**Basın Bülteni Nisan 2023**

**STM’den “ChatGPT” Uyarısı:**

**“Hacker’lar, Siber Saldırılarda ChatGPT Kullanıyor”**

*STM yeni açıkladığı Siber Tehdit Durum Raporunda, tüm zamanların en hızlı büyüyen uygulaması olan ChatGPT’nin hacker’lar tarafından siber saldırılarda kullanıldığına dikkat çekti.* *Raporda, siber saldırganların ChatGPT aracılığıyla oltalama e-postası taslakları ve dezenformasyon amacıyla yalan içerik ürettiği tespiti yer alırken, ChatGPT’nin çeşitli programlama dillerinde çalıştırılabilir kodlar üretmesinin, siber suçlara giriş eşiğinin düşmesine neden olacağı vurgulandı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, Ocak-Mart 2023 tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 8 ayrı konu başlığı bulunuyor. Raporda, Şubat ayında yaşanan depremden faydalanılarak yapılan oltalama tuzakları, siber saldırılarda ChatGPT’nin kullanımı, siber güvenlikte kadının rolü, dronelarda siber güvenlik gibi birçok güncel ve ilginç konu başlıkları yer alıyor.

**Deprem Bağışlarına Oltalama Saldırısı**

Türkiye’de 6 Şubat’ta meydana gelen depremler sırasında, hacker’ların harekete geçtiği ve oltalama saldırıları yaptığı STM’nin yeni siber raporunda mercek altına alındı. Siber saldırganların depremzedelere yardım amaçlı bağış toplayan sitelerin benzerlerini yaparak, para toplamaya çalıştığı ve bununla da yetinmeyerek, resmi bağış sitelerine benzeyen arayüzler kullanarak kimlik avı gerçekleştirdiği belirtildi. Buna göre, sahte web sayfaları, inandırıcılığı artırmak için isimlerini AFAD, Kızılay gibi resmi kurumlara ve AHBAP, TOG Vakfı gibi sivil toplum kuruluşlarına benzetti. AHBAP sivil toplum kuruluşuna kimlik avı ve bağış toplama amaçlı 400 bin siber saldırı gerçekleşti.Raporda bu tarz oltalama saldırılardan korunmak için bilinçli hareket edilmesinin önemine vurgu yapılarak, “URL’nin ‘https’ ile başladığından ve kilit simgesinin olduğundan emin olunmalı, web sitesi ve domain resmi olup olmadığı kontrol edilmelidir” denildi.

**Siber Saldırılarda ChatGPT Nasıl Kullanılıyor?**

Piyasaya sürülmesinden sonraki iki ay içinde dünya çapında 100 milyon kullanıcıya ulaşarak, tüm zamanların en hızlı büyüyen uygulaması olan ChatGPT’nin siber güvenlik boyutu da raporda dönem konusu olarak analiz edildi. OpenAI tarafından geliştirilen ve kullanıcılar tarafından matematik problemleri çözmek, makale yazmak, kod yazmak gibi çeşitli amaçlarla kullanılan bu sohbet robotunun, günlük ziyaret sayısının Şubat ayında 45 milyonu bulduğu belirtildi.

Kullanıcılar ChatGPT’nin yeteneklerini keşfetmeye devam ederken birçok siber güvenlik uzmanı bu teknolojinin potansiyel kötü kullanımına dair endişelerini dile getirmeye başladı. 1.500 bilişim ve siber güvenlik uzmanı arasında gerçekleştirilen bir ankette, katılımcıların yüzde 51’i ChatGPT’nin önümüzdeki 12 ay içinde başarılı bir siber saldırı gerçekleştirilmesinden sorumlu olacağını düşünüyor. Raporda, siber saldırganların ChatGPT aracılığıyla fark edilmesi zor, başarılı oltalama e-postası taslakları ürettiği, otomatik metin üretme konusundaki performansı ile, ChatGPT’nin dezenformasyon amacıyla da kullanıldığı kaydedildi. Yapılan bir çalışmada, yalan haber veritabanlarından seçilen 100 hikâye için, ChatGPT’den içerik yazmayı istendiği, sistemin ise 100 hikâyeden yalnızca 20 tanesinin yanlış bilgi içerdiğini tespit ederek içerik üretmeyi reddettiği, ancak geri kalan 80 tanesi için yalan bilgi içeren haber ürettiğini gösterdi. ChatGPT’nin çeşitli programlama dillerinde çalıştırılabilir kodlar üreterek, siber güvenlik tecrübesi olmayan kişilerin bile zararlı yazılım oluşturabilmesine ve dolayısıyla siber suçlara giriş eşiğinin düşmesine sebep olduğu da vurgulandı.

