SİBER TEHDİT DURUM RAPORU

EKİM-ARALIK 2018

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

Siber güvenlik bakımından hareketli bir yılı daha tamamlamış olduk. Bu sene içinde karşılaşılan siber tehditlerin yanı sıra siber güvenlik alanını ilgilendiren yasa ve yönetmeliklerin de gündemde yer almaya başladığını gördük. 2018 yılı boyunca keşfedilen zafiyetler, saldırı yöntemleri, tehdit aktörleri ve geliştirilen güvenlik çözümleri küresel çapta siber güvenlik alanında kat edilen mesafenin hem saldırı hem de savunma kısımlarında bir dengeye doğru ilerlenmekte olduğunu gösteriyor. Her ne kadar savunma alanda gerçekleşen girişim ve yaptırımların sayısında artış olsa da yıl boyunca gerçekleşen siber olaylar saldırı kısmın üstünlüğü koruduğuna işaret ediyor.

Sene boyunca devam eden sosyal mühendislik ve oltalama saldırılarının ardı arkası kesilmiyor. Sahte uygulama ve siteleri sosyal medya platformlarında reklam şeklinde paylaşan saldırganlar ağırlıklı olarak finans sektörüne yönelmiş durumda. Ağırlıklı olarak Twitter'da karşımıza çıkan bu tehditler hakkındaki gelişmelerin devamını siber tehdit istihbaratı ve zararlı yazılım analizi kısımlarında bulabilirsiniz.

Finans sektöründen bağımsız olarak havacılık endüstrisi de siber saldırılardan payını almış durumda. Uçaklarda çalışan yüzlerce uygulama siber saldırganların yeni hedefi durumuna gelmiş bulunuyor. Önümüzdeki dönemde trend haline gelmesi muhtemel bu konu üzerine çalışmalara ihtiyaç olduğu değerlendirilirken, STM analistlerinin yaptığı çalışmada bu detaylara değiniliyor.

Sene içerisinde birçok güvenlik güncelleştirmesi yayınlayan Microsoft güvenlik anlayışında bir ilke imza attı. "Windows Defender" ürününe "Kum Havuzu" yetenekleri kazandıran Microsoft bu yaklaşımın sahada bir ilk olduğunu belirtti. Atılan yeni bu yeni adıma paralel olarak, "Microsoft Word" yazılımında zararlı kod çalıştırılmasına olanak sağlayan bir zafiyet keşfedildi. Öte yandan sunulan güncellemelerin kritik bir ayardaki varsayılan değeri değiştirmesi sonucunda "Microsoft Mağaza" uygulamalarının kullanıcı verilerine ulaştığı ortaya çıktı.

Facebook vakası olarak da bilinen ve şirket yöneticilerini Amerikan Senato komisyonu karşısına çıkaran veri mahremiyeti ihlallerinin ardından Facebook'ta yeni bir veri sızıntısı oluştuğu ortaya çıktı. Açıklığın Facebook'taki "başkasının gözünden gör" (View as) özelliği üzerinden ortaya çıktığı açıklandı. Bu durum sosyal medya ve veri güvenliği konularının yeniden gündeme gelmesine neden oldu.

İsmi sıklıkla IoT (Internet of Things) teknolojisi ile birlikte anılan Bluetooth teknolojisi, v5.0 ile piyasalarda yerini korumakta. Güncel mobil cihazların büyük kısmında ön tanımlı sürüm olarak gelen Bluetooth 5.0'dan önceki serilerin kullanımı da devam etmekte. Bunlar arasında bulunan Bluetooth 4.0 sürümüne ait BLE çiplerinde yeni bir zafiyet keşfedildi. BLEEDINGBIT olarak adlandırılan ve Cisco ve Aruba network ürünlerini etkilediği belirtilen zafiyet saldırganların söz konusu cihazın kontrolünü ele geçirmesini sağlıyor.

Teknolojik gelişmeler siber güvenlik alanında elde edilen saldırı-savunma kapsamındaki keşiflere de yansıyor. Bu kapsamda dönem raporumuzda; 802.1X standardı ve MACsec güvenlik mekanizmasının atlatılması, Konteyner yapılarındaki çoklu yapıların atak yüzeyini artırması, HL7 standardı üzerinde gerçekleştirilen ortadaki adam (Man In the Middle) saldırıları, parmak izi güvenlik sistemlerinin kopyalanabilmesi, Tesla araçlarının ele geçirilmesi ve IoT cihazlarındaki zararlı yazılım tehlikesiyle ilgili STM siber güvenlik uzmanları tarafından hazırlanan analizler yer alıyor.

Siber güvenlik eğitimleri küresel çapta yeni bir boyut kazanmış durumda. Ülke birliklerinin oluşturduğu eğitim ve tatbikat çalışmalarına olan ilgi artmakta. Bu bağlamda NATO bünyesinde planlanan Siber Koalisyon Tatbikatı geçtiğimiz günlerde tamamlandı. Birçok NATO ülkesinin katıldığı tatbikat konseptini anlatan çalışmamızı raporumuzda bulabilirsiniz.

Siber güvenlik alanında kişi ve kurumların kendilerini sınayarak zayıf yönlerini görmelerini, kendilerini geliştirme imkânı sağlamalarını ve bu alanda çalışan tüm paydaşların tek çatı altında birleştirilmesini ve bilgi paylaşım ağının oluşturulmasını amaçlayan STM Capture The Flag (CTF) yarışmalarından dördüncüsünü 28-29 Eylül 2018 (Online-Ön Eleme) ve 31 Ekim 2018 (Offline-Final) tarihlerinde Ankara'da düzenlemenin heyecanını yaşadık. Bu etkinliğimize ait detaylı bilgi, raporumuzun dönem araştırma konusu başlığı altında yer almaktadır.

2019 yılında hepimiz için siber tehditlerin azalması ve siber tehditlere karşı farkındalığımızın artması dileklerimizle...

2018 yılının siber tehditler yönüyle genel bir değerlendirmesi ile 2019 yılına ait beklentilerden oluşan bilgileri giriş kısmının devamında inceleyebilirsiniz;

1. 2018 Yılı Siber Tehdit Değerlendirmemiz

2017 Ekim-Aralık dönemi Siber Tehdit Durum Raporu'muzda, 2018 yılı için küresel ölçekte ön plana çıkmasını beklediğimiz siber saldırı trendleri olarak şunlar sayılmıştı:

- Fidye yazılım tehdidi (Ransomware),
- Kripto para madenciliği,
- Nesnelerin İnterneti (IoT) cihazlarıyla ilişkili saldırılar,
- Siber saldırılarda yapay zekâ ve makine öğrenmesi kullanımı,

- Kritik altyapılar ve sağlık sektörünü hedef alan saldırılar,
- Devlet destekli saldırılar ve siber casusluk,
- Bulut bilişim verilerine yönelik tehditler,
- Mobil sistemler aracılığıyla siber korsanlık,

Bu noktalarla bağlantılı birçok konuda nabzın yüksek seyrettiğini değerlendirebiliriz. 2018 yılı içinde sunduğumuz rapor içeriklerinde de vurgulandığı gibi küresel çapta yürütülen ransomware saldırılarında dikkat çeken gelişmeler olduğunu gördük. Ransomware saldırılarında yeni varyantların türemesi en çok dikkat çeken gelişmelerden biri olurken, kripto para madenciliği alanında da bulut bilişim ve mobil sistemleri de etkileyen yeni saldırılar gündemdeydi. Bahsi geçen olayların yanında devlet destekli siber saldırı ve casusluk operasyonlarının devam ettiği, kritik altyapıları hedef alan zararlı yazılımların yeni saldırılarda yer aldığı açığa çıktı. IoT cihazlarla ilgili saldırılar dikkat çekerken saldırıların yapay zekâ ve makine öğrenmesi yönünde ilerlemesi bir diğer önemli gelişme oldu. Bunların dışında gelişen siber olaylar ise şöyle sıralanabilir:

- Terör motivasyonlu saldırı gruplarının aktiviteleri,
- Özelleştirilmiş sosyal mühendislik ve oltalama saldırıları,
- Veri sızıntıları,
- Veri koruma kanun ve yaptırımlarıdır.

Terör motivasyonlu saldırılar konusunun ülkemizde yeniden gündeme gelmesi, 2018 yılının ilk çeyreğinde yayınladığımız "Ocak-Mart 2018" tehdit raporumuzda yer alan "*Zeytin Dalı Harekâtı ve Terör Kaynaklı Tepkisel Siber Saldırı Analizi*" başlıklı makalemiz ile oldu. Bu bağlamda Türk Silahlı Kuvvetleri (TSK) tarafından gerçekleştirilen "Zeytin Dalı Harekâtı"nın dünya basınında oldukça ses getirmesinin akabinde gerçekleşen siber saldırıların, dünya siyasetinin siber savaşlardaki doğrudan/dolaylı etkisini daha net gösterdi. Zeytin Dalı Harekâtı ile yeniden gündeme gelen bu örneğin önümüzdeki yıl küresel çapta daha çok gündeme geleceğini değerlendirmekteyiz.

Siber casusluk faaliyetleri ile adından söz ettiren Lazarus Group'un, finans sistemlerini hedef alan saldırılarda kullandığı "Bankshot" isimli yazılımın geliştirilmiş bir sürümüyle geri döndüğü yıl içinde tespit edildi. Bu bağlamda "APT37", "FIN7" ve "Carbanak" gibi devlet destekli tehdit aktörlerinin de gündeme gelmesi, uluslararası temasların siber operasyonların yöneliminde etkili bir faktör olduğunu gösterdi. Ayrıca, "Dragonfly/Energetic Bear/Crouching Yeti" olarak bilinen siber casusluk grubunun yeniden harekete geçmesinin tespit edilmesinin akabinde saldırılarda kritik altyapıların da hedeflendiği ve söz konusu saldırılarda başta Rusya olmak üzere Türkiye, Ukrayna ve birçok Avrupa ülkesinin hedef alındığı ortaya çıktı.

Teknolojik gelişmeler kapsamında ise; IoT güvenliğine yönelik yapılan araştırmalarda IoT ortamlarının kripto para madenciliği ve botnet oluşturma gibi amaçlar için kullanıldığı ve bu bağlamda güvenlik alanında kat edilmesi gereken hayli uzun bir yol olduğu ortaya çıktı. Buna ek olarak "cryptojacking" gibi yeni saldırı çeşitleri kendinden söz ettirdi. Ayrıca bilgisayar donanımlarına ait ısı, ses ve ışık analiziyle kullanıcıların parola ve ekran görüntülerinin elde edilebilmesi dikkat çeken diğer bir önemli gelişme olurken yeni-eski teknoloji sınıfında değerlendirilen faks makinelerinin ağ içinde oluşturabileceği tehditler dikkat çekici diğer bir konu oldu.

Sosyal Mühendislik saldırıları alanında 2018 yılı içinde birçok oltalama saldırısı gerçekleşti. Saldırıların büyük çoğunluğunda e-posta eklentileri kullanılırken, sponsorlu saldırı türlerinde (oltalama saldırılarının sosyal medya ortamlarında reklam olarak yayınlanması) ciddi bir artış olduğu gözlemlendi. Bu kapsamda küresel etkinlikleri de değerlendiren saldırganlar dünya kupasına ve kış olimpiyatlarına yönelik oltalama saldırıları gerçekleştirdi. Bunların yanı sıra güvenli olarak kabul edilen dijital marketlerde ortaya çıkan sahte uygulamalar birçok kullanıcıyı etkiledi. E-posta ve sahte uygulamalar üzerinde yoğunlaşan saldırıların ana hedefinin mobil cihazlara erişim ve kullanıcıların banka hesap bilgileri olduğu görüldü.

Yapay Zekâ uygulamalarıyla zafiyetlerin tespit, sömürme, sistem savunma ve tepki verme aşamalarında etkili yetkinlik ve otomasyon sağlanması gündeme gelen bir diğer konuydu. Bu alanda geliştirilen ürünlerin gelecek dönemdeki saldırı-savunma dengesini etkileyeceği değerlendirilmektedir.

2017 yılının ikinci çeyreğinde keşfedilen donanım tabanlı iki zafiyet 2018'in ilk çeyreğinde de gündemden düşmedi. Bu zafiyetlerin Intel ve AMD işlemcilerini etkilediği ve son 15-20 yıl içinde üretilen hemen hemen tüm işlemcileri kapsadığı belirtildi. Meltdown ve Spectre olarak tanımlanan bu iki zafiyet dünyadaki birçok bilgisayar kullanıcısını etkileyebilecek potansiyelde olduğu için işlemci tasarımları yeniden değerlendirildi.

7 Nisan 2016 tarihinde yürürlüğe giren "Kişisel Verileri Koruma Kanunu" (KVKK)'nun 7 Nisan 2018 tarihinde sona eren geçiş süreci tamamlandı. Buna paralel olarak Avrupa Birliği'nde 24 Mayıs 2016 tarihinde yürürlüğe giren "General Data Protection Regulation" (GDPR)'na uyum süreciyle ilgili 25 Mayıs 2018 tarihine kadar olan geçiş süreci de tamamlandı. Kişisel verilerin mahremiyeti konusuna yoğunlaşan bu iki kanun birçok sosyal medyaya ve dijital içerik toplayan kurum ve kuruluşa yönelik incelemelerde bulunulmasını getirdi. Bu süreçte popüler sosyal medya uygulamalarından Facebook ve Google+'a yönelik hukuki süreç başlatıldı. Yıl boyunca kişisel verileri toplama ve işleme bağlamında birçok kurum ve kuruluşa ciddi yaptırımlar uygulandı. Veri mahremiyeti konusundaki yaptırımlar gündemdeki yerini korurken aralarında sosyal medya platformları, bilet satış merkezleri ve otel/tatil

sektörlerinin de bulunduğu birçok veri sızıntısı vakasının ortaya çıkması ayrı bir gündem maddesi oldu.

2. 2019 Yılı Siber Tehdit Öngörülerimiz

2019 yılında siber tehdit olarak ön plana çıkacağını değerlendirdiğimiz hususları aşağıdaki başlıklar altında sunuyoruz:

2.1. Kritik Altyapıları Hedef Alan Özelleştirilmiş Saldırıların ve Siber Casusluğun Artması

Son yıllarda devlet destekli saldırıların artış gösterdiği dikkate alınırsa, bu alanda faaliyet gösteren aktörlerin sayısında artış olacağını ve yürütülen operasyonlarda yeni yöntemlerin yanı sıra eski saldırı vektörlerinin de güncelleştirilerek kullanılacağını ve bu kapsamda yürütülen siber casusluk operasyonlarının artış göstereceğini değerlendirmekteyiz.

2.2. Makine Öğrenmesi ve Yapay Zekâ Yeteneklerinin Siber Saldırılarda Kullanılması

Makine Öğrenmesi ve Yapay Zekâ yeteneklerinin savunma alanında kullanımına eş zamanlı olarak saldırı alanda da kullanılmaya başlayacağını ve bunun sonucunda siber saldırıların yeni bir boyut kazanacağını öngörmekteyiz.

2.3. Hizmet Olarak Suç İşleme (CaaS) Servisleriyle Gelen Tehlike

Fidye (ransomware) saldırılarında yeniden gündeme gelen CaaS olayının geliştirmesi ve hedef cihazlara Ransomware ve botnet bağlantısının yanı sıra Gamarue gibi zararlı yazılımların da yüklenmesiyle bu alandaki saldırıların artış göstereceği değerlendirilmektedir. Ayrıca, mevcut CaaS seçenekleri arasında hedefe zarar verme, servis dışı bırakma ve veri sızdırma saldırılarının KVKK ve GDPR yaptırımlarıyla ilişkilendirilerek gerçekleştirileceğini öngörmekteyiz.

2.4. IoT Ortamlarını Hedef Alan Saldırılarda Artış

Ransomware saldırılarının yeni hedefleri arasında yer alacağını değerlendiğimiz IoT platformlarının botnet ağlarına katılma oranları göz önünde bulundurulduğunda; gelecek dönemde bunların sayısında artış olacağı ve IoT cihazlarının botnet kapsamında DDoS saldırılarında ve kripto para madenciliği saldırılarında kullanılacağını değerlendirmekteyiz.

2.5. Biyometrik Kimlik Doğrulama Sistemlerinde Oluşacak Tehlikeler

Biyometrik kimliğin giriş sistemlerinde kişiye özgü eşsiz kimlik sağlaması bu uygulamanın güvenlik alanında hızla kullanılmaya başlamasını getirdi. Kullanım alanı mobil cihazlardan gizli bilgilerin tutulduğu veri depolarına kadar uzanan bu sistemin geleneksel parolalara göre nispeten daha güçlü ve aşılması zor bir güvenlik sağladığı bilinmektedir. Bu alanda yapılan güvenlik araştırmaları göz önünde bulundurulduğunda; biyometrik güvenlik mekanizmalarına yönelik siber saldırıların artış göstereceği ve hali hazırda kısmen kopya/taklit edilebilen parmak izi/iris tanıma model anahtarlarının da siber saldırganlar tarafından aşılabileceğini ve çoklu faktör (multi factor) güvenlik mekanizmalarının gündeme geleceğini öngörmekteyiz.

2.6. Anti-Sandbox Yeteneği Kazandırılmış Yeni Nesil Malware Saldırıları

Yeni nesil zararlı yazılımların sanal cihazları ve kum havuzu ortamlarını tespit etme yeteneklerinin dikkat çektiği son dönemde, söz konusu zararlı yazılımların tespit edilmesinin zorlaşacağını ve bu alanda yapılacak saldırıların artarak devam edeceğini değerlendirmekteyiz.

2.7. Ransomware Saldırılarının Birçok Platforma Yayılması

Hizmet Olarak Suç (Crime as a Service – CaaS olayının gelişmesinin de etkisiyle) Ransomware saldırılarının devam edeceğini; düşük beceri, düşük maliyet ile yüksek kazanç dengesi sonucu yasadışı getiri nispeten daha yüksek olduğu için saldırıların bulut platformlarına (veri depolama ve servis barındırma hizmetleri vb.), IoT ortamlarına ve kritik altyapılara da yöneleceğini değerlendiriyoruz.

2.8. Ön Tanımlı Parolaların Oluşturduğu Güvenlik Açıkları

2018 yılında ifşa olan parola listelerinin incelenmesi sonucunda en sık kullanılan parolalar arasında ön tanımlı parolalar ile gizliliği ifşa olmuş parolaların önemli bir yer tuttuğu görülüyor. Siber uzaydaki cihazların artış hızını da göz önünde bulundurduğumuzda; bu tarz zayıf güvenlik uygulamalarının önümüzdeki dönemde birçok saldırıya temel olacağını öngörmekteyiz.

Sonuç olarak 2019 yılında siber tehditler olarak aşağıdaki konuların ön plana çıkacağını öngörüyoruz:

- Siber casusluk faaliyetleri ve kritik altyapı güvenliği,
- Siber saldırılarda Makine Öğrenmesi ve Yapay Zekâ kullanımı,
- Hizmet olarak Suç İşleme (CaaS) Servisleri,
- IoT güvenliği,
- Biyometrik güvenlik sistemlerine yönelik saldırılar,
- Geliştirilmiş/özelleştirilmiş zararlı yazılımlar,
- Fidye yazılım türleri,
- Ön tanımlı ve zayıf parola kullanımları,

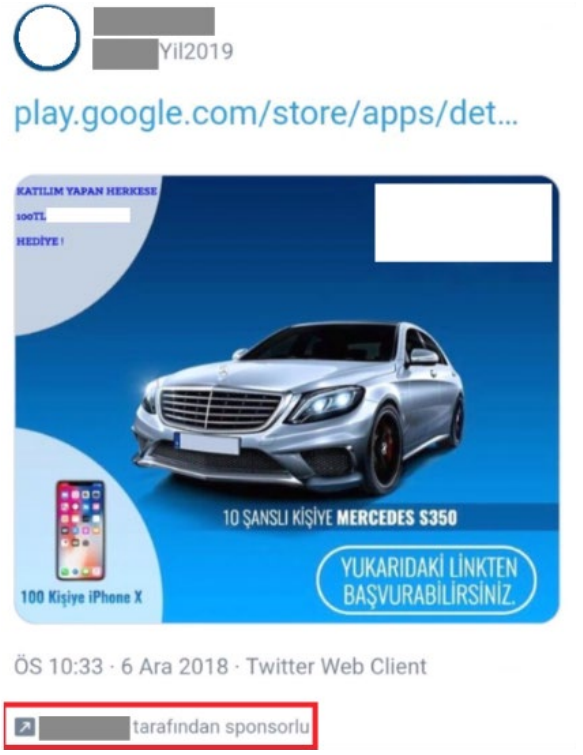
SİBER TEHDİT İSTİHBARATI

3. Bankalara Yönelik Oltalama Saldırı Girişimleri Devam Ediyor

Bankalara yönelik oltalama saldırıları her geçen gün yeni bir saldırı trendi ile karşımıza çıkmaya devam ediyor. Bir önceki dönem raporumuzda belirttiğimiz gibi bu tarz oltalama saldırıları farklı tema ve kurumlar üzerinden devam etmekte. Geçen dönem bir banka üzerine yoğunlaşan oltalama saldırılarının, bu dönem üç ayrı banka müşteri kitlesini hedef alacak şekilde güncellenmiş olduğu STM analistlerince gözlemlendi. Saldırıların popüler sosyal medya uygulamaları üzerinden reklam verilerek "sponsorlu" ibaresi ile yayınlanması güncel saldırının önceki saldırılarla ilişkisi olabileceğini düşündürtüyor. Bu saldırılarda bankalara ait kampanyaların görsellerini kullanarak kullanıcıları kampanya/çekiliş adı altında kopyalanmış/sahte sitelere yönlendiren saldırganların, kullanıcıların kişisel bilgilerini ve bankacılık işlem bilgilerini ele geçirmeyi hedeflediği tespit edilmiştir.

