электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 10, октябрь 2015

УДК 004.491.22

Обзор вредоносного программного обеспечения серверов

Бучнев Я.А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Защита информации»

Вахрушев И.А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Защита информации»

Ковалев А.В., *аспирант*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Астрахов А.В., к. т. н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
zi@bmstu.ru

Linux.Snakso

В ноябре 2012 Лаборатория Касперского получила образец вируса для Linux 64-bit. Программа отличается необычным функционалом – заражение сайтов, располагавшихся на атакуемом сервере – тем самым служа частью drive-by сценария (drive-by или drive-by-download – теневая загрузка на компьютер информации при использовании специально сконфигурированных эксплойтов, багов, ссылок и скриптов).

Модуль разработан для версии ядра 2.6.32-5-amd64 [5]. Размер образца был чуть больше 500 Кбайт, так как он был скомпилирован с отладочной информацией.

Для обеспечения автозапуска вирус добавляет запись в скрипт /etc/rc.local: “insmod /lib/modules/2.6.32-5-amd64/kernel/sound/module_init.ko”

После загрузки в память, руткит пользуется одним из двух способов получения и записи символов ядра в файл “/.kallsyms_tmp”: “/bin/bash -c cat /proc/kallsyms > /.kallsyms_tmp”.

Затем он извлекает адреса памяти нескольких функций и переменных ядра и сохраняет в памяти для дальнейшего использования. Временный файл удаляется: “rm

/.kallsyms_tmp –f". Для сокрытия следов руткит перехватывает функции либо с помощью inline hooking, либо заменяя их адреса указателями на собственные функции:

- vfs_readdir;
- vfs_read;
- filldir64;
- filldir.

Кроме сокрытия собственного модуля, вирус прячет файлы:

- zzzzzz_command_http_inject_for_module_init,
- zzzzzz_write_command_in_file,
- module_init.ko,
- sysctl.conf,
- /usr/local/hide/first_hide_file/*,
- /ah34df94987sdfgDR6JH51J9a9rh191jq97811/*;

потоки

- backconnect_command_thread_name,
- new_backconnect_command_thread_name,
- read_command_http_inject_thread_name,
- write_startup_command_thread_name,
- write_se_linux_command_thread_name,
- get_http_inj_from_server_thread_name.

Механизм вставки iFrame представляет интерес: руткит заменяет системную функцию tcp_sendmsg (отвечает за составление TCP-пакетов) на собственную. Так вредоносные iFrame'ы вставляются в HTTP-трафик прямой модификацией исходящих TCP-пакетов.

Для получения актуальной полезной нагрузки руткит подключается к командному серверу используя зашифрованные аутентификационные данные.

Java.Tomdep

В ноябре 2013 года компанией по разработке программного обеспечения в области информационной безопасности и защиты информации "Symantec" был обнаружен IRC бот типа «червь», размножающийся между серверами Apache Tomcat [4]. Червь представляет собой Java сервлет (*англ.* servlet), исполняемый на серверах Apache Tomcat.

После исполнения, червь загружает на зараженный сервер файл «[TOMCAT APPLICATION ROOT]/ApacheLoader.war», и производится установка бота. После запуска

бот устанавливает соединение зараженного сервера с IRC сервером (фактически являющимся для бота C&C сервером (т.е. сервером контроля и управления)) и выполняет полученные от злоумышленника через IRC сервер команды. Бот сообщает атакующему следующую информацию о зараженной системе: операционная система, её версия, архитектура, локальный IP адрес, глобальный IP адрес, имя хоста.

Бот способен обрабатывать команды и выполнять следующие операции:

- загружать URL;
- отправлять список файлов;
- создать новый процесс;
- открывать терминал управления сервером;
- создание SOCKS-прокси;
- UDP-флудинг против определенной цели;
- самообновляться.

Бот использовался для кражи информации и проведения DDoS(Distributed Denial of Service) атак. Червь распространялся, используя произвольные IP адреса для соединения с другими Apache Tomcat серверами со слабыми паролями. Для попытки соединения использовались порты 80 и 8080, а также следующие связки логинов с паролями: «admin:admin», «tomcat:tomcat», «admin:», «tomcat:», «root:root», «manager:manager», «tomcat:admin», «admin:password». Сервера управления ботом располагались в Тайване и Люксембурге. Зараженные сервера находились в Китае, США и ряде других стран.

Effusion и Trololo_mod

В начале ноября 2013 года в компанию Яндекс поступило несколько обращений от веб-мастеров серверов Nginx [2]. Владельцы столкнулись со сложностями при удалении вирусов со своих сайтов. В ходе расследования было установлено, что исследуемый объект является ранее неизвестной вредоносной программой. Отличительной особенностью стало повреждение вирусом заголовков ELF-файлов и использование техники LD_PRELOAD.

Уязвимыми являются web-серверы Nginx начиная с версии 0.7 и до 1.4.4. Угрозе также подвержен Apache для 32- и 64-битных версий Linux и FreeBSD. Изначально вирус устанавливается злоумышленниками на взломанный сервер. Дальше вирус распространяется по сети путем отправки зараженных пакетов в ответ на запросы клиентов.

Для сокрытия присутствия вирус запускает дочерний процесс. Этот процесс отслеживает активные процессы в системе и перехватывает вводимые консольные команды. При обнаружении имен запрещенных процессов родительская программа приостанавливает свое исполнение. Присутствует функционал отслеживания деятельности пользователя «root».

