**Basın Bülteni Nisan 2025**

**Siber Saldırganların Yeni Hedefi:**

**Kripto Para Borsaları Tehdit Altında**

*STM, yeni açıkladığı Siber Tehdit Durum Raporu’nda, tarihin en büyük kripto para hırsızlığı “Bybit Hack Vakası”nı mercek altına aldı. Yaklaşık 1.5 milyar dolarlık vurgun, transfer işlemi sırasında fark edilmeyen bir güvenlik açığından kaynaklandı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, 2025 Ocak-Şubat-Mart aylarını içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. Siber güvenlik alanında farkındalık yaratmak amacıyla, STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 7 ayrı konu başlığı bulunuyor. Raporda, tarihin en büyük kripto para hırsızlığı “Bybit Hack Vakası”, insan faktörünün siber güvenliğe olan etkisi ve son dönemde en çok siber saldırı yapan ülkeler gibi güncel ve ilginç konu başlıkları yer alıyor.

Şubat 2025'te kripto dünyası, Dubai merkezli önde gelen borsalardan Bybit'e yapılan siber saldırı ile sarsıldı. Bu saldırı, yaklaşık 400.000 Ethereum tokeninin (yaklaşık 1,5 milyar dolar değerinde) çalınmasıyla tarihin en büyük kripto para hırsızlığı olarak kayıtlara geçti. 21 Şubat 2025'te Bybit, platformunda yapılan rutin bir işlem olan soğuk cüzdandan (offline depolama) sıcak cüzdana (online depolama) bir transfer sırasında bir güvenlik açığının kötüye kullanıldığını tespit etti. Saldırganlar, bu süreci manipüle ederek fonları kendi adreslerine yönlendirdi.

**Kuzey Koreli Hackerlar’dan 5 Milyar Dolarlık Kripto Vurgun**

Saldırının ardından FBI'ın yaptığı soruşturmada, saldırının Kuzey Kore destekli ünlü hacker grubu Lazarus tarafından gerçekleştirildiği ortaya çıktı. Çalınan Ethereum’lar, fonların kaynağını gizlemek için Bitcoin ve diğer dijital varlıklara dönüştürüldü ve binlerce farklı blockchain adresine dağıltıldı. Lazarus, önceki yıllarda da Sony Pictures saldırısı ve çeşitli bankalara yapılan SWIFT saldırıları gibi eylemleriyle gündeme gelmiştri. Blockchain istihbarat şirketi olan TRM Labs’e göre, Kuzey Koreli hackerlar 2017’den bu yana toplamda 5 milyar dolardan fazla kripto para çaldı.

Raporda, bu saldırılara karşı yapılması gerekenlere yer verildi. Buna göre, uzmanlar çoklu imza gerektiren cüzdanlar, düzenli güvenlik denetimleri ve kullanıcı farkındalığını artırmaya yönelik eğitimlerin yaygınlaştırılması gerektiği vurguluyor. Aynı zamanda, borsaların soğuk cüzdan kullanımlarını daha güvenli hale getirmek ve sistemlerini sıkılaştırmak için yeni protokoller geliştirmesi öneriliyor.

**Siber Saldırılarda İnsan Faktörüne Dikkat**

Siber güvenlik zincirinin en zayıf halkası olarak kabul edilen insan faktörünün bilinçsiz veya hatalı davranışları, güvenlik mekanizmalarını aşmak için saldırganlar tarafından aktif olarak kullanılıyor. STM raporunda, siber tehditlerin büyük bir kısmının insan hatalarından kaynaklandığına dikkat çekerek, aşağıdaki önlemlere de işaret etti:

* Güçlü ve benzersiz parolalar kullanılmalı, bu parolalar düzenli olarak değiştirilmelidir.
* Çok faktörlü kimlik doğrulama (MFA) aktif edilmelidir.
* Kimlik avı (oltalama) saldırılarına karşı çalışanlara düzenli eğitimler verilmelidir.
* USB ve taşınabilir medyaların kontrolsüz kullanımı engellenmelidir.
* Çalışanlar saldırı simülasyonları ile test edilmelidir.

**En çok Siber Saldırı ABD ve Hollanda’dan**

STM’nin kendi Honeypot sensörleri (Bal küpü-tuzak sunucular) tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. Ocak-Şubat-Mart 2025 ayları boyunca en çok siber saldırı, %26 ile ABD olurken, %15 ile Hollanda ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Hindistan, Çin, Tayvan, Fransa, Japonya, İngiltere, BAE ve Kenya takip etti.

**Raporun Tamamını Okumak için:** [**https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2025**](https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2025)

**STM Hakkında**

Savunma sanayiine mühendislik, teknoloji ve danışmanlık alanlarında 33 yıldır hizmet veren STM, bugün sahip olduğu temel kabiliyet ve teknolojilerini askeri deniz platformlarından taktik mini İHA sistemlerine, komuta kontrol sistemlerinden siber güvenliğe, büyük veri analitiğinden yapay zekâ uygulamalarına varan stratejik alanlarda kullanarak Türkiye'nin ve dost ülkelerin ihtiyacı olan kritik alanlarda çalışmalar yürütmektedir.

[www.stm.com.tr](http://www.stm.com.tr)