ЧТО ТАКОЕ MALWARE?

Malware — это любое **вредоносное ПО или код,** который создается, чтобы нанести вред, использовать уязвимости или получить несанкционированный доступ к устройству, сети или данным.

ВРЕДОНОСНОЕ

Может нанести ущерб системе или данным.

ИСПОЛЬЗУЕТ УЯЗВИМОСТИ

Эксплуатирует слабые места в системе.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП

Дает злоумышленникам контроль без вашего разрешения.

РАСПРОСТРАНЯЕТСЯ

Может копироваться и заражать другие системы.

5 ТИПОВ MALWARE

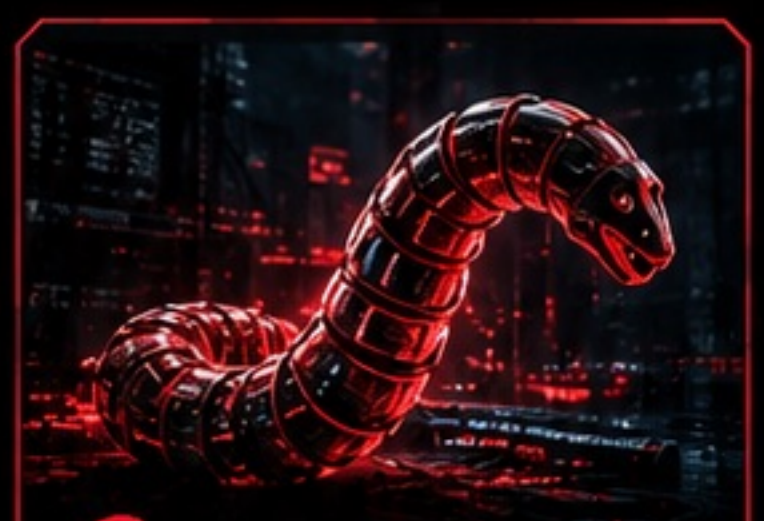
РАЗНЫЕ МЕТОДЫ. ОДНА ЦЕЛЬ.
ТВОИ ДАННЫЕ. ИХ КОНТРОЛЬ.



1 VIRUS

Вирус — это вредоносный код, который внедряется в легитимный файл или программу. Активируется при запуске заражённого файла, распространяется далее и может наносить вред системе.

ЗАРАЖАЕТ / РАСПРОСТРАНЯЕТСЯ
НАНОСИТ ВРЕД



2 WORM

Червь — это самокопирующийся вредоносный код, который распространяется по сети самостоятельно, без участия пользователя и без внедрения в файл. Использует уязвимости, чтобы перемещаться между системами.

