ВИРУСОЛОГИЯ

Осень 2025

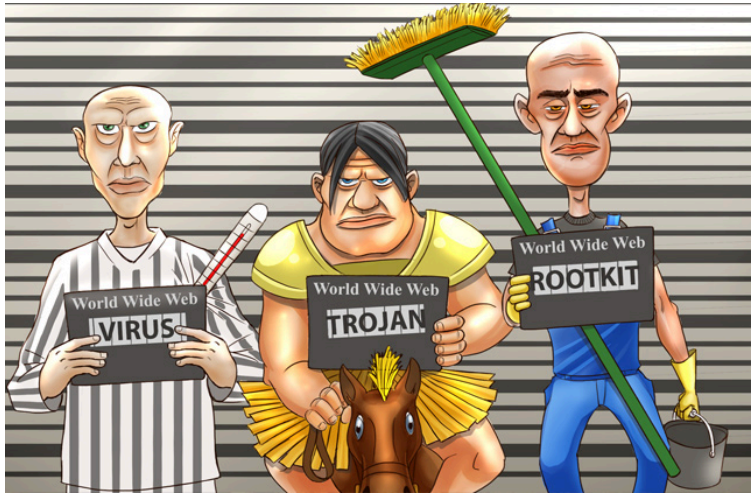
Веричев Александр Владимирович
@xanchelavederiver alexandervерichev@gmail.com

Что такое вредоносная программа

- **Вредоносная программа** (*зловредная программа*, *вредонос*, *зловред*; **malware** - контаминация слов **mal**icious и soft**ware**) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации Wikipedia
- **Malware** — зонтичный термин, объединяющий программы и сэмплы (*samples* - фрагменты кода), предназначенные для причинения вреда компьютеру, сети или серверу CrowdStrike
- Вредоносные программы используются в атаках, целью которых является, среди прочего:
  - извлечение выгоды - вымогательство, продажа конфиденциальных данных
  - нарушение нормальной работы - DOS/DDOS атаки, удаление данных
  - получение [конфиденциальных] данных - промышленный шпионаж, пиратство
  - сделать заявление, привлечь внимание, заслужить *увожение*

Виды вредоносных программ

- Вирус (Virus)
- Червь (Worm, Net-Worm)
- Логическая бомба (Logic Bomb)
- Рекламная закладка (Adware)
- Клавиатурный шпион (Key logger)
- Шпионские программы (Spyware, Stalkerware)
- Стиратель (Wiper)
- Вымогатель (Ransomware)
- Бэкдор (RAT – remote administration tool)
- Загрузчики (Drive-By-Download)
- Троян (Trojan)
- Руткит (Rootkit)
- Ботнет (Botnet)
- и многое другое



Вредоносы, холст, масло
источник: Kaspersky

Вирус

- **Вирус** — самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя Kaspersky Wikipedia
- Внедрение вируса происходит путём вставки своей копии в части существующих файлов
- Вирусы можно «подцепить» разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте
- Вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе
- В настоящее время вирусы встречаются довольно редко в основном по двум причинам:
  - широкое распространение вирусного кода приводит к скорому попаданию в руки антивирусных компаний
  - по большей части вытеснены другими видами вредоносноов, такими как черви и трояны
- Примеры вирусов: **The Creeper**, **Elk Cloner**, **Brain**, **Jerusalem**, **WinVir**, **Bizatch/Boza**, **SCA**, …

Червь

- Червь может считаться видом вируса, так как создан на основе саморазмножающихся программ, хоть и не способен заражать файлы Kaspersky CrowdStrike Wikipedia
- Червь поселяется в компьютере отдельным файлом или вовсе живёт в оперативной памяти (в таком случае его называют *резидентным*)
- Червь ищет уязвимости в системе для дальнейшего распространения
- Для распространения червь использует сеть (локальную или Интернет) и может заражать компьютеры разными способами: по электронной почте, через мессенджеры и т.п.
- Единицей заражения является компьютер целиком, а не отдельный файл на нём
- Главное отличие червя от вируса в том, что червь представляет собой своего рода транспорт для других вредоносных программ
- Например, после успешного заражения червь может «принести» на компьютер троян
- Примеры червей: **червь Морриса**, **SQL Slammer**, **Melissa**, **Concept**, **Mydoom**, **Zeus**, **Storm**, **Conficker**, **Duqu**, **ILOVEYOU**, **WannaCry**, **Code Red**, **Stuxnet**, …

Троян

- В отличие от вирусов и червей, **троян** не самовоспроизводится и не распространяется самостоятельно - его предлагают загрузить под видом законного приложения
  Kaspersky CrowdStrike Wikipedia
- Нередко трояны действительно выполняют заявленные функции полезной программы, однако параллельно предоставляют полезные функции злоумышленникам
- Чаще всего трояны используются для сокрытия выполнения вредоносных и деструктивных действий от системы
- Современные трояны эволюционировали до таких сложных форм, как **бэкдор** или **RAT** (пытающийся взять на себя администрирование компьютера) и **загрузчик** (устанавливающий на компьютер жертвы вредоносный код)
- Примеры троянов: **Zeus**, **Zloader**, **QakBot**, **Andromeda**, **Vundo**, **Linux.Encoder**, **Mac Defender**, **AIDS**, **Emotet**, **DarkComet**, **TrickBot**, **LokiBot**, …

Руткит

- **Руткит** — особый вид вредоносных программ, разработанных специально для маскирования присутствия вредоносного кода и его действий от пользователя и установленного защитного программного обеспечения Kaspersky CrowdStrike Wikipedia
- С целью «спрятаться» руткиты тесно интегрируются с операционной системой и пользуются её механизмами
- Код руткитов выполняется на уровне ядра операционной системы, что позволяет им обходить большинство механизмов защиты - для сокрытия вредоносной деятельности им достаточно отказать в доступе средствам безопасности
- Некоторые руткиты, называемые **буткитами**, могут начать свою работу прежде, чем загрузится операционная система
- Руткиты достаточно трудно обнаружить и уничтожить, для этого применяют сложные современные антивирусные программы
- Примеры руткитов: **NTRootkit**, **Machiavelli**, **Zeus**, **Hacker Defender**, **Vanquish**, **Aphex**, **Cloaker**, **Spicy Hot Pot**, **FU**, **Knark**, **Stoned Bootkit**, **Olmasco**, **Rovnix**, **Stuxnet**, **Flame**, …

Шпионящее ПО

- **Spyware** — категория вредоносных программ, без согласия пользователя собирающих и передающих данные об устройстве и выполняемых на нём действиях CrowdStrike Wikipedia
- Классическим представителем spyware является **клавиатурный шпион** (**keylogger**) – особый вид трояна, который записывает все нажатия кнопок клавиатуры и/или действия мышки на вашем компьютере CrowdStrike
- Чаще всего клавиатурный шпион применяется для кражи паролей и личной информации
- Ещё один популярный вид spyware — **Adware** — отслеживает действия пользователя в сети с целью оптимизации и таргетирования рекламных кампаний; аналогичный функционал выполняют т.н. **Tracking Cookies**
- **RedShell** — особо вредоносный вид ПО, устанавливаемые в систему вместе с какой-либо компьютерной игрой и отслеживающий онлайн-активность
- Примеры spyware: **CoolWebSearch**, **Agent Tesla**, **TrickBot**, **Zeus**, **Pegasus**, **FinSpy**, **DevilsTongue**, **Reign**, **Subzero**, …

Вымогатели

- **Вымогатель** блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных, а затем требует от жертвы выкуп для восстановления исходного состояния CrowdStrike Wikipedia
- Основными способами воздействия на жертву являются: блокировка или помеха работе (в системе или браузере), шифрование файлов и шантаж
- Нередко такие программы используют только разрешенные и безопасные функции системы, из-за чего средства безопасности просто не обращают на них внимания
- В случае применения средств шифрования, данные могут быть потеряны безвозвратно - такие виды вымогателей называют **Wiper** CrowdStrike
- Современные ransomware-атаки используют различные *Тактики, Техники и Процедуры* (*Tactics, Techniques, and Procedures*, *TTPs*)
- Примеры: **CryptoLocker**, **NotPetya**, **Ryuk**, **REvil**, **WannaCry**, **Colonial Pipeline**, **Conti**, **Maze**, **DoppelPaymer**, **BlackCat**, **MOVEit**, …

Источники

1. [Wikipedia] Вредоносная программа
2. [CrowdStrike] Cybersecurity-101 - Malware
3. [Kaspersky] Классификация вредоносных программ
4. [Wikipedia] Computer virus
5. [Wikipedia] Computer worm
6. [CrowdStrike] Cybersecurity-101 - Computer worm
7. [Wikipedia] Trojan horse
8. [CrowdStrike] Cybersecurity-101 - Trojans
9. [Wikipedia] Rootkit
10. [CrowdStrike] Cybersecurity-101 - Rootkits
11. [Wikipedia] Spyware
12. [CrowdStrike] Cybersecurity-101 - Spyware
13. [CrowdStrike] Cybersecurity-101 - Keylogger
14. [Wikipedia] Ransomware
15. [CrowdStrike] Cybersecurity-101 - Ransomware
16. [CrowdStrike] Cybersecurity-101 - Wiper attack