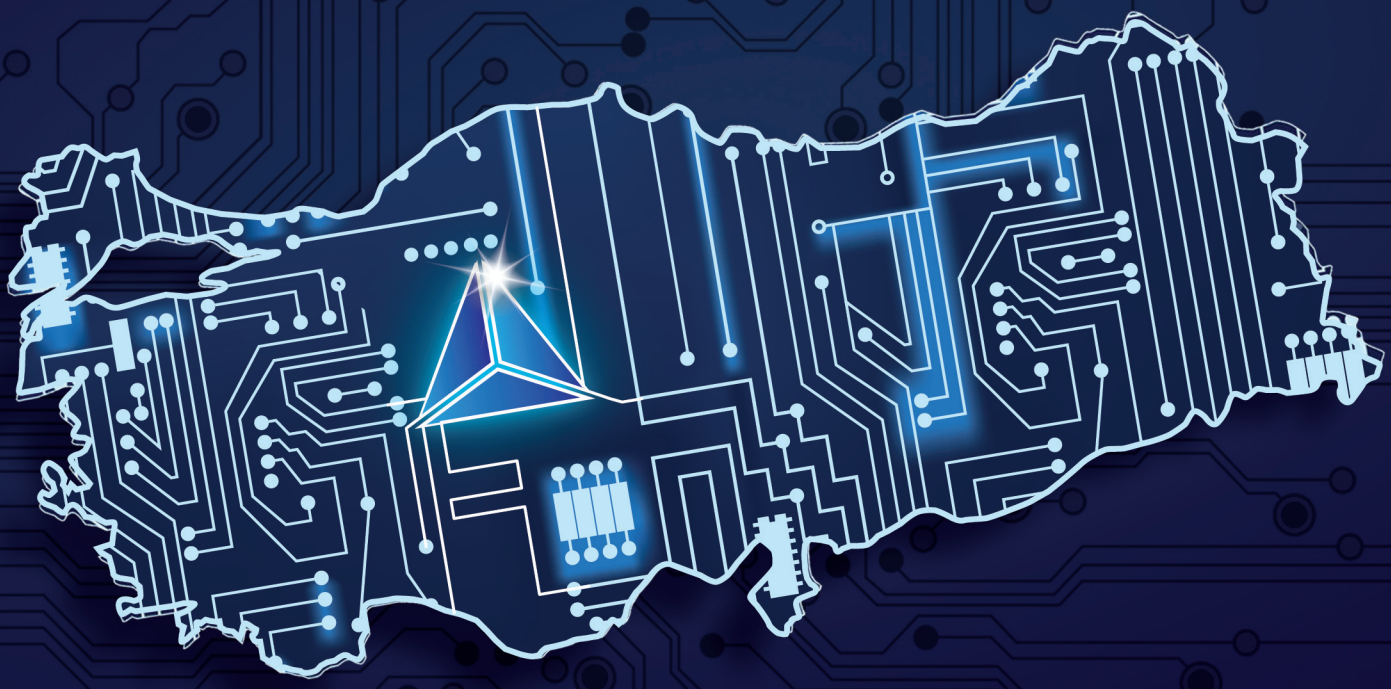
2017 EKİM-ARALIK DÖNEMİ SİBER TEHDİT DURUM RAPORU



STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK

İÇİNDEKİLER

SORUMSUZLUK VE FİKRİ MÜLKİYET HAKKI BEYANI

İşbu eserde/internet sitesinde yer alan veriler/bilgiler ticari amaçlı olmayıp tamamen kamuyu bilgilendirmek amacıyla yayımlanan içeriklerdir. Bu eser/internet sitesinde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde/internet sitesinde sunulan verilerin/bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde/internet sitesinde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir.

Bu eserde/internet sitesinde yer alan bilgilerin her türlü hakkı STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'ye ve/veya eserde atıf yapılan kişi ve kurumlara aittir. Yazılı izin olmaksızın eserde/internet sitesinde yer alan bilgi, yazı, ifadenin bir kısmı veya tamamı, herhangi bir ortamda hiçbir şekilde yayımlanamaz, çoğaltılamaz, işlenemez.

Giriş

Bir yılı daha siber tehditler ve bu tehditlerden kaynaklı siber olaylarla birlikte geride bıraktık. 2017 yılının ilk aşamada özellikle Equifax ve Verizon firmalarında yaşanan büyük çaplı veri sızıntıları, küresel olarak etkili olan WannaCry gibi, ExPetr gibi nihai hedeflerinin birer sır olarak kaldığı, aniden gelişen ve perde arkasında iş dünyasını hedefleyen güçlü aktörlerin olduğu fidye yazılımları ile hatırlanacağını söyleyebiliriz.

2018 yılında da devletler, şirketler, kamu kurumları ve hatta politik kampanyaların siber tehditlere maruz kalacağı aşikâr görünüyor.

2017 yılının siber tehditler yönüyle genel bir değerlendirmesi ile 2018 yılına ait beklentilerden oluşan bilgileri raporumuzun giriş kısmında bulabilirsiniz.

Bu dönemki raporumuzda 2017 Ekim ayında üçüncüsünü gerçekleştirdiğimiz ve artık geleneksel hale gelen Capture The Flag yarışmasının perde arkasında yaşananlara değindiğimiz özel bir eke yer verdik. Bu nedenle aslında bu dönem raporumuzda inceleme konusu olarak yer vermeyi planladığımız yapay zekânın siber güvenlikte her geçen gün artan rolünü ele aldığımız makalemize de bir sonraki raporumuzda yer vereceğiz.

2018 yılında hepimiz için siber tehditlerin azalması, ancak siber tehditlere karşı farkındalığımızın artması dileklerimizle...

2017 Yılı Siber Tehdit Değerlendirmemiz

2016 Ekim-Aralık Dönemi Türkiye Siber Tehdit Durum Raporu'nda 2017 yılı için küresel ölçekte ön plana çıkmasını beklediğimiz siber **saldırı trendleri olarak**;

- IoT platformlarının da kullanılacağı DDoS saldırılarına,
- Çeşitli yöntemlerin deneneceği fidye yazılımlarına,
- Mobil cihazlara yönelik tehditlere,
- Endüstriyel Kontrol Sistemlerine (EKS) ve özellikle de bu tür sistemleri bünyesinde yoğun olarak barındıran enerji dağıtım sistemlerine yönelik saldırı girişimlerine,
- Kurum içi yazışmalara ve süreçlere sızma suretiyle yaşanacak siber olaylara,
- Kapalı sistemlerden (kapalı ağlar, cihazlar vb.) veri çalmaya yönelik teşebbüslere dikkat çekmiştik.