Удаленное управление осуществляется с помощью пакетов, содержащих заголовок «Pragma». В заголовке передается команда управления.

Значения настроек зашифрованы и хранятся вместе в секции данных исполняемого файла вируса. В той же секции хранится ключ шифрования. После анализа было установлено, что используется алгоритм XTEA. Каждая копия вируса использует свой ключ. Настройки можно обновить с помощью HTTP-запросов. Данные в этих запросах шифруются алгоритмом XTEA в режиме электронной кодовой книги.

Effusion продавался на черном рынке с 13 ноября 2013 года. Программа была доступна только для доверенных покупателей. По словам автора покупатель получает вирус в собранном виде. Пользователю достаточно запустить установщик. Effusion не нуждается в командном сервере для своей работы. Ранее тот же разработчик создал модуль «Trololo_mod»(май 2013) для веб-серверов Apache. Оба модуля обладают единой кодовой базой. Разница заключается в среде исполнения.

Функционал Trololo_mod позволяет отслеживать сессии администратора сервера (директория /var/run/utmp) и осуществлять удаленный доступ к командной строке[3]. Для того, чтобы не заражать машины несколько раз, используются файлы cookie PHPSESSID.

Mayhem

Mayhem – многозадачная вредоносная программа, состоящая из модулей, для *nix серверов, содержащая функциональность ботнета. Mayhem был обнаружен исследователями компании Яндекс в апреле 2014 года[1]. После попадания на сервер вредоносного ELF файла создается скрытая зашифрованная файловая система, в которой хранятся дополнительно загруженные плагины Mayhem.

Исследователи группы Malware Must Die обнаружили, что в арсенал ботнета добавлено использование Shellshock эксплоитов. Это придало ботнету новые векторы атаки на серверы, включая CGI (Common Gateway Interface), OpenSSH, DHCP (Dynamic Host Configuration Protocol) и OpenVPN.

Программа попадает на сервер через известные уязвимости, которые еще не устранены на атакуемом сервере, позволяющие выполнить на сервере PHP-скрипт. В

дальнейшем производится установка ботнета через скаченную библиотеку ‘libworker.so’, содержащую собственную обертку функции ‘exit’. После инициализации ‘libworker.so’ удаляется, последний дочерний процесс переходит в основной бесконечный цикл вредоносной программы.

В первую очередь устанавливается соединение с C&C(command and control) сервером. Вредоносная программа сообщает серверу информацию о зараженном хосте (архитектура системы, её тип, права, с которыми программа исполняется в системе) и ждет команды от сервера управления.

Всего ботнет использует 7 команд. Команды делятся на три группы: от бота к серверу управления (HTTP Post запрос), от сервера управления к боту (HTTP Post ответ), и команды, используемые в любом направлении. Команды позволяют: запрашивать информацию о сервере, скачивать файлы с сервера, отправлять на сервер новые файлы (плагины), получать информацию о состоянии ботнета, запускать новые задачи, производить настройку конфигурации, останавливать процессы.

Ботнет использует скрытую файловую систему FAT 16/32 с модифицированными функциями, поддерживающими шифрование. Файловая система содержит расширения вредоносной программы (плагины) и файлы со списками URL, именами пользователей, паролями, а также конфигурационные файлы. Файловая система хранится на сервере в зашифрованном виде, для шифрования используется алгоритм XTEA с 32 циклами в режиме электронной кодовой книги.

Было обнаружено 8 расширений, хранящихся на зашифрованной, скрытой файловой системе. Исследователи Яндекс и команды Malware Must Die обнаружили 3 C&C сервера. Управление ботнетом осуществляется через панель администратора. Наибольшая часть серверов, зараженных Mayhem находится в США, России, Германии и Канаде. Mayhem заразил около 1400 серверов.

Заключение

Веб-серверы представляют особый интерес для злоумышленников. Круглосуточная работа, взаимодействие с большим количеством клиентов наряду с необходимость вручную устанавливать обновления ПО делают их особенно уязвимыми для заражения. За последние годы угрозы для серверов прошли путь от вредоносных модулей до многоцелевой атакующей платформы. Применение схожих техник облегчает обнаружение исследуемой категории вирусов, но вирусописатели всегда на шаг впереди.

Список литературы

1. Kovalev A., Otrashkevich K., Sidorov E. Mayhem – a hidden threat for *nix web servers. Available at: https://www.virusbtn.com/virusbulletin/archive/2014/07/vb201407, available at 24.03.2015.
2. Kovalev A., Otrashkevich K., Sidorov E., Rassokhin A.: Effusion – a new sophisticated injector for Nginx web servers. Available at: https://www.virusbtn.com/virusbulletin/archive/2014/01/vb201401, available at 24.03.2015.
3. Sidorov E., Rassokhin A. Embedding malware on websites using executable webserver files. Available at: https://www.virusbtn.com/pdf/conference_slides/2013/RassokhinSidorov-VB2013.pdf, available at 24.03.2015.
4. Katsuki T. All Your Tomcat Are Belong to Bad Guys. Available at: http://www.symantec.com/connect/blogs/all-your-tomcat-are-belong-bad-guys, available at 24.03.2015.
5. Janus M. New 64-bit Linux Rootkit Doing iFrame Injections. Available at: http://securelist.com/blog/incidents/34623/new-64-bit-linux-rootkit-doing-iframe-injections-30, available at 24.03.2015.