Tespit edilen üç farklı oltalama saldırısından ikisinin kullanıcıları sahte sitelere yönlendirmeye çalıştığı dikkatleri çekerken, diğer saldırının da kullanıcıları uygulama mağazasından sahte bankacılık uygulaması indirmeye yönlendirdiği gözlemlendi. Yönlendirme yapılan sahte sitelerden birinin SSL sertifikasına sahip olması, saldırının özenli bir şekilde hazırlandığını göstermektedir.

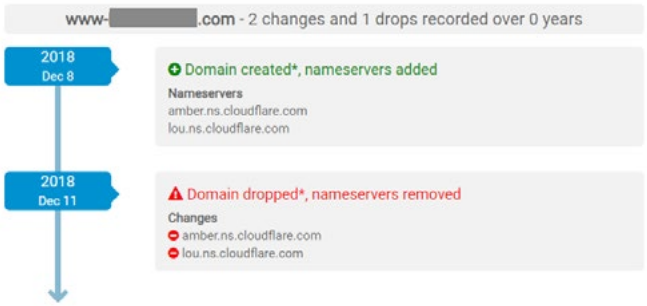
Kullanılan domain adreslerinin ""www-*bankadi*.com" "*bankaadi*-hediyeleri.com" formatında olduğu ve uygulama isimlerinde de hedef kullanıcı kitlesini ikna etme amacıyla bankalarına ait kredi kartı isimlerinin kullanıldığı



Şekil 2: Sahte uygulamalara yönlendirme yapan oltalama saldırısına ait reklam

tespit edildi. Söz konusu oltalama saldırıları karşısında kullanıcıların farkındalıkları ile yapılan paylaşım ve uyarılar sonucunda, oltalama saldırılarında kullanılan sosyal medya profillerinin (@bankaadibanka, @BankaAdi ve @ bankaadi_Anketi) askıya alındığı, ilişkili alan isimlerinin bazılarının iptal edildiği gözlemlendi.

Şekil 1: Sahte sitelere yönlendirme yapan oltalama saldırılarına ait reklamlar

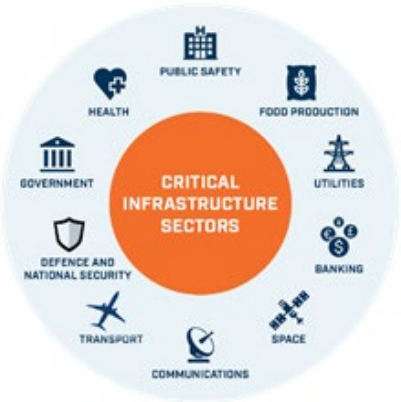


Şekil 3: Sosyal medya üzerinde gelişen farkındalık üzerine iptal edilen sahte alan adı

Bahsi geçen saldırılarda görsellere kurumların uyguladıkları kampanyalara ek hediyeler (araba, puan, telefon) ekleyerek kullanıcıların dikkati çekilmeye çalışılmıştır. Benzer saldırıların farklı kurum ve kuruluşlara ait açıklama/kampanyalar üzerinden devam edeceği ön görülmektedir. Özelikle sene sonunun gelmesiyle saldırganların *"Yılbaşı", "xxxx-2019", "Yeni Yıl", "Ödül" "Kampanya", "Hediye" ve "Müşteri Bağlılığı"* temalarını kullanabilecekleri öngörüldüğünden, kullanıcıların sosyal medya ve e-posta aracılığıyla haberdar oldukları gelişmeleri/kampanyaları ilgili kurum ve kuruluşa ait resmi kanallardan teyit etmeleri önerilmektedir. Geçen dönem görmüş olduğumuz gibi, farkındalık seviyesinin artması bu konuda alınacak en iyi önlemlerden biri olarak değerlendirilmektedir. Kullanıcıların fark ettikleri saldırıları ilgili kurumla paylaşıp teyit alması ve ilgili tehlikeyi sosyal medya platformlarında raporlayarak/paylaşarak diğer kullanıcıları uyarmaları tavsiye edilmektedir.

4. Siber Güvenlik Perspektifinden Havacılık Endüstrisi

Havacılık sektörü, ülkemizde ve dünyada hızlı bir gelişme ve büyüme gösteren en önemli sektörlerden biridir. Birçok alt sektörü de olan havacılık sektörü işlevini kısmen veya tamamen yerine getiremediğinde çevre, toplumsal düzen ve kamu hizmetlerinin yürütülmesi üzerinde çeşitli olumsuz sonuçlar ortaya çıkar. O nedenle havacılık sektörünün ağ, varlık, sistem ve yapıları kritik altyapı sektörleri arasında yer alır.



Şekil 4: Kritik altyapı sektörleri

Havacılık sektörünün kendi yapısına özgü, çok sayıda optimizasyon ve karar problemi söz konusudur ve bunlar tartışma konusudur. Literatürde; havacılık endüstrisinin yolcu sayısının ve trafiğinin tahmini, yedek parça talep tahmini, kapı atama, filo atama, uçuş çizelgeleme ve gelir yönetimi gibi problemlerinin çözümüne yönelik çok sayıda çalışma yer almaktadır. Ayrıca, havacılık endüstrisindeki yeni bir havaalanı seçimi, havayolu rekabetinin değerlendirilmesi, havaalanı hizmet kalitesinin değerlendirilmesi, stratejik ortak seçimi, tedarikçi seçimi, dış kaynak sağlayıcı seçimi ve verimlilik analizi gibi karar verme problemleri bulunmaktadır[1].

Yukarıda sayılan problemlerin çözümünde kullanılan yazılımlar ve havayolu şirketlerinin kullandığı üçüncü parti uygulamalar doğrudan veya dolaylı olarak siber saldırıların hedefinde olan uygulamalardır.

Sivil havacılığın yasadışı müdahalelere karşı korunması için işgücü, zaman ve maddi kaynak faktörlerinin birlikte ele alındığı bir senaryo düşünülmesi gerekir. Bu sektörde sadece güvenlik yatırımı veya sadece nitelikli işgücü yatırımıyla sürdürülebilir güvenlikten söz edilemez.

Havacılık endüstrisinin bağlayıcı sektörlerine baktığımızda, bu kritik altyapının

- Savunma ve Milli Güvenlik
- Ulaşım
- Haberleşme
- Bankacılık
- Enerji Sistemleri

ile doğrudan bağlantılı olduğu görülür. O nedenle bu sektörlerde meydana gelebilecek bir bilgi güvenliği ihlali veya bir siber saldırıda havacılık sektörünün de doğrudan etkilenebileceği açıktır.

Havacılık sektöründe güvenlik değerlendirmesi birkaç ana başlık altında yapılmaktadır. Uçuş güvenliği, sivil havacılık güvenliği, siber güvenlik ve siber güvenlik yönetişimi bizi doğrudan ilgilendiren ana başlıklardır.

4.1. Risk Bazlı Yönetim Yaklaşımı

Risklerle ilgili uygun önlemlerin belirlenebilmesi için tehdit seviyesi sürekli gözden geçirilmeli ve güncel tutulmalıdır. Ulusal ve bölgesel gelişmeler göz önünde bulundurularak risk değerlendirilmesi yapılmalıdır

Havacılık sektörüne yönelik belirli bir tehdit oluştuğunda, önceden belirlenmiş güvenlik önlemleri uygulanmalıdır. Bu noktada "Siber Güvenlik" ekosistemi, havacılık sektörü için kritik seviye önem ifade etmektedir.

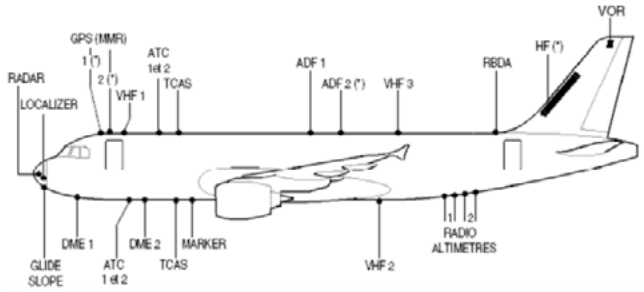
4.2. Havayolu Araçları Güvenliği

Havayolu araçları genelinde siber güvenlik; bir havayolu aracının sistemlerini doğrudan ya da dolaylı olarak teh-

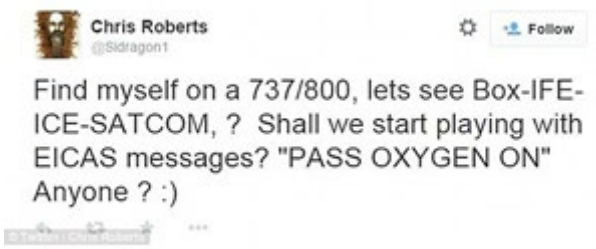
likeye sokmak amacıyla, siber araçlarla yapılan kasıtlı kötü niyetli eylemlerin önlenmesi ve/veya tepki gösterilmesi olarak tanımlanabilir.

Airbus'ın siber güvenlik için kurduğu "*Airbus Cybersecurity*" isimli şirketin bünyesinde 10'dan fazla ülkeden 650'nin üzerinde güvenlik uzmanı bulunması havacılık sektöründe siber güvenliğin çok uluslu kurum ve kuruluşlar tarafından önemsendiğini göstermektedir.

Bir Airbus A380 seyrüseferdeyken yaklaşık bin kadar uygulama çalışır haldedir. Bir keresinde Chris Roberts isimli bir güvenlik uzmanının uçak eğlence sistemi üzerinden motorlardan birini tırmanma moduna geçirdiği bilinmektedir. Bu kişinin FBI'ya verdiği dokümanlarda Boeing 737,757 ve Airbus A-320 uçaklarına 15 ila 20 kez sızdığı görülmektedir[2].



Şekil 5: Bir Airbus A380 uçağında yer alan elektronik haberleşme sisteminin bir kısmı



Şekil 6: Chris Roberts'in konuyla ilgili Twitter paylaşımı

Motor indikasyonu ve Kabin Alarm Sistemini (EICAS) devreye alarak oksijen maskelerini açmanın mümkün olduğunu iddia eden Roberts, FBI tarafından Syracuse'de yaklaşık 4 saat süren bir sorguya maruz kalmıştır.

4.3. Temel Güvenlik Prensipleri

Bir havayolu aracıyla ilgili dikkat edilmesi gereken birçok faktör bulunmaktadır. Temel güvenlik prensipleri; uçuş kontrolü, kabin (operasyonel) ve kabin (yolcu) olmak üzere üç ana başlık altında toplanır[3]:

a. Uçuş Kontrolü: Uçağı uçurmak için gerekli kritik emniyet sistemlerini ifade eder. Bozulma ya da devre dışı kalma güvenliği doğrudan etkiler. *Yüksek Etki / Düşük Olasılık*

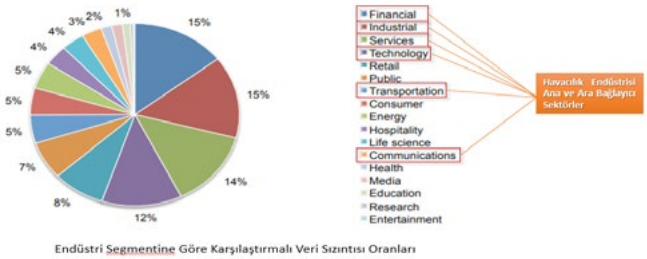
b. Kabin (Operasyonel): Uçağı çalıştırmak ve korumak için kullanılan sistemlerini ifade eder. Bozulma ya da devre dışı kalma kritik operasyonları ve bakımı doğrudan etkiler. *Orta Etki / Orta Olasılık*

c. Kabin (Yolcu): Yolcuların doğrudan etkileşime girdiği sistemler/ara yüzleri ifade eder. Bozulma veya devre dışı kalma en az etkiye sahiptir, fakat güvenilmeyen cihazlar ile belirtilen sistemler ortak kullanım alanı olarak kabul edilmektedir. *Düşük etki / Yüksek olasılık*

4.4. Sivil Havacılık ve Siber Güvenlik

Siber saldırılar, sivil havacılık endüstrisi için giderek büyüyen bir tehdit oluşturmaktadır. Havacılık kurumları rutin operasyonlarının dışında kritik operasyonlar için de giderek artan ölçüde elektronik sistemlere bel bağlamaktadır. Elektronik sistemlerin saldırılardan korunması (yasa dışı müdahale) ve güvenlik seviyesinin 7/24 sürdürülebilir olması zorunluluk haline gelmiştir.

Uluslararası Sivil Havacılık Organizasyonu (ICAO), 2016 yılında ICAO Meclisinin 39uncu oturumunda siber güvenlik için sivil havacılığın kritik altyapısını, bilgi ve iletişim teknolojisi sistemlerini ve verileri koruma kapsamında koordineli bir yaklaşım çağrısında bulunmuştur. Bu amaçla, alınan A39-19 nolu kararda; sivil havacılıkta siber güvenlik için devletler ve diğer paydaşlar tarafından sivil havacılığa karşı çapraz, yatay ve işbirlikçi bir yaklaşımla siber tehditlere karşı alınan önlemleri ortaya koyma zorunluluğu açıklanmıştır.



Şekil 7: Endüstri segmentine göre karşılaştırmalı veri sızıntısı oranları

Havacılık sektörünün ana ve ara bağlayıcı sektörleri arasında yer alan sektörlere yönelik saldırıların doğrudan ya da dolaylı olarak havacılık endüstrisini de etkilediğinden yazının başında bahsetmiştik. Level One Robotics isimli yedek parça üreticisi ve çizim şirketinin uğradığı saldırı sonucu içinde Volkswagen, Tesla, Boeing gibi büyük

üreticilerin de olduğu şirketlere yönelik çizimler, sözleşmeler ve personel bilgisinde sızıntı olmuştur[4].

Yıl içinde birçok havayolu şirketinin siber saldırıya maruz kaldığı ve bu saldırılar sonucunda maddi boyutu yüksek olan sızıntıların meydana geldiği basına yansımıştır. Hatta British Airways şirketi bir ay arayla iki kez saldırıya uğramış ve bu saldırı neticesinde yaklaşık 570.000 kişinin kredi kartı verisinde sızıntı olmuştur.

SİBER SALDIRILAR

5. "Windows Mağaza" Uygulamaları Verilerinize Erişiyor Olabilir

Microsoft'un güncel işletim sistemlerinden olan Windows 10'da oluşan bir hata (bug), işletim sistemi üzerinde kurulu olarak gelen Windows Uygulama Mağazasından indirilen uygulamaların kullanıcı verilerine erişmesine neden oldu.

Windows 10 ile gelen "Universal Windows Platform" (UWP) özelliği uygulamaların Windows 10 kurulu olan birçok cihazda (masaüstü bilgisayarlar, oyun konsolları ve diğer akıllı cihazlar) çalışabilmesini sağlıyor. UWP platformu birçok uygulama programlama arayüzü (API) ile iletişim kurabilecek şekilde tasarlanmış ve hem resim, müzik gibi içeriklere hem de kamera, mikrofon gibi donanımlara erişebilen bir platformdur. UWP sistemi, temelde kullanılacak uygulamanın ihtiyaçlarına bağlı olarak gereken kaynağa erişmek için kullanıcıdan izin talep edecek şekilde tasarlanmıştır.

Windows sistemindeki varsayılan ayarlarda, UWP tabanlı uygulamaların cihaz içindeki birçok dizine (uygulamanın kurulu olduğu ve veri kayıt edebileceği dizinler; *local*, *roaming* ve *temporary* dizinler) erişim izni önceden tanımlanmıştır. UWP ile birlikte çalışan "*broadFileSystemAccess*" isimli yetenek ise kullanıcın çalıştırdığı uygulamanın söz konusu kullanıcı ile aynı seviyedeki yetki çerçevesinde çalışmasını sağlamaktadır. Microsoft dokümantasyonlarında ise bu yeteneğin kısıtlanmış olduğu ve söz konusu yetki seviyesindeki bir işleme ihtiyaç duyulması durumunda uygulamanın kullanıcıdan izin talep ettiği ifade edilmekte. Buradaki kritik nokta ise; söz konusu uygulamaların bahsi geçen izinlere sadece ilk çalıştırıldıklarında ihtiyaç duyması ve sistemin yapılan tercihi ayarlara yansıtmasıdır. Kullanıcı bu tercihleri daha sonra ayarlar kısmında değiştirme hakkına her zaman sahiptir, fakat problemin asıl çıkış noktası Windows 10'daki oluşan hatanın söz konusu izin sürecini devreden çıkarmış olmasıdır. Windows uygulama geliştiricisi *Sébastien Lachance,* söz konusu hatanın Ekim ayında dağıtılan güncelleştirme paketiyle ortaya çıktığını belirtti. Microsoft mühendislerinin daha sonra yaptıkları açıklamalar da Windows 10 için dağıtılan son güncelleştirme "broadFileSystemAccess" yeteneğini pasifleştirdiği için böyle bir hatanın oluştuğunu teyit etti[5].

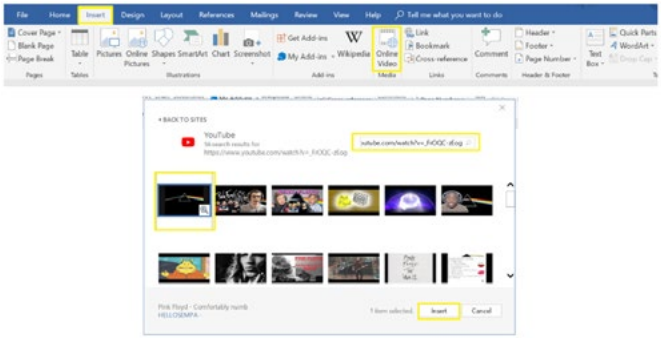
Söz konusu hatadan ayrı olarak dosya silme hatalarına da neden olan Ekim güncelleştirmesini durduran Microsoft, bahsi geçen risklere karşı kullanıcıların UWP altyapısı altında çalışan uygulamaları güncellemesi gerektiğini belirtti. Güncelleştirmenin yüklenmesinden bağımsız olarak Windows 10 işletim sistemini kullanan kullanıcıların gizlilik ayarları kısmındaki dosya sistemine erişen uygulamaları kontrol etmelerinde fayda var.

6. Microsoft Ofis Uygulamalarında Yeni Bir Açık Keşfedildi

Cymulate Araştırma grubu Microsoft Ofis uygulamalarında (2016 ve önceki sürümler) zararlı kod çalıştırılmasına olanak sağlayan yeni bir zafiyet keşfetti. İlgili sürümlerde bulunan MS Word uygulamasında yer alan "Çevrimiçi Video" özelliği üzerinden Word belgelerinde zararlı kod çalıştırmayı başaran Cymulate grubu, söz konusu zafiyetin oltalama saldırılarında ve daha farklı kod çalıştırma senaryolarında kullanılabilecek potansiyele sahip olduğunu belirtti. İlgili zafiyeti bir güvenlik zafiyeti olarak Microsoft'la paylaşan araştırmacılar, Microsoft'un bu durumu güvenlik zafiyeti olarak değerlendirmediğini belirtmesi üzerine, bulgularını kendi blog sayfaları üzerinden paylaştılar[6].

Kullanıcıların Word dokümanına YouTube videoları eklemesine olanak sağlayan "Çevirimi Video" özelliği; araştırmacıların keşfettiği bir yöntemle dokümana eklenen videoya ait olan iframe kodunun maniple edilmesiyle zararlı kod çalıştırılmasına imkân sağlamaktadır. Saldırganlar ilgili dokümana ait XML dosyası içindeki videoya ait kodlara müdahale ederek hedef bilgisayar üzerinde zararlı kod çalıştırabilmektedir. Zafiyetin sömürülebilmesi için hedef kullanıcının, saldırgan tarafından maniple edilen dokümanı açıp içindeki linki tıklaması gerekmektedir. Burada en çok dikkat çeken nokta Word uygulamasının kullanıcıyı uyarmak için ilgili duruma ait herhangi bir uyarı penceresi çalıştırmaması olmuştur.

MS Word dosya formatı olan .docx dosya tipi; dosya içindeki tüm verinin depolandığı bir paket gibi çalışır. Dosyanın paket haline getirilip açılmasıyla doküman



Şekil 8: MS Office çevrimiçi video özelliğinin kullanılması[7]

Şekil 9: Manipülasyona açık iframe kodu[7]

içindeki tüm görsel ve yazılı detayları farklı dosyalar altında görmek mümkündür. Bu yöntemle açılan dosya içindeki iframe kodunun maniple edilmesi sonucunda Internet Explorer uygulaması kodu işlemekte ve maniple edilen kodu çalıştırmaktadır.

Microsoft'un bu durumu güvenlik zafiyeti olarak değerlendirmeyip yama sunmaması üzerine, Cymulate grubu, "embeddedHtml" etiketi içeren dokümanları engellemenin bir korunma yolu olabileceğini belirtti. Daha sonra, Trend Micro™ XGen™ security isimli grup söz konusu zafiyete yönelik YARA kuralı oluşturup yayınladı[7].

```
rule EMBEDDEDHTML_WITH_SCRIPT {
meta:
description = "possible abuse of Office video embeddedHtml"
reference = "https://blog.cymulate.com/abusing-microsoft-office-online-video"
strings:
$embeddedHtmlre1 = /\sembeddedHtml="[^"]+/
$embeddedHtmlre2 = /\sembeddedHtml='[^']+/
$script = "<script" nocase
condition:
(
for any i in (1..#embeddedHtmlre1): (
for any j in (1..#script): (
@embeddedHtmlre1[i] < @script[j] and
@script[j] < @embeddedHtmlre1[i] + !embeddedHtmlre1[i]
)
)
)
or
(
for any i in (1..#embeddedHtmlre2): (
for any j in (1..#script): (
@embeddedHtmlre2[i] < @script[j] and
@script[j] < @embeddedHtmlre2[i] + !embeddedHtmlre2[i]
)
)
)
```

Şekil 10: Zafiyet için önerilen YARA kuralı[7]

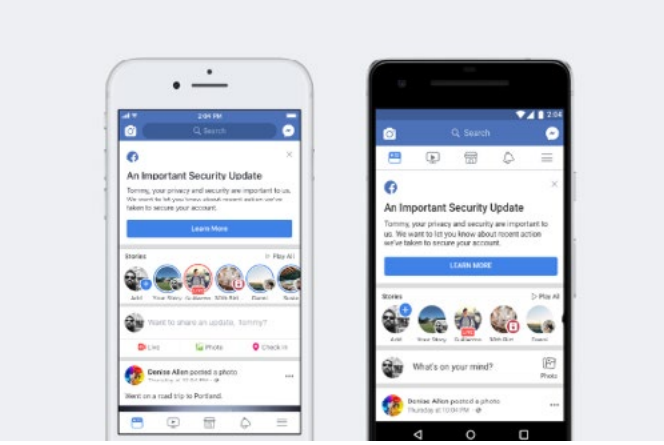
Zafiyete ilişkin kavram kanıtlama (PoC/proof-of-concept) videosunun araştırma grubu tarafından yayınlanmasıyla zafiyetin sömürülmesi daha da kolay hale geldi. Henüz resmi bir yama yayınlanmış olmadığı için, kullanıcıların önerilen iki yöntemden mevcut sistemleri için uygun olan çözümü uygulaması söz konusu zafiyete karşı güvende olmalarını sağlayacaktır.

7. Facebook Veri Sızıntısı

Eylül 2018 sonunda Facebook, bilgisayar ağlarına yapılan saldırı sonucunda yaklaşık 50 milyon kullanıcıya ait kişisel bilginin ele geçirilmiş olduğunu duyurdu.

Facebook tarafından yayınlanan bir blog yazısında ürün yönetimi başkan yardımcısı Guy Rosen, kullanıcıların kendi profillerini başkalarının gözünden görmelerini sağlayan "View as" özelliğini etkileyen koddan kaynaklanan güvenlik açığının, kullanıcıların erişim belirteçlerinin çalınmasına ve hesaplarının ele geçirilmesine neden olduğunu ifade etti. Saldırıya neden olan açığın tespit edildiğini ve düzeltildiğini, ayrıca olayla ilgili soruşturma başlatıldığını açıkladı[8].

Blog yazısında ayrıca verileri sızan 50 milyon kullanıcının güvenlik belirteçlerinin sıfırlandığı, önlem olarak "View as" özelliğinin devre dışı bırakıldığı ve diğer bir 40 milyon kullanıcının da güvenlik belirteçlerinin sıfırlandığı belirtildi ve 90 milyon kullanıcının Facebook'a ya da Facebook ile bağlantılı diğer uygulamalara yeniden giriş yapmaları gerektiği ifade edildi. Tekrar giriş yaptıktan sonra kullanıcıların ana sayfasında, haberler bölümünün üst kısmında neler olduğunu açıklayan bir bildirim görecekleri söylendi. Ekim ayının başında yayınlanan bir diğer blog yazısında,



Şekil 11: Facebook mobil ekran görüntüsü

Facebook tarafından yüklenen veya Facebook ile giriş yapılan tüm üçüncü parti yazılımların analiz edildiği ve saldırganların Facebook girişini kullanarak herhangi bir uygulamaya eriştiğine dair kanıt bulunamadığı belirtildi. Ancak kullanıcıların erişim belirteçlerinin nasıl doğrulandığına bağlı olarak, güvenlik açığının Facebook girişini kullanan üçüncü parti uygulamalar için tehdit oluşturabileceği ifade edildi[9].

Kullanıcıların erişim bilgilerini doğrulamak için Facebook'un resmi SDK'lerini (yazılım geliştirme kiti - software development kit) kullanmayan pek çok web sitesi, saldırganların iptal edilen erişim belirteçlerini kullanarak hesapları ele geçirmesine neden olabilir.

Facebook'un resmi SDK'lerini kullanan ve kullanıcıların erişim belirteçlerini düzenli olarak kontrol eden üçüncü taraf uygulamaların tehdit altında olmadığı belirtildi. Resmi Facebook SDK'lerini kullanmayan ya da erişim belirteçlerinin geçerli olup olmadığını düzenli olarak kontrol etmeyen geliştiricilerin, saldırıdan etkilenen kullanıcıları manuel olarak belirleyebilmeleri için bir araç oluşturulduğu açıklandı.

Tüm bu gelişmelerin ardından Ekim ayının ikinci haftasında yapılan yeni bir açıklamayla, saldırıdan etkilenen kullanıcı sayısının 30 milyon olduğu duyuruldu. Saldırganların 29 milyondan fazla Facebook kullanıcısının kişisel bilgisine eriştiği ancak herhangi bir üçüncü parti uygulamanın verilerine erişemedikleri belirtildi[10].

Saldırganların ilk olarak Facebook arkadaşlarıyla bağlantılı olan bir dizi hesabı ele geçirdiği, hesaptan hesaba geçiş yapmak için otomatik bir teknik kullandıkları ve böylece yaklaşık 400.000 kullanıcının hesabını ele geçirdikleri ifade edildi. Ardından bu 400.000 kullanıcının arkadaş listeleri kullanılarak yaklaşık 30 milyon hesabın erişim belirteçleri çalındı. 15 milyon kullanıcıya ait isim ve iletişim bilgileri (telefon numarası, e-posta adresi ya da her ikisi birlikte), 14 milyon kullanıcının ise isim ve iletişim bilgilerine ek olarak kullanıcı adı, cinsiyet, din, doğum tarihi vb. bilgilerini de içeren pek çok veriye ulaşıldı. 1 milyon kullanıcının ise herhangi bir bilgisine erişilememişti.

Yapılan açıklamada ayrıca saldırıdan etkilenip etkilenmediğini merak eden kullanıcıların Facebook'un "Yardım Merkezi"ni ziyaret edebilecekleri belirtilirken, saldırıdan etkilenen 30 milyon kullanıcıya hangi bilgilerinin ele geçirildiğini ve kendilerini korumak için neler yapmaları gerektiğini içeren bir açıklama mesajı gönderileceği ifade edildi.

8. BLEEDINGBIT Bluetooth Zafiyeti

Kasım 2018 başında güvenlik araştırmacıları erişim noktalarını ve yönetilmeyen cihazları etkileyen iki tane zafiyet tespit etti. Texas Instruments (TI) tarafından tasarlanan çiplerdeki BLE (Bluetooth Low Energy) kullanımıyla ilişkili olan bu zafiyet "BLEEDINGBIT" olarak adlandırılmaktadır[11].

BLEEDINGBIT, zafiyeti içeren cihazlarının kontrolünü tamamen ele geçirmek ve bu cihazları barındıran kurumsal ağlara erişim sağlamak için uzak ve kimliği doğrulanmamış bir saldırgan tarafından kullanılabilmektedir.

Şekil 12: BleedingBit zafiyetine ait görselleştirme çalışması

Zafiyet Bluetooth Low Energy (Bluetooth 4.0 - BLE) çiplerini etkilemektedir. BLE düşük güç tüketimli cihazlar için kullanılmaktadır. Aynı zamanda bu çipler erişim noktalarında, Cisco ve Aruba Networks tarafından üretilen ağ cihazlarında da kullanılmaktadır.

Zafiyetten etkilenen cihazların tam sayısı bilinmemekle birlikte, Cisco ve Aruba Networks'ün her yıl işletmelere satılan kablosuz erişim noktalarının yüzde 70'ini sağladığı tahmin edilmektedir.

CVE-2018-16986 olarak bilinen ilk zafiyet BLE-STACK 2.2.1 ve önceki sürümleri çalıştıran CC2640 ve CC2650 çiplerini ve 1.0 veya daha önceki sürümleri çalıştıran CC2640R2'yi etkilemektedir. Saldırgan yalnızca cihaz aktif olarak taranıyorsa zafiyetten yararlanabilmektedir. Hedeflenen cihazın menzili içindeki bir saldırgan, uzaktan kod yürütme için zafiyeti tetikleyebilir. Eğer BLE etkinse ve cihaz aktif bir şekilde taranıyorsa, saldırgan bellek taşmasını tetiklemek ve keyfi kod çalıştırmak için özel hazırlanmış paketler gönderebilir.

Zafiyet çipin üzerine bir arka kapı yüklemek üzere tetiklenebilir ve böylece cihazın kontrolü tamamen ele geçirilebilir. Uzmanlar, erişim noktalarının ele geçirilmesiyle birlikte saldırganların ağdaki diğer cihazlara da erişebileceği konusunda uyarıda bulunmaktadır.

CVE-2018-7080 olarak bilinen ikinci zafiyet ise CC2642R2, CC2640R2, CC2640, CC2650, CC2540 ve CC2541 çiplerini etkilemektedir. Bu zafiyet yazılım güncellemelerine izin verecek şekilde tasarlanmış BLE çiplerindeki bir arka kapıdır. OAD (dahili yazılım indirme) özelliği genellikle bir geliştirme aracı olarak kullanılır ancak bazı üretim erişim noktalarında aktiftir. Yakındaki bir saldırganın, üretici tarafından doğru bir şekilde uygulanmayan BLE çipinin işletim sistemini yeniden yazarak aygıt yazılımının tamamen yeni ve farklı bir sürümüne erişmesine ve kurmasına izin verebilir.

Varsayılan olarak OAD özelliği güvenli yazılım güncellemelerini adreslemek için otomatik olarak yapılandırılmamıştır. Aruba'nın erişim noktalarında OAD özelliğinin saldırganlar tarafından kolayca kötüye kullanılmasını önlemek için sabit kodlanmış (hardcoded) bir parola (BLE'yi destekleyen tüm Aruba AP'lerinde aynıdır) eklenmiştir. Ancak yasal bir güncellemeyi dinleyerek (sniffing) veya Aruba'nın BLE yazılımına tersine mühendislik yaparak parolayı elde eden bir saldırgan, zafiyet içeren bir erişim noktasındaki BLE çipine bağlanabilir ve saldırganın işletim sistemini yeniden yazmasına, dolayısıyla tüm kontrolleri ele geçirmesine neden olabilir.

Zafiyetin ortaya çıkmasının ardından tedarikçiler zafiyet hakkında bilgilendirildi ve Texas Instruments tarafından BLU-Stack 2.2.2 yayınlandı. Hem Cisco hem de Aruba etkilenen tüm ürünler için güvenlik yamaları yayınladı.

9. Sosyal Medya ve Bilgi Paylaşımı

Sosyal medya platformlarının iletişim kurma, bilgi paylaşma ve etkileşimi artırma temelleri üzerinde geliştiği bilinmekte ve bu alandaki dijital ürünler benzer kullanım amaçlarıyla kullanıcılara sunulmaktadır. Günümüzde sık kullanılan 50'nin üzerinde sosyal medya platformu olduğu bilinmekle birlikte, söz konusu platformların sosyalleşme kavramından uzaklaşarak bir anlamda veri tabanlarına dönüştüğünü söylemek mümkün. Nitekim daha önce Facebook vakası olarak gündeme gelen veri sızıntıları ve verilerin çeşitli amaçlarla işlenmesiyle girişilen eylemler dünyada büyük yankı uyandırmıştı. Bu durumda güncel sosyal medya platformlarının kapasitesinin iletişim, sosyalleşme ve etkileşimden çok kimileri tarafından daha çok bir istihbarat aracı olarak değerlendirildiği ortaya çıkmakta. Bu gibi durumlarda bahsi geçen iletişim kavramlarının bir nevi gizleme/savunma mekanizması olarak işlev görmesi mümkün.

Akıllı telefon teknolojisinin gelişmesi ve bilgisayarlardaki uygulama/platformların mobil ortama aktarılmasıyla gerek profesyonel gerek sosyal ihtiyaçlar gibi nedenlere bağlı olarak kullanıcıların 7/24 çevrimiçi olması bir gereksinim haline geldi. Bu sayede toplanan bilgi seviyesinde inanılmaz bir artış gerçekleşti. Daha önceleri masaüstü bilgisayar kullanıcıların daha çok kullanım alışkanlıkları, ziyaret ettiği adresler (web), iletişim kurduğu kişiler (bilgisayar kullanan kitleyle sınırlı) hobiler, oynadığı oyunlar gibi bilgiler elde edilebilirken. Günümüzde akıllı ve mobil cihaz kullanıcılarının kullanım alışkanlıkları, ziyaret ettiği adresler (web ve fiziksel) iletişim kurduğu kişiler (bilgisayar/akıllı cihaz kullanan kitle ile sınırlı değil), hobiler, yaşam tarzı, görüşler, planlar, özel hayat, sağlık durumu, yemek tercihleri, yetkinlikler gibi çok çeşitli kişisel bilgilerini elde etmek mümkün hale geldi. Ayrıca paralel hesaplara ait şifrelerden yola çıkarak, kişinin genel şifre oluşturma politikasının anlaşılmasıyla veya olası veri sızıntılarından elde edilecek şifrelerle kullanıcıların banka hesaplarından akıllı ev sistemlerinin yönetimine kadar uzanan bir risk mevcut.

Aşağıda tipik bir sosyal medya platformuna ait mobil uygulamanın kullanıcılardan talep ettiği izinler görülmektedir:

- Arama Özelliği,
- SMS Gönderme Özelliği,
- Kişi Listesi,
- Kamera,
- Mikrofon,
- Takvim,
- Depolanmış Veriye Erişim,

Bahsedilen izinleri kullanarak veya suistimal ederek kullanıcı hakkında pek çok kritik bilgi elde edilebileceği aşikâr; bu nedenle kullanım ihtiyacı bağlamında bir sınırlandırma ve önceliklendirme yapılması tarafımızdan önerilmektedir. Sonuç olarak bugün hem profesyonel hem de sosyal ihtiyaçlara hizmet ettiği bilinen sosyal medya platform ve araçlarının ciddi boyutta bilgi topladığını da unutmamak gerekir. Paylaşılacak bilginin içeriğine bu nokta göz önünde bulundurularak karar verilmelidir. Her ne kadar kişisel verileri koruma kanunu (KVKK) varsa ve benzer kapsamda küresel önlemler (GDPR ve PDPR) alınsa da kullanıcıların bu konuda bilinçli olup veri toplama ve işleme konularında verecekleri izinlerde daha dikkatli olmaları önerilmektedir.

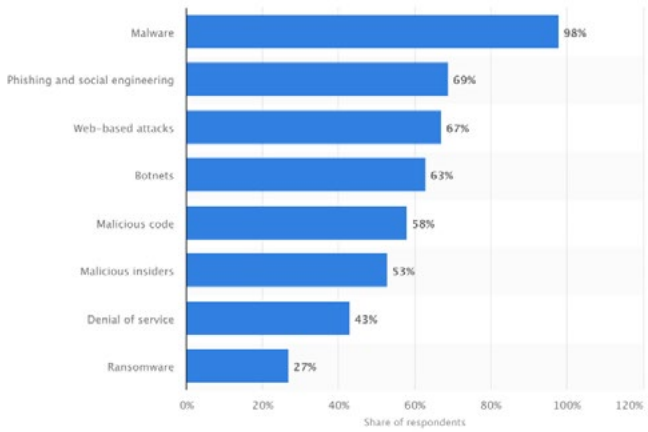
10. Siber Uzay ve Asimetrik Tehdit

Kara, deniz, hava ve uzaydan sonra siber uzay yeni bir güvenlik alanı olarak savunma ve saldırı alanlarına eklenmiş bulunuyor. Siber uzay; ağ sistemleri ve fiziksel yapılar üzerinde veri depolamak, değiştirmek ve geliştirmek amacıyla elektronik ve elektromanyetik spektrumun kullanılması olarak tanımlanabilir[12]. Siber uzay diğerlerinden farklı olarak insan eliyle oluşturulan tek alandır.

Fiziki sınırların önemini kaybettiği, devletlerin yanı sıra çok uluslu şirketlerin ve bireylerin aktör olarak yer aldığı, kontrol edilmesi zor bir güvenlik alanı olan siber uzay, 2000'li yılların başından itibaren uluslararası ilişkilerde de etkisini göstermeye başlamıştır[13].

Uluslararası ilişkilerde en önemli sorunlardan biri olan güvenlik meselesi teknolojik alandaki gelişmelerden daha keskin şekilde etkilenmektedir ve küresel risk toplumunda siber politikalar çok daha karmaşık bir hal almıştır[14]. Bu risk, uluslararası hukuk tarafından sınırları belirlenmiş ve kontrol altına alınmış olan konvansiyonel savaşın yerine, bilinmezliklerin hâkim olduğu ve sınırları belirlenemeyen yeni bir güvenlik alanı ortaya çıkarmıştır.

Klasik savunma ve saldırı alanlarından farklı olarak asimetrik unsurlara sahip olan bu güvenlik alanında saldırıyı kimin başlattığı, saldırganın konumunun neresi olduğu, elinde ne gibi siber silahlar olduğu bilinememektedir. 2008 yılında Bükreş'te yapılan NATO Zirvesi'nde, Müt-



Şekil 13: 2017 yılında gerçekleşen saldırıların dağılım oranları[32]

tefikler siber savunma kavramını ilk defa resmi bir zirve çerçevesinde ele aldılar. Bükreş Zirvesi ile eşzamanlı olarak gerçekleştirilen NATO ve Siber Savunma konulu toplantının sonuç raporunda "Global bilgi ekonomisinde, interneti iş dünyası için açık ve büyük tehlikelerden uzak tutmak, denizleri ve hava koridorunu açık tutmakla eşdeğerdir" cümlesi vurgulanıyordu[15].

Sektörden bağımsız olarak artan siber saldırılara karşı kurum ve kuruluşların aldığı önlemler genellikle yetersiz kalmaktadır. Kurumların geliştirdiği savunma uzayına karşın saldırganlar da yeni yöntemler ve yeni atak vektörleri geliştiriyor. Şekil 14'de Ağustos 2017 yılı itibariyle dünya genelinde karşılaşılan siber saldırıların oranlarına yer veriliyor.

Günümüzün geniş ve gelişmekte olan tehdit ortamında siber güvenlik faaliyetlerini Siber Füzyon Merkezi olarak adlandırılan tek bir oluşum halinde entegre etmek, riskleri azaltmak ve operasyon sürdürülebilirliği kazanmak için önemlidir.

Siber tehditler ve saldırgan yetenekleri hızla geleneksel tehdit algılama teknolojilerini geride bırakmaktadır. Bir bilgi güvenliği ihlalinin tespit edilmesi için gereken ortalama gün sayısı 146 güne ulaşmış durumdadır. Birçok kuruluş kendi başına ihlalleri tespit edememektedir. Kurumsal ağları düzgün bir şekilde korumak ve savunmak için, kuruluşların gerçek ve teknik bilgileri kapsamlı ve birbiriyle ilişkilendirilebilecek bir ortamda birleştiren bir füzyon merkezine ihtiyaçları vardır.

10.1. Siber Füzyon Merkezi Nedir?

Siber Füzyon Merkezi (SFM), kritik teknoloji ve bilgi varlıklarının güvenliğine yönelik proaktif ve koruyucu faaliyetleri içerir. SFM, bilgi teknolojileri operasyonları ile tehdit istihbaratından gelen bilgi akışını ve güvenlik fonksiyonlarını yönetir ve koordine eder. Bu sayede, harekât etkinliğini artırır, siber tehdit istihbaratının zamanında dağıtılmasıyla saldırıları önleyerek veya etkisini azaltarak güvenlik seviyesini artırır[16].

Ülkemizde ilk kez 2016 yılında STM tarafından kurulan ve devreye alınan siber füzyon merkezi üç ana unsurdan meydana gelmektedir. Bunlar; siber operasyon merkezi, siber istihbarat merkezi ve zararlı yazılım analiz laboratuvarıdır.

Amerika Birleşik Devletleri'nde her yıl düzenlenen Aspen Güvenlik Forumu (ASF), tüm ilgili ulusal güvenlik kurumlarından üst düzey mevcut ve eski yetkililer ile endüstri liderleri ve önde gelen düşünürlerin bir araya geldiği bir güvenlik forumudur. Bu yıl Aspen'de tartışılan konulardan biri de siber füzyon merkezlerinin olgunluk modeliyle ilgiliydi.

Şekil 15: STM Siber Füzyon Merkezinden bir görüntü

Burada tarif edilen yapıya göre, bir kuruluşun bütün bileşenleri SFM'de önemli bir rol oynar. Siber Tehdit İstihbarat ekibi akıllı kararlar vermemize yardımcı olmak için siber uzaydaki trend ve aktiviteleri yakından izler ve analiz eder. Siber güvenlik olay müdahale ekibi (CSIRT), hedef odaklı algılama teknikleri geliştirir, sistemleri ve ağları izler, herhangi bir olay anında ilgili olayı bildirmeye hazır durumdadır. Güvenlik test ekibi, kod güvenliği veya sunucu konfigürasyonundan gerekli yamalara kadar, bütün alanları taramak için yeni ve mevcut teknolojiyi kullanırken, Kırmızı Takım savunma kontrolündeki zayıflıkları açığa çıkarmak için, hedefe yönelik gerçek dünya saldırılarını simüle eder. Başka bir ekip ise sürekli iyileştirmeyi devamlı hale getirmek için ekiplerin faaliyetlerini kayıt altına alır, metrikleri ve raporları oluşturur, takım çalışmalarını kontrol eder.

Şekil 14: STM Siber Füzyon Merkezi SOC (Security Operations Center)'dan bir görüntü

Forumda tavsiye edilen yapının beş ayrı ekipten oluştuğu görülmektedir:

1. Siber Tehdit İstihbaratı Ekibi,
2. Siber Güvenlik Olay Müdahale Ekibi,
3. Güvenlik Test Ekibi,
4. Kırmızı Takım,
5. Denetim Ekibi.

Askeri kuruluşlar, devlet kuruluşları, danışmanlık şirketleri gibi çok geniş yelpazede ve birçok sektörde hizmet veren siber füzyon merkezleri eğitim sektöründe de en önemli ihtiyaçlardan biridir. Buna en güzel örnek ABD'deki Maryville Üniversitesidir. Maryville üniversitesi bünyesinde yer alan füzyon merkezi yeni nesil güvenlik konseptiyle kurulmuştur. Merkezi diğer füzyon merkezlerinden ayıran en önemli özellik bu merkezde 35 öğrencinin çalışıyor olmasıdır. Öğrencilere yeteneklerine göre görevler verilmektedir. Bu görevler sızma testi, güvenlik açığı yönetimi, adli analiz ve siber tehdit izleme konularını kapsamaktadır[17].

Şekil 16: Maryville Üniversitesi Siber Füzyon Merkezi[33]

Siber saldırılar çok uluslu şirketler ve büyük şirketler açısından başta ekonomik kayıp olmak üzere birçok risk faktörü barındırır. Bu faktörlerden biri de prestij kaybıdır. Örneğin 2016 yılında *Park Jin Hyok* isimli Kuzey Koreli bir bilgisayar programcısının Sony Pictures şirketine siber saldırı düzenlediği tespit edilmiştir[18]. Sony'e yapılan bu siber saldırının getirdiği ekonomik zararın bombalı bir saldırı ile eşdeğer olduğunu iddia eden ABD Temsilciler Meclisi İç Güvenlik Komitesi Başkanı Michael McCaul, bu konuda bürokrasinin azaltılarak devletin özel şirketler ile işbirliği yapması gerektiğinin altını çizmiştir[19].

Yaşanılan örnek olaylar kamu kurumlarının siber güvenlik konusunda ilgili özel sektörle işbirliği yapması gerekliliğini de ortaya koymaktadır. Amerikan İç Güvenlik Bakanlığı, devleti, bölgeyi ve toplumu tehdit eden konular için Füzyon Merkezlerinin oluşturulmasını önermiştir. Devlet ve yerel yönetimler tarafından yönetilen bu merkezler, çeşitli konularda farklı bilgi parçaları olarak görülebilecek ama bir araya geldiğinde potansiyel terör saldırılarının göstergelerini açığa çıkarabilecek verileri bir araya getirecek şekilde tasarlanmıştır. Bu merkezler genellikle istihbarat ve yasal bilgi altyapısına sahip personel ile çalışmaktadır. Bu merkezlerde çalışan çok az personelin siber güvenlikle ilgili bilgi sahibi olduğu ve potansiyel siber saldırıların göstergelerini nelerin oluşturduğunu bilmedikleri bilinmektedir[20].

Bölgesel, toplumsal ve uluslararası ilişkilerde yaşanan olayların öncesinde veya sonrasında taraflar arasında bir siber saldırının gerçekleşme ihtimali bir konvansiyonel savaş ihtimalinden çok daha fazladır. Siber saldırı vektörlerini tanımak, farklı yeteneklerle donanmış personeli bir araya getirmek ve 7/24 sürdürülebilir bir güvenlik mimarisi kurmak 21'inci yüzyıl devletleri ve özel sektör bileşenleri için bir zorunluluk haline gelmiştir.

11. Tesla Araçlarının Ele Geçirilmesi

2016 ve 2017 yıllarında Tencent Keen Security Laboratuvarı araştırmacıları Tesla Model X ve S araçlarına yönelik iki uzaktan saldırı gerçekleştirmeyi başarmışlardı ancak yaptıkları ikinci saldırının detaylarını ilk kez Blackhat 2018 konferansında açıkladılar[28]. Buradan birçok 0-day (0. gün) saldırısı tespit edilmiş olduğu anlaşılıyor. Araçların hedef noktaları ve yazılım sürümleri Şekil 17'de görülüyor.

Model	Test Target	Version (Build Number)
Model S P85 Model X 90D	CID/gateway Vulnerability	v8.1(17.24.28)
Model X 90D	APE Vulnerability	V8.1(17.17.4)
Model X 90D	Custom Holiday Show	V8.1(17.18.50)

Şekil 17: Yazılım sürümleri ve hedefler

Tesla araçlarda Autopilot ECU (Autopilot Electronic Control Unit) denilen otopilot sistemini kontrol eden gömülü sistemler bulunuyor. Araştırmada ilk saldırı zinciri Tesla araçlarındaki tarayıcıda bulunan zafiyetten başlayarak cihazdaki gateway'i ve bu kontrol ünitesini ele geçirmeyi hedefliyor.

Webkit günümüzde Tesla araçlar dahil olmak üzere birçok uygulama ve platform tarafından kullanılan açık kaynak kodlu bir tarayıcı motorudur. Aynı araştırmacıların Blackhat 2017 ile ilgili olarak açıkladığı Tesla araçlarındaki Webkit zafiyetlerini Tesla güvenlik takımı kapatmış olmakla birlikte söz konusu araçlarda Webkit uygulamasının eski 534.34 versiyonunu bütün zafiyetlerini çözmeden kullanmaya devam etmişti. Araştırmacılar da bu versiyondaki kod çalıştırma zafiyetini sömürmeyi başarmışlardır.

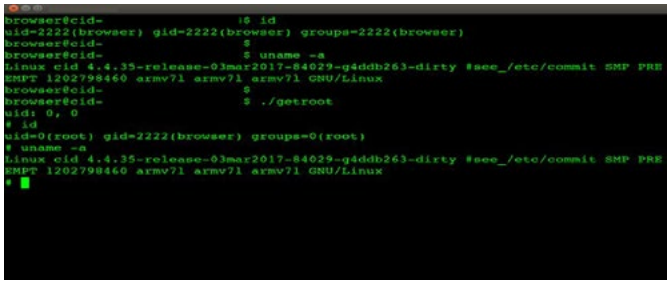
Use-after-free zafiyeti bir programın çalışmasının durmasına ya da uzaktan kod çalıştırılmasına sebep olabilecek bir zafiyettir. Bu zafiyet temel olarak hafızadaki bir lokasyonda, oradaki objenin kullanımdan kaldırılmasına rağmen (free) hâlâ erişime açık olan, referans edilebilecek

değişkenler kaldığında ortaya çıkıyor(use). Hafızadaki o kısma istenilen değerin yazılabilmesi durumunda uzaktan kod çalıştırma işlemini gerçekleştirilebilmektedir.

Araştırmacılar Tesla araçlarındaki Webkit motoru üzerinde bu zafiyeti sömürebilecekleri obje, metot ve değişkenleri tespit etmişler ve bu bilgilerle hafıza shellcode yazabilmeyi başarmışlardır. Bu sayede Tesla CID'de (merkezi bilgi ekranı) shell erişimi sağlanabilmektedir.

AppArmor Linux kernel güvenlik modüllerinden (LSM) biri olup erişim kontrollerini kullanıcı değil program tabanlı düzenleyen bir sistemdir. 2016 yılındaki çalışmalarında çokça bilinen bir kernel zafiyetiyle araştırmacılar Tesla araçlarındaki AppArmor'u aşıp root kullanıcı hakkı elde edebilmişlerdi. Ancak Tesla 2.6.36'dan 4.4.35'e yükseltilen kernel sürümüyle neredeyse bütün zafiyetlerini kapatmıştı.

Araştırmacılar kodlama içinde hafızada erişilecek objenin adresini hesaplarken yapılan bir hatayı fark etmişlerdir. Bu sayede kullanıcının kernel hafızasındaki bütün integer verilerini azaltabileceği bir durum oluşmuştur. Bu durumda ROP gadgetin adresi olacak şekilde *accept4* sistem çağrısının adresini azaltarak istedikleri adrese istedikleri veriyi yazmaları mümkün hale gelmesinin mümkün olduğu tespit edilmiştir. Böylece uygun argümanlarla bu çağrıyı yapıp herhangi bir adrese yazma işlemini gerçekleştirilmesinin ardından çekirdek üzerinde *aa_g_profile_mode'u APPARMOR_COMPLAIN* yaparak AppArmor'u devre dışı bırakılmakta ve setresuid metodunu bütün processlerin root olabileceği şekilde modifiye edilmektedir. Araştırmacılar, söz konusu 0. gün saldırısıyla root kullanıcı yetkisi elde edip CID'yi yönetebilmişler.



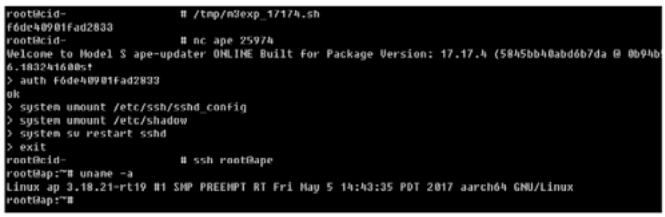
Şekil 18: Linux 4.4.35 CID Shell

Araştırmacılar, 2016 yılındaki çalışmalarında Tesla araçlarında zararlı hale getirilmiş bir firmware güncelleyici kullanmışlardı. Bunun neticesinde Tesla güvenlik ekibi yazılım güncelleme kısmı için imza doğrulama özelliği eklemişti. Araştırmacıların bu özelliği de devre dışı bıraktığı gözlemlenmiştir. Tesla araçlarında TCP 1050 portunda çalışan "*file operate agent*" tarafından sağlanan bir servis ile dosya isimleri değiştirilebilmektedir. Ancak script dosya ismini "boot.img" olarak değiştirmeyi engellemektedir.

Bootloader tarafından bu isimdeki dosya direkt olarak yüklenebildiği için bu iyi bir yöntem olarak görünüyor. Ancak araştırmacılar derinlemesine incelediğinde dosya ismi kontrolünde bir zafiyet tespit ediyorlar.

Tesla'nın kullandığı bir dosyayı yeniden isimlendirme metodu olan *fatfs_rename*'de string'in başındaki boşluk ve noktaların kaldırıldığı görülüyor bunun neticesinde yeni isim değişkeni *\x20boot.img* olarak belirlendiğinde dosya ismi *boot.img* 'a eşit mi kontrolü "False" olarak cevap vermekte ve ardından baştaki boşluk karakteri kaldırılmaktadır. Bu sayede araştırmacılar kendi hazırladıkları dosyayı yeni firmware olarak gösterip, kod imzalama koruması atlatmayı başarmış ve kendi kodlarını çalıştırabilmişler.

Tesla Model X araçlarında otopilot modülü aracın en önemli bileşenlerinden birisi. Ancak CID'nin aksine bu modülün (APE) kullanıcı etkileşimi yapılabilecek arayüzü oldukça az. Araştırmacılar ape-updater ismindeki çalıştırılabilir dosyayı kullanarak root kullanıcı hakkı elde etmişler. Bu dosya APE sistemini güncellerken bunu açtığı iki TCP portu ile yapıyor. İlki CID üzerinden komut okumasını sağlarken ikincisi ise basit bir HTTP sunucusu görevi görmektedir. Komut portundan çalıştırılabilecek *install, auth,m3-factory-deploy* gibi birçok komut mevcut. Bazı komutları çalıştırmak için önce *auth* komutu ile yetkilerin yükseltilmesi gerekmektedir. Örneğin 17.17.4 versiyonunda *install ve m3-factory-deploy* komutları yetki yükseltmeden çalıştırılabiliyor. *m3-factory-deploy* komutu içinde URL değişkeni de barındıran JSON çıktı veren bir komut ve *handshake* komutunun sonuçlarını geçersiz kılabiliyor. *install* komutu da kendinden önce üretilmiş JSON çıktısının içerisindeki URL değişkeninde bulunan dosyayı indirme görevini üstleniyor. Bunun neticesinde iki düşük izinli komut ile Tesla HTTP sunucusuna "tesla1" kullanıcısının parolasını içeren dosyanın indirilmesi sağlanıyor. Ardından bu dosya kullanılarak *system* komutuyla oto pilot modülünde root hakkı kazanılmış oluyor.



Şekil 19: Oto pilot modülünde root hakkı kazanılması

Tesla araçlarında easter egg denilen bazı sürprizler de mevcut. Araçlar çeşitli durumlarda bazı gösteriler yapıyor. Örneğin "araçta kimse yokken" "araç park durumunda" "Easter Egg aktif değil" gibi koşullar sağlandığında aşağıdaki Şekil 20'deki gibi görsel bir şov yapıyor.

Araştırmacılar Easter Egg mekanizmasının çalışma sistemini anlayıp, tersine mühendislik ve yukarıda bahsedilen "imzasız kod çalıştırma" zafiyetini birleştirerek kendi Easter Egg sürprizlerini de hazırlayıp çalıştırabilmişler. Fonksiyonellik arttıkça bu gibi akıllı araçlarda bulunan zafiyetlerin sayısı ve çeşitliliği artacağı değerlendirilmektedir.

Şekil 20: Tesla Easter Egg gösterisi[34]

ZARARLI YAZILIM ANALİZİ

12. Yılbaşı Çekilişi Temalı Uygulamalar

Yeni yılın yaklaşmasıyla birlikte mobil bankacılık uygulamalarını hedef alan zararlı yazılım sayısında artış kaydedilmiştir. Android işletim sistemine sahip son kullanıcıları hedef alan ve Google Uygulama Mağazasından yüklenen uygulamalarla ilgili teknik incelemeler yapılmıştır. Son kullanıcıların uygulama mağazasında yer alan bankacılık uygulamalarını indirmeden önce geliştirici bilgisi, yorum ve değerlendirme puanı vb. gibi bilgileri incelemesinin önem arz ettiği değerlendirilmektedir.

İncelemeye konu olan zararlılar, farklı kamu ve özel bankaların müşterilerini hedef alan zararlılardır. Bireysel giriş adı altında müşterilerin ***TC Kimlik/Müşteri Numaraları*** ve ***müşteri parolalarını*** isteyen zararlı, aynı zamanda SMS okuma ve gönderme izinlerini de kullanmaktadır.

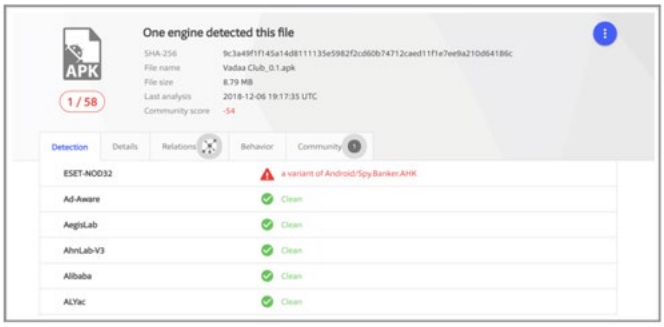
İnceleme yapılan zararlıların uygulama yapıları, paket içerikleri vb. unsurları birbiriyle aynı olmakla beraber sadece isimleri farklılık göstermektedir. Bu özellik, uygulama mağazasına farklı (sahte) isimler ve e-posta adresleriyle konulan zararlı uygulamaların ***geliştiricisinin aynı olduğunu*** göstermektedir.

12.1. Teknik İnceleme

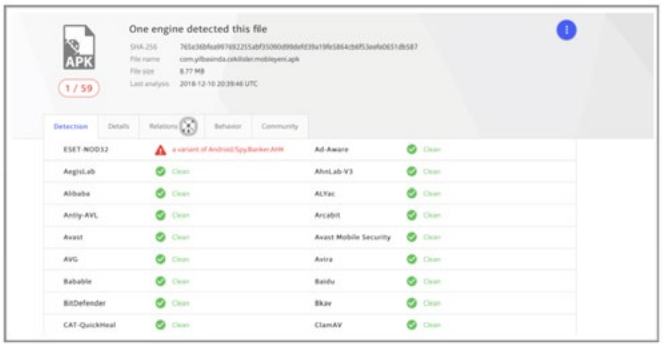
Zararlı uygulamanın açılış ekranı aşağıdaki gibidir.

Şekil 21: Açılış ekranı

İncelenen uygulamaların SHA256 değerlerinin, inceleme sırasındaki VirusTotal sonuçları aşağıdaki gibidir.



Şekil 22: Zararlıya ait VirusTotal sonuçları



Şekil 23: Zararlıya ait VirusTotal sonuçları

Uygulamanın istediği izinler aşağıda görülebilir. İstenen izinler herhangi bir uygulama tarafından da istenebilecek izinler olup son kullanıcı tarafında bir şüphe uyandırmamaktadır.

Şekil 24: İstenen izinler

Kaynak kod incelemesi yapıldığında zararlı uygulamaların Google'ın Firebase hizmetini kullandığı ve zararlı aktivitelerinin sonucunu Firebase hizmetine yüklediği görülmektedir. İncelenen zararlıların bağlantı kurdukları Firebase adresleri "hxxps://vadacue[.]firebaseio[.]com", "hxxps://mobleyeni[.]firebaseio[.]com" olarak tespit edilmiştir. Uygulamalar "Bireysel Giriş" adı altında kullanıcıdan aldığı bilgileri yukarıda belirtilen Firebase adreslerine göndermektedir.

Uygulamalar aynı zamanda SMS ve SDCard ile ilgili yetkileri barındırmıyorsa da, bu yetkileri kullanıcıdan istemektedir.

Şekil 25: Kullanıcı bilgilerinin karşıya yüklenmesi

Şekil 26: Kullanıcıdan istenen yetkiler

Gerekli yetkileri edindiği takdirde uygulamalar kurbanlarının SMS bilgilerini de Firebase adreslerine göndermektedir.

Şekil 27: Kullanıcı SMS'lerinin karşıya yüklenmesi

12.2. Tehdit Vektörü Göstergeleri (Indicator of Compromises)

a) Zararlının iletişime geçtiği alan adı bilgileri
- hxxps://vadacue.firebaseio.com
- hxxps://mobleyeni.firebaseio.com

b) Tespit edilen zararlılara ait hash(özet) bilgileri

1	9c3a49f1f145a14d8111135e5982f2cd60b74712caed-11f1e7ee9a210d64186
2	48b97d3b9b20ef23ca1bc82907968d35efba8cddb4e-a8d93506dae995ed38584
3	765e36bfea997692255abf35090d99defd39a-19fe5864cb6f53eefe0651db587

Tablo 1: Zararlı hash bilgileri

12.3. Tavsiyeler

İlgili zararlılar üzerinde yapılan analiz ve incelemeler sonucunda, zararlının kullanıcılara ait bankacılık bilgilerini çalmayı hedefleyen zararlı android uygulamaları olduğu tespit edilmiştir. Google Uygulama Mağazası bünyesinden uygulama indirirken sahte uygulamalara dikkat edilmelidir. Bu bağlamda uygulama yazarının güvenilir olduğuna ve uygulamanın adının doğru olduğundan emin olunmalıdır. İlgili zararlının iletişime geçtiği IP adresleri ve domain bilgileri anlamında kurum telefon ve cihazlarının iletişimi gözden geçirilmeli, ilgili IP ve domain adresleri kara listeye alınarak engellenmelidir.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

13. Microsoft'tan Uç Nokta Güvenliği Üzerine Yeni Bir Yaklaşım: Kum Havuzu

Geçtiğimiz günlerde Microsoft, Windows işletim sistemlerinde ön tanımlı olarak kullanıcılara sunulan "Windows Defender" anti-virüs yazılımının kendi alanında ilk olarak kum havuzu (sandbox) yeteneğini desteklemeye başladığını açıkladı.

Kum havuzu sistemleri şüpheli dosya ve uygulamaların işletim sisteminden izole edilmiş bir alanda çalıştırılıp analiz edilmesini sağlayan platformları tanımlar. Bu platformlar zararlı yazılım analizi faaliyetlerinin olmazsa olmazlarındandır. Zararlı yazılım türlerine karşı yapılan savunma aşamalarında kullanılan anti-virüs ve benzeri uç nokta güvenlik uygulamalarında tespit edilen veya raporlanan zararlı yazılımların analiz ortamında incelenmesi kum havuzu sistemlerinin temel çalışma prensibidir.

Gelişen teknolojiye paralel ivme kazanan zararlı yazılım çeşitleri ve saldırı yöntemleri, işletim sistemlerinde en yüksek seviyede çalışan uç nokta güvenlik sistemlerini de hedef almakta ve söz konusu uygulamalara yönelik zafiyetlerin keşfedilmesiyle kullanıcılara yönelik tehdit oluşturmaktadır. Önceden sahte güvenlik yazılımı formunda kullanıcıların karşısına çıkan zararlı türlerinin güvenlik yazılımlarındaki açıkları sömürecek kapasiteye ulaşmasıyla uç nokta güvenlik çözümlerinde sandbox ve davranış analizi (behavior analysis) yeteneklerine ihtiyaç olduğu ortaya çıkmıştır. Bu ihtiyacı birkaç yıl önce saldırganların uç nokta güvenlik zafiyetlerini istismar ederek hedef sistemde tam kontrol sağlaması tetikledi. Microsoft'un attığı bu adımın birçok uç nokta güvenlik uygulamasına da benzer yeteneklerin entegre edilmesini getireceği söylenebilir[21].

Sandbox özelliğini henüz tüm kullanıcılar için otomatik olarak aktive etmeyen Microsoft, Windows 10 işletim sistemi kullanıcılarından işletim sistemini sürüm 1703 (Creators Update) veya sonraki güncellemelerle güncellemiş olanların bu özelliği aktive edebileceğini belirtiyor. Söz konusu yeteneğin sisteme entegre edilmesinin birçok önemli değişiklik gerektirdiğini belirten ve bu nedenle olası potansiyel performans problemlerini çözmek için kullanıcılardan performans, fonksiyonellik ve güvenlik bağlamında geribildirim bekleyen Microsoft, bu gelişmenin inovasyon yolculuğunda ("Windows Defender ATP" ve "Microsoft Threat Protection") doğru bir adım olduğunu söylüyor ve kullanıcılardan gelen geribildirimler sonrası yapılacak iyileştirmelerin akabinde sandbox özelliğini tüm kullanıcıların kullanımına sunacağının altını çiziyor[22].

Sandbox özelliğini aktive etmek isteyen kullanıcıların CMD (Command Prompt) konsolunu yönetici haklarıyla çalıştırdıktan sonra aşağıdaki kod çağrısını yapıp cihazlarını yeniden başlatmaları gerekiyor.

- **"setx /M MP_FORCE_USE_SANDBOX 1"**

Sandbox özelliği aktive edildiğinde MsMpEngCP.exe ve MsMpEng.exe işlemleri çalıştığı görülebilir.

Her ne kadar bu değişimin temelinde Windows Defender ve benzer uç nokta güvenlik uygulamalarına yönelik zafiyetlerin araştırmacılar tarafından keşfedilip sömürülmesi yatıyor gibi görünse de, söz konusu yeteneğin bir ihtiyaç olduğunun ve gelecek dönemlerde daha da ön plana çıkacağının altını çizmekte fayda var.

14. 802.1X ve MACsec Güvenliği

2001 yılında tanımlanan 820.1x standardı ağda yer alan ikinci katman haberleşme sırasında, cihazlar arasında kimlik doğrulama için kullanılmaktadır. Standart 2001 yılından sonra 802.1x-2004 ve 802.1x-2010 olarak iki defa güncellendi. 802.1x-2010 ile birlikte gelen şifreleme (MACsec) ve her pakette bütünlüğün kontrol edilmesi ile önceki versiyonlara yapılan "injection" türündeki saldırılar önlenmiş oldu.

802.1x protokolünde 3 temel bileşen yer alıyor. Bunlar:

- Ağa katılacak uç nokta (supplicant)
- Ağa giriş iznini verecek anahtarlama (switch) cihazı (authenticator)
- RADIUS benzeri kimlik doğrulama ve yetkilendirmeyi sağlayacak sunucu (authentication server)

Ağa katılım süreci ise şu sırayla işliyor:

1. Ağa yeni katılacak uç noktanın kullandığı port, anahtarlama cihazı tarafından algılanarak sadece 802.1x trafiğinin geçmesine izin verilir.
2. Uç nokta "EAPOL-Start" paketiyle ağa katılmak istediğini bildirir. Daha sonra "EAP-Response-Identity" paketiyle kullanıcı adı gibi bir kimlik belgesini anahtarlama cihazına iletir. Anahtarlama cihazı bu bilgiyi AAA sunucusuna iletir.
3. AAA sunucusu ve uç nokta arasındaki kimlik doğrulamanın hangi EAP (Extensible Authentication Protocol) metoduyla yapılacağı kararlaştırılır.
4. Kararlaştırılan EAP metoduyla (EAP-MD5, EAP-TTLS, EAP-TLS gibi) kimlik doğrulama gerçekleştirilir ve uç cihazın ağa katılıp katılamayacağına karar verilir.

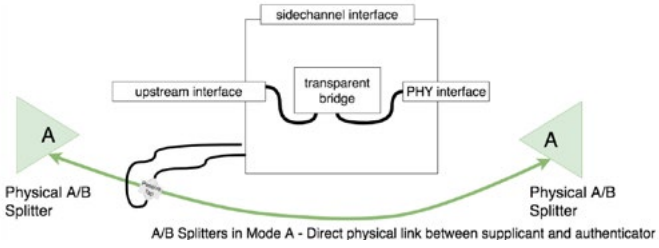
vmcompute.exe	< 0.01	4588	Hyper-V Host Compute Servi...	Microsoft Corporation	System
vmwp.exe		116	Virtual Machine Worker Proc...	Microsoft Corporation	High
svchost.exe		4596	Host Process for Windows S...	Microsoft Corporation	System
MsMpEng.exe	0.45	4612	Antimalware Service Execut...	Microsoft Corporation	System
MsMpEngCP.exe		12868	Antimalware Service Execut...	Microsoft Corporation	AppContainer
vmms.exe	< 0.01	4660	Virtual Machine Managemen...	Microsoft Corporation	System
svchost.exe		5012	Host Process for Windows S...	Microsoft Corporation	System
svchost.exe		5032	Host Process for Windows S...	Microsoft Corporation	System

Şekil 28: Windows Defender Sandbox özelliği altına çalışan işlemler

DEF CON 26 'da sunulan bir makalede MACsec dahi kullanılsa özel hazırlanmış bir saldırı cihazıyla 802.1x-2010 ve MACsec güvenliğinin atlatılabileceği gösterildi. Araştırmacılar Şekil 29'da örneği görülen mekanik Ethernet ayıraçlarından esinlenerek bir prototip saldırı cihazı oluşturdular[23].

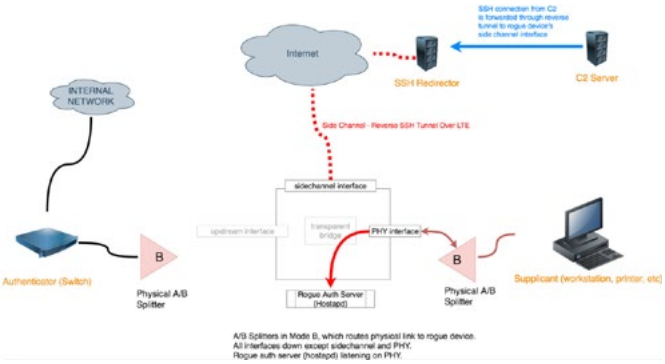
Şekil 29: Mekanik ethernet ayıraçları

Bu prototip cihazda fiziksel Ethernet yollarını mekanik olarak ayırabilen ve bir Arduino kart tarafından kontrol edilen selenoid valflar mevcut. Ayrıca uç nokta ve anahtarlama cihazına bakan ağ arayüzleri (upstream anahtarlama cihazına, PHY interface de uç noktadaki cihaza bakıyor) var. Sidechannel interface arabirimi de uzaktan ssh erişimine izin veren bir arkakapı. Tüm bu arayüzler Intel NUC bir mini-pc cihaza yerleştirilip üzerine de Fedora 28 işletim sistemi kurulmuş.



Şekil 30: Sahte anahtarlama cihazı

Böylelikle saldırganlar normalde Şekil 30'de göründüğü gibi iki cihaz arasındaki tüm trafiği pasif bir şekilde dinleyebiliyor. Bu dinleme sırasında 802.1x-2004 ile birlikte EAP-MD5 gibi zayıf bir kimlik doğrulama metodu kullanılıyorsa, bunu da sözlük saldırılarıyla kırmaya çalışıp kimlik doğrulama bilgilerini ele geçiriyor. İstenildiğinde aradaki fiziksel bağlantıyı kesip uç noktadaki cihazı ağdan atıyor ve ele geçirdiği kimlik bilgileriyle kendini ağa dahil edebiliyor. Ancak ortamda 802.1x-2010 protokolü kullanılıyorsa ve EAP-TTLS vb. şifreli kimlik doğrulama protokolleri aktifse araya girip pasif bir şekilde dinleme yapmak mümkün değil. Bu durumda saldırganlar sırasıyla aşağıdaki adımları izliyorlar.



Şekil 31: 802.1x-2010 bypass adımları –Sahte RADIUS sunucusu ile kimlik bilgilerinin çalınması

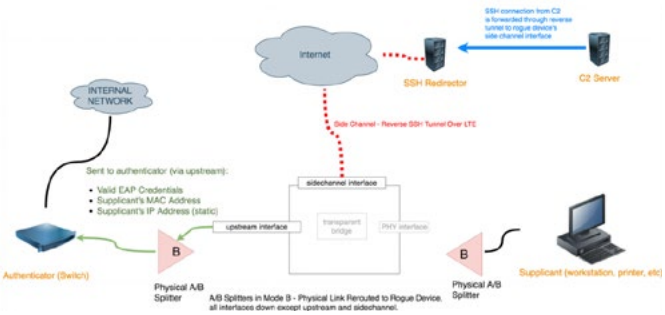
1. Saldırı cihazında sahte bir RADIUS sunucu ayağa kaldırılıyor ve bu sunucu için sahte bir sertifika üretiliyor. Uç nokta ve anahtarlama cihazı arasındaki trafik kesiliyor.

2. RADIUS sunucusundan uç cihaza "EAP-Request-Identity" paketi yollanarak kimlik doğrulama adımlarının tekrar başlanması tetikleniyor.

3. Uç nokta bu sunucunun sertifikasının geçersiz olduğunu anlıyor. Ancak bu durumda devam edip etmemek kullanıcılara bırakılmış durumda, kullanıcı sertifikayı kabul ederse kimlik bilgileri RADIUS sunucu tarafından alınmış oluyor (Şekil 31). Araştırmacılar yazıcı, IP telefon vb. aygıtlarda 802.1x-2010'un çoğunlukla doğru gerçekleşmediğini ve sahte sertifikaların bazı cihazlar tarafından varsayılan olarak kabul edilebildiğini de belirtiyorlar. Bu durumda yazıcı, IP telefon, kamera vb. cihazlar ağa sızmak için en zayıf halkaları oluşturuyor.

4. Gerekli kimlik bilgileri ele geçirildikten sonra uç cihazın ağ bağlantısı tamamen kesiliyor ve anahtarlama cihazıyla saldırı yapılan cihaz tekrar konuşmaya başlıyor. "Upstream Interface" arabirimine uç cihazın IP'si ve MAC adresi yazılıyor ve fark edilmeksizin cihaz ağa sızmış oluyor.

5. Cihaz üzerindeki SSH servisi ve NAT kullanımıyla uzaktan ağa sızma işlemi başarıyla gerçekleşmiş oluyor (Şekil 32).



Şekil 32: 802.1x ve MACsec kullanılan ağa sızılması

Bu yöntem her ne kadar geliştirilen ufak bir cihazın ağa yerleştirilmesi gibi bir senaryoyu içerse de, büyük binalarda, ziyaretçilerin fazla olduğu yerlerde hatta kötü niyetli kullanıcılar tarafından fark edilmeden uygulanabilir bir yöntem olarak gözüküyor. Yine de kullanıcılara verilecek farkındalık eğitimiyle sahte sertifikalara güvenmemeleri sağlanabilir. Yazıcı, IP telefon vb. cihazların da konfigürasyonları izin verdiği ölçüde sahte sertifikalara güvenmemesi sağlanmalıdır. Ayrıca EAP-MD5 vb. zayıf kimlik doğrulama algoritmalarının da kullanılmaması gerekir. En güvenli yöntemin EAP-TLS gibi çift taraflı kimlik doğrulama gerektiren bir protokol olduğunu ve mümkünse 802.1x-2010 ile birlikte EAP-TLS'in kullanılması gerektiğini de hatırlatmakta fayda var.

15. Konteyner Güvenliği

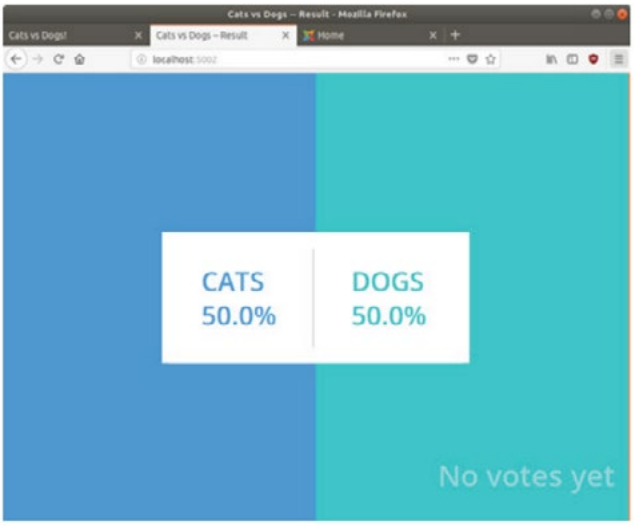
Konteyner güvenliği hakkında son 3-4 senedir art arda araştırmalar yayınlanıyor. DEF CON 23 konferansında David Mortman, Docker mimarisi, mevcut ve planlanan güvenlik özellikleriyle geliştiricilerin alması gereken önlemler hakkında bir tebliğ sundu. Yine aynı konferansta Aaron Grattafiori, daha alt seviyede Linux çekirdeğinin konteynerler için uygunluğu hakkında bir konuşma yaptı ve Linux sıkılaştırmalarına dikkat çekti. Black Hat USA 2017 konferansında ise Michael Cherney ve Sagie Dulce ikilisinin Docker üzerinde bulunan zafiyetlere odaklandığını görüyoruz. Ağustos ayında gerçekleştirilen DEFCON 26 kapsamında yapılan bir çalışma ise büyük ölçekli dağıtımlarda çoklu konteyner yapılarına odaklanmıştır[24].

Konteynerin yaptığı soyutlaştırmadan dolayı dağıtımı konteynerle yapılmış uygulamalar, sadece uygulama güvenliği alanında eğitimli uzman kişiler değil, uygulama güvenliği konusunda uzmanlaşmamış ama taktiksel ağ saldırısı yapabilen kişiler tarafından da istismar edilebilir hale gelebilir. Ayrıca konteyner mimarisinin getirdiği soyutlaştırma, uygulama güvenliği yetkinliğine sahip olmayan saldırganların geleneksel sızma testi araçlarını ve taktiklerini kullanmasını da olanaklı kılar.

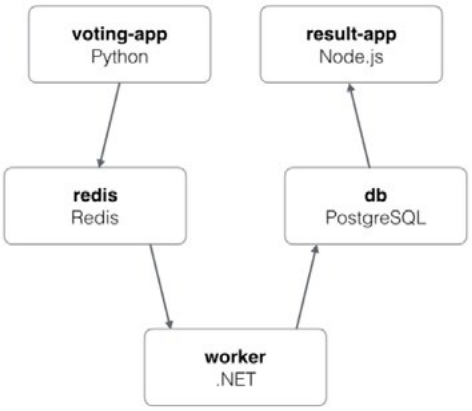
Docker hedef bir uygulama platformu olarak tekil uygulama mimarisi ya da çoklu servis mimarisi dağıtımı için kullanılabilir. Konteyner üzerinde tekil mimaride dağıtımı yapılmış uygulamalar için saldırı geleneksel uygulama dağıtımlarından çok farklı olmayacaktır. Fakat istismar işlemi sonrasında Docker sahip olduğu varsayılan ayarlar yüzünden ve dışarıyla haberleşmede kullandığı portlarla saldırılara açık olacaktır.

Araştırmacılar çoklu konteyner yapısının saldırı yüzeyini ne kadar artırdığını göstermek için, konteyner mimarisini yeni öğrenmeye başlayan kişilerce çok sık kullanılan "The Docker Example of Voting App" isimli bir uygulamayı temel almışlar (Şekil 33). Uygulama 5 ayrı Docker imajından oluşuyor ve her imajın görevi özetle şu şekilde tanımlanıyor[25] (Şekil 34).

- Python web arayüzü
- Oyları toplayan redis sunucu
- Redis sunucudan oyları alan ve veritabanına yazan .Net uygulaması
- PostgreSQL veritabanı sunucusu
- Sonuçları görmek için Node.js web arayüzü



Şekil 33: Docker oylama uygulaması



Şekil 34: Docker imajlarının etkileşimi

Birlikte bir bütün oluşturan her biri bağımsız bir dilde yazılmış bu imajlar uygulama geliştiriciler için çok büyük kolaylık sağlamakta, ancak zafiyet yüzeyini genişlettiği de aşikâr. Araştırmacılar joomla'nın zafiyetli bir versiyonunu barındıran bir imajı da konteyner yapısına ekleyerek saldırganların nasıl ilerleyebildiğini görmek istemişlerdir. Joomla üzerindeki zafiyet istismar edildikten sonra saldırgan ilk olarak konteyner yapısından haberdar değildir. Ancak basit bir port taraması veya /proc/1/cgroup

dosyasının içeriğinin okunmasıyla diğer imajlar hakkında bilgi sahibi olabilir. Tüm imajlar aynı ağ arayüzü üzerinden haberleştiğinden saldırgan port taraması sonrası aşağıdaki bilgilere ulaşabilir.

