Часть 2

Противодействие вирусам-шифровальщикам

Владимир Безмалый

Напомню читателям, что в данной статье мы рассматриваем тему вымогательства с применением специальных вирусов, которые часто обозначают термином ransomware. Как было показано в первой части статьи, современные темпы развития вирусов-шифровальщиков представляют серьезную проблему, на которую нельзя не обращать внимания. Столкнувшись с шантажом, жертва оказывается перед выбором — платить либо потерять информацию. Поэтому лучше предупредить угрозу, нежели заниматься устранением последствий. Сегодня мы обсудим, как это сделать, а также рассмотрим способы борьбы с шифровальщиками.

Что делать?

На самом деле это основной вопрос. Например, в своем выступлении начальник ФБР порекомендовал платить (http://uk.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10). Поможет ли это? Думаю, нет. Потому что никто не даст вам гарантий, что даже после этого вы сможете получить свои данные в целости и сохранности. Кроме того, ущерб не ограничивается одной только суммой выкупа: пока вы разбираетесь со злоумышленником, ключевые процессы бизнеса простаивают, и вы теряете средства и клиентов. Общие рекомендации будут выглядеть стандартно:

1. Регулярно обновлять операционную систему и приложения.
2. Установить и регулярно обновлять надежное антивирусное программное обеспечение.
3. Не использовать программы из сомнительных источников, а лучше иметь в организации список приложений, которые будут регулярно обновляться, то есть везде, где это возможно, работать по принципу белого списка.
4. Не открывать письма и уж тем более вложения, если вы не знаете отправителя.
5. Регулярно обновлять резервные копии. Успешное восстановление данных после атаки вируса-вымогателя возможно только путем восстановления данных. При этом для компании важно оценить затраты, связанные с восстановлением данных при возможной атаке вируса-вымогателя. Соблюдать правило «3-2-1»: должно быть минимум три копии данных на двух различных носителях, причем одна из них должна находиться вне основного места расположения данных.

По мере развития методов вымогательства совершенствуются и технологии противодействия им. На сегодня фактически это многоступенчатая защита, причем антивирусные продукты — всего лишь одна, хоть и огромная ее часть.

Обновления решают все

Как ни странно, несмотря на то что о своевременном обновлении операционных систем и прикладных продуктов говорят много, делается в этом отношении очень мало. И если на серверах операционные системы еще как-то обновляются, то на персональных компьютерах практически нет. А ведь, по данным Microsoft в период от 8 до 24 часов после выпуска обновления появляются вредоносные программы, которые используют закрываемую уязвимость! Обратимся к цифрам: 77% российских пользователей работают с устаревшим программным обеспечением, а в среднем на одном компьютере в нашей стране сегодня содержится

семь приложений, которые требуют обновления. Такие данные получила «Лаборатория Касперского» с помощью «облачной» инфраструктуры Kaspersky Security Network (KSN), http://www.kaspersky.ru/about/news/virus/2016/KSN-multi-device-security. Необновленные приложения довольно часто имеют уязвимые места, через которые на устройство могут проникнуть вредоносные программы. Львиную долю подобных уязвимых приложений составляют широко распространенные программы — веб-браузеры и пакеты офисных программ. Так, в первом полугодии 2016 года на эти приложения в совокупности приходилось более 80% уязвимостей.

Однако, помимо этого, на компьютерах пользователей имеются программы, о существовании которых они могут даже и не знать. Зачастую ими оказываются различные модули и приложения, которые устанавливаются автоматически при загрузке какого-либо бесплатного программного обеспечения. Как свидетельствуют данные из KSN, подобные «дополнения» есть у каждого четвертого пользователя в России. В среднем на одном компьютере содержатся две такие программы, и если пользователь их не обнаружит, то они «проживут» на устройстве приблизительно год.

Риск, исходящий от программ, устанавливаемых без ведома пользователя, крайне высок. Во-первых, они пополняют число неиспользуемых и необновляемых приложений и таким образом способствуют увеличению числа уязвимостей на устройстве. А во-вторых, никто не может гарантировать, что эти программы не являются вредоносными.

Как обновлять? В данном случае имеет смысл не только воспользоваться встроенными в программное обеспечение системами оповещения об обновлениях, но и подумать о внедрении специализированного решения. Если вы, например, корпоративный пользователь, то вам управлять уязвимостями и обновлениями поможет Kaspersky Endpoint Security для бизнеса. Если же вы персональный пользователь, то существует решение Kaspersky Internet Security для всех устройств. Функция «Обновление программ» в его составе проверяет все имеющееся на компьютере программное обеспечение и определяет, какие обновления необходимо установить. При наличии соответствующих обновлений от разработчиков защитное решение автоматически установит их, причем сделает это в фоновом режиме, оказывая минимальное воздействие на работу устройства.

Если же вы решитесь обновлять программное обеспечение с помощью сторонних средств, обратите внимание на Personal Software Inspector от компании Secunia. Это бесплатное программное обеспечение, с помощью которого вы сможете обновлять сторонние приложения.

Другая проблема — удаление неиспользуемого программного обеспечения. Надеюсь, в вашей организации существует утвержденный список применяемых программ? Если нет, то давно пора бы его составить. Однако следует понимать, что создавать такой список вручную долго, дорого и никому не нужно. Как быть? Стоит воспользоваться функцией аудита программного обеспечения, также реализованной в корпоративных версиях некоторых продуктов.

