2016 EKİM-ARALIK DÖNEMİ SİBER TEHDİT DURUM RAPORU

STM | MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

İÇİNDEKİLER

GİRİŞ

Siber saldırılar her geçen gün kişisel olsun kurumsal olsun kâbus olmaya devam ediyor. Özellikle son yıllarda artan Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service - DDoS) saldırıları karşısında irili ufaklı birçok firma maddi-manevi zarara uğruyor. Eylül 2016 ayında siber güvenlik blog sitesi KrebsOnSecurity'ye karşı 665 Gbps, Fransız hosting firması OVH'ye yaklaşık 1 Tbps genişliğinde saldırılar düzenlenmesinin ardından, Ekim 2016 ayında bu kez ABD'de konuşlu Dyn DNS sağlayıcısı firma da aynı saldırı tipinden etkilendi. 2016 yılının son çeyreğinde şüphesiz en çok konuşulan siber saldırı ABD'ye yönelik gerçekleştirilen ve ülkemiz dâhil birçok ülkede çeşitli erişim sorunlarına yol açan bu tarihi DDoS saldırısı oldu. Bahse konu saldırının en dikkat çeken yönü "Mirai" adlı zararlı yazılımdan etkilenen ve Nesnelerin İnterneti (Internet of Things – IoT) olarak adlandırdığımız ağda bulunan çok sayıda cihazın saldırı içerisinde kullanıldığının anlaşılmasıydı. Bu saldırının ardından ABD menşeli siber güvenlik çözümleri sunan Imperva firmasına ait ağa Aralık 2016 ayı ikinci yarısında bu kez "Leet Botnet" olarak adlandırılan ağdan 650 Gbps'ye ulaşan iki siber saldırı gerçekleştirildi. Bu saldırılarda da ele geçirilmiş IoT cihazlarının kullanıldığı yönünde açıklamalar yapıldı.

Ekim 2016 ayında gerçekleştirilen ve Avrupa, Orta Doğu ve Afrika ülkelerini içine alan bir araştırmada1, ülkemizin herhangi bir "botnet"e ("botnet"ler, tekrarlanan görevleri ve hedeflerini tamamlamak için bir çaba ile diğer benzer makinelerle iletişim kuran internet bağlantılı bilgisayarların bir dizisidir) dâhil olan cihaz sayısı sıralamasında 1'inci, İstanbul ve Ankara'nın da "botnet"lere bağlı en çok cihaz bulunan şehirler sıralamasında ilk iki sırada yer aldığını görüyoruz. Kontrol dışı bilgisayar sorunumuz devam ediyor.

Türkiye'de faaliyet gösteren 250 kurumun katılımı ile gerçekleştirilen siber güvenlik araştırmasına2 göre, son beş yıllık dönemde siber saldırıların sayısında artış yaşandığı ve bu bağlamda Türkiye ekonomisine yönelik saldırıların arttığı ifade ediliyor. Ortaya çıkan tabloya göre:

- Ticari kuruluşların %47'si, 2011 yılından bu yana maruz kaldıkları siber saldırıların sayısında artış olduğu görüşünde birleşiyor.

- Sadece zararlı yazılımlar ve bilgisayar korsanları değil, çalışanlar da farkında olmadan şirketlerinin siber güvenliklerini tehdit ediyor.

- Türkiye'deki şirketlerin dörtte üçünün halen uygulamakta olduğu bir siber güvenlik politikası bulunuyor. Bu kurumların %43'ü siber güvenlik politikalarını günlük, haftalık ve aylık bazda gözden geçiriyor ve revize ediyor.

- Kurumların %23'ü siber güvenlik harcamaları için bütçe ayırmazken, toplam BT bütçesinin %11'i ile 30'u arasında bir kısmını siber güvenliğe ayıranların oranı %50'yi buluyor. %10'luk bir kesim ise toplam BT bütçesinin %31'inden fazlasını siber güvenlik için harcadığını ifade ediyor.

2016'nın son günlerinde siber saldırıların ülke ilişkilerini ne denli etkileyebileceğini gösteren bir olaya şahit olduk. Rusya ile ABD arasında patlak veren diplomatik krizde, Washington Moskova'yı, 'ABD seçimlerini manipüle edebilecek ölçüde' bir siber saldırı düzenlemekle suçladı.

2016 yılının son çeyreğinde dikkatinizi çekmek istediğimiz siber olaylar ve araştırma sonuçlarından sonra, bu dönemki raporumuzda 2016 yılına ait genel bir değerlendirmeyi ve 2017 yılı tehdit beklentilerini sizlerle paylaşmak istiyoruz. Görülüyor ki siber tehditler 2017 yılında da azalmayacak ancak oluşturacağı risklerin mümkün olduğunca en aza indirilebileceği bir yıl olmasını temenni ediyoruz.

1. https://uk.norton.com/emeabots
2. http://bilgicagi.com/turkiye-ekonomisine-yonelik-siber-saldirilar-artista/

2016 Yılı Değerlendirmesi

Siber tehditlerin yine hep gündemde olduğu bir yılı daha geride bıraktık. 2016 yılında her üç ayda bir düzenli olarak yayımladığımız Türkiye Siber Tehdit Durum Raporlarımızda 2016 yılı için küresel ölçekte ön plana çıkmasını beklediğimiz siber saldırı trendleri olarak;

- İç tehditlerin siber tehdit unsurlarının en önemlisi olmaya devam edeceğine,

- Mobil teknolojilere yönelik saldırılarda artış görüleceğine,

- Windows işletim sistemi yanında diğer işletim sistemlerine yönelik saldırılarda artış gözleneceğine,

- POS cihazlarının siber saldırılara maruz kalmaya devam edeceğine ve mobil cihazlar vasıtasıyla gerçekleştirilen ödeme sistemlerine yönelik saldırılara,

- Kritik altyapılara yönelik saldırılara,

- Fidye yazılımlarıyla yapılacak saldırılara,

- Nesnelerin İnternetinin (IoT) siber saldırıların öncelikli hedefleri arasında yer alacağına,

- Botnet saldırılarına,

- Hedef odaklı saldırılara dikkat çekmiştik.

2016 yılını siber saldırılar özelinde değerlendirdiğimizde, yukarıda belirttiğimiz trendlerle uyumlu olarak dünya genelinde fidye yazılımlarının, özellikle DDoS maksatlı gerçekleştirilen IoT bağlantılı Botnet saldırılarının, bankacılık sistemlerine yönelik saldırıların, mobil teknolojilere yönelik saldırıların ve veri ihlâllerinin oluşturduğu tehditlerin ön planda olduğu bir yıl geçirdiğimizi görüyoruz.

Siber tehditler arasında 2016 yılında en çok dikkat çeken ve gittikçe yaygınlaşan fidye yazılımlarının farklı çeşitlerde ortaya çıkması, ulaştığı bilgisayar ve ağlara bulaşmasını da kolaylaştırıyor. Fidye yazılımları son dönemlerde daha çok fidye yazılımı dağıtan istismar yazılımları vasıtası ile yayılıyor ve bazı saldırılarda da uzaktan kontrol uygulamaları araç olarak kullanılıyor. Fidye yazılımlarının dağıtımında bu şekilde değişik yöntemler kullanılması, saldırganların koruma yöntemlerini ihmâl eden kuruluşları hedef almaları gerçeğinden hareketle, alınan güvenlik tedbirlerinin de kullanılan yöntemlere karşı koyacak şekilde çeşitlendirilmesi ve özellikle önümüzdeki dönemde tehdit istihbaratının kullanılmasının önemini ortaya koymaktadır.

Ülkemizin 2016 yılında Avrupa bölgesinde fidye yazılım saldırılarını en fazla yaşayan ülke olması, dünyada ise ABD ve Brezilya'dan sonra 3'üncü sırada yer alması, maalesef tehlikenin ülkemiz için kritik seviyede olduğunu gösterdi.

Bir başka tehdit, Avrupa ülkeleri arasında birinci olduğumuz online bankacılık saldırıları olarak karşımıza çıkıyor. Kullanıcı adlarının, parolaların, kredi kartı numaralarının, PIN kodlarının çalınmasına yönelik zararlı yazılımlar veya çoğunlukla e-postalardaki linkler vasıtasıyla gerçekleştirilen oltalama saldırıları, online bankacılığa yönelik en yaygın saldırı çeşitleri olarak tanımlanıyor.

Rus siber korsan gruplarının Rusya'nın dünyadaki çıkarlarına aykırı hareket eden ülke ve kuruluşları hedef alan "Piyon Fırtınası" saldırılarına maruz kalmamız, İstanbul Elektrik, Tramvay ve Tünel İşletmeleri Genel Müdürlüğü (İETT) sistemlerine saldırı, ülkemizi de etkileyen ticari casusluk amaçlı "Ghoul Operasyonu", Anonymous'un Sağlık Bakanlığı Hastanelerine ve İzmir Gaz'a yaptığı saldırılar, bazı bankalarımızı da etkileyen Society for Worldwide Interbank Financial Telecommunication Sistemi'ne (SWIFT) yönelik saldırılar, 2016 yılında ülkemize yönelik diğer saldırılar olarak ön plana çıktılar.

Kontrol dışı bilgisayarların fazlalığı 2016 yılında ülkemizi yakından ilgilendiren diğer önemli bir tehdit oldu. Bu durum bizi en fazla botnet, zararlı yazılım ve istismar kiti tespit edilen ülkeler sıralamasında ilk beş ülke arasına sokmaya devam ediyor.

2016 yılının ikinci yarısına özellikle IoT olarak adlandırdığımız ağda bulunan çok sayıda cihazın da kullanıldığı DDoS saldırıları damgasını vurdu. "Mirai Botnet" ve "Leet Botnet" etkili DDoS saldırılarına sebep olan "botnet"ler olarak ön plana çıktılar.

Dönemsel olarak bakıldığında hangi saldırı ana tehdit unsuru olarak ön plana çıkarsa çıksın, veri

ihlâlleri dünya genelinde sürekli bir zafiyet unsuru olmaya devam ediyor. Nisan 2016 ayında Panama menşeili Mossack Fonseca adlı kurumda 214 bini aşkın off-shore kurum için düzenlenmiş olan 11,5 milyon gizli belgenin, kimliği belirsiz bir kaynak tarafından ifşa edilmesi, bilgi çağının bu zamana kadarki en büyük bilgi sızıntısı olarak nitelendirildi. 2016 üçüncü çeyreğinde en az 500 milyon Yahoo kullanıcı hesap bilgisinin 2014 yılında ele geçirildiğinin anlaşılması ve bugüne kadar gerçekleştirilmiş en büyük veri ihlâli olarak tarihe geçmesinden sonra Yahoo bu kez 2013 yılına dayanan bir siber saldırı sonucunda yaklaşık 1 milyar kullanıcısının hesap bilgilerinin çalındığını bildirdi. Amerikan Ulusal Güvenlik Ajansı (National Security Agency – NSA) nın siber operasyonlarında kullandığı siber araçların siber korsanların eline geçmesi ve satışa sunulması da son dönemlerin en çok ses getiren veri ihlâllerinden birisi olma özeliğini taşımaya devam ediyor. 117 milyon LinkedIn, 32 milyon Twitter, 68 milyon Dropbox kullanıcısına ait bilgilerin İnternet'e sızması da diğer önemli veri ihlâlleri olarak gündemimizdeydi.

Ülkemizde de 2016 yılı başından itibaren 50 milyon vatandaşımıza ait nüfus bilgilerinin, Sağlık Bakanlığına bağlı bazı hastanelerdeki hasta bilgilerinin, İzmir Gaz veri tabanındaki bazı bilgilerin İnternet'e düşmesi, Makine ve Kimya Endüstrisi Kurumu'nda (MKE) 2 adet silahın üretim ve çizim planlarının para karşılığı satılma girişimi gündemimize giren veri ihlâlleri olarak ön plandaydı.

Gelişmiş yapısıyla fark edilmesinin neredeyse imkânsız olduğu öne sürülen casusluk amaçlı "ProjectSauron"u, fidye zararlı yazılımları "Locky", "Petya", "Misha" ve "PTT Kargo" virüslerini, bilgisayar ve akıllı telefonları ele geçirme amaçlı "Zeus" ve "Zitmo" virüslerini, "Tordow" bankacılık trojanını ve Google hesaplarına yönelik "Gooligan" zararlısını, 2016 yılında gündeme gelen zararlı yazılım örnekleri olarak verebiliriz.

Günümüzde elektrik, su, atık su, petrol, doğal gaz, ulaştırma, kimya, ilaç üretimi, kâğıt, yiyecek, içecek ve otomotiv, uzay/havacılık ve dayanıklı tüketim malları gibi parçalı/montaj tipi imalat sektörlerinde, akıllı şehirler, akıllı evler, akıllı arabalar ve tıbbi cihazların kontrolünde kullanılan Endüstriyel Kontrol Sistemlerindeki (EKS) zafiyetler kritik altyapılarımız için büyük bir tehdit oluşturmaktadır. EKS parçaları ile ilgili olarak 2016 yılında yapılan bir araştırma3 sonuçlarına göre;

- EKS parçaları ile uyumlu 170 ülkede toplam 188.019 sistem bulunmaktadır.

- Uzaktan kontrol edilebilen EKS'lerin %92'sinde açık mevcuttur. Bu sistemlerin %87'si orta derecede zayıf nokta taşırken %7'sinin tehditlere açıklık oranı yüksek olarak belirlenmiştir.

2016 yılının son günlerinde Enerji ve Tabii Kaynaklar Bakanlığı, elektrik dağıtım hatlarına yönelik yurtdışı merkezli yoğun siber saldırı olacağı ihbarıyla tedbirlerini almış ve beklenen saldırının 2017 yılının ilk haftasında gerçekleştiği duyurulmuştur.4

Ayrıca, teknolojik gelişmelere bağlı olarak küresel olarak kullanımları artan akıllı televizyonlar, giyilebilir teknoloji ürünleri ve üç boyutlu yazıcılar, beraberlerinde getirdikleri riskler nedeniyle kullanımlarına dikkat edilmesi gereken cihazlar olarak 2016 yılında haber konusu oldular.

