Руководство малвари для начинающих. Инструменты скрытия вредоносной активности

Ред Канари, Malwarebytes · Стивенсон, Ксионг · Дмитрий Сомерфилд

Содержание статьи

- Малвари есть, но никто ничего не видит
- RootKit: невидимый вредонос
- Hooking
- Методы для внедрения кода в процессы
  - Внедрение в процесс через DLL
  - Использование Windows API для внедрения кода в процесс
  - Внедрение через реестр
  - Внедрение через файлы конфигурации
  - Внедрение через сервисы
  - Внедрение в процесс с использованием shim-ов
- Методы для перехвата вызовов API
  - Hooking в User Mode
  - Hooking в Kernel Mode
  - Hooking в Windows Kernel x64
  - Hooking в Windows Kernel x64 с использованием Patchguard
  - Hooking в Windows Kernel x64 с использованием Patchguard и Hypervisor
  - Hooking в Windows Kernel x64 с использованием Patchguard, Hypervisor и Secure Boot
- Методы для скрытия вредоносного ПО
  - Скрытие файлов
  - Скрытие ключей реестра
  - Скрытие процессов
  - Скрытие сетевых соединений
  - Скрытие при помощи Windows Kernel Callbacks
  - Скрытие при помощи Windows Kernel Callbacks и Patchguard
  - Скрытие при помощи Windows Kernel Callbacks и Patchguard и Hypervisor
  - Скрытие при помощи Windows Kernel Callbacks и Patchguard и Hypervisor и Secure Boot
- Заключение
- Ссылки

Привет, мир! Если вы впервые читаете эти замечательные статьи «Руководство малвари ведущих» и не знаете практически ни одного слова, то для обсуждения сегодняшнего материала вам необходимо знать, что такое малвари, как с ней обращаются, как она выполняется и, в конечном счете, как ее обнаружить. Если вы уже прочитали предыдущие статьи, то вы уже знаете, что такое малвари, как ее обнаружить и как ее обезвредить. Сегодня мы также поговорим о малвари, но на этот раз мы остановимся на некоторых очень сложных методах, которые используются для скрытия вредоносной активности. Мы также обсудим, как малвари может использовать эти методы для скрытия своей деятельности, а также как специалисты по информационной безопасности могут обнаружить такие методы. Сегодня мы также поговорим о некоторых очень сложных методах, которые Windows использует для внедрения кода в процессы, а также как специалисты по информационной безопасности могут использовать эти методы для обнаружения вредоносной активности.

В этом материале мы разберем три различных технологии скрытия вредоносной активности в Windows: RootKit, Hooking и Code Injection. Мы также обсудим, как специалисты по информационной безопасности могут обнаружить вредоносную активность, использующую эти технологии.

Все вредоносные программы выполняются в операционных системах. Это вредоносное ПО может быть вирусом, червем, троянским конем, шпионским ПО, рекламным ПО, ботом, или чем-то еще. Но, в конечном счете, вредоносное ПО — это просто программа. Чтобы вредоносное ПО выполнялось, оно должно быть запущено.

Malware hosts, или искусственное окружение

В операционных системах все выполняемые коды являются нитями — и нитью частным случаем процесса, а процессы, в свою очередь, являются частным случаем задачи. Задачи — это контейнеры, которые обеспечивают изоляцию, обеспечивают контроль, контролируют доступ к ресурсам. Все выполняемые нити принадлежат задачам. Задачи могут быть изолированными, а могут и не быть изолированными. Задачи могут иметь доступ к ресурсам, а могут и не иметь доступ к ресурсам. Задачи могут быть привилегированными, а могут и не быть привилегированными. Задачи могут быть 32-разрядными, а могут и 64-разрядными. Задачи могут быть 32-разрядными, а могут и 64-разрядными. Задачи могут быть 32-разрядными, а могут и 64-разряд

В ночь перед 30 сентября — между Вторым Иском (вторым кусочком трояна) и Третьим Иском (третьим кусочком трояна) — в сети появился новый кусочек трояна. Его назвали Четвертым Иском.

Сегодня мы разобрали его.

WARNING

Data on this website was collected from public sources. Malware malware no warranty. Do not re-upload any malware! Hosting is strongly against malware! Do not contact us about malware! Do not ask us for malware! Do not ask us for passwords, accounts or keys! Do not ask us for hacks!

Analysis created by malwarebytes@0x5a

Анализ сэмпла malware0f5

Инструменты:

- IDA Pro
- Wireshark
- Microsoft Visual Studio Express 2010
- Windows SDK

Первым делом мы скачали PE-файлик с сервера через wget. Итак, файл получен. Он называется 1.exe. Запускаем его. Ничего не происходит. Ну, ладно, видимо, Control Panel — вещь капризная. Что-нибудь запускать мы пока не обязаны. Запускаем Process Monitor — и видим, что 1.exe пытается прицепиться к Internet Explorer. Ну, ладно, видимо, Control Panel — капризная вещь. Ждем. Ждем. Ждем. Ничего не происходит. Ладно, видимо, 1.exe — не Control Panel. Ждем. Ждем. Ждем. Ничего не происходит. Ладно, видимо, 1.exe — не Control Panel. Ждем. Ждем. Ждем. Ничего не происходит.

Открываем сэмпл в старом добром IDA Pro и запускаем trace manager.

Сегодня Control Panel капризничает. Ждем. Ждем. Ждем. Ничего не происходит. Ладно, видимо, это не Control Panel