**Basın Bülteni Ağustos 2022**

**STM BU YILIN İKİNCİ SİBER RAPORUNU AÇIKLADI:**

**“AKILLI TELEFONLAR KAPALIYKEN BİLE SİBER SALDIRIYA UĞRAYABİLİR”**

**STM ThinkTech, bu yılın ikinci çeyreğini kapsayan Siber Tehdit Durum Raporu’nu açıkladı. Akıllı telefonlara yönelik siber saldırıların son dönemde arttığına vurgu yapılan raporda, iPhone cihazların kapalıyken bile siber saldırıya maruz kalabildiğine dikkat çekildi.**

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, Nisan-Haziran 2022 tarihlerini kapsayan yeni Siber Tehdit Durum Raporu’nu açıkladı. 2022’nin ikinci çeyreğini kapsayan raporda, 8 konu başlığı bulunuyor.

**Kapalı bir IOS cihazı siber saldırıya maruz kalabilir**

Akıllı telefonlar; e-posta, sosyal medya, banka hesapları ve adres bilgileri gibi birçok kişisel veri barındırıyor. Son zamanlarda telefonlara yapılan siber saldırılar öne çıkarken, saldırganlar kişisel verileri ele geçirmek için birçok farklı yönteme başvuruyor. Telefon üzerinden yapılan saldırılarda, sosyal medya mesajlarındaki linkler üzerinden ele geçirmeye veya e-posta üzerinden gelen phishing (oltalama) saldırılar üzerinden verilere hızlı bir şekilde erişilmeye çalışılıyor.

Almanya’da iPhone telefonlar üzerinde yapılan bir araştırmaya mercek tutulan raporda, cihaz kapatıldığında bile önemli sistemlerin aktif olmaya devam ettiği vurgulandı. Telefonlarda konum özelliği bulunan uygulamaların aktif olmasının bazı olumsuz durumları beraberinde getirdiği belirtilen raporda, “Örneğin iOS cihazlar kapalıyken yürütülen bir Bluetooth yongası kötü amaçlı yazılım yüklenmesine olanak sağlayabilir. LPM (Low Power Mode) iOS cihazlar kapandığında işlev halindedir. Bir iOS cihaz kapalı olsa bile, kaybolduğunda ‘iPhone’umu bul’ uygulaması etkin durumda olur. Araştırmacılar ‘iPhone’umu bul’un aktif takip cihazı gibi olmasının tehlike oluşturduğunu söylüyor” tespitlerine yer verildi.

**Siber saldırı gerçekleşmeden engellemek mümkün!**

Raporun dönem konusunu ise siber tehdit istihbaratının önemi oluşturdu. Siber tehdit istihbaratı, olası siber güvenlik tehditleriyle ilgili toplanmış verilerin birleştiririlip ilişkilendirme, anlamlandırma ve analiz yapılmasıyla tehditlerin proaktif bir şekilde belirlenmesine ve bunlara karşı savunma mekanizmaları geliştirilmesine olanak sağlıyor. İnternet kullanımının artması ise tehdit aktörlerinin ve bıraktıkları izlerin çoğalmasına neden oluyor. Bu sebeple tehdit istihbaratı verilerinin analizi giderek zorlaşıyor. Raporda, bu yüzden otomatik programlara olan ihtiyacın arttığına dikkat çekilerek, açık kaynak siber tehdit istihbarat platformlarından OpenCTI mercek altına alınıyor. Elde edilen istihbarat bilgileri sayesinde, siber saldırıların daha gerçekleşmeden engellenebilmesi için OpenCTI ve benzeri platformların kurulmasının gerekliliği vurgulanıyor.

**En çok siber saldırı Hindistan ve ABD’den**

STM’nin kendi Honeypot sensörleri tarafından veriler; en çok siber saldırı toplanan ülkeleri de ortaya koydu. 2022’nin Nisan, Mayıs ve Haziran ayları boyunca STM’nin Honeypot sensörlerine toplam 8 milyon 65 bin 301 saldırı yansıdı. En çok saldırı yapan ülke 1 milyon 629 bin saldırı sayısı ile Hindistan olurken, 897 bin saldırı ile ABD ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Türkiye, Rusya, Vietnam, Çin, Meksika, Japonya, Tayvan ve Brezilya izledi. Önceki üç aya göre, gelen saldırı miktarlarında büyük artış gözlemlendiği belirtilen raporda, buna sürekli tehdit aktörlerinin, Rusya-Ukrayna savaşıyla birlikte arttırdıkları aktivitelerin neden olduğu işaret edildi.

Rapora Erişim Linki: <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2022>

**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 çeyrek asırdan uzun bir süredir hizmet veren STM, bugün sahip olduğu temel kabiliyet ve teknolojilerini askeri deniz platformlarından taktik mini İHA sistemlerine, uydu çalışmalarından 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)