Автор:
06.03.14 16:40 -

Во время трансляции ТВ-передач ваш телевизор наблюдает за вами. Ноутбук отслеживает ваши действия при просмотре сайтов, а смартфон тайно сканирует каждую деталь вашего дома. Все эти изображения затем попадают в руки хакеров. И это вовсе не шутка, а вполне реальная угроза, поскольку наши устройства постоянно подключены к Сети, а также — что самое ужасное — оснащены камерами, которые порой плохо защищены от несанкционированного доступа извне.

В США уже зафиксирован инцидент скрытого слежения прокатными фирмами ноутбуков за своими клиентами, а также случаи, когда учителя присматривают за учениками. Все, на что способны установленные по умолчанию программы, вполне может выполнять и вредоносное ПО. Сегодня уже существуют вирусы, отображающие картинку с веб-камеры, чтобы усилить воздействие при шантаже, связанным с якобы заблокированной системой. Последствия становятся гораздо драматичнее, когда хакеры захватывают камеры мобильных устройств. Поскольку их используют в совершенно разных местах и постоянно перемещают, трояны при помощи регулярной незаметной съемки могут создавать подробные масштабируемые панорамы домов и офисов. Таким образом, к примеру, считывается информация с разложенных бумаг или настенных календарей. Ученые уже разработали соответствующее программное обеспечение Proof-of-concept для демонстрации принципиальной возможности подобной слежки.

Наряду с компьютерами и смартфонами существуют и современные телевизоры Smart TV со встроенными веб-камерами, которые тоже можно взломать . Мы выяснили степень опасности и расскажем, как защитить свои устройства и себя.

ПК и ноутбук: глаза постороннего

Веб-камеры для компьютеров существуют уже давно, так же как и способы их применения в преступных целях. Данные устройства можно было приобрести уже с середины 1990-х годов. Чаще всего они использовались для видеочатов и простого наблюдения. Сегодня большинство ноутбуков и моноблоков выходят с завода уже с расположенными в верхней части монитора встроенными камерами. Любая подходящая программа на ПК может их активировать и пересылать фото, видео, а также запись с микрофона на любой сервер в Интернете.

Вплоть до сентября 2012 года некоторые американские фирмы предлагали компьютеры

и лэптопы на правах лизинга. На них была предустановлена защитная программа от разработчика DesignerWare, позволяющая отследить и заблокировать аппараты пользователей, за которыми числился долг. Сотрудники семи таких лизинговых фирм нелегально использовали это ПО для получения доступа ко всевозможной информации: частным электронным письмам, данным для входа на различные сайты, банковским сведениям и даже фотографиям детей и взрослых с веб-камер. Американская Федеральная торговая комиссия запретила таким фирмам заниматься шпионажем, однако они даже не были наказаны. Подобный случай еще в 2010 году наделал много шума, когда выяснилось, что в школах одного из округов штата Пенсильвания осуществлялось скрытое наблюдение за учениками посредством выданных напрокат ноутбуков.

К каким последствиям может привести шпионаж через веб-камеру в эпоху киберпреследований, показывает самоубийство 18-летнего студента Тайлера Клементи из Нью-Джерси. Его сосед по общежитию с помощью веб-камеры тайно заснял компрометирующие сцены, сообщил об этом в Twitter, а затем выложил демонстрационную запись в свободный доступ в Интернет.

