**Basın Bülteni Ekim 2022**

**STM 2022’nin Üçüncü Siber Raporunu Açıkladı:**

 **“Hırsızlar, sinyal bozucu sistemlerle araba kilitlerini aşıyor”**

*STM ThinkTech, bu yılın üçüncü çeyreğini kapsayan Siber Tehdit Durum Raporu’nu açıkladı. Raporda hırsızların, anahtarsız araba kilitlerini sinyal bozucu sistemler ile açabildiği tespiti yer aldı. Savunma sanayiindeki platformların siber güvenliğinin de mercek altına alındığı raporda, siber saldırılar ile mühimmatların hedefe gönderilmesinin engellenebileceği, radar sistemlerinin kapatılabileceği ve hatta müttefik unsurların düşman gibi gösterilerek imha edilebileceğine dikkat çekildi.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, Temmuz-Ağustos-Eylül 2022 tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 7 ayrı konu başlığı bulunuyor. Raporda, anahtarsız araba kilidinin hırsızlar tarafından nasıl açıldığı, dünya genelinde en çok siber saldırı yapan ülkeler, savunma sanayiinde platformların siber güvenliği gibi birçok güncel ve ilginç konu mercek altına alındı.

**Hırsızların, araçlardaki uzaktan kumanda tuzakları**

Raporda, anahtarsız araba kilitlerinin işleyiş yapısı ve bu yapıya yönelik saldırılar arasında olan “RollBack” ile “RollJam” saldırılarının teknik analizi yer alıyor. Ucuza temin edilebilen bir sinyal yakalayıcı ve bozucu olan RollJam ile, öncelikle dinleme yapılır ve araç sahibi ilk kilit aç tuşuna bastığında bu sinyal RollJam tarafından yakalanır ve sinyal boğucu (jammer) özelliği kullanılarak araca ulaşması engellenir. Aracın kilidi açılmaz. Kullanıcı ikinci defa kilit açma tuşuna bastığında yine aynı adımlar uygulanır ve sinyal araca ulaşmaz. Ardından saldırgan ilk kilit açma sinyalini RollJam ile yayar ve aracın kilidi açılır. Kullanıcı aracını kullanır ve işi bittiğinde kilitler. Saldırgan ikinci kilit aç sinyalini ele geçirdiği için sahibi yokken aracın kilidini rahatlıkla açabilir.

“RollBack” saldırılarının ilk adımları ise RollJam ile bire bir aynıdır: Araç sahibi tarafından iki defa kilit aç tuşuna basılır ve saldırgan sinyallerden birini daha sonra kullanmak üzere kaydeder. Burada RollJam saldırısından farklı olarak arabanın kilidini açmak için hangi sinyalin gönderildiği önemli değildir ve anahtardan çıkan sinyalin bozulmasına da gerek yoktur, HackRF, yani sinyali yakalayan/ yayan aygıtın sinyali yakalaması yeterlidir. Telsiz frekansını yakalayan aygıt sayesinde aracın kilit açma sinyalleri yakalanır.

**Savunmada platformların siber güvenliği**

Raporun dönem konusunda ise savunma sanayiindeki platformların siber güvenliğine dikkat çekildi. Günümüz savaşlarının önemli bir kısmının artık siber dünyada gerçekleştiğine vurgu yapılan raporda, ülkelerin savunma yeteneklerinin zayıflatılması için sıklıkla siber saldırı düzenlendiği belirtildi. Devletlerin savunma stratejilerinin önemine bağlı olarak platformlara yönelik siber güvenlik saldırılarının arttığı gözlemlenen rapora göre, örneğin dünyada arabalara yapılan siber saldırıları sıklığının 2018’den 2021’e yüzde 225 arttığını tespit edildi.

Türkiye’deki platformların siber güvenlik risklerinin de göz önüne alınarak geliştirilmesi gerektiği kaydedilen raporda, İHA ve SİHA sistemleri (TOGAN, KARGU ve ALPAGU), suüstü ve denizaltı platformları, Muharip İnsansız Uçak Sistemi (MİUS), Milli Muharip Uçak (MMU), MİLGEM, TOGG yerli otomobilin bu anlamda önemli olduğunun altı çizildi.

**“Siber saldırı ile mühimmatın hedefe gönderilmesi engellenebiliyor”**

Savaş uçaklarının görevlerini yerine getirmek için hem bilgi teknolojilerine hem de ilişkili fiziksel altyapılara ihtiyaç duyduğu belirtilen raporda şu ifadelere yer verildi:

“Uçağın mühimmatı hedefe göndermesi için gereken basıncın nasıl düzenleneceği, uçak ekipmanlarının tahmini kullanım ve bakım periyodu, pilota iletilmesi gereken bilgilerin anlaşılabilir ve düzenli şekilde kokpitte nasıl gösterileceği gibi fonksiyonların yerine getirilmesi için hem bilgi teknolojilerine hem de ilişkili fiziksel altyapılara ihtiyaç vardır. Sistemlerin karmaşıklığı göz önüne alındığında gerekli güvenlik önlemleri alınmazsa platformlar siber saldırılara açık durumda kalabilir. Örneğin hafife alınan sosyal mühendislik saldırısı sonucu bir USB ile zararlı yazılım platformlara bulaşabilir, DDOS saldırısı ya da bilgilerin ifşası gerçekleşebilir veya injection saldırıları ile verilerin bütünlüğü bozulabilir. Bu ve benzer saldırıların sonucunda mühimmatın hedefe gönderilmesi engellenebilir, radar sistemlerinin kapatılmasına neden olabilir veya daha kötüsü müttefik unsurların düşman gibi gösterilerek imha edilmesine neden olunabilir.”

**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 Temmuz, Ağustos ve Eylül ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu) sensörlerine toplam 6 milyon 137 bin 330 saldırı yansıdı. En çok saldırı yapan ülke 1 milyon 46 bin saldırı sayısı ile Hindistan olurken, 403 bin saldırı ile ABD ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Vietnam, Rusya, Almanya Meksika, Tayvan, Laos, Çin ve Türkiye izledi.

**Siber saldırganların en çok denediği parolalar**

Raporda, üç aylık dönemde siber saldırganların en çok denediği parolalar da tespit edildi. Birçok yönetim arayüzünün standart olarak kullandığı “admin, root, password, 12345” gibi parolaların siber saldırganlar tarafından en çok denendiği gözlemlendi. Uzmanlar, bu parolaların test süreci tamamlanır tamamlanmaz değiştirilmesi ve 12-16 karakterli, özel karakter içeren parolalarla güncellenmesi gerektiğini kaydetti.

Rapora Erişim Linki:

**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)