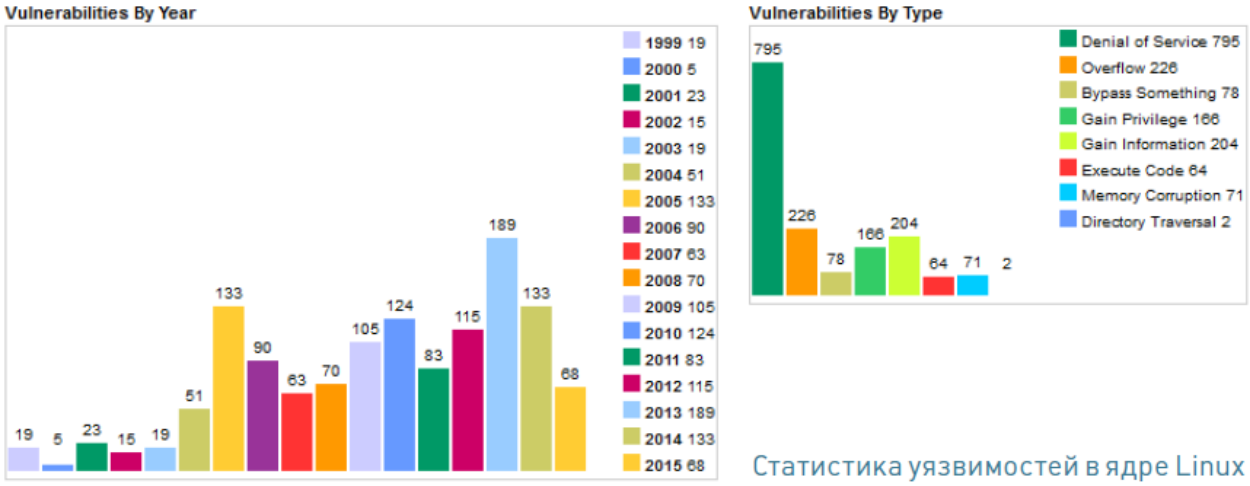
ЛЕКЦИЯ 14. УЯЗВИМОСТИ LINUX И WINDOWS

14.1. УЯЗВИМОСТИ LINUX

В драйвере Linux 4.0.5 ozwpan, имеющем статус экспериментального, выявлено пять уязвимостей, четыре из них позволяют организовать DoS-атаку через крах ядра, отправив специально оформленные пакеты. Проблема связана с выходом за границы буфера из-за некорректной обработки знаковых целых чисел, при котором вычисление в memcpy между required_size и offset возвращало отрицательное число, в итоге данные копируются в кучу.

Находится в функции oz_hcd_get_desc_cnf в drivers/staging/ozwpan/ozhcd.c и в функциях oz_usb_rx и oz_usb_handle_ep_data файла drivers/staging/ozwpan/ozusbsvc1.c. В других уязвимостях возникала ситуация возможного деления на 0, зацикливания системы или возможность чтения из областей вне границ выделенного буфера.

Драйвер ozwpan, одна из новинок Linux, может быть сопряжен с существующими беспроводными устройствами, совместимыми с технологией Ozmo Devices (Wi-Fi Direct). Предоставляет реализацию хост-контроллера USB, но фишка в том, что вместо физического подключения периферия взаимодействует через Wi-Fi. Драйвер принимает сетевые пакеты с типом (ethertype) 0x892e, затем разбирает их и переводит в различную функциональность USB. Пока используется в редких случаях, поэтому его можно отключить, выгрузив модуль ozwpan.ko.



14.1.1. Linux Ubuntu

ОС: Linux Ubuntu 12.04–15.04 (ядро до 15 июня 2015 года)
Уровень: Critical
Вектор: Local
CVE: CVE-2015-1328

Критическая уязвимость в файловой системе OverlayFS позволяет получить права root в системах Ubuntu, в которых разрешено монтирование разделов OverlayFS непривилегированным пользователем. Настройки по умолчанию, необходимые для эксплуатации уязвимости, используются во всех ветках Ubuntu 12.04–15.04. Сама OverlayFS появилась в ядре Linux относительно недавно — начиная с 3.18-rc2 (2014 год), это разработка SUSE для замены UnionFS и AUFS. OverlayFS позволяет создать виртуальную многослойную файловую систему, объединяющую несколько частей других файловых систем.

ФС создается из нижнего и верхнего слоев, каждый из которых прикрепляется к отдельным каталогам. Нижний слой используется только для чтения в каталогах любых поддерживаемых в Linux ФС, включая сетевые. Верхний слой обычно доступен на запись и перекрывает данные нижнего слоя, если файлы дублируются. Востребована в Live-дистрибутивах, системах контейнерной виртуализации и для организации работы контейнеров некоторых настольных приложений. Пространства имен для пользователей (user namespaces) позволяют создавать в контейнерах свои наборы идентификаторов пользователей и групп. Уязвимость вызвана некорректной проверкой прав доступа при создании новых файлов в каталоге нижележащей ФС.

Если ядро собрано с параметром CONFIG_USER_NS=y (включение пользовательского пространства имен), а при монтировании указан флаг FS_USERNS_MOUNT, OverlayFS может быть смонтирована обычным пользователем в другом пространстве имен, в том числе там, где допускаются операции с правами root. При этом операции с файлами с правами root, выполненные в таком namespaces, получают те же привилегии и при выполнении действий с нижележащей ФС. Поэтому можно смонтировать любой раздел ФС и просмотреть или модифицировать любой файл или каталог.

14.1.2. Уязвимости в основных приложениях

ОС: Linux
Уровень: Critical
Вектор: локальная, удаленная
CVE: CVE-2015-0235

Опасная уязвимость в стандартной библиотеке GNU glibc, которая является основной частью ОС Linux, и в некоторых версиях Oracle Communications Applications и Oracle Pillar Axiom, обнаруженная во время аудита кода хакерами из Qualys. Получила кодовое имя GHOST. Заключается в переполнении буфера внутри функции __nss_hostname_digits_dots(), которую используют для получения имени узла такие функции glibc, как gethostbyname() и gethostbyname2() (отсюда и название GetHOST).

Для эксплуатации уязвимости нужно вызвать переполнение буфера при помощи недопустимого аргумента имени хоста приложению, выполняющему разрешение имени через DNS. То есть теоретически эту уязвимость можно применить для любого приложения, использующего в той или иной мере сеть. Может быть вызвано локально и удаленно, позволяет выполнить произвольный код.

Самое интересное, что ошибка была исправлена еще в мае 2013 года, между релизами glibc 2.17 и 2.18 был представлен патч, но проблему не классифицировали как патч безопасности, поэтому на нее внимания не обратили. В итоге многие дистрибутивы оказались уязвимы. Вначале сообщалось, что самая первая уязвимая версия — 2.2 от 10 ноября 2000 года, но есть вероятность ее появления вплоть до 2.0. Среди прочих уязвимости были подвержены дистрибутивы RHEL/CentOS 5.x–7.x, Debian 7 и Ubuntu 12.04 LTS. В настоящее время доступны исправления. Сами хакеры предложили утилиту, поясняющую суть уязвимости и позволяющую проверить свою систему. В Ubuntu 12.04.4 LTS все нормально:

Практически сразу был выпущен модуль к Metasploit, позволяющий удаленно выполнить код на x86 и x86_64 Linux с работающим почтовым сервером Exim (с включенным параметром helo_try_verify_hosts или helo_verify_hosts). Позже появились и другие реализации, например модуль Metasploit для проверки блога на WordPress.

Чуть позже, в 2015 году, в GNU glibc были обнаружены еще три уязвимости, позволяющие удаленному пользователю произвести DoS-атаку или переписать ячейки памяти за пределами границы стека: CVE-2015-1472, CVE-2015-1473, CVE-2015-1781.