Если же вы персональный пользователь, то в том же Kaspersky Internet Security для всех устройств реализована функция «Удаление программ», она занимается поиском подозрительных и редко используемых приложений. В ходе проверки выявляются программы, установленные без согласия пользователя, замедляющие запуск операционной системы, запускающиеся самопроизвольно и неотключаемые, а также давно забытые и не использовавшиеся на протяжении долгого времени. В итоге пользователь получает список всех программ, о существовании которых он мог не знать или забыть, и на основании этой информации он может принять решение, что удалить, а что оставить. Если же говорить именно об антивирусных технологиях, то здесь стоит в первую очередь рассмотреть уровни анализа информации.

Анализ всего и вся

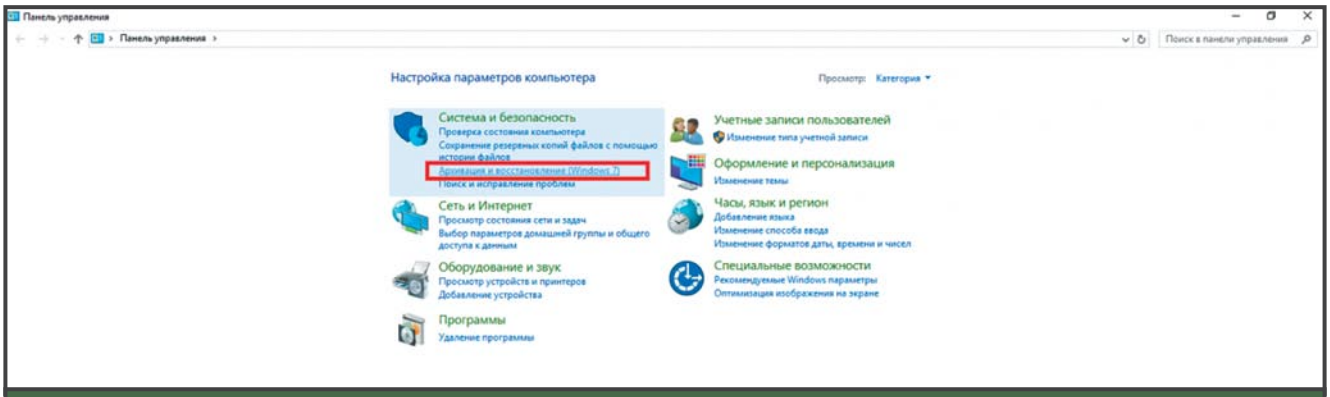
Анализ репутации файлов и веб-страниц с помощью «облачных» технологий, web monitoring and url filtering (WMUF), существует уже давно, но тем не менее это один из самых, на мой взгляд, эффективных способов предотвращения заражения. Кроме того, стоит вспомнить о фильтровании веб-трафика и блокировании зараженных объектов электронной почты. Также напомню, что сегодня любой антивирус обладает эвристическим и сигнатурным анализом объекта. Другое дело, что качество этого анализа у всех разное, но ведь это уже второй вопрос, не так ли? Например, для возможного предотвращения заражения в решении Kaspersky Endpoint Security для бизнеса применяются перечисленные ниже технологии.

- Квалификация уязвимостей (Patch management).
- Противодействие заражению:
  - репутационная фильтрация с использованием «облачных» технологий;
  - контроль запуска приложений;
  - запуск приложений в безопасной среде;
  - автоматическая защита от эксплойтов (AEP).
- Анализ функционирования приложений:
  - контроль активности программ;
  - поведенческий анализ;
  - откат вредоносных действий.

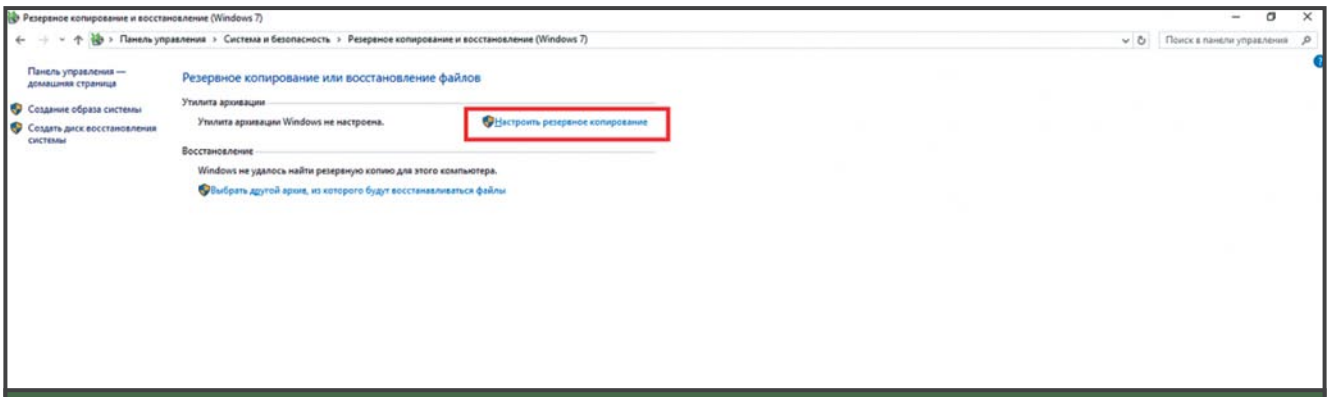
Но все же наилучшим способом защиты, а главное, беспроигрышным, является проведение регулярного резервного копирования, причем здесь важно не забывать и о мобильных устройствах, в особенности о смартфонах под управлением Android.

Резервное копирование как якорь

О пользе резервного копирования написано уже столько статей, что в них можно утонуть. И тем не менее, если уж не удалось пре-



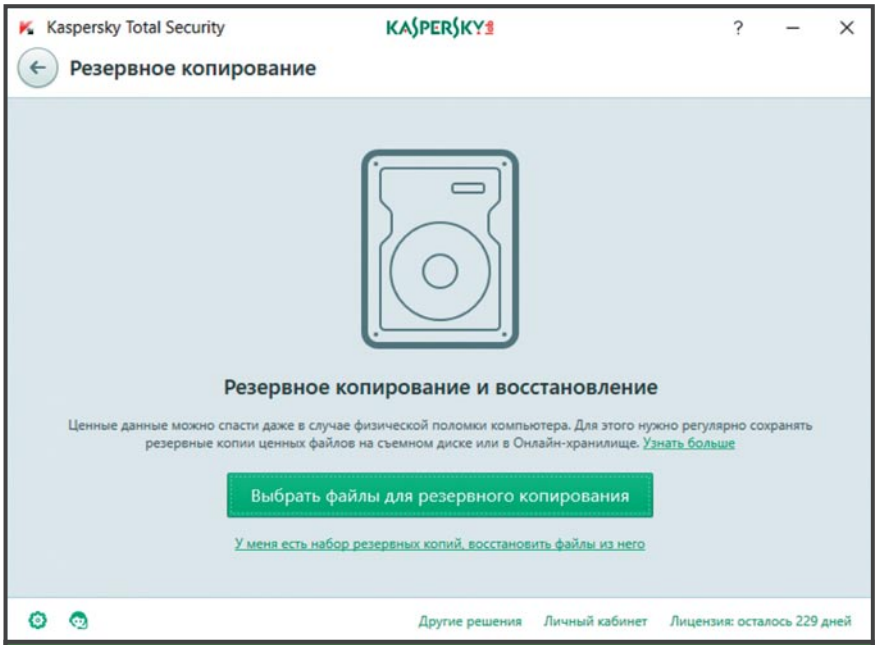
Экран 1. Создание резервной копии в Windows 10



Экран 2. Настройка резервного копирования

дотвратить заражение, спасти ваши данные, а вместе с ними и бизнес, поможет именно восстановление из резервной копии. Настоятельно рекомендую вам регулярно выполнять резервное копирование своих систем и данных. Какое решение выберете вы, я не знаю. Но оно должно позволить вашей компании:

- выполнять резервное копирование регулярно и по расписанию;
- сохранять резервные копии за несколько периодов в различных местах, в том числе в недоступной для программ-вымогателей среде — защищенном «облаке»;
- составить план восстановления, чтобы точно знать, как будет проходить восстановление и сколько времени оно займет;
- проводить регулярное тестирование — только в этом случае резервное копирование и восстановление окажутся эффективными;
- установить решение автоматизированного аварийного восстановления для повышения уровня защиты.



Экран 3. Резервное копирование и восстановление в Kaspersky Total Security

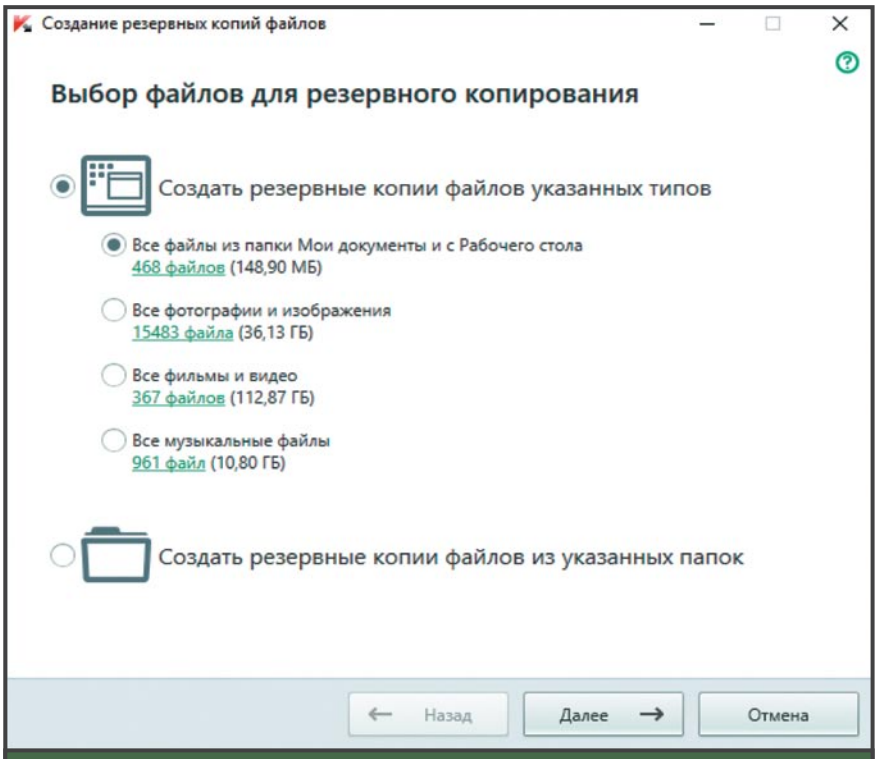
О резервном копировании для персональных пользователей также написано огромное количество статей. Что можно предложить? Для пользователей Windows проще всего задействовать встроенное решение от Microsoft, тем более что резервная копия настраивается буквально парой щелчков мыши (см. экраны 1 и 2).

В случае использования резервного копирования от Microsoft вам будет предложено создать образ системного диска и настроить резервное копирование данных по вашему выбору или применить стандартные параметры. Но недостаток такого решения в том, что настраивать придется несколько решений: одно для компьютера, второе для смартфона, третье для планшета... Увы, потребуется масса времени.

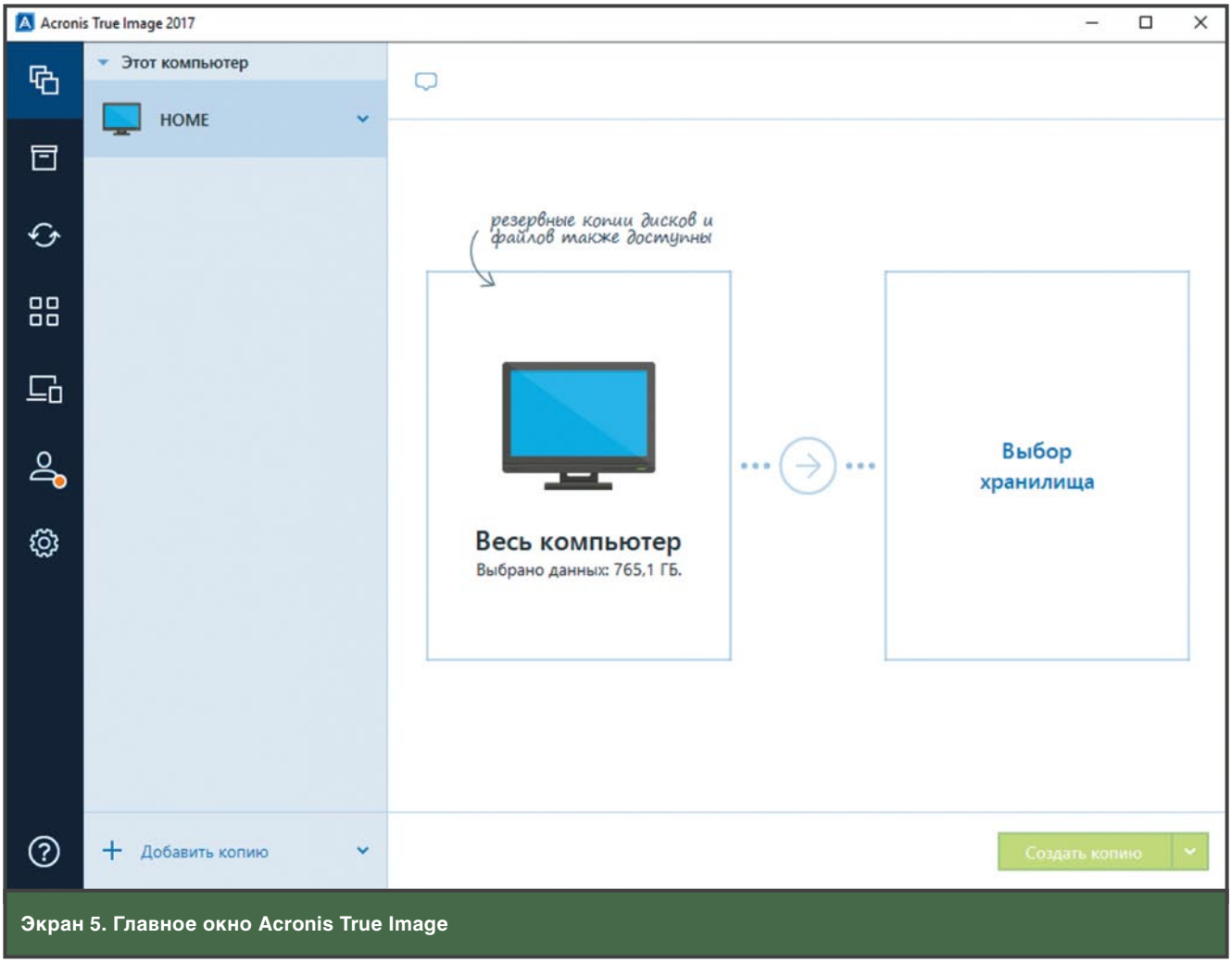
Другой вариант настройки резервной копии используется в продуктах сторонних разработчиков, в качестве примера расскажу, как это делается в Kaspersky Total Security (см. экран 3).

В ходе создания резервной копии вам будет предложено либо самому выбрать, что именно вы хотите сохранить, либо использовать стандартные решения (см. экран 4).

