2016 TEMMUZ-EYLÜL DÖNEMİ SİBER TEHDİT DURUM RAPORU

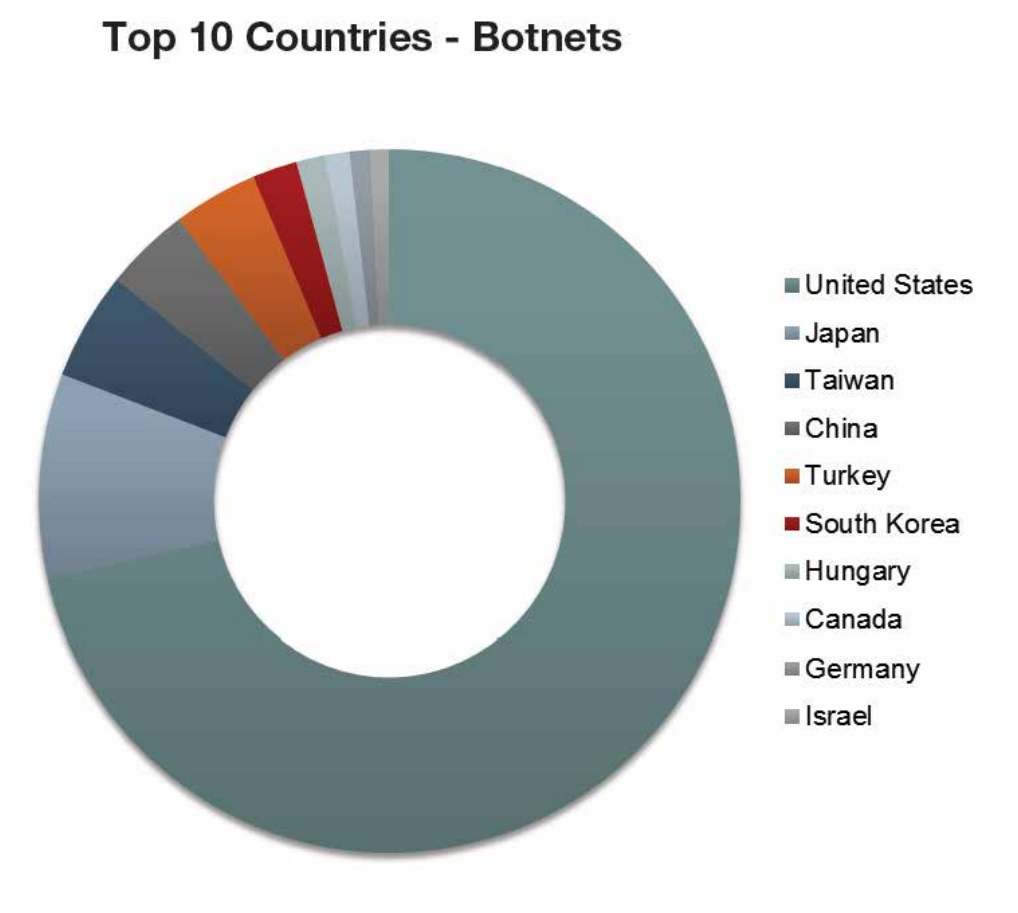
STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK

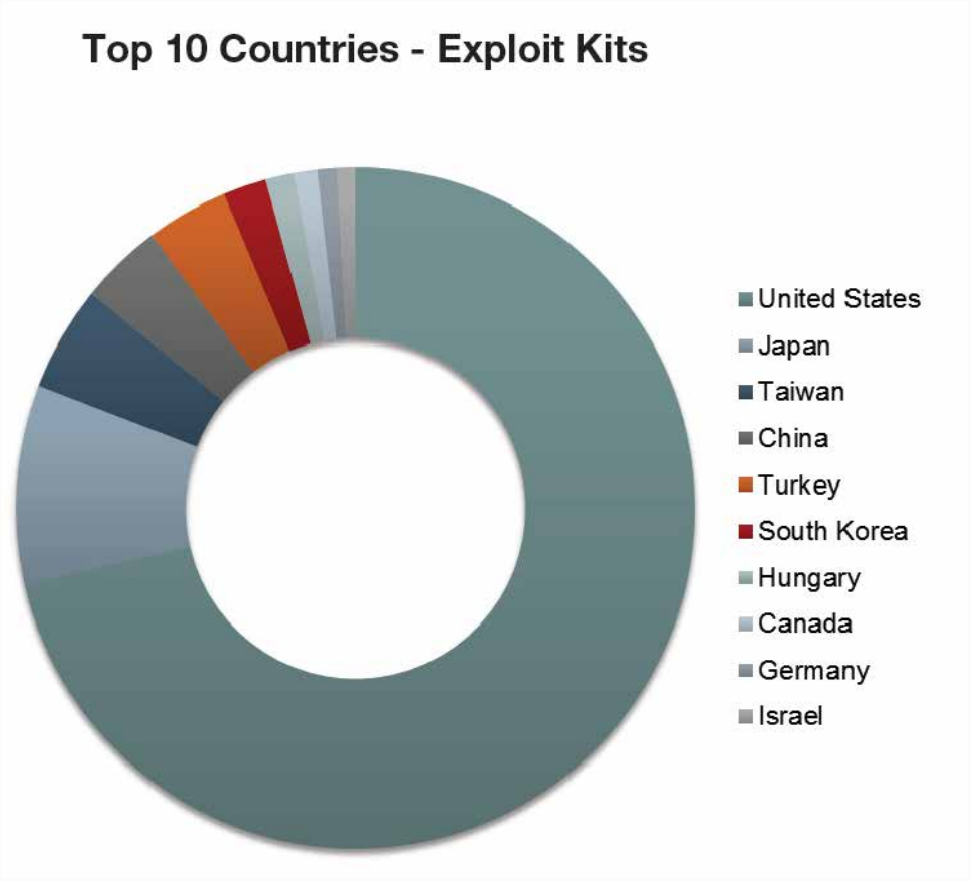
İÇİNDEKİLER

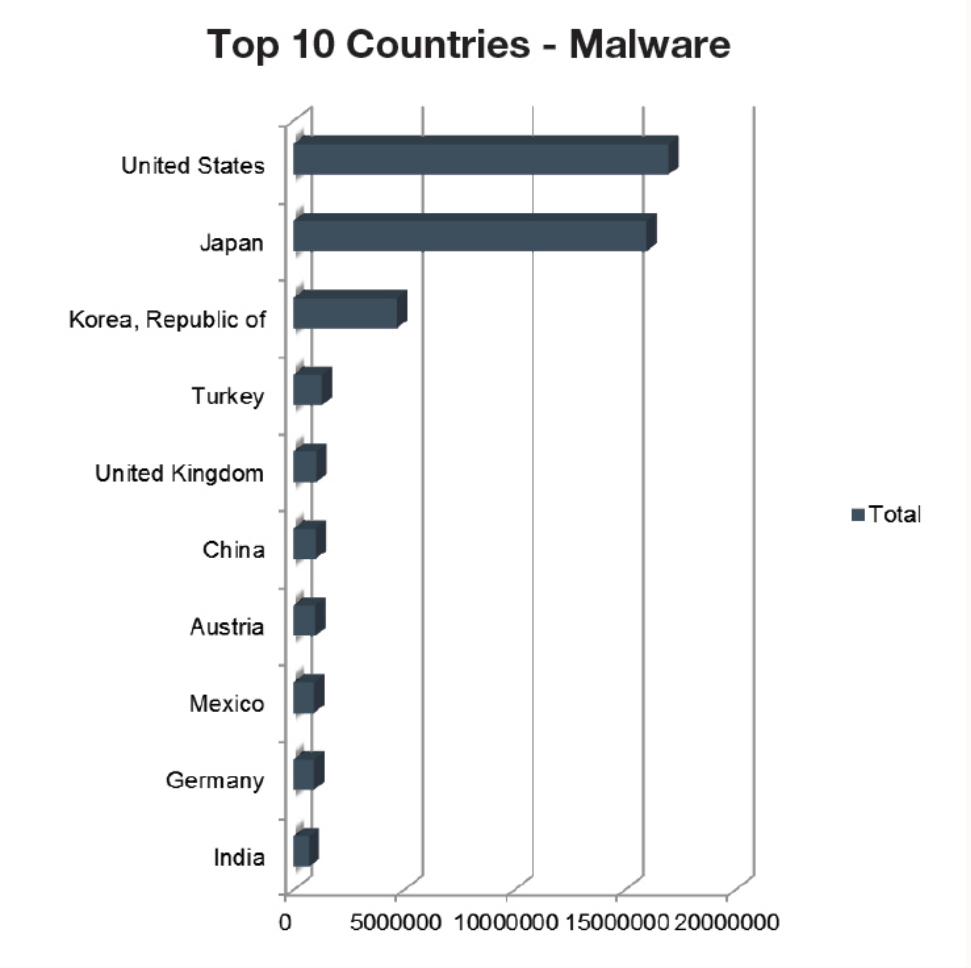
GİRİŞ

Bilişim teknolojilerinin hızlı gelişimi sayesinde artan İnternet kullanımı; kamuda, özel sektörde ve hatta kişisel ölçekte hayatın olağan ve hatta vazgeçilmez bir parçası haline geldi. Kurumlar ve kişiler birbirleriyle elektronik ortamda sürekli bir bağlantı halindeler. Bu durum, ülkemizin de içinde bulunduğu bölgede son dönemde tırmanan çatışmalar ve bunun küresel ölçekteki yansımaları ile birlikte değerlendirildiğinde, fiziksel ortamda maruz kaldığımız tehditlere siber tehditlerin de eklenmesi riskinin her geçen gün arttığı çıkarımını yapmamızı kolaylaştırmaktadır. Temmuz-Eylül 2016 aylarını kapsayan raporumuza; bu konuya bir kez daha önemle dikkat çekerek, kurumsal anlamda ülkemizin tüm kuruluşlarının, kişisel olarak da vatandaşlarımızın, siber ortamda daha belirgin hedefler haline geldiği bir dönemde bulunduğumuzu hatırlatarak, her düzeyde alınan siber güvenlik tedbirlerinin sürekli gözden geçirilmesi gereğine vurgu yaparak ve bu konuda bazı araştırma sonuçlarını paylaşarak başlamak istiyoruz.

Fortinet firması tarafından Ağustos 2016 ayında yayımlanan 2016 ikinci çeyrek siber tehdit analiz raporunda **botnet, zararlı yazılım (malware)ve istismar kiti (exploit kit)** tespit edilen ülke istatistiklerinde ülkemizin ilk 5 içerisinde yer aldığı görülüyor. Bu durum, ülkemizdeki **kontrol dışı** bilgisayarlara yönelik sorun sahasına bir kez daha işaret etmektedir.




Top 10 Countries - Exploit Kits
United States
Japan
Taiwan
China
Turkey
South Korea
Hungary
Canada
Germany
Israel


Top 10 Countries - Malware
United States
Japan
Korea, Republic of
Turkey
United Kingdom
China
Austria
Mexico
Germany
India
0
5000000
10000000
15000000
20000000
Total

Trend Micro tarafından yayımlanan 2016 yılının ilk yarısına ait bir diğer güvenlik raporundaki veriler, tüm dünyada fidye yazılım saldırılarının yüzde 172 oranında arttığını, ülkemizin Avrupa bölgesinde fidye yazılım saldırılarını en fazla yaşayan ülke olduğunu, dünyada ise ABD ve Brezilya'dan sonra üçüncü sırada yer aldığı ifade ediyor.

Diğer yandan, yine Trend Micro'nun araştırması ülkemizde on-line bankacılığa yönelik tehditlerin de hız kesmeden devam ettiğini gözler önüne seriyor. Tespitlere göre ülkemiz 11 bin 516 saldırı ile Avrupa bölgesinde en fazla on-line bankacılık saldırısı alan ülke olurken, ülkemizi 4 bin 880 saldırı ile Almanya ve 3 bin 529 saldırı ile Fransa izliyor.

Akamai'nin güvenlik araştırmalarında 2015 son çeyreği ve 2016 ilk çeyreğinde Dağıtık Servis Dışı Bırakma (DDoS) saldırılarına kaynak olan ülkeler sıralamasında Rusya'daki saldırganların Doğu Avrupa ülkeleri üzerinden saldırılarını gerçekleştirme eğilimine bağlı olduğu değerlendirmesiyle ilk 5 ülke arasında bulunan ülkemiz, ikinci çeyrekte ilk 10 ülke arasında bulunmuyor. Umarız bu iyileşme önümüzdeki dönemlerde de devam eder. Çin'in bu sıralamada birinciliği sürüyor. Yayımlanan son raporda dünya üzerindeki DDoS saldırılarının %56'sının Çin kaynaklı olduğu belirtiliyor.

Öte yandan zarar verilen veya imha edilen veriler, çalınan paralar, kaybedilen verimlilik, fikri mülkiyet hak hırsızlıkları, kişisel veya finansal veriler, yolsuzluklar, dolandırıcılık, saldırı sonrası normal iş akışlarındaki bozulmalar, adli bilişim incelemeleri, siber korsanlığa tabi olan verinin ve sistemlerin kurtarılması ve itibar kaybından doğacak maliyetlere bağlı olarak küresel siber suçlardaki artış devam ediyor. Cybersecurity Ventures firması tarafından en son yayımlanan 2016 üçüncü çeyrek siber güvenlik market raporuna göre önümüzdeki 5 yıl içerisinde siber suçların 2015 yılında 3 trilyon ABD Doları olan maliyetinin 2021 yılında 6 trilyon ABD Dolarına ulaşması bekleniyor. Raporda dikkat çekici bir diğer husus da 2020 yılına kadar günümüzdekinin 50 katı daha fazla veriyi siber tehditlerden korumak zorunda olacağımız. Siber suçlardaki bu artışlar doğal olarak siber saldırılarla mücadele için ayrılan bütçeleri gittikçe çok daha yukarılara çekiyor. Kurumlar bu tarz durumların yaşanmaması adına bilgi güvenliği hizmetleri sunan şirketlerden ürün ve danışmanlık satın alıyorlar. Bu kapsamda 2015 yılında 75 milyar ABD Dolarını bulan siber güvenlik harcamalarının, önümüzdeki 5 yıl içerisinde toplamda 1 trilyon ABD Dolarına ulaşacağı öne sürülüyor.

Bu arada, İran yeni bir zararlı yazılım ile boğuşuyor. Petrokimya komplekslerinde meydana gelen yangınlar sonucu sistemlerinde geniş analizler başlatan İranlı siber güvenlik uzmanları, durumun Stuxnet gibi zararlı bir yazılım sonucunda meydana gelip gelmediğini araştırıyor. Uzmanların yaptığı açıklamalara göre analizler hala sürüyor; ancak tahminler son günlerde yaşanan yangınların yeni bir zararlı yazılımdan kaynaklı olduğu yönünde. Daha önce tespit edilen Stuxnet zararlısı da sisteme bulaştıktan uzun bir süre sonra keşfedilebilmişti. Bu tür zararlı yazılımların etkili olduğu endüstriyel kontrol sistemlerine yönelik tehdit hususu, bu dönemki raporumuzun önemli bir konu başlığı olarak yer alıyor.

2016 yılı üçüncü çeyreği için dikkatinizi çekmek istediğimiz hususları içeren genel bir girişten sonra, bu dönemde öne çıkan konuları derlediğimiz tehdit raporumuzu bilgilerinize sunuyoruz.

Siber Saldırılar

Ghoul Operasyonu

Sanayi ve mühendislik sektörü şirketlerini hedef alan yeni bir saldırı dalgası keşfedildi. Ticari casus yazılımı kitini temel almış, şirketler veya bireylerden geliyor gibi gözüken e-postalar ve kötücül yazılımlar kullanan suçlular, kurbanlarının ağlarında kaydedilmiş değerli iş verilerinin peşine düşüyor. Kaspersky Lab tarafından yapılan açıklamada, aralarında ülkemizin de bulunduğu 30 ülkedeki 130'dan fazla şirkete bu grup tarafından başarılı saldırılar gerçekleştirildiği ifade ediliyor. Bu şirketlerin tamamı, daha sonra kara borsada satılabilecek önemli bilgilere sahip. Ghoul operasyonu saldırganlarının temel motivasyonunu da finansal kazanç oluşturuyor.

