РАЗРАБОТКА МЕТОДА ИДЕНТИФИКАЦИИ АНОНИМНЫХ ПОЛЬЗОВАТЕЛЕЙ СЕТИ TOR

РешетниковС.Ю.
Научный руководитель Ботыгин И.А.
Томский политехнический университет
resh.sersh@gmail.com

Введение

В настоящее время все большую популярность среди анонимных пользователей набирает сеть TOR. Это сеть, состоящая из прокси-серверов, которые позволяют устанавливать анонимное сетевое соединение, свободное от прослушивания. Она также может рассматриваться как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Сеть TOR написана, преимущественно, на языках программирования C, C++ и Python. Среди анонимных пользователей данной сети могут быть и злоумышленники. Поэтому поиск способов их идентификации является актуальной задачей.

В современных автоматизированных системах, основанных на компьютерных технологиях, известны методы идентификации пользователей, построенные на хранении IP-адресов компьютеров и записи на компьютер пользователя данных в виде cookie-файлов. Более сложным является метод, основанный на семантико-синтаксическом анализе данных пользователя. Данные методы идентификации обладают рядом недостатков, одними из которых является низкая степень достоверности идентификации, либо необходимость создания специализированных семантико-синтаксических и морфологических анализаторов [1-3]. Помимо вышеуказанных методов, существуют и другие технологии, позволяющие собирать информацию, характеризующую рабочую среду пользователя. Методы таких технологий предполагают выявление с помощью JavaScript «уникального отпечатка» пользователя, по которому его можно идентифицировать. К таким идентификационным меткам можно отнести:

- Скорость взаимодействия с колёсиком мыши, которая зависит от конфигурации операционной системы, от аппаратной составляющей, а также и от настроек пользователя.
- Скорость перемещения курсора мыши.
- Характеристики процессора пользователя.
- Объект TextRectangle, содержащий свойства для чтения left, top, right и bottom, описывающие бокс пользователя с границами в пиксельном измерении [4].
- Тег canvas в HTML5, который предназначен для создания растрового изображения. У данного тега есть особенность отрисовки шрифтов. Их рендеринг каждый браузер осуществляет по-разному в зависимости от различных факторов [5].

Описанные методы с помощью JS-кода могут быть установлены на нескольких участниках информационного обмена в частной сети и идентифицировать их. Например, реализацией MITM-атаки (Exit-node), в ходе которой JS-код внедряется во все веб-страницы, которые посещает во внешней сети резидент сети Tor. Или реализацией атаки межсайтового скриптинга (XSS) при взаимодействии внедренного кода с сервером злоумышленника.

Таким образом, если еще учесть, что достаточно большое число проанализированных ресурсов частной сети подвержены таким атакам, то это дает возможность скомпрометировать веб-приложения и поднять дорвеи (doorway), разместить там необходимый JS-код и начать составлять базу данных уникальных фингерпринтов [5]. Это, в том числе, позволит выявить уникальные идентификаторы («отпечатки») пользователей сети Tor, чтобы отслеживать их деятельность в Интернете и соотносить с посещением различных страниц.

Целью настоящей работы является разработка метода идентификации злоумышленников, использующих сеть Tor для анонимного доступа к сетевым ресурсам и выработка рекомендаций по обеспечению информационной безопасности сетевых сообществ и веб-сервисов от таких атак.

Постановка задачи

Исходя из проведенного анализа работы сети Tor, можно сделать вывод об ее очень хорошей защищенности, но, тем не менее, не свободной от недостатков. Все отмеченные уязвимости технически учесть достаточно сложно из-за их сложности, поэтому в данной работе будет использоваться для изучения ограниченный набор уязвимостей. В качестве основного разрабатываемого положения предложим метод внедрения маркера на компьютер злоумышленника. Для этого необходимо будет провести следующий комплекс работ:

а) проанализировать трафик сети Tor;

б) разработать инфраструктуру тестового веб-приложения;

в) разработать и использовать идентификационный маркер;

г) провести исследования на тестовом веб-приложении по идентификации пользователя.

Ход работы

В качестве инструмента для захвата сетевого трафика использовалась консольная версия программы Wireshark – утилиты с интерфейсом

командной строки tshark, которая является бесплатной и содержит все необходимые средства для анализа трафика. Утилита выполняет, в том числе, захват пакетов в формате libpcap, что позволяет их удобно анализировать уже в самой программе Wireshark. Исследования по идентификации проводились на тестовых ОС Windows, работающих на Virtualbox.

С помощью средств языка PHP был создан корректный JavaScript-сценарий, который перезагружал текущую страницу и одновременно с этим передавал файлу vkr.php методом GET значение, содержащееся в JS-переменной. Для этого на страницу выводился открывающий блок JS-кода с помощью оператора echo, внутри которого задавалась средствами JS перезагрузка текущей страницы (document.location.href). В качестве адреса страницы использовалось значение элемента REQUEST_URI из глобального массива $_SERVER и к нему добавлялся параметр с именем u_name со значением, равным значению содержащегося в JS-переменной.

Полученные значения хешировались и помещались в базу данных. Полученный хеш – это и есть уникальный идентификатор (фингерпринт).

В проведенных исследованиях использовались Java-уязвимости. Этому есть несколько причин:

а) Java-уязвимости в подавляющем большинстве своем – платформо независимые, что позволяет активно использовать их против целевых систем под управлением Windows, OS X и Linux;

б) Java работает на большом количестве персональных компьютерах и в миллиардах устройств (в том числе в мобильных телефонах и в телевизорах) по всему миру;

в) Java-уязвимости довольно просто эксплуатируются, так как не требуют обхода DEP/ASLR и прочих механизмов безопасности;

В качестве инструмента для создания, тестирования и использования идентификационного маркера, основывающегося на апплетах java, использовалась платформа Metasploit Framework. И инструментарий Social-Engineer Toolkit. Это фреймворк, который используется для испытания проникновением (Penetration Testing).

В эксперименте использовался Java signed applet эксплойт. Данный эксплойт динамически создает файл с расширением .jar, а затем подписывает его. Получившийся подписанный апплет представляется пользователю через веб-страницу с тегом <applet>.

В качестве полезной нагрузки (шелл-код) использовалась Reverse tcp. Она выполняется в результате успешного действия Java signed applet эксплойта. Это исполняемый код, который передает управление командному процессору, т.е. вызывает cmd.exe в ОС Windows.

После того как управление было передано командному процессору, т.е. получен доступ к командной строке от имени администратора, можно с легкость узнать ip-адрес пользователя.

Исследования по идентификации злоумышленника проводились для операционной системы Windows 7.

Используемые в исследовании браузеры: Google Chrome, Firefox.

Заключение

В ходе исследования трафика сети Tor были сделаны выводы, что, размещая JS-код на ресурсах сети Интернет, можно составлять базу данных уникальных фингерпринтов, чтобы отслеживать их деятельность в Интернете и соотносить с посещением различных страниц. На разработанном тестовом приложении показана реализация получения фингерпринта. Показан способ получения маркера с помощью ПО Metasploit и Social-Engineer Toolkit, предназначенных для Penetration Testing (испытания проникновением).

Из полученных результатов исследований можно сделать вывод, что использование средств эксплуатации уязвимостей не позволяет осуществлять постоянную идентификацию пользователей сети Tor, так как жизненный цикл эксплойтов очень короткий и существование разных версий браузера (содержащих конкретную уязвимость и не содержащих ее) ставит под удар очень узкий круг пользователей.

Литература

1. Гвоздев А.В. Вероятностная модель оценки информационного воздействия // Научно-технический вестник информационных технологий, механики и оптики. - 2012. - № 2. - С. 99-103.

2. Гвоздев, А.В. Метод обработки коротких сообщений открытых источников сети Интернет для системы мониторинга информационной безопасности/А.В.Гвоздев// Труды 2 межвузовской научноо-практической конференции "Актуальные проблемы организации и технологии защиты информации". - 2012. - С. 31-35.

3. Бессонова, Е.Е. Метод идентификации пользователей в сети Интернет с использованием компонентного профиля [Электронный ресурс]. – http://aspirantura.ifmo.ru/file/other/81THG1qGOW.pdf

4. Advanced Tor Browser Fingerprinting [Электронныйресурс]. – URL: http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html

5. ХАКЕР #197. Социальная инженерия [Электронный ресурс]. – URL:

https://xakep.ru/issues/xa/197 (дата обращения: 18.01.2016).