**Basın Bülteni Ocak 2022**

**STM 2021’İN SİBER SALDIRI BİLANÇOSUNU AÇIKLADI**

**EN FAZLA SİBER SALDIRIYI İRLANDA VE ÇİN YAPTI**

**Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin Teknolojik Düşünce Merkezi “ThinkTech”, Ekim-Aralık 2021 tarihlerini kapsayan yeni Siber Tehdit Durum Raporu’nu açıkladı. 2021 yılının siber saldırı bilançosuna yer verilen raporda, en çok siber saldırı yapan ülkenin İrlanda ve Çin olduğuna dikkat çekildi. Saldırganların en çok denediği kullanıcı adı ve parolalar da raporda yer aldı.**

STM ThinkTech’in 2021 yılı son çeyreğini kapsayan raporunda 8 ayrı konu başlığı bulunuyor. Raporun zararlı yazılım analizleri bölümünde “AsyncRAT” ve “STOP” isimli zararlı yazılımlar mercek altına alınırken, teknolojik gelişmelerbölümünde ise, kötü amaçlı sosyal medya hesaplarının nasıl tespit edildiği, ileri yaşlı yetişkinlerde parola yöneticilerinin kullanımı ve bluetooth yöntem karıştırma saldırısı gibi analizler öne çıkıyor.

**En çok siber saldırı yapan ülke: İrlanda ve Çin**

STM’nin kendi Honeypot sensörleri tarafından topladığı veriler; 2021 yılında en çok saldırı toplanan ülkeler, portlar, en çok denenen parolalar ve kullanıcı isimleri gibi önemli bilgileri ortaya koydu.

Buna göre, 2021 yılı boyunca toplamda 62 milyon 508 bin 710 siber saldırı meydana geldi. En çok saldırı yapan ülke 9 milyon 879 bin ile İrlanda olurken, 5 milyon 637 bin saldırı ile Çin ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Rusya, Hindistan, ABD, Vietnam, Hollanda, Panama, Türkiye ve Brezilya izledi. Türkiye’de ise 1 milyon 757 bin siber saldırı toplandığı kayıtlara geçti. İrlanda’dan gelen saldırı sayısının bir sonraki ülkeye kıyasla bile yüksek sayıda olması dikkatleri çekerken, Panama’nın en çok saldıran ülkeler arasında yer alması ise bir dikkat çekici detay olarak değerlendirildi.

**Saldırganların en çok denediği parolalar**

Uzaktan erişilebilen servisler üzerinde en çok denenen parolalar ve denenme sayıları raporda detaylıca incelendi. Denenen parolalar incelendiğinde bunların, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan admin, root, test, user gibi kelimeler olduğu gözlemlendi. “Admin” 390 bin kez, “1234” 311 bin kez, “root” 279 bin kez saldırganlar tarafından denenen parolalar olarak listenin başında yer aldı.

**Bu kullanıcı adlarına dikkat**

Kullanıcı adları incelendiğinde ise, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, test, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görüldü. Saldırganlar “root” kullanıcı adını 1 milyon 479 bin kez, “admin” kullanıcı adını ise 490 bin kez denedi.

STM analistleri, parolaların test süreci tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli parolalar ile güncellenmesi gerektiğini vurguluyor. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının da en kısa zamanda değiştirilmesi, mümkün ise yönetim panellerinin internet üzerinden erişime kapatılması tavsiye ediliyor.

**En çok saldırı alan portlar**

En çok saldırının SMB servisinin kullandığı port 445’e geldiği raporda yer aldı. SMB servisi, sunucuların paylaşılan dosyalar ve yazıcılar için kullandığı servis olduğundan, bu servisin diğer servislere kıyasla çok daha fazla saldırı alması beklenen bir durum olarak değerlendirildi. SMB’yi sırasıyla RDP, SSH ve VNC servisleri takip etti.

**Akıllı Sözleşmelerdeki Zafiyetler**

Raporun dönem konusu ise, son zamanlarda hızla gelişen ve vazgeçilmez bir teknoloji hâline gelmiş olan Ethereum blok zincirindeki akıllı sözleşmelerin zafiyetlerinin incelenmesini oluşturuyor.

**Rapora Erişim Linki:** <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-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 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)