НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

РАЗВЕДЫВАТЕЛЬНАЯ АКЦИЯ АМЕРИКАНСКИХ СПЕЦСЛУЖБ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ ФИРМЫ APPLE

ALRT-20230601.1 | 1 июня 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	Федеральной службой безопасности Российской Федерации совместно с Федеральной службой охраны Российской Федерации вскрыта разведывательная акция американских спецслужб, проведенная с использованием мобильных устройств фирмы Apple (США). В ходе обеспечения безопасности российской телекоммуникационной инфраструктуры выявлены аномалии, характерные только для пользователей мобильных телефонов Apple и обусловленные работой ранее неизвестного вредоносного программного обеспечения (ВПО), использующего предусмотренные производителем программные уязвимости. Установлено, что заражению подверглись несколько тысяч телефонных аппаратов этой марки. При этом кроме отечественных абонентов выявлены факты заражения зарубежных номеров и абонентов, использующих sim-карты, зарегистрированные на диппредставительства и посольства в России, включая страны блока НАТО и постсоветского пространства, а также Израиль, САР и КНР. Заражение ВПО происходит по следующему алгоритму: • Целевое iOS-устройство получает сообщение iMessage со специальным вложением, содержащим эксплойт • Без какого-либо взаимодействия с пользователем эксплойт из сообщения вызывает выполнение вредоносного кода • В ходе выполнения кода устанавливается соединение с сервером управления и происходит последовательная загрузка нескольких модулей вредоносной программы, включая дополнительные эксплойты для повышения привилегий • После успешной отработки всех вредоносных компонентов загружается конечная вредоносная нагрузка • Сообщение и вложение с эксплойтом удаляются в процессе заражения • В результате злоумышленники могут получить несанкционированный доступ к информации о пользователе и системе, а также возможность выполнить произвольный код на уязвимом устройстве С описанием методов выявления признаков функционирования ВПО на устройствах компании Apple можно ознакомиться в отчете компании «Лаборатория Касперского» по следующей ссылке: https://securelist.ru/operation-triangulation/107470/

Центры удаленного управления ВПО	addatamarket.net ans7tv.net anstv.net backuprabbit.com businessvideonews.com cloudsponcer.com datamarketplace.net mobilegamerstats.com snoweeanalytics.com tagclick-cdn.com topographyupdates.com unlimitedteacup.com virtuallaughing.com web-trackers.com growthtransport.com