ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ПОДКЛЮЧЕНИЯ К ВЕБ-КАМЕРЕ

В. О. Патраков
Пермский государственный национальный исследовательский университет,
614990, Пермь, Букирева, 15

Сегодня практически у любого человека есть персональный компьютер или ноутбук, на котором установлена (или чаще встроена) веб-камера. Веб-камеры применяются для фиксации и дальнейшей передачи видео или скриншотов в программах типа Skype, Instant Messenger или в любых других видеоприложениях. Но задумывался ли кто-нибудь из нас о том, что веб-камера может использоваться не только в тот момент, когда мы этого хотим? Что злоумышленник может подключиться к нашей веб-камере, вторгаясь тем самым в наше личное пространство?

Я исследовал возможность такого вторжения и на основании полученных результатов разработал меры защиты от него.

Первое, о чём стоит сказать, - нельзя несанкционированно подключиться к любому человеку. Для того, чтобы получить какие-то данные с камеры, необходимо запустить на компьютере некоторый набор команд – какой-либо скрипт или программу, который будет отправлять данные с камеры в Интернет. Мной был написан один из вариантов такого скрипта.

Для отправки данных с камеры я использовал несколько программ: **MPlayer** – свободный медиаплеер, работающий на большинстве современных операционных систем; **RemCam2** – программа для подключения к веб-камере извне; **Sendmail** – консольный почтовый сервер, позволяющий из консоли отправлять электронные письма, а также прикладывать к ним файлы; **Rar** – архиватор, поддерживающий консольный режим.

Для установки этих программ на компьютер жертвы было решено использовать ftp-сервер, с которого нужные программы будут скачиваться в скрытом режиме. Для этого необходимо заранее создать ftp-сервер (в работе был использован сервис net2ftp.ru) и скачать на него нужные программы.

Основную проблему при подключении к веб-камере составляет подключение к компьютеру. Для подключения к компьютеру через Интернет надо знать его IP-адрес. Проблема состоит в том, что подавляющее большинство клиентов телекоммуникационных компаний имеют на своих компьютерах «серые» IP-адреса. Они не маршрутизируются в Интернете и на них нельзя отправить трафик из Интернета, только из конкретной частной локальной сети. К такому адресу невозможно подключиться несанкционированно. Таким образом, из-за особенностей топологии сети невозможно подключиться к компьютеру жертвы извне. Однако это не значит, что к компьютеру жертвы нельзя подключиться вообще. Большинство людей имеет дома маршутизатор, предоставленный

провайдером. К маршрутизатору уже подключаются все домашние устройства – домашний компьютер, ноутбук, телефон и т.д. Каждое из этих устройств имеет свой внутренний («серый») IP-адрес. При этом некоторая часть устройств подключается по беспроводному каналу – Wi-Fi.

Например, если жертва – ваш друг, и вы знаете пароль от его сети Wi-Fi, фактически вы можете незаметно находиться во внутренней сети, при условии, что вы находитесь внутри зоны покрытия этого Wi-Fi. Находясь во внутренней сети, вы можете подключиться к компьютеру жертвы, зная его IP-адрес, и затем подключиться к его веб-камере.

Для подключения к веб-камере из внутренней сети я использовал программу RemCam2. Программа имеет две части – серверную и клиентскую. Необходимо запустить серверную часть на компьютере жертвы. После запуска серверной части на удалённом компьютере необходимо запустить клиентскую часть, ввести IP-адрес жертвы (для получения IP-адреса используется команды ipconfig и почтовый клиент sendmail), и нажать кнопку ОК. Если всё установлено верно, то установится соединение с веб-камерой жертвы. Пример подключения представлен ниже.

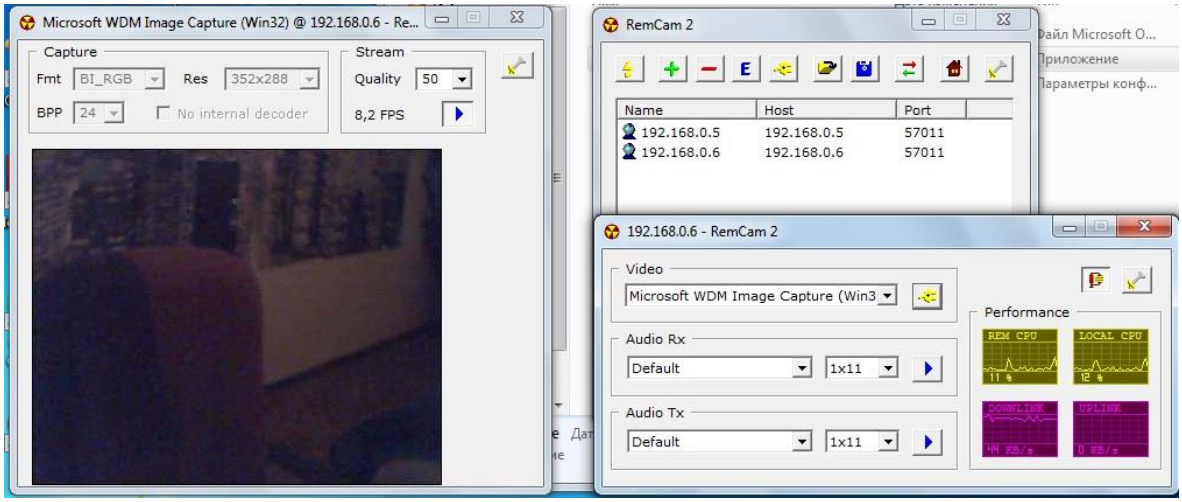

Рис 1. *Подключение к веб-камере при помощи RemCam2*

Для подключения из внешней сети используется Mplayer. Проигрыватель имеет один существенный недостаток – он не позволяет транслировать видео. Однако он позволяет делать скриншоты с видеоустройства, при этом не обязательно указывать его имя – оно выбирается по умолчанию. При этом первым видеоустройством является веб-камера, если же она отсутствует, в качестве видеоустройства выбирается рабочий стол. В данном случае было решено делать 20 скриншотов через каждые полторы минуты и соответственно каждые полчаса создавать архив с помощью программы Rar и с помощью Sendmail отсылать его на почту. Полученный результат представлен ниже.

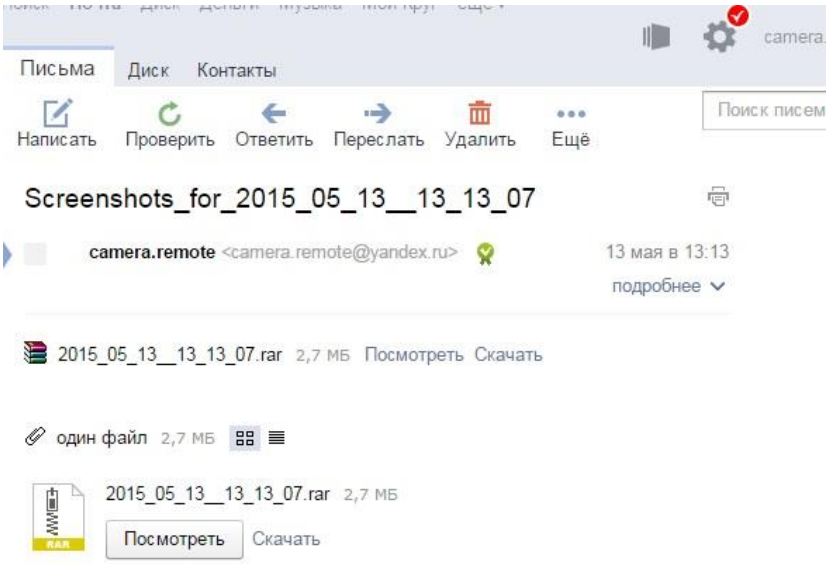

Рис 2. *Пример полученного письма*

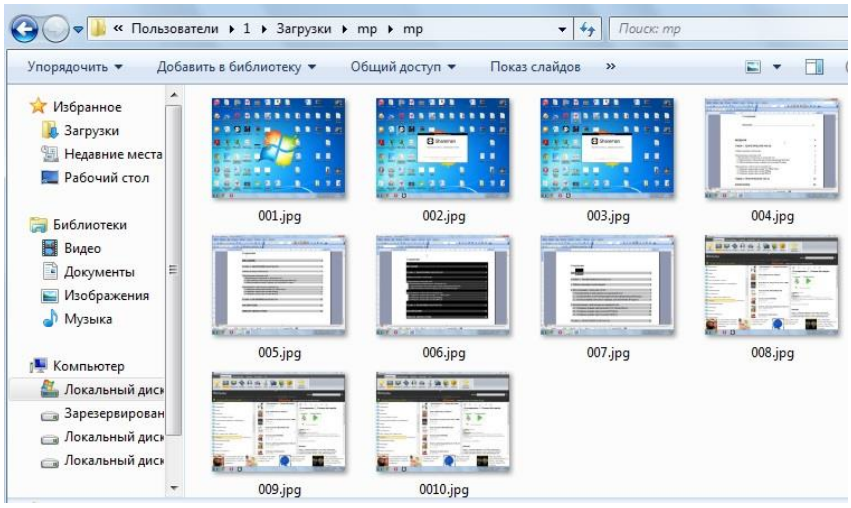

Рис 3. *Содержание полученного письма*

Написанный скрипт встроен в макрос в документе Microsoft Word. В результате, после открытия определённого файла Word (внедрить который на компьютер жертвы не составляет никакого труда) на компьютере выполняется набор команд, который позволяет в любой момент подключиться к камере при помощи программы RemCam2, а также периодически отправляет снимки с камеры на почту.

В ходе работы скрипта на компьютер жертвы с заранее подготовленного ftp-сервера скачиваются нужные программы и помещаются в папку, куда пользователь не заходит, например, C:\Windows\Server. Далее создаются правила для брандмауэра, разрешающие указанным программам и портам использовать соединение с Интернетом, запускается и прописывается в автозагрузку серверная часть программы RemCam2. Затем создаются еще 2 bat-файла: файл, отправляющий снимок с камеры и результат команды ipconfig на почту при старте системы и файл, который циклически делает

снимки, каждые 30 минут архивирует их и отправляет архив на почту. Все неиспользуемые в дальнейшем файлы удаляются, всем используемым присваивается атрибут «скрытый» и «системный».

Стоит заметить, что это только один из вариантов такого скрипта. Можно написать другую реализацию данной идеи, которая будет использовать другие программы и, возможно, другую логику.

На основании полученных данных можно сделать несколько выводов о том, как предотвратить такое подключение.

1. Лучше всего использовать на домашнем компьютере учётную запись пользователя, не имеющего прав администратора. Это будет эффективно, т.к. большинство используемых в работе программ при запуске будут требовать разрешения пользователя, и, таким образом, подключение не получится провести несанкционированно.
2. Можно отключить макросы в документах Microsoft Word, но это не будет эффективным, т.к. макросы использовались в данной работе для примера. Аналогичный представленному в работе скрипт можно запустить из любой другой программы, либо с любой ссылки в Интернете.
3. Более эффективный способ защиты – отключать веб-камеру, либо заклеивать её, если она встроена, когда вы её не используете. Но при этом, исходя из результатов данной работы, человек, подключающийся к вам, может увидеть ваш рабочий стол, что тоже представляет собой угрозу. Кроме того, стоит помнить, что аналогично веб-камере можно подключиться к любым другим устройствам, например – к микрофону.
4. Самый эффективный способ защиты – аккуратность. Будьте аккуратны со всеми документами и программами, которые вы скачиваете, со всеми страницами в Интернете, которые вы посещаете.

Список литературы

1. Mihoel Pikovsky. Тестируем софт для записи скринкастов в Windows и Linux. URL: https://xakep.ru/2013/11/26/screencast-soft-windows-linux
2. RemCam2 – программа для скрытого подключения к удалённой вебкамере. URL: http://www.spy-soft.net/remcam-2