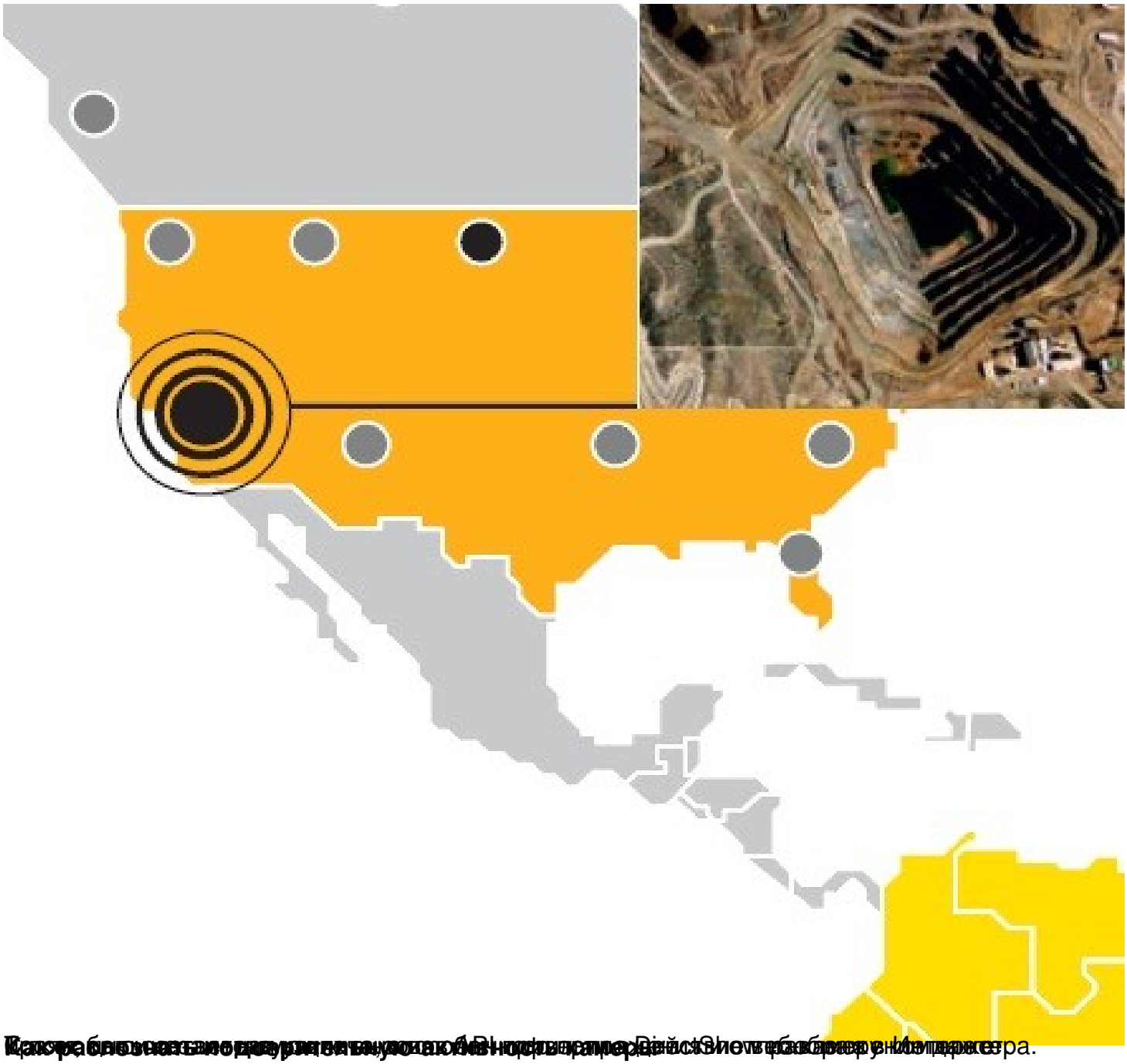
Как защитить свой компьютер?

Внешние USB-камеры предлагают больше возможностей контроля: если вы не пользуетесь ими, вы можете их накрыть чем-нибудь, отвернуть в сторону или же (самый надежный способ) отсоединить от порта. Модели, оснащенные светодиодом, могут сообщить о своей активности: если диод загорается в тот момент, когда не запущена соответствующая программа или видеочат, — это сигнал тревоги. Отключите камеру и запустите тщательное антивирусное сканирование.

Программные средства для шпионажа посредством веб-камер — это в первую очередь трояны-бэкдоры. Поэтому для предотвращения атак подобного рода подойдут те же меры, что и в целом для борьбы с вредоносным ПО — установка приложений только из достойных доверия источников и регулярное обновление баз антивируса. Кроме того, необходимо активировать брандмауэр Windows, а созданные для него исключения должны быть вам действительно необходимы и понятны.