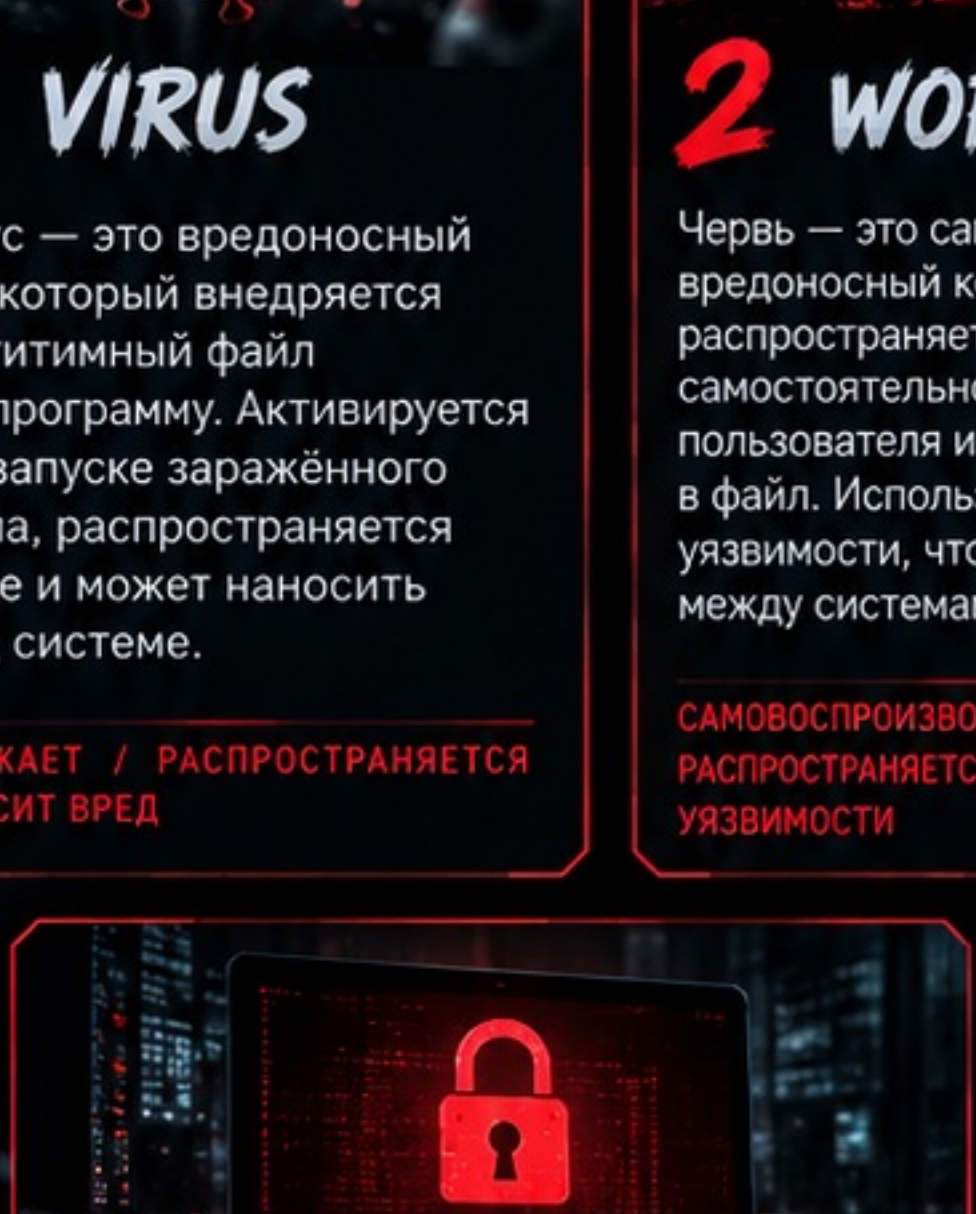
САМОВОСПРОИЗВОДИТСЯ
РАСПРОСТРАНЯЕТСЯ / ЭКСПЛУАТИРУЕТ УЯЗВИМОСТИ



3 TROJAN HORSE

Троян выглядит как легитимный файл или программа, но скрывает в себе вредоносную функциональность. Обманом заставляет пользователя установить его, предоставляя атакующим несанкционированный доступ.

