Статья Разбираемся, как устроен Hajime, известный троян для IoT

Разбираемся, как устроен Hajime, известный троян для IoT

5 октября 2016 года на одном из ханипотов, принадлежащих исследовательской группе Rapidity Networks, был обнаружен подозрительный трафик. По всем признакам выходило, что в заботливо приготовленную специалистами по информационной безопасности ловушку угодил очередной клон Mirai — как минимум симптомы заражения казались очень похожими. Однако стоило исследователям взглянуть на находку чуть пристальнее, чтобы прийти к выводу: они имеют дело с чем-то принципиально новым.

Вредонос оказался не просто трояном для работающих под управлением Linux умных устройств, а самым настоящим сетевым червем, способным объединять зараженные девайсы в ботнеты. Трой получил имя Hajime — это слово используется в японских единоборствах в качестве команды к началу поединка. Схватка между Linux.Hajime и интернетом вещей получилась увлекательной, но главное — она продолжается до сих пор.

Взлом устройства
Как и в случае Mirai, в архитектуре Hajime используется генератор случайного диапазона IP, из которого исключаются локальные и служебные адреса, после чего полученный массив данных передается сканеру. Тот последовательно стучится на 23-й TCP-порт по каждому из адресов, пробуя установить Telnet-соединение. Если попытка увенчалась успехом, Hajime начинает брутить атакуемый хост с использованием словаря, зашитого в самом трояне.

Список логинов и паролей в словаре аналогичен тому, который использует Mirai, разве что к нему добавились пары значений root/5up и Admin/5up, с помощью которых Hajime атакует ряд моделей роутеров TP-Link и Atheros с дефолтной прошивкой. Главное отличие кроется в том, что Mirai пытается авторизоваться на удаленном устройстве, перебирая логины и пароли в случайном порядке, в то время как Hajime строго следует списку, причем после каждой неудачной попытки авторизации он закрывает текущее Telnet-соединение и создает новое.

Подобно разработчикам Mirai, создатели Hajime предполагали, что пользователи умных устройств далеко не всегда меняют заводские настройки, поэтому словарь содержит набор дефолтных логинов и паролей для разных девайсов. Взлом будет

успешен только в том случае, если владелец аппарата поленился изменить предустановленные на заводе-изготовителе параметры авторизации, то есть сам себе злобный антропоморфный дендромутант.

Username	Password
root	xc3511
root	vizxv
root	klv123
root	root
guest	guest
root	admin
admin	admin
admin	password
root	Zte521
admin	<None>
guest	12345
admin	smcadmin

Словарик для брута Hajime

Если брут удался, Hajime отправляет устройству команду enable, чтобы получить доступ к привилегированному режиму интерфейса командной строки. За ней следует команда systemдля перехода в меню системных опций, а затем команды shell и sh запускают командный интерпретатор. Чтобы проверить, запустился ли нужный для его работы шелл, Hajime передает на атакуемый хост строку /bin/busybox ECCHI. Специфические оболочки не смогут обработать эту команду, в то время как стандартный sh запустит BusyBox, который вернет сообщение об ошибке в аргументе — ECCHI: applet not found. Это позволит Hajime понять, что он на верном пути.

Исследование девайса

Окончательно убедившись в том, что он попал в Linux-окружение и имеет доступ к командной строке, Hajime начинает исследовать взломанное устройство. Для начала он получает из файла /proc/mounts список смонтированных файловых систем и ищет открытые на запись папки. Обнаружив первую такую папку, отличную от /proc, /sys

или /, Hajime проверяет, действительно ли в нее разрешена запись и не хранится ли уже в ней троянский бинарник. В дальнейшем эта папка будет использоваться в качестве рабочей директории.

Затем Hajime исследует заголовок файла /bin/echo, чтобы определить тип процессора скомпрометированного устройства. В зависимости от аппаратной архитектуры на девайс будет скачан соответствующий ELF-файл, в котором реализован инфектор, доставляющий в систему полезную нагрузку. Hajime поддерживает ARMv5, ARMv7, MIPS и, конечно же, Intel x86-64.

Инфектор

Выяснив, какой процессор установлен на взломанном девайсе, Hajime отправляет командному интерпретатору директиву wget для загрузки бинарника для соответствующей архитектуры. Этот ELF-файл занимает менее 500 байт и изначально написан на ассемблере. Семплы бинарника, разработанные под различную аппаратную конфигурацию, отличаются друг от друга незначительно, в частности имеют разную структуру sockaddr размером 6 байт, в которой сохраняется IP-адрес и номер порта девайса, откуда изначально выполнялся брут скомпрометированного устройства. В этом и есть одна из особенностей Hajime: адрес для получения полезной нагрузки записан в структуре sockaddr самого инфектора, а не определяется динамически.

Инфектор устанавливает TCP-соединение с указанным хостом и принимает оттуда поток байтов. Этот поток перенаправляется на стандартный вывод stdout и по конвейеру сохраняется в файл, который будет запущен на выполнение. Так на взломанное устройство попадает основной модуль трояна.

Где-то с середины 2017 года создатели некоторых версий Hajime перестали заморачиваться с ассемблерными инфекторами и вместо этого начали качать полезную нагрузку с помощью Wget или TFTP. Процесс заражения стал проще, но при этом несколько потерял в надежности.

Основной модуль трояна

Запустившись в системе, основной модуль Hajime пытается убить все процессы, имеющие входящие и исходящие соединения с 23-м портом, для чего анализирует содержимое файлов /proc/net/tcp и /proc/net/tcp6. Затем троян модифицирует iptables, чтобы перекрыть доступ к портам 7547, 5555, 5358, и удаляет цепочку CWMP_CR, которая используется в части роутеров Movistar:
Code:

```
iptables -A INPUT -p tcp --destination-port 7547 -j DROP
iptables -A INPUT -p tcp --destination-port 5555 -j DROP
iptables -A INPUT -p tcp --destination-port 5358 -j DROP
iptables -D INPUT -j CWMP_CR
iptables -X CWMP_CR
```

После инициализации Hajime отправляет NTP-запрос к серверу pool.ntp.org, чтобы определить временную зону устройства, а также корректное значение текущей даты. Если запрос не дал результата, используется локальное время. Точное определение времени и даты очень важно для синхронизации ботнета, а некоторые умные устройства, где используются установленные по умолчанию параметры авторизации, имеют неправильную конфигурацию системного времени. Если пользователь не изменил логин и пароль, с чего бы ему менять другие настройки? Создатели Hajime учли этот тонкий момент.

Затем командой unlink трой удаляет собственный файл из системы, после чего при помощи функции strcpy меняет символьную строку argv[0], в которой хранится имя программы, на telnetd. Наконец, с использованием системного вызова prctl(PR_SET_NAME, argv[0])он меняет имя своего процесса. Таким хитрым способом Hajime пытается замаскироваться под стандартный демон Telnet, чтобы не вызывать у юзера подозрений.

Дальше управление передается модулю, который отвечает за работу DHT-протокола Kademlia, предназначенного для организации одноранговых децентрализованных файлообменных сетей. Непосредственно для приема и передачи данных ботнет использует транспортный протокол uTorrent. Это, в частности, позволяет зараженным девайсам успешно работать под NAT.

Ботнет

Маршрутизация в ботнете Hajime базируется на модифицированном проекте KadNode, который поддерживает шифрование и инфраструктуру открытых ключей (PKI). Передаваемые файлы сжимаются при помощи модифицированного алгоритма LZ4, но некоторые файлы могут транслироваться и в несжатом виде.

После инициализации протокола Hajime устанавливает соединение с пирами Torrent-ботнета и скачивает актуальный конфиг. Для опознавания пиров в сети используются уникальные идентификаторы ботов, генерируемые на основе текущей даты и хеша SHA-1, полученного от имени файла трояна. Наличие свежего конфигурационного файла на других узлах ботнета Hajime проверяет с интервалом в десять минут.

Типичный конфиг содержит обозначение процессорной архитектуры, для которой собраны исполняемые файлы, имена этих файлов и timestamp, позволяющий трою определить их версию. Если файл в сети свежее того, информация о котором

сохранена в локальном конфиге вредоноса, он скачивает бинарник для соответствующей аппаратной конфигурации и запускает его в качестве своего дочернего процесса. Аналогичным образом работает самообновление Hajime.

P2P-ботнет, созданный по такой схеме, получается одноранговым, а значит, децентрализованным и отказоустойчивым. Он не зависит от наличия управляющих серверов, следовательно, не прекращает свою деятельность, если какое-то количество инфицированных устройств вдруг «вылечится» или перестанет работать. Да и засинкхолить такой ботнет, чтобы перехватить управление, физически невозможно.

Обосновавшись в системе, Hajime запускает цикл генерации и опроса IP-адресов, чтобы продолжить заражать уязвимые сетевые устройства. При этом сам хост выступает в роли сервера, с которого скачивается исполняемый файл инфектора и тело троянца. Если для заражения какого-то удаленного хоста требуется файл с поддержкой другой аппаратной архитектуры, Hajime может подтянуть его из пиринговой сети.

Цели, задачи и выводы

В Hajime по умолчанию не предусмотрены какие-либо деструктивные функции за исключением одной: трой может скачивать и запускать на инфицированном устройстве любые приложения. Ключевое слово здесь — «любые». Поэтому для ботовода не составит никакого труда при необходимости установить на все зараженные девайсы модуль для реализации DDoS-атак, бэкдор, майнер или просто продавать инсталлы всем желающим, зарабатывая за счет других вирусописателей. Иными словами, готовый ботнет можно монетизировать множеством различных способов. Но как бы то ни было, о назначении трояна до сих пор строятся догадки и предположения.

Существует несколько методов защиты от Hajime. Можно закрыть на потенциально уязвимом устройстве порт 4636, через который трой качает полезную нагрузку. Можно блокировать все входящие соединения на порт 23, если в запросе присутствует строка /bin/busybox ECCHI— явный индикатор атаки. Но лучше всего правильно настроить параметры авторизации по протоколам Telnet и SSH, используя сложные пароли: это защитит девайс от брута по словарю, который применяют Hajime и Mirai, а владельцу такого устройства позволит сберечь нервы.

(c) Валентин Холмогоров