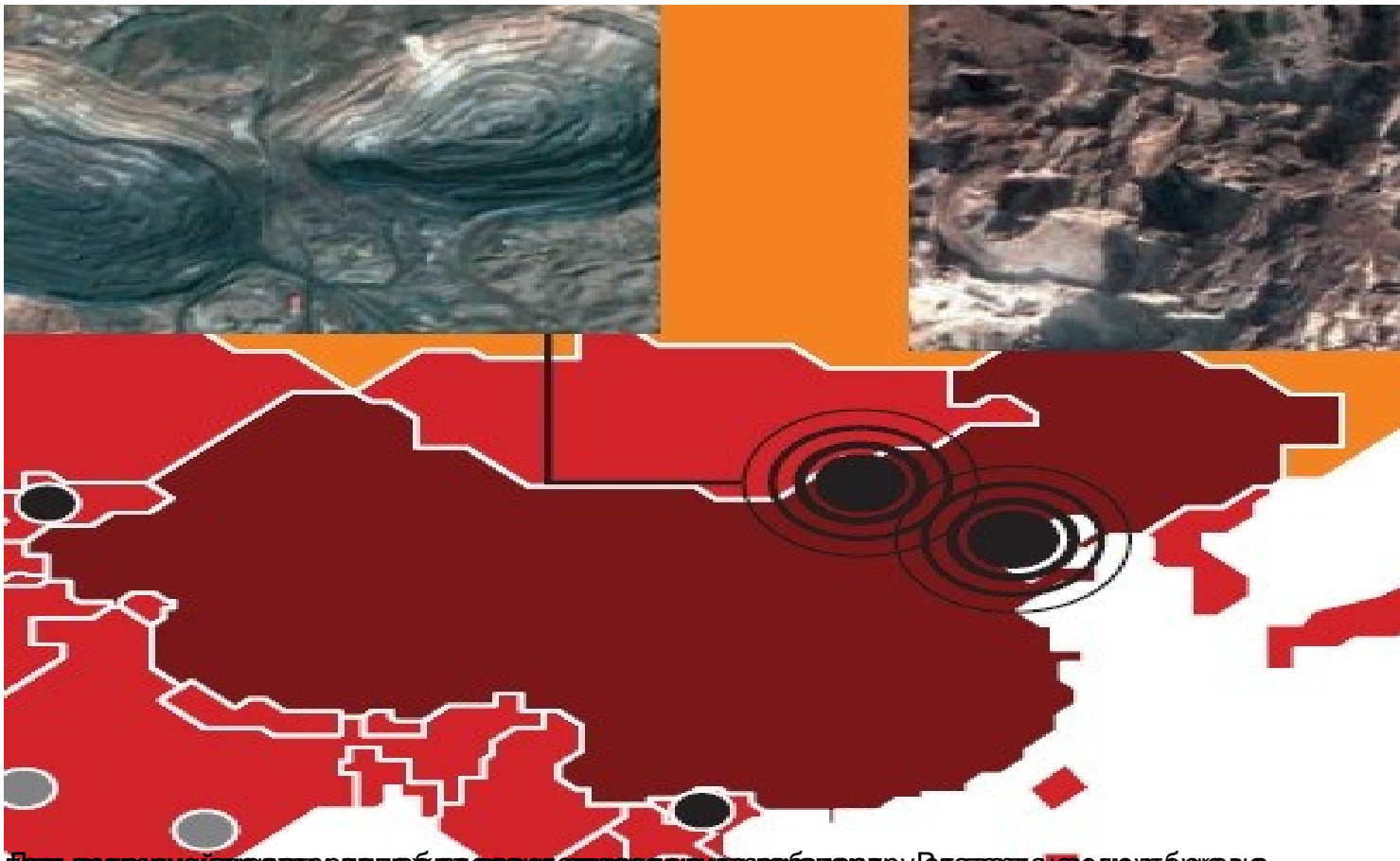
Как вредоносная программа перехватывает вашу веб-камеру

Автор:
06.03.14 16:40 -



Автор:
06.03.14 16:40 -

Автор:
06.03.14 16:40 -



Дополнительно

Read more http://www.chip.ua/stati/kak-ne-stat-obektom-slezhki-v-sobstvennoi-kvartire/