STM olarak 2017 yılında üçer aylık dönemlerde yayımladığımız tehdit durum raporlarında dikkatlerinize sunduğumuz konulara baktığımızda, yukarıda belirttiğimiz trendlere uyumlu olarak dünya genelinde gerçekten de **fidye** yazılımlarında gözle görülür bir artış olduğunu gözlemledik. **Wannacry**, **NotPetya**, **Retefe** ve **Bad Rabbit** bu türde ses getiren haberlerin başlıkları oldu. 2017'de siber suç pazarında CaaS (Crime-as-a-service) suç menüsü altında **Ransomware-as-a-Service**'in oldukça aktif olduğu görülmesi fidye yazılımlarına ait tehdidin boyutlarını göstermesi açısından önemliydi.

Bilindiği gibi 2016 Ağustos ayında dünyayı sarsan siber olay, National Security Agency (NSA) tarafından Equation Group ile beraber geliştirilen casus araçların Shadow Brokers siber korsan grubu tarafından sızdırılmasıydı. Shadow Brokers'ın en etkili icraatı 2017 Nisan ayında geldi. **EternalBlue** olarak adlandırılan ve daha sonra hem WannaCry hem de NotPetya fidye yazılımı saldırılarında kullanılacak olan Windows açıklığı ve NSA'in diğer yazılım aracı havuzu ortaya çıkarıldı. Bu araçlar ve açıklıklar, siber güvenliğin yasa dışı ortamı Dark Web'de açık arttırmaya sunuldu. Daha sonra WannaCry ile dünya genelinde birçok ülkede kamu hizmetleri ve büyük kurumların bilgi teknolojileri hizmetleri sekteye uğratıldı.

WannaCry dünya siyasetinde de etkisini gösterdi. Kuzey Kore ile ABD arasındaki politik gerilimin artmasının ardından Beyaz Saray'ın WannaCry siber saldırısının arkasında Kuzey Kore'nin olduğunu açıklayarak suçlaması

ve ardından Kuzey Kore'nin suçlamayı yalanlaması, siber saldırıların giderek dünya siyasetinde argüman olarak kullanılacağının sinyallerini vermesi bakımından önemli haberler arasında yerini aldı. Daha da önemlisi ABD'nin birkaç devlet kurumunda Kaspersky firmasına ait yazılımların kullanımını yasaklaması ve yeni siber güvenlik stratejisinde siber güvenliğin daha belirgin bir şekilde vurgulanması, konunun sadece argüman olarak kullanılmadığını ve ülke stratejilerinde tekrar tekrar güncellenen ciddi bir konu olduğunu da gösterdi.

İngiltere Dış İşleri Bakanı'nın, Rusya Devlet Başkanı Putin'i yapacakları siber saldırılara karşı koyacakları yönünde uyarması ve bu alanda iyi olduklarını, Batı demokrasilerinin seçim sonuçlarına nüfuz edecek herhangi siber saldırıya karşı hazırlıklı olduklarını ve ülkesinin Government Communications Headquarters (GCHQ) istihbarat kurumunun bu yönde saldırılara karşı koyacak son teknoloji araçları olduğunu belirtmesi de yine dünya siyasetinde ve devletler nezdinde siber güvenliğin önemini gösterdi.

2016'daki bir başka fidye yazılımı saldırısı olan Petya, bu kez 2017'de benzer özellikler gösteren **NotPetya** olarak karşımıza çıktı ve büyük firmaları etkiledi. ABD bazlı ilaç sanayi sektöründen Merck, Danimarka kargo şirketi Maersk ve Rusya petrol devi Rosneft etkilenenlerden bazılarıydı.

Aynı saldırı Ukrayna altyapı sistemlerinde daha büyük etkiler yaptı. Ukrayna'daki enerji şirketleri, havaalanı, toplu taşıma ve ülkenin merkez bankası bundan etkilendi.

Yılın son çeyreğinde **Bad Rabbit** fidye yazılımı ile hedeflenen kurbanların çoğu Rusya'daydı; ancak Ukrayna, Türkiye ve Almanya da bu saldırıdan etkilendiler.

2017 aynı zamanda birçok **veri ihlâli** olayının da gerçekleştiği bir yıl oldu.

Hindistan'ın en büyük restoran arama motoru **Zomato** siber saldırıya uğradı. Buraya kayıtlı 17 milyon kullanıcının bilgileri Dark Web'de satışa çıkarıldı. Kredi kartı bilgilerini ayrı bir yerde tutan firma finansal bir kayıp ya da kullanıcı mağduriyeti yaşamadığı için şanslıydı.

Finans sektöründe yer alan **Equifax** kredi raporlama kuruluşunun başından geçen güvenlik olayı, ABD tarihinin en büyük veri sızıntısı olarak tüm dünya basınına yansıdı. Mevcut bir yazılımın yamasının zamanında uygulanmaması sonucu bilgisayar korsanlarının bu zafiyetten faydalanmasıyla 145 milyon Amerikalının kişisel verisi (sosyal güvenlik numarası, doğum tarihi, kredi kartı vb.) sızdı. Bu vaka tüm dünyada yılın en önemli siber güvenlik olaylarından biri olarak büyük yankı uyandırdı.

Bir başka veri sızıntısı olayında ise ilginç gelişmeler yaşandı. **Uber**'in 2016 son çeyreğinde başına gelen siber saldırı neticesinde uygulamaya kayıtlı 600.000 sürücünün ve 57 milyon kullanıcının adı, e-posta adresi, seyahatlerin güzergâh verisi sızdırıldı. Uber'in bu olayı hemen duyurmak yerine bilgisayar korsanlarıyla anlaşma yoluna giderek 100.000 ABD doları ödeme karşılığı verilerin silinmesi ve bu olayın üzerinin kapatılmasını istemesi büyük tepki çekti. Bu olay da saldırganların milyon dolarlarca bütçeye sahip olan şirketleri gündeme bir anda kötü bir şekilde getirmesine ve müşterilerinin önünde itibarını zedelemesine örnek bir olay olarak tarihteki yerini aldı.

Android uygulama pazarı Google Play'de sahte Whatsapp uygulamasının 1 milyon kez indirilmesi ve MacOS High Sierra işletim sisteminde **bir Türk geliştirici** tarafından bulunan açıklık, mobil siber güvenlik alanında öne çıkan olaylardı.

Bu yıl ülkemizde **endüstriyel kontrol sistemlerine** yönelik siber saldırılarda bir hareketliliğin görülmesi de dikkat çeken bir gelişme oldu. Farklı isimlerle tanınan siber korsan grubu **Dragonfly/Energetic Bear**'ın, Türkiye'deki bir

enerji grubunun web sitesinde, bu siteye bağlanabilecek iş birliği yapılan kurumları/şirketleri de etkileyen bir düzenek kurduğu tespit edildi. Hedefte olanlar kritik altyapı sektöründe çalışanlardı.

Son çeyrekte gerçekleşen ve ağırlıklı olarak ülkemizle beraber Rusya'yı etkileyen başka bir olay ise siber korsan grubu **Cobalt**'ın finansal kurumları hedef alması ve e-postalara zararlı kod içeren ek koyarak oltalama saldırısı düzenlemesiydi. Ülkemiz ve Rusya dışında ABD, İtalya, Avusturya, Ukrayna, Ürdün, Kuveyt ve Çek Cumhuriyeti de saldırıdan etkilenen ülkeler arasında yer aldı.

Sonuç olarak 2017 yılında;

Siber tehditler arasında gittikçe yaygınlaşan fidye yazılımlarının farklı uygulamalarla ortaya çıktığını, bankacılık ve finans sistemlerine yönelik saldırılar ile mobil teknolojilere yönelik saldırıların arttığını ve veri ihlallerinin oluşturduğu tehditlerin ön planda olduğunu görüyoruz.

Siber güvenlik saldırıları küçük ve orta ölçekli şirketlerin korkulu rüyası olmaya devam ediyor. Şirketlerin verilerini korumak için siber güvenlik alanına yatırım yapması gerektiği, gerekli tedbirler alınmadığı takdirde büyük ölçekli şirketlerin bile siber tehditler karşısında aciz durumlara düştükleri bu yıl yaşanan siber olaylar sonucunda bir kez daha ortaya çıktı; ancak yatırımların yalnızca teknoloji bazlı olarak donanım ve yazılıma değil, bunları işletecek **insan kaynağının eğitilmesi** ve siber güvenliğin sağlanmasına yönelik **kurumsal süreçlerin etkin işletilmesi** doğrultusunda da yapılmasının bir zorunluluk olduğunun unutulmaması gerekiyor. Nitekim Equifax olayı, teknolojik olarak çeyrek milyar dolarlık siber güvenlik yatırımı yapılmasına rağmen, insan merkezli bir hatanın ABD'nin en büyük veri sızıntısına sebep olabileceğini, güvenlik prosedürlerinin proaktif ve kuvvetli olması gerektiğini ve şirket içi iletişimin en basit güvenlik açığının tespit edildiği durumda bile ne kadar önemli olduğunu ortaya koydu.

STM olarak 2017 yılının son çeyreğinde siber güvenlik alanında hedeflerimiz arasında olan;

- "Siber Güvenlik Ekosisteminin Yenilikçi Çözümlerle Geliştirilmesi Çalıştayı"nı 5 Ekim 2017 tarihinde ODTÜ Teknokent'te gerçekleştirdik. Siber güvenlikle ilgili ekosistemdeki paydaşların bir araya geldiği etkinlikte 15'in üzerinde firmadan 100'ü aşkın katılımcı yer aldı. Çalıştayda özellikle siber güvenlik alanındaki kümelenme eksikliği ve geliştirilecek yenilikçi çözümlerle inovatif yerli ürünlerin yaygınlaştırılmasına vurgu yapıldı.

- Siber güvenlik alanında kişilerin ve kurumların kendilerini deneyerek zayıf yönlerini görmelerini, kendilerini geliştirme imkânı sağlamalarını ve bu alanda çalışan tüm paydaşların tek çatı altında birleştirilmesini ve bilgi paylaşım ağının oluşturulmasını amaçlayan **Capture The Flag** yarışmalarından üçüncüsünü 26 Ekim 2017 tarihinde Ankara'da düzenlemenin heyecanını yaşadık. Bu etkinliğimize ait detaylı bilgi, raporumuzun özel ekinde yer almaktadır.

2018 Yılı Siber Tehdit Beklentilerimiz

2017 yılında karşılaşılan siber olayları dikkate aldığımızda, 2018 yılında siber tehdit olarak ön plana çıkacağını değerlendirdiğimiz hususları aşağıdaki başlıklar altında sunuyoruz:

Fidye yazılım tehdidi hız kesmiyor:

Siber saldırganların kurbanlarından en kolay para kazanabilme yöntemlerinden birisi olan fidye yazılımlarının (ransomware) 2018'de de büyük tehditlerden birisi olmasını bekliyoruz. 2017'de siber suç pazarında CaaS (Crime-as-a-service) suç menüsü altında Ransomware-as-a-Service'in oldukça aktif olduğunun görülmesini fidye yazılımlarına ait tehdidin devam edeceğine yönelik önemli bir ipucu olarak değerlendiriyoruz. Bu alandaki bir öngörümüz de, saldırganların kendilerine daha çok para kazandıracak hedeflere yönelerek hedef büyütmeleri.

Kripto para madenciliğine yönelik saldırılar:
Hızla değer kazanmalarına bağlı olarak artan ilgi, kripto para birimlerinin 2018'e de damga vuracağını düşünmemize neden oluyor. Buna bağlı olarak da siber saldırganlar için cazibesi artan kripto para madenciliğine yönelik saldırıların artarak devam edeceğini değerlendiriyoruz.

Nesnelerin İnterneti (IoT) cihazlarının kullanıldığı botnet saldırıları:
Akıllı cihazlara ve diğer Nesnelerin İnterneti (IoT) cihazlarına gittikçe artan talep nedeniyle, bu cihazlara yönelik gelişmiş güvenlik ihtiyaçlarını da gündemde kalacak konular arasında görüyoruz. Sahip oldukları güvenlik zafiyetleri nedeniyle bu cihazlara yönelik saldırıların da devam edeceğini ve özellikle botnetlere dâhil edilerek istismar edileceklerini değerlendiriyoruz.

Siber saldırganlar tarafından yapay zekâ ve makine öğrenmesi kullanımı:
Yapay zekâ ve makine öğrenmesinin sağladığı imkânlar bugüne kadar daha çok siber güvenliğin temin edilmesinde tespit ve koruma maksatlı kullanımları ile gündeme geldi. Buna karşılık artık siber korsanların da makine öğrenmesini kendi saldırılarını desteklemek ve yeni keşfedilen zafiyetleri en kısa zamanda istismar edebilmek için gittikçe daha fazla kullanacaklarını öngörüyoruz.

Kritik altyapılar ve sağlık sektörünü hedef alan saldırılar:
2017 ve daha önceki yıllardaki siber tehdit trendlerini incelediğimizde kritik altyapılara ve sağlık sektörüne yönelik saldırıların sürekli var olduğunu görüyoruz. İnsan hayatını da ilgilendiren önemli servisler içeren bahse konu sektörlerin 2018'de de siber korsanların hedefinde olacaklarını değerlendiriyoruz.

Devlet destekli saldırılar ve siber casusluk :
Sık sık devlet destekli saldırılarla adları anılan devletlerin, bilgi sistemlerine sızarak bilgi çalma, casusluk, zarar verme eylemlerine devam edeceklerini ve bu tür faaliyetlerin ülkeler arası siyasi ve politik ilişkileri de etkileyeceğini değerlendiriyoruz.

Bulut bilişim verilerine yönelik tehditler:
Yazılım, donanım ve altyapı alanındaki hizmetleriyle şirketler için cazip imkânlar sunan ve hızla gelişip yaygınlaşan bulut bilişimin henüz giderilemeyen güvenlik riskleri bulunmaktadır. Bu kapsamda şirketlere ait büyük miktarlarda verinin, siber korsanların hedefleri arasında bulunmaya ve özellikle veri sızıntıları için risk taşımaya devam edeceğini değerlendiriyoruz.

