Изначально мобильный вредонос сместил фокус на настольные платформы.

Вредоносное ПО под названием LightSpy, ранее известное только в атаках на Android и iOS, теперь замечено и на macOS – операционная система, разработанная компанией Apple для компьютеров Mac. Она представляет собой современную, интуитивно понятную и надёжную платформу, которая объединяет в себе мощные функции и простоту использования.

 Система предлагает широкий спектр возможностей, обеспечивая удобство работы с файлами, приложениями и интернетом. Интерфейс macOS дружелюбен и стильно оформлен, с минималистичным дизайном и плавными анимациями.

 Одна из ключевых особенностей macOS – это интеграция с другими устройствами Apple. Пользователи могут без проблем синхронизировать данные и работать с ними на своём Mac, iPhone, iPad и Apple Watch." data-html="true" data-original-title="macOS" >macOS, что подтверждает его широкие возможности по сбору данных.

LightSpy — это модульный шпионский фреймворк, который используется для кражи разнообразной информации, включая файлы, снимки экрана, данные о местоположении, записи голосовых вызовов в WeChat и данные из Telegram и QQ Messenger.

Согласно новому отчёту ThreatFabric, версия LightSpy для macOS активно используется с января 2024 года, хотя пока что она действует лишь в тестовых средах и нескольких заражённых устройствах, принадлежащих самим исследователям.

Специалисты получили доступ к панели управления LightSpy, использовав уязвимость конфигурации, что позволило им понять функциональность, инфраструктуру и список заражённых устройств.

Злоумышленники используют уязвимости WebKit (CVE-2018-4233 и CVE-2018-4404), чтобы выполнить код в Safari на macOS 10.13.3 и более ранних версиях.

Первоначально на устройство доставляется 64-битный бинарный файл MachO, замаскированный под PNG-изображение («20004312341.png»). Этот файл затем расшифровывает и выполняет встроенные скрипты для загрузки следующего этапа.

Второй этап уже загружает эксплойт для повышения привилегий («ssudo»), утилиту для шифрования/дешифрования («ddss») и ZIP-архив («mac.zip») с двумя исполняемыми файлами («update» и «update.plist»).

Затем скрипт получает root-доступ на заражённом устройстве и устанавливает устойчивость в системе, конфигурируя «update» для запуска при старте системы.

Следующий шаг выполняется компонентом «macircloader», который загружает, расшифровывает и выполняет LightSpy Core, управляющий плагинами шпионского ПО и отвечающий за связь с командным сервером.

LightSpy Core также может выполнять shell-команды на устройстве, обновлять сетевую конфигурацию и устанавливать расписание активности для обхода обнаружения.

Схема атаки

Хотя вредоносная программа использует 14 плагинов для Android и 16 плагинов для iOS, macOS-версия использует лишь следующие 10:

Эти плагины позволяют LightSpy собирать обширные данные с заражённых macOS систем, обеспечивая гибкость работы вредоноса.

Исследуя веб-панель управления LightSpy, специалисты ThreatFabric – это компания, которая специализируется на исследовании и анализе мобильной безопасности. Они используют свои знания и инструменты, чтобы помочь клиентам защититься от угроз и атак.
 Компания выпускает информационные отчеты об угрозах, способных повлиять на мобильные устройства, и предоставляет готовые решения для защиты от этих угроз." data-html="true" data-original-title="ThreatFabric" >ThreatFabric также обнаружили потенциальное существование имплантатов для Windows, Linux и роутеров, однако пока что нет информации о способах их доставки и использования в реальных атаках.

Таким образом, несмотря на некоторые ограничения последних версий вредоноса LightSpy, его модульная природа и обширный функционал по сбору конфиденциальных данных, представляют серьёзную угрозу безопасности не только для пользователей macOS, но и, гипотетически, других настольных платформ.

Пользователям необходимо проявлять бдительность, своевременно обновлять программное обеспечение и использовать надёжные средства кибербезопасности для защиты своих устройств и данных.