

УДК 004.056
ББК 32.973.202
М33

М33 Алекс Матросов, Евгений Родионов, Сергей Братусь
Руткиты и буткиты. Обратная разработка вредоносных программ и угрозы следующего поколения / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2022. – 442 с.: ил.

ISBN 978-5-97060-979-8

Эта книга посвящена обнаружению, анализу и обратной разработке вредоносного ПО. В первой части описываются примеры руткитов, показывающие, как атакующий видит операционную систему изнутри и находит способы надежно внедрить свои импланты, используя собственные структуры ОС. Вторая часть рассказывает об эволюции буткитов, условиях, подхлестнувших эту эволюцию, и методах обратной разработки таких угроз.

Издание адресовано широкому кругу специалистов по информационной безопасности, интересующихся тем, как современные вредоносные программы обходят защитные механизмы на уровне операционной системы.

УДК 004.056
ББК 32.973.202

Copyright © 2019 by Alex Matrosov, Eugene Rodionov, and Sergey Bratus. Title of English-language original: Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats, ISBN 9781593277161, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2022 by DMK Press Publishing under license by No Starch Press Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-59327-716-1 (англ.)

ISBN 978-5-97060-979-8 (рус.)

Copyright © 2019 by Alex Matrosov, Eugene Rodionov, and Sergey Bratus

© Перевод, оформление, издание, ДМК Пресс, 2022

СОДЕРЖАНИЕ

От издательства	13
Об авторах.....	14
О техническом рецензенте.....	14
Вступительное слово	15
Благодарности.....	17
Список аббревиатур	18
Введение	22
Для кого предназначена эта книга	23
Структура книги	23
Как читать эту книгу.....	26
Часть I. Руткиты.....	27
Глава 1. Что такое руткит: TDL3	28
История распространения TDL3 по миру.....	29
Процедура заражения	30
Управление потоком данных	32
Скрытая файловая система	36
Итог: TDL3 встретил свою Немезиду.....	37
Глава 2. Руткит Festi: самый продвинутый бот для спама и DDoS-атак	39
Дело о сети ботов Festi	40
Устройство драйвера руткита.....	41
Конфигурационная информация Festi для взаимодействия с командно-управляющим сервером.....	42
Объектно-ориентированная структура Festi	43
Управление плагинами.....	44
Встроенные плагины	45
Методы противодействия виртуальной машине.....	47
Методы противодействия отладке.....	48
Метод сокрытия вредоносного драйвера на диске.....	49
Метод защиты раздела реестра Festi	51
Сетевой протокол Festi	52
Фаза инициализации	52
Рабочая фаза.....	53
Обход средств обеспечения безопасности и КТЭ.....	54
Алгоритм генерирования доменных имен в случае отказа C&C-сервера.....	57
Вредоносная деятельность.....	57
Модуль рассылки спама.....	58
Проведение DDoS-атак	58
Плагин прокси-сервиса	60
Заключение.....	61

Глава 3. Обнаружение заражения руткитом	62
Методы перехвата	63
Перехват системных событий	63
Перехват системных вызовов	65
Перехват операций с файлами	67
Перехват диспетчера объектов	68
Восстановление ядра системы	71
Великая гонка вооружений с руткитами: ностальгическая нотка	72
Заключение	74
Часть II. Буткиты	75
Глава 4. Эволюция буткита	76
Первые буткиты	76
Инфекторы загрузочного сектора	77
Эволюция буткитов	78
Закат эры BSI	78
Политика подписания кода режима ядра	79
Взлет безопасной загрузки	80
Современные буткиты	80
Заключение	83
Глава 5. Основы процесса загрузки операционной системы	84
Общий обзор процесса загрузки Windows	85
Старый процесс загрузки	86
Процесс загрузки Windows	87
BIOS и предзагрузочное окружение	87
Главная загрузочная запись	88
Загрузочная запись тома и начальный загрузчик программы	90
Модуль bootmgr и конфигурационные данные загрузки	91
Заключение	96
Глава 6. Безопасность процесса загрузки	97
Модуль раннего запуска антивредоносной программы	97
API обратных вызовов	98
Как буткиты обходят ELAM	100
Политика подписания кода режима ядра	101
Драйверы, подлежащие проверке целостности	101
Где находятся подписи драйвера	102
Слабость проверки целостности унаследованного кода	103
Модуль ci.dll	104
Дополнительные защитные меры в Windows 8	106
Технология безопасной загрузки	107
Безопасность на основе виртуализации в Windows 10	108
Трансляция адресов второго уровня	109
Виртуальный безопасный режим и Device Guard	109
Ограничения, налагаемые Device Guard на разработку драйверов	110
Заключение	111
Глава 7. Методы заражения буткитом	112
Методы заражения MBR	112