Mobil sistemler aracılığıyla siber korsanlık:
2017'de olduğu gibi 2018'de de kullanıcıların sahte uygulamalarla hedef alınacağını, Android ve iOS işletim sistemlerinde keşfedilen zafiyetler kullanılarak yapılan saldırıların devam edeceğini ve ele geçirilen cihazların kullanıldığı siber olaylarda artış olacağını öngörüyoruz.

2018 yılında özetle;
- Fidye yazılımlarının,
- Kripto para madenciliğine yönelik saldırıların,
- IoT cihazlara yönelik saldırıların ve IoT botnetlerin,
- Hem siber saldırı hem de savunma maksatlı olarak yapay zekâ ve makine öğrenimi kullanımının,
- Kritik altyapılara ve sağlık sektörüne yönelik saldırıların,
- Devlet destekli saldırılar ve siber casusluğun,
- Bulut bilişime yönelik saldırıların,
- Mobil cihazları hedef alan saldırıların

siber tehdit olarak ön plana çıkacağını öngörüyoruz.

Zararlı Yazılımlar

Bad Rabbit

Bu yıl içerisinde maruz kalınan fidye yazılımlarından "Bad Rabbit"ten öncelikli olarak Rusya, sonrasında Ukrayna, Türkiye ve Almanya da etkilendi[1]. Rusya'da yayın yapan 3 internet sitesi, Ukrayna'daki bir havaalanı ve Ukrayna'nın başkenti Kiev'deki metro sistemi en fazla etkilenen unsurlar arasında yer alıyor.

WannaCry ve Petya ile benzerlikleri bulunan ve birçok antivirüs yazılım programının tespit edemediği Bad Rabbit'in, 2017 Ekim ayı sonlarında sahte bir Adobe Flash güncellemesiyle birlikte yayıldığı ifade edildi.

Zararlı yazılım temel olarak ele geçirilmiş haber siteleri aracılığıyla yayılıyor. Siber korsanlar "Watering Hole" tabir edilen saldırılar kullanarak belirli kullanıcı grupları veya şirketleri hedefleyebiliyorlar. Bir kullanıcı enfekte olmuş bir siteyi ziyaret ettiğinde, otomatik olarak başlayan bir işlem ile Adobe Flash güncellemesi bilgisayara indiriliyor. Bu dosyanın çalıştırılması ile beraber Bad Rabbit sisteme giriyor ve zorunlu olarak yeniden başlayan bilgisayardaki tüm veriler şifreleniyor[2].

Bad Rabbit, WannaCry ve Petya gibi bir ağ içerisinde yayılabiliyor, ancak SMB Protokolü'nün 1.0 sürümünde bulunan EternalBlue istismar aracı yerine, zararlı yazılım diğer bilgisayarları Windows Yönetim Aracı (WMI) üzerinden etkiliyor.

Bad Rabbit'ten kurtulmanın çareleri olarak Kaspersky Lab tarafından yapılan açıklamada antivirüs yazılımlarının güncel ve çalışır vaziyette olması gerekirken WMI hizmetlerinin kapatılmasının virüsün ağ içerisinde yayılmasını engelleyeceği kaydediliyor.

Öte yandan yetkililer, fidyenin ödenmemesi gerektiğini vurgularken verilerin de başka depolama araçlarına aktarılarak orada güvenle saklanması gerektiğini ifade ediyorlar. Ayrıca, Adobe Flash güncellemelerinin, bizzat üretici sitesinden indirilmesi de tavsiye ediliyor.

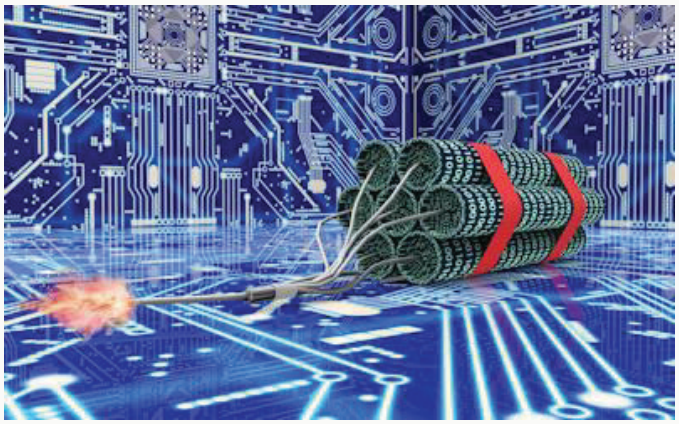
Triton

Özellikle endüstriyel kontrol sistemleri (EKS) için tasarlanmış ve "Triton" adı verilen yeni bir zararlı yazılım keşfedildi.

Triton zararlı yazılımı, 2017 Aralık ayı içerisinde Suudi Arabistan'daki ismi açıklanmayan bir kritik altyapı kuruluşunu hedef alan saldırılarda kullanıldı. Saldırıların hedefinin niteliği ve finansal bir amaca dayanmaması nedeniyle devlet destekli bir aktörün dâhil olduğu değerlendiriliyor[3].

Dragos güvenlik firmasından araştırmacılar da zararlı yazılımın varlığını tespit ve analiz ettikten sonra bulgularını bir raporla duyurdular ve "Trisis" olarak adlandırdıkları zararlı yazılımın Orta Doğu'da bir endüstriyel kuruluşa karşı kullanıldığını iddia ettiler[4].

[1] http://www.bbc.com/news/technology-41740768
[2] https://www.hornetsecurity.com/en/services-en/bad-rabbit-ransomware
[3] http://resources.infosecinstitute.com/triton-malware-hits-critical-infrastructure-saudi-arabia/
[4] https://thehackernews.com/2017/12/triton-ics-scada-malware.html



Dragos saldırıları belirgin bir kaynakla bağdaştırmaktan kaçınırken FireEye saldırıların daha önce Rusya, İran, ABD, Kuzey Kore ve İsrail'den devlet destekli aktörlere mal edilmiş küresel birçok saldırı ve keşif eylemleri ile uyuştuğu yönünde tahminde bulunuyor. Uzmanlar tehdit aktörlerinin bir sabotaj ortamı hazırladıklarını ve gözlemledikleri saldırıların kazara sebep olunmuş bir hizmet dışı kalma harekâtının keşif safhasına ait olduğunu düşünüyorlar.

FireEye tarafından yapılan analizde; Triton'u geliştirenlerin endüstriyel sistemlerde bir sürecin durumunu izlemek, onu güvenli bir evreye döndürmek veya eğer göstergeler potansiyel tehlikeli bir duruma işaret ediyorsa güvenli olarak kapatmakta kullanılan "Schneider Electric's Tritonex Safety Instrumented System (SIS)" kontrol ünitelerini hedefledikleri belirtiliyor.