Saldırılarda kullanılan e-postaların ekinde bulunan HawkEye adı verilen kötü amaçlı yazılım, Darkweb'de açıkça satılan ticari casus yazılımını temel alıyor ve saldırganlar için çeşitli araçlar sunuyor. HawkEye, yüklenmesinden sonra kurbanın bilgisayarından ilginç veriler topluyor. Bu bilgilerin bazıları şöyle:

- Tuş vuruşu,
- Pano (clipboard) verileri,
- FTP sunucu bilgileri,
- İnternet tarayıcılarındaki hesap bilgileri,
- Paltalk, Google talk, AIM'daki gibi müşteri mesajlaşma araçlarındaki hesap verileri,
- Outlook, Windows Live mail gibi e-posta araçlarındaki hesap verileri,
- Microsoft Office gibi yüklenmiş uygulamalar hakkında bilgiler.

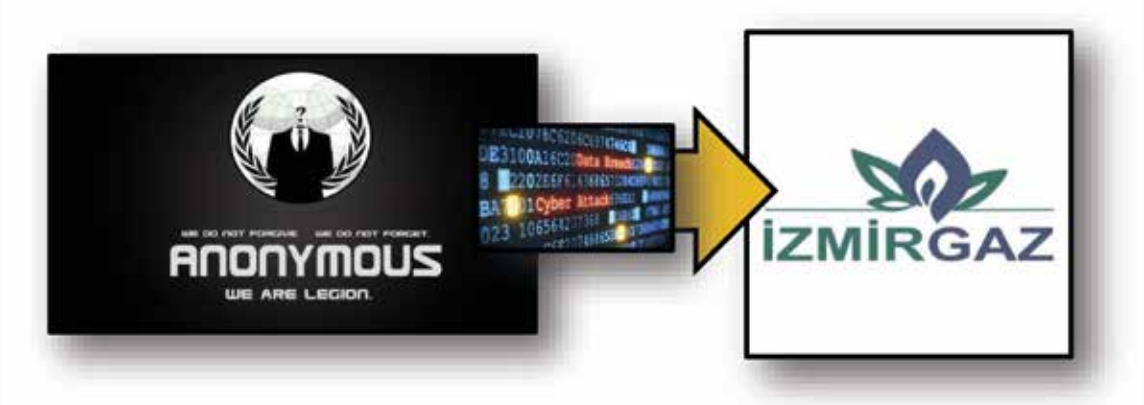
Daha sonra bu veriler tehdit aktörünün komuta ve kontrol sunucularına gönderiliyor. Bazı komuta ve kontrol sunucularından toplanan bilgiye bakıldığında, kurbanların çoğu sanayi ve mühendislik sektörlerinde faaliyet gösteren şirketler. Diğerleri ise nakliyat, ilaç, üretim, ticaret, eğitim şirketleri ve diğer kurumlardan oluşuyor.

Kaspersky Lab araştırmacıları tarafından 'Ghoul Operasyonu' adı verilen kampanya, aynı grup tarafından yürütüldüğü tahmin edilen başka birçok kampanyanın arasında yer alıyor. Grubun hala aktif olarak faaliyette olduğu belirtiliyor.

İzmir Gaz'a Anonymous Saldırısı

Son dönemlerde adından sıkça bahsedilen Anonymous siber korsan grubunun, Türkiye'ye yönelik #opTurkey adındaki operasyonu devam ediyor. Anonymous'un son olarak siber saldırı yaptığı şirket İzmir Gaz oldu.

İzmir'deki doğal gaz dağıtım ve tedarikini sağlayan İzmir Gaz İnternet sitesi, Temmuz 2016 ayının ikinci yarısındaki siber saldırı nedeniyle erişime kapatılarak bir süreliğine servis dışı bırakıldı.



Yapılan saldırı sonucunda şirketin veri tabanından 479 kullanıcının şifrelerini, şirketin bütçe ve bakım raporlarını, üye detaylarını, faturalama bilgilerini elde eden Anonymous'un saldırılarının, görünüşe göre devam edeceği değerlendiriliyor.

Sanatçıların Fanları Terör Örgütlerinin Hedefinde

Sosyal medya ve siber güvenlik uzmanları, sosyal medya platformlarında bazı sanatçı ya da tanınmış kişilerin isimleriyle sahte profiller oluşturulduğu, takipçi sayısının artmasının ardından da bu hesapların terör örgütlerinin propagandası için kullanıldığı uyarısını yapıyorlar.

Uzmanlar, ünlülerin sahte hesaplarına otomatik takipçi yüklenmesinin ardından vatandaşların asıl amacı anlamaması için o ünlüye ait eserlerin, şarkıların veya video kliplerin paylaşıldığına dikkati çekerek, son aşamada binlerce kişiye ulaşabilen bu hesaplarla terör örgütü propagandası yapıldığını bildiriyorlar.

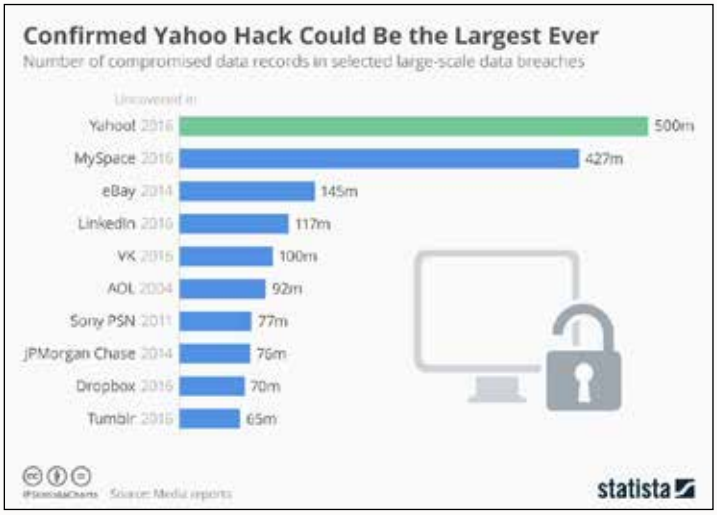
Yahoo Hesap Bilgilerine Yönelik Saldırılar

200 milyon Yahoo hesap bilgisinin bir siber korsan tarafından Ağustos 2016 ayı başlarında Dark Web'te satışa sunulduğu bilgisi ortaya çıktı. Aynı siber korsanın daha önce de LinkedIn, MySpace, Fling ve VK.com'a ait veri tabanlarını satışa sunan "Peace_of_mind" olduğu anlaşıldı.

Ayrıca, bu siber korsan tarafından satışa sunulan bilgilerin 2012 yılına ait olduğu, ifşa edilen bilgiler arasında kullanıcılara ait e-postalar, kullanıcı adları, ikincil e-posta adresleri, adres kodları, doğum tarihleri ve MD5 formatında parolalarının bulunduğu ifade edildi.

Eylül 2016 ayının sonlarına doğru bu defa Yahoo tarafından yapılan açıklamada, incelemeler sonucunda 2014 yılı sonlarında veri merkezine yapılan siber saldırı neticesinde, en az 500 milyon kullanıcının adı, e-posta adresi, telefon numarası, doğum tarihi, özet değeri (hash) alınmış parolası, hesap doğrulamak için gereken güvenlik sorusu ve cevabının bulunduğu verinin çalındığı belirtildi. Yapılan açıklamada ayrıca bu saldırının devlet destekli saldırganlar tarafından yapılmış olabileceği belirtildi ancak ülke ismi verilmedi.

Çalındığı ifade edilen en az 500 milyon kaydın, bugüne kadar gerçekleştirilmiş en büyük veri hırsızlığı olduğu belirtiliyor.



Araştırma sonuçlarına göre çalınan bilgiler arasında korumasız parolalar, banka kartı bilgileri ve banka hesap bilgilerinin bulunmadığı ve bilgisayar korsanlarının hâlâ firmanın ağında olduğuna dair bir ize rastlanmadığı ileri sürüldü.

Dropbox Saldırısı

Geçtiğimiz üç aylık dönemde, popüler bulut depolama firması Dropbox'a yönelik olarak, yine 2012 yılında gerçekleştirilmiş bir saldırıda ele geçirilen bilgiler de İnternet'e sızdı. O tarihte Dropbox tarafından yapılan açıklamada, bir saldırıya maruz kalındığı ve bir grup kullanıcının e-posta adreslerinin çalındığı belirtilmiş ancak parolaların çalındığı rapor edilmemişti.

Dropbox, bilgilerin İnternet'e sızması sonrasında, müşterilerine parola değişim zorunluluğu uygulayacağını duyurdu. Çalınan bilgiler, 2012 yılında yaklaşık 100 milyon müşterinin üçte ikisinden fazlasına karşılık gelen 68 milyon kullanıcıyı ilgilendiriyor ve kullanıcılara ait e-posta adresleri ile özet değeri alınmış parolalardan oluşuyor.

NSA'in Siber Silahları Kimlerin Elinde?

Amerikan Milli Güvenlik Ajansı (NSA), 2013 yılında eski çalışanı Edward Snowden'ın arkasında olduğu sızıntılardan sonra, saldırıya dayalı harekâtını ifşa eden yeni bir olayla bir kez daha sarsıldı. NSA'nın casusluk amacıyla kullandığı siber araçlar, elde edilerek Ağustos 2016 ayı ortalarında İnternet'e sızdırıldı.

Kendilerine Shadow Brokers adını veren ve sızıntının sorumluluğunu üstlenen grup, ellerindekilerin bir kısmından oluşan dosyayı yayımlayarak açık artırmaya sundu ve açık artırmanın 1 milyon bitcoin'e (yaklaşık 570 milyon dolar) ulaşması durumunda ellerindeki ikinci dosyayı da dünyaya duyuracaklarını açıkladı. Fakat konunun henüz siber silah tüccarlarının ilgisini çekmediği ifade ediliyor.

300 MB bilginin bulunduğu dosyada, güvenlik duvarlarını ele geçirerek ağı kontrol etmek için kullanılan istismar araçları ile veri sızdırmaya ve bilgiyi değiştirmeye yarayan yazılımlar bulunuyor. Uzmanlar tarafından yapılan değerlendirmelerde, yazılımların dünyanın en büyük ve en kritik ticari, eğitim kurumlarının ve hükümetlerin kullandığı Cisco ve Fortinet gibi üst düzey güvenlik duvarları için kullanılabilecek pahalı ve karmaşık yazılımlar olduğu ve 2013 yılına ait olduklarının tahmin edildiği belirtiliyor.

Shadow Brokers, bahse konu siber araçların NSA ile bağlantılı olduğu iddia edilen Equations Grup tarafından geliştirildiğini açıkladı. Equations Group, Kaspersky Labs tarafından keşfedilen, dünyanın en gelişmiş siber saldırı gruplarından biri olarak tanımlanan, hatta İran'ın nükleer çalışmalarını sekteye uğratan Stuxnet solucan yazılımının geliştirilmesine katkı sağladığı da iddia edilen bir grup.

Diğer yandan, siber araçların siber korsanların eline nasıl geçtiği konusunda yapılan son değerlendirmeler, NSA'ya doğrudan siber saldırı yapılmadığı, eski bir NSA çalışanının siber araçları bir operasyon sonrasında uzaktan bağlanılan bir sunucu bilgisayarda üç yıl önce kazara bıraktığı ve bir grup Rus siber saldırganın onları bulduğu yönünde.

The Washington Post'ta yayımlanan bir habere göre de "Uyarlanmış Erişim Operasyonları - Tailored Access Operations (TAO)" olarak bilinen NSA'nın siber korsanlık biriminin eski bir çalışanı, sızdırılan dosyanın gerçek olduğunu, kurum ve hükümetlerin bu durum karşısında ciddi bir risk altında bulunduğunu iddia ediyor.

Cisco, Fortinet ve Juniper, bahse konu istismar araçlarının güvenlik duvarı ürünlerini etkilediklerini duyurmuş durumdalar. Bu kapsamda firmaların güvenlik yamalarına yönelik çalışmalarının takip edilmesi önem arz ediyor. Sistem yöneticilerinin, gerekli tüm güvenlik yamaları yayımlanıncaya kadar saldırı tespit ve önleme sistemlerinin istismar araçlarına karşı etkin kullanımına dikkat etmeleri gerekiyor.

Siber Saldırılar - Genel Değerlendirme

Tehdit Hedefi: Gizlilik

Risk: Bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda, vatandaşa ait kişisel bilgilerin veya kamuya ait gizli/özel bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

Alınabilecek Karşı Önlemler:

- Parola bilgilerinin çalındığına yönelik haberler duyulduğunda ilk iş olarak o uygulamaya ait parolanın değiştirilmesi,

- Değişik platformlarda kullanılan kullanıcı parolalarının karmaşıklık kurallarına da riayet edilerek periyodik olarak veya ihtiyaç duyulan her an değiştirilmesi, eski parolaların tekrar kullanılmaması ve farklı siteler için farklı parolaların kullanılması,

- Sistemlerin zafiyetlerinin sürekli olarak taranması ve giderilmesi,

- Sistemlerde bulunan zararlı yazılım önleme yazılımlarının (Antivirüs, vb.) güncel bulundurulması,

- Periyodik risk değerlendirmeleri yapılarak gerektiğinde zafiyeti bulunan servislerin risk giderme çalışmalarının yapılması,

- 0-gün saldırılarına karşı davranış tabanlı güvenlik sistemlerinin tesis edilmesi,

- Kritik ve önemli zafiyetlerin sistem yöneticileri tarafından test edilip uygulanması,

- Gerçek e-postalar ile linklerin sahtelerinden ayırt edilebilmesi için kullanıcı eğitimlerine önem verilmesi,

- Etkisi kanıtlanmış güvenlik sistemlerinin kullanılması,

- Güncel tehdit istihbarat verilerinin temin edilmesi.

Zararlı Yazılımlar

Project Souron

'Sauron Projesi' adında neredeyse 5 yıldır fark edilmemiş ve alışılmadık derecede gelişmiş bir virüs keşfedildi.

Kaspersky Lab tarafından Ağustos 2016 ayı içerisinde deşifre edilen virüsün 5 yıldır çeşitli hükümetlerin sunucularından casusluk yaptığı ve gelişmiş olması nedeniyle fark edilmesinin neredeyse imkânsız olduğu ifade ediliyor.

Asıl adı "ProjectSauron" olan zararlı yazılım, adını Yüzüklerin Efendisi filminin şeytani karakteri olan Sauron'dan alıyor. 2011 yılında aktif hale gelen virüsün amacı, hükümet kuruluşlarına karşı casusluk yapmak.

Virüsün hedeflerinden bazıları:

- Hükümetler,

- Silahlı kuvvetler,

- Bilimsel araştırma merkezleri,

- Telekom operatörleri,

- Finansal organizasyonlar.

Virüs'ün şu ana kadar fark edilmemesinin nedeni ise diğer virüslere hiç benzememesi ve özel araçlar ile sıra dışı teknikler kullanması. Virüs her hedefine göre ayrı bir kod kullanıyor ve saldırıdan sonra o kodu bir daha kullanmıyor. Hedeften aldığı verileri birden fazla farklı veri kaçırma mekanizmaları ile kurum dışına çıkartılabiliyor; böylece güvenlik mekanizmalarının, verilerin nereye gittiklerini bulması zorlaşıyor.

Virüs şu ana kadar İsveç, Çin ve Rusya'nın yüksek profilli ağlarını hedef almış gibi görünüyor fakat Kaspersky Lab daha birçok kuruluşun ve ülkenin etkilenme olasılığının olduğunu söylüyor.

Kaspersky Lab yetkilileri, böylesi tehditlere karşı dayanabilmenin tek yolunun, kurumsal iş akışında en ufak bir anomaliyi bile izleyen sensörler zincirine dayalı, ortada hiçbir şey yokken bile belirli kalıpların peşine düşecek adli analiz ve tehdit zekâsıyla zenginleştirilmiş birçok güvenlik katmanını devreye sokmak olduğunu ifade ediyorlar.

