pt

ptsecurity.com

РУТКИТЫ

хронология появления

2011

ZeroAccess

- Поддерживает запуск майнера или кликера после заражения
- Может быть использован для атак на GSM-станции

Hikit

- Используется APT Axiom
- Предоставляет удаленный доступ к скомпрометированным узлам
- Направлен на сбор данных

Ebury

- Используется APT Windigo
- Крадет учетные данные для OpenSSH
- Предоставляет удаленный доступ к скомпрометированным узлам

2012

Flame

- Используется APT Equation Group
- Перехватывает сетевой трафик
- Стирает следы активности злоумышленника на зараженной машине
- Может записывать звук и делать скриншоты, а также передавать полученные данные, в том числе по Bluetooth

Necurs

- Может загружать вымогатели и банковские трояны, был замечен в кампании по распространению Dridex
- Отключает средства защиты
- Использует алгоритмы генерации доменов (DGA)
- Содержит модуль для спам-рассылок, модули для проведения других атак и модуль для перенаправления трафика

Regin

- Использует APT Equation Group
  Может заражать контроллеры GSM-станций
- Содержит набор инструментов для шпионажа
- Предоставляет удаленный доступ к скомпрометированным узлам

2013

Careto

- Используется APT Mask
- Имеет два модуля: руткит и буткит
- Исходный код вредоноса подписан цифровым сертификатом
- Собирает файлы конфигурации VPN, RDP и ключи SSH
- Позволяет злоумышленникам запускать свои команды

2014

Kronos

- Осуществляет сбор данных для доступа в интернет-банкинг
- Сочетает в себе функции банковского трояна и загрузчика
- Распространяется в рамках фишинговых кампаний

2015

Shedun

- Используется группировкой Yingmob
- Имитирует популярные приложения
- Может применяться для загрузки дополнительного ВПО, в том числе рекламного ПО

Umbreon

- Устанавливает бэкдор Espeon
- Создает локальных пользователей для доступа к зараженной системе
- Перехватывает вызовы функции libc, чтобы скрыть наличие нового пользователя в файле /etc/passwd

2016

Remsec (Cremes)

- Используется APT Strider
- Применяется в кибершпионских кампаниях
- Предоставляет удаленный доступ к скомпрометированным узлам, а также позволяет загружать дополнительное ПО
- Содержит модуль для перехвата сетевого трафика и нажатий клавиш на клавиатуре

2017

DirtyMoe

- Распространяется подобно червю, объединяя жертв в ботнет
- Использует вычислительные ресурсы жертв для проведения DDoS-атак и майнинга криптовалюты

2018

Moriya

- Используется предположительно APT1
- Скрывает связь с сервером управления
- Предоставляет удаленный доступ к скомпрометированным узлам

2019

Skidmap

- Загружает модуль для майнинга криптовалюты
- Показывает поддельные данные о загрузке процессора

Scranos

- Внедряет рекламное ПО на скомпрометированных узлах
- Похищает учетные данные из браузера
- Распространяет рекламное ПО для мобильных устройств через взломанные аккаунты в социальных сетях

2020

Drovorub

- Используется APT28
- Обеспечивает канал связи с командным сервером
- Обладает возможностью перехвата и перенаправления сетевого трафика
- Изменяет правила на межсетевом экране

Ориентация руткитов на ОС Unix IOS Android Windows

Тип атаки Целевые атаки Массовые атаки