**Basın Bülteni Kasım 2024**

**STM, Türkiye’yi Hedef Alan Siber Grupları Mercek Altına Aldı**

*STM, yeni açıkladığı Siber Tehdit Durum Raporu’nda, Türkiye’yi hedef alan siber gruplara dikkat çekerek, bu grupların özellikle Türkiye’de spesifik kurumları hedef aldığına vurgu yaptı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, 2024 Temmuz-Ağustos-Eylül aylarını içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. Siber güvenlik alanında farkındalık yaratmak amacıyla, STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 9 ayrı konu başlığı bulunuyor. Raporda, Türkiye’yi hedef alan APT grupları, gelişmiş kimlik doğrulama yöntemleri ve en çok siber saldırı yapan ülkeler gibi güncel ve ilginç konu başlıkları yer alıyor.

Bir hedefe yönelik, uzun süreli siber saldırı olarak adlandırılan Gelişmiş Sürekli Tehditler (APT’ler), siber casusluk grupları tarafından ekonomik, politik ve stratejik avantajlar elde etmek amacıyla değerli bilgileri ele geçirmek için gerçekleştiriliyor. Ulusal savunma, üretim ve finans gibi sektörleri hedefleyen APT saldırıları, fikri mülkiyet, askeri planlar ve kritik kaynaklar gibi yüksek değerli varlıkları odak noktası olarak alıyor. Ulusal güvenlik için önemli bir tehdit oluşturan bu gruplar, dünya genelinde küresel bir endişe kaynağı olarak görülüyor.

**Hedeflerinde kritik kurum ve kuruluşlar var**

STM yeni siber tehdit durum raporunda, Türkiye’yi hedef alan APT gruplarını mercek altına aldı. Dört APT grubunun geçmişleri ve saldırıları ele alınan raporda, bu grupların özellikle Türkiye’de spesifik unsurları hedef aldıklarına dikkat çekildi. Bu grupların, taktik ve tekniklerini sürekli olarak geliştirdiği belirtilen raporda, karmaşık saldırıların tespitinin giderek zorlaştığına işaret edildi. Raporda, “bu saldırıların karmaşıklığı arttıkça, bu büyüyen siber tehditlere karşı savunmamızı güçlendirmek için proaktif bir yaklaşım benimsemek gerekmektedir” uyarısı yapıldı. APT gruplarının kimlikleri özetle şöyle:

**MuddyWater:** Türkiye de dahil olmak üzere Ortadoğu’ya odaklanıyor. 2017’den beri aktif. Grubun İranlı tehdit aktörleriyle bağlantılı olduğu değerlendiriliyor. Türkiye’ye yönelik stratejik hedefleri arasında, hükümet kurumları, telekomünikasyon ve kritik altyapı sektörleri bulunuyor.

**MurenShark:** Yeni bir APT organizasyonu olarak ön plana çıkıyor. Türkiye ve bölgesel dinamiklere odaklanan bir profil sergiliyor. İleri düzey yetenekler kullanan grup, Türkiye’deki önemli kuruluşları, stratejik olarak hedef alarak fikri mülkiyet ve hassas verileri ele geçirmeyi amaçlıyor.

**Cozy Bear (APT29):** 2010’ların ortalarından beri aktif olan ve Rus devleti tarafından desteklenen bir APT grubu. Grubun, özellikle Rusya Dış İstihbarat Servisi’ne (SVR) bağlı Rus istihbarat kurumlarına atfedildiği bilinmektedir. Dünya çapında faaliyet gösteren ve sürekli saldırılar düzenleyen Cozy Bear; bu saldırılarda oltalama, sıfır gün açıkları, özel zararlı yazılımlar ve araçlar kullanıyor. Hedefleri arasında hükümetler ve kritik altyapılar yer alıyor.

**StrongPity:** İlk olarak 2016 yılında gözlemlenen StrongPity’nin devlet, destekli olduğu düşünülmekte ve dünya genelinde siber casusluk kampanyalarına katıldığı biliniyor. Hedefler arasında hükümet kuruluşları, sivil toplum örgütleri ve siyasi faaliyetler veya insan hakları savunuculuğu ile uğraşan kişiler yer almakta olup, bu faaliyetler Avrupa, Ortadoğu ve Kuzey Afrika’ya yayılmaktadır. StrongPity, hedef kitlesinin sıkça ziyaret ettiği web siteleri üzerinden sistemleri ele geçirmek, hassas bilgileri çalmak ve kalıcı bir varlık sürdürmek amacıyla Truva atı zararlı yazılımını dağıtmaktadır.

**En çok Siber Saldırı Rusya’dan**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. Temmuz-Ağustos-Eylül 2024 ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu)’larına toplam 1 milyon 583 bin saldırı yansıdı. En çok saldırıyı yapan ülke, 204 bin saldırı ile Rusya olurken, 126 bin saldırı ile Hindistan ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Çin, ABD, Estonya, Bulgaristan, Singapur, Tayland, Vietnam ve Ukrayna izledi.

Raporun dönem konusunda ise Bilgi Teknolojileri (IT) ve Operasyonel Teknolojilerin (OT) farklı siber güvenlik öncelikleri mercek altına alındı.

**Rapora Erişim Linki:** <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-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 33 yıldır hizmet veren STM, bugün sahip olduğu temel kabiliyet ve teknolojilerini askeri deniz platformlarından taktik mini İHA sistemlerine, komuta kontrol sistemlerinden 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)