**Basın Bülteni Ekim 2021**

**STM YENİ SİBER TEHDİT DURUM RAPORUNU AÇIKLADI**

**BİLGİSAYAR OYUNLARINDA HİLE TEHLİKESİ:**

**HİLE GÖRÜNÜMLÜ ZARARLI YAZILIMLARLA, BİLGİLERİNİZ ÇALINABİLİR!**

**Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin Teknolojik Düşünce Merkezi “ThinkTech”, Temmuz-Eylül 2021 tarihlerini kapsayan yeni Siber Tehdit Durum Raporu’nu açıkladı. Raporda, bilgisayar oyunlarında başvurulan oyun hilelerinin, zararlı yazılım üreticilerini harekete geçirdiği ve oyun hilesi görünümünde zararlı yazılımlar üretilmeye başlandığına dikkat çekildi. Veri merkezleri arasındaki transferlerde kullanılan kriptoloji tekniklerinin de ele alındığı raporda, bir Wi-Fi güvenlik standardı olan WPA3 mercek altına alındı.**

Bu yılın üçüncü çeyreğini kapsayan STM ThinkTech’in raporunda 9 konu başlığı bulunuyor. İki zararlı yazılımın analizinin yer aldığı raporda, bilgisayar oyunlarındaki hile yöntemlerinin getirdiği tehlikeler incelendi.

**Hile görünümlü zararlı yazılım, kredi kartı bilgilerine kadar erişebiliyor**

Bilgisayar oyunlarının popülerleşmesiyle bu oyunlarda başvurulan oyun hileleri de oldukça yaygın hâle geldi. Raporda, kazanma hırsıyla bu tür hilelere kapılabilen kurbanlardan faydalanmak isteyen zararlı yazılım üreticilerinin, oyun hilesi görünümünde zararlı yazılımlar üretmeye yöneldiğine dikkat çekildi. Henüz yeni sayılabilecek bir bilgisayar oyunu olan VALORANT’da da bu tarz yazılımlara sıkça rastlanıldığı belirlenirken, STM Sandbox kum havuzunda yapılan statik analiz sonucunda; zararlının 32/64 bit Windows işletim sisteminde çalıştırılabilir olduğu, virustotal etiketlerinin zararlının bir truva atı türevi olduğu ve komut kontrol sunucuyla iletişim kurmaya çalıştığı tespit edildi.

Kurban bilgisayardaki birçok veriyi toplayan bu yazılım, topladığı verileri kategorilere ayırdıktan sonra bir zip dosyası oluşturarak, Telegram sohbet uygulamasında oluşturduğu bir bot aracılığıyla, zararlı yazılımın sahibine özel mesaj olarak gönderiyor. Bu yolla, kurban bilgisayarın sistem bilgileri, yüklü sohbet ve e-posta bilgileri, yüklü web tarayıcılardaki bilgiler (kayıtlı parolalar, kredi kartları, indirme geçmişi vb.), çeşitli coin cüzdan bilgilerinin ele geçirildiği tespit edildi. Zararlı yazılımın, kurban bilgisayar bilgilerini toplama işlevinin yanı sıra her 10 saniyede bir, Telegram üzerinden gelen mesajları okuyarak aldığı komutları uyguladığı görüldü. Raporda, zararlı yazılımın görev yöneticisinde işlemler arasında rastlanılması durumunda, işleminin durdurulması ve dosya konumlarına gidilerek silinmesi gerektiği vurgulandı.

**Veri merkezleri arası veri kriptolojisi**

Raporda, veri merkezleri arasındaki veri eşitleme işlemlerinin daha güvenli yapılabilmesi için kullanılan maskeleme teknolojileri de ele alındı. Uzak şubeler veya veri merkezleri için akla ilk gelen veri maskeleme teknolojisinin IPSEC VPN (L3-IP Crypto) olduğu belirtilen raporda, veri merkezleri arasında kurulan iletişim altyapısının 40Gbps hızının üzerinde olması durumunda, alternatif teknolojiler (L1-Link Crypto, MACsec, veya donanımsal Crypto L2-Link, L3-IP Crypto) detaylıca incelendi.

**WPA3 ile gelen yeni güvenlik yetenekleri**

Bir Wi-Fi güvenlik standartı olan WPA3 ile gelen yeni güvenlik yetenekleri de raporda mercek altına alındı. WPA3 ile kablosuz ağ yönetim paketlerinin artık şifreli olarak iletildiğine vurgu yapılan raporda, böylece kablosuz ağ sızma testi eğitimlerinde ilk öğretilen deauth paketleri kullanılarak kablosuz ağa bağlı olan kullanıcıların kablosuz ağdan kopmasının ve yeniden bağlanmak için istek yaptıklarında parola hashlerinin çalınmasının önüne geçildiği belirtildi.

STM ThinkTech’in raporunda dönem konusu olarak, bilgi işlem cihazlarının belleğini hedef alan ve bellek içinde faaliyet gösteren “Praying Mantis” isimli, APT (Gelişmiş Kalıcı Tehdit) grubunun analizi yer aldı. İsmi bilindik birçok organizasyonu hedef alan ve internete açık sunucuları sömürerek organizasyonların ağlarını açığa çıkaran bu tehdit aktörlerinin, hangi yolları izlediği raporda aktarıldı.

**Rapora Erişim Linki:** <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-2021>

**STM ThinkTech Hakkında**

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.

**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 uydu çalışmalarına, siber güvenlikten büyük veri analitiği ve 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)