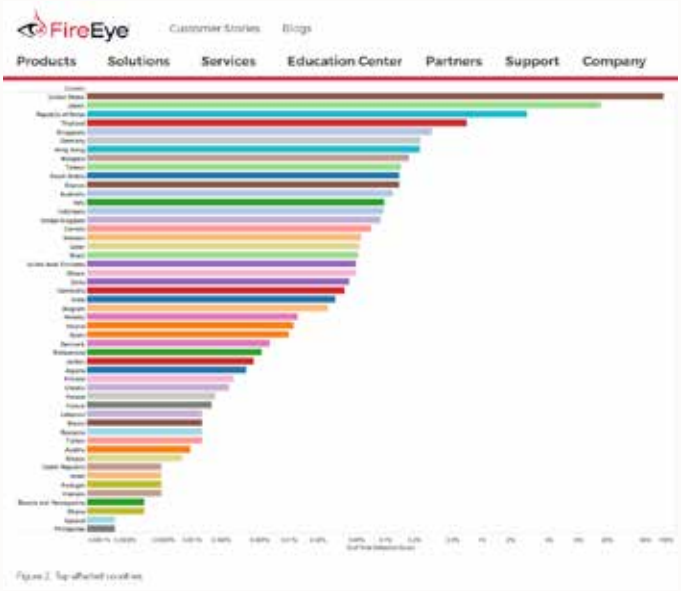
STM olarak üzerinde önemle durduğumuz siber tehdit istihbaratı ve buna bağlı olarak açılışını gerçekleştirdiğimiz Siber Füzyon Merkezi imkân ve kabiliyetleriyle ulaşmayı arzu ettiğimiz hedefler arasında, bu tür tehditlere karşı mücadeleler de öncelikli olarak yer alıyor.

Locky Fidye Zararlı Yazılımı Yayılıyor

Ağustos 2016 ayında FireEye Laboratuvarlarında Locky fidye zararlı yazılımı yayan birkaç yoğun e-posta operasyonu gözlemlendi. Bu operasyonların başta sağlık, telekomünikasyon, ulaşım, üretim ve servis sağlayıcı sektörlerinin, ülke olarak ise en çok ABD, Japonya, Kore Cumhuriyeti, Tayland ve Singapur'un etkilendiği açıklandı. Etkilenen 50 ülke arasında ülkemiz de 40'ıncı sırada yer alıyor.

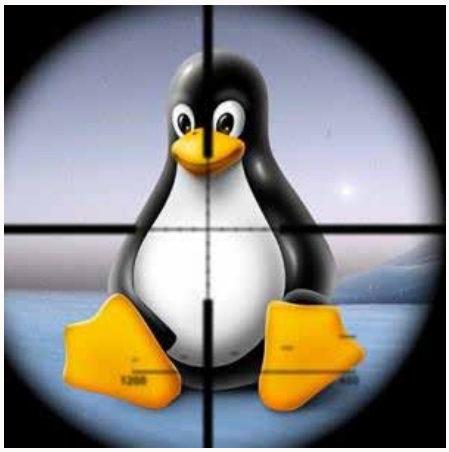
Locky zararlı yazılımını yaymak için kullanılan teknikler sürekli değişiyor. Mart 2016 ayındaki JavaScript tabanlı indirici yerine bu defa e-posta eklerinde bulunan DOCM formatlı eklerle yayılıyor. Ayrıca, son dönemde siber saldırganların bankacılığa yönelik Truva atları yerine daha kârlı gördükleri fidye yazılımlarına yöneldikleri anlaşılıyor.

Bu tür e-posta operasyonları, kurumsal/kişisel iş süreçlerine verebilecekleri zararlar göz önünde bulundurulduğunda, kullanıcıların e-posta eklerini açarken çok dikkatli olmaları gerektiğini gösteriyor.



Linux Cihazlar İçin Botnet Riski

Linux Windows işletim sistemlerine nazaran daha güvenli bir işletim sistemi olarak kabul edilmektedir. Ancak, siber korsanlar kendilerini yeni araçlarla geliştirdikçe bu husus da sorgulanacak gibi görünüyor. Dr.Web firmasına ait bir araştırma grubu tarafından, son dönemde bulaştığı Linux cihaz ve web sitelerini botnetlere çeviren "Linux.Rex.1" isimli bir Linux Truva Atı keşfedildi. Genelde bir zararlı yazılım, mali ve kişisel bilgileri çalmak amacıyla cihazlara bulaştırılmak üzere tasarlanır; ancak "Linux.Rex.1" zararlı yazılımı, bulaştığı cihazlardan DDoS saldırıları gerçekleştirme, kötü amaçlı mesajlar gönderme ve kendini diğer ağlara dağıtma kabiliyetlerine sahip bulunuyor.



Bahse konu zararlı yazılımın, web sitesi sahiplerine, onları DDoS saldırıları için tehdit eden ve saldırılardan sakınmaları için Bitcoin bazında fidye ödemelerini isteyen spam mesaj gönderdiği, ayrıca erişim sağladığı ağlarda Drupal, Magento, JetSpeed ve WordPress tabanlı web siteleri için özel bir modülü sayesinde taramalar yapabildiği de ifade ediliyor.

Veri Kaçağında Artık Hava Boşluğu da İşe Yaramayacak!

İnternet'ten veya diğer ağlardan hava boşluğu ile izole edilmiş olarak daha güvenli olduğuna inanılan bilgisayarlar, son yıllarda siber saldırganlar tarafından doğal hedef haline geldiler.

İsrail Ben-Gurion Üniversitesinde bir grup araştırmacı tarafından, aralarında hava boşluğu bulunan bilgisayarlar arasında USB portlarına özel bir donanım takmadan radyo frekansı transmisyonu üzerinden hassas bilgi aktarımı gerçekleştirebilen bir yöntem bulundu.

USBee adı verilen yazılım, eski NSA çalışanı Edward Snowden tarafından sızdırılan belgelerde adı geçen NSA yapımı USB üzerinden bilgi sızdırma donanımı CottonMouth'un gelişmiş bir hali. USBee, CottonMouth'dan farklı olarak, hava boşluğuyla diğer ağlardan ayrılmış hedef bilgisayarın, bulunduğu ofise özelleştirilmiş bir USB cihazı sokmaya gerek kalmaksızın ve ofiste bulunan USB cihazlarda donanımsal bir değişiklik yapılmaksızın birer RF vericisi olarak kullanılmasını sağlıyor. Hatta USBee, saldırı gerçekleştirmek için USB gömülü yazılımı veya sürücü yazılımının içerisine bir müdahaleye gerek duymuyor.

Araştırmacılar, USBee'nin saldırı metodunun sadece yazılım tabanlı olduğunu vurgulamakla beraber aşağıda belirtilen bazı koşulların sağlanması gerektiğini ifade ediyorlar:

- Hedef bilgisayara çok büyük ihtimalle içeriden birisi tarafından zararlı yazılımın bulaştırılması,

- Hedef bilgisayara herhangi bir USB cihaz takılması,

- Saldırganın, hedef bilgisayarın genellikle en fazla 3-5 metre yakınında bulunması.

USBee şu aşamada ikili (binary) veri çalabildiği için, saldırganların büyük dosyaları çalabilecekleri bir yol değil, ancak 80 bytes/saniye'lik hızla veri aktarımını sağlayarak hedef bilgisayarda depolanan parola gibi küçük boyuttaki hassas verilerin çalınmasını sağlayabiliyor.

Siber ekosisteminde tehditlerin miktar ve boyutlarının değişmesi, doğal olarak bu tehditlere yönelik alınan tedbirlerin yeniden sorgulanmasına ve yeni tedbir arayışlarına yol açmaktadır. Bu kapsamda önceden güvenliği sağladığı değerlendirilen bir tedbir, gelişen teknolojik buluşlar çerçevesinde etkinliğini kaybedebilecektir. "Her tedbiri aldım, bize bir şey olmaz" türü yaklaşımlarla siber tehditlerin varlığını ve etkisini küçümsemek günümüzün en büyük yanılgılarından biri olacaktır.

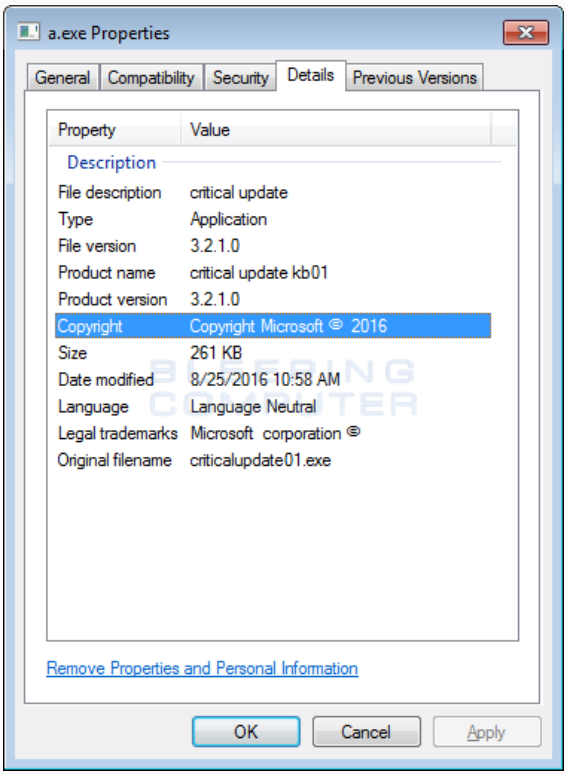
Microsoft Windows Güncellemelerine Dikkat!

Ağustos 2016 ayı sonlarında AVG zararlı yazılım araştırmacısı Jakup Kroustek tarafından, "Fantom" adı verilen ve açık kaynak EDA2 fidye yazılımı projesi tabanlı yeni bir fidye yazılımı keşfedildi.

Fantom fidye yazılımı, kritik bir güncelleme yapıyormuş gibi görünen sahte bir Windows Güncelleme Ekranı kullanıyor. Bu esnada arka planda ise kurbanının dosyalarını şifreliyor.

Maalesef şu aşamada Fantom'un şifrelediği dosyaları çözebilecek bir yöntem yok ve EDA2 tabanlı fidye yazılımı anahtarlarını elde etmek için kullanılan metotlar, bu tür için henüz mevcut değil.

Fantom'u geliştirenlerin, yazılımın kötücül aktivitelerini saklamak için ekstra bir çaba gösterdikleri anlaşılıyor ve dosya özelliklerini gösteren pencere kritik bir Windows güncellemesi görüntüsünü meşrulaştırmak için yapılandırılmış.



Yazılım şifreleme sonunda ekrana kurbanı için bir fidye notu getiriyor, verilerin kurtarılması için parola satın alınması ve ödeme talimatları için "fantomd12@yandex.ru" veya "fantom12@techemail.com" adreslerinin kullanılması isteniyor.

Fidye zararlı yazılımlarının, bu örnekte görüldüğü gibi kullanıcıların güvenli olduğu düşüncesine kapılacakları şekilde tuzaklanarak bilgisayarlara kurulumlarının sağlanması, ne kadar aldatıcı olabildiklerini göstermesi açısından oldukça dikkat çekici.

Genel Değerlendirme (Zararlı Yazılımlar)

Tehdit Hedefi: Bütünlük ve Erişilebilirlik

Risk: Toplumun siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle zararlı yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.

Alınabilecek Karşı Önlemler:

- Kurumsal e-posta adreslerinin kişisel amaçlar için kullanılmaması,

- Kurumsal sistemlerde önemli ve hassas bilgilerin yedeklenmesi,

- Alınan bu yedeklere kullanıcı ağ bölümlendirmelerinden erişimlerin engellenmesi,

- Sistemlerin zafiyetlerinin sürekli olarak taranması ve giderilmesi,

- Şüpheli linkler ve e-posta eklerine tıklanmaması,

- Makroların varsayılan ayar olarak devre dışı bırakılması,

- Sistemlerde bulunan zararlı yazılım önleme yazılımlarının (Antivirüs, vb.) güncel bulundurulması,

- Siber güvenlik farkındalık eğitimlerinin verilmesi, tatbikatların ve testlerin periyodik olarak yapılması.

Siber Zafiyetler

Endüstriyel Kontrol Sistemleri Siber Saldırılara Açık

Endüstriyel Kontrol Sistemleri (EKS) 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 kullanılmaktadır. Akıllı şehirler, akıllı evler ve arabalar, tıbbi cihazlar hep EKS'ler tarafından kontrol edilmektedir.

EKS'ler İnternet'teki hızlı büyüme nedeniyle siber saldırganlar için kolay bir av niteliği kazanmışlardır. Başlangıçta birçok EKS çözümü ve protokolünün izole ortamlar için tasarlandığı dikkate alındığında, bu durum çoklu kabiliyetlere sahip siber saldırganlara güvenlik kontrollerinin eksikliğine bağlı olarak EKS'lerin arkasındaki altyapıları etkileme imkânı vermektedir. Bunun da ötesinde EKS'lerin bazı bileşenlerinin zaten kendileri korunmasızdır. Kaspersky Lab tarafından hazırlanan rapordaki ana bulgulara göre:

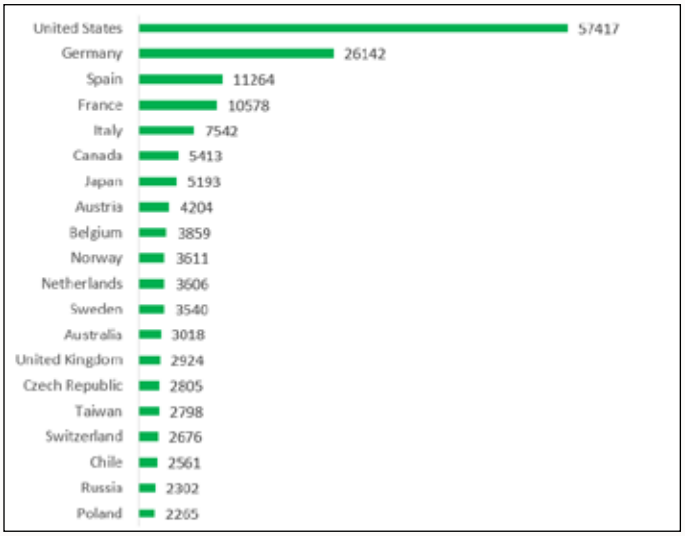
- EKS parçaları ile uyumlu 170 ülkede toplam 188.019 sistem bulunmaktadır.

- Uzaktan kontrol edilebilen ve EKS ile uyumlu parçaları bulunan sistemlerin büyük çoğunluğu Amerika Birleşik Devletleri (%30.5 – 57.417) ve Avrupa'da bulunuyor. Avrupa'ya bakıldığında ise Almanya'nın (%13.9 – 26.142) liderliği elinde bulundurduğu, onu takip eden ülkelerin ise İspanya (%5.9 – 11.264) ve Fransa (%5.6 – 11.264) olduğu görülüyor.

- Uzaktan kontrol edilebilen EKS'lerin %92'sinde (172.982) açık bulunuyor. Bu sistemlerin %87'si orta derecede zayıf nokta taşırken %7'sinin tehditlere açıklık oranı yüksek olarak belirlenmiştir.

- EKS bileşenlerinin zafiyetlerinin tespiti için eldeki ilk bilgiler 1997'yi göstermektedir. 1997'de tespit edilen zafiyet sayısı 2 iken o zamandan günümüze sürekli bir artış söz konusudur. Son beş yıl içinde (2010-2015) yayımlanan zafiyet sayısı 19'dan 189'a yükselmiştir. Tehditlere en açık EKS bileşenleri ise İnsan Makina Arayüzü (HMI), Elektronik Aygıtlar ve SCADA sistemleridir.

- Dıştan erişime açık EKS aygıtlarının %91.6'sı (172.338 farklı host) zayıf internet protokolleri kullanıyorlar ve bu da onları "ortadaki adam (man-in-the-middle)" tipi saldırılara karşı savunmasız kılıyor.



Kullanımı yaygınlaşan EKS'lerle ilgili araştırma sonuçlarından da görüleceği gibi, sistemlerin zafiyetlerinin arttığı, 21'inci yüzyıl koşullarına bağlı olarak dış sistemler ve ağlarla entegre ihtiyaçları bulunduğu ve buna bağlı olarak siber saldırılara karşı çok iyi korunması gerektiği anlaşılmaktadır. Bu kapsamda alınması tavsiye edilen önlemler aşağıda sıralanmıştır:

- Sistemlerin açıklıklarının bulunmasına yönelik sürekli olarak güvenlik denetimleri yapılması,

- Saldırıların tespiti ve müdahale hususlarında iyi bir siber güvenlik stratejisine sahip olunması,

- Sistemlerin gelişmiş siber güvenlik sistemleri ile korunması,

- Saldırıların önceden tahmin edilebilmesine yönelik olarak siber istihbarata önem verilmesi,

- Kullanıcıların siber tehditlere karşı farkındalıklarının artırılması.