Модификация кода в MBR: метод заражения TDL4.....	113
Модификация таблицы разделов в MBR	120
Методы заражения VBR/IPL.....	120
Модификации IPL: Rovnix	121
Заражение VBR: Gapz	122
Заключение.....	122
Глава 8. Статический анализ буткита с помощью IDA Pro	124
Анализ MBR буткита.....	125
Загрузка и дешифрирование MBR	125
Анализ службы дисков BIOS.....	129
Анализ зараженной таблицы разделов MBR.....	134
Техника анализа VBR.....	135
Анализ IPL	136
Оценка других компонентов буткита.....	136
Продвинутая работа с IDA Pro: написание собственного загрузчика MBR.....	138
Файл loader.hpp	138
Реализация accept_file.....	139
Реализация load_file	140
Создание структуры, описывающей таблицу разделов	141
Заклучение.....	142
Упражнения	143
Глава 9. Динамический анализ буткита: эмуляция и виртуализация	145
Эмуляция с помощью Bochs	146
Установка Bochs.....	147
Создание окружения Bochs	147
Заражение образа диска	150
Использование внутреннего отладчика Bochs.....	152
Комбинация Bochs с IDA.....	153
Виртуализация с помощью VMware Workstation.....	155
Конфигурирование VMware Workstation	156
Комбинация VMware GDB с IDA	157
Microsoft Hyper-V и Oracle VirtualBox	160
Заклучение.....	161
Упражнения	161
Глава 10. Эволюция методов заражения MBR и VBR: Olmasco	163
Сбрасыватель.....	164
Ресурсы сбрасывателя.....	164
Средства трассировки для будущих разработок.....	166
Средства противодействия отладке и эмуляции	167
Функциональность буткита	169
Метод заражения.....	169
Процесс загрузки зараженной системы	170
Функциональность руткита.....	171
Подключение к объекту устройства диска и внедрение полезной нагрузки.....	172
Обслуживание скрытой файловой системы.....	172
Реализация интерфейса транспортного драйвера для перенаправления сетевого трафика	175
Заклучение.....	176

Глава 11. Буткиты начального загрузчика программы:

Rovnix and Carberp	177
Эволюция Rovnix	178
Архитектура буткита	179
Заражение системы	180
Процесс загрузки после заражения и IPL	182
Реализация полиморфного дешифровщика	182
Дешифрирование начального загрузчика Rovnix с помощью VMware и IDA Pro	184
Перехват управления путем изменения начального загрузчика Windows	190
Загрузка вредоносного драйвера	193
Функциональность вредоносного драйвера	194
Внедрение модуля полезной нагрузки	194
Механизмы скрытности и самозащиты	196
Скрытая файловая система	198
Форматирование раздела под файловую систему Virtual FAT	198
Шифрование скрытой файловой системы	198
Доступ к скрытой файловой системе	199
Скрытый канал связи	200
Реальный пример: троян Carberp	202
Разработка Carberp	202
Усовершенствования сбрасывателя	204
Утечка исходного кода	205
Заключение	205

Глава 12. Garpz: продвинутое заражение VBR

Сбрасыватель Garpz	208
Алгоритм сбрасывателя	210
Анализ сбрасывателя	211
Обход NIPS	212
Заражение системы буткитом Garpz	216
О блоке параметров BIOS	217
Заражение VBR	218
Загрузка вредоносного драйвера	220
Функциональность буткита Garpz	221
Скрытое хранилище	224
Самозащита от антивредоносных программ	225
Внедрение полезной нагрузки	227
Интерфейс взаимодействия с полезной нагрузкой	232
Собственный стек сетевых протоколов	235
Заклучение	238

Глава 13. Взлет программ-вымогателей, заражающих MBR

Краткая история современных программ-вымогателей	240
Вымогатель с функциональностью буткита	241
Образ действий программ-вымогателей	242
Анализ вымогателя Petya	244
Получение привилегий администратора	244
Заражение жесткого диска (этап 1)	245
Шифрование с помощью конфигурационных данных вредоносного начального загрузчика	248

