**Basın Bülteni Şubat 2025**

**Siber Tehdit Durum Raporu’nun Yeni Sayısı Yayımlandı:**

 **“Mobil Uygulamalardaki Güvenlik Açıkları Siber Tehditleri Artırıyor"**

*STM, yeni açıkladığı Siber Tehdit Durum Raporu’nda, mobil uygulamalar üzerinden gerçekleştirilen siber saldırıları mercek altına aldı. Kritik bilgilerin güvenli olmayan ortamlarda saklanmasının siber saldırılara zemin hazırladığını vurgulayan STM, hassas verilerin açık metin yerine güçlü şifreleme algoritmalarıyla korunması gerektiğine dikkat çekti.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, 2024 Ekim-Kasım-Aralık aylarını içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. Siber güvenlik alanında farkındalık yaratmak amacıyla, STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 8 ayrı konu başlığı bulunuyor. Raporda, mobil uygulama güvenliğinde dikkat edilmesi gerekenler, NFT satış platformu kullanıcılarını hedef alan oltalama saldırıları, kuantum bilgisayarların geldiği son nokta ve son dönemde en çok siber saldırı yapan ülkeler gibi güncel ve ilginç konu başlıkları yer alıyor.

**Mobil Uygulama Güvenliğinde İhmalin Bedeli**

Son günlerde, bir sigorta şirketi ve hızlı geçiş sistemine ait mobil uygulamalar, yetkisiz erişim nedeniyle kullanıcılara kötü içerikli bildirimler gönderdi. Ayrıca, belirli bir cüzdana bitcoin gönderilmesi talep edildi. Yapılan incelemelerde, uygulamaların mesaj bildirimlerini OneSignal kütüphanesiyle gerçekleştirdiği ve kritik bilgilerin (API Key, App ID gibi) güvenli olmayan şekilde saklandığı tespit edildi.

STM, bu tür saldırılara karşı, mobil uygulama güvenliğinde önem verilmesi gerekenlere dikkat çekti. Buna göre, hassas bilgiler açık metin olarak saklanmamalı ve güçlü şifreleme algoritmaları kullanılmalı. Veriler mümkünse cihazda saklanmamalı, harici depolamadan kaçınılmalı. Tüm iletişim HTTPS protokolü üzerinden yapılmalı. Kullanıcıların yalnızca yetkili oldukları verilere erişebildiği sistemler uygulanmalı. Kritik bilgiler kaynak koda dahil edilmemeli, kod karıştırma teknikleri kullanılmalı. Çok faktörlü kimlik doğrulama ve güçlü parola politikaları uygulanmalı. Güncel olmayan veya zafiyeti olan kütüphaneler kullanılmamalı.

**Dijital Varlıklarda Artan Tehdit: NFT Pazar Yerlerine Oltalama Saldırıları**

Dijital dünyada benzersiz varlıkları temsil eden ve son yıllarda büyük bir yatırım aracı hâline gelen NFT’ler (Non-Fungible Token), siber saldırganların hedefi olmaya devam ediyor. Özellikle oltalama (phishing) saldırıları, sahte NFT pazar yerleri aracılığıyla kullanıcıları tuzağa çekerek kripto cüzdan bilgilerini ele geçirmeyi amaçlıyor. Kullanıcılar, sahte e-postalar veya sosyal medya bağlantıları yoluyla oluşturulan sahte sitelere yönlendiriliyor ve bu sitelerde kripto varlıklarını kaybetme riskiyle karşı karşıya kalıyor. 2020 yılında siber saldırganlar, Barack Obama, Bill Gates ve Elon Musk gibi ünlü isimlerin Twitter hesaplarını ele geçirerek sahte paylaşımlar yaptı. Bu saldırı sırasında, saldırganların cüzdan adresine 110.000 dolar değerinde Bitcoin gönderildi.

Raporda, bu tür tehditlerden korunmak için bazı ipuçlarına yer verildi. E-posta ve bağlantıların kaynağı dikkatlice incelenmeli, resmi görünen paylaşımlara dahi temkinli yaklaşılmalı ve herhangi bir bağlantıya tıklamadan önce güvenilirliği doğrulanmalı. Sosyal medya hesaplarının ele geçirilmesi gibi durumlar da ciddi kayıplara yol açabileceğinden, her adımda dikkatli ve şüpheci olunması dijital varlıkların güvenliği için büyük önem taşıyor.

**En çok Siber Saldırı Estonya’dan**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. Ekim-Kasım-Aralık 2024 ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu)’larına toplam 1 milyon 551 bin saldırı yansıdı. En çok saldırıyı yapan ülke, 270 bin saldırı ile Estonya olurken, 248 bin saldırı ile Bulgaristan ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Rusya, Romanya, ABD, Hindistan, Hollanda, Bolivya, İran ve Mısır izledi.

**Rapora Erişim Linki:** [**https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-2024**](https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-2024)

**STM ThinkTech Hakkında**

STM ThinkTech, savunma–güvenlik ve mühendislik-teknoloji alanlarında var olan bilgi birikimi ve insan kaynağıyla bölgesel ve küresel stratejiler, teknolojik öngörüler, olası senaryolar ve karar destek sistemleri geliştiriyor. Türkiye’nin gelecek vizyonuna uygulanabilir, düşünsel ve pratik katkılar sunan STM ThinkTech, başta savunma olmak üzere havacılık, enerji, ulaştırma, eğitim ve sağlık alanlarında objektif bir yaklaşımla teknoloji odaklı analizler ile özgün çözümler geliştiriyor ve veri işleme yeteceğiyle raporlar yayımlıyor. STM ThinkTech, geliştirmekte olduğu öngörüler ve stratejik çözümler için akademisyenler, diğer düşünce kuruluşları, üniversiteler, yüksek teknoloji üreten firmalar, kamu kurumları ve karar vericilerle iş birliği gerçekleştiriyor.

<https://thinktech.stm.com.tr>

**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)