- *examplevotingapp_result_1.examplevotingapp_front-tier (172.20.0.2)*
- *a3f280146222 (172.20.0.3) (Joomla)*
- *examplevotingapp_vote_1.examplevotingapp_front-tier (172.20.0.4)*
- *db.examplevotingapp_back-tier (172.21.0.2)*
- *redis.examplevotingapp_back-tier (172.21.0.3)*
- *examplevotingapp_result_1.examplevotingapp_back-tier (172.21.0.4)*
- *a3f280146222 (172.21.0.5)*
- *examplevotingapp_worker_1.examplevotingapp_back-tier (172.21.0.6)*
- *examplevotingapp_vote_1.examplevotingapp_back-tier (172.21.0.7)*

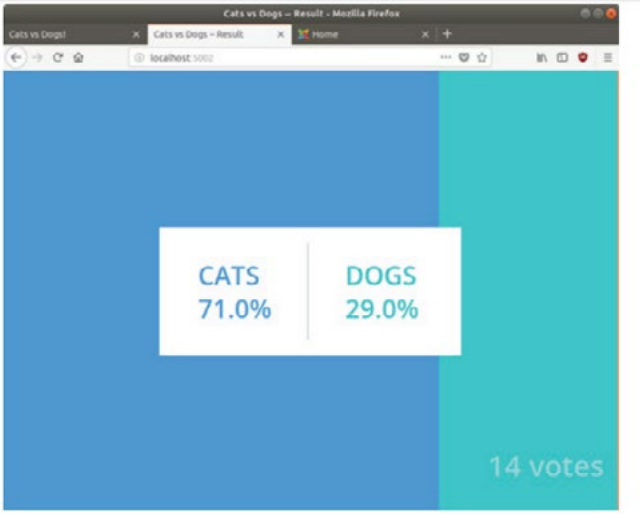
Varsayılan olarak bir kimlik doğrulama gerektirmeyen Redis konteynerine bağlanılarak yapılan bağlantılar izlendiğinde yapılan oylamaların formatı çözülebiliyor (Şekil 35).

```
+1517345973.133383 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.235806 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.338204 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.440434 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.503102 [0 172.21.0.7:49212] "RPUSH" "votes" "{\"vote\": \"b\",
\"voter_id\": \"6318cb4c0b00af50\"}"
+1517345973.543386 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.875534 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345973.977387 [0 172.21.0.6:48177] "LPOP" "votes"
+1517345974.078515 [0 172.21.0.6:48177] "LPOP" "votes"
```

Şekil 35: Redis sunucunun izlenmesi

Daha sonra ise saldırganın herhangi bir "root" yetkisi olmamasına rağmen, redis konteyneri üzerinden veritabanına istenilen formatta oylar yollanarak manipülasyon yapılabiliyor (Şekil 36).

Sonuç olarak çoklu konteyner yapıları saldırganlara ağ üzerinden saldırmaya daha fazla olanak verir ve içerideki yerel ağ yapısı çözüldüğünde atak yüzeyini genişletir. Burada verilen örneklerde de görüldüğü gibi saldırgan uygulama güvenliği alan bilgisine ihtiyaç duymaksızın ağ saldırı yetenekleriyle ve herhangi bir yetki kazanmadan uygulamaları maniple edebilir. Bununla birlikte konteyner altyapısına ve çalışma prensiplerine de hâkim olursa çoklu konteyner yapılarına etkili saldırılar yapabilir. Bu sebeple konteyner mimarisi tasarlanırken ağ mimarisine ve güvenliğine çok daha fazla önem verilmelidir.



Şekil 36: Manipülasyon sonrası oy durumu

16. Master Parmak İzi

Her kilit sistemi açılabildiği gibi her biyometrik sistemi de aldatabilen bir yöntem mevcuttur. Araştırmacılar yıllar boyunca akıllı telefonları korumak için kullanılan popüler parmak izi sensörlerinin, parmak izleri ya da dijital parmak izi verileri kullanılarak aldatılabildiğini göstermiştir. Ancak, New York Üniversitesi (NYU) Tandon Mühendislik Okulundan araştırmacıların bu konudaki son çalışmaları çok daha farklı ve çarpıcı sonuçlar ortaya koymaktadır. Araştırmacılar, akıllı telefon sensörlerini aldatan ve aynı anda birçok kişinin parmak iziymiş gibi gösterilebilen "DeepMasterPrints" olarak adlandırdıkları taklit parmak izlerini üretmek için makine öğrenmesi yöntemleri geliştirdiler. Yöntem kabaca, parmak izi korumalı cihazlar için bir mastır anahtar olarak düşünülebilir[26].

Yöntem parmak izlerinin yaygın özelliklerini birleştiren "master iz" konseptinin geliştirilmesine dayanmaktadır. İlk çalışmalarda NYU araştırmacıları, değişik özellik ve karakteristikleri bir arada içererek birçok kişi için kimlik doğrulaması yapabilecek master izlerini manuel yöntemlerle tanımlamaya çalışmıştı. Yeni çalışma ise makine öğrenmesiyle manuel yöntemin başarısının artırılmasına dayanıyor.

Çalışmanın istismar ettiği ana zayıflık, mobil cihaz parmak izi tarayıcılarının nispeten küçük olması nedeniyle kullanıcıların parmak izlerinin sadece bir kısmının taranabilmesi ve bunun sonucu olarak parmağın taranmayan kısımları için varsayımlar yapılmasıdır. Dolayısıyla, bu sistemleri aldatmak için daha az sayıdaki değişken için veri üretilmesine ihtiyaç vardır.

Araştırmacılar önce gerçek parmak izi imajlarıyla oluşturdukları yapay sinir ağını eğiterek bir takım gerçekçi parmak izi parçaları oluşturmuşlar. İkinci aşamada ise, "evrimsel optimizasyon" (evolutionary optimization) olarak adlandırdıkları yöntemle master parmak izini üretmişler. Ardından geliştirdikleri sentetik mastır parmak izlerini

VeriFinger ve iki ayrı ticari ürün üzerinde test etmişler. Test neticesinde, kullanılan mastır parmak izine bağlı olarak, orta seviyeli bir korunma düzeyinde, sistemlerdeki mevcut parmak izlerinde yüzde 2 ila yüzde 20 arasında değişen oranlarda başarılı eşleşme sağlanmıştır.

Makine öğrenmesi yöntemiyle mastır parmak izi üretilerek biyometrik sistemlerin kandırılmasına ilişkin elde edilen ümit verici sonuçlar bu yöntemin daha başarılı uygulamalarının geliştirilebileceği anlamına geliyor. Bu kapsamda, bu yeni yöntemle ilgili farkındalık artırılarak, birçok sistemin bu yöntemle üretilen parmak izi saldırılarını da dikkate alacak şekilde algoritmik olarak güncellenmesine ve güvenlik sıkılaştırılması yapılmasına ihtiyaç vardır.

17. HL7 Protokolü ve Zafiyetler | Pestilence

HL7 standardı genellikle hastane ağı üzerinde bilgilerin, kimlik doğrulama ve şifreleme olmadan belli bir formatta aktarılmasını sağlamaktadır. HL7 protokolüne yapılan saldırılar kişisel bilgilerin ortaya çıkmasının yanı sıra, hastaların fiziksel olarak zarar görmesine de sebep olabilir. Bir grup araştırmacı Black Hat USA 2018'de geliştirdikleri bir araç yardımıyla yaptıkları ortadaki adam (man-in-the-middle) saldırısıyla hastaların klinik bilgilerini normal düzeyden kritik durumları işaret eder hale gelecek şekilde maniple etmeyi başarmışlar[27]. Verilerin bu şekilde değiştirilmesiyle sağlık personeli hastanın durumu hakkında yanlış bilgilendirilerek farklı ilaç dozları veya yöntemler kullanmaya yönlendirilebilir. Bunun sonucu olarak da, hasta daha ciddi sağlık problemleriyle hatta ölümle yüz yüze kalabilir.

Tıp pratiği, hipotez geliştirilmesi ve test edilmesi üzerine inşa edilmiştir. Hastalık, öznel semptomların bir takım halinde ortaya çıkması ve bunun da sağlık personeli tarafından teşhis edilmesiyle ortaya çıkarılır. Günümüzde doktorlar bu tanıları koyarken gelişmiş birçok teknolojik donanım kullanıyor. Elektronik tıbbi kayıtları içeren geniş bir teknolojik altyapı, otomatik sipariş sistemleri, dijital görüntüleme ve internet bağlantılı tıbbi cihazlar bunlara örnek olarak verilebilir.

Sağlık hizmetlerini kolaylaştıran sayısız teknoloji ve alt yapı arasında en önemlisi HL7 (Health Level 7) standardıdır. Çok yaygın olarak kullanılan bu iletişim sistemi neredeyse bütün hastane içi iş akışları için protokoller belirlemektedir. Sağlık bilgilerinin elektronik ortamda paylaşımı, laboratuvar sonuçlarının izlenmesi, görüntüleme sonuçları, hastane kabulleri ve ilaç siparişleri bunlardan bazılarıdır. 1970'ler de akademik olarak geliştirilmeye başlamış olan HL7, 1990'lardan itibaren yaygın bir şekilde kullanıma girmiştir.

Günümüzde kullanılan HL7 standardının iki ayrı versiyonu vardır. Biri 1989 yılında tasarlanan ve daha yaygın olarak kullanılan 2. versiyondur. Diğeri ise 2005 yılında tasarlanan 3. Versiyondur, ancak geriye uyumlulukla ilgi sıkıntıları yüzünden daha güncel olmasına rağmen bu versiyon daha az kullanılmaktadır. Şekil 37'te görüldüğü gibi tipik bir HL7 mesajı açık metin olarak iletilmektedir. Mesajlar, laboratuvar bilgi sistemi (LBS) ile medikal kayıt sistemi (MKS) arasında çift yönlü olarak aktarılmaktadır. Test istekleri LBS'ye yapılırken, laboratuvar test sonuçları da MKS'ye gönderilmektedir. Aradaki iletişim klasik TCP istemci sunucu mimarisini içerir ve bağlantılar kısa ömürlü olduğu için bu iletişim ARP zehirlemesi saldırılarına karşı zafiyet barındırmaktadır.

```
MSH|^~\&|Rapidcomm |Hospital|OpenEMR|Hospital|20180719164041||ORU^R01|0C0AGPD228ZGM001D808|P|2.4|||AL|AL|
PID|||99||TTT^ST|||U|
ORC|RE|
OBR|1|6|0C0AGPD228ZGM001D808|666^Venous Blood Gas|R|||||O||||BLDA^^^^^^P|^Administrator|||||||F|
OBX|1|ST|pH||7.12|7.350-7.450|L|||F|||20150528093432|||^^0143^RAPIDPoint 405|20150528093432|
OBX|2|ST|pCO2||27|mmHg|35.0-45.0|||F|
OBX|3|ST|pO2||77|mmHg|75.0-100.0|H|||F|
OBX|4|ST|tHb||21.5|g/dL|12.0-18.0|H|||F|
OBX|5|ST|O2Hb||97.0|%|94.0-97.0|||F|
OBX|6|ST|COHb||0.4|%|0.5-1.5|L|||F|
OBX|7|ST|MetHb||0.6|%|0.0-1.5|||F|
OBX|8|ST|HHb||2.0|%|0.0-5.0|||F|
OBX|9|ST|HCO3act||7|mmol/L|||||F|
OBX|10|ST|BE(B)||-12|mmol/L|||||F|
OBX|11|ST|sO2||98.0|%|92.0-98.5|||F|
OBX|12|ST|Samp. Type||BLDV|||||F|
```

Şekil 37: Tipik bir HL7 mesajı

Göründüğü gibi hiçbir şifreleme işlemine tabi tutulmadan bilgiler ağ üzerinden aktarılır. HL7 Standart Komünitesi Health Level Seven International, şifrelemenin uygulama katmanının altında gerçekleştirilmesini tavsiye ediyor. Ayrıca, HL7 standartı kimlik doğrulama ve mesaj kaynağının doğrulanması noktalarında da eksiklikler içermektedir. Bu yüzden sistemler arasında dolaşan veriler manipülasyona karşı savunmasız durumdadır. Kötü niyetli bir kişi eğer ağı dinleme imkânına erişirse arada akan veriyi yakalayıp basit regex ve söz dizimi değişiklikleri yaparak manipülasyon yapabilir.

Araştırmacılar, geliştirdikleri bir siber saldırı aracıyla simülasyonunu yaptıkları bir man-in-the-middle saldırısıyla laboratuvar ortamında kan analiz cihazı ile HL7 ara yüz motoru arasındaki trafiğin yakalanıp değiştirilebildiğini pratik olarak göstermiştir.

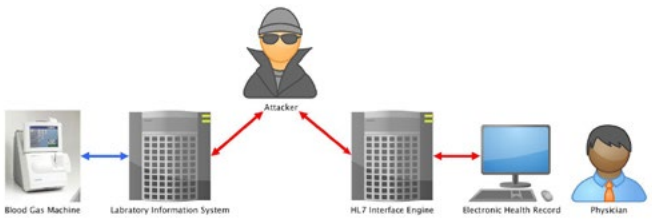
Simülasyonun gerçekleştirildiği ortamda kullanılan cihazlar, açık kaynak kodlu bir elektronik medikal kayıt sistemi (OpenEMT v5.0.1, OEMR), HL7 bağlantı motoru (Mirth Connect v3.6.1 NextGen Healthcare, Irvine CA), Laboratuvar Bilgi Sistemi (Siemens RapidComm v6.1) ve RAPIDPoint 405 Kan Analiz Cihazıdır (Siemens Healthcare v3.9). Elektronik hasta kaydı, HL7 ara yüz motoru ve Laboratuvar Bilgi Sistemi iki ayrı bilgisayar üzerinde konumlandırılmışken cihazlar arasındaki ağ bağlantısı da Ethernet üzerinden sağlanmaktadır. Sistemdeki her cihazın sabit IP adresleri atanmaktadır.

Şekil 38: Saldırı yapılan mimari

Bu simülasyonda araştırmacılar, Python programlama dilinde bir paket manipülasyon kütüphanesi olan Scapy'yi, çoklu işlem parçalarını ve diğer TCP/IP soket kütüphanelerini kullanarak geliştirdikleri bir araç olan "Pestilence"i kullanarak tipik bir man-in-the-middle saldırısı gerçekleştiriyorlar.

İlk olarak Pestilence hedeflerine yönelik olarak ARP zehirleme saldırısı yapılıyor. Bunun için ağ yönetiminin ARP zehirlemesi için ekstra bir önlem almamış olması gerekmektedir. Bu adımdan sonra program her bir hedef için bir tane olacak şekilde iki adet iş parçacığı oluşturuyor. Arada akan çift yönlü trafikte bir hedeften gelen bilgileri okuyup gerekli işlemleri yaptıktan sonra diğer iş parçacığıyla değişen bilgileri sanki hastadan geliyormuş gibi tekrar ağ trafiğine gönderiyor.

Her iş parçacığı çift yönlü olan trafiğin bir yönünden sorumludur. İlk iş parçacığı bir TCP sunucu gibi hedeften gelecek olan bağlantıyı beklemeye başlıyor. Hedef tarafından Pestilence'i TCP bağlantısı kurulunca (bu bağlantıya A-bağlantısı diyelim), program hemen cevap vererek karşı tarafta gerçek bir sunucu olduğu izlenimini yaratıyor. Bununla eş zamanlı olarak Pestilence başka bir TCP bağlantısını diğer hedef olan gerçek sunucuyla gerçekleştiriyor (B-bağlantısı). Daha sonraki adımlarda her iki bağlantı ayrı ayrı sürdürülmektedir. A bağlantısından alınan paketler bir kuyruk yapısında tutularak sıraya konuyor ve istenilen değişiklikler yapıldıktan sonra B bağlantısına gönderiliyor. Burada her iki bağlantıda kendi ACK/SEQ numaralarını tutarak farklı farklı bağlantılar olarak saldırı süresince devam ediyor.



Şekil 39: Saldırı illüstrasyonu

Sonuç olarak araştırmacıların klinik ortamlardaki bu zafiyetleri en aza indirmek için önerdiği üç önemli strateji var:

1. Güvenli ağ alt yapıları kurmak, ağ yapısını VLAN ile bölümlere ayırmak ve güvenlik duvarları kullanmak: Bu yöntem eski veya operasyonel olarak bütçe sıkıntısı yaşayan sağlık bilgi sistemleri için alınabilecek en önemli önlemdir. Zafiyet içeren cihazların saldırı yüzeylerinin azaltılması kuşkusuz saldırı olasılığını da düşürecektir. Bu tip bir uygulama deneyimli BT uzmanlarına ihtiyaç duyar. Ağda var olan ve zafiyet barındıran cihazları izole etmek saldırı olanaklarını en aza indirecektir.
2. Doğru ve uygun yapılandırma: Diğer bir seçenek ise var olan ağ cihazlarının güvenli şifreleme protokolleri kullanacak şekilde yapılandırmasıdır.
3. Güvenlik bilinci yüksek ekosistemler: Daha ileri bir adım olarak da, cihaz geliştiricilerinin, servis sağlayıcılarının, standartları belirleyen organizasyonların ve politika belirleyicilerin gerekli güvenlik önlemleri için daha aktif ve bilinçli roller alarak ekosistemi yönlendirmeleridir. Örneğin güvenlik tanımları ve kullanımı açısından daha başarılı, HL7'ye alternatif olacak bir standart geliştirilebilir.

18. Zararlı Yazılımların Yeni Hedefi IoT Cihazlar

Ampullerden kol saatlerine, kalp monitör implantlarından arabalara kadar IoT cihazlar artık her alanda hayatımıza girmiş bulunuyor; bu durum IoT cihaz sayısında ve çeşitliliğinde durdurulamayan bir artışa neden olmaktadır. 1980'li yıllarda ilk kez bir kola makinesinin durumunu takip etmek için kullanılmış olan IoT cihazların sayısı şimdiden insan nüfusunu geçti ve tahminlere göre 2020 yılında insan nüfusunun 6 katını aşmış olacak. Sayılarının bu kadar büyümesi ve artmaya devam etmesi bu cihazları saldırganlar ve zararlı yazılımlar için olası hedef haline getiriyor[29].

Sürekli açık ve internete bağlı olmaları, güvenlik farkındalığının ve zararlı yazılımlara karşı korunma yöntemlerinin bilgisayarlara göre çok daha az olması bu cihazların hedef olmasının başlıca nedenlerini oluşturuyor. Ayrıca IoT platform sayısının fazla olması, zararlı yazılımların sistemde saptanmasının ve kum havuzu içinde çalıştırılmasının da zor olması bu cihazları saldırganlar için kusursuz hedef haline getiriyor.

Black Hat USA – 2018'de yayınlanan bir araştırmaya göre sadece 2018 yılının ilk yarısında 120.000'den fazla zararlı yazılım türevi kullanılarak IoT cihazlara saldırı gerçekleştirildi. Bu sayı 2017 yılı boyunca gerçekleşen zararlı yazılım türevlerinin 3 katından daha fazla. Çığ gibi bir hızla büyüyen zararlı yazılım sayısı, 2017 yılında bir önceki yılın 10 katına çıkmıştı[30],[31].

Bilinen tüm zararlı yazılım ailelerinden (60 tane) 24'ü incelendiğinde, zararlı yazılımın ilk olarak ortaya çıkması ve bu zararlı yazılımla ilgili kuralın IDS/IPS sistemlerde tanımlanması arasında hiç de küçümsenmeyecek bir süre geçtiği fark ediliyor.

Metrik Adı	Ortalama (gün)	Medyan (gün)
Zararlı yazılımın ilk ortaya çıkması ve ilgili IDS kuralının kamuya duyurulması arasında geçen süre	675	166
Zararlı yazılımın analiz örneğinin yayınlanması ve ilgili IDS kuralının kamuya duyurulması arasında geçen süre	241	63
Zararlı yazılımın teknik raporunun yayınlanması ve ilgili IDS kuralının kamuya duyurulması arasında geçen süre	32	25

Tablo 2: Zararlı yazılımın ortaya çıkması, analiz örneğinin yayınlanması ve teknik raporun yayınlanmasıyla IDS/IPS kuralının yayınlanması arasında geçen süre

Zararlı yazılımların genellikle ilk amaçları çok sayıda cihaza erişerek güçlü botnet oluşturmaktır. Saldırgan, botneti oluştururken ele geçirdiği cihazları da yeni kurbanlar bulmak için kullanabilir ve böylece kurban arayış hızını giderek artırabilir. 400.000'den fazla sisteme, 5 günden kısa bir sürede bulaşan Blaster (worm) zararlı yazılımını buna iyi bir örnek olarak verebiliriz. İlk tabloya benzer şekilde 60 zararlı yazılım ailesinden 17 yazılım ailesinin sahip olduğu botnet büyüklüğü, bir zararlı yazılımın botnet kullanarak yapacağı saldırıların ne kadar korkunç sonuçlar doğurabileceğini gösteriyor.

Zararlı Yazılım	Botnet büyüklüğü (cihaz sayısı)
BrickerBot	10.000.000+
ChuckNorris	300.000-330.000
SOHOPharming	300.000
Hajime	130.000-300.000
Wifatch/Ifwatch	60.000-300.000
Mirai	49.657-145.607+
Bashlite/Gafgyt	120.000
Persirai	120.000
Psyb0t	80.000-100.000
ExploitKit/DNSChanger	56.000
Moose/Elan	50.000
http81	43.621
Darlloz/Zollard	31.000
RaspberrPi_Linux.ProxyM	10.000+
PNScan1	1.439
TheMoon	1.000
Slingshot	100

Tablo 3: Zararlı yazılımlar ve Botnet büyüklükleri

Zararlı yazılımların arka planda kullandığı zafiyetlerin odaktan kaçması da ayrı bir problemdir. Zararlı yazılımdan korunmak yerine ilgili zafiyeti gidermek bazen çok daha kolay olacakken bu durum göz ardı edilebiliyor. D-Link DIR645 yönlendiricilerine (router) yönelik oluşturulan Hydra zararlı yazılımı tahminlere göre ilk 2008'de görüldü. Bu zararlı yazılım, varsayılan parolaları kullanarak ya da kimlik doğrulamayı (authentication) bypass ederek cihaza izinsiz erişim sağlanmasına neden olan bir zafiyete dayanıyordu. 2011 yılında bu zararlı yazılımın kaynak kodu sızdırıldı ve açık kaynak olarak paylaşıldı. Ancak bu süreçte Ulusal Zafiyet Veri tabanı (NVD) üzerinde CVE numarası almadı. Ardından aynı zafiyet Kasım 2017'de tekrar kullanılarak IoTReaper saldırısı gerçekleşti. Arada geçen 10 yıldan fazla süreye, bir zararlı yazılım saldırısının yaşanmasına, bu zararlı yazılımın yayınlanmasına ve zafiyete ait bir Metasploit modülünün olmasına rağmen bu zafiyet hâlâ geçerli bir CVE numarasına sahip değil!

