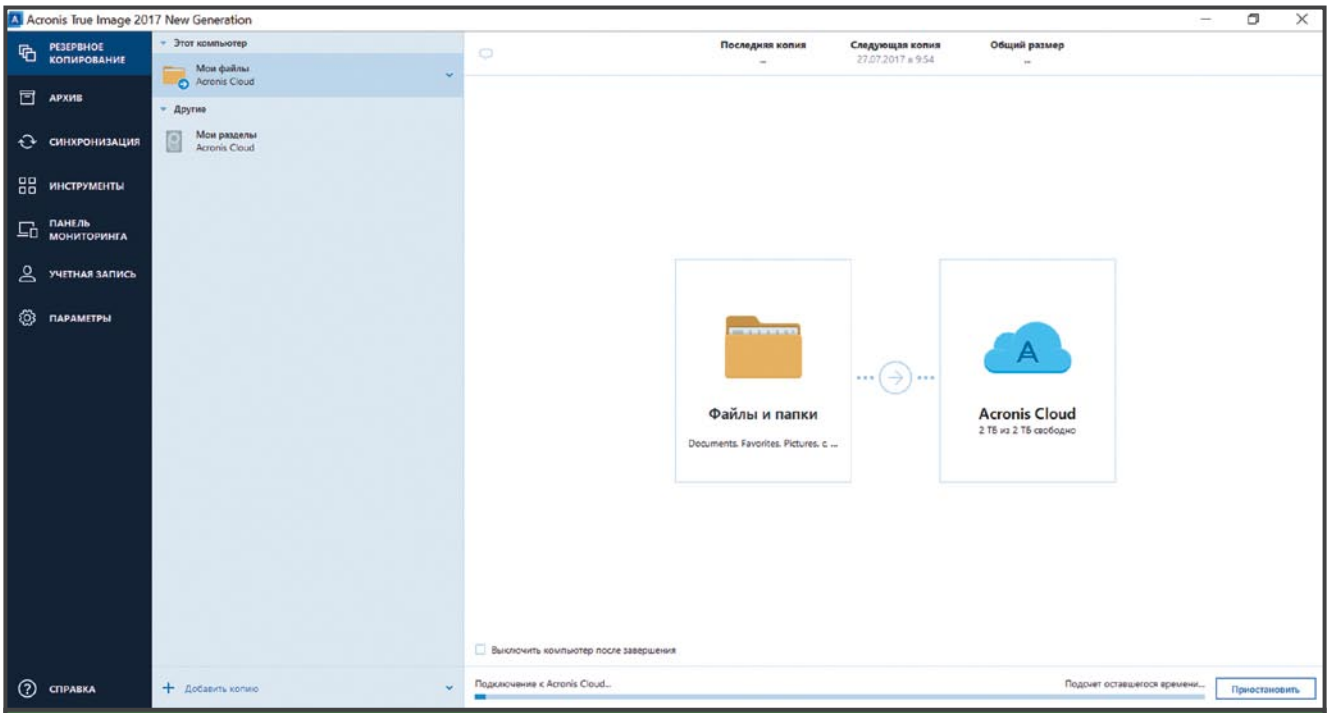
Экран 4. Выбор необходимых файлов и папок

копирования в «облачное» хранилище (экран 5).

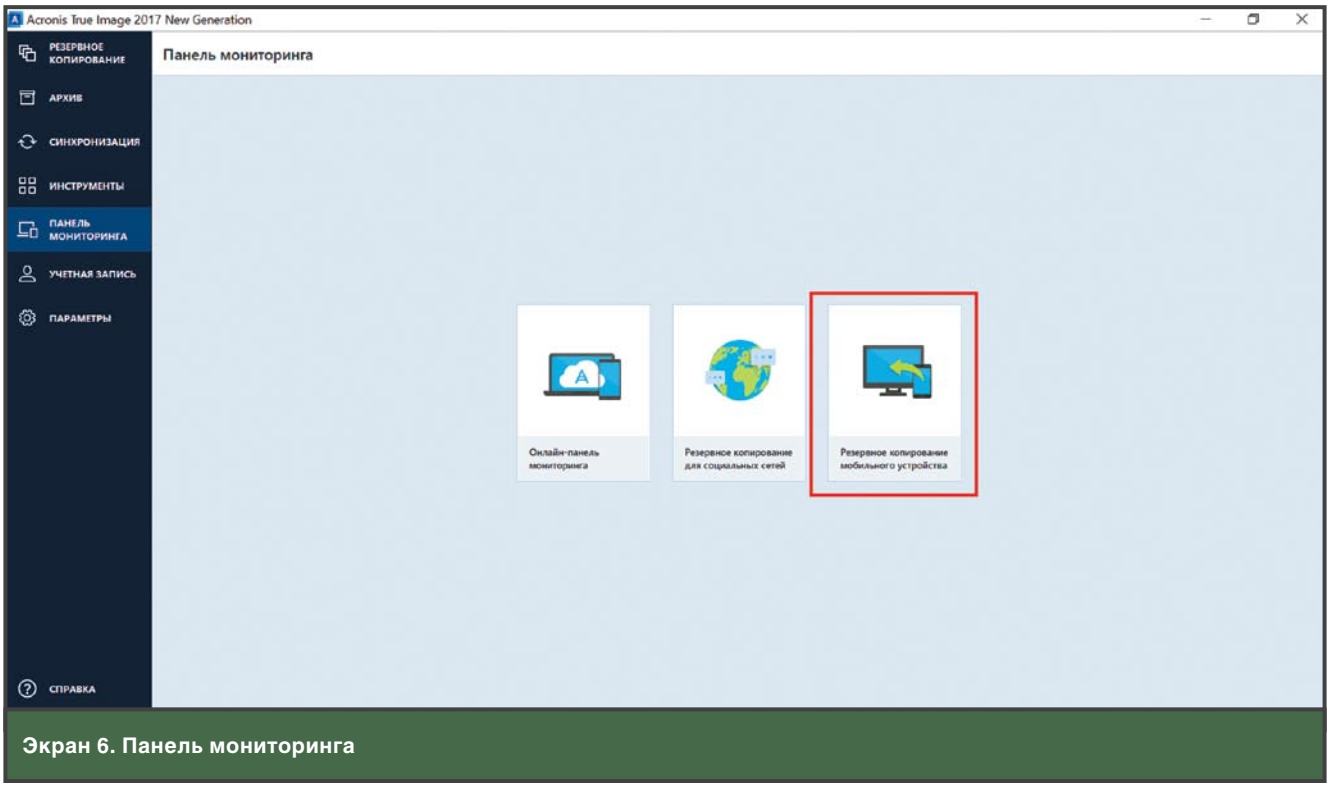
Создание резервной копии всего компьютера тоже процесс несложный. Для этого вам нужно также выбрать вариант «Добавить копию», но затем указать «Изменить место хранения» и выбрать ваше подключенное внешнее хранилище. Почему я не рекомендую выбирать «облачное» хранилище? Все просто. Дело в объеме информации, которую требуется перенести в это «облачное» хранилище. Безусловно, если у вас высокоскоростной Интернет, то можно воспользоваться и «облаком».

Создание резервной копии для устройств Android

Однако гораздо чаще сегодня встречается ситуация, когда пользователю нужно создать резервную копию своего смартфона (планшета). Особенно на базе операционной системы Android. Увы, несмотря на то что на данном рынке средства



Экран 5. Создание «облачной» резервной копии



Экран 6. Панель мониторинга

резервного копирования довольно многочисленны, чаще всего это либо специализированные решения от конкретного производителя, либо программы, требующие прав администратора устройства, что само по себе уже снижает безопасность вашего смартфона или планшета. Что можно предложить в таких условиях? Тот же продукт Acronis.

Наверное, многие из вас сталкивались с тем, что по какой-то причине смартфон выходил из строя. Рано или поздно это случается. Вы шли в сервисный центр и слышали там сакраментальную фразу: «Резервная копия есть? Мы не гарантируем сохранность данных!». Поэтому еще раз повторю: резервные копии жизненно необходимы, нравится нам это или нет. Для создания резервной копии устройства под управлением Android необходимо:

1. Выбрать раздел «Панель мониторинга».
2. Выбрать вариант «Резервное копирование мобильного устройства» (экран 6).
3. Загрузить приложение Acronis Mobile и следовать полученным инструкциям.

В случае заражения вашего смартфона необходимо сбросить его в заводские настройки (этому посвящено достаточно много статей в Интернете). Учтите, что вам потребуется способ сброса при помощи кнопок. У каждой модели устройства есть стандартное сочетание кнопок, которое переключает его на меню Recovery. Для этого выключите свой телефон (планшет). Дождитесь полного отключения. Учтите, что комбинация для вашей модели может отличаться от общепринятых. Уточните на сайте производителя.

Как правило, это:

- кнопка «уменьшить громкость» + «включение» (она же Power) — самая распространенная комбинация;
- на некоторых телефонах компании LG нужно нажать названные выше клавиши, дождаться появления на экране логотипа, отпустить кнопку включения и затем снова ее нажать;
- комбинация кнопок «громкость вверх» + «громкость вниз» + «включение»;
- комбинация кнопок Power + Home.

Используйте одну из комбинаций, пока не войдете в режим Recovery, чтобы затем сбросить устройство в заводские настройки. Перемещение по пунктам меню происходит кнопками увеличения и уменьшения громкости. Если версия Recovery сенсорная, то можно выполнить перезагрузку и стандартным образом (прикосновениями к экрану). Для подтверждения выбора нужно нажимать кнопку Power или «Контекстное меню».

Далее:

1. Выберите пункт Clear eMMC или wipe data/factory reset, иногда он еще называется Clear Flash.
2. Подтвердите действие yes — delete all user data, чтобы сбросить данные.
3. После завершения процесса выберите Reboot System.

Затем вы можете восстановить свои данные и установить те приложения, которые были у вас до сброса. Как видите, все достаточно просто. Таким совсем не сложным образом вы сможете спасти свои данные в случае непредвиденной аварии (совсем не обязательно это будет атака вредоноса-шифровальщика). Надеюсь, рекомендации, приведенные в этой статье, помогут вам.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, Kaspersky Lab Certified Consultant, Kaspersky Lab Certified Trainer, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor