**Basın Bülteni Nisan 2022**

**STM 2022’NİN İLK SİBER RAPORUNU AÇIKLADI:**

**Rusya, Ukrayna’ya Siber Saldırılarını Yüzde 196 Artırdı**

*STM ThinkTech, bu yılın ilk çeyreğini kapsayan Siber Tehdit Durum Raporu’nu açıkladı. Ukrayna-Rusya savaşındaki siber operasyonların ele alındığı raporda, Rusya’nın Ukrayna askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 artırdığı vurgulandı. Ukrayna’nın ise, Rusya’daki askeri ve kritik altyapı hedeflerine saldırmak için siber güvenlik uzmanları ordusu oluşturduğuna dikkat çekildi.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin Teknolojik Düşünce Merkezi “ThinkTech”, Ocak-Mart 2022 tarihlerini kapsayan yeni Siber Tehdit Durum Raporu’nu açıkladı. 2022’nin ilk üç ayını kapsayan raporda, 7 konu başlığı bulunuyor.

**Rus istihbaratı, Ukrayna savunma sitelerine saldırdı**

STM ThinkTech, son aylarda dünya gündemini en çok meşgul eden, Ukrayna-Rusya savaşındaki siber operasyonları mercek altına aldı. Raporda, iki tarafın birbirine karşı gerçekleştirdiği siber saldırılar analiz edildi.

Buna göre, Rusya 24 Şubat’ta Ukrayna’da başlattığı işgalin ilk günlerinde, Ukrayna askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 arttırdı. Rus askeri istihbaratı GRU, 2022’nin Şubat ayı başlarında Ukrayna web sitelerine karşı bir dizi DDoS (Distributed Denial of Service) saldırısı başlattı. Saldırılar Ukrayna bankacılık ve savunma web sitelerini hedef aldı. Rus taraftarı grupları malware-as-a-service platformu olan “DanaBot” aracını kullanarak, Ukrayna Savunma Bakanlığı web sitelerine yönelik DDOS saldırılarına devam etti. Rusya, 24 Şubat 2022’de IsaacWiper adlı bir wiper yazılımıyla Ukrayna hükümet sistemlerine saldırdı. Isaac-Wiper saldırılarının yanı sıra HermeticWiper ve CaddyWiper saldırıları da tespit edildi.

**Oltalama atak ile Ukrayna Ordusu hedef alındı**

Ukrayna’nın Bilgisayar Acil Müdahale Ekibi, Belarus devlet destekli hacker grubu UNC1151’i toplu bir kimlik avı saldırısında askeri personelinin e-posta hesaplarını hack’lemeye çalışmakla suçladı. Hacker’lar ele geçirdikleri hesaplarla, daha fazla kötü amaçlı e-posta gönderdi.

**Ukrayna’dan siber uzayda benzersiz strateji**

Rusya’nın saldırılarına karşılık olarak Ukrayna, uluslararası duyarlılığı harekete geçirmeye ve Rusya’daki askeri ve kritik altyapı hedeflerine saldırmak için bir siber güvenlik uzmanları ordusu oluşturmaya çalışarak siber uzayda benzersiz bir strateji izledi.

Anonymous grubu, 1 Mart’ta Rus devletine karşı “savaş ilan” etti. Rus devletine ait birkaç televizyon kanalını hack’lediğini iddia eden Anonymous, 10 Mart’ta, medyayı izlemekten ve sansürlemekten sorumlu Rus ajansı Roskomnadzor’un sistemlerini ihlal ettiğini duyurdu. Grup 360.000’den fazla dosya sızımına sebep oldu.

IT Army of Ukraine birkaç Rus bankasının web sitelerini, Rus elektrik şebekesini ve demiryolu sistemini hedef aldı ve stratejik öneme sahip diğer hedeflere yönelik yaygın DDoS saldırıları başlattı. Belarus Siber Partizanları, Belarus demiryollarına atak gerçekleştirdi ve bilet satın almak için kullanılan web sitelerini çökertti.

**En çok siber saldırıyı Hindistan ve ABD yaptı**

STM’nin kendi Honeypot sensörleri tarafından veriler; bu yılın ilk aç ayında en çok siber saldırı toplanan ülkeleri de ortaya koydu. 2022’nin Ocak, Şubat ve Mart ayları boyunca STM’nin Honeypot sensörlerine toplam 6 milyon 137 bin 330 saldırı yansıdı. En çok saldırı yapan ülke 1 milyon 308 bin saldırı sayısı ile Hindistan olurken, 632 bin saldırı ile ABD ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Vietnam, Rusya, Çin, Meksika, Pakistan, İran, Japonya ve Brezilya izledi. Rusya’nın bu dönemde saldırı sayısını büyük bir oranda artırdığı ve 467 bin saldırı gerçekleştirdiği kayıtlara geçti. Raporda bu artışın sebebi olarak, Rusya’nın Ukrayna’yı işgal girişimiyle birlikte, Rus tehdit aktörlerinin eylemlerini artırması gösterildi.

**Akıllı saatlerde kimlik doğrulama yöntemi**

IoT sistemlerinin gelişmesi ve giyilebilir teknolojilerin popülerleşmesiyle birlikte en çok tercih edilen ürünlerden biri hâline gelen akıllı saatlerin gün geçtikçe akıllı telefonlara olan bağımlılıklarının azalması, bu cihazların yeni yetenekler kazanmasını getiriyor. Raporda buna örnek olarak “Akıllı Saatler için Geliştirilen Kullanıcı Dostu Kimlik Doğrulama Yöntemi” konusunu detaylıca incelendi.

**Rapora Erişim Linki:** [**https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2022**](https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2022)

Türk savunma sanayii için yol gösterici nitelikte analiz ve raporlara imza atan STM ThinkTech, geçen ay savunma sanayii ve diplomasi bağlamında Ukrayna-Rusya savaşını ele alan bir odak toplantı da gerçekleştirmişti.

**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 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**](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)