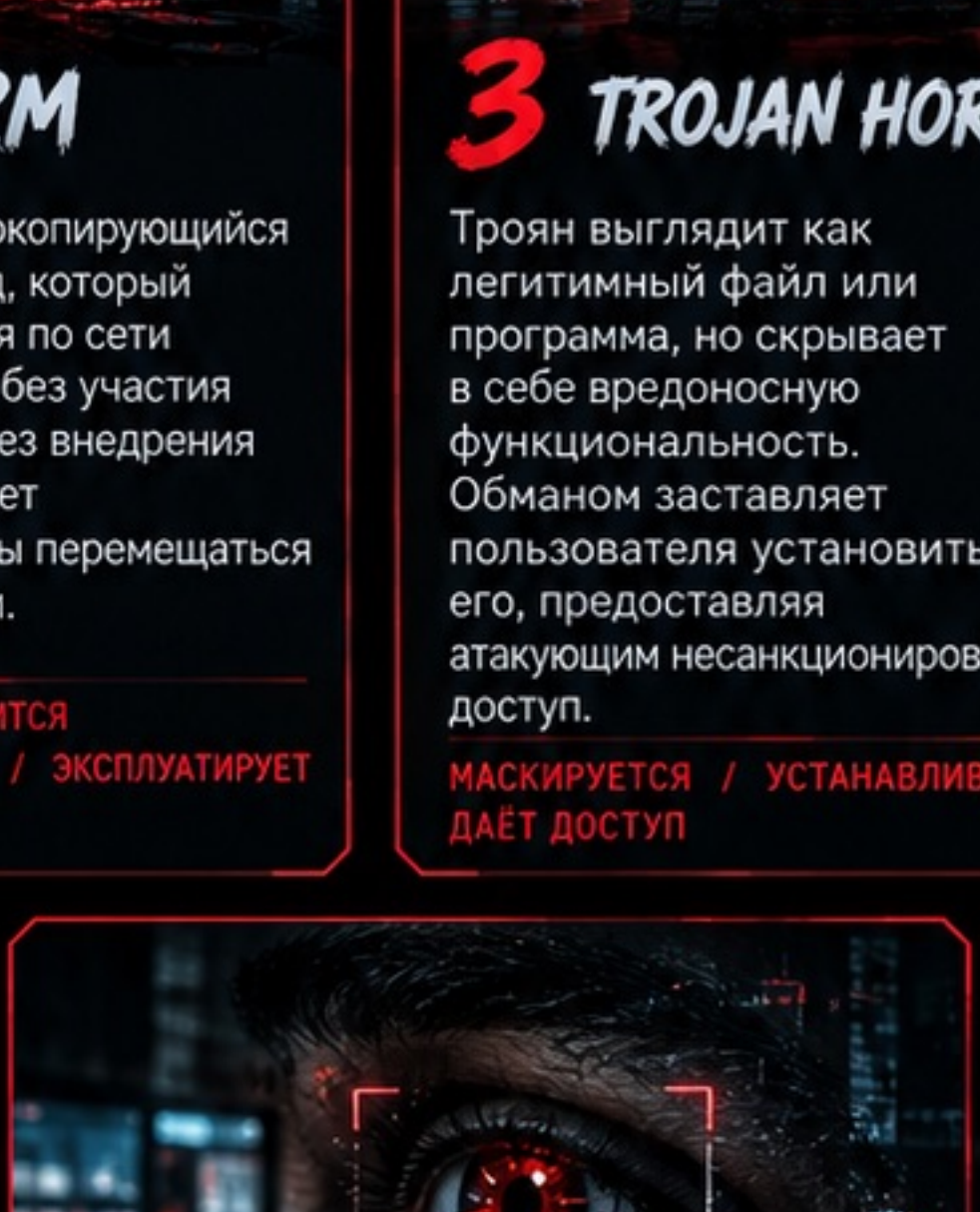
МАСКИРУЕТСЯ / УСТАНАВЛИВАЕТСЯ
ДАЁТ ДОСТУП



4 RANSOMWARE

Блокирует доступ к файлам или системе, шифруя данные, и требует выкуп (например, в криптовалюте) за их разблокировку.

