Kaspersky Industrial Cybersecurity Conference 2023

Техники, тактики и процедуры атак на промышленные организации в 2023

Круглов Кирилл,
Kaspersky ICS CERT

kaspersky

Содержание

Удаленный доступ

Удаленный доступ
Проникновение и закрепление в сети АСУ.

Сбор данных
Проникновение в физически изолированные сети

Эксфильтрация
Использование облачных сервисов хранения данных

Импланты

- FourteenHi
- MeatBall
- И один, использующий Yandex Disk в качестве C2

Импланты (первичные данные)

- Имя компьютера
- Имя пользователя
- IP-адрес
- MAC-адрес
- Версия ОС
- Путь к %System%

Импланты

- Загрузка/выгрузка данных
- Выполнение команд (CMD)
- Интерактивный терминал (shell)

- Обновление адреса командного сервера (C2)
- Списки процессов / дисков / устройств / папок / файлов
- Удаление папок / файлов
- Остановка процессов

- Сохранение снимков экрана
- Сбор ввода с клавиатуры
- ...

Фишинг –один из наиболее вероятных векторов атаки.

Сбор данных

Удаленный доступ
Проникновение и закрепление в сети АСУ.

Сбор данных
Проникновение в физически изолированные сети

Эксфильтрация
Использование облачных сервисов хранения данных

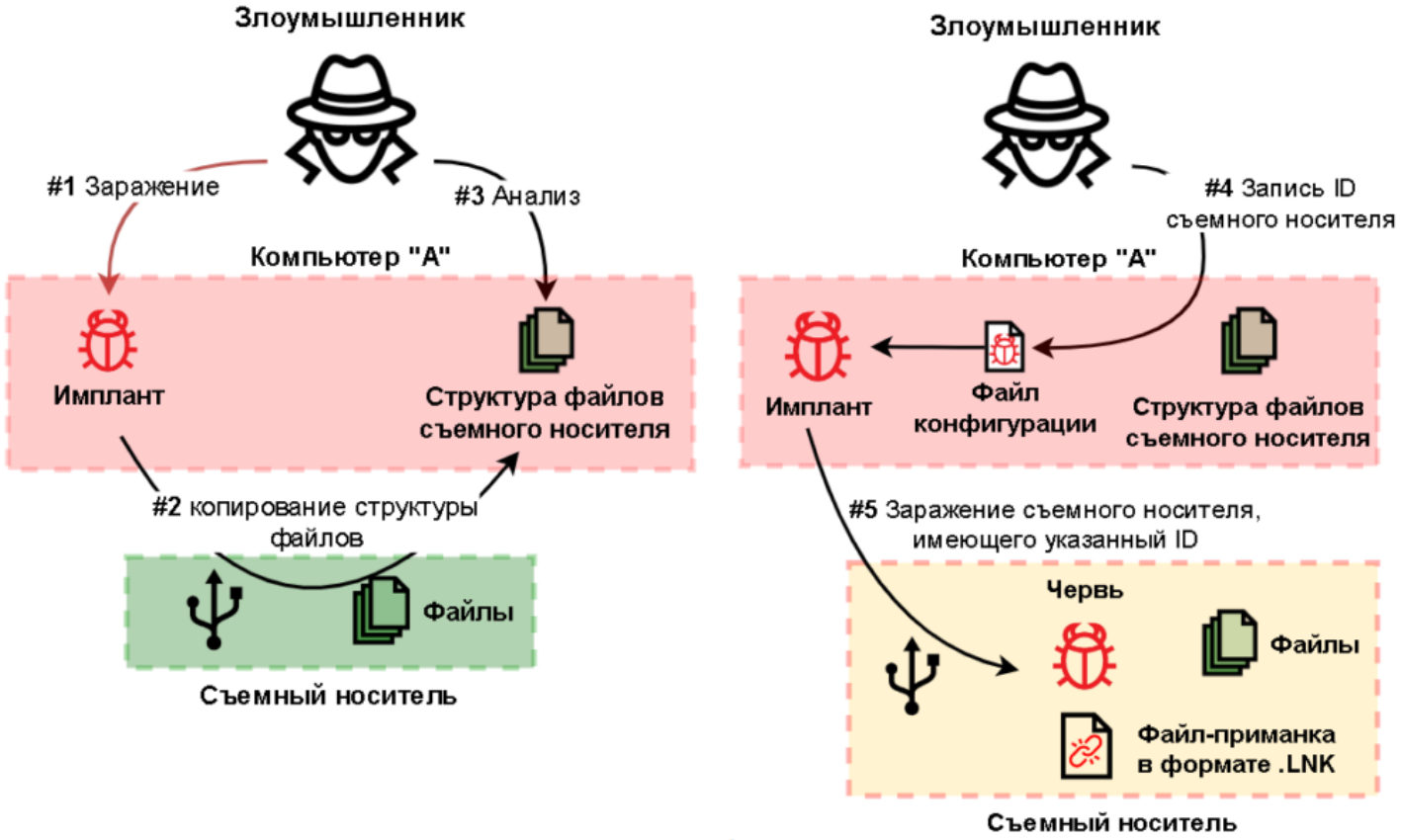
Длительность атак - от 3 до 24 месяцев.