SMS-Tabanlı İki Faktörlü Kimlik Doğrulama, OpenSSL ve Wi-Fi bağlantı noktalarının güvenlikleri, sahip oldukları açıklıklar nedeniyle tartışılmaya devam ediliyor. Alternatif çözümlere yönelik yapılan çalışmaların ve yayımlanan güvenlik yamalarının takibi önem arz ediyor.

Temmuz 2016 ayında icra edilen NATO zirvesinde, siber uzayın, kara, deniz ve havaya ilaveten askeri harekât alanı olarak resmen ilan edilmesi, NATO'nun İnternet'i bir savaş alanı olarak kabul ederek olası siber saldırılara karşı ittifakın konvansiyonel silahlarla karşılık vermesinin önünü de açması yönüyle önemli bir karar olarak tarihe geçmiş oldu.

STM olarak 2016 yılında siber güvenlik alanında hedeflerimiz arasında olan;

- Her anlamda pek çok ilki bünyesinde barındıran, siber saldırılara karşı reaktif değil proaktif bir yaklaşımla yeni nesil siber güvenlik anlayışının bir ürünü olan "Siber Füzyon Merkezi"mizi hizmete sunmanın,

- Siber güvenlik alanında kişilerin ve kurumların kendilerini deneyerek zayıf yönlerini görmelerini, kendilerini geliştirme imkânı sağlamalarını ve bu alanda çalışan tüm paydaşların tek çatı altında birleştirilerek bilgi paylaşım ağının oluşturulmasını amaçlayan Capture the Flag (CTF) yarışmalarından ikincisini düzenlemenin heyecanını yaşadık.

3. http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Kaspersky-Lab-Discovers-Vulnerable-Industrial-Control-Systems-Likely-Belonging-to-Large-Organizations
4. http://www.milliyet.com.tr/elektrik-hatlarina-sabotaj-var-mi--ekonomi-2374138/

Ülkemizin siber güvenlik altyapısının güçlendirilmesine yönelik faaliyetler olarak;

- Siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleştirilmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasını amaçlayan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın duyurulması,

- Kamu kurum ve kuruluşlarının yalnızca kamu kurumları için oluşturulmuş sanal özel bir ağ olan KamuNet'e dâhil edilmelerine yönelik genelgenin yayımlanması,

- Hazırlık çalışmaları uzun zaman alan ve kişisel verilerin belirlenen usul ve esaslara uygun olarak işlenmesi sağlanmasını hedefleyen 6698 sayılı "Kişisel Verilerin Korunması Kanunu"nun 24 Mart 2016 tarihinde TBMM'de kabul edilmesi,

siber güvenlikle ilgili olarak mevzuat anlamında 2016'ya damgasını vuran önemli gelişmeler oldu. Bu konularda tüm ilgili kurumların üzerlerine düşen yükümlülükleri yerine getirmesini önemsiyor ve sonuçlarının ulusal güvenliğimize hedeflenen katkıları sağlamasını diliyoruz.

2017 Yılı Beklentileri

Akıllı Tehditler: Tehditler her geçen gün daha da akıllanıyor ve gittikçe daha fazla otomatikleşiyor. Siber saldırganların değişik ülkelerde değişik kurum ve kuruluşları hedef seçmeleri ve saldırılarında kullandıkları araçları, taktikleri ve yöntemleri her saldırıya yönelik olarak uyarlayabilmeleri, gelecekteki saldırılarda da yeni ve beklenmedik tekniklerle karşılaşabileceğimiz şeklinde yorumlanıyor. Önümüzdeki yıl FortiGuard Lab'ın tabiri ile "insan benzeri" zararlı yazılımların görülmesi bekleniyor. Bu yazılımların saldırıların etkisini artırmak için kendilerini duruma göre uyarlayacağı ve başarıyı temel alan öğrenme yeteneğini kullanacakları değerlendiriliyor. Bu da bilgi teknolojileri ve güvenlik sistemlerinin yöneticilerine daha fazla iş düşmesi ve saldırılarla başa çıkabilmek için farklı güvenlik çözümlerini bir arada kullanmak durumunda kalacakları manasına geliyor.

DDoS Saldırıları: Özellikle 2016 yılında ses getiren DDoS saldırılarının 2017 yılında da devam edeceği değerlendiriliyor. Daha önceki DDoS saldırılarında kullanılan "Mirai" benzeri zararlı yazılımların kullanımının, 2017 yılında daha da artacağı, saldırılarda IoT platformlarının da etkin olarak kullanılacağı konusunda güvenlik uzmanlarının çoğunluğu hemfikir.

Buluta Saldırılar: Bulut güvenliğinin en zayıf halkası mimarisi değil, aksine bulut kaynaklarına uzaktan erişim sağlayan milyonlarca cihazdır. Bu nedenle son kullanıcıların cihazlarındaki açıkları kullanan ve böylece bulut servis sağlayıcılarını daha etkili bir şekilde hedef alan saldırılarda artış bekleniyor.

Kurum İçi Yazışmalara ve Süreçlere Sızma: Kurum E-Postaları Dolandırıcılığı (Business E-mail Compromise - BEC) ve İş Süreçleri Dolandırıcılığı (Business Process Compromise - BPC) yöntemleri, kurumların sistemlerine yapılan saldırılara oranla daha kolay ve daha fazla getirisi olduğundan siber korsanlar tarafından çoğunlukla tercih ediliyor ve edilmeye devam edeceği öngörülüyor. Bu yöntemlerle siber korsanlar, kurumun özellikle finansal yazışmalarını takip edip kişiler adına gönderdikleri e-postalarla ödemeleri kendi banka hesaplarına yönlendiriyorlar ve/veya kurumun süreçlerine sızıp işlemlerde yaptıkları değişikliklerle kendilerine mal veya para yönlendiriyorlar. Özellikle bankacılık sektöründe 2016 yılında artan SWIFT saldırıları, bu alanda 2017 yılında da dikkate alınması gereken öncelikli tehditlerden birisi olarak dikkat çekiyor.

Siber Propaganda: 2016 yılında dünya nüfusunun %46,1'i akıllı telefonlar, bilgisayarlar, tabletler veya İnternet erişimli hizmet terminalleri (kiosklar) aracılığıyla bağlantılı hâle geldi. Bu da her gün daha fazla kişinin kaynağına veya güvenirliğine bakılmaksızın bilgiye hızlı ve kolayca erişmesi anlamına geliyor. İnternet erişiminin artmasıyla birlikte siber propaganda faaliyetleri de giderek çoğalıyor. Çeşitli grupların 2017 yılında da siber propaganda aracılığıyla kitlelerin görüşlerini etkileyecek girişimlerde bulunarak siyasi ve toplumsal olaylara yön vermeye çalışmaları, sosyal medyanın çok daha fazla taciz ve suiistimal maksatlı kullanılması bekleniyor.

Fidye Yazılımları: 2016 yılında %400 oranında ar-

tan fidye yazılımlarını 2017 yılında da görmeye devam edeceğimiz değerlendiriliyor. Trend Micro'nun tahminlerine göre bu yıl fidye yazılımları çeşitliliğindeki artış %25 olacak. Bu da her ay 15 yeni fidye yazılım çeşidine denk geliyor. Bu durum eldeki birçok fidye yazılımı çeşidiyle gerçekleştirilen saldırı yöntemlerinin giderek daha da çeşitleneceğine işaret ediyor. 2017 yılında fidye yazılımlarının IoT platformlarının yanında,POS cihazları ve ATM'ler başta olmak üzere PC dışındaki platformlara da yayılması bekleniyor.

Kritik Alt Yapı Zafiyetleri: İmalat ve enerji üretimi gibi endüstriyel ortamlara verimlilik kazandırdığından dolayı, endüstride Nesnelerin İnterneti (ki Endüstriyel Nesnelerin İnterneti (Industrial Internet of Things – IIoT) olarak adlandırılıyor) kullanımı yaygınlaşıyor. Tehdit aktörlerinin BlackEnergy truva atı türü saldırılarının etkinliğini kendi amaçları doğrultusunda kullanmak isteyecekleri ihtimal dâhilinde. Buna ilave olarak SCADA sistemlerinin artan zafiyetleri karşısında (Tipping Point'in 2016 yılında tespit ettiği zafiyetlerin %30'una karşılık geliyor), IIoT'ye geçişin kuruluşlara ve onların hizmetlerinden etkilenen tüketicilere, örneğine rastlanmamış tehlike ve riskler getireceği öngörülüyor.

Bütün bu tehdit unsurları dikkate alındığında özellikle, kamu, sağlık, enerji ve telekomünikasyon gibi kritik sektörlerde faaliyet gösteren kuruluşların siber güvenlik konusuna eğilmelerinde büyük fayda bulunuyor.

Kısa Ömürlü Zararlı Yazılımların Yükselişi: Kaspersky Lab uzmanları, 2017 yılında cihazların belleklerinde konuşlanan ve ilk yeniden başlatma sırasında kendisini silecek olan zararlı yazılımların ortaya çıkacağını öngörüyor. Söz konusu yazılımların, genel anlamda bir keşif ve kimlik bilgileri toplama amacını taşıdığı, tespit edilmemeye önem veren saldırganların son derece hassas ortamlarda kullanacağı yöntemler olarak belirtiliyor.

Özetle 2017 yılında siber saldırı trendleri olarak;

- IoT platformlarının da kullanılacağı DDoS saldırılarının,

- Çeşitli yöntemlerin kullanılacağı fidye yazılımları saldırılarının

- Mobil cihazlara yönelik saldırıların,

- EKS'lere ve özellikle de bu tür sistemleri bünyesinde yoğun olarak barındıran Enerji Dağıtım Sistemlerine yönelik saldırıların,

- Kurum İçi Yazışmalara ve Süreçlere Sızma suretiyle yapılacak saldırıların,

- Kapalı sistemlerden (kapalı ağlar, cihazlar vb.) veri çalmaya yönelik saldırıların ön plana çıkması beklenmektedir.

Siber Saldırılar

ABD'ye Tarihin En Büyük Siber Saldırısı

İnternet dünyası 21 Ekim 2016'da tarihi günlerinden birini yaşadı. Ülkemiz dâhil birçok ülkede çeşitli İnternet siteleri ve servislerine erişim sorunları yaşandı. Twitter, SoundCloud, Spotify ve Shopify gibi site ve servislerde yaşanan yavaşlık veya erişilememe gibi problemlerin, ABD menşeli DYN isimli

DNS firmasına yapılan DDoS saldırıları neticesinde oluştuğu ortaya çıktı. Dyn DNS, birçok popüler web sitesi tarafından kullanılan bir servis. Bu siteler arasında yukarıda sayılanlar dışında SaneBox, Reddit, Box, GitHub, Zoho CRM, PayPal, Airbnb, Freshbooks, Wired.com, Pinterest, Heroku ve Vox Media gibi diğer önemli hizmetler de bulunuyor. (Harita üzerinde saldırıdan en yoğun etkilenen bölgeler gösterilmiştir.)

Tehdit istihbaratı alanında lider yazılım ve servis sağlayıcısı olan "Flashpoint" firması tarafından, saldırılarda ana kaynak olarak "Mirai" adında zararlı yazılımın kullanıldığı yönünde ipuçları bulunduğu açıklandı. Mirai'nin hedefinde IoT olarak adlandırılan ve İnternet'e bağlı yazıcılar, yönlendiriciler, video kameralar, akıllı televizyonlar gibi cihazların oluşturduğu ağ üzerindeki cihazlar bulunuyor.

Bu cihazlar genellikle üzerinde gelen zayıf parolalarla kullanıldığı için siber korsanlar tarafından kolaylıkla ele geçirilip DDoS saldırıları için kullanılan "botnet"lerin üyesi olabiliyorlar.

Son DDoS saldırılarının çok iyi planlanmış ve yürütülmüş olduğu ve IoT cihazlarının da dâhil olduğu en az 14 milyon IP adresinden geldiği ifade ediliyor.

Yahoo'dan Yeni Saldırı Duyurusu

ABD'nin en büyük teknoloji şirketlerinden Yahoo, 2013 yılında gerçekleşen bir siber saldırıda yaklaşık 1 milyar kullanıcısının hesap bilgilerinin çalındığını bildirdi.

Çalınanlar arasında müşterilerin gizli bilgileri, e-posta adresleri, telefon numaraları, doğum tarihleri ve hesap doğrulama kayıtlarının yer aldığı belirtilen açıklamada, kullanıcıların finansal bilgilerinin zarar görmediğine yer verildi. Açıklamada, 2013'teki siber saldırının "devlet destekli" korsanlarca gerçekleştirildiğine inanıldığı ifade edildi.

Bir önceki 3 aylık tehdit raporumuzda da yer aldığı gibi Yahoo'nun 2014'de de 500 milyon kullanıcı bilgisi çalınmıştı. Bahse konu siber saldırıyla ilgili olarak yapılan açıklamada, bilgisayar korsanlarının ele geçirdiği bilgiler arasında kullanıcıların adı, e-posta adresi, telefon numarası, doğum tarihi, karıştırılmış şifresi, hesap doğrulamak için gereken güvenlik sorusu ve cevabının bulunduğu ancak kredi kartı bilgisi gibi finansal bilgilerin çalınmadığı ifade edilmişti.

Son dört ayda tarihinin en büyük iki siber saldırı olayını kamuoyuna duyuran Yahoo'nun güvenlik protokollerinin ne derece "güvenli" olduğu tartışması, Amerikan medyasında yeniden alevlenmiş durumda.

ABD'nin en büyük telekomünikasyon firmalarından Verizon, geçen Temmuz ayında Yahoo'nun ana işletme birimlerini 4,8 milyar dolara satın alma anlaşması yapmış, ilk siber saldırı haberlerinden sonra anlaşma koşullarının yeniden müzakere edilebileceğini belirtmişti.

Yahoo kullanıcıları için Yahoo tarafından yapılan güvenlik önerileri şu şekilde:

- Yahoo hesabınız ve benzer bilgileri kullandığınız diğer hesaplar için şifrelerinizi ve güvenlik sorularınızı ve yanıtlarınızı değiştirin.

- Şüpheli etkinlikler için tüm hesaplarınızı inceleyin.

- Kişisel bilgilerinizi isteyen veya sizi kişisel bilgiler isteyen bir web sayfasına yönlendiren herhangi bir iletişime karşı temkinli olun;

- Şüpheli e-postalardan gelen bağlantılara tıklamaktan veya eklentileri indirmekten kaçının.

- Yahoo'da bir şifre kullanma gereğini ortadan kaldıran doğrulama aracı olan Yahoo Hesap Anahtarı'nı kullanın.

NSA Siber Silahları Bu Kez Doğrudan Satışta

Temmuz-Eylül 2016 tehdit raporumuzda NSA siber araçlarının İnternet'e sızdırıldığı ve sızıntının sorumluluğunu üstlenen Shadow Brokers grubu tarafından açık artırmaya sunulduğu haberi yer almıştı. Açık artırmanın siber silah tüccarlarının ilgisini çekmemesi üzerine, Shadows Brokers bu defa siber araçları Aralık ayı ortalarında doğrudan satışa sundu.

Yeni keşfedilen bir yeraltı web sitesinde The Shadow Brokers'a ait elektronik anahtarla imzalanan bir dosyada, grubun NSA siber araçlarını birer birer satacağı ifade ediliyor. Shadow Brokers bu işlem için, DNS sunucuları olarak "blockchain şifreleme", dosya sunucuları olarak "BitTorrent" teknolojilerini kullanan web sitelerini barındıran ve merkezi olmayan İnternet benzeri bir ağ olan "ZeroNet"i kullanıyor.

Sitenin, ziyaretçilerine her bir araç için ekran görüntüleri ve dosyaları indirme imkânı sunduğu, araçları, "Exploits", "Trojans", "Implant" gibi kategorilere ayırdığı, araçların her birinin 1 ilâ 100 bitcoin (Aralık 2016 sonu itibarıyla yaklaşık 930 ABD Doları ilâ 93.000 ABD Doları) arasında fiyatlandırıldığı ve bütün araçlar satın almak istendiğinde toplam rakamın yaklaşık 930.000 ABD Doları olacağı dikkat çeken bilgiler arasında yer alıyor.

Türk Bankalarına SWIFT Saldırısı

2016 İkinci Üç Aylık Türkiye Siber Tehdit Raporumuzdaki başlıklardan birisi olan SWIFT Sistemindeki saldırılardan Aralık ayında bu kez Türk bankaları etkilendi. Üç Türk bankasının saldırıdan etkilendiği ifade edilirken şu ana kadar sadece Akbank resmi açıklama ile zarara uğradığını belirtti.

SWIFT Sistemine yapılan saldırılar Bangladeş, Ukrayna, Ekvator ve Filipinler'deki bankalardaki kayıplarla gündeme gelmiş, bir Vietnam bankası da devam eden bir siber soygunu blokladığını açıklamıştı. Son olarak Aralık ayı başında da Rusya Merkez Bankasına yapılan saldırılar sonucu bankanın 2 milyar Ruble (31 milyon ABD Doları) kayba uğradığı duyurulmuştu.

Society for Worldwide Interbank Financial Telecommunication" ifadesinin baş harfleriyle anılan SWIFT, uluslararası bir ödeme ağı üzerinden para transfer etmeye yönelik mesajlaşma sistemine verilen addır ve sistem bugün itibarıyla ülkeler arasındaki para transferinde en önemli araç durumundadır.. Günümüzde dünya çapında 11.000 kadar finansal kurum ve bankanın kullandığı bilinen " Brüksel merkezli servis, üye olan finansal kurumların birbirlerine para transferi için standart ve güvenli bir çerçeve sağlamaktadır. Ancak para transferinin kendisi değil, sadece bilgileri aktarılmaktadır ve siber korsanların sızdığı alan da ödeme bilgilerinin gönderildiği mesaj içeriğidir. Böylece günlük normal para transferlerinin gideceği yer, gönderenin istediği değil, korsanların planladığı yer oluyor. Meblağ veya diğer bilgiler de değiştirilebiliyor.

SWIFT'in bu sene meydana gelen saldırı olayları sonrasında; siber korsanların banka sistemlerini ele geçirmek için yeni ve karmaşık metodlar kullandığını belirterek bankaları güvenlik konusunda uyardığı ve tespit edilen tüm saldırıların müşterileri tarafından kullanılan SWIFT ara yüzlerine yapıldığını, kendi merkezi iletişim ağının ele geçirilmediğini ifade ettiği belirtiliyor.

Akbank tarafından kendisine yönelik saldırı hakkında yapılan açıklamada ise;

- Söz konusu atağın 8 Aralık 2016 tarihinde AKBANK bilgisayar sistemlerine yöneltildiği,

- Saldırı sonrasında teknik ekipler tarafından duruma ivedilikle müdahale edildiği, gerekli tedbirlerin alındığı ve konu ile ilgili kamu makamlarına derhal bilgi verildiği,

- Tüm sistemlerinin sorunsuz olarak çalışmaya devam ettiği,

- Bu veya başka herhangi bir konuda müşterilerine yansıyan herhangi bir olumsuzluk, kayıp veya güvenlik sorunu bulunmadığı,

- Azami risk tutarının 4 milyon ABD Doları seviyesinde olduğu ve olası zararın bankayı koruyan sigorta kapsamına girdiği yönündeki bilgiler kamuoyu ile paylaşılmıştır.

Bankacılık sektörünün Sektörel Siber Olaylara Müdahale Ekibi (SOME) olan Bankacılık Düzenleme ve Denetleme Kurulu'nun (BDDK) alınacak önlemler konusunda bankalara yaptığı uyarıda, SWIFT sistemine mesaj iletilene kadar gerekli kontrollerin, alarm tanımlamalarının ve sıkılaştırmaların yapılması gerektiğini vurguladığı belirtiliyor.

ABD İle Rusya Arasında Siber Saldırı Krizi

Rus siber korsanlar tarafından Kasım 2016 ayında sonuçlanan ABD Başkanlık Seçimlerine karşı siber saldırı düzenlendiği iddiası, iki ülke arasında devam eden tartışmaları diplomatik krize dönüştürdü.

ABD yönetimi, Rusya'nın, Demokrat başkan adayı Hillary Clinton'ın seçim kampanyası ekibine ait e-posta sızdıran siber korsanların arkasında olduğu öne sürdü.

ABD istihbaratına göre, bu saldırı nedeniyle seçim Cumhuriyetçi aday Donald Trump'ın lehine değişti ve saldırıların arkasında, Rusya devletine bağlı bilgisayar korsanlarının olduğuna ilişkin güçlü kanıtlar mevcut. Kremlin ise suçlamaları reddediyor.

ABD, bilgisayar korsanlığı yoluyla başkanlık seçimlerine müdahale iddiaları nedeniyle 35 Rus diplomatı sınır dışı etme kararı aldı. ABD Dışişleri Bakanlığı söz konusu diplomatların 'diplomatik statülerine uygun olmayan faaliyetler' içerisinde olduklarını bildirdi. Washington yönetimi ayrıca, misilleme önlemlerinin bir parçası olarak Maryland ve New York'da istihbarat toplamak için kurulan iki Rus merkezinin kapatılacağını duyurdu.

Bu arada Rusya Dışişleri Bakanlığı'ndan yapılan ilk açıklamada, ABD yönetimince alınan yaptırım

kararının ikili ilişkilerin düzeltilmesine zarar vereceği bildirildi. ABD'nin 35 Rus diplomatı sınır dışı etme kararını değerlendiren Rusya Devlet Başkanı Vladimir Putin, Washington yönetiminin attığı yeni düşmanca adımları provokasyon olarak nitelendirdi. 'Hiç kimseyi sınır dışı etmeyeceklerini' vurgulayan Putin, ABD'ye verilecek yanıta yeni başkan Donald Trump'ın tavrına göre karar vereceklerini vurguladı.

Yaşanan bu olaylar, siber saldırıların ülkeleri telafisi oldukça zor zararlara ve maddi kayıplara uğratabildiğini bir kez daha gözler önüne seriyor.

Zararlı Yazılımlar

Tordow Bankacılık Trojanı

Geçtiğimiz Eylül ayı sonlarında Kaspersky Laboratuvarı araştırmacıları tarafından duyurulan bankacılık işlemlerine yönelik ilk mobil zararlı yazılım olan Tordow'ın, ikinci sürümü keşfedildi. Özellikle Android işletim sistemli cihazları için yazılan Tordow v2.0 trojanı, şu aşamada Rusya'daki kullanıcıları etkiliyor.

Android kullanıcıları için çok ciddi bir tehdit oluş-

turan Tordow trojanı, diğer bankacılık trojanlarından farklı olarak etkiledikleri cihazlarda yönetici yetkilerini elde etmeye çalışıyor. Bunun sebebi ise saldırganın cihazın tam kontrolünü ele geçirmek istemesi ve bu sayede bir seri işlem gerçekleştirebilmesi.

Bahse konu trojanın etkilediği cihaz üzerinde aşağıdaki işlemleri gerçekleştirebildiği ifade ediliyor:

- Telefon çağrısı yapabilme,
- SMS mesajlarını izleme,
- İlave yazılım indirme,
- Login yetkilerini çalma,
- Rehbere erişim,
- Cihaz üzerindeki bilgileri şifreleme,
- Web sayfalarını açma ve ziyaret etme,
- Bankacılık verilerini kullanma,
- Güvenlik yazılımlarını silme,
- Cihazı yeniden başlatma,
- Dosyaları yeniden adlandırma,
- Fidye yazılımı gibi davranarak fidye talep etme,
- Cihazın yazılım, donanım, işletim sistemi, model, İnternet Servis Sağlayıcı, üretici ve konum bilgilerini toplama.

Tordow 2.0, üçüncü-parti mağazalardan indirilen uygulamalar aracılığıyla yayılıyor. Bahse konu trojan şu aşamada Rusya'daki kullanıcıları etkiliyor olsa da bu tür başarılı korsanlık operasyonlarının genellikle diğer ülkelere kısa sürede yayıldıkları bir gerçek. Bu açıdan tüm Android kullanıcılarının güvenlik yazılımlarını güncel tutmaları, talep edilmeden ekrana gelen eklenti ve web adreslerini açarken dikkatli olmaları ve mutlaka bilinen ve güvenilir kaynaklardan uygulama indirmeye özen göstermeleri önem arz ediyor.

Google'da Gooligan Zararlısı Tehlikesi

Bir milyon Google hesabı yeni bir Android zararlı yazılımı tarafından kırılmış durumda. "Gooligan" olarak adlandırılan bu zararlı yazılım her gün yaklaşık 13.000 cihazı daha etkilemeye devam ediyor. Gooligan, cihazları önce root ederek tüm yetkileri ele alıyor, arkasından e-posta adreslerini ve kimlik doğrulama anahtar bilgilerini ele geçiriyor.

Saldırganlar da bu ele geçirilen bilgileri kullanarak kurbanlarının Google hesaplarına sızıp hassas bilgileri barındıran Gmail, Google Photos, Google Docs, Google Play, Google Drive ve G Suite uygulamalarına erişebiliyorlar.

Eğer yönetici yetkilerini ele geçirme işlemi başarılı ise, saldırganlar cihazın tüm kontrolünü ele almış ve uzaktan komut çalıştırabilir hale gelmiş oluyorlar. Şu aşamada Android 4 ve 5 (Jelly Bean, KitKat and Lollipop) kullanıcıları en çok risk altında olanlar. Bahse konu işletim sistemlerini kullanan cihaz sayısı tüm Android pazarının %74'ü olan yaklaşık 1,03 milyar cihaza karşılık geliyor.

Ele geçirilmiş durumda olan cihazların Android işletim sisteminin temiz kurulum (Flash) ile en baştan kurulması gerekiyor.

Siber Zafiyetler

"Botnet"e Dâhil Cihaz Sayısında İlk Sıradayız

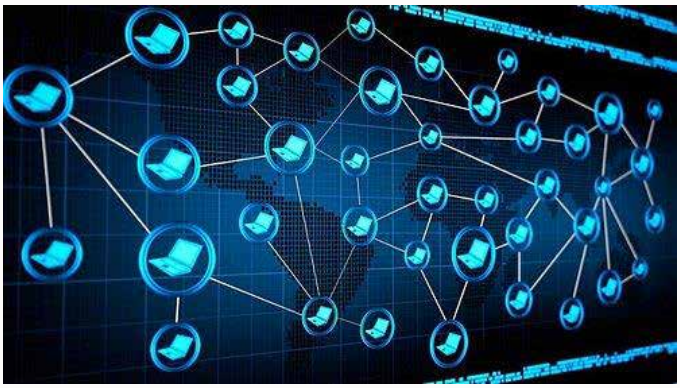
Avrupa, Orta Doğu ve Afrika ülkelerinin kısaca ifade edildiği EMEA (Europe, Middle East and Africa) ülkeleri için yapılan ve Ekim 2016 ayında yapılan bir çalışmada5;

- Ülkemizin, herhangi bir "botnet"e dâhil olan cihaz sayısı sıralamasında birinci, ülkedeki tüm cihazlara göre oranlandığında elde edilen bot yoğunluğu sıralamasında da beşinci olduğunu,

- İstanbul ve Ankara'nın da "botnet"lere bağlı en çok cihaz bulunan şehirler sıralamasında ilk iki sırada yer aldığını görüyoruz.

Rakamsal olarak bakıldığında da her 1.139 İnternet kullanıcından birisinin bir "botnet"e dâhil olduğu gibi olumsuz bir tablo ile karşı karşıyayız. Bilindiği gibi bir bilgisayar, dizüstü bilgisayar veya akıllı telefon bir bot haline geldiğinde, bir botnet içerisinde yüzlerce veya binlerce cihazın bulunduğu bir ağa dâhil olmuş oluyor. Bu şekilde web sitelerinin kullanılmaz hale gelmesine neden olan hizmet dışı bırakma (DOS – Denial of Service) saldırıları gibi bazı suçların işlenmesine alet oluyorlar ve çoğu zaman cihazların kullanıcıları bu durumun farkında olmuyorlar.

Dizüstü bilgisayarlar ve akıllı telefonlardan, fitness takip cihazlarına, yönlendiricilere, ev güvenlik sistemlerine, akıllı televizyonlara, bebek monitörlerine kısaca İnternete bağlı tüm cihazlar özellikle de ön tanımlı (default) parola ile kullanılanlar, düzenli güncelleme yapılmayanlar ve zayıf güvenlik protokolüne sahip olanlar,"botnet"ler için potansiyel hedef oluyorlar.



Bot haline gelme riskini azaltmak için, kullanıcıların cihazların ön tanımlı parolalarını değiştirmeleri, lisanslı işletim sistemi ve güvenlik yazılımları kullanmaları, kullanılmayan servisleri etkisizleştirmeleri, güvenlik ayarlarını gözden geçirmeleri, güvenlik ve cihaz yazılımlarının (firmware) güncelliğini sağlamaları gerekiyor.

Wi-Fi Bağlantı Noktalarındaki Tehlike

Türkiye dâhil, dünya çapında 31 milyondan fazla Wi-Fi bağlantı noktasını analiz eden Kaspersky Lab, her dört noktadan birinin (%28) korumasız olduğunu ve kullanıcıların kişisel bilgilerini riske attığını ortaya çıkardı. Bu da özel mesajlar, şifreler, dokümanlar gibi pek çok veriyi içeren ve söz konusu ağlar üzerinden iletilen tüm trafiğin siber korsanlar tarafından kolaylıkla ele geçirilip kullanılabileceği anlamına geliyor.

Kaspersky Güvenlik Ağı'dan alınan bilgilere göre, dünyadaki Wi-Fi ağlarının %25'i herhangi bir şifreleme ile korunmuyor. Yani bu ağlar üzerinden geçen tüm bilgiler tamamen erişime açık ve üçüncü şahıslar tarafından okunabilir olarak iletiliyor. Diğer bir %3'lük kısım ise verileri şifrelemek için WEP (Wired Equivalent Privacy) protokolünü kullanıyor. Güvenilir olmayan bu protokolün şifresi, İnternet'te

5. https://uk.norton.com/emeabots

ücretsiz olarak bulunan araçlar ile dakikalar içerisinde kırılabiliyor.

Geriye kalan Wi-Fi bağlantı noktaları ise WPA (Wi-Fi Protected Access) protokolleri temelli olan, daha güvenilir bir şifreleme kullanıyor. Bu ağları ele geçirmek için harcanacak gayret, seçilen parolanın güçlülüğü dahil olmak üzere kullanılan ayarlara bağlı olarak değişebiliyor. Örneğin; zayıf veya bazı İnternet kafelerde olduğu gibi halka açık bir parola kullanılıyorsa, saldırganlar bu ağlardan geçen verileri rahatlıkla deşifre edebiliyor.

Konuyla ilgili olarak kullanıcılara; Wi-Fi ağlarına bağlanırken dikkatli olmaları, şifrelenmemiş kablosuz ağ noktalarına bağlanmamaları ve halka açık Wi-Fi noktalarını online bankacılık, alışveriş veya önemli bilgileri paylaşma gibi amaçlar için kullanmamaları tavsiye ediliyor. Üçüncü bir kişinin bu tarz bir veri trafiğine erişmesi durumunda maddi kayıplar da dâhil olmak üzere ciddi sıkıntılar yaşanabileceği ifade ediliyor. Ayrıca veri trafiğinin korunması adına sanal özel ağlar (Virtual Private Network - VPN) gibi bir takım ek tedbirler alınması da öneriliyor.

ATM'lere Uzaktan Erişim

Siber korsanların kredi kartı bilgilerini ve İnternet Bankacılığı bilgilerini çalmak için kullandıkları yöntemler biliniyordu. Saldırganlar, artık doğrudan ATM'lere yönelip para çalma teşebbüsü içindeler. "Cobalt" adlı siber korsan grubu, Avrupa'daki ATM'lere yönelik kapkaç operasyonları gerçekleştiriyor. Rusya menşeli Group-IB tarafından yapılan açıklamada, saldırganların zararlı yazılım kullanarak ATM'lere uzaktan saldırdığı ve ATM'lerin etrafa para saçmalarını sağladığı belirtiliyor.

Yöntemin adı "ATM Jackpotting" ve bu yılın yaz aylarında Tayvan ve Tayland'da rapor edilmiş vakalardan sonra hâlihazırda Ermenistan, Bulgaristan, Estonya, Gürcistan, Belarus, Kırgızistan, Moldovya, İspanya, Polonya, Hollanda, Romanya, İngiltere, Rusya Federasyonu ve Malezya saldırılara uğramış ülkeler arasında sayılıyor.

Aslında ATM'lere yönelik saldırılar en az beş yıldır görülüyor, ancak fiziki olarak erişim sağlama zorunluğu nedeniyle çoğunlukla az sayıda makine etkileniyordu. Ancak şimdi saldırganlar, bankalar saldırıyı anlamadan bir anda çok sayıda uzaktan etkilenmiş makine üzerinden kapkaç ile para çalma imkânı elde edebiliyorlar.

Dünyanın büyük küresel ATM üretici firmalarının yetkilileri, saldırılardan haberdar olduklarını, müşterileri ile beraber tehdidi azaltacak çalışmalar yaptıklarını ve bankaları bu tür saldırıların nasıl engellenebileceğine yönelik bilgilendirdiklerini ifade ediyorlar.

Siber Güvenlik Altyapısı

Capture the Flag 2016

STM tarafından geleneksel hale getirilerek bu yıl Ankara'da 2'ncisi düzenlenen Capture The Flag (Bayrağı Yakala) Yarışması, 20 Ekim 2016 tarihinde gerçekleştirildi.

Siber güvenlik alanında kişilere ve kurumlara kendilerini deneyerek ve zayıf yönlerini görerek gelişim imkânı sağlayan ve bu alanda çalışan tüm paydaşları tek çatı altında birleştirerek bilgi paylaşım ağının oluşturulmasını amaçlayan yarışmaya, bu yıl kamu kurum ve kuruluşlarından 3, özel sektörden 6, üniversitelerden ise 17 olmak üzere toplam 26 takım katıldı. Yarışmada, katılımcılar kriptoloji ve tersine mühendislik gibi dallarda beş farklı kategorideki soruları cevaplandırarak "bayrağı" yakalayan ilk takım olmak için yarıştı.

Yaş ortalaması 21 olan toplam 96 kişinin katıldığı yarışmada, 89 erkek, 7 kadın katılımcı yer aldı.