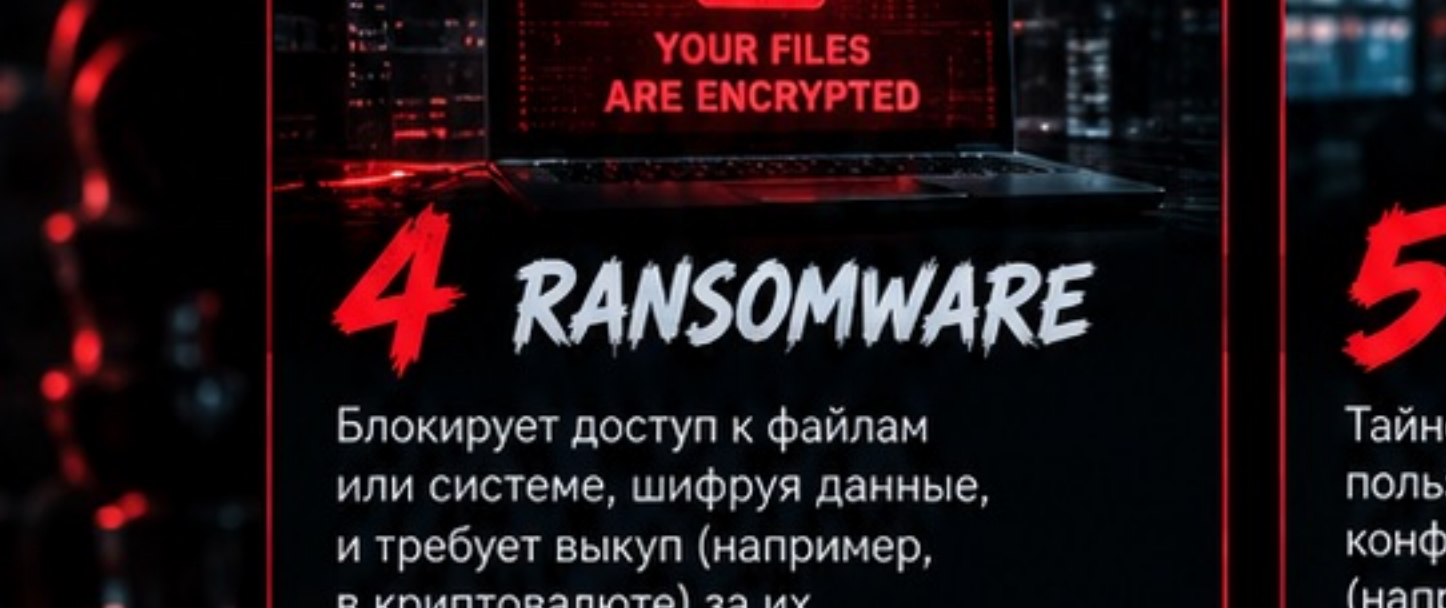
БЛОКИРУЕТ / ШИФРУЕТ / ВЫМОГАЕТ



5 SPYWARE

Тайно отслеживает активность пользователя, собирает конфиденциальную информацию (например, пароли, сообщения, историю браузера) и отправляет её злоумышленникам.

СЛЕДИТ / КРАДЁТ / ПЕРЕДАЁТ ДАННЫЕ



KNOW
DETECT
STAY SAFE

КАК MALWARE ПОПАДАЕТ В СИСТЕМУ?

Злоумышленники используют разные методы,
чтобы доставить вредоносный код на твое устройство.



PHISHING

Обманные письма, ссылки или сообщения, которые выглядят как от доверенного источника.



ВРЕДОНОСНЫЕ ВЛОЖЕНИЯ

Файлы в письмах, мессенджерах или документах (например, Office), содержащие вредоносный код.



ФЕЙКОВОЕ ПО

Загрузка и установка поддельных программ, кряков, активаторов или фейковых обновлений.

КОМПРОМЕТИРОВАННЫЕ САЙТЫ

Посещение заражённых или скомпрометированных веб-ресурсов, которые автоматически эксплуатируют уязвимости в браузере.





ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Использование известных или нулевых уязвимостей в ОС, браузере или приложениях.





ЗАРАЖЁННЫЕ USB

Вредоносный код на съёмных носителях, который запускается при подключении к устройству.







КАК ПОНЯТЬ, ЧТО СИСТЕМА ЗАРАЖЕНА?

Malware часто старается оставаться незаметным, но есть признаки, на которые стоит обратить внимание.

ПОДОЗРИТЕЛЬНЫЕ ПРОЦЕССЫ

Неизвестные процессы в Task Manager или необычное использование CPU, RAM, Disk.

svchost.exe	32.4%
unknown.exe	18.7%
chrome.exe	1.2%
explorer.exe	0.6%

НЕОБЫЧНАЯ СЕТЕВАЯ АКТИВНОСТЬ

Подозрящие исходящие соединения (outbound), особенно на неизвестные IP или домены.



ИЗМЕНЕНИЕ ФАЙЛОВ

Файлы неожиданно шифруются, удаляются или изменяются без вашего участия.