Сбор локальных данных
ВПО предназначенное для сбора и упаковки данных в архивы, для последующей отправки наружу

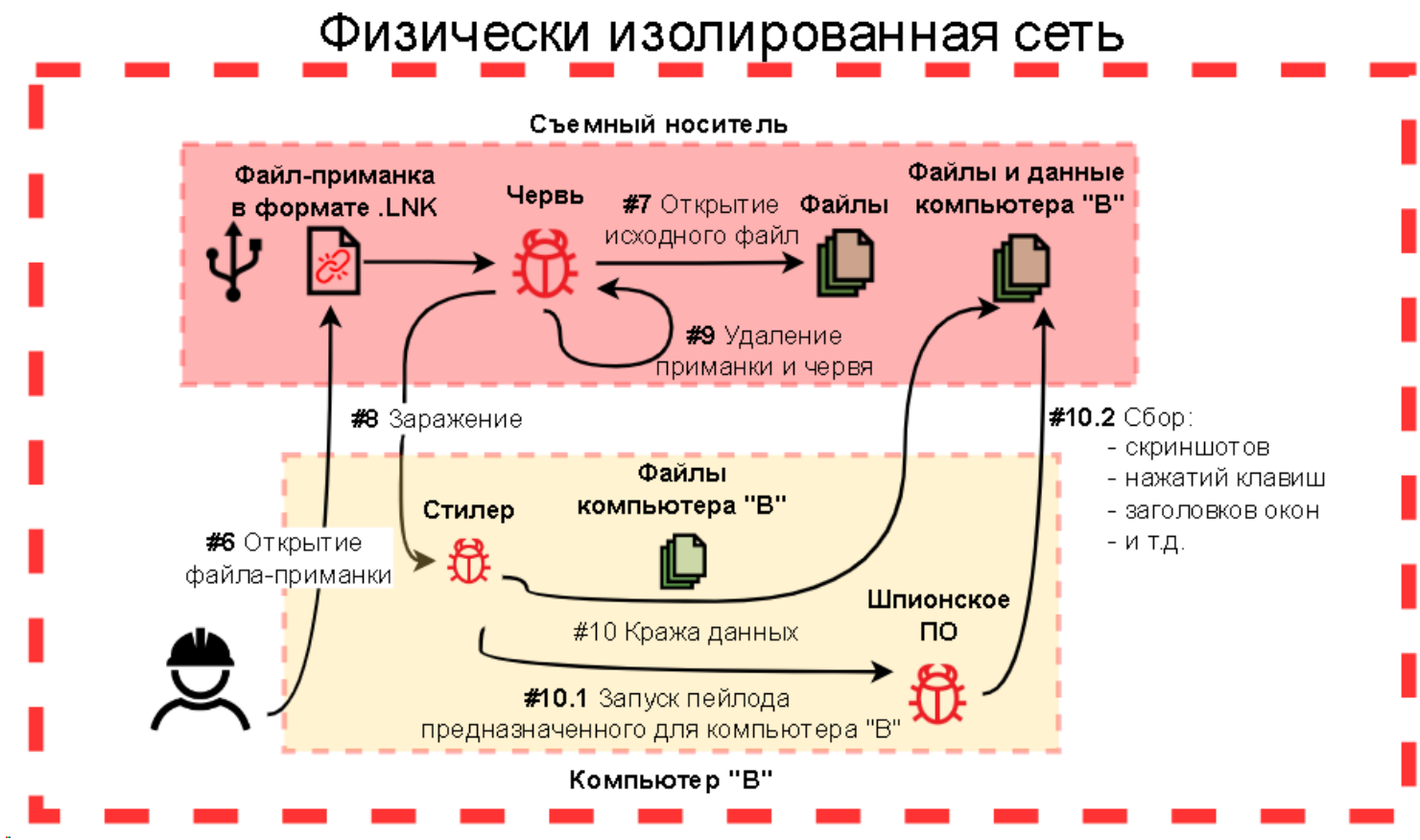
Изолированные сетей
ВПО предназначенное для заражения изолированных систем через съемные устройства

Сбор данных из изолированных сетей

Сбор данных из изолированных сетей



Сбор данных из изолированных сетей



Эксфильтрация

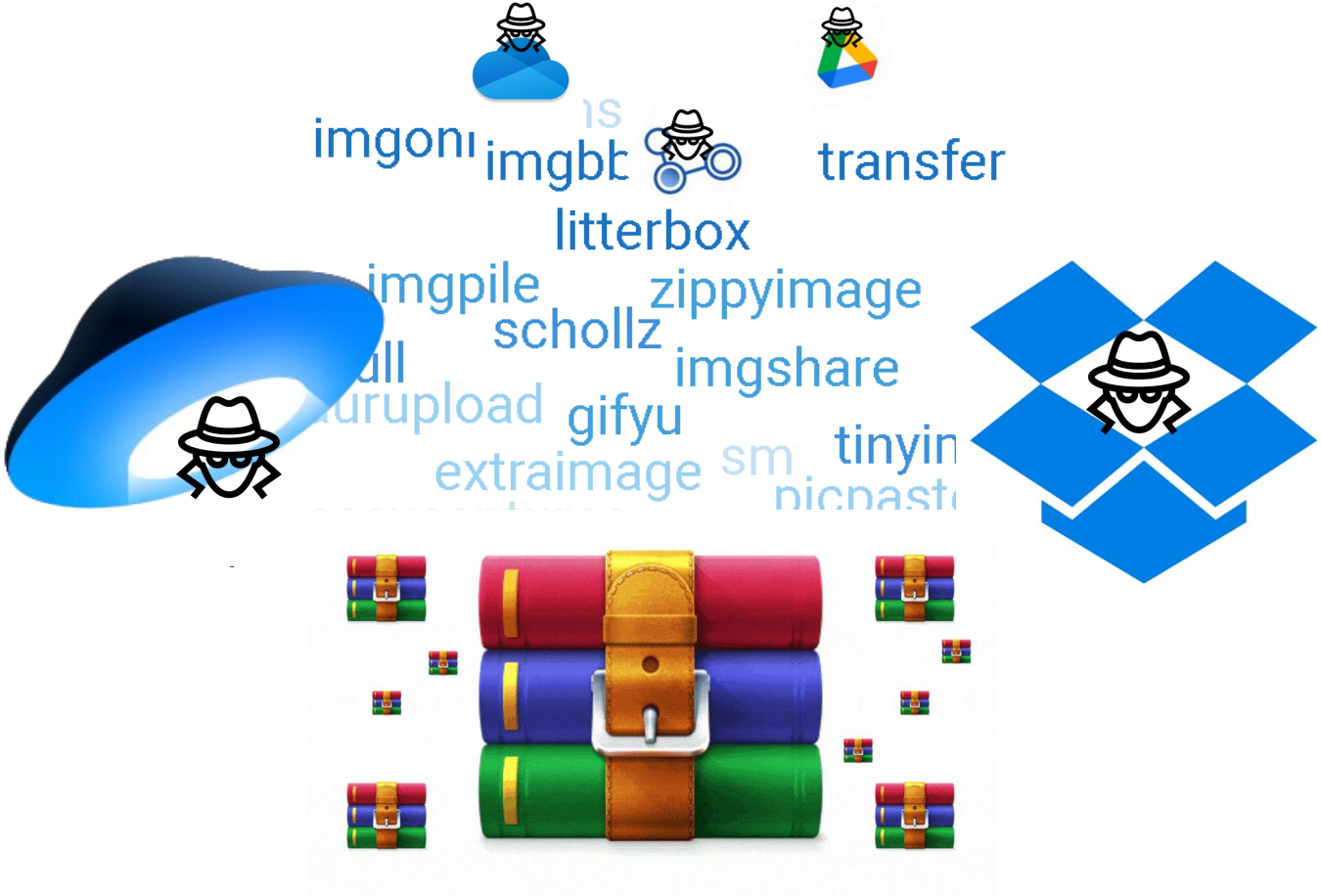
Удаленный доступ
Проникновение и закрепление в сети АСУ.

Сбор данных
Проникновение в физически изолированные сети

Эксфильтрация
Использование облачных сервисов хранения данных

Эксфильтрация

Эксфильтрация



Заключение

Основные техники, тактики и процедуры

Проникновение
T1566.001 - Фишинг

Закрепление
T11547, T1543, T1053 – Ключи реестра autorun, сервисы, планировщик задач

Обход защиты
T140, T1055, T1574 – Шифрование полезной нагрузки, отложенное выполнение, использование DLL hijacking и внедрение в память доверенных процессов

Основные техники, тактики и процедуры

Эксфильтрация

T1041 – Использование облачных сервисов

Удаленное управление

T1071, T1573- Использование WEB протоколов + шифрование SSL

Обнаружение

T1083, T1016, T1033, T1057 – Поиск файлов заданных типов, сбор конфигурации компьютера / сети, сбор информации о пользователе, анализ окружения (процессы, устройства)

Вопросы?

Спасибо за внимание

Kaspersky ICS CERT

kaspersky