А. Г. Бельтов, И. Ю. Жуков, Д. М. Михайлов, А. В. Стариковский, А. М. Толстая

АТАКИ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ, ИСПОЛЬЗУЮЩИЕ МЕХАНИЗМ АВТОМАТИЧЕСКОЙ НАСТРОЙКИ

На сегодняшний день мобильный Интернет, бесспорно, является необходимым инструментом современного делового человека. Получить и отправить почту, проверить курсы ценных бумаг, выйти на связь в интернет-пейджере и многое-многое другое, что необходимо сделать вне стен офиса или дома, — для этих целей операторы сотовой связи предлагают технологию передачи данных с помощью сетей мобильной связи GPRS.

Аббревиатура GPRS расшифровывается как General Packet Radio Service, что переводится как «пакетная радиосвязь общего пользования». По сути, это дополнение мобильной технологии GSM, поддерживающее пакетные данные.

К сожалению, этот стандарт не обеспечивает должной защищенности передаваемой информации, в результате чего злоумышленники получают возможность прослушивать интернет-трафик, что позволяет им узнать конфиденциальные данные пользователя, пароли, банковскую информацию и другие критические сведения.

Способы обхода встроенных в GPRS механизмов защиты известны достаточно давно и по мере сил закрываются сотовыми операторами и производителями мобильных телефонов и программного обеспечения для них [1]. В данной статье рассматриваются атаки с использованием технологии удаленной настройки, которым ранее не уделялось должного внимания.

На современном рынке мобильной связи существует новый механизм удаленной настройки мобильных устройств, разработанный и внедряемый корпорацией «Open Mobile Alliance».

Суть разработки заключается в том, что с помощью специальных SMS-сообщений можно осуществить переконфигурацию сотового телефона для подключения различных служб: Интернета, синхронизации с персональным компьютером, поддержки MMS-сообщений, загрузки необходимых приложений из Сети.

Подобные сообщения для последних моделей телефонов имеют название «OMA-настройки», для более старых моделей — «OTA-настройки». Почти все мобильные устройства в настоящее время поддерживают один из этих двух типов настроек.

Данный механизм достаточно гибок, что позволяет OMA/OTA-технологии постепенно завоевывать рынок. Частные организации нередко прибегают к разработке собственных настроек для конфигурирования корпоративных телефонов сотрудников. Иногда такими услугами пользуются банки, что помогает им настроить мобильные кошельки на телефонах пользователей.

К сожалению, гибкость технологии позволяет использовать ее и в преступных целях — для перехвата интернет-трафика пользователя. Для этого злоумышленник может использовать механизм удаленной настройки телефона для подмены DNS-сервера, который при каждом подключении обеспечивает трансляцию имен сайтов в IP-адреса.

Как правило, атакующий меняет адрес DNS-службы на указатель своего Proxy-сервера, который ретранслирует через себя все запросы пользователя, ведя при этом подробный список всех ресурсов, к которым обращалась жертва, и перехватывая все пароли. Если сервер настроен определенным образом, то он может вместо доступа к ресурсам, которые хочет увидеть атакуемый абонент, перенаправлять его на альтернативные сайты. А это дает обширные возможности для мошенничества.

Для того чтобы осуществить подмену DNS-сервера, злоумышленник формирует следующую автоматическую настройку:

```
<wap-provisioningdoc>
<characteristic type="NAPDEF">
<parm name="NAME" value="NewAPN"/>
<parm name="NAPID" value="NewAPN NAPID ME"/>
<parm name="BEARER" value="GSM.GPRS"/>
<parm name="NAP.ADDRESS" value="apn . new . com"/>
<parm name="NAP.ADDRTYPE" value="APN"/>
<parm name="DNS.ADDRESS" value="x . y .w. z "/>
</characteristic>
<characteristic type="APPLICATION">
<parm name="NAME" value="NewAPN"/>
<parm name="APPID" value="w2"/>
<parm name="TO.NAPID" value="NewAPN NAPID ME"/>
</characteristic>
</wap-provisioningdoc>
```

В поле DNS.ADDRESS указывается адрес Proxy-сервера злоумышленника. Остальные поля устанавливаются таким же образом, как и в стандартной настройке сотового оператора. Далее сообщение переводится в формат WBXML и отправляется жертве.

При его получении на экране телефона появится предложение принять настройку. Злоумышленник может подписать ее произвольным образом, например: «Перенастройка Интернета в связи со снижением тарифа». А в качестве телефона отправителя с помощью атаки с использованием SMS-шлюза можно указать имя сотового оператора жертвы [2].

Интеграция современных информационных технологий в мобильную связь не только предоставляет широкие возможности владельцам устройств, но и несет в себе серьезную угрозу. Согласившись на подключение к одному из предлагаемых сетевых сервисов, пользователь может дать разрешение на установку вредоносной программы в свой сотовый телефон. Такие программы, по аналогии с подслушивающими устройствами, часто называют «жучками».

Приложением злоумышленник сможет управлять дистанционно. Подобная программа может передавать содержание полученных SMS-сообщений, перехватывать информацию о звонках, а также о местоположении телефона в настоящий момент. Приложение-жучок будет иметь полный доступ к записной книжке и списку контактов.

Типичным способом проникновения «жучка» является получение вышеупомянутой автоматической настройки. Рассмотрим спецификацию и механизм работы данного типа услуг и укажем на уязвимости, которые приводят к попаданию на мобильное устройство приложений-жучков.

Для конфигурации телефонного аппарата необходимо правильно составить текст настройки для конкретного производителя и модели телефона с помощью языка XML. Приведем пример настройки Интернета-WAP:

```
<wap-provisioningdoc>
<characteristic type="NAPDEF">
<parm name="NAPID" value="JAVA_NAPID"/>
<parm name="BEARER" value="JAVA_OMA_BEARER"/>
<parm name="NAP-ADDRESS" value="JAVA_APN"/>
<parm name="NAP-ADDRTYPE" value="JAVA_NAP-ADDRTYPE"/>
<characteristic type="NAPAUTHINFO">
<parm name="AUTHTYPE" value="JAVA_PPP_AUTHTYPE"/>
```

```
<parm name="AUTHSECRET" value="JAVA_AUTHSECRET"/>
</characteristic>
</characteristic>
<characteristic type="PXLOGICAL">
<parm name="PROXY-ID" value="JAVA_PROXY-ID"/>
<parm name="STARTPAGE" value="JAVA_STARTPAGE"/>
<characteristic type="PXPHYSICAL">
<parm name="PXADDR" value="JAVA_IP"/>
<parm name="PXADDRTYPE" value="JAVA_PXADDRTYPE"/>
<parm name="TO-NAPID" value="JAVA_NAPID"/>
<characteristic type="PORT">
<parm name="PORTNBR" value="JAVA_PORT"/>
</characteristic>
</characteristic>
</characteristic>
<characteristic type="BOOTSTRAP">
<parm name="NAME" value="JAVA_NAME"/>
</characteristic>
<characteristic type="APPLICATION">
<parm name="APPID" value="JAVA_APPID"/>
<parm name="NAME" value="JAVA_NAME"/>
<characteristic type="RESOURCE">
<parm name="URI" value="JAVA_STARTPAGE"/>
</characteristic>
</characteristic>
</wap-provisioningdoc>
```

Тег param с именем STARTPAGE представляет собой явное указание стартовой страницы, на которую пользователь попадет при первом входе в Интернет. Злоумышленник может указать в данном поле адрес вредоносного приложения. Это означает, что неопытный пользователь вместе с настройкой установит на свой телефон приложение-«жучок». Отметим, что как раз неопытные пользователи больше других нуждаются в автоматических настройках, так как не уверены, что смогут сделать это самостоятельно. Конечно, опытный пользователь сможет определить угрозу и отменить передачу подозрительных программ. Но если данное приложение будет иметь название «Дополнительный пакет к настройке», то даже он с трудом сможет распознать вирус. В настоящее время такие вредоносные программы малоизвестны, и поражающий эффект от первой волны подобных атак может быть значительным.

Ситуация усугубляется тем, что, согласно данной технологии, отправить настройку можно, перекодировав XML-файл в бинарный вид с помощью программ, находящихся в открытом доступе, например xml2wbxml.

Чтобы отправить полученный бинарный файл настройки через коммерческий SMS-шлюз, необходимо правильно составить заголовок SMS-сообщения. Такой заголовок называется UDH [3].

Спецификация заголовка является открытой. Это означает, что любой злоумышленник может вместо простого текстового сообщения отправить настройку, указав на коммерческом SMS-шлюзе, что он собирается отправить сообщение, которое уже закодировано в бинарный вид.

Приведем пример запроса к коммерческому шлюзу, который внедряет вирусный код.

https://somesmscenter.org/https/sendmsg?session_id=11AB23CCD2349&udh=123456789&text=AB12373BCDACB34234CBDEF34234534323ACBDDDABCD124523224256789111110230423 54BCAADHFEEABCDD23445C54C1123BCAB1ACBA234CBCABDBAECDEACCAEBCDF2342352434444444442342342341345785782342881234 13

В этом запросе в параметре UDH указывается составленный для данного приложения заголовок сообщения. В поле text передается программа настройки. Заголовок сообщения и текст настройки представлены в шестнадцатеричном виде.

Как видно из представленных примеров, злоумышленниками при совершении атаки на мобильное устройство используется совмещенная техника — социальная инженерия плюс применение возможностей мобильной платформы. Если сами по себе функции операционной системы не являются уязвимыми в прямом смысле этого слова, то при невнимательности и неосторожности пользователя они становятся мощным инструментом для совершения противоправных действий.

Попытки повысить техническую грамотность пользователей мобильных устройств продолжаются в течение всей истории существования мобильной связи, однако из-за массовости этого сектора успеха не имеют. Поэтому социальная инженерия всегда будет использоваться при совершении подобных атак.

По-другому дело обстоит с реализацией функций операционной системы. Постоянно повышающиеся требования к безопасности мобильных устройств, которые из разряда средства связи переходят в класс личного помощника, хранящего огромное количество персональной информации, вынуждают производителей мобильных платформ создавать новые механизмы повышения безопасности и контролируемости мобильной операционной системы. Тем не менее рынок все еще ожидает создания продукта, краеугольным камнем архитектуры которого стала бы безопасность использования устройства во враждебной среде.

СПИСОК ЛИТЕРАТУРЫ:

1. *Xenakis C., Apostolopoulou D., Panou A., Stavrakakis I.* A Qualitative Risk Analysis for the GPRS Technology // IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008.

2. *Зуйков А. В., Михайлов Д. М., Стариковский А. В., Фроимсон М. И.* Уязвимость системы коммерческих SMS-шлюзов в инфраструктуре GSM-сетей // Сборник материалов II Ежегодной Всероссийской научно-практической конференции с международным участием. Новосибирск: СИБПРИНТ, 2010. С. 321–326.

3. *Henry-Labordere A., Jonack V.* SMS and MMS interworking in mobile networks, Artech House Inc., Boston, 2004.