Rapora göre saldırganların bir SIS mühendislik bilgisayarına uzaktan erişim sağladıkları, kontrol ünitelerini yeniden programlamak amacıyla Triton zararlı yazılımını yükledikleri ifade ediliyor. Bu da saldırganların bu tür sistemler hakkında derin bilgilere sahip olduklarına işaret sayılıyor.

SIS kontrol ünitelerine yönelik saldırıların, ünite ele geçirildikten sonra hedeflenen ortamda oluşan ciddi etkilerden sonra bile güvenli durum gösterecek ve kontrol ünitesinin, göstergeler tehlike değerleri algılasalar bile bunu iletmeyecek şekilde yeniden programlanabileceğinden dolayı oldukça tehlikeli olduğu vurgulanıyor.

Schneider Electric tarafından yapılan açıklamada tehlikenin farkında olunduğu ve bu tür bir saldırının risklerinin bertaraf edilmesine yönelik olarak hedef alınan ünitenin üreticisi ile beraber çalışılmakta olduğu ifade edilerek müşterilerine ilk aşamada almaları için gereken güvenlik tedbirleri konusunda duyuru yapıldı.

Triton, tehdit aktörlerinin EKS'lere yönelik sabotaj amaçlı ilgilerinin artmakta olduğunu göstermesi ve etkilerinin endişe verici olması yönleriyle tehdit ölçeğinde yeni ve önemli bir tespit olarak yerini almış durumda. Araştırmacılar, fiziksel hasar veya devre dışı bırakma kabiliyetleri ile Triton'un; Stuxnet, IronGate ve Industroyer gibi kritik altyapılara ciddi bir tehdit olduğuna inanıyorlar.

Digimine

2017 Aralık ayında, kripto para birimlerindeki artışla birlikte Google Chrome masaüstü kullanıcılarını hedefleyen ve Facebook Messenger vasıtasıyla yayılan kripto para üreten yeni bir bot virüsü keşfedildi[5].

"Digimine" ünvanlı Monero kripto parası üreten bu bot, sayfaya gömülü olmayan bir video dosyası olarak gözüküyor ve video_xxx.zip dosya ismine sahip, ama aslında Autolt çalıştırılabilir betiğine sahip bir dosya olarak görev yapıyor.

Tıkladıktan sonra hedef bilgisayara bulaşıyor. Bileşenlerini ve ilgili yapılandırma dosyalarını uzak bir komuta kontrol sunucusundan hedef bilgisayara indiriyor.

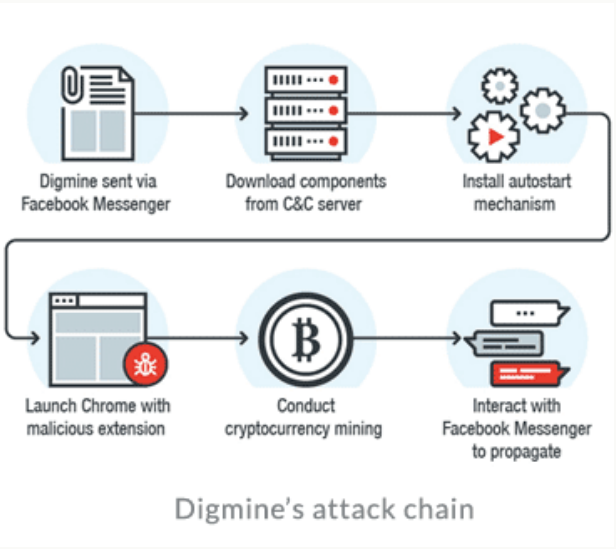
Digimine, öncelikli olarak kripto para üreten miner.exe dosyasını hedef bilgisayara yüklüyor. Bu dosya XMRig diye bilinen açık kaynak Monero kripto para birimi üreticisinin modifiye edilmiş sürümü.

[5] https://thehackernews.com/2017/12/cryptocurrency-hack-facebook.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1649.gh0ao08pqk.zxa

Bu üretici sessizce arka planda hedef bilgisayarın işlemcisini kullanarak saldırganlar için para üretiyor.

Kripto para birimi üretimi yanında Digimine bot, otomatik başlatma mekanizması ile Chrome'u zararlı bir eklentiyle başlatarak kurbanın Facebook profiline erişimine izin verip aynı zararlı yazılımın kurbanın Facebook arkadaşlarına Messenger vasıtasıyla bulaşmasını sağlıyor. Normalde Chrome eklentileri sadece Chrome Web Mağazası'ndan indirilebildiğinden saldırganlar zararlı eklenti içeren Chrome'u komut satırından başlatıyorlar. Bu eklentinin yapılandırma dosyasını komuta kontrol sunucusundan okuduğu ve eklentiye Facebook'ta oturum açmasını ya da sahte bir sayfa açarak videoyu oynatması gerektiğini bildirdiği belirtiliyor. Videoyu oynatan sahte site aynı zamanda komuta kontrol merkezi yapısının bir parçası ve video oynatan bir siteymiş gibi davranıyor. Aslında zararlı yazılımın birçok bileşenini ve yapılandırma dosyasını da tutan bir site olduğunu da gizliyor.

Mobil cihazlarından bu video dosyasını açanlar zararlıdan etkilenmiyor. Kripto parayı kurbanın bilgisayarının işlemcisini kullanarak üreten bu botun komuta kontrol sunucusundan yönetilmesinden dolayı bu zararlıyı yazanlar farklı fonksiyonları da ekleme kolaylığına sahip oluyor. Digimine, ilk olarak Güney Kore'deki kullanıcılara bulaştığında



Digmine's attack chain

tespit edildi. Daha sonra Vietnam, Azerbaycan, Ukrayna, Filipinler, Tayland ve Venezuela'ya yayıldı; fakat Facebook Messenger dünya genelinde kullanıldığından zararlının küresel olarak yayılma potansiyeli var.

Araştırmacılar tarafından Facebook uyarıldıktan sonra bu sosyal ağa bulaşan Digimine botların hepsi temizlendi. Facebook Spam kampanyalarının oldukça meşhur olduğu biliniyor.

Bu sosyal medya platformu vasıtasıyla yayılan bağlantılara tıklama konusunda kullanıcıların uyanık olması tavsiye ediliyor.

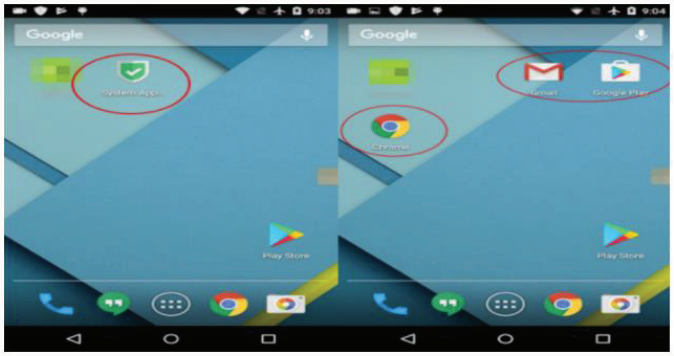
Catelites

2017 Aralık ayı sonlarında yayımlanan bir araştırmanın sonuçlarına göre yeni bir Android zararlı yazılımının parolaları çalmak ve dolandırıcılık yapmak üzere yaklaşık 2200 bankayı etkileyebileceği belirtildi[6]. "Catelites Bot" diye adlandırılan zararlının, ünlü Rus gangsterlerin milyonlarca cihaza Cronbot trojanı bulaştırarak 900.000 $ çalmasıyla ilişkilendirilebilecek potansiyel bağlantılara sahip olduğu ifade ediliyor.

Catelites, 3. parti uygulama mağazaları veya oltalama sitelerinde mevcut olan sahte ve zararlı uygulamalarla veya kötü amaçlı zararlı yazılım vasıtasıyla Android cihaza yükleniyor. Zararlı yazılım; metinleri yakalayabiliyor, telefonu kilitleyebiliyor, cihaz verisini silebiliyor, telefon numaralarına erişebiliyor, hoparlör ses düzeyini değiştirebiliyor, kısa mesajları ele geçirebiliyor ve cihaz kilidini açabiliyor.

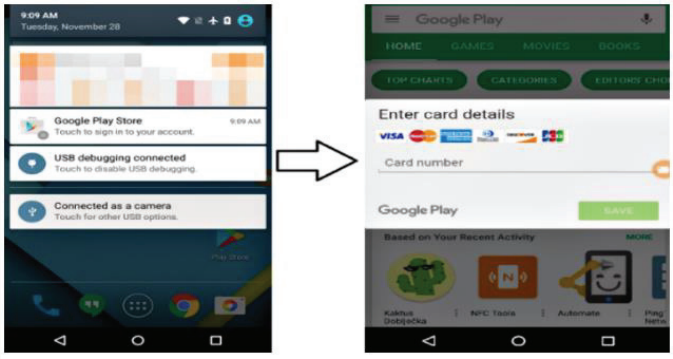
[6] https://www.hackread.com/catelites-android-malware-poses-as-2200-bank-apps/

Yüklendikten sonra, ekranda "Sistem Uygulaması" başlığı ile bir uygulama simgesi beliriyor. Kullanıcı bu simgeye tıkladığında, yazılım yönetici haklarını almak için soruyor. Kurban bu haklara izin verdiğinde simge kayboluyor ve botun görevi başlıyor. Ekranda Gmail, Google Play ve Chrome olmak üzere 3 adet güvenilir uygulamaya ait simge görüntülüyor. Sonrasında da kredi kartı bilgisi arıyor.



Kurban bu yeni simgelerden herhangi birini açarsa, sahte bir pencerede hassas mali bilgiler isteniyor. Bu simgeler gerçekçi güvenilir uygulamalara ait olarak gözüktüğü için çoğu kullanıcı bu tuzağa maalesef düşüyor ve bilgilerini giriyor. Bununla beraber eğer kullanıcılar durumdan şüphelenirlerse bu kez başka bir tuzak mekanizması işliyor, çıkan pencere bir türlü kapanmayarak kullanıcının verisini almak için diretiyor ve ancak bu şekilde kapanıyor.

Zararlının önceliği banka hesap giriş bilgilerini elde etmek. Zararlı, en zirvedeki banka ve finansal kurumlara tehlike yaratabileceğinden, kullanıcılar bu tuzağa düşürülmeye çalışılıyor. Bir bankacılık uygulaması açıldığında zararlı, tıpkı gerçek banka uygulamasının penceresine benzeyen sahte bir pencere açıyor ve kullanıcı bunun gerçek bankaya ait olup olmadığına karar veremiyor ve tuzağa düşerek kredi kartı ve uygulamaya giriş bilgilerini verebiliyor. Bu bilgiler de saldırganların eline geçtiğinde çok kolay şekilde banka hesaplarına erişebiliyorlar.



Güvenlik uzmanlarının belirttiğine göre CronBot ve Catelites birbirlerine oldukça benziyorlar. Catelites Bot aktörü ile CronBot arasında ilişki olduğuna dair herhangi bir kanıt bulunmamasına rağmen Catelites faillerinin Cron zararlısını ele alarak kendi kampanyaları için yeniden şekillendirmeleri muhtemel görülüyor. Yapılan değerlendirmede ayrıca zararlının otomatik ve etkileşimli bir şekilde Android bankacılık uygulamalarının logolarını ve isimlerini Google Play mağazasından çektiği, manipülatif mobil bankacılık uygulama ekranları ile orijinalleri benzemiyorken, asıl gücün milyonlarca bankacılık uygulaması kullanıcısından birkaç tanesinin olsun tuzağa düşürülebilmesini hedefleyen yaklaşımda yattığı ifade ediliyor.

Bu tür zararlılardan korunmak için güvenlik uzmanlarınca;

- Güncel Android antivirüs uygulaması kullanılması,

- Antivirüs programı olmayan kullanıcıların, telefonlarını emniyetli modda başlatıp zararlının yüklenip yüklenmediğinden emin olmaları,

- Uygulama indirmek için üçüncü parti uygulama mağazaları yerine bilinen platformlardan yararlanılması,

- Şüpheli bir uygulama bulunursa acilen silinmesi,

- Uygulamanın güvenilir ve gerçek olduğuna inanılmadığı müddetçe asla yönetici hakları için izin verilmemesi tavsiye ediliyor.

Zararlının şu ana kadar Rusya'da tespit edildiği, yaklaşık 9.000 kullanıcının hedeflenmiş olduğu belirtiliyor. Fakat bunun sadece test aşaması olduğuna inanılıyor ve saldırganların müteakiben dünyadaki diğer bankaları da hedefleyecekleri düşünülüyor.

Cutlet Maker

ATM'ler, maksimum kazanç elde etmek için değişik yöntemler kullanan dolandırıcılar için önemli bir gelir kaynağı olmaya devam ediyor. Bazı dolandırıcılar metal kesiciler kullanarak fiziksel tahribe yönelik yöntemler tercih ederken bazıları da para dağıtım ünitelerini zararlı yazılımların yardımıyla manipüle etmeyi tercih ediyorlar.

2017 Ekim ayında DarkNet pazarında açıktan satılan ve ATM'leri hedef alan bir zararlı yazılım

keşfedildi. "Cutlet Maker" adı verilen zararlı yazılım, ATM'ye fiziksel erişim sağlayan saldırgana ATM'den para çalma imkânı tanıyor[7].

Araştırmaya göre, zararlı yazılım kiti üç bileşenden oluşuyor:

- ATM'nin para dağıtım ünitesiyle iletişim kurmak için ana modül olarak görev yapan Cutlet Maker yazılımı,

- Cutlet Maker uygulamasını çalıştırmak ve yetkisiz kullanımdan korumak için bir parola oluşturmak üzere tasarlanan "c0decalc" adlı program,

- ATM'in para kasetlerinin mevcut durumunu belirleyerek suçlulara zaman kazandıran "Stimulator" uygulaması. (Bu uygulamayı yükleyerek kullanan saldırganın her kasetteki para birimi, değer ve banknot sayısı hakkında kesin bilgi alması ve bu sayede birer birer para çekme yerine, en büyük miktarı içeren kaseti hedef olarak seçmesi hedefleniyor.)

Zararlı yazılım şu şekilde kullanılıyor:

- Önce zararlı yazılımı yüklemek üzere kullanılacak USB portuna ulaşmak için ATM'nin içerisine doğrudan erişim sağlanıyor.

- Başarılı bir erişimden sonra zararlı yazılımı barındıran USB yardımıyla ATM'ye Cutlet Maker yazılımı yükleniyor.

- Diğer suçluların bu yazılımdan ücretsiz olarak yararlanmasının önüne geçen bir tür "telif hakkı" koruması maksadıyla şifre korumalı olduğu değerlendirilen zararlı yazılım için dizüstü veya tablet gibi başka bir cihaza kurulan "c0decalc" programı kullanılıyor.

- Son olarak kodun oluşturulmasıyla beraber suçlular, Cutlet Maker arayüzüne girerek para çekim işlemine başlıyorlar.

Zararlı yazılımın arkasında kimin olduğu bilinmiyor fakat dil, gramer ve üslup hataları, potansiyel suçluların ana dili İngilizce olmayan kişiler olabileceğine işaret ediyor.

Uzmanlar tarafından, Cutlet Maker'ın neredeyse hiçbir gelişmiş yeteneğe veya profesyonel bilgisayar kullanma becerisine ihtiyaç duymadığına, birkaç bin doları olan herhangi bir suçlunun oldukça karmaşık bir saldırı operasyonu gibi görünen ATM saldırılarını rahatlıkla yapabileceğine dikkat çekiliyor ve bu durumun finansal kuruluşlar için potansiyel bir tehdit haline geldiği ifade ediliyor. Ancak daha da önemlisi, Cutlet Maker'ın çalıştığı esnada ATM'lerin yazılım ve donanımlarıyla etkileşime girdiği ve neredeyse hiçbir güvenlik engeliyle karşılaşmadığı, bu şartlar altında ATM makinelerinin daha güvenli hale getirilmesi gerektiği vurgulanıyor.

Cutlet Maker gibi zararlı araçlara karşı ATM'leri korumanın ve fiziki güvenliklerini artırmak için uzmanların önerileri şunlar:

- Yetkisiz yazılımların ATM'de çalışmasını engelleyen "baştan yasaklı" sıkı politikalar uygulanması,

- Yetkisiz cihazların ATM'ye bağlanmasını sınırlamak için cihaz kontrol mekanizmalarının etkinleştirilmesi,

- ATM'lerin Cutlet Maker gibi zararlı yazılımlar kullanılarak gelen saldırılardan korunması için özel güvenlik çözümü kullanılması.

Siber Saldırılar

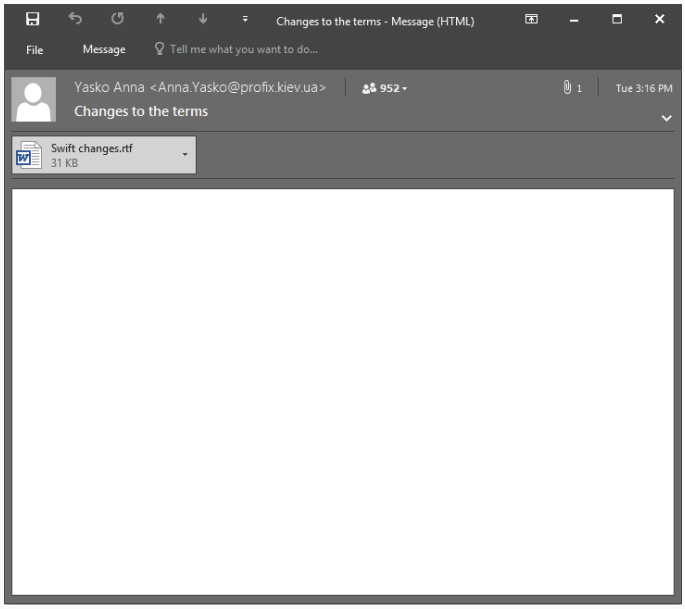
Cobalt Strike

2017 Kasım ayında Cobalt adlı siber korsan grubu tarafından çoğunlukla Türkiye ve Rusya'daki çeşitli finans kuruluşlarında çalışan bireylerin hedef alındığı bir hedef odaklı oltalama saldırı operasyonu gerçekleştirildi[8].

[7] https://www.kaspersky.com/about/press-releases/2017_atm-jackpotting-for-dummies-kaspersky-lab-identified-cutlet-maker

[8] https://www.riskiq.com/blog/labs/cobalt-strike/

Cobalt grubu tarafından hedefteki bireyleri ağlarında bir tutunma noktası elde etmek için gönderilen oltalama e-postaları, bankalar arası para transfer sistemi olan SWIFT'e ait vadelerdeki değişikleri içeriyormuş gibi görünen tek ekli ve gövdesinde metin olmayan e-postalardan oluşuyor.

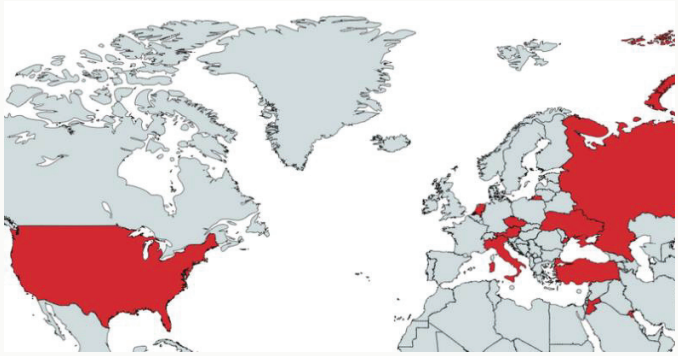


E-postalarda dikkat çeken bir husus, muhtemel ki grubun hedef adreslerini gizli haneye koymak yerine sehven KİME hanesine koyarak tüm listeyi ifşa etmeleri.

Saldırılarda kullanılan e-postaların eki, zararlı kodu çalıştırmak için Microsoft Office'in 2007 ila 2016 sürümlerini kullanabilen bir istismar aracını sömüren RTF dosyasından oluşuyor. RTF dosyası tarafından yüklenen zararlı kod aslında sızma testi ve kırmızı takım angajmanlarında kullanılan bir tehdit emülasyon yazılımı olan Cobalt Strike'ın bir parçasından oluşuyor ve bu kod aracılığıyla saldırganların komuta kontrol sunucularına bağlanılıyor.

Gerçekleştirilen saldırıların başta Türkiye ve Rusya olmak üzere ABD, Hollanda, İtalya, Avusturya, Ukrayna, Ürdün, Kuveyt ve Çek Cumhuriyeti'nden oluşan, toplamda on bir ülkeyi etkilediği ifade ediliyor.