Обрушение системы	252
Шифрование MFT (этап 2)	253
Подводя итоги: заключительные мысли о Petya	258
Анализ вымогателя Satana	258
Сбрасыватель Satana	259
Заражение MBR	259
Отладочная информация сбрасывателя	260
Вредоносная MBR вымогателя Satana	261
Подводя итоги: заключительные мысли о Satana	264
Заключение	264
 Глава 14. Сравнение процессов загрузки с помощью UEFI и MBR/VBR	266
Единый расширяемый интерфейс прошивки	267
Различия между процессами загрузки через BIOS и UEFI	268
Последовательность загрузки	268
Разбиение диска на разделы: MBR и GPT	269
Прочие отличия	270
Особенности таблицы разделов GUID	271
Как работает прошивка UEFI	275
Спецификация UEFI	276
Внутри загрузчика операционной системы	278
Начальный загрузчик Windows	284
Преимущества прошивки UEFI с точки зрения безопасности	287
Заключение	288
 Глава 15. Современные UEFI-буткиты	289
Исторический обзор угроз BIOS	290
WinCIH, или первый вредонос, нацеленный на BIOS	290
Mebromi	291
Краткий обзор других угроз и контрмер	292
У любого оборудования есть прошивка	296
Уязвимости прошивки UEFI	297
Неэффективность битов защиты памяти	298
Проверки битов защиты	299
Способы заражения BIOS	300
Модификация дополнительного ПЗУ неподписанной UEFI	302
Добавление или модификация DXE-драйвера	304
Как происходит внедрение руткита	305
UEFI-руткиты на воле	311
Руткит Vector-EDK от группы Hacking Team	312
Заключение	320
 Глава 16. Уязвимости прошивок UEFI	321
Почему прошивка может быть уязвимой?	322
Классификация уязвимостей UEFI	325
Постэксплуатационные уязвимости	327
Скомпрометированная цепочка поставок	327
Борьба с уязвимостью цепочки поставок	329
Исторический обзор защиты прошивок UEFI	329
Как работает защита BIOS	330

Защита флеш-памяти SPI и ее уязвимости	331
Риски неаутентифицированного обновления BIOS	334
Защита BIOS с помощью технологии безопасной загрузки.....	335
Intel Boot Guard	336
Технология Intel Boot Guard	336
Уязвимости Boot Guard	337
Уязвимости в модулях SMM.....	339
Что такое SMM	339
Эксплуатация обработчиков SMI	340
Уязвимости в загрузочном скрипте S3	344
Что делает скрипт S3.....	344
Атаки на слабости загрузочного скрипта S3	345
Эксплуатация уязвимости в загрузочном скрипте S3	346
Исправление уязвимости в загрузочном скрипте S3	349
Уязвимости в Intel Management Engine	349
История уязвимостей ME	349
Атаки на код ME	350
Пример: атаки на Intel AMT и BMC.....	351
Заключение	354
Часть III. Методы защиты и компьютерно-технической экспертизы	355
Глава 17. Как работает безопасная загрузка UEFI	356
Что такое безопасная загрузка?	357
Детали реализации безопасной загрузки UEFI.....	358
Последовательность загрузки	358
Аутентификация исполняемого файла с помощью цифровых подписей	359
База данных db	361
База данных dbx	364
Аутентификация с учетом времени.....	366
Ключи безопасной загрузки	366
Безопасная загрузка UEFI: полная картина.....	369
Политика безопасной загрузки.....	370
Защита от буткитов с помощью безопасной загрузки	372
Атаки на безопасную загрузку	374
Изменение прошивки PI с целью отключения безопасной загрузки	374
Модификация переменных UEFI для обхода проверок безопасности	375
Защита безопасной загрузки с помощью технологии	
верифицированной и измеренной загрузки.....	377
Верифицированная загрузка.....	378
Измеренная загрузка	378
Intel BootGuard	378
Где искать ACM	379
Изучение FIT.....	382
Конфигурирование Intel BootGuard	382
Trusted Boot Board в ARM.....	385
ARM Trust Zone	385
Начальные загрузчики в ARM	386
Поток выполнения в Trusted Boot	388
Верифицированная загрузка и руткиты прошивки	389
Заклучение	390

Глава 18. Подходы к анализу скрытых файловых систем	391
Обзор скрытых файловых систем	392
Извлечение данных буткита из скрытой файловой системы	393
Извлечение данных из незапущенной системы	393
Чтение данных из активной системы	394
Подключение к драйверу мини-порта устройства хранения	394
Разбор образа скрытой файловой системы	400
Программа HiddenFsReader	401
Заключение	402
Глава 19. Компьютерно-техническая экспертиза BIOS/UEFI:	
подходы к получению и анализу прошивок	403
Ограничения наших методов КТЭ	404
Почему компьютерно-техническая экспертиза прошивки так важна	404
Атака на цепочку поставок	405
Компрометация BIOS через уязвимость прошивки	405
Как получить прошивку	405
Программный подход к получению прошивки	407
Местоположение регистров из конфигурационного пространства PCI	408
Вычисление адресов регистров конфигурации SPI	409
Использование регистров SPI	409
Чтение данных из флеш-памяти SPI	412
О недостатках программного подхода	413
Аппаратный подход к получению прошивки	414
Описание процедуры на примере Lenovo ThinkPad T540p	415
Местоположение микросхемы флеш-памяти SPI	416
Чтение флеш-памяти SPI с помощью мини-модуля FT2232	418
Анализ образа прошивки с помощью UEFITool	420
Какие существуют регионы флеш-памяти SPI	421
Просмотр регионов флеш-памяти SPI с помощью UEFITool	421
Анализ региона BIOS	423
Анализ образа прошивки с помощью Chipsec	427
Знакомство с архитектурой Chipsec	427
Анализ прошивки с помощью Chipsec Util	429
Заключение	431
Предметный указатель	432