BİLGİ NOTU

KONU : Suriye'deki Çatışma Ortamında Rusya'nın Siber Alanı Kullanımı

AÇIKLAMA :

1. Rusya'nın; Suriye'deki çatışma ortamında siber alanı kullanımına dair bilgiler, **NATO dokümanları ve açık kaynaktan** derlenerek aşağıda sunulmuştur.

a. Gelişmiş siber alt yapı ve yeteneklerine sahip Rusya'nın siber alandaki faaliyetlerinin, **Askeri İstihbarat Direktörlüğü** sorumluluğunda 2007 yılında teşkil edilmiş olan "**Gelişmiş Kalıcı Tehdit (APT28)**" adlı grup vasıtasıyla yürütüldüğü,

b. Rusya'nın, jeopolitik amaçlarını elde edebilmek maksadıyla, **siber alandaki teknik yeteneklerini** önceki harekatlarda (Ukrayna, G.Osetya, Gürcistan vb.) olduğu gibi Suriye'deki çatışma ortamında da etkin olarak kullandığı,

c. Hedefinde; **Suriye karşıtı gruplar, sivil toplum kuruluşları, NATO** ve Rusya uçağının düşürülmesi sonrası **Türkiye** olduğu,

ç. APT28 vasıtasıyla **siber casusluk** yanında, hedef sistemlerin **iletişiminin engellenmesi** faaliyetlerinin yürütüldüğü,

d. APT28 grubunun haricinde diğer Rus kökenli siber korsanlar tarafından da, **İnsan Hakları Örgütleri, yardım kuruluşları, Türkiye'deki devlet kuruluşları ve özel sektör** kuruluşlarına saldırılar düzenlendiği, 2016 yılı başında başlayan bu siber saldırıların iki safhalı olarak gerçekleşeceği;

(1) **İlk safhasında hedef sistemlere sızarak casusluk** faaliyetinin yürütülmeye başlanacağı,

(2) Müteakip safhalarda;

(a) Zararlı yazılımlarla verilerin **silinebileceği, değiştirilebileceği veya yok edilebileceği,**

(b) Resmi elektronik posta hesaplarından gönderilecek veriler ile **bilgi kirliliği yaratılarak propaganda yapılabileceği**,

(c) **Sistemlerdeki açıklıklar istismar edilerek** hükümet dışı kuruluşlardan daha **hassas bilgilerin** elde edilebileceği belirtilmektedir.

2. Siber alandaki gelişmiş yeteneklerini icra ettiği harekâtlarda etkin olarak kullanan Rusya, Rusya'ya ait uçağın düşürülmesi sonrasında ülkemizi siber operasyonlarda hedef almıştır. Özellikle, ülkemizin **internet alt yapısı ve finans sektörüne yapılan siber saldırılar ile sağlık kuruluşlarının verilerinin silinmesine yönelik siber saldırılar**, Rusya'nın yukarıda arz edilen siber alandaki faaliyetlerinin bir göstergesidir.

3. Ayrıca, Genelkurmay Başkanlığı İnternet web sitesinin hizmet dışı bırakılmasına yönelik olarak 26 Kasım 2015 tarihinde icra edilen saldırının Rusya kaynaklı olduğu da değerlendirilmektedir. Söz konusu saldırıda sistemlerde herhangi bir **veri kaybı ve hizmet dışı kalma** durumu meydana gelmemiştir.

4. Sonuç olarak;

a. TSK-Ağı'nın (TSK-İç NET) internete bağlı olmaması, hizmetin kapalı bir iletişim ortamı olan **TAFICS üzerinden sağlanması** nedeniyle dışarıdan (iç tehditler hariç) Rusya kaynaklı bir tehditle karşılaşılmayacağı,

b. Tasnif Dışı gizlilik dereceli bilgilerin işlendiği TSK İnternet (TSK-Dış NET) sistemlerine Rusya kaynaklı saldırıların **hizmet dışı bırakma, zararlı yazılım gönderme vb yöntemlerle** devam edeceği değerlendirilmektedir.

c. Yapılan/yapılacak saldırılara karşı "**Derinliğine Savunma**" yaklaşımıyla tüm sistemler 7/24 esasına uygun olarak takip edilmekte ve siber tehditlere karşı kullanıcıların farkındalığını artırmaya yönelik bültenler hazırlanarak eğitim ve tatbikatlar icra edilmektedir.

MEBS Bşk.