



Просьба о помощи, поступившая от одного из наших читателей, заставила следственный отдел CHIP столкнуться с очень опасным трояном. Если не знать, как с ним бороться, то за короткое время он может поразить множество компьютеров, в том числе и ваш.

Москва, 13:00 по местному времени. Тревожный телефонный звонок раздается в следственном отделе CHIP. Растерянный пользователь К. сообщает нам о неизвестном шантажисте, который заблокировал его раздел Windows, содержащий деловую информацию на десятки тысяч рублей. И теперь за «заложника» требуют выкуп: на указанный номер следует отправить SMS стоимостью 300 руб., после чего мошенники обещают прислать код для разблокировки раздела.

Нашей задачей было установить алгоритм, с помощью которого злоумышленник закодировал жесткий

диск, спасти раздел Windows и ценную деловую информацию, найти вымогателя и вернуть компьютер господину К., а также защитить его от подобных коварных атак в будущем.

Надеемся, что эта захватывающая, основанная на реальных событиях история заставит вас задуматься. Мы советуем прислушаться к нашим рекомендациям по защите компьютера, приведенным в конце этой статьи.

Деактивация: разблокировка Windows

Москва, 14:30 по местному времени. Следственная группа CHIP прибывает на место преступления. Это небольшая московская фирма, занимающаяся грузоперевозками. Пострадавший

К. включает свой компьютер. Вместо приветствия на экране появляется сообщение от вымогателя на русском языке. Для экстренного решения проблемы мы позвонили в антивирусную компанию «Доктор Веб» и обратились к ее техническому директору Игорю Данилову. Выслушав нас, он сообщил о вредителе следующее: «Скорее всего, речь идет о Trojan.Winlock.20 — новом трояне из категории ransomware. Цель у этого вредоносного ПО одна — получение денег путем требования выкупа». Как выяснилось, специалисты «Доктор Веб» уже имеют опыт «общения» с этим вредителем: «Данный троян появляется в основном в русскоязычном сегменте. И «вакцина» против него

ФОТО: КОМПАНИЯ ПРОИЗВОДИТЕЛИ

уже существует». Игорь Данилов сообщил нам следующий веб-адрес: <http://news.drweb.com/show/?i=304&c=9&p=0>. В размещенной на этой странице онлайн-форме нужно ввести номер, на который вымогатель требует отправить SMS. В ответ вы абсолютно бесплатно получите два кода, с помощью которых сможете осуществить разблокировку Windows. Алгоритм сработал: после ввода кода компьютер господина К. снова запустился в обычном режиме.

Но опасность пока не устранена окончательно: вредоносное ПО все еще остается на жестком диске. С помощью Игоря Данилова мы справились и с удалением вируса: для предотвращения его повторной загрузки сначала мы деактивировали управление системой с помощью апплетов Панели управления. Если бы на компьютере господина К. была установлена версия Windows XP Professional, это можно было бы легко сделать посредством групповых политик. Но с его вариантом системы (Home) нам пришлось поступить по-другому. В меню «Пуск | Выполнить» мы ввели команду «regedit» и нашли в реестре строку HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Здесь мы создали параметр типа DWORD с именем NoControlPanel и задали ему значение «1». Далее запустили перезагрузку, нажав при этом клавишу «F8», и в появившемся меню выбрали «Безопасный режим». И снова нас интересует реестр. Как сообщили нам специалисты компании «Доктор Веб», вирус записал новый код, который необходимо удалить вручную. В ветке HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon в значении параметра Userinit стираем все записи вида «%Temp%

don[любая последовательность символов].tmp». Снова перезагружаем Windows в обычном режиме и удаляем сделанную ранее запись (параметр NoControlPanel), чтобы получить доступ к управлению системой. Теперь все последствия работы трояна удалены, и мы переходим к следующему этапу.

Расследование: как вирус попал на компьютер?

