**Basın Bülteni Mayıs 2024**

**STM’den Fidye Yazılım ve İnternet Dolandırıcılığına Karşı Uyarı**

*STM, yeni açıkladığı Siber Tehdit Durum Raporu’nda, küresel ekonomi ve bankacılığı hedef alan LockBit fidye yazılım saldırılarında ciddi bir artış yaşandığına dikkat çekerek, kurum ve kullanıcıların alması gereken önlemleri sıraladı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, 2024 Ocak-Şubat-Mart tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. Siber güvenlik alanında farkındalık yaratmak amacıyla, STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 11 ayrı konu başlığı bulunuyor. Raporda, küresel ekonomi için büyük bir siber tehdit olan LockBit fidye yazılımı, VR gözlükler üzerinden çalınan veriler, IOT cihazlara yapılan siber saldırılar, oltalama ve internet bankacılığı dolandırıcılığı gibi güncel ve ilginç konu başlıkları yer alıyor.

**26 Milyar Kullanıcı Verisi Sızdırıldı**

Raporda, Ocak 2024’te Twitter, LinkedIn, Dropbox gibi sosyal medya sitelerinde “The Mother Of All Breaches” olarak isimlendirilen veri sızıntısında yaklaşık 26 milyar kullanıcının verisinin sızdırıldığı aktarıldı. Buna göre, ABD, Brezilya, Almanya, Filipinler ve Türkiye’nin de aralarında bulunduğu çok sayıda ülke bu sızıntıdan etkilendi. MySpace (360M), Twitter (281M), Linkedin (251M), Adobe (153M), Dropbox (69M), Telegram (41M) verilerinin çalındığı tespit edildi.

**VR Gözlük Kullanıcıları Siber Saldırıya Maruz Kalabilir**

Son dönemde kullanımı giderek artan Sanal Gerçeklik (VR) gözlüklerin, siber saldırıya nasıl maruz kaldığı da raporda ele alındı. Inception adı verilen yöntem ile saldırganların, yapay zekâ araçlarını kullanarak gerçekçi simülasyonlar oluşturup, VR’de ses ve görselleri gerçek zamanlı olarak değiştirebildiği ve bu esnada kullanıcının çevrimiçi etkileşimlerinin kaydedildiği ortaya kondu. Inception saldırıları üzerinden, kullanıcıların kişisel bilgileri ve finansal verileri ele geçirilerek, sahte banka uygulamaları veya kimlik avı sitelerinin oluşturulabildiği belirtilen raporda, siber casusluk ve propaganda amaçlı da bu saldırılardan faydalanıldığının altı çizildi. Raporda, bu saldırılardan korunmak için, geliştirici mod kullanımının kısıtlanması, güvenlik yazılımlarının kullanılması, kimlik doğrulamalarının aktif yapılması ve çeşitli ağ güvenlik çözümleri önerisinde bulunuldu.

**Küresel Ekonomi ve Güvenliğe Karşı Yükselen Tehdit: LockBit Fidye Yazılımı**

Kritik altyapı tesislerinden sağlık kuruluşlarına, eğitim kurumlarından kamu kuruluşlarına kadar geniş bir yelpazede hasara yol açan LockBit fidye yazılımı saldırıları; veri kaybı ve hasarına, sistem kesintileri ve gecikmelerine, finansal kayıp ve itibar zedelenmelerine yol açarak, küresel ekonomi ve güvenlik için ciddi bir tehdit oluşturuyor. LockBit’in arkasındaki grubun Rusya kökenli olduğu ve grubun, fidye ödemelerini Bitcoin ve Monero gibi kripto para birimleri aracılığıyla talep ettiği biliniyor. Saldırganlar, e-posta, sahte web sitesi, sosyal medya mesajları ile kullanıcıları kötü niyetli bağlantılara yönlendirerek veya sistemlerin güvenlik açıklarından faydalanarak bilgisayarlara sızabiliyor. Kurbanların bilgisayarlarındaki dosyaları şifreleyerek, onları geri yüklemek için fidye talep eden LockBit, yazılımı diğer saldırganlara kiralayabiliyor ve onlar da bu yazılımı kullanarak saldırıları genişletebiliyor.

Bu saldırı örneklerine yer verilen raporda, Aralık 2023’te, LockBit ransomware grubunun, Portekiz limanlarını hedef aldığını ve 1,5 milyon dolar fidye talep ettiğini belirtti. Toronto’daki SickKids Hastanesi de LockBit saldırısına uğradı ve bu durum hastanenin bilgisayar sistemlerinin bozulmasına ve hastaların tedavisinde gecikmelere neden oldu. 2024’ün Ocak ayında ise LockBit, dünyanın en büyük otomobil üreticilerinden birisine saldırdı ve üretimde aksamalara yol açtı. Rapora göre, LockBit’e karşı korunmak için; güvenlik farkındalık eğitimleri artırılmalı, siber güvenlik politikaları ve prosedürleri eksiksiz uygulanmalı, güvenlik duvarı ve antivirüs yazılımları daima güncel tutulmalı, veri yedekleme yapılmalı ve siber güvenlik sigortaları tercih edilmeli.

**İnternet Dolandırıcılığından Korunmanın Yolları Neler?**

STM’nin siber güvenlik uzmanları raporda, günlük hayatta phishing (oltalama) ve internet bankacılığı dolandırıcılığı gibi tehditlerden korunmak için şu yöntemleri sıraladı:

* Bilgilerinizi paylaşmak için gelen şüpheli e-posta veya bağlantılara tıklamaktan kaçının.
* Bilgilerin her zaman güvenilir kaynaklardan geldiğinden emin olun.
* Bankacılık işlemleri için güvenli ve güvenilir internet bağlantıları kullanın.
* Açık veya şüpheli ağlardan kaçının ve sadece güvenli web sitelerine erişin.
* Banka hesaplarınızı ve diğer çevrimiçi hesaplarınızı güçlü ve benzersiz şifrelerle koruyun.
* Şifrelerinizi düzenli olarak değiştirin ve iki faktörlü kimlik doğrulamayı etkinleştirin.
* Bankanıza herhangi bir şüpheli faaliyeti hemen bildirin.
* Hesap geçmişinizi düzenli olarak kontrol ederek, şüpheli işlemleri tespit etmeye çalışın.

**Siber Savaşın Modern Savaştaki Önemi**

Raporda, Amerikan uydu şirketi Viasat’a yapılan siber saldırı da mercek altına alındı. Rusya’nın Ukrayna’ya yönelik saldırısının başlamasından sadece bir saat önce gerçekleşen siber saldırıda, Ukrayna askeri güçlerinin, Viasat’ın hizmetlerine dayandırdıkları komuta ve kontrol sistemlerini önemli ölçüde etkiledi. Viasat’ın KA-SAT uydu geniş bant servisine karşı gerçekleştirilen siber saldırıda SATCOM modemleri hedef alındığı, saldırıda kullanılan zararlı yazılım ile Viasat modem ve yönlendiricilerindeki tüm verilerin silinerek, cihazların kalıcı olarak devre dışı bırakılmasına neden olduğu belirtildi. Saldırı, aynı zamanda Ukrayna dışında Avrupa’nın orta kesimlerinde bulunan binlerce internet kullanıcısını ve rüzgâr çiftliklerini de etkiledi. Raporda, Rusya’nın koordineli ve yıkıcı siber saldırısının, siber saldırıların modern savaşta nasıl aktif ve stratejik bir şekilde kullanıldığına dikkat çekilerek, “Saldırının, konvansiyonel savaş operasyonlarıyla eşzamanlı olarak yürütülmesi, siber savaşın modern savaşta giderek artan bir rol oynamaktadır” tespitinde bulunuldu.

**IoT Cihazlardaki Siber Zafiyetler**

Raporun dönem konusunda ise “Açık Kaynak Kod Güvenliği” ve “IOT Cihazların Siber Güvenlik Regülasyonları” analiz edildi. 2030 yılına kadar 500 milyar cihazın internete bağlanmasının beklendiği belirtilen raporda, IoT cihazların bu bağlantı potansiyeli ile siber tehditler için geniş bir saldırı yüzeyi oluşturacağı vurgulandı.

Web bağlantılı buzdolabı, fırın, akıllı saat ve web kamera gibi çok sayıda akıllı cihazların şifrelerinin değiştirilmediği, çoğunda siber saldırılara karşı güncellenen bir savunma programının bulunmadığı belirtilen raporda, güvenlik açıkları üzerinden siber saldırganların cihazlara uzaktan erişebileceği kaydedildi. 2023’ün ilk altı ayında, küresel olarak IoT kötü amaçlı yazılım saldırıları yüzde 37 arttığı ve toplamda 77,9 milyon saldırının gerçekleştiği rapora yansıdı. Beyaz eşya ve elektrikli ev aletleri sektöründe Avrupa’da ve dünyada başı çeken en büyük üreticilerden biri olan Türkiye’de de, Sanayi ve Teknoloji Bakanlığı tarafından, önümüzdeki dönemde akıllı ev aletlerinde siber güvenlik standartlarının belirlenmesi ve uygulanması için çalışmalar başlatılacağı belirtildi.

**En Çok Siber Saldırı Almanya ve ABD’den**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. Ocak-Şubat-Mart 2024 ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu)’larına toplam 3 milyon 192 bin saldırı yansıdı. En çok saldırıyı yapan ülke, 826 bin saldırı ile Almanya olurken, 421 bin saldırı ile ABD ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Polonya, Singapur, Hollanda, Estonya, Çin, Hindistan, Ukrayna ve Vietnam izledi.

**Rapora Erişim Linki:** [**https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2024**](https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2024)

**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)