BALKANLAR'A ÇİFT NAMLULU SİBER SALDIRI

-

16.09.2019

Balkan Günlüğü (15 Eylül 2019)

Siber güvenlik kuruluşu ESET, Balkan ülkelerini hedef alan yeni ve hayli ilginç bir zararlı yazılım dalgası tespit etti. Şirketlere odaklanan siber hırsızlar, BalkanDoor ve BalkanRAT adlı iki zararlı yazılımı aynı anda kullanarak mali kazanç elde etmeyi hedefliyor.
ESET araştırmacılarının belirlediği olayda, Sırbistan, Bosna Hersek, Karadağ ve Hırvatistandaki şirketler hedef alınmış gibi görünüyor. İki zararlı yazılımın aynı anda devreye sokulduğu siber saldırıda, bir arka kapı zararlısı olan BalkanDoor ve bir uzaktan erişim truva atı olan BalkanRAT kullanılmış.

Benzer işlevlere sahip ama…

BalkanRAT, ele geçirilmiş bilgisayarın, bir grafik arabirim aracılığıyla uzaktan kontrol edilmesini sağlarken, BalkanDoor ise aynı işlevi bir komut satırı aracılığıyla yapıyor.

Bu ikili saldırı setinin ise şöyle çalıştığı tahmin ediliyor: Siber saldırgan, kurbanın ekranının kilitlendiğini ve dolayısıyla büyük olasılıkla bilgisayarı kullanmadığını tespit ediyor. Saldırgan, BalkanDoor arka kapısından ekran kilidini açmak için bir arka kapı komutu gönderiyor. Daha sonra da BalkanRAT kullanarak, bilgisayarda ne isterse onu yapabiliyor.

https://balkangunlugu.com/2019/09/balkanlara-cift-namlulu-siber-saldiri/

Kaynak/Source: