НТВ APT Проведение доменного имени через RPC и использование Windows Defender для обхода песочниц

Windows Security Internals @SecuriTeam_SSI

В этой статье с названием SOLORIGATE (ru:ядро, EN:gate) группа ботов, связанная с российской APT-группой Turla, использует доменное имя, зарегистрированное через Windows Telephony. Кроме доменного имени для дальнейшего захвата бекдоров APT Turla, в данном докладе затрагиваются вопросы того, какие средства антивирусного ПО Windows Defender используются для обхода песочниц.

Примечание:
Все материалы, связанные с Российской группой Turla, мы по-прежнему называем APT, потому что в отличие от большинства сообществ, мы не можем с достоверностью определить, кто за ней стоит.

Содержание статьи

Реализация
Доменная группа Turla
Доменная группа Turla
Доменная группа Turla
Доменная группа Turla
Реализация
Реализация
Доменная группа Turla
Доменная группа Turla
Доменная группа Turla
Доменная группа Turla