Г. А. Европейцев, М. И. Фроимсон, Г. А. Урванов

АТАКИ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ С ПОМОЩЬЮ SMS-СПАМА

С ростом функциональных возможностей мобильных телефонов увеличивается диапазон угроз, которым подвержены их владельцы, направленных на перехват конфиденциальной информации, получение финансовой выгоды и вывод устройств из строя.

SMS-спам мобильных телефонов — достаточно редкое явление в настоящее время, но весьма эффективное, если целью злоумышленника является отключение функции приема текстовых сообщений мобильного устройства пользователя. Выглядят подобные атаки обычно следующим образом: на мобильный телефон неожиданно приходит SMS со странным содержанием: «Скоро ваш телефон не сможет принимать сообщения» или же с любым другим текстом. Через секунду приходит еще одно SMS, потом еще и еще. За минуту может прийти до ста подобных сообщений, которые будут поступать до тех пор, пока память телефона, выделенная для хранения SMS-сообщений, не будет полностью исчерпана. Даже если владелец мобильного устройства постарается быстро удалить поступающие SMS, то ему не удастся этого сделать, так как они будут поступать слишком интенсивно. Узнать, от кого приходят странные сообщения, невозможно, так как каждое может иметь различные телефонные номера отправителей, например: '+700000000', '+700000001' и т. д.

Это запланированная и хорошо продуманная атака, направленная на отказ мобильного устройства принимать SMS-сообщения. К тому же отправка даже ста SMS — это совсем не дешево, а значит, либо злоумышленник не скупится на средства, чтобы вывести телефон из строя, либо в его арсенале есть весьма эффективный метод атаки.

В ближайшее время SMS-спам для мобильных устройств может стать серьезной угрозой. Эта атака стала возможна благодаря плохой защищенности SMS-шлюзов — сервисных служб, которые позволяют отправлять и получать SMS-сообщения без использования мобильного телефона [1]. В общем виде SMS-шлюз представляет собой некий сервер в сети Интернет, который установлен на передающей и принимающей GSM-станции и имеет возможность не только взаимодействовать по тем или иным протоколам с компьютерами в Глобальной сети, но и обмениваться SMS-сообщениями с мобильными телефонами пользователей. При этом SMS-шлюз получает из сети Интернет запросы на отправку SMS-сообщений и направляет их получателю. Аналогичным образом происходит обратная пересылка.

Такие службы известны многим пользователям именно благодаря возможности бесплатной отправки SMS-сообщений с сайтов в сети Интернет.

Мало кто знает, что эти же SMS-шлюзы позволяют подключаться к ним приложениям для массовой рассылки.

Многие коммерческие программы пользуются этими возможностями для того, чтобы внедрить на предприятии систему оповещения сотрудников о выплате заработной платы, изменениях в расписании работы или автоматизировать процесс отправки SMS-сообщений с поздравлениями в дни рождений работников компании.

Для связи с коммерческими приложениями в SMS-шлюзах предусмотрен специальный интерфейс взаимодействия, который обычно представляет собой четко прописанную последовательность обмена HTTP-запросами [2].

К сожалению, в настоящее время какого-либо серьезного контроля таких SMS-шлюзов нет. Поэтому злоумышленник может зарегистрироваться на сервере и отсылать SMS-сообщения на любые номера с произвольным содержанием. Все, что необходимо для этого злоумышленнику, — это оплатить создание своей собственной учетной записи и пополнить свой баланс на определенную сумму, из которой будут вычитаться деньги за отправленные SMS-сообщения.

С учетом того, что многие мобильные устройства выделяют ограниченный размер памяти для хранения SMS, злоумышленник может организовать непрерывную отправку сообщений на произвольный номер и, переполнив память телефона, препятствовать получению важной информации через текстовые сообщения.

Приведем конкретные примеры подобного вида атак.

Примитивный HTTP/HTTPS-интерфейс для доступа к SMS-шлюзам позволяет организовать массовую рассылку с помощью скриптового языка даже не самому опытному пользователю. При этом какая-либо проверка на большинстве серверов на предмет спама отсутствует.

Более того, некоторые команды, предоставляемые пользователю, работающему через SMS-шлюз, позволяют непрерывно отправлять однотипные сообщения на несколько мобильных телефонов. Содержание SMS-сообщений в большинстве случаев не проверяется на SMS-шлюзе. Создание бесконечного цикла отправки приводит к переполнению памяти телефона. Имея на счету даже небольшую сумму денег, злоумышленник способен атаковать несколько мобильных устройств, так как цена одного сообщения на SMS-шлюзе для коммерческой организации крайне мала.

В примере приведен код на интерпретируемом языке PHP, который организует переполнение памяти телефона, посылая 100 одинаковых сообщений с помощью услуг SMS-шлюза.

```
<?
$user="user";
$password="password";
$api_id="xxx";
$baseurl="http//some-sms-gate.com";
$text=urlencode("Текст сообщения");
$to="7903xxxxxxx";        //Телефон атакуемого

//запрос на начало сессии по отправке sms

$url="$baseurl/http/auth?user=$user&password=$password&api_id=$api_id";

//получение положительного ответа от gate

$ret= file ($url); $sess=split(":", $ret[0]);

//непосредственная отправка sms

if ($sess[0]=="OK")
{
$sess_id=trim($sess[1]);
for ($i=0;$i<100; i++)
{
$url="$baseurl/http/sendmsg?session_id=$sess_id&to=$to&text=$text";
$ret=file($url);
$send=split(":",$ret[0]);
if ($send[0] == "ID") echo "success <br> message ID: ".$send[1];
else echo "send message failed";
}
}
else { echo "Authentification failure:".$ret[0]; exit(); }
?>
```

Для осуществления атаки злоумышленник запускает с персонального компьютера, имеющего доступ в Интернет, скрипт, подобный приведенному выше. Программа может иметь произвольное название, например spam.php. Выполнение скрипта осуществляется набором в браузере следующей строки: “http://<имя сервера>/spam.php”.

В начале программы приводится определение основных используемых переменных, которые нужны для прохождения аутентификации на SMS-шлюзе. Переменные user и password используются соответственно для хранения имени пользователя и его пароля. Идентификатор api_id используется для того, чтобы SMS-шлюз мог сопоставить пользователя с его учетной записью и проверить, достаточно ли на соответствующем счету денежных средств для отправки SMS-сообщений. Каждый зарегистрированный на сервере пользователь может иметь несколько учетных записей с раздельными денежными балансами. Текст сообщения и адрес атакуемого записываются соответственно в переменные $text и $to. Далее эти переменные используются в самом скрипте.

Согласно протоколу работы SMS-шлюза сначала осуществляется запрос на начало сессии. Ответ принимается с помощью PHP-функции file и проверяется на наличие разрешения на отправку SMS путем сравнения ответа с эталонным «OK». В случае удачной проверки запускается цикл из ста проходов.

В каждом шаге цикла на номер атакуемого абонента отправляется по одному SMS-сообщению. Если отправка прошла удачно, то на экран выводится сообщение: «Success. Message was sent». Строчка с сообщением «Authentification failure» будет показана браузером в том случае, если указан неверный идентификатор в переменной $api_id или же на балансе учетной записи пользователя на SMS-шлюзе не хватает денежных средств.

К явным признакам атаки со стороны SMS-шлюза относятся:

- большое количество телефонных номеров, с которых приходят сообщения;
- высокая интенсивность получения сообщений в случае, если номер телефона отправителя не меняется, а текст различен;
- нетипичный телефонный номер отправителя.

В случае осуществления действительно преднамеренной атаки необходимо понимать, что экстренно удалять сообщения не имеет смысла, так как интенсивность их поступления слишком высока.

Защиту от возникновения подобной ситуации должен осуществлять сотовый оператор, к которому подключены атакуемые телефоны. К сожалению, существование по всему миру огромного количества SMS-шлюзов, не все из которых хранят подробные данные о клиентах, имеющих на их серверах учетные записи, затрудняет контроль над этими сервисами.

Решение проблемы может также лежать в установке на телефон операционной системы, предусматривающей защиту от переполнения SMS-памяти. Тем не менее в настоящее время таких специализированных на безопасности платформ на рынке нет, а устанавливаемые поверх операционной системы приложения и патчи не могут считаться полностью доверенными и могут не только не защитить пользователя от атаки, но и, обладая собственными уязвимостями, и, возможно, закладками, напротив, ослабить защиту мобильного устройства.

СПИСОК ЛИТЕРАТУРЫ:

1. *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.
2. *Henry-Labordere A., Jonack V.* SMS and MMS interworking in mobile networks. Artech House Inc., Boston, 2004.