14.1.3. GNU Coreutils

ОС: Linux (GNU Coreutils)
Уровень: Low
Вектор: Local, Remote
CVE: CVE-2014-9471

GNU Coreutils — один из основных пакетов *nix, включающий практически все базовые утилиты (cat, ls, rm, date…). Проблема найдена в date. Ошибка в функции parse_datetime позволяет удаленному атакующему, не имеющему учетной записи в системе, вызвать отказ в обслуживании и, возможно, выполнить произвольный код, используя специально сформированную строку даты с использованием timezone.

14.1.4. Утилита grep

ОС: Linux (grep 2.19–2.21)
Уровень: Low
Вектор: Local
CVE: CVE-2015-1345

В утилите grep, которая используется для поиска текста по шаблону, редко находят уязвимости. Но эту утилиту часто вызывают другие программы, в том числе и системные, поэтому наличие уязвимостей гораздо проблематичнее, чем кажется на первый взгляд. Ошибка в bmexec_trans function в kwset.c может привести к чтению неинициализированных данных из области за пределами выделенного буфера или краху приложения. Этим может воспользоваться хакер, создав специальный набор данных, подаваемых на вход приложения при помощи grep -F. В настоящее время доступны обновления. Эксплоитов, использующих уязвимость, или модуля к Metasploit нет.

14.1.5. Уязвимость в FreeBSD

ОС: FreeBSD
Уровень: Low
Вектор: Local, Remote
CVE: CVE-2014-0998, CVE-2014-8612, CVE-2014-8613

Сразу три уязвимости были найдены в FreeBSD 8.4–10.x в конце января 2015-го исследователями из Core Exploit Writers Team. CVE-2014-0998 связана с реализацией драйвера консоли VT (Newcons), который предоставляет несколько виртуальных терминалов, включаемых параметром kern.vty=vt в /boot/loader.conf. CVE-2014-8612 проявлялась при использовании протокола SCTP и вызвана ошибкой в коде проверки идентификатора потока SCTP, реализующего SCTP-сокеты (локальный порт 4444).

Суть в ошибке выхода за пределы памяти в функции sctp_setopt() (sys/netinet/sctp_userreq.c). Это дает локальному непривилегированному пользователю

возможность записать или прочитать 16 бит данных памяти ядра и повысить свои привилегии в системе, раскрыть конфиденциальные данные или положить систему.

CVE-2014-8613 позволяет инициировать разыменование нулевого указателя при обработке полученного извне SCTP-пакета, при установке SCTP_SS_VALUE опции сокета SCTP. В отличие от предыдущих, CVE-2014-8613 может быть использована для удаленного вызова краха ядра через отправку специально оформленных пакетов.

В FreeBSD 10.1 защититься можно, установив переменную net.inet.sctp.reconfig_enable в 0, тем самым запретив обработку блоков RE_CONFIG. Или просто запретить использовать SCTP-соединения приложениям (браузерам, почтовым клиентам и так далее). Хотя на момент публикации разработчики уже выпустили обновление.

14.1.6. Уязвимость в OpenSSL

ОС: OpenSSL
Уровень: Remote
Вектор: Local
CVE: CVE-2015-1793

В 2014 году в OpenSSL, широко используемом криптографическом пакете для работы с SSL/TLS, была найдена критическая уязвимость Heartbleed. Инцидент в свое время вызвал массовую критику качества кода, и, с одной стороны, это привело к появлению альтернатив вроде LibreSSL, с другой — сами разработчики наконец взялись за дело.

Критическая уязвимость обнаружена Адамом Лэнгли из Google и Дэвидом Бенджамином из BoringSSL. Изменения, внесенные в OpenSSL версий 1.0.1n и 1.0.2b, привели к тому, что OpenSSL пытается найти альтернативную цепочку верификации сертификата, если первая попытка построить цепочку подтверждения доверия не увенчалась успехом.

Это позволяет обойти процедуру проверки сертификата и организовать подтвержденное соединение с использованием подставного сертификата, говоря другими словами — спокойно заманивать пользователя на поддельные сайты или сервер электронной почты или реализовать любую MITM-атаку там, где используется сертификат.

После обнаружения уязвимости разработчики 9 июля выпустили релизы 1.0.1p и 1.0.2d, в которых эта проблема устранена. В версиях 0.9.8 или 1.0.0 этой уязвимости нет.

