Детальный анализ бэкдора Linux/Ebury

Наш пост посвящен анализу OpenSSH бэкдора и похитителя паролей Linux/Ebury. Этот анализ является результатом совместной работы ESET с немецким CERT-Bund, шведским центром SNIC и европейской организацией CERN, а также других организаций, которые входят в международную рабочую группу (Working Group). Linux/Ebury представляет собой сложный бэкдор, используемый злоумышленниками для похищения аутентификационных данных OpenSSH, а также получения доступа к скомпрометированному серверу (backdoor).

Согласно предыдущим отчетам, этот бэкдор уже активен как минимум два года. Linux/Ebury может дистрибуцироваться в двух различных формах: вредоносная библиотека и патч к бинарным файлам OpenSSH. Вредоносная библиотека представляет собой модификацию файла *libkeyutils.so*. Эта библиотека является общей для компонентов OpenSSH и загружается его исполняемыми файлами, такими как *ssh*, *sshd* и *ssh-agent*. В анализе будет опубликована информация о том, как вредоносный код осуществляет кражу аутентификационных данных учетных записей и как системные администраторы могут обнаружить зараженную систему.

Вредоносный код Linux/Ebury является интересным по некоторым причинам. Прежде мы видели вредоносные библиотеки под Windows и это первый случай когда мы наблюдаем схожий модуль для систем POSIX. Он также использует инновационные приемы для перехвата функций, внедрения в адресное пространство процесса, который загружает библиотеку и модифицировать код во время исполнения. Мы полагаем, что прежде чем использовать метод внешней библиотеки для получения доступа к OpenSSH процессу, автор Linux/Ebury использовал специальный патч для модификации исходного кода OpenSSH, тем самым добавив «новые возможности» к этому ПО. Первые варианты вредоносного кода выглядили именно так, поскольку мы обнаружили модифицированные бинарные файлы OpenSSH на диске одного из скомпрометированных серверов: *ssh*, *sshd* и *ssh-add*. Мы также наблюдали использование комманд rpm для удаления сигнатур из оригинального пакета ПО OpenSSH (*openssh-server* и *openssh-clients*), а также модификацию базы данных RPM для обновления хэшей файлов на их вредоносные

модифицированные аналоги. Такая модификация позволяет не допустить обнаружения модификации файлов через проверку их хэшей с использованием команды *rpm --verify openssh-servers*. В то же время команда *rpm -qi openssh-servers* покажет их отсутствие.

Более поздние варианты Linux/Ebury не модифицируют файлы OpenSSH напрямую. Вместо этого они используют свой вариант библиотеки libkeyutils.so, которая подключается всеми исполняемыми файлами OpenSSH. Изменения, которые проводятся над оригинальной библиотекой, похожи на те, которые использовались для модификации бинарных файлов OpenSSH, которые мы упоминали выше, за исключением того, что выполняется перехват некоторых функций, а также осуществляется их патчинг в процессе исполнения (runtime patching). Обычно этот файл имеет размер 10 Кб. Вредоносный код добавляет около 20 Кб своего кода к этому файлу, после чего размер файла равен уже 30 Кб.

Ниже представлены два примера того, как бэкдор устанавливается в системе. Первый показывает зараженный Linux/Ebury файл, который следует за чистым файлом libkeyutils.so. Символьная ссылка модифицирована и указывает на вредоносную версию.

```
lrwxrwxrwx 1 root root    20 Jun 22  2012 /lib64/libkeyutils.so.1 -> libkeyutils.so.1.3.0*
-rwxr-xr-x 1 root root 10192 Jun 22  2012 /lib64/libkeyutils.so.1.3*
-rwxr-xr-x 1 root root 32920 Jun 22  2012 /lib64/libkeyutils.so.1.3.0*
```

Следующий скриншот показывает сценарий, при котором библиотека libkeyutils.so перезаписана вредоносной версией.

```
[root@localhost ~]# ls -al /lib*/libkey*
lrwxrwxrwx 1 root root    18 Jun 21  2012 /lib64/libkeyutils.so.1 -> libkeyutils.so.1.3
-rwxr-xr-x 1 root root 32888 Jun 21  2012 /lib64/libkeyutils.so.1.3
```

Хотя практика размещения вредоносного кода внутри библиотек уже наблюдалась ранее, это первый случай когда мы обнаружили ее в Linux для изменения поведения OpenSSH.