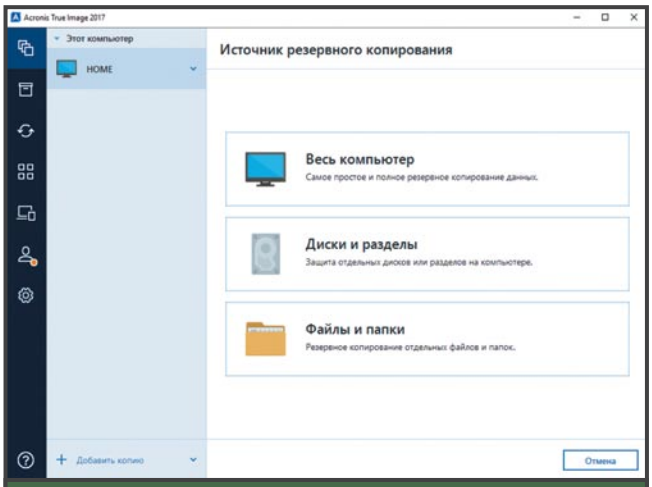
На следующем этапе вы сможете выбрать сетевое, «облачное» хранилище или хранилище на подклю-



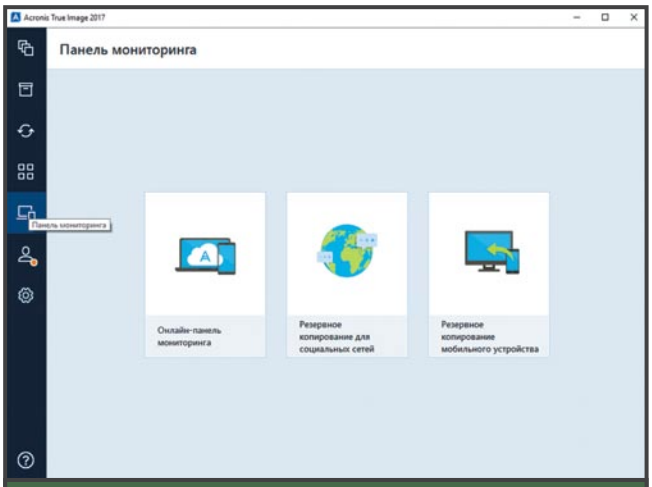
Экран 4. Выбор файлов для резервного копирования



Экран 5. Главное окно Acronis True Image



Экран 6. Выбрать источник резервного копирования



Экран 7. Панель мониторинга

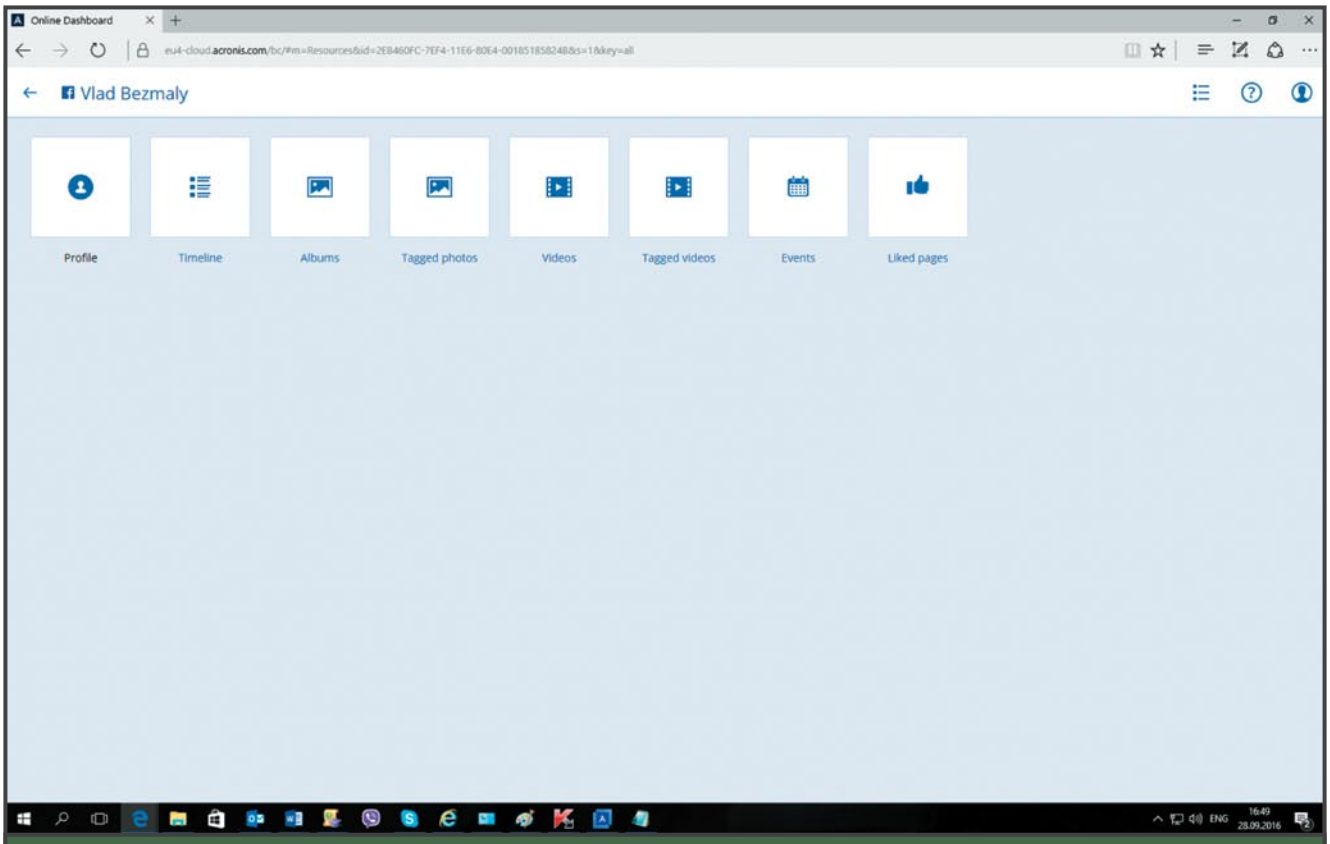
ченном внешнем диске и начать собственно копирование.

