Реверсинг малварей для начинающих. Введение: выбираем инструменты, репозитории и источники знаний

Кирилл «kelvin» Соколов | 2 сентября, 08:00 | 1 | 2 комментариев | 47 мин | 1 добавление

Содержание статьи

0. Реверсинг как искусство
1. Готовим домашнюю лабораторию
1.1. Виртуальная машина для малвари
1.2. Основные инструменты для исследования
1.3. Основные инструменты для реверсинга
1.4. Репозитории и источники знаний
2. Реверсинг инструментов динамического анализа
2.1. Process Monitor
2.2. Process Explorer
2.3. Regshot
2.4. Wireshark
2.5. Apimonitor
2.6. Winmon
2.7. Inetsim
3. Реверсинг инструментов статического анализа
3.1. Hex Editor Neo
3.2. Resource Hacker
3.3. Dependency Walker
3.4. Strings
3.5. Binwalk
4. Специализированные инструменты для продвинутого анализа
4.1. Procmon
4.2. Process Hacker
4.3. Ollydbg
4.4. Ida Free
4.5. Radare2
5. Рекомендуемые к изучению ресурсы
5.1. Malware Unicorn
5.2. Reverse Engineering Stack Exchange
5.3. Malware Analysis and Reverse Engineering
5.4. Malware Analysis and Reverse Engineering
6. Практикуем

Представляем первую статью цикла «Реверсинг малвари для начинающих». Сегодня мы выберем инструменты, репозитории и источники знаний, которые пригодятся нам в грядущих материалах. В первой статье мы основательно разберем инструменты, которые нам понадобятся для статического и динамического анализа, а также обзор наиболее интересных и полезных репозиториев и источников знаний.

Все материалы серии помечены соответствующим и индивидуальным цветом. Все материалы, не относящиеся к малвари, помечены серым. Материалы, посвященные реверсингу, помечены синим.

Реверсинг как искусство

Исторически реверсинг развивался как ответ на попытки ПО и вирусов к обеспечению своей безопасности. Вирусы, трояны, ботнеты, шифровальщики, шпионы, рекламное ПО, ПО для цифровых платежей, майнеры, криптовалюты, ransomware, ransomware-as-a-service, ransomware-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service, ransomware-as-a-service, ransomware-as-a-service, ransomware-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service-as-a-service

- Dave Aitel & Charlie Miller & Nitesh of Nesse Security Centre, Belarus — Exploitation and security of Windows kernelspace [EN]

Наиболее интересные платные обучающие курсы

- Practical Malware Analysis — курс по анализу вредоносного ПО от сотрудников Carnegie Mellon. Можно слушать бесплатно, но тесты и лабораторные работы доступны только за деньги. Курс рассчитан на начинающих специалистов, знакомых с ассемблером, базовыми навыками отладки, знанием основ сетевых протоколов. Бесплатного нет, зато преподаватели формируют, выдают и дотошно проверяют домашки, а в конце курса сдаешь экзамен. Ещё обязательно для прохождения — книга, которая в основном и продается вместе с курсом.
- Platinum edition курс от компании TheFlow, рассчитанный с самых основ и полезен даже тем, кто уже занимается реверсом. Сильно отличается от предыдущего варианта курса. Там как раз рассчитан на не знающих, что и как проверять и отладчиков, но с большим уклоном в сетевые протоколы, а в этом варианте — в сторону реверса.
- Reverse Engineering — курсы от компании TheFlow, рассчитанный исключительно на опытных специалистов, которые уже знают как пользоваться отладчиком, понимают ассемблер и способны к самостоятельному, а не рецептурному реверсу.

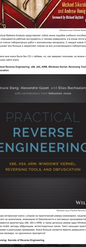
Форумы

- Tuts 4You — интересный форум, один из самых популярных и авторитетных среди профессионалов. Большинство тем посвящено взлому, но есть и разделы, посвященные отладке, реверсу и т.п. Обсуждаются также и обходы различных средств защиты, которые подвергаются постоянному обсуждению. Также на форуме проводятся различные конкурсы, в ходе которых участники соревнуются в решении различных задач, которые ставят перед ними организаторы. Для обсуждения и дискуссии есть отдельный раздел.
- Reverse Engineering Stackexchange — вопросы-ответы, в отличие от предыдущего ресурса, ориентированы на профессионалов. Из минусов — сильно мало тем, для обсуждения есть только один раздел.

Книги

Книги по исследованию вредоносного обеспечения и обратной инженерии — интересная вещь, потому что в большинстве своем они рассчитаны на то, что вы уже знаете, что вас интересует (например, какие как ломать, бороться, защищать и т.п.), но есть и исключения.

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software



Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software

Книга Practical Malware Analysis пишется самими авторами курсов, которые мы рекомендовали выше. Поэтому, если вы решили пройти курс, то в плане знаний вы ничего нового не почерпнете. Но, если вы решили ограничиться только книгой, то вы получите всё то же самое, что и на курсе, за исключением, разумеется, ответов на домашки и ответов на тесты.

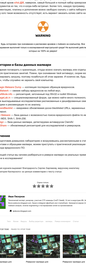
Достоинства книги Все то же, что и у курсов: знания, не в ущерб качеству, и на каком-то абстрактном уровне цель.

- Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

Тоже вроде не написан если с нуля не практиковаться новичкам, зависит от конкретного человека, но в принципе, если вы уже что-то знаете, то можете и сами. Если рассматривается на примере x86, x64, ARM, то в принципе можно прочитать, чтобы понять, что вообще есть. Достоинства: есть примеры, отладчики, инструменты. Цель: тот же самый, что и у предыдущих книг, но с большим уклоном в обфускацию.

- Reversing: Secrets of Reverse Engineering



Reversing: Secrets of Reverse Engineering

Книга стала полным не бесмыслицей — это такая классическая книга по реверсу, которая, к сожалению, обновлению. Поэтому такие примеры, как, например, на примере Windows 2000 — это, конечно, не то, что вам нужно. Но, если вы хотите разобраться в фундаментальных принципах декомпилирования, разобраться, как работает то или иное приложение, то эта книга вам подойдет. Достоинства: есть примеры, есть отладчики, есть инструменты, но, опять же, на примере Windows 2000. Цель: то же, что и у предыдущих книг.

- Reverse Engineering for Beginners Yan Kinsh, Dennis Yurichev

Reverse Engineering for Beginners
Dennis Yurichev
Yan Kinsh
Lebrac 한국어 번역자
실전 연습으로 배우는
리버싱
Reverse Engineering for Beginners
Dennis Yurichev
Yan Kinsh
Lebrac 한국어 번역자
Hmm...
Wrong!
Hmm...
Wrong!
Hmm...
Wrong!