Цифровые вредители чаще всего проникают на жесткий диск с сомнительных веб-сайтов или файлообменников. Мы спросили у господина К., не посещал ли он подобные ресурсы (например, www.cracks.am) и не использовал ли какой-либо торрент-клиент, например Vuze (Azoreus). Последовал отрицательный ответ: «Было бы слишком неосторожно делать это со своего рабочего места». На компьютере установлены вирусный сканер и брандмауэр, включено автоматическое обновление Windows. Таким образом, жертва предприняла все необходимые меры предосторожности. Несмотря на это, мы все же перепроверили заявление потерпевшего с помощью специальной программы BTF-Sniffer (к сожалению, она имеет только немецкоязычный интерфейс). В отчете данной утилиты подробно перечислялись недавно открытые файлы, установленные приложения, веб-сайты и т. д. Среди этого набора данных мы обнаружили указание на USB-накопитель фирмы Imapion. Господин К. уверен, что такого устройства в его компании не существует. Чтобы собрать больше информации об этом носителе, мы использовали программу USBDeview. Эта утилита показала все USB-устройства, независимо от того, подключены они в данный момент или нет. Она отобразила присвоенные им



ИНСТРУМЕНТЫ ДЕТЕКТИВА

Avast! 4 Home Edition

Надежно блокирует вирусы и трояны.

KeePass

Защищает секретность с помощью мастер-кода.

LauschAngriff

Разоблачает эксплойты «нулевого дня».

McAfeeAvert Stinger

Удаляет цифровых вредителей.

MUICacheView

Создает список установленных программ.

Password Safe

Управляет паролями.

PC Security Test

Симулирует хакерские атаки.

PeerGuardian

Блокирует опасные IP-адреса.

Powerbullet Presenter

Создает презентации данных.

Secunia PSI

Закрывает имеющиеся бреши в безопасности.

SpyBot — S&D

Находит шпионское ПО и уничтожает его.

USBDeview

Показывает подключение USB-накопителей.

при подсоединении имени, серийные номера и, что самое главное, время подключения. Для Imapion указано время «10:26:22» в день, предшествовавший нападению трояна. Господин К. заверяет нас, что в тот момент он был на деловой встрече за пределами офиса, и мы склонны ему верить. Итак, теперь нам известно, как троян попал на компьютер: это случилось во время отсутствия господина К. Но кто подключил к его компьютеру накопитель и скопировал вирус на жесткий диск? Теперь от обнаружения вымогателя нас отделяет всего один небольшой шаг.

Обнаружение: разоблачаем преступника

На этом этапе мы столкнулись с трудностями, поскольку у нас не было «орудия преступления». Однако нам сопутствовала удача: уборщица нашла накопитель Imapion в мусорной корзине после окончания рабочего дня. Его владельца недавно уволили, так что мотив преступления налицо: это месть. Путем криминалистической экспер- ➔



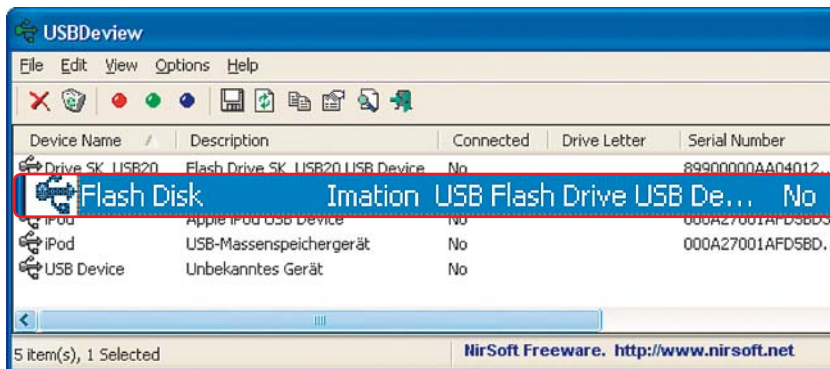
тизы мы нашли все доказательства и указали на преступника.

Чтобы не произвести никаких изменений на жестком диске злоумышленника, нам нужно было, не загружая ОС его компьютера, найти важные улики злонамеренных действий. Для этого мы запустили ПК с помощью загрузочного диска DEFT Linux (www.deflinux.net), основанного на системе Ubuntu и предназначенного как раз для таких случаев. В BIOS мы настроили привод CD как «First Boot Device». При перезапуске сначала выбрали язык, а затем в загрузочном экране ввели «defit-gui» для запуска Linux с графическим интерфейсом пользователя. С помощью ярлыка на рабочем столе мы запустили Partition Editor, чтобы узнать, какое имя дисков Linux присвоила жесткому диску преступника. Оно было задано как «sda1». С этого носителя мы выполнили резервное копирование, выбрав в качестве целевого привода внешний жесткий диск достаточной емкости, чтобы сохранить весь раздел.

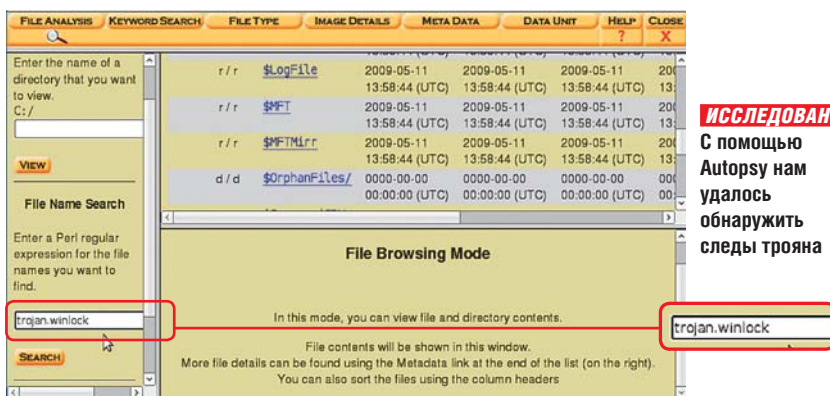
После резервного копирования мы открыли полученный образ, исследовали его содержание с помощью утилиты Autopsy и нашли ссылки на троян и посещенные интернет-страницы. HTML-файлы приводят нас на Russian Business Network, а также WSLabi — аукцион наподобие eBay, специализирующийся на продаже вредоносного ПО. Именно там преступник и приобрел вирус.



С помощью текстового редактора Gedit мы сохранили найденные улики. Описание действий преступника мы получили с помощью утилиты Autopsy, выбрав «File Activity Timelines | Create Data File».



РАЗЪЯСНЕНИЕ На компьютере пострадавшего мы нашли указания на USB-накопитель преступника



ИССЛЕДОВАНИЕ
С помощью Autopsy нам удалось обнаружить следы трояна

Итак, мы собрали все доказательства — теперь мы знаем, когда, куда и какой файл скопировал преступник, а также откуда появился троян. Чтобы потерпевший К. смог представить своему адвокату всю последовательность совершения преступления с точным указанием времени, мы оформили собранные данные в виде эффектной презентации.

Autopsy, к сожалению, не предусматривает такой возможности. Поэтому мы использовали Powerbullet Presenter. Эта программа работает как Microsoft PowerPoint, однако обладает серьезным преимуществом: созданную презентацию можно с помощью «File | Export» преобразовать в файл EXE, просмотр которого не требует наличия специального ПО. Утилита помещает этот файл в папку «Мои документы/Powerbullet». Мы скопировали ее на USB-накопитель. Господину К. теперь нужно просто открыть эту директорию на компьютере своего адвоката и запустить презентацию.

ПРИМЕЧАНИЕ Кодировка, по умолчанию используемая в Linux Ubuntu, — UTF-8, а в Windows — windows-1251 (cp1251). Текстовый редактор Gedit при открытии файлов, созданных в

Windows, не может правильно определить ее. Чтобы устранить это недоразумение, необходимо произвести некоторые манипуляции с файлом конфигурации данного редактора. Нажмите «Alt+F2» — при этом запустится gconf-editor. В открывшемся окне перейдите в раздел «/ | apps | gedit-2 | preferences | encodings». Отредактируйте ключ auto_detected, щелкнув по нему левой кнопкой мыши. Переместите в списке значение windows-1251 на самый верх, а затем сохраните изменения. Теперь русский текст в Gedit будет отображаться правильно.

Защита: вешаем на компьютер амбарный замок

Москва, 16:10 по местному времени. Мы удалили троян, нашли злоумышленника, уличили его в преступлении и оформили все доказательства таким образом, что в них разберется даже слабо подкованный в технике адвокат или судья. Главная улика, то есть жесткий диск преступника, не была подвергнута никаким изменениям. Но у нас осталось еще одно дело — защитить компьютер потерпевшего от подобных атак в будущем.

133