**Siber Saldırıların Yeni Hedefi: Drone’lar**

STM’nin önemli faaliyet alanlarından olan taktik mini iha sistemleri ve drone’ların siber güvenliği de raporda ele alınan bir diğer konu başlığı oldu. Raporda, birçok alanda kullanılan drone’ların maruz kalabileceği siber saldırılara ve drone’lardaki yaygın kullanımın, bu platformlara siber saldırıları artıracağına dikkat çekildi. Olası bir güvenlik zafiyetinden faydalanan siber saldırganların, drone’lara kötü amaçlı yazılım enjekte edebileceği ve bu sayede kontrolü ele geçirebileceği uyarısı yapıldı. Örneğin, “Wifi Jamming” yolu ile hacker’lar, erişim noktası ile drone’u kontrol eden cihaz arasında bir kimlik doğrulama işlemi göndererek drone’u ele geçirebilir. Saldırgan sahte sinyaller göndererek veya sinyal bozarak İHA üzerinde kontrol sağlamasına olanak tanıyan RF (Radyo Frekansı) veya GPS sahteciliğine kadar sistemi manipüle edebilir. Raporda bu saldırıların önüne geçilmesi için sistem bütünlüğü, gizlilik, bilgi bütünlüğü, erişim gibi konularda neler yapılması gerektiği kaleme alındı.

**Siber Güvenlikte Kadının Rolü**

Raporda, siber dünyadaki cinsiyet dağılımına da yer verildi. Siber güvenlik ve bilişim teknolojileri (BT) sektöründe erkek rolünün baskın olduğu kanısına dikkat çekilen raporda, BT kuruluşlarının yüzde 37’sinin daha çok sayıda kadın çalışan çekmeye yönelik resmi prosedüre sahip olduğu belirtildi. Siber suçluların demografisine bakıldığında ise, siber suç forumlarına katılanların yaklaşık yüzde 30’unun kadın olduğu; her 10 siber suçludan üçünün kadın olduğu bilgisi yer aldı.

**Yazılım Tedarik Zinciri Saldırılarında Yüzde 650’lik Rekor Artış**

Bilişim dünyasında 2020’den bu yana hızla artan, yazılım tedarik zinciri saldırıları, STM’nin yeni siber raporunda öne çıkan konulardan biri oldu. Sistemlerin uzun süre işlev dışı kalmasına, kurum, şirket hatta ülkelerin para ve itibar kaybına neden olan bu saldırıların 2021 yılında yüzde 650’lik bir rekor artış gösterdiğinin altı çizildi. Hem üreticilerin hem de tedarik eden kurumların, yazılım tedarik zinciri saldırılarından korunmak için nasıl bir yol izleyeceği de raporda detaylandırıldı.

**En Çok Siber Saldırı Rusya’dan**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. 2023’in Ocak, Şubat ve Mart ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu) sensörlerine toplam 4 milyon 365 bin saldırı yansıdı. En çok saldırı yapan ülke 481 bin bin saldırı sayısı ile Rusya olurken, 394 bin saldırı ile Hollanda ikinci sırada yer aldı. Bu ülkeleri sırasıyla; ABD, Çin, Hindistan, Vietnam, Almanya, Türkiye, Romanya ve Güney Kore izledi.

**Rapora Erişim Linki: <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2023>**

**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)