Еще можно воспользоваться специализированным платным решением. Хорошим примером такого решения может служить Acronis True Image (см. экран 5), основным преимуществом которого является использование единой консоли для копирования информации как с компьютера, так и с мобильных устройств с операционными системами Android и iOS. Причем вы сами можете выбрать, хотите ли вы сохранить резервную копию мобильного устройства в «облаке» или на локальном жестком диске своего компьютера.

В этом окне вы сможете выбрать данные, которые хотели бы копировать, или создать полную копию компьютера (см. экран 6).

Возможно, вы захотите иметь резервную копию своих данных из социальной сети или копию мобильного устройства (под управлением Android или iOS, значения не имеет; см. экран 7). Если вы захотите выбрать «Резервное копирование для социальных сетей», сначала вам необходимо подключиться к «облачному» хранилищу Acronis и к вашей учетной записи в социальной сети, а затем указать, что именно вы хотите копировать (см. экран 8).

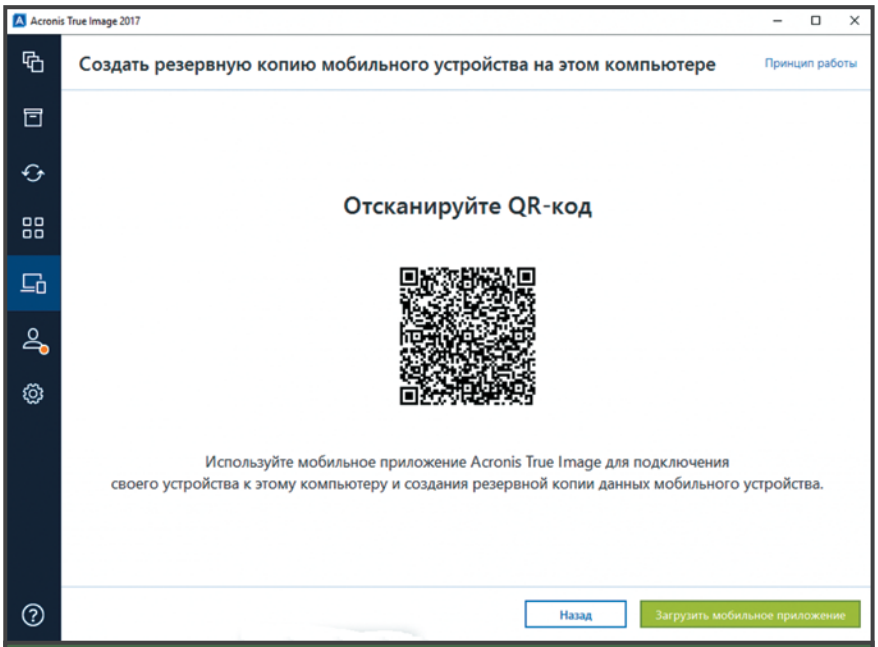
Если же вы захотите создать резервную копию своего мобиль-



Экран 8. Создание резервной копии учетной записи Facebook

ного устройства, то вам придется предварительно загрузить соответствующее мобильное приложение (см. экран 9).

Учтите, что резервную копию мобильного устройства вы сможете создать как на своем компьютере, так и в «облаке». Я не знаю, какой вариант вы выберете, но помните, что очень часто это единственное, что может вам помочь в случае заражения.



Экран 9. Резервная копия мобильного устройства

Как защититься от ransomware

Чтобы обезопасить себя от ransomware, можно сделать следующее:

1. Регулярно создавайте резервные копии всех важных файлов. Желательно, чтобы у вас было две резервных копии данных: одна в «облаке», например в Dropbox, Google Drive и других специализированных службах, а другая — на сменном носителе (съемный жесткий диск, большая флешка, запасной ноутбук). Для этого устройства установите ограниченные права доступа только на чтение и запись, без возможности удаления или перезаписи. Резервные копии пригодятся вам и в других случаях: если вы случайно удалите важный файл или при поломке основного жесткого диска. Регулярно проверяйте, в порядке ли сделанные резервные копии. Система создания резервных копий — это тоже программа, она может скопировать данные с ошибками.
2. Преступники часто создают сообщения, похожие на письма от интернет-магазинов или банков, чтобы распространять вредоносные программы — это называется «фишинг». Так что настройте в почте спам-фильтр и никогда не открывайте вложения к письмам, отправленным незнакомыми людьми. Не доверяйте никому — вредоносную программу могут прислать со взломанной учетной записи вашего друга в Skype или «Вконтакте», партнера по онлайн-играм или даже коллеги с работы.
3. Включите функцию «Показывать расширения файлов» в настройках. Так вам будет легче разобраться, какой файл является опасным. Троянцы — это программы, значит, опасаться нужно в первую очередь подозрительных файлов с расширениями exe, vbs и scr. Но расслабляться нельзя в любом случае, так как многие другие файлы тоже могут быть опасными. Мошенники часто ставят несколько расширений подряд, чтобы замаскировать вредоносную программу под видео, фото или документ, например: hot-chics.avi.exe или report.doc.scr.
4. Регулярно устанавливайте обновления для операционной системы, браузера, антивируса и другого программного обеспечения. Преступники используют бреши в программном обеспечении, чтобы заразить устройства пользователей.
5. Установите надежный антивирус, который умеет бороться с троянцами-вымогателями и в большинстве случаев просто не позволит вирусам попасть к вам в систему, а если это произойдет, защитит важные файлы с помощью специальной функции.
6. Если вам кажется, что вы обнаружили какой-то подозрительный процесс, отключите компьютер от Интернета. Если троянец-вымогатель не успеет стереть ключ шифрования на вашем компьютере, то есть шанс восстановить файлы. Правда, новейшие его версии используют заранее заданный ключ, так что с ними этот совет не сработает.
7. Если вы уже попались, то не платите выкуп, если в этом нет острой необходимости. Помните: каждый денежный перевод — это вливание в преступный бизнес, который будет развиваться и дальше, до тех пор пока поступают деньги.
8. Еще один совет для уже заразившихся: проверьте — возможно, вам повезло, и вам попался один из старых вариантов программ-шифровальщиков. Раньше вымогатели были далеко не такими продвинутыми, как сейчас, и зашифрованные ими файлы сравнительно несложно восстановить.
9. Кроме того, соответствующие службы и специалисты по кибербезопасности периодически ловят преступников и выкладывают инструменты для восстановления файлов в Интернет. Есть смысл проверить, можно ли вернуть свои файлы бесплатно. Для этого посетите, например, noransom.kaspersky.com.

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

Как создать загружаемый накопитель USB с Windows Server 2016?

Приведенные ниже инструкции помогут сделать накопитель USB загружаемым. Измените буквы диска и тех дисков, которые имеются в вашей системе. Обратите особое внимание на диск для USB, поскольку он будет очищен и все данные будут удалены! В данном случае диск F: содержит установочные файлы, принадлежащие Windows Server 2016, а диск E: является моим диском USB.

Создание загружаемого накопителя USB с Windows Server 2016:

```
C:\WINDOWS\system32>diskpart
Microsoft DiskPart version 10.0.14393.0
Copyright (C) 1999-2013 Microsoft Corporation.
On computer: JOSAV
DISKPART> list disk
Disk ### Status Size Free Dyn Gpt
-------- ------------- ------- ------- --- ---
Disk 2 Online 476 GB 0 B *
Disk 3 Online 1853 GB 0 B *
Disk 4 Online 14 GB 0 B
DISKPART> select disk 4
Disk 4 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> select partition 1
Partition 1 is now the selected partition.
DISKPART> active
DiskPart marked the current partition as active.
DISKPART> format fs=ntfs quick label=»2016»
100 percent completed
DiskPart successfully formatted the volume.
DISKPART> exit
Leaving DiskPart...
C:\WINDOWS\system32>f:
F:\>cd boot
F:\boot>bootsect /nt60 e:
Target volumes will be updated with BOOTMGR compatible bootcode.
E: (\\?\Volume{1d782b00-383c-11e6-9bc5-f62fb78d6ab6})
Successfully updated NTFS filesystem bootcode.
Bootcode was successfully updated on all targeted volumes.
xcopy f:\* e: /H /F /E
```

Каким образом проще всего импортировать несколько виртуальных машин из набора папок и автоматически исправить основные ошибки, такие как неправильное имя коммутатора или наличие большего количества ядер, чем поддерживается системой?

Представленный далее сценарий импортирует все виртуальные машины, обнаруженные в указанном наборе папок, и автоматически настроит коммутатор на новое подключение, которое он создает (вы можете изменить эту настройку на использование текущего подключения, которое у вас есть). Сценарий также составит отчет о том, есть ли у виртуальных машин больше ядер, чем поддерживает система, и решит эту проблему, изменив их количество на 4.

Импорт нескольких виртуальных машин из набора папок:

```
import-module hyper-v

$VMRootPath = 'C:\Workshop'

New-VMSwitch -Name "InternalSwitch" `
 -SwitchType Internal

$VMXMLFiles = Get-ChildItem -recurse
$VMrootPath\*.xml

foreach($VMXMLFile in $VMXMLFiles)
{
 #Import will fail as switch name is different
 $report = Compare-VM -Path $VMXMLFile
 foreach($incompatibility in
 $report.Incompatibilities)
 {
  if($incompatibility.MessageId -eq '33012')
  #Switch problem
  {
   Write-Output "Binding to different VMSwitch"
   $incompatibility.Source |
   Connect-VMNetworkAdapter
   -SwitchName "InternalSwitch"
  }
  if($incompatibility.MessageId -eq '25014')
  #Cannot restore saved state
  {
   Write-Output "Removing saved state"
   $Report.VM | Remove-VMSavedState
  }
  if($incompatibility.MessageId -eq '14420')
  #Too many cores
  {
   Write-Output "Changing number of cores to 4"
   $Report.VM | Remove-VMSavedState
   #Need to remove saved state to change cores
   $Report.VM | Set-VM -ProcessorCount 4
  }
 }
 $newvm = import-vm -CompatibilityReport $report
 start-vm -VM $newvm
}
```

Какую можно увидеть скорость подключения синтетических сетевых адаптеров в Hyper-V 2016?