- report.docx.encrypted
- photo.jpg.encrypted
- database.zip.encrypted
- notes.txt.encrypted

МЕХАНИЗМЫ PERSISTENCE

Создаются новые записи в автозагрузке, задачи в планировщике или неизвестные сервисы.

- HKCU\:::\Run
- Windows Task Scheduler
- Unknown Service
- Startup Folder

ОТКЛЮЧЕНИЕ ЗАЩИТНЫХ ИНСТРУМЕНТОВ

Malware может пытаться отключить антивирус, EDR или firewall.

Real-time protection is turned off

Disabled

НЕОБЫЧНОЕ ПОВЕДЕНИЕ СИСТЕМЫ

Снижение производительности, частые сбои, неизвестные окна, перенаправления в браузере, появление сторонних приложений.

- Unknown application installed
- Browser settings changed
- Suspicious activity detected
- System performance degraded



SECURE TODAY
A SAFER TOMORROW

КАК ЗАЩИТИТЬСЯ ОТ MALWARE?

Полностью исключить риск невозможно,
но эти меры значительно его снижают.

1 PATCH MANAGEMENT

Своевременно устанавливай обновления OS, приложений и закрывай известные уязвимости.



2 EDR / ANTIVIRUS

Используй современные средства защиты и регулярно проверяй систему.



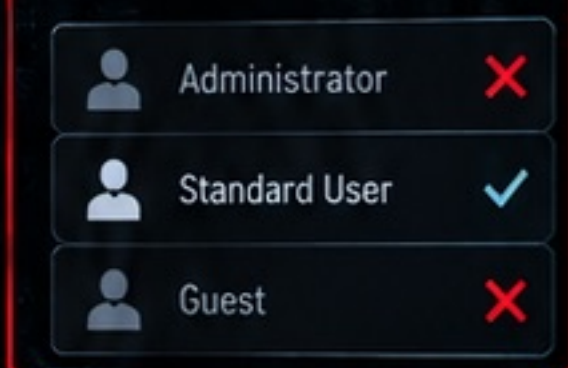
3 MFA

Включай многофакторную аутентификацию на всех важных сервисах.



4 LEAST PRIVILEGE

Используй только необходимые права доступа. Ограничивай права пользователей и сервисов.



5 APPLICATION CONTROL

Разрешай запуск только доверенного ПО и блокируй неизвестные приложения.



6 EMAIL / WEB FILTERING

Фильтруй подозрительные письма, ссылки и веб-ресурсы. Обучай пользователей кибергигиене.



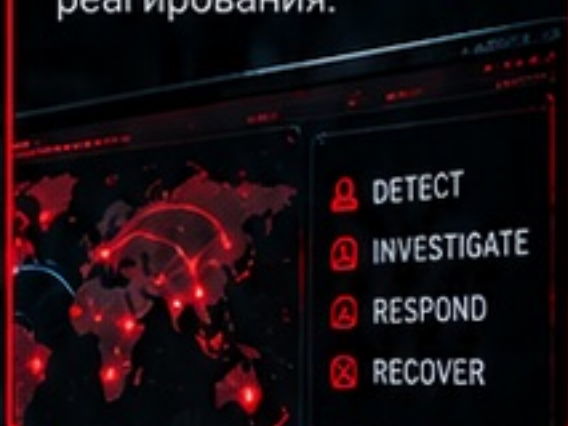
7 BACKUPS

Регулярно создавай резервные копии данных. Храни их отдельно и проверяй возможность восстановления.



8 MONITORING

Используй логи, SIEM и мониторинг для раннего выявления угроз и быстрого реагирования.



MALWARE МЕНЯЕТСЯ. ПРИНЦИПЫ ЗАЩИТЫ — НЕТ.

ТЕ ЖЕ ПРАВИЛА.
БОЛЬШАЯ БЕЗОПАСНОСТЬ.
ТЫ КОНТРОЛИРУЕШЬ РИСКИ.

MORE KNOWLEDGE
SAFER TOMORROW