Büyük ölçekte etki oluşturan, aynı zamanda giderek gücünü artıran bu zararlı yazılımlara gereken önem verilmiyor. Eğer gerekli önlemler alınmazsa daha güçlü botnetlerin oluşacağını ve saldırıların etkisinin artacağını kolaylıkla söyleyebiliriz.

19. NATO Siber Koalisyon Tatbikatı – 2018

Siber savunma alanında kurum, kuruluş ya da ülkelere gerekli bilinçlendirme ve eğitimleri kazandırmada siber savunma tatbikatları çok önemli rol oynamaktadır. NATO tarafından düzenlenen Siber Koalisyon (Cyber Coalition) Tatbikatı 2008 yılının Kasım ayından bu yana her yıl yapılmaktadır. Tatbikat, NATO Siber Savunma Eylem Planı gereği Müttefik Dönüşüm Komutanlığı koordinatörlüğünde, üye ülkeler ve NATO'ya bağlı ilgili kurumların katılımıyla gerçekleşmektedir. İlk zamanlar Siber Savunma yetkinliği bulunan az sayıda ülkenin dâhil olduğu bu tatbikat, katılım sağlayan NATO üyesi ülkelerin ve partnerlerin yıldan yıla artmasıyla, günümüzde NATO'nun en geniş çaplı siber savunma organizasyonu haline gelmiştir.

Bu tatbikat ile şunlar hedeflenmektedir:

- Siber olaylara müdahale yetkinliği kapsamında stratejik seviyede karar verme süreçlerinin test edilmesi,
- Oynanan senaryolara bağlı olarak enjekte edilen zararlı yazılımlar ve oluşturabilecekleri tahribatla ilgili katılımcı ülkelerin teknik ve idari kabiliyetlerinin test edilmesi,
- Üye ülkeler ile NATO arasında, olası bir siber saldırı durumunda, bilgi paylaşımı ve iş birliği senkronizasyonunun artırılması.

Bu sene 27-29 Kasım 2018 tarihleri arasında 11'incisi düzenlenen tatbikat, 30 Kasımda yapılan faaliyet sonu incelemesiyle tamamlanmıştır. Tatbikatın icrası, ana

kontrol merkezi olarak belirlenen ve NATO Mükemmeliyet Merkezi (CCDCOE) olarak kurulan Estonya ve tatbikata katılan ülkelerin yerel kontrol merkezlerinde gerçekleşmiştir. NATO ve NATO dışı ortaklık ülkelerin katıldığı tatbikata Türkiye de katılım sağladı. Genelkurmay Başkanlığı ile Ulaştırma ve Altyapı Bakanlığına bağlı Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesindeki Ulusal Siber Olaylara Müdahale Merkezi (USOM) tatbikatın ulusal anlamdaki koordinasyonunun sağlanmasında aktif olarak yer aldılar. Tatbikat ulusal anlamda stratejik öneme sahip kamu ve özel sektör kuruluşlarından gelen siber güvenlik uzmanları ve TSK mensuplarından oluşan yaklaşık bir ekiple gerçekleştirildi.

Tatbikat, hayali olarak oluşturulan bir coğrafya ve ülkelerde cereyan eden senaryo üzerinden oluşturulmuştur. İnsani yardıma muhtaç, siber güvenlik yetkinliği zayıf dost bir ülke ile bölgenin teknolojisi ve ekonomisi güçlü, gelişmiş hasım ülkesi arasında geçen siber olaylar test edilmiştir. Bu kapsamda özellikle SCADA sistemleri gibi kritik altyapı tesislerine yapılan saldırılar ve NATO bilgi sistem ağına yapılan saldırılar simüle edilerek NATO'nun eş güdüm içindeki yetkinlikleri denenmiştir.

Farklı senaryoların işlendiği tatbikatta, her senaryo için siber güvenlik alanındaki çeşitli disiplinlere ait yetkinlikler test edilmeye ve geliştirilmeye çalışılmıştır.

Siber Koalisyon Tatbikatı, formatı gereği bir yarışmadan ziyade siber savunma alanında ulusal ve uluslararası ortamda farkındalık oluşturmayı amaçlamaktadır. Olası bir siber saldırı durumunda üye ülkelerin hızlı bir şekilde koordine olarak aksiyon almasını, zayıf noktalarını fark etmesini ve bu konuda geliştirici neler yapılabileceği hakkında bilgi edinilmesini sağlar. Düzenlenen bu tür tatbikatlar, siber güvenlik alanında çalışan insanların teorik bilgilerinin uygulamaya dökülmesi ve öğrenilenlerin akılda kalması açısından oldukça faydalıdır. Ayrıca, NATO Siber Savunma Mükemmeliyet Merkezi koordinasyonunda teknik yetkinliklerin ön plana çıktığı Kilitli Kalkan (Locked Shields) tatbikatı da teknik altyapısı ve senaryoları ile küresel basında da ses getirmektedir.

DÖNEM İNCELEME KONUSU

20. STM CTF'18

Çalışmalara Mayıs ayında başladık. Önce ne yapalım, nasıl yapalım toplantıları yaptık. Kaç soru hazırlayalım, ne soralım derken bu sene kaç takım alacağız konusuna geldi sıra. Malum her sene gittikçe artan sayıda takım alıyoruz. 2015'te 21 takım, 2016'da 26 takım, 2017'de 31 takım katılmıştı. Bu seneki planımız CTF'i 50 takımla gerçekleştirmekti ve yarışmaya olan ilgi her geçen sene daha da arttığı için başvuru sayısı da artmıştı. Geçen sene 100'e yakın takım arasından sadece 31 takım seçmemiz gerekmişti. Bu sene ise bu sorunu çözmemiz gerektiğini düşündük ve bırakalım yarışmacılar kendi kendilerini elesin dedik. Bu fikrin bir ürünü olarak CTF'i iki aşamalı yapmaya karar verdik. İlk aşama, 28-29 Eylül 2018'de 36 saat sürecek ve başvuru yapan tüm takımların katılabileceği online bir yarışma olacaktı. Dereceye giren ilk 45 takım ve STM yönetimi tarafından özel davetle çağrılacak 5 takım 31 Ekim 2018'de Ankara'da gerçekleşecek offline CTF'e katılmaya hak kazanacaktı. Ayrıca, ilk 10'a giren takımların yol masrafları da karşılanacaktı.

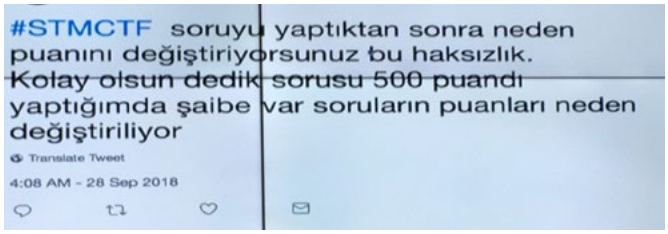
Kararlar alındı ve planlar yönetime anlatıldı. Yönetimin tam destek vermesiyle süreç başladı. Önümüzde 5 ay ve hazırlamamız gereken 2 CTF vardı.

20.1. STM CTF'18 Online Ön Eleme (28-29 Eylül 2018)

Ön eleme için birinci görevimiz 36 saat boyunca sistemi ayakta tutabileceğimiz bir altyapı hazırlamaktı. Bayrakların altyapısal yetersizlikler yüzünden girilmediği online CTF deneyimlerimiz olmuştu ve böyle bir problem istemiyorduk. Madem böyle bir işe girdik, kesinlikle her türlü testten geçecek bir altyapımız olmalıydı.

İkinci görevimiz ise 36 saate yayabileceğimiz yapıda sorular hazırlamaktı. Bu bağlamda 18 kişi ilk aşama için yaklaşık 40 soru, ikinci aşama içinse 30 soru hazırlayacaktı. "Acaba ben yarışmacı olsam bu soruyu görünce beğenir miyim?" kaygısıyla başlayan soru hazırlama süreci, sorunun başkaları tarafından kontrol edilmesi ve farklı şekillerde çözülmeye çalışılmasıyla, her ne kadar zorlu bir süreç gibi görünse de her zaman en çok eğlendiğimiz süreç olmuştur. Bu sene ekip olarak toplam 89 soru hazırladık. Çözülme sürelerine bağlı olarak soruları ilk aşama ve ikinci aşama için paylaştırdık.

Önceki senelerde soru puanları ekip tarafından belirleniyordu. Bazen sorunun çözümünü bildiğimiz için bize çok kolay gelen ve düşük puan verdiğimiz soruların (*bak*. 2017 senesi Nurella sorusu) kimse tarafından çözülemediği oluyordu. Bazen de hiç aklımıza gelmeyen veya bilmediğimiz bir yöntemle, bazen "strings"le sadece 30 saniyede bulunabilecek soruya kafamızdaki çözüm yolunun zor olması sebebiyle yüksek puan veriyorduk. Bu sene bırakalım sorular kendi puanını belirlesin dedik ve bir yandan da bayrak paylaşımı için de caydırıcı olduğunu düşündüğümüz, çözüldükçe değeri azalan soru şeklinde bir puanlama sistemi oluşturduk. Hali hazırda kullandığımız CTF paneli CTFd'nin Dynamic Value Challenge eklentisini kendi algoritmamıza göre değiştirip kullanmaya karar verdik. CTF sırasında — yarışmacılar tarafından başta anlaşılması zor olsa da — bir sorunun değeri soru çözüldükçe herkes için düşüyordu. Bu düşüş, soruyu hali hazırda çözenler için de geçerliydi. Online ön eleme ilk başladığında yaklaşık bir saat boyunca puanlarla ilgili sorulara cevap verdik.



Şekil 40: Çözüm sayısı artan soruların puan değerinin azalması yarışmacıları şaşırttı

Şekil 41: SOC odasındaki dev ekranlardan süreci takip ederken

Üçüncü ve son görevimiz ise bir teknik destek hizmeti sunmaktı. Bunun için bir IRC kanalı açmaya karar verdik. 36 saat boyunca bu kanalda yarışmacılara teknik destek hizmeti verdik. Kanal hiç boş kalmadı, sorularına cevap alamayan yarışmacı da olmadı.

Bütün bu görevler planlandıktan sonra testlere başladık. Altyapı hazırlıkları tümüyle Furkan'a bırakıldı. Furkan, hem panel kurulumunu hem de CTF'i en efektif ve sıkıntısız şekilde yapabileceğimiz konfigürasyon ayarlarını ve testlerini yaptı. Sunucular ve panel hazırlandıktan sonra Şeref ile Kürşat güvenlik ve yük testlerini yaptılar. Tüm testler bittiğinde altyapı olarak bir eksiğimiz görünmüyordu.

Sorular panele eklendikten sonra, hazırlayanlar tarafından birden fazla kere kontrol edildi. Kontrollerden sonra da ekip tarafından bir yarışmacı gibi tekrar çözüldü. Tüm ekip tek başına bir yarışmacı gibi panele girip tüm soruları çözdüğü için soru ve bayrakların kontrolünün kaç kere yapıldığını saymayı artık bırakmıştık. Hazırlık boyunca sorularda yapılan en küçük bir değişiklik bile sorunun kontrol ve çözüm sürecini tekrar etmemize neden oluyordu.

Sistem ve soruların hazır olmasıyla artık biz de hazırdık. Kayıt olan takım sayısı 129 olmuştu. Yarışmayı, herkes katılabilsin diye cuma ve cumartesi olarak iki güne yaymaya karar vermiştik. İlk defa online bir yarışma yapacaktık. Bu yüzden her ne kadar sistemi testten geçirsek ve güvenlik önlemlerimizi almış olsak da kesinlikle yarışma başlangıcında saldırıya uğrayacak gibi hareket ediyorduk. 28 Eylül Cuma saat 11:00'de yarışma başladı. Ön eleme sürecini Siber Füzyon Merkezi (SFM) bünyesindeki SOC (Security Operations Center)'deki dev ekranlardan yönetmek tüm süreci an ve an takip etme konusunda oldukça faydalı oldu. Tüm CTF ekibi, SOC'da toplanmış ve büyük ekranlardan durumu izlemeye başlamıştık, bir yanda SFM bünyesindeki çalışmalar sürerken diğer yanda CTF sürecinin yönetimi tek merkezden devam ediyordu ve heyecan doruktaydı. İlk saatimiz yarışmacıların soruları dışında problemsiz geçti. SOC'da süreci ekranlardan takip ettiğimiz süre içinde hem IRC kanalında hem de Twitter'da sürekli aktiftik ve SFM bünyesindeki ekip arkadaşlarımız ile birlikte hiç uyumadık.

Gecenin ilerleyen saatlerinde artık hem uyanık kalan yarışmacı sayısı azalmıştı, hem de bizim enerjiye ihtiyacımız vardı. Bu sırada hâlâ soru açmaya da devam ediyorduk ve SFM'deki çalışmalar devam ediyordu. 36 saat boyunca hiç ara vermeden belirli aralıklarla soru açtık. Elimizde 40'a yakın soru vardı ve bunları 36 saate yayacak şekilde setlere bölerek sıralamaya koymuştuk. Soruların çözülme sıklığına göre soru setleri açıyorduk. 36 saatlik yarışma esnasında, "Şöyle bir soru da olsa güzel olurdu" diyerek Kürşat, Sinan, Mert Can, Anıl ve Furkan ekstra sorular bile hazırladılar.

Normalde CTF ekibi dönüşümlü olarak kalacaktı, ama biz bu süreçte eğlendiğimiz için neredeyse gece 02:00'ye kadar bütün ekip ayaktaydık. Sonra CTF ekibi yavaş yavaş nöbetleşe çalışmaya başladı. Ama altyapıdan sorumlu olan arkadaşlar gerçekten 36 saat boyunca hiç "uyumadan" ayakta kaldılar.

Biz uyumayınca yarışmacıları da uyutmadık tabii. Onlar da bir yandan dinlenmek istiyorlar bir yandan da soruları bırakamıyorlardı.

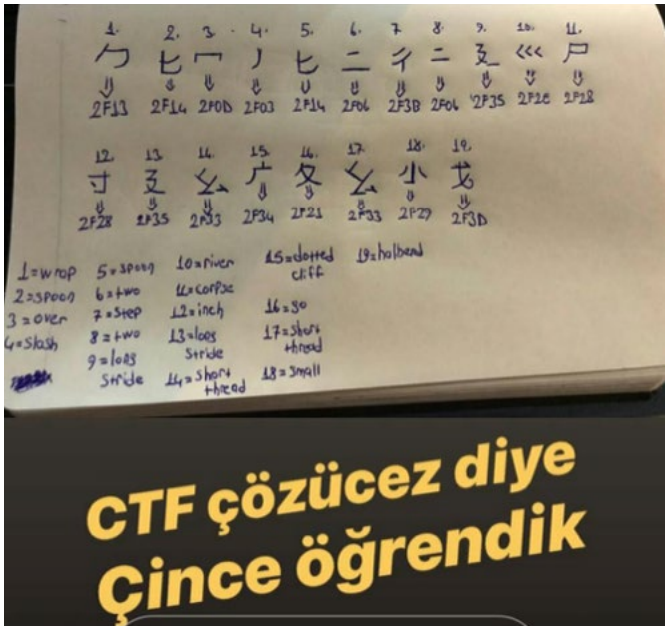
```
01:37] <iv3m> cidden sorular yeni bitti
01:37] <iv3m> uyku arasi
01:37] <pr0logueq> olm hiç uyumuyormusunuz
01:37] <d1scharg3d> yok mu soyle iz surmeli adam kovalamali
01:38] <lvmbdv> https://www.youtube.com/watch?v=dGS6G9nu3_c
01:38] <d1scharg3d> ya da simetrik sifreleme sorun da keyiflenelim
01:38] <lvmbdv> sleep is for those who are broke
01:39] <@_nl_> bizlere uyku yok
01:39] <@pennylaneparker> biz burda bi iz sürüyoruz ki sormayın :))
01:39] <@pennylaneparker> ya siz de ne uykucu çıktınız
01:40] <@_nl_> Yeni Mobile sorusu geldi.
01:40] <iv3m> uykucu cikmadik ki
01:40] <pr0logueq> 11den beri başındayız
01:40] <d1scharg3d> begendim ama ekibin performansini
01:40] <iv3m> derste cozuyorduk
01:40] <pr0logueq> derse girmedim
01:40] <iv3m> evdeyim hala cozuyok
```

Şekil 42: IRC kanalında geçen diyaloglar

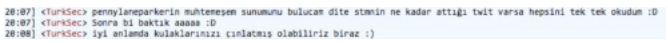
```
[23:14] <numan> sysadmine
[23:14] <numan> selamlar
[23:14] <numan> adam uyumadı
[23:14] <@TUFAN> sysadmin kral :)
[23:14] <GoF> iyi geceler hepinize
[23:15] <numan> iyi geceller
[23:15] <numan> rahatlıka uyuyabiliriz artık
[23:15] <GoF> Takim tasimak nedir bugun anladim
```

Şekil 43: IRC kanalında geçen diyaloglar

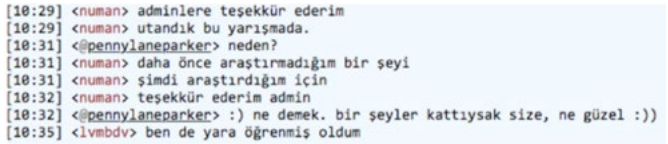
Cuma gününe göre daha sakin bir cumartesi geçirdik. STM'deki dinlenme alanına inip langırt turnuvası bile yaptık. Yarışmacılar da açılan soru setlerinden soru tiplerine aşina hale gelmişti ve daha az soru geliyordu. Hem Twitter'dan hem de IRC'den paylaştıklarından anladığımız kadarıyla bayrağa ulaşmak için her yolu deniyorlardı. Yarışmacıların birçoğu hem soruyu çözmeye uğraşıyor, hem yeni bir şeyler öğrenebilmek için boğuşuyor, en önemlisi de bunu eğlenerek yapıyordu.



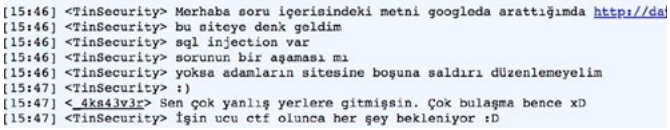
Şekil 44: Takımlardan gelen mesajlar



Şekil 45: IRC kanalında geçen diyaloglar



Şekil 46: IRC kanalında geçen diyaloglar



Şekil 47: Bazı yarışmacılar çok ince düşünüp yarışma dışında olan platformlarda zafiyet keşfettiler

CTF'in sonuna yaklaştığımızda bir yandan sorulara cevap veriyor, bir yandan da son incelemelerimizi yapıyorduk. İşin ucunda para ödülü olunca ve yarışma online olunca olabilecek her türlü haksızlığa karşı elimizden geleni yapmamız gerektiğine inanıyorduk. Kimsenin hakkını yemek istemediğimiz için yapılan paylaşımlardan ve yardımlaşmalardan tam olarak emin olmadan kimseye bir şey söylemedik. Bizim için CTF'in son 1-2 saati resmen Şekil 49'daki gibi geçti :). İncelemeler sonucunda 120 takımdan 2 takımı elemek durumunda kaldık. CTF sonucunda katılan 120 takımdan ilk 45'i Ankara'da gerçekleşecek final yarışmasına katılmaya hak kazandı.

CTF bittiğinde yorgun ama mutluyduk. Yarışmacılardan gelen dönüşler olumluydu. Ekip güzeldi, CTF güzeldi ve yarışmacılar güzeldi. Kısacası problemsiz ve eğlenceli bir ön elemeyi arkamızda bırakmıştık.

Sıra Ankara'da gerçekleşecek final yarışmasındaydı.

Şekil 48: Ön eleme sonrasında finaldeki yarışmacıları bekleyen ekibimiz

20.2. STM CTF'18 Final (31 Ekim 2018)

Online ön elemeyi problemsiz ve eğlenceli bir şekilde atlattıktan sonra sıra Ankara'da gerçekleşecek olan final yarışmasına gelmişti.

İlk önce dereceye giren 45 takımla iletişime geçilerek katılım onayları alındı. STM yönetimi tarafından belirlenen 5 takıma özel davet gönderildi. 50 takımın da katılım onayları alındıktan sonra sıra bizim tarafta yapılacak hazırlıklara gelmişti. Sorularımız hazırdı. Sadece altyapıyı kurmamız, yarışma boyunca kullanacağımız video ve müzikleri hazırlamamız gerekiyordu. Altyapı kurulumunu Furkan, Sinan, Sedat, Ahmet ve Yunus üstlenirken video ile müzikleri Anıl ve Mert Can üstlendi.

Hazırlıklar için bütün ekip olarak 29 Ekim'de yarışmanın gerçekleşeceği Sheraton Otele gittik. İki gün boyunca kablo çektik. Firewall ve switchlerin testlerini yaptık.

Sırayla bütün takımların giriş bilgilerini oluşturup test ettik. Hatların kontrolü, yük testi, panel kontrolü, soruların son kontrolleri derken yarışma sabahı geldi çattı.

Şekil 49: Final yarışması açılış konuşması için hazırlıklar tamamlanırken

Kayıt masası sabah saat 08:00 itibariyle açılmıştı. Takımı tam olarak gelen tüm yarışmacıları salona almaya başladık. Yarışmanın 10.00'da başlayıp 18.00'da tamamlanması planlanmıştı. Takım olarak içeri girenlerin takım bilgisayarlarını masada bulunan switchlere bağlayıp "Hoş geldin" sorusunu çözmesini bekliyorduk, çünkü yarışma başlamadan önce yaşanabilecek olası bağlantı sorunlarını çözmek ve yarışma başladığında olabildiğince az sorunla karşılaşmak istiyorduk.

Şekil 50: Yarışmacılar "Hoşgeldin" ve ısınma soru setini çözerken

Resmi olarak yarışma başlamamıştı ama puan tablosu ilk puanlarını alan yarışmacı takımların isimleriyle dolmaya başlamıştı. Bu sürece paralel olarak saat 09:30 itibariyle sahnedeki konuşmalar başladı. Biz de bu sırada ısınma soru setini açmıştık. Konuşmalar bittikten ve yarışma kuralları anlatıldıktan sonra saat 10:00 itibariyle, geçen sene de olduğu gibi, ilk olarak bir tane soru açtık. Bu sene ilk seçtiğimiz soru "MALWARE" kategorisindeki, çalıştırılınca "BSOD" veren "Çok mu Çok Maviyiz" sorusuydu. Bu sene de gelenek bozulmadı ve bu ilk soru sadece bir takım tarafından çözülebildi.

Tüm destek ekibi masalar arasında dolaşıp sorun yaşayan takımlarla görüşüyordu. Admin masasında sunucuların yük durumları kontrol ediliyordu ve her şey yolundaydı. Soruları açmaya başlayabilirdik. Yarışma resmi olarak başlamıştı.

Şekil 51: Yarışma boyunca ekip gelecek olan tüm sorulara destek için hazırdı

Yarışmacılar online ön elemeden geçerek geldikleri için panel ve soru tiplerine aşinaydılar. Ayrıca, takımlar ön elemeyle geldikleri için geçen senelere göre daha bilinçli ekiplerle karşı karşıyaydık ve daha az soruyla karşılaşıyorduk.

Şekil 52: Takımlar soruları çözerken

Şekil 53: Takımlar soruları çözerken

CTF yarışmalarını izlemek keyiflidir, fakat yarışmacı değilseniz bu keyif kısa sürer. Bu sene de geçen seneki quiz etkinliğini devam ettirdik. Yarışma günü quiz için 100'ün üzerinde soru hazırladık. Her saat başı izleyicilerin bulunduğu salonda ekrandan "Bilişim Dünyası" ağırlıklı sorularla alternatif yarışma alanı oluşturduk. Sorulara doğru ve en hızlı cevap veren yarışmacılar ufak ödüller kazandılar. Kahoot uygulaması üzerinden gerçekleştirdiğimiz quiz yarışmasında izleyiciler cep telefonlarıyla yarışmaya katılıyordu. Yarışma alanında bulunan dev ekranda beliren sorulara cep telefonundan en hızlı ve doğru cevabı vermek için çekişmeli anlar yaşandı.

Şekil 54: Saat başı gerçekleşen quiz yarışmasında izleyiciler ödül için yarıştı

CTF yarışmasının tamamlanmasına 30 dakika kala puan tablosunu dondurduk. Yarışmacı takımlar soru çözmeye devam edip puan kazanabiliyorlardı ama güncel puanlarını ve sıralamadaki yerlerini göremiyorlardı. Herkesi tam bir heyecan sarmıştı. Son 30 dakika içinde kapanan puan tablosuyla bayrak saklayan takımlar da bayrak girişlerini yapmaya başladı. Son 5 dakika içinde bazı takımlar ataklar gerçekleştirerek pek çok soruyu çözdüler. Yarışma bittiğinde sahnede konuşmalar yapılırken ilk 3'e giren takımların isimlerini zarflara yazıp açıklanması için teslim ettik.

Online ön elemedeki birincilik değişmedi ve Lorem Checksum takımı birinci oldu.

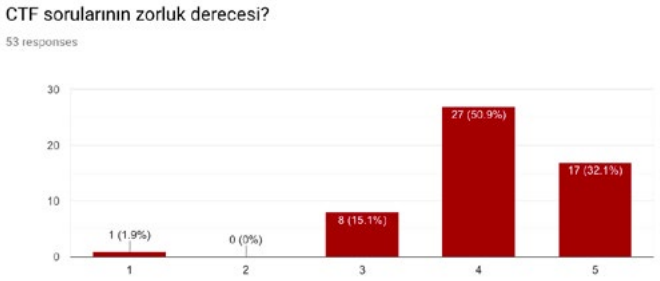
Şekil 55: Birinci olan "LoremChecksum" takımı ödülünü Genel Müdürümüz Sn. Murat İKİNCİ'den alırken

Geçen seneden farklı olarak bu sene dereceye giremeyen 3 yarışmacıya iPad, 10 yarışmacıya da hediye çeki ödülü verdik. Kura sırasında ekip olarak sahneye çıktık ve kazanan yarışmacılara hediyelerini takdim ettik.

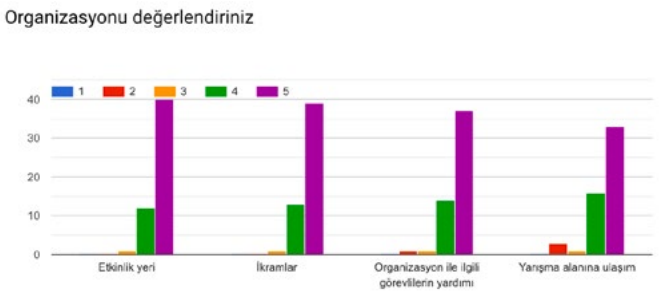
Yarışmanın son 30 dakikası kapalı kalan skor tablosunun yarışma bitimindeki halini aşağıda görebilirsiniz.

Şekil 56: Son 30 dakikada kapalı olan skor tablosu

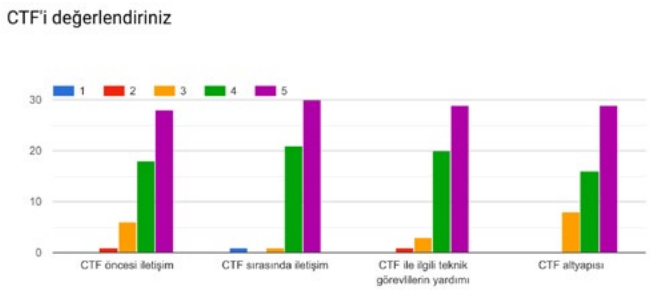
Yarışmacıların yarışma konusunda doldurduğu anket için teşekkür ederiz. Anket sonuçlarını aşağıda bulabilirsiniz.



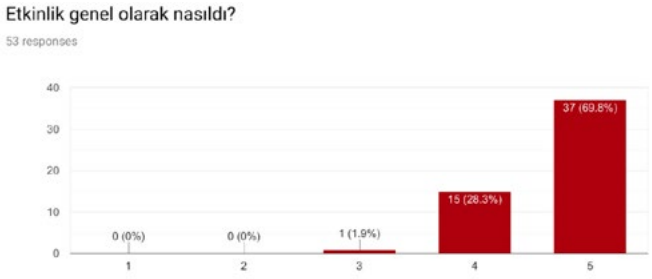
Şekil 57: CTF anket sonuçları



Şekil 58: CTF anket sonuçları



Şekil 59: CTF anket sonuçları



Şekil 60: CTF anket sonuçları

120 takım 464 yarışmacı ile başladığımız STMCTF'18, online ön eleme aşamasından sonra finale kalan 50 takım 190 yarışmacı ile son buldu. CTF altyapısını ve sorularını 20 kişilik bir ekip hazırladı.

Belirtmek isteriz ki, büyük başarılar ancak uyumlu bir ekip çalışmasıyla kazanılabilir. Seneye daha güzel bir organizasyonda görüşmek üzere.

Şekil 61: STM CTF'18 Ekibi

REFERANSLAR

[1] Özcan T. (2018). "A Hybrid Multi-Criteria Desicion Making Approach for New Destination Selection in Aviation Industry." *Alphanumeric Journal*, 6(1), DOI: 10.17093/alphanumeric.369758

[2] Weise, E. (2015). Computer expert hacked into plane and made it briefly fly sideways, according to FBI. https://www.independent.co.uk/ news/world/americas/computer-expert-hacks-into-plane-and-makes-it-fly-sideways-accord ing-to-fbi-10256145.html [Erişim Tarihi: 08.12.2018]

[3] Gualino M. (2017). "Cybersecurity from an aviation security perspective". Deputy Director - ICAO Aviation Security Training Center. https://ww w.euroco ntrol.int/sites /default/files/events/presentation/art-workshop-atm-security-and-cybersecurity-5-gualino.pdf [Erişim Tarihi: 20.11.2018]

[4] Korosec, K. (2018). "Data breach exposes trade secrets of carmakers GM, Ford, Tesla, Toyota." *Tech Crunch,* https://techcrunch.com/2018/ 07/20/data-breach-level-one-automakers/ [Erişim Tarihi: 09.12.2018]

[5] Khandelwal, S. (2018). "Windows 10 Bug Let UWP Apps Access All Files Without Users' Consent", The Hacker News https://thehackernews.com/ 2018/10/windows10-uwp-apps.html [Erişim Tarihi: 20.12.2018]

[6] Kumar, M. (2018). "Unpatched MS Word Flaw Could Allow Hackers to Infect Your Computer", https://thehackernews.com/2018/10/microsoft-office-online-video.html [Erişim Tarihi: 18.12.2018]

[7] Ben-Yossef, A. (2018). "Abusing Microsoft Office Online Video", Blog Cymulate, https://blog.cymulate.com/abusing-microsoft-office-online-video [Erişim Tarihi: 15.12.2018]

[8] Facebook Security Update (2018). Facebook News Room https://newsroom.fb.com/news/2018 /09/security-update/ [Erişim Tarihi: 14.12.2018]

[9] Facebook Login Update (2018). Facebook News Room, https:// newsroom.fb. com/ news/2018/10/facebook-login-update/ [Erişim Tarihi: 13.12.2018]

[10] Facebook Update On Security İssue (2018). Facebook News Room, https://newsroom.fb.com/news/2018/10/update-on-security-issue/ [Erişim Tarihi: 13.12.2018]

[11] Armis Labs (2018). "BleedingBit Information from the Research Team" https://armis.com/bleedingbit/ [Erişim Tarihi: 13.12.2018]

[12] Altıner, M. ve Çakır F. (2017) "Siber uzay ve uluslararası ilişkiler teorisi". http://dergipark.gov.tr/download/article-file/418767 [Erişim Tarihi 28.11.2018]

[13] Ermiş, U. (2018). "Bir güvenlik sorunu olarak siber uzay." http://www.ta sam.org/tr-TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay [Erişim Tarihi 25.11.2018]

[14] Güntay, Vahit (2017), "Siber Uzay ve Güvenlik Politikası Üzerine Teorik Bir Yaklaşım", Siber Politikalar Dergisi, ISSN:2587-1218, Sf: 9

[15] Rex B. H. (2008). "NATO and Global Cyber Defence", Romanya Dışişleri Bakanlığı Bükreş Konferansı Sonuç Bildirisi, Mayıs 2008

[16] Siber Füzyon Merkezi, https://www.stm.com.tr/tr/urunler/siber-fuzyon-merkezi [Erişim Tarihi: 24.12.2018]

[17] Cyber Fusion Center, Next-Gen facility, https://www.maryville.edu/bu/cybersecurity/cyber-fusion-center [Erişim Tarihi: 20.12.2018]

[18] SputnikNews (2018). ABD'den 'Sony'yi hackleyen' Kuzey Koreli bilgisayar programcısına yaptırım", https://tr.sputniknews.com/abd/2018090610350835 95-abd-sony-hack-kuzey-koreli-bilgisayar-programcisina-yaptirim/ [Erişim Tarihi: 25.12.2018]

[19] Eggerton, J. (2014). "McCaul: Sony Move Empowers Cyber Hackers", Broadcastingcable, https://www.broadcastingcable.com/news/mccaul-sony-move-empowers-cyber-hackers-136525 [Erişim Tarihi: 05.12.2018]

[20] N. Granado and G. White (2008). "Cyber Security and Government Fusion Centers," Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, 2008, pp. 205-205.

[21] Kumar, M. (2018). "Windows Built-in Antivirus Gets Secure Sandbox Mode – Turn It ON" The Hacker News, https://thehackernews.com/2018/10/windows-defender-antivirus-sandbox.html [Erişim Tarihi: 24.12.2018]

[22] Cloudblogs | Microsoft Secure (2018). "Windows Defender Antivirus can now run in a sandbox". https://cloudblogs.microsoft.com/microsoftsecure/2018/10/26/windows-defender-antivirus-can-now-run-in-a-sandbox/ [Erişim Tarihi: 28.12.2018]

[23] Ryan G. (2018). "Whitepaper: Bypassing Port Security In 2018 – Defeating MACsec and 802.1x-2010", DEFCON 26, https://www.digitalsilence.com/wp-content/uploads/2018/08/DEF-CON-26-Gabriel-Ryan-Whitepaper-Bypassing-Port-Security-In-2018-Defeating-MacSEC-and-802.1x-2010.pdf [Erişim Tarihi: 20.12.2018]

[24] McGrew, W. (2018). "An Attacker Looks at Docker: Approaching Multi-Container Applications" DEFCON 26, https://defcon.org/html/defcon-26/dc-26-speakers.html#McGrew [Erişim Tarihi: 15.12.2018]

[25] Official Docker Samples, "Docker Samples: example-voting-app" GitHub, https://github.com/dockersamples/example-voting-app [Erişim Tarihi: 01.12.2018]

[26] Newman, L. H. (2018). Machine Learning Can Create Fake 'Master Key' Fingerprints. https://www.wired.com/story/deep-masterprints-fake-finger prints-machine-learning/ [Erişim Tarihi: 25.11.2018]

[27] Dameff, C., Tully, J., ve Bland, M. (2018). "Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives" BlackHat USA 2018, https://www.blac khat.com/us-18/briefings/schedule/#pestilential-protocol-how-unsecure-hl7-messages-threaten-patient-lives-11726 [Erişim Tarihi: 22.12.2018]

[28] Nie, S., Liu, L., Du, Y., ve Zhang, W., (2018). "Over-The-Aır: How We Remotely Compromısed The Gateway, Bcm, And Autopılot Ecus Of Tesla Cars" BlackHat USA 2018, https://i.blackhat.com/us-18/Thu-August-9/us-18-Liu-Over-The-Air-How-We-Remotely-Compromised-The-Gateway-Bcm-And-Autopilot-Ecus-Of-Tesla-Cars-wp.pdf [Erişim Tarihi: 22.12.2018]

[29] Cisco Whitepaper (2011). "The Internet of Things How the Next Evolution of the Internet Is Changing Everything" Cisco, https://www.cisc o.com/c/dam/en_us/ about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Erişim Tarihi: 18.11.2018]

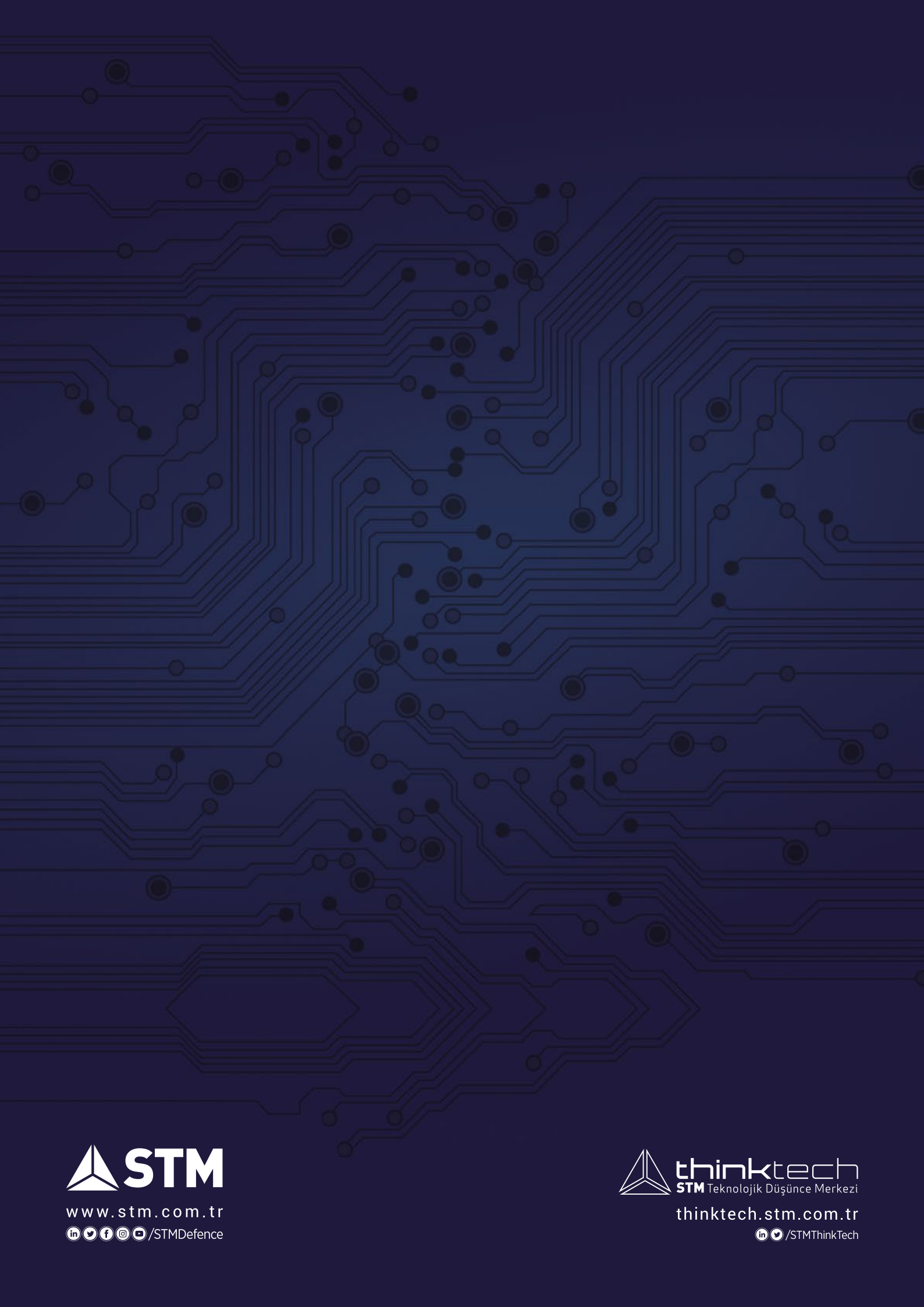
[30] Costin, A. ve Zaddach J., (2018). "IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies" BlackHat USA 2018, https://i.blackhat.com/us-18/Thu-August-9/us-18-Costin-Zaddach-IoT-Malware-Comprehensive-Survey-Analysis-Frame work-and-Case-Studies -wp.pdf [Erişim Tarihi: 24.12.2018]

[31] Kaspersky Labs (2018). "New IoT-malware grew three-fold in H1 2018", https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018[ErişimTarihi:24.12.2018]

[32] Statista (2017). Cyber crime attacks experienced by global companies 2017 | Statistic. https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/ [Erişim Tarihi: 26.11.2018]

[33] Marville University (2017). Cyber Fusion Center, https://www.maryville.edu/mpress/cyber-fusion-center-provides-major-opportunities/maryville-universitys-cyber-fusion-center-on-august-24-2016-2/ [Erişim Tarihi: 16.12.2018]

[34] Maglia B. (2017). Tesla Model X Lightshow [Video], https://youtube.com/watch?v=-jyPkg0yXzM [Erişim Tarihi: 15.11.2018]



STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech