SAHTE KRIPTO PARA UYGULAMALARI ARASTIRMA RAPORU

Berkay Özenler
CySec Specialist

2023

SAHTE KRIPTO PARA UYGULAMALARI RAPOR

Amaç :

Yapılan araştırmada özellikle hedef alınan rus kökenli web sitelerinden edinilen bilgilere göre 2019 yılında 7-13 haziran tarihi aralıklarında gerçekleşen, two-factor authentication kodlarının ele geçirilmesi için kötü niyetli kişilerin yaptıkları bu sahte, taklit edilmiş BTCTURK, Binance, Huobit, Bybit gibi uygulamaların Android apk yoluyla indirildiği gözlemlenmiştir.Bu two-factor authentication kodlarını uygulama yoluyla bildiriler üzerinden okuyabildikleri bildirilmiştir.Kullanıcıların kripto para cüzdanlarının ve kimlik bilgilerinin çalınmasıyla sonuçlanan bu kötü amaçlı yazılımın yapıldığı araştırılmıştır. Bu araştırmada edinilen bilgilere göre BTCTURK, Binance, Huobit, Bybit adında sahte, gerçeği yansıtmayan uygulamaların piyasaya sürüldüğü ortaya çıkmıştır.Kullanıcıların bilgilerinin ve bakiyelerinin çalındığı bildirilmiştir.
Farklı bir atak yolu olarak kötü niyetli kişilerin piyasaya sürdüğü birden fazla amaca uygunluk gösteren uygulamaların olduğu, bu uygulamaların cihazda bekletilip bayram, özel günler gibi zamanlarda meşru banka ve borsa uygulamalarının logo değiştirme sürecinde olmasından yararlandıkları gözlemlenmiştir.Bu zararlı uygulamalar logo taklidi yaparak firmaların güncel olmayan logolarının taklit edilmesi yoluyla kullanıcıların farkedemedikleri bir anda yanılgıya düşmelerine sebep olmaları ve cüzdan bilgilerini çalıp suç işledikleri gözlemlenmiştir.
Başka bir vakada ise Google Play Store içerisinde gizlenmiş olan "clipper" adlı uygulama, "Metamask" adlı meşru bir hizmeti taklit ederek hedefin ethereum birikimi üzerinde yoğunlaşıp, kimlik bilgilerini ve özel şifrelerini çaldığı bildirilmiştir.

Kapsam :

Kapsam alanı kullanıcılar olmasıyla birlikle kuruluşa maddi ve manevi zararlarının verilmesi, marka değerine büyük bir zarar verilmesi, veri sızıntıları sebebiyle kullanıcıların bilgilerinin açık ortamlara yayılması şeklinde zararlar gözlemlenip, bu tür olayların tekrarlanma ihtimalinde kullanıcıların güven kaybı, kuruluşa korku ile yaklaşması kesindir.

Sorumluluklar :

- Tüm bilgi teknolojisi çalışanlarının siber güvenlik olay müdahalesi hakkında bilgi ve eğitim almış olmaları ve en hızlı şekilde olaya müdahale etmeleri
- Tüm kullanıcılara farkındalık yaratmak gereğiyle önceden bilgilendirilme yapılması ve bu tarz bir saldırıdan nasıl korunacakları hakkında bilgi iletilmesi

Güvenlik Çözümleri

- Zero trust güvenlik modeli uygulanabilir bu güvenlik modeli ile kullanıcıya güven sıfıra düşürülüp, kullanıcı birden fazla denetimden geçilerek erişim sahibi olabilir.
- Just In Time ve Just Enough Access gibi erişim denetimleri uygulanabilir.
- E-mail veya text olarak gelen auth mesajlarının yerine kullanıcının aranması ile kod kullanıcıya sunulabilir.
- MFA kullanılabilir yada yüksek düzey işlem yapan kullanıcılara tamamen biyometrik şekilde uygulamaya girişi sağlanabilir.
- Shadow IT hakkında BT çalışanları bilgilendirilebilir çünkü her zaman suç kullanıcının olmayabilir.
- Mail tarafından phishing alan ve kanan kullanıcılara Office 365 E-mail Protection tavsiyesi verilebilir.
- Defense in depth gibi çok katmandan oluşan güvenlik modelleri uygulanabilir ve geliştirilebilir.

- Siber güvenlik alanında çalışan kişilere deepweb/darkweb gibi networkler hakkında eğitim verilebilir ve kuruluşa yapılacak atakların bilgisi toplanabilir, yeni bir exploit yada kötü amaçl yazılımlar tespit edilebilir ve erkenden güvenlik önlemleri alınabilir.

- SOC kadrosuna özel sertifika eğitimleri verilebilir.

Kaynakça

Exploit.in

Deepweb & Darkweb

Independent & Indyturk.com