Siber güvenlik alanında kişilere ve kurumlara kendilerini deneyerek ve zayıf yönlerini görerek gelişim imkânı sağlayan ve bu alanda çalışan tüm paydaşları tek çatı altında birleştirerek bilgi paylaşım ağının oluşturulmasını amaçlayan yarışmaya, bu yıl kamu kurum ve kuruluşlarından 3, özel sektörden 6, üniversitelerden ise 17 olmak üzere toplam 26 takım katıldı. Yarışmada, katılımcılar kriptoloji ve tersine mühendislik gibi dallarda beş farklı kategorideki soruları cevaplandırarak "bayrağı" yakalayan ilk takım olmak için yarıştı.

Yaş ortalaması 21 olan toplam 96 kişinin katıldığı yarışmada, 89 erkek, 7 kadın katılımcı yer aldı.

Siber güvenlik alanında kişilere ve kurumlara

kendilerini deneyerek ve zayıf yönlerini görerek gelişim imkânı sağlayan ve bu alanda çalışan tüm paydaşları tek çatı altında birleştirerek bilgi paylaşım ağının oluşturulmasını amaçlayan yarışmaya, bu yıl kamu kurum ve kuruluşlarından 3, özel sektörden 6, üniversitelerden ise 17 olmak üzere to-

plam 26 takım katıldı. Yarışmada, katılımcılar kriptoloji ve tersine mühendislik gibi dallarda beş farklı kategorideki soruları cevaplandırarak "bayrağı" yakalayan ilk takım olmak için yarıştı.

Yaş ortalaması 21 olan toplam 96 kişinin katıldığı yarışmada, 89 erkek, 7 kadın katılımcı yer aldı.

KamuNet Tanıtımı Yapıldı

yapılan konuşmada, yoğun çalışmalar sonucunda uçtan uca güvenlik platformu olan KamuNet ağının geliştirildiği, sisteme şu an sekiz kurumun dâhil olduğu ve tüm kamu kurumlarının KamuNet ağına dâhil olması için çalışmaların sürdüğü vurgulandı. Çalışmalar sonucunda da kamu kurum ve kuruluşlarının KamuNet'e dâhil edilmesine ilişkin genelge 3 Aralık 2016 tarihinde Resmi Gazete'de yayımlandı. Genelgede, kamu kurum ve kuruluşları-

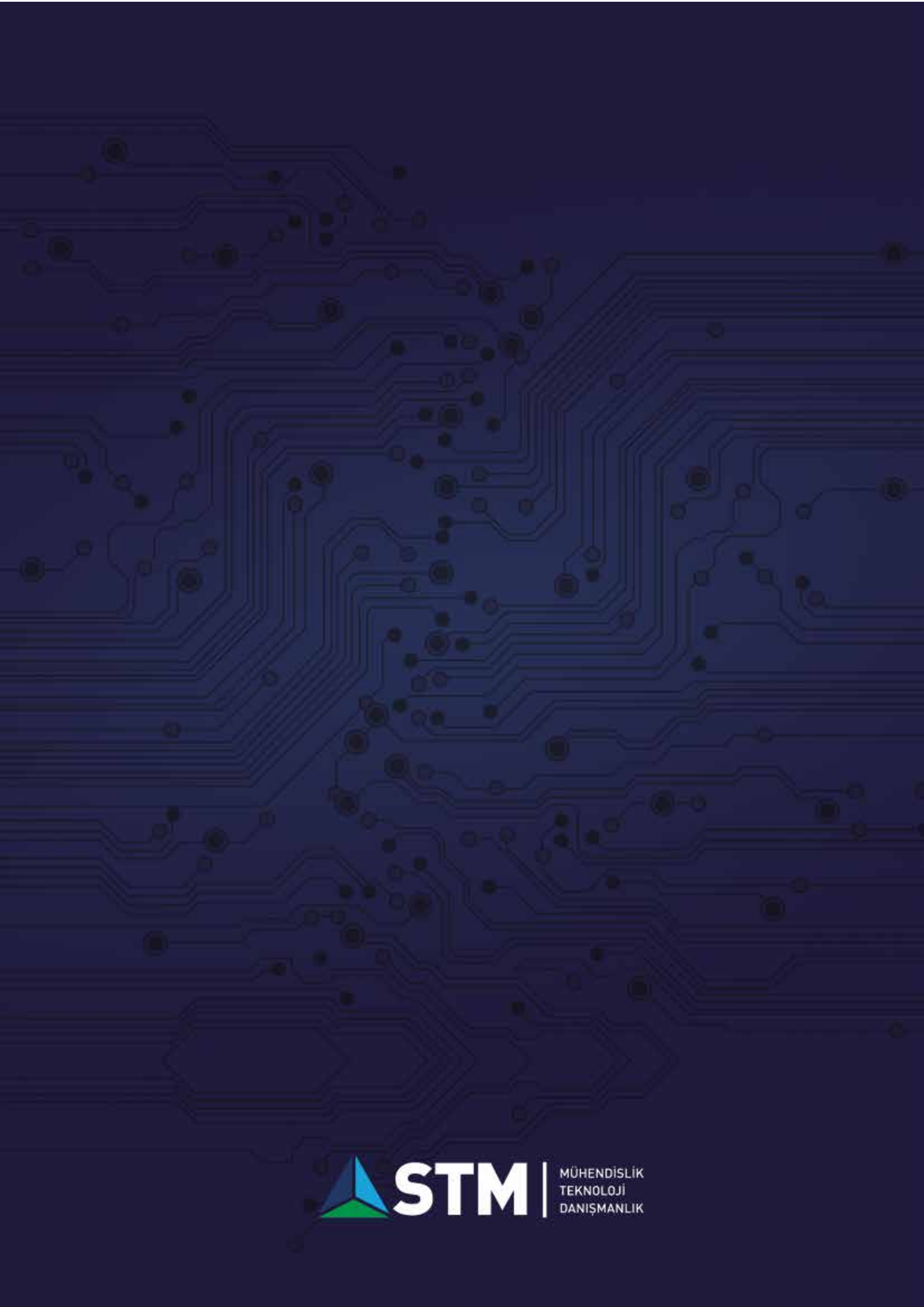
KamuNet, 23 Kasım 2016'da düzenlenen KamuNet Projesi Tanıtım Etkinliği ile 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Çalıştayı'nda tanıtıldı.

Yalnızca kamu kurumları için oluşturulmuş sanal özel bir ağ olan KamuNet, herkese açık olan İnternet ağını kullanmıyor ve sadece kamu kuruluşlarının iletişim kurmasını sağladığı için siber güvenlik risklerini de en aza indirgiyor. Ayrıca, tüm sistem tek bir noktadan izlenebiliyor.

KamuNet ile kamu verilerinin KamuNet ağı üzerinden daha güvenli şekilde iletilmesi ve hem kamu verilerinin, hem de vatandaşların kişisel bilgilerinin saklandığı büyük veri altyapılarının güvenliğinin sağlanması hedefleniyor.

Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan tarafından bahse konu çalıştayda

na, ilgili bakanlık ve kurum arasında imzalanacak protokol çerçevesinde yürütülecek çalışmalara her türlü desteği vermesi ve siber güvenlik bakımından önemi bulunan bu projenin, en kısa sürede tamamlanabilmesi için KamuNet'e dâhil olması talimatı verildi.


STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK