Bilgisayar Korsanlarından İlginç Talep

Geçtiğimiz günlerde, ünlü çip üreticisi NVIDIA'nın kurumsal sistemlerine giren bilgisayar korsanları, toplamda 1 terabayt büyüklüğünde gizli belgeleri ele geçirdiğini iddia etti. Kendisine "Lapsus$" adını veren grup, elde ettiği bilgilerden bazılarını yayımlayarak gerçekten önemli bilgilere sahip olduğunu kanıtlamaya çalıştı. Şirkete ait önemli sistem bilgilerinin ve kaynak kodların bulunduğu bu gizli dosyaları yayımlamamak için bilgisayar korsanlarının istediği fidye ise hayli ilginçti. NVIDIA, geçen yıl raflarda yerini alan GeForce RTX 3060 serisi ekran kartlarının kripto para madenciliği için kullanılmasını zorlaştıran LDR adında bir özellik tanıtmıştı. Bu özellik, bilgisayar oyunları için geliştirilen bu ekran kartlarının kripto para madenciliğinde kullanıldığını tespit edince cihazın performansının yarı yarıya düşürülmesini sağlıyor. Diğer yandan, NVIDIA kripto para madenciliği yapmak isteyenler için NVIDIA CMP serisi kartların kullanılmasını istiyor. Yetkili iş ortakları aracılığıyla satılan bu kartlar, en iyi madencilik performansı ve verimliliği için optimize ediliyor. Örneğin, CMD kartlarda ekran çıkışları yerine daha iyi havalandırma sağlayan kanallar bulunuyor ve böylelikle daha az enerji tüketimi gerçekleşiyor. Şirketin böyle bir ayrıma gitmesinin nedeni, kripto para madencilerinin ekran kartlarına yoğun talep göstermesi nedeniyle oyuncuların ekran kartı bulmakta zorlanması. Bu yüzden bilgisayar korsanları şirketin söz konusu özelliği devre dışı bırakmasını istiyor. Taleplerinin karşılanmaması durumunda firma çalışanlarına ait özel bilgilerin de içinde bulunduğu birçok gizli bilginin ifşa edileceğini belirtiyor. Şirketin bilgisayar korsanlarının taleplerini karşılayıp karşılamayacağı bilinmese de bilgisayar korsanlarının yayımladıkları verilere bakılırsa NVIDIA'yı zor günler bekliyor.

Elbette iyi niyetli bilgisayar korsanları da var. Beyaz şapkalı veya etik hacker gibi isimlerle anılan bu kişiler, sistemlerdeki açıkları tespit ettiklerinde yetkili kişileri bilgilendirerek onların önlem almasını sağlıyor. Tree of Alpha takma adlı bir beyaz şapkalı hacker, dünyanın en büyük kripto para pazarlarından biri olan Coinbase'in sistemlerinde bir açık tespit etti. Coinbase kodunda, 50 Bitcoin'i (2 milyon dolar değerinde) 50 SHIB jetonu (10 kuruştan az değerinde) ile takas etmeye izin veren bir hata buldu. Tree of Alpha isteseydi bu açığı kullanarak Coinbase'in güvenlik konusundaki itibarını yerle bir etmekle kalmayıp yüz milyonlarca lira haksız kazanç elde edebilirdi. Ancak bu kişi firma yetkilileriyle gerekli bilgileri paylaşarak güvenlik açığının kapatılmasını sağladı. Firma da ödül olarak beyaz şapkalı hacker'a 250.000 dolar verdi. Bu meblağ aslında büyük olsa da firmayı milyarlarca dolar zarardan kurtaran bu kişiye ödenen ücreti düşük bulan birçok kişi sosyal medyada Coinbase'e tepki gösterdi. Bu alanda, bazı firmaların koyduğu ödüllerin üst limiti 10 milyon doları bulabiliyor.

Öte yandan sıfır dokunuş (*zero-click*) denilen bir hackleme türü, özellikle Android ve IOS akıllı cihaz kullanıcılarını tehdit ediyor. Bu işletim sistemlerindeki bazı açıklardan faydalanan bilgisayar korsanları, hedefledikleri kişilere gönderdikleri bir mesajla, kurbanlar hiçbir işlem yapmasa bile, cihazın kontrolünü ele geçirerek veri çalma, çağrıları dinleme ve kullanıcının konumunu izleme gibi işlemleri gerçekleştirebiliyor. Bunun yanında, sıfır dokunuş ile saldırıya uğramış bir telefonda hiçbir iz kalmayabiliyor. Geçtiğimiz günlerde bir gazetecinin telefonuna bu tür bir yöntemle sızan bilgisayar korsanlarının kullandıkları yazılımda oluşan bir hata sonucu, nasıl bir açıktan faydalandıklarını ortaya koyan bir ipucu elde edildi. Güvenlik uzmanları tarafından incelenen telefondan edinilen bilgiler Apple ile paylaşıldı. Apple hem tespit edilen açıkları kapattı hem de bu tür kötü niyetli yazılımlar geliştiren firmalara dava açtı. Elbette sistemlerde tespit edilemeyen başka bazı açıklar da olabilir.

Bu noktada, böylesi saldırıların ileri düzey uzmanlık gerektirdiği ve maliyetli işler olduğunu da belirtmek gerekiyor. Bir başka deyişle sadece özel olarak hedeflenen önemli kişiler bu tür saldırıların hedefi oluyor. –

https://bit.ly/kripto-korsan
https://bloom.bg/3tTtfIJ