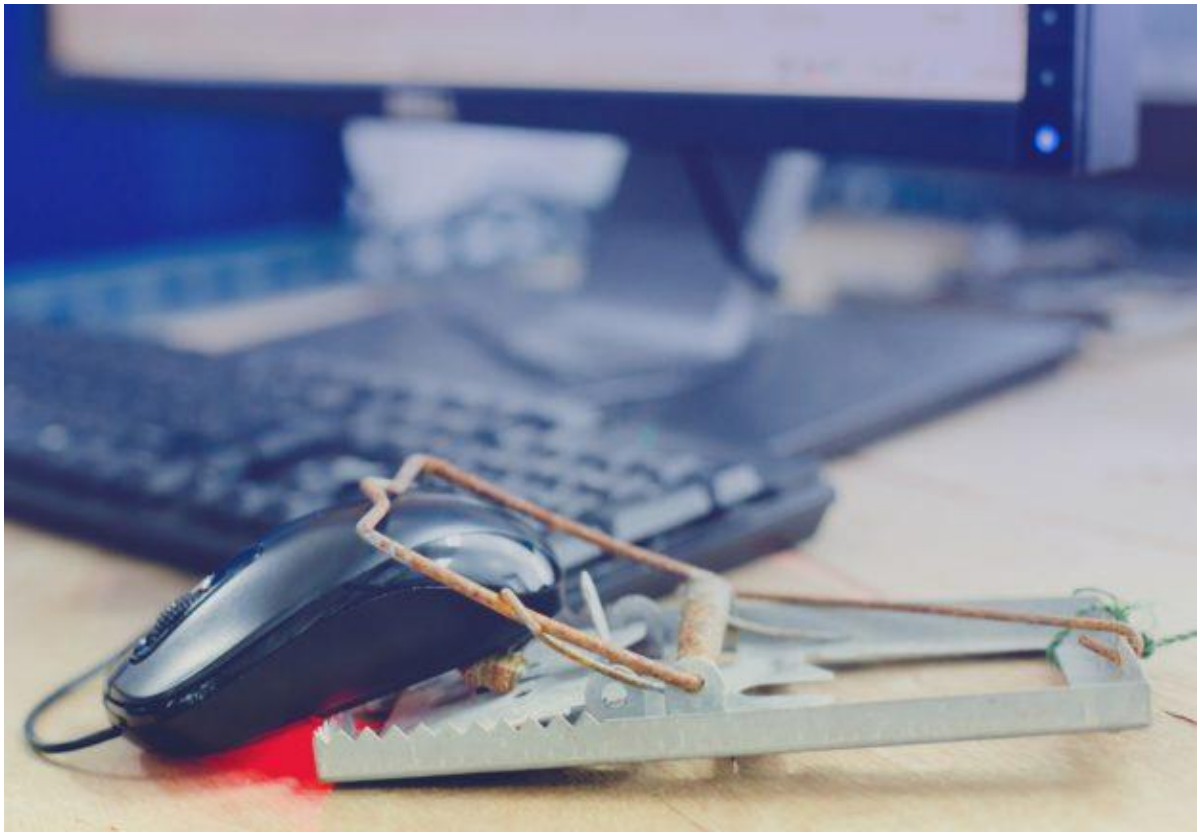
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET: новый Android RAT использует протокол Telegram

20 июня 2018 года

Специалисты ESET открыли новое семейство вредоносного ПО – Android RAT (Remote Administration Tool – средство удаленного управления), использующее протокол Telegram для управления и эксфильтрации данных.



Мы изучали повышение активности ранее описанных IRRAT и TeleRAT, но затем, разобравшись в происходящем, выявили новое семейство вредоносных программ, активное минимум с августа 2017 года. В марте 2018 года исходный код малвари распространялся через Telegram-каналы хакеров, в результате чего сотни модификаций сегодня действуют in the wild.

Одна из версий отличается от остальных. Несмотря на доступность исходного кода, она продается под коммерческим названием HeroRat через специальный Telegram-канал. Малварь доступна в трех комплектациях с разными функциями и обучающим видеоканалом. Неясно, был ли этот вариант написан на базе слитого кода или, напротив, является оригиналом, исходный код которого затем появился в сети.

Как это работает

Злоумышленники распространяют RAT через сторонние магазины Android-приложений, социальные сети и мессенджеры. Мы видели, как вредоносную программу маскируют под приложения, обещающие биткоины в подарок, бесплатный мобильный интернет или накрутку подписчиков в соцсетях. В Google Play данной малвари не обнаружено. Большинство заражений зафиксировано в Иране.

Рисунок 1. Несколько приложений, используемых для распространения RAT

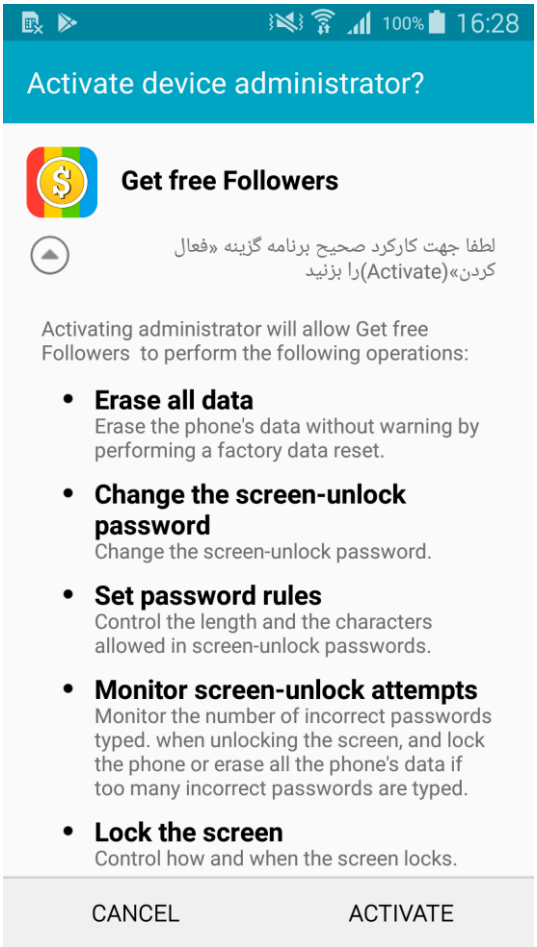


Рисунок 2. RAT запрашивает права администратора устройства

После установки и запуска вредоносного приложения на экране появляется небольшое всплывающее окно. В нем сообщается, что программа не может работать на устройстве и будет удалена. Мы видели образцы с сообщениями на английском и персидском языках (в зависимости от языковых настроек устройства).

Когда удаление завершено, иконка приложения исчезнет. Одновременно с этим на стороне атакующих будет зарегистрировано новое зараженное устройство.

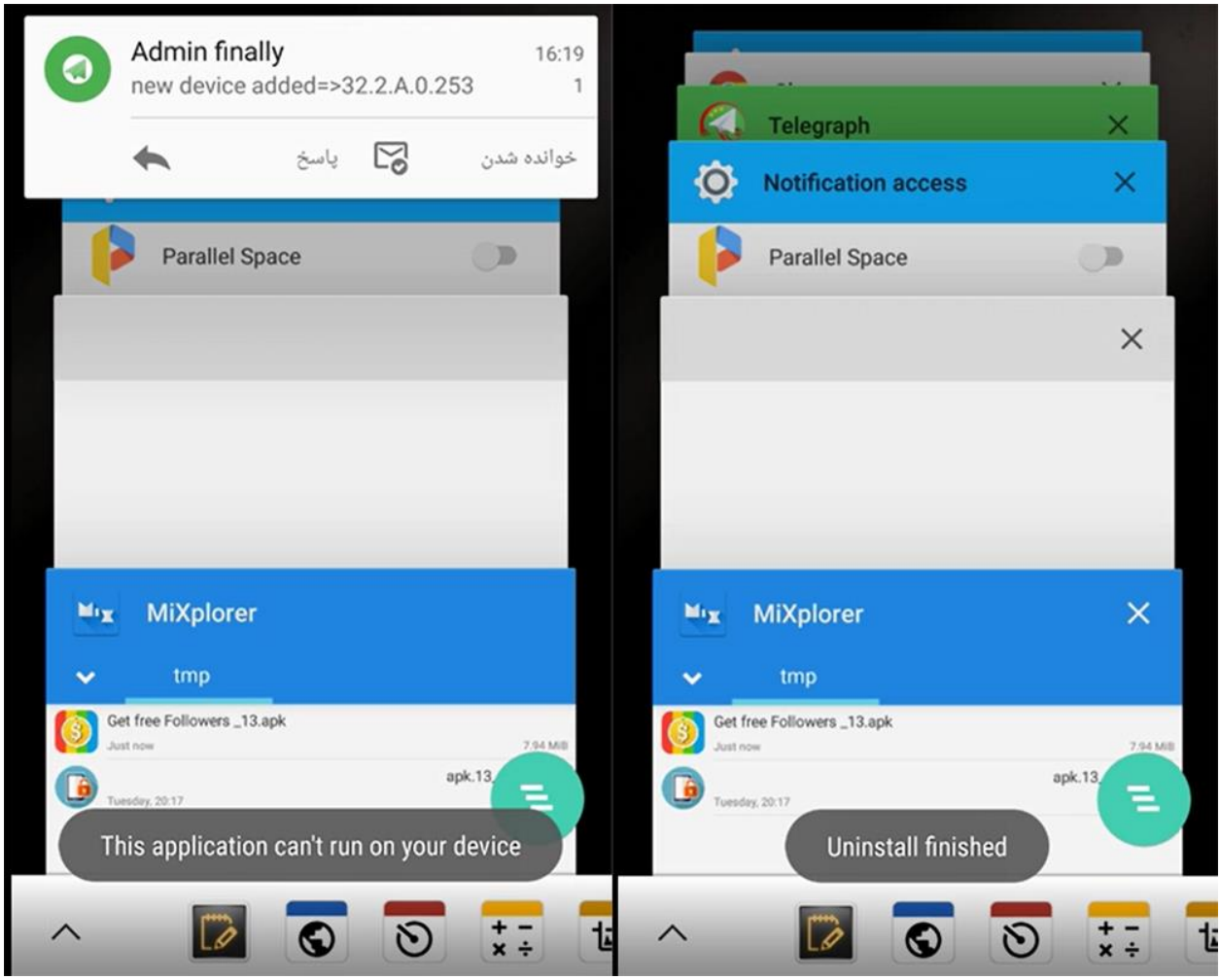


Рисунок 3. Демонстрация установки HeroRat на устройство (скриншоты из обучающего видео авторов малвари)

```
inf.Values.sharep.Edit().PutBoolean("ftr", false).Commit();
string[] array = new string[]
{
    "This Application Can't Run On Your Device",
    "Uninstalling...",
    "Uninstall finished"
};
if (!Locale.get_Default().get_Language().Equals("en"))
{
    array[0] = "این نرم افزار قادر به اجرا بر دستگاه شما نمیباشد";
    array[1] = "درحال حذف نصب";
    array[2] = "حذف نصب پایان یافت";
}
Toast.MakeText(this, array[0], 1).Show();
Toast.MakeText(this, array[1], 1).Show();
Toast.MakeText(this, array[2], 1).Show();
```

Рисунок 4. Исходный код малвари с поддельным сообщением об удалении на английском и персидском

Получив доступ к скомпрометированному устройству, атакующий использует возможности бота Telegram для управления новым девайсом. Каждое зараженное устройство управляется с помощью бота, настраивается и контролируется через приложение Telegram.

Вредоносная программа обладает широким спектром инструментов шпионажа и эксфильтрации файлов, включая перехват текстовых сообщений и контактов, отправку текстовых сообщений и вызовы, запись звука и создание скриншотов, определение местоположения устройства и управление его настройками.

HeroRat продают в трех комплектациях (бронзовый, серебряный и золотой пакеты) за 25, 50 и 100 долларов соответственно. Исходный код от автора HeroRat предлагается купить за 650 долларов.

Доступ к функциям HeroRat осуществляется с помощью интерактивных кнопок в интерфейсе Telegram-бота. Атакующие могут управлять зараженными устройствами, нажимая кнопки, доступные в той версии RAT, которую они оплатили и используют.

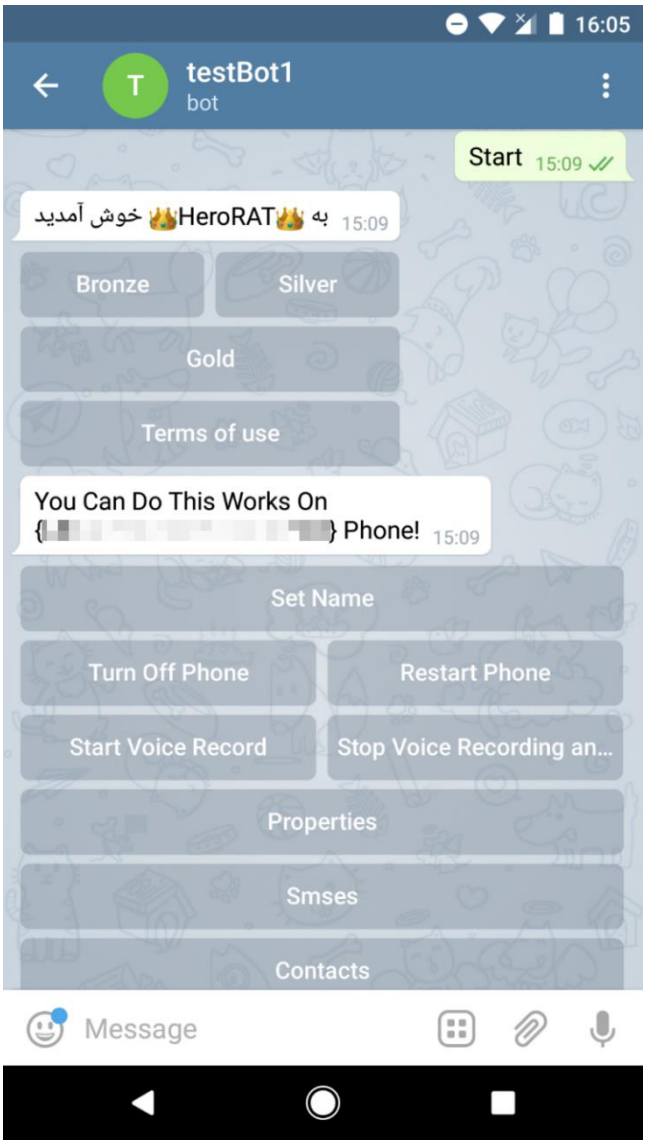


Рисунок 5. Панель управления HeroRat

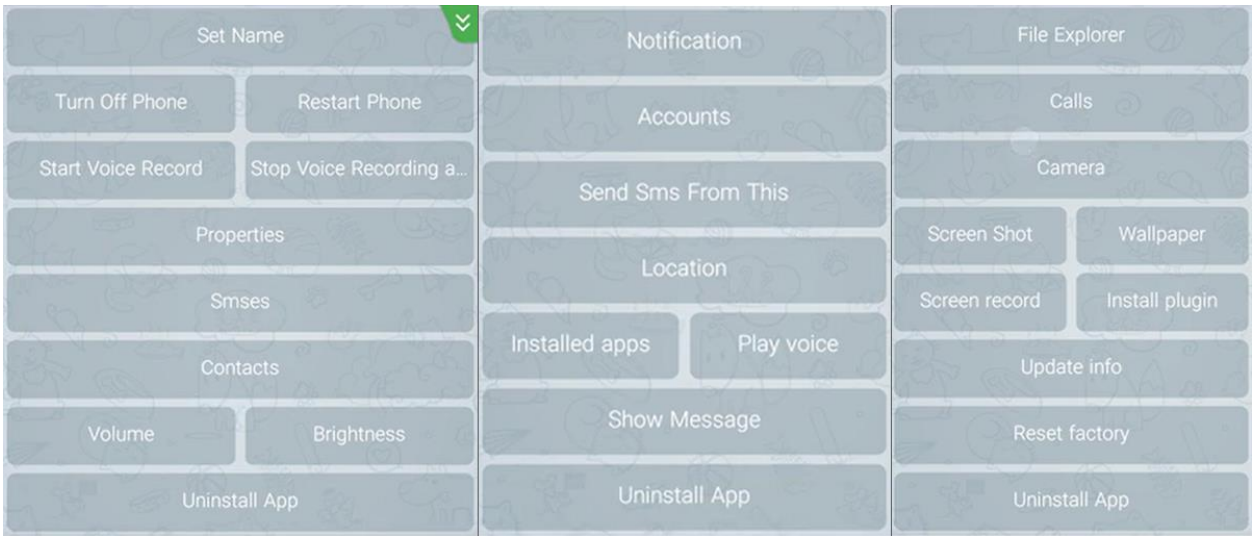


Рисунок 6. Функции HeroRat (слева направо): бронзовый, серебряный и золотой пакеты (скриншоты из обучающего видео авторов малвари)

В отличие от ранее изученных Android RAT, использующих Telegram, которые написаны на стандартном Android Java, новое семейство разработано с нуля на C# с использованием фреймворка Xamarin – редкое сочетание для Android-малвари.

Способ коммуникации через протокол Telegram адаптирован к языку программирования – вместо Telegram Bot API, который использовали ранее изученные RAT, новое семейство применяет Telesharp, библиотеку для создания ботов Telegram на C#.

Передача команд и эксфильтрация данных с зараженных устройств полностью покрываются протоколом Telegram – эта мера направлена на противодействие обнаружению на основе трафика на известные серверы загрузки.

Профилактика заражения

Благодаря утечке исходного кода, новые модификации малвари могут появиться в любой точке мира. В каждом случае схема заражения и способ маскировки будут меняться, поэтому проверки устройства на наличие/отсутствие каких-либо приложений недостаточно.

Если вы считаете, что устройство было заражено, просканируйте его надежным мобильным антивирусом. ESET детектирует угрозу как Android/Spy.Agent.AMS и Android/Agent.AQO.
Чтобы избежать заражения, загружайте приложения только в официальном магазине Google Play, читайте отзывы пользователей и обращайте внимание на запросы разрешений.

Индикаторы заражения

Package Name	Hash	Detection
System.OS	896FFA6CB6D7789662ACEDC3F9C024A0	Android/Agent.AQO
Andro.OS	E16349E8BB8F76DCFF973CB71E9EA59E	Android/Spy.Agent.AMS
FreeInterNet.OS	0E6FDBDF1FB1E758D2352407D4DBF91E	Android/Agent.AQO