**Basın Bülteni Şubat 2023**

**Son Yılların Popüler Siber Tehdidi:**

**Fidye Yazılım Saldırıları Yüzde 62 Arttı!**

*STM yeni açıkladığı Siber Tehdit Durum Raporunda, son yılların en kazançlı siber suçlardan biri haline gelen fidye yazılım saldırılarının, dünya çapında yüzde 62 arttığına dikkat çekti. Raporda, fidye yazılımından korunmak için izlenilmesi gereken yol haritasına yer verilirken, deniz platformları ve silah sistemlerine yönelik yapılan siber güvenlik saldırıları da mercek altına alındı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, Ekim-Aralık 2022 tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 9 ayrı konu başlığı bulunuyor. Raporda, deniz platformlarında ve silah sistemlerinde siber güvenliğin önemi, son yılların en popüler siber tehditlerinden fidye yazılımları, siber dünyada kırmızı ve mavi takımların ortaklaşa çalışmasından doğan “mor takım” gibi birçok güncel ve ilginç konu yer alıyor.

**Fidye Yazılım Hizmeti Karaborsada Sunulmaya Başladı**

Son yıllarda yükselişte olan siber suçların, 2025 yılına kadar dünyaya yılda 10,5 trilyon dolara mal olacağı tahmin ediliyor. STM yayımladığı son siber raporda, en kazançlı siber suçlardan biri olan fidye saldırılarına dikkat çekerken, siber güvenlik alanında saldırganlar için ciddi bir gelir kaynağına dönüşen fidye yazılım saldırılarının 2019 ile 2020’de dünya çapında yüzde 62 arttığını vurguladı. Saldırganların, fidye yazılımlarını çok çeşitli yöntemlerle cihazlara bulaştırdığına değinilen raporda, saldırı boyutlarının genişlediği ve birçok önemli firma ve kurumun bu saldırılara maruz kaldığı kaydedildi.

Birçok kuruluşun, verilerini daha iyi korumak için gerekli yatırımı yapmak yerine, ele geçirilen verilerini geri almak için ödeme yapmayı tercih ettiği belirtilen raporda, bunun da suçluları daha fazla motive ettiği ve “Fidye Yazılım Hizmeti” (Ransomware as a Service-RaaS) adı altında yeni bir siber suçun türediğinin altı çizildi. Raporda, “Daha da endişe verici olan, fidye yazılımının artık metalaşarak Fidye Yazılım Hizmeti olarak karaborsada sunulur hâle gelmiş olmasıdır. Programlama becerisi olmayan kişilerin aktif saldırganlar hâline gelmesini ve fidye yazılımı ekonomisine dâhil olmasını sağlayan RaaS bu kazançlı alanı daha da genişletti. Bu yazılımların hızlı büyümesine darknet pazar yerleri temel olurken, blok zinciri teknolojisindeki yeni gelişmeler de suçluların fidye yazılımı oluşturmasını ve paylaşmasını kolaylaştırıyor” ifadelerine yer verildi.

**Fidye Yazılımlarından Korunma Yöntemleri**

Raporda, fidye yazılımından korunmak için yapılması gerekenler ise şu şekilde sıralandı:

“Tehlike oluşturacağını düşündüğümüz url, e-posta gibi bağlantılardan uzak durmalı, e-posta girişinde kimlik doğrulması yapılmalıdır. Önemli olduğu düşünülen dosyalar yedeklenmeli, güncel antivirüs programları ve güçlü spam filtreleri kullanılmalıdır. Güncellemeler sıklıkla yapılmalı ve kişisel bilgilerin paylaşılmasından kaçınılmalıdır. Bilinen kara listeye eklenen IP’lerin engellenmesi de sağlanabilir.”

**Deniz Platformlarında Siber Güvenlik**

Deniz platformlarına yapılan siber saldırılar da raporda detaylıca ele alındı. Bir deniz platformunun yerleşik bilgi teknolojisi ve operasyonel teknoloji sistemlerinin, karadaki sistemler kadar kolay hack’lenebileceği belirtilen raporda, bu tür güvenlik ihlallerinin gemilerin, limanların, deniz tesislerinin ve diğer unsurların emniyet ve güvenliğine önemli zararlar verebileceğine dikkat çekildi.

Saldırganların kötü amaçlı yazılımları kullanarak, gemilerin otomatik tanımlama sistemi, elektronik harita gösterim ve bilgi sistemi (ECDIS), küresel konumlanma sistemi (GPS), makine daireleri ve radarlarına siber saldırı yapabildiğine değinilen raporda, bu saldırıların gemilerin kaçırılmasına, seyir sistemlerinin devre dışı bırakılmasına veya yanlış yönlendirilmesine, iletişimin kesilmesine, platform verilerinin imhası ve çalınmasına yol açabileceği tespitinde bulunuldu.

**200’den Fazla Geminin Seyir Sistemine Siber Saldırı**

Geçmişte deniz platformlarına yapılan çeşitli saldırıları sıralayan rapora göre, 2010 yılında Güney Kore’den Güney Amerika’ya götürülen bir petrol platformunun sistemleri zararlı yazılım kullanılarak çökertildi. Platformun arızalarının giderilip tekrar operasyona başlaması 19 gün sürdü. Yine 2012 yılında, uzaktan yapılan müdahale sonucu, yanıltıcı ve karıştırıcı sinyaller ile 200’den fazla açık deniz gemisinin GPS (Uydu Konumlama) cihazları bozularak açık deniz seyirlerinin zorlaştığı raporda yer aldı. 2020 yılında, uluslararası deniz taşımacılığı firması, kötü amaçlı yazılım saldırısına maruz kaldı ve şirket saldırıyı kontrol altına almak için sunucularını bir kaç gün devre dışı bırakmak zorunda kaldı.

**Dijitalleşme Riskleri de Beraberinde Getiriyor**

Raporda, ABD’de daha önce yapılan bir araştırmanın, silah sistemlerinin bilgisayarlaşmasına yönelik çarpıcı istatistiğine de yer verildi. Buna göre, 1960 yılında F-4 uçağı için yüzde 8 olan sistem işlevlerinin yazılımla karşılanma oranı, 1982’de F-16 uçağı için yüzde 45’e, 2000 yılında F-22 uçağı için yüzde 80’e yükseldi. Sistemlerdeki dijitalleşmenin, siber saldırı olasılığını da artırdığına vurgu yapıldı.

**En Çok Siber Saldırı Almanya ve Hindistan’dan**

STM’nin kendi Honeypot sensörleri tarafından veriler; en çok siber saldırı toplanan ülkeleri de ortaya koydu. 2022’nin Ekim, Kasım ve Aralık ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu) sensörlerine toplam 3 milyon 777 bin saldırı yansıdı. En çok saldırı yapan ülke 451 bin saldırı sayısı ile Almanya olurken, 423 bin saldırı ile Hindistan ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Rusya, ABD, Türkiye, Çin, Hollanda, Vietnam, Moldova ve Tayland izledi. Saldırganların en çok denediği parolalar ise admin, root, password gibi kelimeler oldu.

**Bilgi ve İletişim Güvenliği Rehberi’ne Yakından Bakış**

Raporun dönem konusunda ise, kamu kurumlarında ve kritik altyapı hizmetleri sağlayan özel sektör şirketlerinde uygulanacak bilgi ve iletişim güvenliği kurallarını içeren Cumhurbaşkanlığı Dijital Dönüşüm Ofisi BİG Rehberi Uyumluluk Denetimi’nin detayları ele alındı.

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