В отличие от vmNIC на хостах виртуальных машин до появления Windows Server 2016, которые видели заданную скорость, на Windows Server 2016 и более поздних версиях хосты Hyper-V видят реальную скорость подключения адаптеров vmNIC, обслуживающих коммутатор vSwitch. Например, vSwitch, подсоеди-

Платформа HPE Superdome X и современные центры обработки данных

Современный центр обработки данных кардинально отличается от тех центров обработки данных, с которыми мы имели дело еще несколько лет назад. Тогда каждая рабочая нагрузка, как правило, обслуживалась отдельным сервером, и сотрудникам ИТ-подразделений приходилось работать со множеством серверов. Со временем на смену данной модели пришла виртуализация, и в дополнение к этому большое количество серверных систем было консолидировано. В современном дата-центре рабочие нагрузки перераспределяются в соответствии с откликом на нагрузку, а степень консолидации серверов сегодня выше, чем когда-либо прежде. Рассмотрим более подробно те важнейшие средства, необходимость в которых испытывают современные центры обработки данных, а также вопрос о том, как платформа HPE Superdome X удовлетворяет эти потребности.

Масштабируемость в рамках предприятия и производительность

Среди всех характеристик современного центра обработки данных самыми важными являются масштабируемость и производительность. Разумеется, «облако» снимает с компаний часть рабочих нагрузок. Но не все. «Облако» — это совместно используемая инфраструктура, доступ к которой предоставляется на всем пространстве Интернета. А это означает, что оно не в состоянии обеспечить того исключительно высокого быстродействия, которое мы можем получить при использовании выделенных серверов предприятия. Более того, как показывают расчеты аналитиков, ежегодный прирост объема обрабатываемых данных составляет от 30 до 50%, что требует соответствующего наращивания как вычислительной мощности, так и масштабов хранилищ данных. Платформа HPE Superdome X в состоянии обеспечить исключительно высокий уровень масштабируемости как для вычислительных мощностей, так и для памяти, а также для объемов средств хранения данных. Платформа Superdome X, способная поддерживать до восьми серверных модулей с 384 ядрами и 24 Тбайт оперативной памяти, позволяет справляться с самыми жесткими рабочими нагрузками, типичными для современных условий эксплуатации. При использовании в сочетании с флеш-массивом накопителей, таким как 3 PAR StorServ, она дает возможность достигать исключительно высоких показателей быстродействия в системе ввода-вывода и емкости массовой памяти.

Гибкость при работе с ресурсами и в управлении рабочими нагрузками

Необходимость реализовывать новые приложения может повлечь за собой кардинальные изменения в том, что касается требований к инфраструктуре предприятия и рабочих нагрузок. Способность системы адаптироваться к новым тенденциям приобретает исключительное значение. Реализованная в HPE Superdome X функция аппаратного разделения ресурсов (nPar) позволяет работать со множеством различных рабочих нагрузок точно так же, как если бы они выполнялись на отдельных серверах, и при этом нет необходимости управлять несколькими серверами. Средства nPar полностью изолированы друг от друга, так что требования каждого раздела не зависят от других разделов. В дополнение к этому, если в дальнейшем требования изменятся, средства nPar можно будет соответствующим образом переконфигурировать.

Доступность уровня предприятия

Число приложений, которые должны быть доступны ежедневно и круглосуточно, постоянно растет. Кроме того, информационные технологии ориентируются на потребителя, и у конечных пользователей формируется представление о том, что ИТ-услуги должны быть доступны всегда. Ориентированные на взаимодействие с рабочими нагрузками уровня предприятия встроенные в HPE Superdome X технологии, обеспечивающие надежность, доступность и удобство обслуживания (reliability/availability/serviceability, RAS), а также технологии микропрограмм реализуют поуровневый подход к выявлению, регистрации, анализу и восстановлению. В результате сокращаются перебои в обработке данных, а также время, затрачиваемое на поиск и исправление ошибок. Реализованная в Superdome X функция Firmware First обеспечивает возможность использования микропрограмм для выявления проблем и устранения неисправностей еще до того, как последние окажут влияние на операционную систему и программное обеспечение более высокого уровня.

Упрощенное управление и автоматизация

Используемые в центрах обработки данных технологии развиваются экспоненциально и становятся все сложнее. Виртуализация используется повсеместно, и многие компании прилагают усилия для реализации многочисленных серверных платформ, а также внедрения новых технологий, таких как контейнеры и Интернет вещей. Чтобы обеспечить решение подобных задач, необходимо высвобождать ресурсы, расходуемые на производственные операции и диагностику.

Платформа Superdome X позволяет сводить функциональные возможности группы серверов в единую систему. В результате снижается уровень требований к работе ИТ-подразделений, сокращаются операционные издержки и может быть снижен объем требований, касающихся лицензирования.

Майкл Оти (motey@windowsitpro.com) — технический директор Windows IT Pro и SQL Server Magazine, автор Microsoft SQL Server 2008 New Features (Osborne/McGraw-Hill)