Giyilebilir Teknoloji Ürünlerindeki Tehlike

Yapılan araştırmalar, giyilebilir teknoloji ürünlerinin siber korsanların ATM makinalarında kullanılan parolaları ele geçirmede nasıl kullanılabileceğini gözler önüne seriyor. Bu tür ürünler kullanıcılarının hareketlerini takip eden gömülü sensörlere sahipler. Bahse konu sensörler bu özellikleriyle kullanıcılarının klavye ve ATM tuş takımlarındaki el hareketlerini de yakalıyorlar. İşte korsanlar, giyilebilir teknoloji cihazı ile akıllı telefon arasındaki Bluetooth bağlantısı sayesinde gönderilen veri paketlerini kablosuz algılayıcılar kullanarak dinliyor ve böylece cihazlardaki sensör verilerini ele geçirip yorumluyorlar. Hatta ilave olarak korsanların bu tür cihazlara uzaktan yükleyecekleri zararlı yazılımı kullanarak verilerin kendilerine gönderilmesini bile sağlayabilecekleri ifade ediliyor. Veriler ele geçirildikten sonra giyilebilir teknoloji ürünlerini kullanan kişilerin tuş takımlarını nasıl ve hangi hızda kullandıkları analiz ediliyor. Kulağa zormuş gibi gelse de araştırmacıların kullanıcı parolalarını ilk denemede %80, üçüncü denemeden sonra ise %90'lık bir başarıyla tahmin edebildikleri ortaya konuluyor.

Maalesef giyilebilir teknoloji ürünlerini çekici kılan, sağlıklı ve formda olmak amacıyla bilgi sağlayan hareket sensörleri. Araştırmacılar, bu tür ürünlerin tasarımcı ve üreticilerine, cihazların çalışmalarına etki etmeyecek ancak korsanları yanıltabilecek bir takım gürültüler üretmesinin bir çare olabileceği tavsiyesinde bulunuyorlar. Yukarıda bahse konu korsanlığa tabi olmamak için şu aşamada alınabilecek tek tedbir ATM'lere parola girerken bu tür cihazların çıkarılması veya parola girişlerinin bu cihazların bulunmadığı el ile yapılması.

Üç Boyutlu Yazıcılar Sabotajlara Alet Olabilir

Üç boyutlu yazıcılar günümüzde oyuncak, giyim ve hatta yiyecek sektöründe kullanılıyor. Araştırmacılar hızla yaygınlaşan kullanımıyla birlikte bu teknolojinin endüstriyel sabotaj potansiyeli konusunda uyarılarda bulunuyorlar.

Araştırma firması Gartner, geçmişte üç boyutlu yazıcıları prototip oluşturmak için kullanan firmaların, son gelişmeler ışığında bu cihazları gerçek ürün üretiminde de kullanacaklarını öngörüyor. Bu durum gerçekleşirse firmaların olası suistimallere karşı tetikte olmaları gerektiği çünkü çoğu üç boyutlu yazıcının İnternet'e bağlı ve uzaktan kontrole açık olduğu ifade ediliyor. Siber korsanların bu tür yazıcıları hedef almaları ve üretim sürecinde dâhili sorunlar oluşturmaları mümkün görülüyor.

Örneğin; ürünlerin gerilmelere karşı daha az dayanıklı basılmasına yol açacak bir müdahale, ürünün zamanından önce parçalanmasına yol açabilir ve eğer bu ürün bir otomobil veya bir uçak bileşeni olarak basılıyor ise insan hayatını etkileyecek bir tehdit söz konusu demektir.

Küreselleşmeye bağlı olarak teknolojik yeniliklerin ülkeler arasında süratle yaygınlaşabildiğine tanık oluyoruz. Üç boyutlu yazıcılar konusundaki olası tehdit unsurunun da önemsenmesinin ve üretim planlamalarında bu tür yazıcıların İnternet'e bağlı olmadan kullanılmasına ve tasarım dosyalarının şifrelenmesine dikkat edilmesinin uygun olacağını değerlendiriyoruz.

SMS-Tabanlı İki Faktörlü Kimlik Doğrulamanın Sonu mu Geldi?

SMS-tabanlı iki faktörlü kimlik doğrulamanın (2FA - 2-Factor Authentication) güvensiz olduğu ve yakın bir gelecekte kullanım dışı kalacağı iddia ediliyor.

Artan veri güvenliği ihlallerine tedbir olarak, siber korsanların hesapları ele geçirmek için kullanıcının hem parolasına hem de mobil telefonuna sahip olmaları gerektiğinden yola çıkılarak birçok hizmet için SMS-tabanlı iki faktörlü kimlik doğrulama kullanımı standart hale gelmiş durumda.

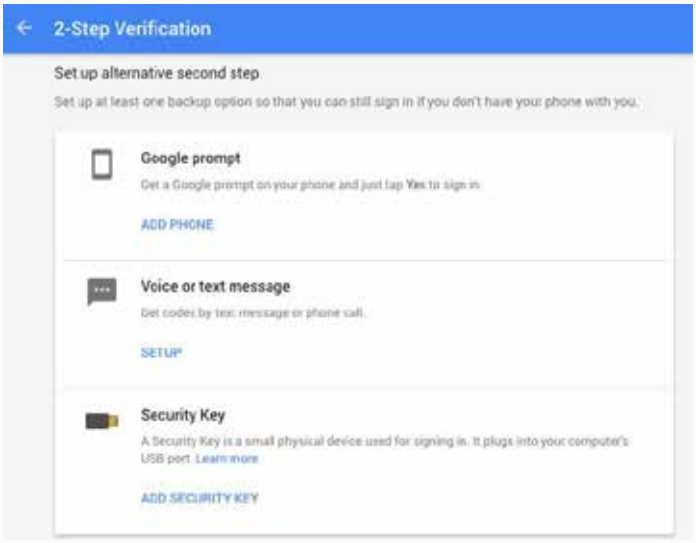
Bilindiği gibi iki faktörlü kimlik doğrulamada, kullanıcının hesabına girdikten sonra ilave bir koruma katmanı olarak kendisine SMS olarak veya çağrı

yoluyla iletilen rastgele belirlenen bir kodu girmesi isteniyor. Fakat ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST – US National Institute of Standards and Technology), yayımladığı son sürüm Dijital Kimlik Doğrulama Kılavuzunda (Digital Authentication Guideline) SMS-tabanlı iki faktörlü kimlik doğrulamanın güvenlik nedenleriyle gelecekte yasaklanması gerektiğini belirtiyor. NIST artık bir kişinin bir telefona sahip olmasının çok kolay olduğunu ve bir web sitesi işletmeninin 2FA kodunu doğru kullanıcının alıp almadığını teyit etmesinin mümkün olmadığı için uygulamanın güvensiz olduğunu ileri sürüyor.

SMS-tabanlı iki faktörlü kimlik doğrulama eğer kullanıcı geniş bant İnternet bağlantısı üzerinden telefon hizmeti sağlayan Voice-Over-Internet-Protocol (VoIP) servisi kullanıyorsa aynı zamanda çalınmaya karşı da zafiyete sahip. Bazı VoIP servislerinin SMS mesajlarının çalınmasına karşı da zafiyetleri bulunduğundan, korsanlar SMS-tabanlı iki faktörlü kimlik doğrulama ile korunan kullanıcı hesaplarını da ele geçirebilirler. Hatta bazı cihazlar SMS yoluyla alınmış gizli 2FA kodlarını kilitlenmiş ekranda bile gösterebilirler.

Bütün bu risklere karşı NIST iki faktörlü kimlik doğrulamada güvenli bir uygulama veya biyometri kullanımını öneriyor.

Diğer taraftan Facebook ve Google gibi bazı teknoloji firmaları, SMS veya ağ kullanımına dayanmayan uygulama içi kod üreteçlerini iki faktörlü kimlik doğrulama için alternatif bir çözüm olarak sunuyor. Bu kapsamda, Google son olarak "Google Prompt"



adını verdiği ve kullanıcının hesabına girişini onaylaması için mobil telefonuna hafifçe vurmasını gerektiren basit bir anlık bildirim uygulamasını hizmete sundu.

Her ne kadar güvenliği tartışılmaya başlasa da sanal ortamda aldığımız hizmetlerde SMS-tabanlı iki faktörlü kimlik doğrulama vazgeçilmezlerimiz arasında yerini almış durumda. Şu aşamada, bilgisayarlarda ve akıllı cep telefonlarında mutlaka güncel ve pro-aktif bir güvenlik uygulaması kullanılmalı, hizmet sunan kurumların getireceği yeni iki faktörlü kimlik doğrulama çözümlerini takip edilmelidir.

