Comodo Android kullanıcılarını uyardı:

"Tordow v2.0 salgınına dikkat"

COMODO, 20.12.2016 – Siber güvenlik araştırmaları ve çözümleriyle ünlü COMODO, Rusya'daki istemcileri etkileyen zararlı Android yazılımı "Tordow v2.0" ait kimi örnekler keşfetti. Tordow, Android işletim sistemine yönelik ilk mobil bankacılık trojanı ve bulaştığı cihazlarda yönetici ayrıcalıkları elde etmeyi hedefliyor.

Normal koşullarda zararlı bankacılık yazılımları, zararlı faaliyetlerini yönetici erişimi olmadan da gerçekleştirebilir ama hackerlar yönetici erişimi ile daha geniş kapsamlı bir dizi işlev kazanabiliyorlar. Tordow 2.0 telefonla arama yapabilir, SMS mesajlarını kontrol edebilir, program indirip kurabilir, oturum açma bilgilerini çalabilir, irtibat kişilerine erişebilir, dosyaları şifreleyebilir, internet sayfalarını ziyaret edebilir, bankacılık verilerini kendi çıkarları için kullanabilir, güvenlik yazılımlarını kaldırabilir, cihazları yeniden başlatabilir, dosyalara yeniden isim verebilir ve fidye yazılımı olarak hareket edebilir. Depolanan hassas bilgileri bulmak için Android ve Google Chrome tarayıcılarını araştırır. Tordow 2.0'ın ayrıca cihaz donanımı ve yazılımı, işletim sistemi, üretici, internet hizmet sağlayıcısı ve kullanıcı konumuna ilişkin verileri de topladığını teknik detaylar ortaya koyuyor.

Tordow 2.0 sahip olduğu CryptoUtil sınıfı işlevler ile AES algoritmasını kullanarak dosyaları şifreleyebilir ve şifrelerini açabilir. Bunu yaparken ise 'MIIxxxxCgAwIB' gömülü kodlanmış anahtarını kullanır. Android uygulama paketi (APK) dosyaları, "cryptocomponenet.2" gibi isimlerle, AES algoritması ile şifrelenmiştir.

Tordow 2.0 yönetici ayrıcalıklarını kazandığını dokuz farklı yolla doğrulayabilir. Statüsü saldırganın kumanda ve kontrol (C2) sunucularından birine (https://2ip.ru adresindeki gibi) aktarılır. Yönetici erişimi ile saldırgan neredeyse istediği her şeyi yapabilir ve sistemi böylesine köklü yerleşmiş bir zararlı yazılımdan kurtarmak oldukça zor hale gelir.

Tordow kötü amaçlı kodlayıcılar tarafından indirilen, tersine mühendisliğe tabi tutulan ve sabote edilen yaygın sosyal medya ve oyun uygulamaları yoluyla yayılıyor. Şu ana kadar istismar edilen uygulamalar arasında VKontakte (Rusya'nın Facebook'u), Pokemon Go, Telegram ve Subway Surfers var. Her ne kadar Google Play ve Apple mağazaları geçmişte virüslü uygulamalara ev sahipliği yapmak ve bunları yaymakla ilgili sorunlar yaşamış olsa da virüslü programlar genellikle bu iki resmi internet sayfasına bağlı olmayan üçüncü taraf sitelerinden dağıtılıyor. Ele geçirilen bu uygulamalar tıpkı orijinal uygulamalar gibi hareket ediyor ancak C2 iletişimleri de dahil olmak üzere gömülü ve şifreli kötü amaçlı işlevler içeriyor. Bu aslında, yönetici erişimi ve indirilebilir Trojan modüllerine erişim sağlayacak bir kötüye kullanım paketi.

Her ne kadar kurbanların çoğu Rusya'da olsa da başarılı hacker teknikleri genellikle dünyanın diğer bölgelerine yayılma eğilimindedir. Kullanıcılar Tordow 2.0 ve benzeri tehditlerden korunmak için güvenlik yazılımlarını güncel tutmalı, talep edilmemiş bağlantı ve eklere karşı tedbirli olmalı ve uygulamaları yalnızca resmi internet sitelerinden indirmeliler. Android telefonlardaki güvenliği sağlamak üzere, Comodo Türkiye ekibinin geliştirmiş olduğu mobil güvenlik uygulaması Savungan, bu alanda kullanılabilecek ücretsiz bir çözümdür.