Пугин Михаил Сергеевич
Эксперт отделения компьютерных экспертиз
отдела инженерно-технических экспертиз
ЭКЦ УМВД России по Архангельской области

Mikhail Sergeevich Pugin
Expert of computer expertise department
of engineering and technical expertise Forensic Center
of the Ministry of Internal Affairs of the
Russian Federation in the Arkhangelsk region

ДЕМОНСТРАЦИЯ ПРОГРАММЫ «HTTP&DNS SERVER», РАЗРАБОТАННОЙ ДЛЯ ДИНАМИЧЕСКОГО АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ «ВРЕДОНОСНОГО» ПО

DEMONSTRATION OF THE PROGRAM «HTTP & DNS SERVER», DEVELOPED FOR DYNAMIC ANALYSIS OF NETWORK ACTIVITY OF «MALWARE»

Аннотация: «HTTP&DNS Server» – программа используется для производства компьютерных экспертиз и исследований «вредоносного» ПО и позволяет имитировать работу «командного» Web-сервера с использованием стендового компьютера без выхода в сеть Интернет. Программа обладает возможностями перехвата, обработки и последующего перенаправления HTTP запросов по заданным критериям.

Abstract: «HTTP & DNS Server» – a program used for the production of computer expertise and research «malware», which allows you to simulate the «command» Web-server, using a bench computer, without access to the Internet. The program has the ability to intercept, process and redirect HTTP requests on the specified criteria.

Ключевые слова: HTTP, DNS, Server, компьютерная, экспертиза, вредоносное, эмулятор, Андроид.

Keywords: HTTP, DNS, Server, computer, expertise, malware, emulator, Android.

Программа «HTTP&DNS Server» разработана в ЭКЦ УМВД России по Архангельской области экспертом отделения компьютерных экспертиз Пугиным М.С. Она используется для исследования «вредоносного» ПО при производстве компьютерных экспертиз и исследований, позволяет имитировать работу «командного» Web-сервера без использования сети Интернет (рис. 1).

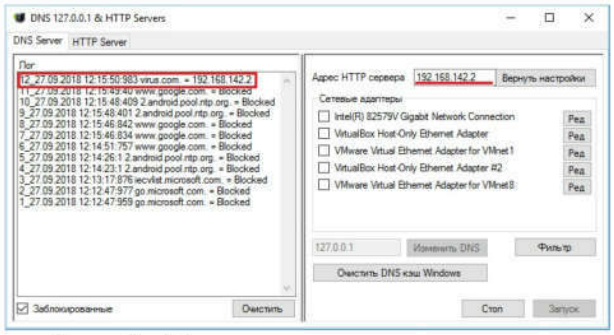

Рис. 1. Главное окно программы

Программа обладает возможностями перехвата, обработки и последующего перенаправления HTTP-запросов по заданным критериям и состоит из двух основных частей. Первая отвечает за обработку DNS-запросов[1], вторая – за обработку HTTP запросов[2].

Для взаимодействия с DNS-запросами необходимо в сетевых настройках исследуемой операционной системы установить IP-адрес DNS-сервера, соответствующий IP-адресу, установленному в сетевых настройках операционной системы, на которой исполняется программа «HTTP&DNS Server».

Далее в программе требуется установить IP-адрес HTTP-сервера (в автоматическом либо ручном режиме). В автоматическом режиме выбирается первый имеющийся IP-адрес в сетевых настройках операционной системы. HTTP-сервер может быть запущен на удаленной операционной системе, поэтому требуется установить корректный IP-адрес HTTP-сервера, на который будут перенаправляться все DNS-запросы.

Во время использования DNS-сервера отображаются все DNS-запросы от запущенных приложений. Для исключения не интересующих DNS-запросов имеется гибкая система фильтров (рис. 2). Не интересующие DNS-имена добавляются в список «заблокированных DNS адресов», которым не присваивается IP-адрес.

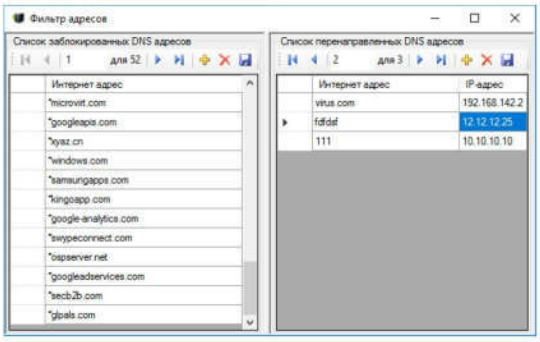

Рис. 2. DNS-фильтр

Имена, добавленные в список «перенаправленных DNS адресов», будут

[1] Далее – DNS-сервер.
[2] Далее – HTTP-сервер.

перенаправляться независимо от списка «заблокированных DNS адресов».

Вторая часть «HTTP-сервер» предназначена для взаимодействия с приложениями по протоколу «HTTP». Главное окно программы «HTTP-сервер» представлено на рис. 3.

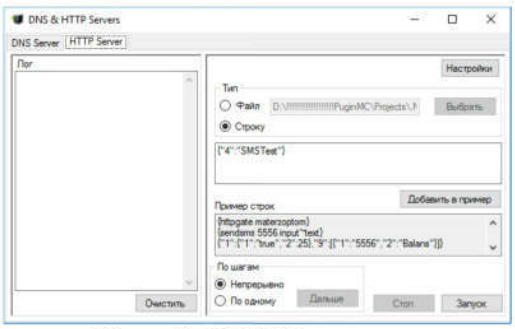

Рис. 3. HTTP-сервер

В качестве ответа можно отправить заданную строку с параметрами либо выбранный файл. При отправке требуется сформировать заголовок ответа, свойства которого описаны в настройках. Пример сформированного заголовка ответа от сервера «virus.ru» представлен на рис. 4.

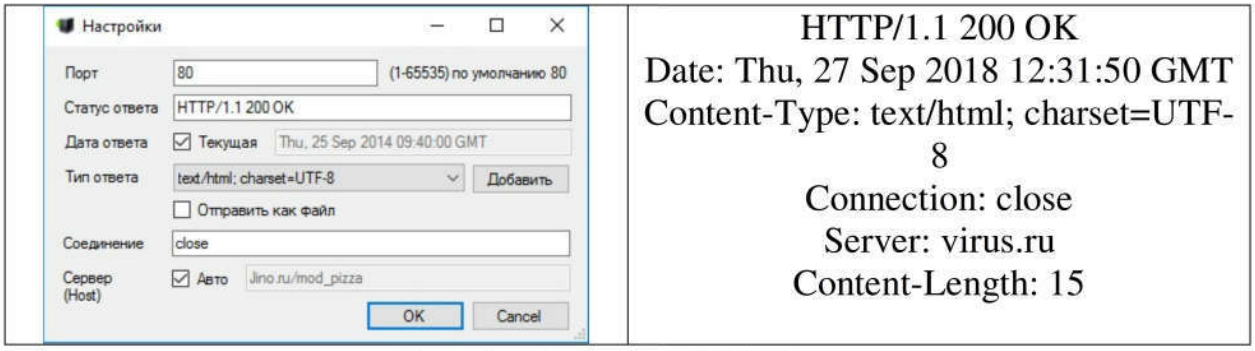

Рис. 4. Настройки HTTP-сервера

При отправке ответа требуется выбрать, например, «text/html; charset=UTF-8» (для текста) либо «application/vnd.android.package-archive» (для исполняемого файла-архива с расширением «apk»). Для удобного пошагового управления HTTP-ответами имеется возможность выбора обработки запросов «По одному».

Пример использования. Имеется исполняемый файл-архив «Viber.apk», содержащий программу с именем пакета программы «com.g.biz.inj», определяемый программой «Kaspersky Endpoint Security 10» как «HEUR:Trojan-Spy.AndroidOS.SmsThief.de». Для динамического анализа указанной программы были запущены две виртуальные машины «Android Virtual Device» под управлением операционной системы «Android 4.1.1 с абонентскими номерами «5554» и «5556»[1]. Указанный файл был установлен в Эмулятор 5554.

При запуске файла в операционной системе выдается ошибка.

[1] Далее – Эмулятор 5554 и Эмулятор 5556.

Предположительно, программа, имеющаяся в файле «Viber.apk», проводит проверку оборудования. При статическом анализе декомпилированного кода обнаружены строки, содержащие проверку оборудования (например, модель устройства). Наименование оборудования, имеющегося в проверке, было переименовано, и файл «Viber.apk» заново скомпилирован.

После запуска файла «Viber.apk» появляется окно активации прав администратора, далее в окне «DNS Server» – запись о запросе DNS-имени «trustcompanyfire.in.ua», который был перенаправлен на IP-адрес «192.168.142.2», являющийся IP-адресом сетевой карты «Virtual Box Host-Only Ethernet Adapter #2» (рис. 5).

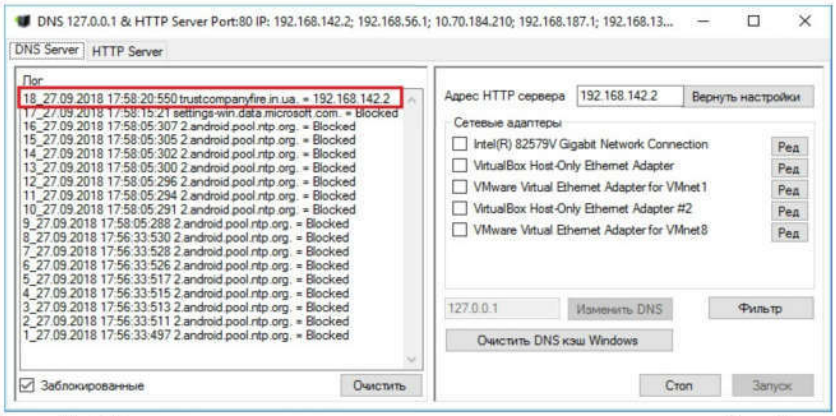

Рис. 5. Перенаправление адреса «trustcompanyfire.in.u»

Далее в окне «HTTP Server» появляется запись о POST-запросе (рис. 6) по протоколу HTTP версии 1.1 на ресурс «/oki_google.php?m=set&imei=123456789012300&b=rucarlone&time=10» сервера «trustcompanyfire.in.ua», содержащий текст:

model=RRRRRRRRRRRRRRRRRRRRRR86&phone=11111115554&admin=true&imei=123456789012300&device=GENERIC_X86&api=4.1.1&type=registration&simserial=89014103211118510720&operator=Android&country=ru

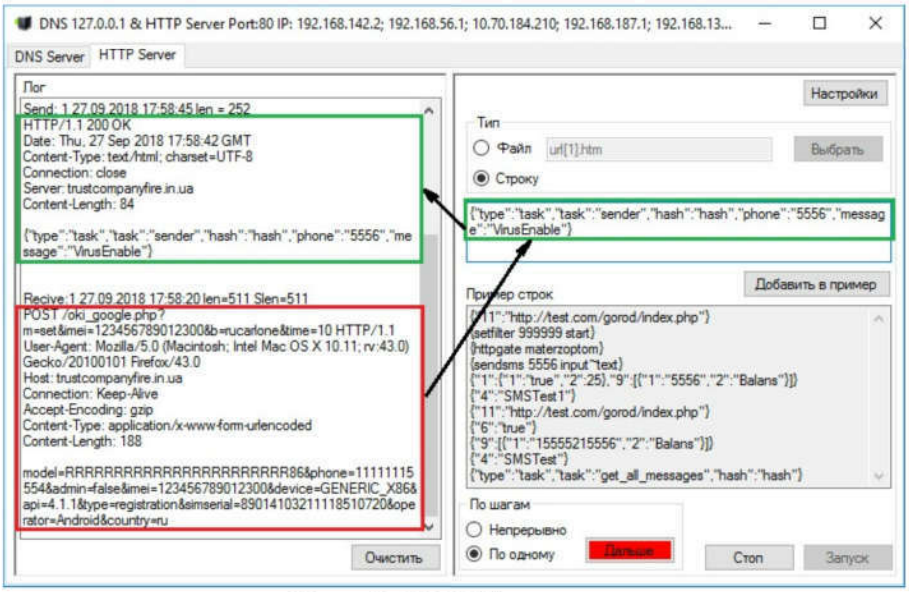

Рис. 6. POST-запрос

Указанный текст содержит сведения об оборудовании, в том числе IMEI, IMSI, модель устройства, абонентский номер телефона, сведения об операторе связи, версия sdk. На указанный запрос отправляется ответ, содержащий строку с параметрами:

```
{"type":"task","task":"sender","hash":"hash","phone":"5556","message":"VirusEnable"}
```

Строка содержит команду на отправку SMS-сообщения на номер «5556» с текстом «VirusEnable». Она получена путем статического анализа декомпилированного кода. В результате указанных действий на «Эмуляторе 5556» отобразилось принятое SMS-сообщение с текстом «VirusEnable» и номером отправителя «15555215554», а на «Эмуляторе 5554» сведения об отправленном сообщении не отображаются (рис. 7). Аналогичным образом анализируются и другие команды исследуемого приложения.

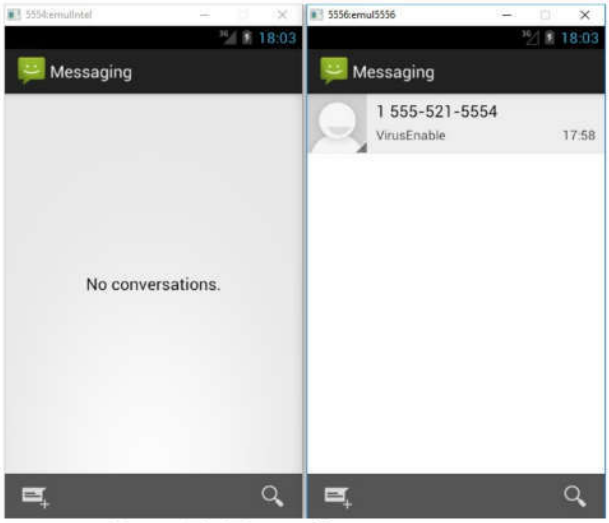

Рис. 7. Два «Эмулятора»

В итоге данная программа позволяет экспериментально показать направленность «вредоносной» программы на совершение преступлений, связанных с хищением денежных средств в сфере дистанционного банковского обслуживания.

Использование программы «HTTP&DNS Server» значительно ускоряет процесс исследования «вредоносных» программ, разработанных для различных операционных систем.