14.1.7. Linux.Encoder

Появился целый ряд вирусов-шифровальщиков, вначале Linux.Encoder.0, затем последовали модификации Linux.Encoder.1 и Linux.Encoder.2, заразивших более 2500 сайтов. По данным антивирусных компаний, атаке подвергаются серверы на Linux и FreeBSD с веб-сайтами, работающими с использованием различных CMS — WordPress, Magento CMS, Joomla и других. Хакеры используют неустановленную уязвимость. Далее размещался шелл-скрипт (файл error.php), при помощи которого и выполнялись любые дальнейшие действия (через браузер). В частности, запускался троян-энкодер Linux.

Encoder, который определял архитектуру ОС и запускал шифровальщик. Энкодер запускался с правами веб-сервера (Ubuntu — www-data), чего вполне достаточно, чтобы зашифровать файлы в каталоге, в котором хранятся файлы и компоненты CMS. Зашифрованные файлы получают новое расширение .encrypted.

Также шифровальщик пытается обойти и другие каталоги ОС, если права настроены неправильно, то он вполне мог выйти за границы веб-сайта. Далее в каталоге сохранялся файл README_FOR_DECRYPT.txt, содержащий инструкции по расшифровке файлов и требования хакера. На данный момент антивирусные компании представили утилиты, позволяющие расшифровать каталоги. Например, набор от Bitdefender. Но нужно помнить, что все утилиты, предназначенные для расшифровки файлов, не удаляют шелл-код и все может повториться.

Учитывая, что многие пользователи, занимающиеся разработкой или экспериментирующие с администрированием веб-сайтов, часто устанавливают веб-сервер на домашнем компьютере, следует побеспокоиться о безопасности: закрыть доступ извне, обновить ПО, эксперименты устраивать на VM. Да и сама идея может в будущем использоваться при атаке на домашние системы.

14.1.8. Уязвимость Dirty COW

Название Dirty COW расшифровывается как Copy on Write. Ошибка возникает в файловой системе во время копирования при записи. Это локальная уязвимость, которая позволяет получить полный доступ к системе любому непривилегированному пользователю.

Если коротко, то для использования уязвимости нужно два файла, один доступен на запись только от имени суперпользователя, второй для нас. Начинаем очень много раз записывать данные в наш файл и читать из файла суперпользователя, через определенное время настанет момент, когда буферы обеих файлов смешаются и пользователь сможет записать данные в файл, запись которого ему недоступна, таким образом можно выдать себе права root в системе.

Уязвимость была в ядре около 10 лет, но после обнаружения была быстро устранена, хотя остались еще миллионы устройств Andoid в которых ядро не обновлялось и не думает и где эту уязвимость можно эксплуатировать. Уязвимость получила код CVE-2016-5195.

14.1.9. Уязвимость Stagefright

Если уязвимость получила кодовое имя, это однозначно означает, что она заслуживает внимания. Уязвимость Stagerfight не исключение. Правда, это не совсем проблема Linux. Stagefright — это библиотека для обработки мультимедийных форматов в Android.

Она реализована на C++, а значит обходит все защитные механизмы Java. В 2015 году было обнаружено целую группу уязвимостей, которые позволяли выполнить удаленно произвольный код в системе. Вот они CVE-2015-1538, CVE-2015-1539, CVE-2015-3824, CVE-2015-3826, CVE-2015-3827, CVE-2015-3828 и CVE-2015-3829.

Злоумышленнику было достаточно отправить MMS на уязвимый смартфон со специально модифицированным медиафайлом, и он получал полный контроль над устройством с возможностью записывать и читать данные с карты памяти. Уязвимость была исправлена разработчиками Android но до сих пор миллионы устройств остаются уязвимыми.

14.1.10. Уязвимость нулевого дня ядра

Это локальная уязвимость, которая позволяет повысить права текущего пользователя до root из-за ошибки в системе работы с криптографическими данными ядра, которые хранятся в памяти. Она была обнаружена в феврале 2016 года и охватывала все ядра начиная от 3.8, а это значит что уязвимость существовала 4 года.

Ошибка могла использоваться хакерами или вредоносным программным обеспечением для повышения своих полномочий в системе, но очень быстро была исправлена.

14.1.11. Уязвимость в MySQL

Эта уязвимость получила код CVE-2016-6662 и затронула все доступные версии сервера баз данных MySQL (5.7.15, 5.6.33 и 5.5.52), базы данных Oracle и клоны MariaDB и PerconaDB.

Злоумышленники могли получить полный доступ к системе через SQL запрос передавался код, который позволял заменить my.conf на свою версию и перезагрузить сервер. Также была возможность выполнить вредоносный код с правами суперпользователя.

Решения MariaDB и PerconaDB выпустили патчи достаточно оперативно, Oracle отреагировал, но намного позже.

14.1.12. Уязвимость Shellshock

Эта уязвимость была обнаружена в 2014 году перед тем как просуществовала 22 года. Ей был присвоен код CVE-2014-6271 и кодовое имя Shellshock. Эта уязвимость сравнима по опасности с уже известной нам Heartbleed. Она вызвана ошибкой в интерпретаторе команд Bash, который используется по умолчанию в большинстве дистрибутивов Linux.

Bash позволяет объявлять переменные окружения без аутентификации пользователя, а вместе в ними можно выполнить любую команду. Особой опасности это набирает в CGI скриптах, которые поддерживаются большинством сайтов. Уязвимы не только серверы, но и персональные компьютеры пользователей, маршрутизаторы и другие устройства. По сути, злоумышленник может выполнить удаленно любую команду, это полноценное удаленное управление без аутентификации.

Уязвимости были подвержены все версии Bash, включая и 4.3, правда после обнаружения проблемы разработчики очень быстро выпустили исправление.

14.1.13. Уязвимость Quadrooter

Это целая серия уязвимостей в Android, которая была обнаружена в августе 2016. Они получили коды CVE-2016-5340, CVE-2016-2059, CVE-2016-2504, CVE-2016-2503. Ошибке подвержены более 900 миллионов Android устройств. Все уязвимости были обнаружены в драйвере ARM процессора Qualcomm и все они могут использоваться для получения root доступа к устройству.

Как и DirtyCOW здесь не нужно никаких полномочий, достаточно установить вредоносное приложение и оно сможет получить все ваши данные и передать их злоумышленнику.

14.1.14. Уязвимость в OpenJDK

Это очень серьезная уязвимость linux 2016 в Java машине OpenJDK с кодом CVE-2016-0636, она затрагивает всех пользователей, работающих с Oracle Java SE 7 Update 97 и 8 Update 73 и 74 для Windows, Solaris, Linux и Mac OS X. Эта уязвимость позволяет злоумышленнику выполнить произвольный код за пределами Java машины, если вы откроете специальную страницу в браузере с уязвимой версией Java.

Это позволяло злоумышленнику получить доступ к вашим паролям, личным данным, а также запускать программы на вашем компьютере. Во всех версиях Java ошибка была очень оперативно исправлена, она просуществовала с 2013 года.

14.1.15. Уязвимость протокола HTTP/2

Это целая серия уязвимостей, которая была обнаружена в 2016 году в протоколе HTTP/2. Они получили коды CVE-2015-8659, CVE-2016-0150, CVE-2016-1546, CVE-2016-2525, CVE-2016-1544. Уязвимостям были подвержены все реализации этого протокола в Apache, Nginx Microsoft, Jetty и nghttp2.

Все они позволяют злоумышленнику очень сильно замедлить работу веб-сервера и выполнить атаку отказ от обслуживания. Например, одна из ошибок приводила к возможности отправки небольшого сообщения, которое на сервере распаковывалось в гигабайты. Ошибка была очень быстро исправлена и поэтому не вызвала много шума в сообществе.

14.2. УЯЗВИМОСТИ WINDOWS

К августу 2017 г. Microsoft исправила в общей сложности 48 уязвимостей безопасности в своих продуктах, в том числе 15 различных проблем безопасности в разных версиях Windows, начиная от Windows 7 и заканчивая Windows 10.