Siber Güvenlik Altyapısı

NATO'da Siber Uzay Artık Bir Askerî Harekât Alanı

8-9 Temmuz 2016 tarihinde Varşova'da gerçekleştirilen NATO zirvesinde, siber uzay hava, kara ve denize ilave olarak askeri harekât alanı olarak resmen kabul edildi.

Bu, ittifak üyesi 28 ülkenin politik ve askeri en üst seviye otoritelerinin, ağ güvenliği ile ulusal güvenlik arasında doğrudan bir ilişki olduğunu teyit ettiklerinin ve ulusal kritik altyapıların düşmanca bir siber saldırıya karşı korunması gerektiği konusunda hem fikir olduklarının en önemli göstergesi olarak kabul ediliyor. Bu karar aynı zamanda NATO'nun İnternet'i bir savaş alanı olarak kabul ederek olası siber saldırılara karşı ittifakın konvansiyonel silahlarla karşılık vermesinin önünü de açıyor.

Alınan kararla, NATO üyesi ülkelerden birisinin kritik altyapılarına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabileceği, bu nedenle üye ülkelerin siber savunma imkân ve kabiliyetlerinin artırılmasının önemi de vurgulanıyor.

Günümüzde siber saldırılar, ittifakın güvenliği için açık bir tehdit oluşturmakta ve modern toplumlar için konvansiyonel saldırılar kadar zararlı olabilmektedir. Zirvede, siber savunmanın NATO'nun müşterek savunmaya yönelik temel görevinin bir parçası olduğu ve siber uzayın NATO'nun kendisini hava, kara ve denizde etkinlikle koruduğu harekât alanının bir parçası olarak tanınması konusunda mutabık kalındı.

Varşova Zirvesinde siber savunmanın ön plana çıkmasının ardından, uzmanlar tarafından ittifakın siber saldırı kabiliyetleri sorgulanmaya başlandı. Birçok ülkenin siber saldırı kabiliyetlerini artırmak için çaba gösterdiği günümüzde, ittifakın siber saldırı konusundaki niyetlerinin ve bu yönde bir niyet varsa nasıl gerçekleştirileceğinin açıklığa kavuşturulması gerektiği tartışma konusu. Bu konuda diğer bir sorun da NATO dışı ülkelerin, NATO'nun yeni siber güvenlik yaklaşımına verecekleri tepkiler. Bazı uzmanların görüşleri, o ülkeler tarafından verilecek benzer kararların siber uzayın askerileşmesini hızlandıracağı, Bilgi Harbi konusundaki tartışmaları ve ortaya çıkan soruları ilgilendiren yeni bir hukuki çerçeveye olan ihtiyacı körükleyeceği yönünde.

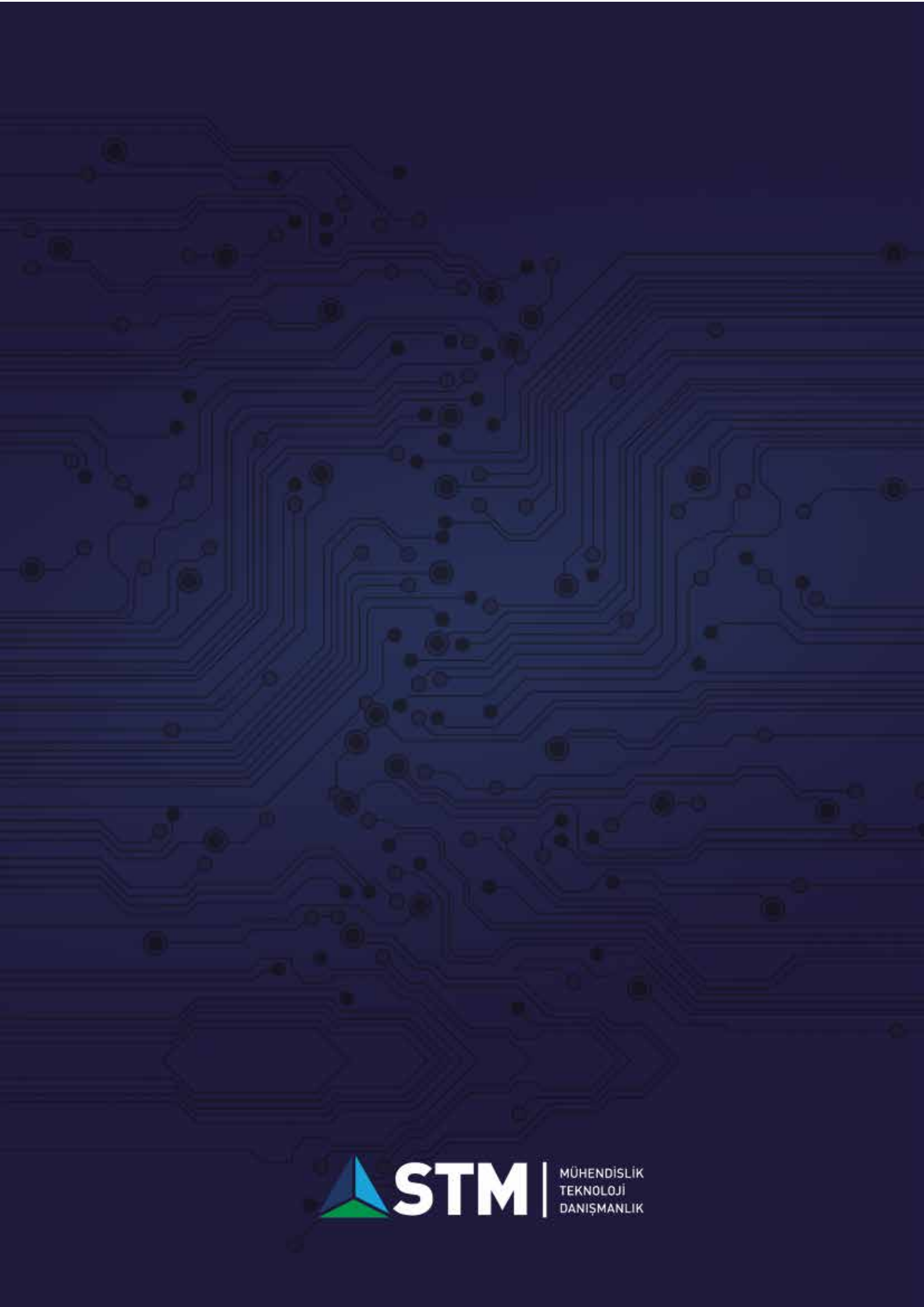
2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Tanıtıldı

"2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" 9 Eylül 2016 tarihinde gerçekleştirilen bir toplantı ile tanıtıldı. Toplantıda, Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan tarafından, Türkiye'nin 4 yıllık süreçte siber güvenlik konusunda izleyeceği yolu belirleyen 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın amacının; 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 kazanılması olduğu ifade edildi ve söz konusu strateji ile eylem planının, 5 ana eylem ve 41 alt eylemden oluştuğu kaydedildi.

Ulusal Siber Güvenlik Stratejisi içerisinde yer verilen siber güvenlik risklerine karşılık belirlenen eylemlerin;

- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması,
- Siber Suçlarla Mücadele,
- Farkındalık ve İnsan Kaynağı Geliştirme,
- Siber Güvenlik Ekosisteminin Geliştirilmesi,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu

ana stratejik eylem başlıkları altında gerçekleştirilmesi planlanmaktadır. Siber ortama ait tehditlerin günümüzde ulaştığı ve gittikçe artan seviyesi dikkate alındığında, ana eylemlere bağlı 41 alt eylem için kamu, özel sektör, STK ve diğer paydaşların, belirlenen sorumluluklar doğrultusunda vakit kaybetmeden çalışmalarını planlayıp tamamlamaları milli güvenliğimiz için gerekli görülmektedir. Bu açıdan, yürütülecek çalışmaların bütüncül yapıda ele alınarak etkin koordinasyonunun sağlanmasının ve neticelerinin ilgili paydaşlarla paylaşılmasının büyük öneme sahip olduğu değerlendirilmektedir.


STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK