Уклонение от средств защиты: 3 Часть. – Telegraph

telegra.ph/Uklonenie-ot-sredstv-zashchity-3-CHast-07-16

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 16, 2024

Сегодня рассмотрим еще несколько способов уклонения от антивирусного ПО.

Статический анализ

Статический анализ — это процесс анализа двоичного файла вредоносного ПО без фактического выполнения кода. Статический анализ обычно выполняется путем определения контрольной суммы двоичного файла, которая является уникальной идентификацией, а также извлечения информации из самого файла (например, описания файла, названия компании, цифровых подписей, строк, названий функций и т.д.). Это означает, что при использовании известных шанс быть пойманым AV значительно увеличивается. Существует несколько способов обойти такого рода обнаружение:

Хеширование

Хеширование - это метод, который преобразует кусок данных в фиксированное представление, называемое хеш-значением или хеш-кодом. Хеш-алгоритмы разработаны таким образом, что невозможно обратно получить исходные данные из хеш-значения. Хеш-код обычно имеет более короткий формат и обрабатывается быстрее. При сравнении строк хеширование может быть использовано для быстрого определения их равенства вместо сравнения самих строк, особенно если строки длинные.

В контексте разработки вредоносных программ хеширование строк полезно для скрытия строк, так как строки могут использоваться как сигнатуры для обнаружения вредоносных бинарных файлов.

Encryption (Шифрование)

Если вы зашифруете двоичный файл, у AV не будет возможности обнаружить вашу программу, но вам понадобится какой-нибудь загрузчик для расшифровки и запуска программы в памяти.

Obfuscation (Обфускация)

Иногда все, что вам нужно сделать, это изменить некоторые строки в вашем двоичном коде или скрипте, чтобы пропустить AV, но это может занять много времени, в зависимости от того, что вы пытаетесь запутать.

Ссылки на полезные ресурсы и инструменты для самостоятельного изучения:

1) https://cocomelonc.github.io/

2) https://github.com/NUL0x4C/FetchPayloadFromDummyFile

3) https://github.com/BC-SECURITY/Beginners-Guide-to-Obfuscation

4) https://www.youtube.com/watch?v=lP2KF7_Kwxk

5) https://www.youtube.com/watch?v=wvKwk1wcXvM

6) https://github.com/KDot227/SomalifuscatorV2

7) https://github.com/JoelGMSec/Invoke-Stealth

8) https://github.com/dashingsoft/pyarmor

9) https://github.com/tokyoneon/Chimera

10) https://github.com/Bashfuscator/Bashfuscator

11) https://github.com/guillaC/BatchObfuscator

12) https://github.com/naksyn/DojoLoader

13) https://github.com/Maldev-Academy/MaldevAcademyLdr.1

14) https://github.com/NUL0x4C/AtomLdr

15) https://github.com/D1rkMtr/ObfLoader

16) https://github.com/optiv/Freeze

17) https://github.com/Cracked5pider/KaynLdr

18) https://github.com/chvancooten/NimPackt-v1

19) https://github.com/boku7/BokuLoader

20) https://redteamrecipe.com/malware-development-evading-diaries