Технологический гигант утверждает, что информация о реальных атаках, использующих исправленные уязвимости, не поступала. Тем не менее, пользователям рекомендуется как можно скорее обновить свои системы.

25 из 48 уязвимостей были помечены Microsoft как критические. 27 из них могли применяться для проведения атак удаленного исполнения кода, а значит злоумышленники могли получить полный контроль над необновленной системой в случае успешной эксплуатации уязвимости.

Компания снова исправила уязвимость протокола SMB, но на этот раз в службе Windows Search. Данная уязвимость никаким образом не связана с атаками шифровальщиков WannaCry и Petya, которые также использовали слабые места протокола SMB в качестве вектора нападения.

В документации к CVE-2017-8620 Microsoft поясняет, что все версии Windows были затронуты данной проблемой безопасности. Эксплуатация уязвимости была возможна, если во время установки SMB подключения, служба Windows Search обрабатывала объекты в памяти. Злоумышленник мог устанавливать программы, получать доступ и редактировать данные или создавать новые учетные записи с полными правами пользователя.

Microsoft поясняет: “Для успешной эксплуатации данной уязвимости злоумышленник должен был отправить специально созданное сообщение в службу Windows Search. При наличии доступа к целевому компьютеру, злоумышленник мог эксплуатировать данную уязвимость для повышения привилегий и управления устройством. В случае с организациями, неавторизированный злоумышленник мог удаленно запускать эту уязвимость через SMB-соединение, а затем получать полный контроль над целевой системой”.

Пользователи Microsoft Edge и IE также подвержены рискам безопасности.

Браузеры Microsoft Edge и Internet Explorer также получили свою порцию патчей, а пользователям Windows 10 следует уделить особое внимание CVE-2017-0293 - уязвимости удаленного исполнения кода в библиотеке Windows PDF.

Microsoft отмечает уязвимость могла успешно эксплуатироваться, когда библиотека Windows PDF обрабатывала объекты в памяти, в результате чего злоумышленник получал такие же права, как и авторизированный пользователь. Эксплойты должны были содержать вредоносный PDF документ, который мог быть загружен в Microsoft Edge или Internet Explorer с вредоносных сайтов.

Для завершения установки обновлений безопасности потребуется выполнить перезагрузку системы. На данный момент о наличии проблем установки ничего неизвестно, и пользователи сообщают об успешной и беспроблемной установке обновлений.

14.2.1. Слежка за пользователями в Windows

О том, что Windows 10 стала активно и акцентировано собирать максимальное количество данных о каждом своем пользователе и использовать их в дальнейшем по непрозрачным схемам - стало довольно-таки резонансным событием.

Еще в 2014 году компания Microsoft опубликовала заявление о конфиденциальности, из которого следует, что на ее серверы может передаваться информация об использованных программах, устройстве и сетях, в которых они работают. Эти данные могут объединяться с идентификатором пользователя (учетная запись Microsoft), также собирается информация об адресе электронной почты, предпочтениях, интересах местоположении, и многом другом.

Чешское издание Aeronet.cz опубликовало расследование неназванного ИТ-специалиста, который решил отследить активность Windows 10 по сбору данных. По мнению исследователя, Windows 10 больше похожа на терминал по сбору данных, чем на операционную систему.

Наиболее активным «сборщиком» данных в новой ОС является голосовой помощник Cortana. Всю собранную информацию о пользователе сервисы новой ОС отправляют на десятки серверов. При этом исследователь заметил, что информация отправляется на серверы один раз в 15 минут (примерно по 80 мегабайт). При этом даже если отключить такие сервисы по передачи информации в настройках ОС, то передача информации и работа таких служб всё равно продолжает происходить в фоновом режиме.

Также ОС отслеживает поисковые запросы пользователя, анализирует почтовую переписку, чтобы узнать предпочтения и расписание владельца компьютера.

Все данные, передающиеся на серверы Microsoft, зашифрованы, поэтому понять, что конкретно отправляет система без необходимости взлома шифрования, просто невозможно.

