Win32.Ntldrbot (aka Rustock.C) – не миф, а реальность!

Ищут пожарные, ищет милиция,
Ищут фотографы в нашей столице,
Ищут давно, но не могут найти
Парня какого-то лет двадцати.

С.Михалков

Rootkit (руткит, от англ. root – «корень» и kit – «набор») — программа или набор программ, позволяющие компьютерному злоумышленнику закрепиться во взломанной системе и скрыть следы своей деятельности путём сокрытия файлов, процессов, а также самого факта присутствия.

По материалам Wikipedia

Предисловие

В последнее время, одним из основных направлений развития вредносных программ стало применение в них всевозможных способов защиты от обнаружения антивирусными средствами. Руткиты становятся все более изощренные, их количество растет с каждым годом. Большинство из них – это чужие идеи, воплощенные не лучшим образом в коде, однако, есть и крайне интересные экземпляры. Об одном таком мифическом и неопределяемом до недавнего времени рутките эта статья.

Ботнеты

Для того чтобы понять, о чем пойдет речь дальше, необходимо ознакомиться с некоторыми терминами, один из них – ботнет. По данным все той же Wikipedia, ботнет или бот-сеть (англ. botnet) — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета скрытно устанавливается на компьютере жертвы и позволяет злоумышленнику выполнять некие действия, эксплуатируя ПО и ресурсы заражённого компьютера. Как правило, ботнеты используются для нелегальной или несанкционированной деятельности — рассылки спама, перебора паролей в удалённой системе, атак на отказ в обслуживании и многого другого.

Компания SecureWorks провела исследование наиболее крупных бот-сетей, занимающихся рассылкой спама. Нас же интересует только один из них, а именно Rustock, который занимает третье место в этом своеобразном рейтинге. Краткая информация по ботнету выглядит так:

- предполагаемое количество зараженных машин: порядка 150, 000;
- способность ботнета рассылать спам: порядка 30 миллиардов сообщений в день;
- наличие руткит-составляющей: да.

Теперь вы представляете с чем мы имеем дело и каков размах подобных сетей в Интернет.

Взросление Rustock

Название Rustock придумали специалисты антивирусной компании Symantec, и оно так понравилось автору вредоносного кода, что в дальнейшем он стал его использовать. Изначально в первых версиях руткита можно было встретить такую строку: «Z:\NewProjects\spambot\last\driver\objfre\i386\driver.pdb». В последующих кроме строки с использованием «spambot» появилась строка «Rustock rootkit v 1.2».

Принято считать и делить поколения данного руткита на три «возрастные группы» (A, B, C). Это не совсем верно, так как автор постоянно экспериментировал и изменял код, методы перехвата функций и улучшал стабильность, но в целом кардинальных изменений за одну версию не вносил. На самом деле ситуацию с «версионностью» руткита достаточно просто отследить.

В конце 2005 – начале 2006 года появились первые бета-версии Rustock.A на которых обкатывались технологии. Отличить их можно по названиям драйверов: i386.sys, sysbus32. Для скрытия себя в системе использовался перехват системной таблицы вызовов (SSDT) и перехват IRP-пакетов.

Далее появилась полноценная версия Rustock.A – pe386.sys (версия 1.0), которая отличалась от первых версий техниками скрытия себя в системе. Прежде всего, автор отказался от SSDT и перехватил прерывание 0x2E (Windows 2000) и MSR_SYSENTER(Windows XP+). Для скрытия файла на диске были использованы ADS (Alternate Data Stream). Данная технология поддерживается на файловой системе NTFS. Тело руткита находилось в %SystemRoot%\system32:[случайный_набор_цифр].

В том же 2006 году появилась бета-версия Rustock.B (huy32.sys), а сразу за ней полноценная версия Rustock.B - lzx32.sys (версия 1.2), в которой использовались перехваты INT2E/MSR_SYSENTER, ADS (%Windir%\System32:lzx32.sys). Кроме всего прочего, автор добавил перехват функций сетевых драйверов: tcpip.sys, wanarp.sys и ndis.sys, который позволял ему обходить фаерволы и прятать спам-трафик.

Также были выпущены варианты с урезанным функционалом, варианты, которые восстанавливали перехваты в случае их обнаружения и снятия антируткитами или антивирусами, а также различные варианты со случайными именами драйверов.

Некоторые антивирусные вендоры, например TrendMicro, выложили в своих вирусных библиотеках описание Rustock.C, но после проверки этот экземпляр оказался очередной экспериментальной версией Rustock.B

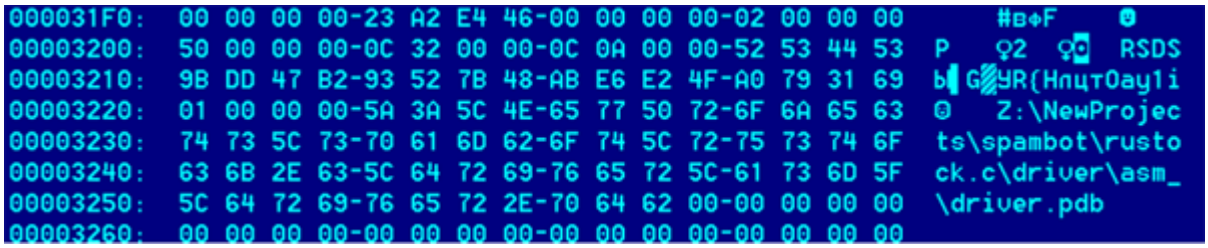
Rustock.C

Первые слухи о Rustock.C появились летом 2006 года. Тогда же его начали искать как антивирусные лаборатории, так и вирусописатели. Антивирусные лаборатории искали для того, чтобы проанализировать и улучшить свои методы обнаружения руткитов, а вирусописатели просто для того, чтобы наворовать чужих идей и встроить в свои вредоносные программы защиту и методы сокрытия «попрактичнее».

Шло время, а образец то ли не находился, то ли времени на его анализ у антивирусных лабораторий не хватало, ведь ежедневно приходится иметь дело с тысячами файлов. Официальных подтверждений или опровержений так и не появилось,

были лишь какие-то разговоры на различных форумах. Многие вендоры предпочли «откреститься» от C-варианта и заняли позицию: «Ну, раз мы его не видим/не нашли, значит он не существует. Это миф!», или: «Давайте еще вспомним “Rustock.C”, который где-то живет, а его никто не видит и видеть не может».

Но оказалось, что Rustock.C не миф. Не все антивирусные лаборатории бросили его поиск, и он дал результаты.



Как видно на изображении автор окончательно принял предложенное название Rustock. Прошло всего полтора года, и Rustock.C был найден в начале 2008 года. Все это время он работал, рассылал спам.

Службой вирусного мониторинга компании «Доктор Веб» было обнаружено порядка 600 экземпляров данного руткита, сколько их существует на самом деле неизвестно. Дата сборки большинства – сентябрь или октябрь 2007 года. На распаковку, детальный анализ и улучшение методов детектирования подобных экземпляров вирусные аналитики «Доктор Веб» потратили несколько недель.

Даже если предположить, что руткит работает с октября 2007 года совершенно невидимо для антивирусов, можно сделать выводы о громадном количестве паразитного трафика который он разослал. Спам превратился в серьезную общемировую проблему, с которой приходится бороться каждый день. Пользователи жалуются на утечку трафика, их личные почтовые ящики переполнены совершенно ненужной и раздражающей информацией. Теряется время, тратятся деньги, расходуются нервы. То, что у Rustock.C было столько времени действовать безнаказанно, не рискуя быть пойманным антивирусом, означает, что никто не даст гарантии, что и ваша машина не является частью одной из бот-сетей и не рассылает спам прямо сейчас.

Некоторые технические характеристики руткита

- имеет мощный полиморфный протектор, затрудняющий анализ и распаковку руткита;
- реализован в виде драйвера уровня ядра, работает на самом низком уровне;
- имеет функцию самозащиты, противодействует модификации времени исполнения;
- активно противодействует отладке: контролирует установку аппаратных точек останова (DR-регистры); нарушает работу отладчиков уровня ядра: Syser, SoftIce. Отладчик WinDbg при активном рутките не работает вообще;
- перехватывает системные функции неклассическим методом. Такие функции как:
  - NtCreateThread
  - NtDelayExecution

  - NtDuplicateObject
  - NtOpenThread
  - NtProtectVirtualMemory
  - NtQuerySystemInformation
  - NtReadVirtualMemory
  - NtResumeThread
  - NtTerminateProcess
  - NtTerminateThread
  - NtWriteVirtualMemory
- работает как файловый вирус, заражая системные драйверы;
- конкретный экземпляр руткита привязывается к оборудованию зараженного компьютера. Таким образом, на другом компьютере руткит с большой вероятностью работать не будет;
- имеет функцию «перезаражения», срабатывающую по времени. Старый зараженный файл при «перезаражении» излечивается. Таким образом, руткит «путешествует» по системным драйверам, оставляя зараженным какой-нибудь один.
- фильтрует обращения к зараженному файлу, перехватывая FSD-процедуры драйвера файловой системы и подставляет оригинальный файл вместо зараженного;
- имеет защиту от антируткитов;
- имеет в составе библиотеку, внедряемую в один из системных процессов ОС Windows. Данная библиотека занимается рассылкой спама. Для связи драйвера с DLL используется специальный механизм передачи команд.

Выводы

Сразу после обнаружения этого руткита вирусописателями следует ожидать всплеск подобных технологий и внедрение их во вредоносные программы.

На текущий момент, кроме антивируса Dr.Web, ни один современный антивирус не детектирует Rustock.C. Также ни один антивирус, кроме антивируса Dr.Web, не лечит зараженные им системные файлы. Тем, кто не является пользователем Антивирус Dr.Web, рекомендуется скачать бесплатную лечащую утилиту Dr.Web CureIt! и произвести проверку компьютера.

Закончить статью хотелось бы фразой, которая стала популярной в 90-х годах. Сегодня она посвящается автору Rustock: *«Все что может быть запущено, может быть сломано»*.

Вирусный аналитик

Русаков Вячеслав Евгеньевич

Компания «Доктор Веб»

Dr.WEB®
АНТИВИРУС

О компании «Доктор Веб»

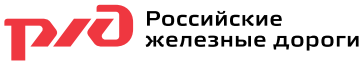
«Доктор Веб» — российский разработчик средств информационной безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности. Сертификаты и награды, а также обширная география пользователей Dr.Web свидетельствуют о высокой степени доверия к продуктам компании.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственной уникальной технологией детектирования и лечения вредоносных программ; имеет собственную службу вирусного мониторинга и аналитическую лабораторию. Это обуславливает высокую скорость реакции специалистов компании на новые вирусные угрозы, способность оказать помощь клиентам в решении проблем любой сложности в считанные часы.

Опыт крупных проектов

Среди клиентов «Доктор Веб» — крупные компании с мировым именем, российские и международные банки, государственные организации, учебные заведения и научно-исследовательские институты, сети которых насчитывают десятки тысяч компьютеров. Антивирусным решениям «Доктор Веб» доверяют высшие органы государственной и исполнительной власти России, компании топливно-энергетического сектора.





125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97
www.drweb.com
www.freedrweb.com