Рассмотрим детально, что Microsoft берет с вашего компьютера:

1. Весь печатаемый текст. Не важно, каким приложением вы пользуетесь. Нажатия клавиш перехватываются на уровне операционной системы, данные собираются в пакеты и отправляются с периодичностью 1 раз в 30 минут на сервера корпорации.

Например, пользователь пишет письмо с помощью сервиса Gmail, работающего в Chrome или Firefox. Но текст письма всё равно будет перехвачен на низком уровне ОС и отправлен на сервера Microsoft. Зачем? Для того, чтобы работал этот сервис. Формальное объяснение от Microsoft: нужно для улучшения работы системы предиктивного ввода (ускоренный набор текста).

2. Геолокационные данные. И названия сетей Wi-Fi поблизости. Накапливаются и передаются раз в 30 минут. Позволяют отслеживать физические перемещения

пользователя с точностью до нескольких метров. Объяснение от Microsoft: данные нужны для поисковой системы Bing, чтобы она могла выдавать более релевантные ответы. Что это значит для пользователя: Microsoft знает ваш домашний адрес (зачем он нужен см. п. 5). Если у вас мобильное устройство с Windows 10, в Microsoft знают о всех местах, где вы бываете.

3. Запись с микрофона. Микрофон в Windows 10 включен постоянно (см. статью «Windows 10 тайно включает микрофон». Сначала высказывались предположения, что это необходимо для работы сервиса Cortana (голосовой помощник), но чуть позже стало известно, что отключение Cortana не решает проблему. Записи голоса пользователя могут накапливаться, какая-то часть из них отправляется на сервера Microsoft. Эксперты по компьютерной безопасности предупреждают: если вы пользуетесь зашифрованными средствами связи (например, используете SIP-телефонию с шифрованием трафика), такая несанкционированная запись звуков с микрофона может поставить вашу безопасность под удар. Использовать надежный канал VoIP одновременно с Windows 10 - совершенно бессмысленное занятие.

4. Телеметрия. Фантастическая по своей потенциальной небезопасности функция, которая даже не скрывается компанией-разработчиком. Телеметрия - это передача данных в Microsoft о состоянии вашего компьютера и вашей активности. Собирается буквально всё: какие программы установлены, какие запущены, объем занятой памяти, журналы приложений, фрагменты оперативной памяти и так далее. Учитывая, что в оперативной памяти может оказаться что угодно - от данных для служебного пользования до номеров кредиток - такая передача на чужие сервера является потенциальной уязвимостью. Хотя в Microsoft уверяют, что данные надежно шифруются, кто может гарантировать, что шифр не будет тайком взломан злоумышленниками? Ведь всем известно, что у Microsoft всегда были большие проблемы с безопасностью. Точнее, с устойчивой неспособностью эту безопасность обеспечить.

5. Борьба с пиратством. Windows 10 просматривает названия пользовательских файлов и сверяет с постоянно обновляемым списком пиратских новинок. Если находятся соответствия, листинги пользовательских директорий отправляются в Microsoft. Фактически, компьютер доносит на своего же владельца.

Напомним, данные об антипиратской активности Windows 10 были известны давно. Но предполагалось, что акцент будет сделан на борьбе с контрафактными играми. Сейчас становится понятно, что главная цель — лишить пользователей возможности скачивать с торрентов пиратские копии американских фильмов и сериалов.

Особо следует отметить, что сопоставление данных о наличии нелицензионного видео на компьютере пользователя с собранными геолокационными данными открывает отличную возможность для MPAA (Американская ассоциация кино) и RIAA (Американская ассоциация звукозаписи) отсудить у какой-нибудь американской домохозяйки очередную пару миллионов долларов. Российским пользователям, похоже, пока бояться нечего: система срабатывала только при обнаружении американских фильмов.

6. Портрет на память. Некоторые пользователи заметили, что после первой активации Windows 10 на короткий период включается web-камера. Исследования это подтверждают - в Microsoft передается 35 Мб данных сразу после активации и включения встроенной камеры. Предположительно, данные привязываются к пользовательскому аккаунту Microsoft.

Как итог, пользователи-программисты создали несколько утилит, противодействующие слежке со стороны Windows 10.