Birçok güvenlik teknolojileri ve güvenlik araştırmacıları zararlı yazılımlar için yeni tespit mekanizmaları ortaya koyuyor olabilirler, ancak siber saldırganlar da taktiklerini bu yeni mekanizmaları geçersiz kılacak şekilde geliştiriyorlar. Cobalt Grubu'nun bu son saldırılarında da kendi zararlı kodları için geçit olarak kullanmak amacıyla güncel Windows programlarını veya araçlarını inceledikleri anlaşılıyor[9].



Uzmanların bu olay benzeri durumlara karşı savunma yapabilmek için önerileri şu şekilde sıralanıyor:

- PowerShell, odbcconf.exe ve regsvr.exe gibi yorumlayıcı (interpreter) veya komut satırı uygulamalarının (command line application) kara listeye alınması, kullanım dışı bırakılması veya kullanımlarının güvenli hale getirilmesi,

- Saldırganların bilinen zafiyetleri istismar etmelerini önlemek için sistem ve uygulamaların düzenli olarak yamalarının yapılması ve güncel olarak idameleri,

- E-posta geçitlerinin güvenli hale getirilmesi,

- Yanal yayılmanın önüne geçmeyi önlemek için ağ segmentasyonu ve veri kategorizasyonunun uygulanması,

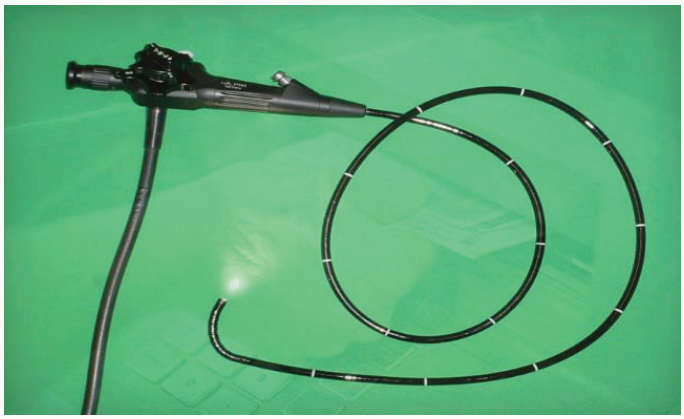
- Güvenlik duvarları, kum havuzları, saldırı tespit ve önleme sistemleri kullanılarak ağ ve uç kullanıcıların anormal aktiviteler için proaktif olarak izlenmesi.

ATM'lere Endoskopi Cihazı İle Saldırı

ATM'lere saldırılarda kullanılan araçlara endoskopi cihazı da eklendi. Doktorların insan vücudunun içerisine bakmasına destek olmak maksadıyla 150 yıl önce icat edilen, ışıklar ve kameralarla gelişen teknoloji artık ATM'lerin sensörlerini kandırarak içindeki paraları almak maksadıyla kullanılıyor[10].

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/

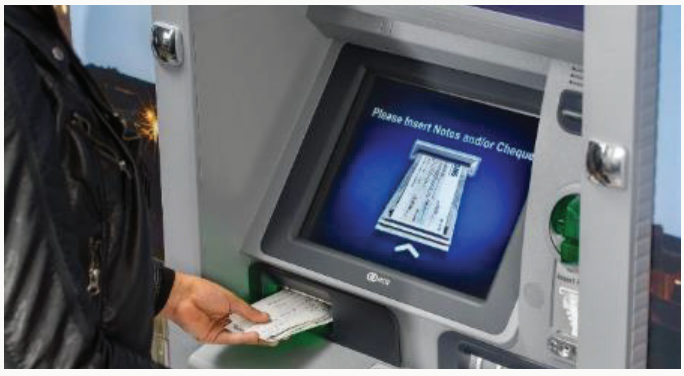
[10] https://www.bankinfosecurity.com/hackers-practice-unauthorized-atm-endoscopy-a-10369

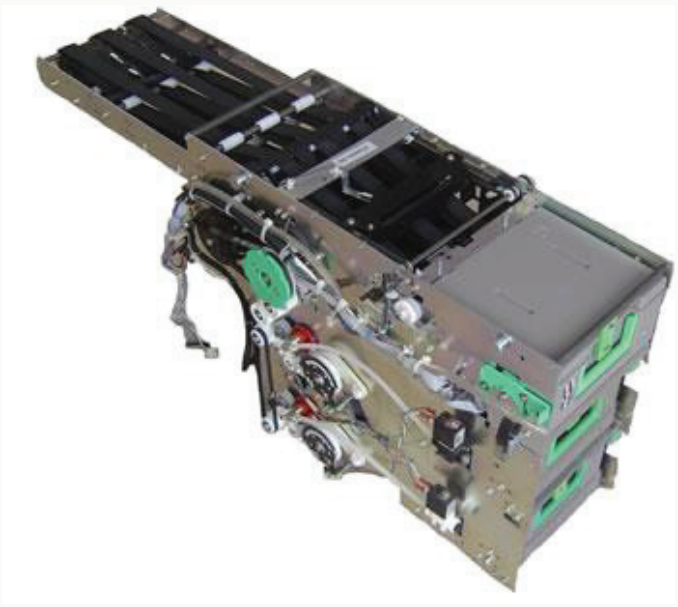


ATM üreticisi olan NCR firması tarafından 2017 Ekim ayında yapılan açıklamada uygulamanın şu ana kadar Meksika'da bir dizi saldırı içerisinde kullanıldığı ve en az bir tanesinde cihaza fiziksel erişimin başarılı olduğu ifade edildi.

Bu tür saldırılarda müstakil ATM modelleri hedefleniyor. Saldırganlar ATM'nin içine erişip USB portu vasıtasıyla bir kara kutu kontrol ünitesi (black box) bağlantısı sağlanıyor. İlaveten, saldırganlar ATM cihazının ön kapısını açıyorlar ve kasetlere fiziksel erişim için para dağıtan kapağı çıkarıyorlar. Bu aşamadan sonra endoskopi teknolojisi işin içine giriyor ve endoskopi cihazı para çıkış deliğinden içeri sokulduktan sonra para dağıtıcısının içerisinde bulunan sensörler yanıltılarak fiziksel kimlik denetimini simüle ediliyor. Bu sahte kimlik denetimi kara kutu tarafından ATM cihazına para dağıtımı komutlarının verilmesi sağlanıyor.

Güvenlik uzmanları tüm ATM'lerin iyi izlenebilen mahallere kurulmasını ve ATM'lerin içine fiziksel olarak erişim sağlayan saldırganların saldırı başlatabileceklerinden dolayı dış muhafazalarının güvenli hale getirilmesini, alarm ile güvenliklerinin artırılması konusunda uyarılar yapıyorlar.





Endoskopi yöntemiyle yapılan saldırılar tespit edildikten sonra, NCR tarafından saldırıları önleyecek acil gömülü yazılım güncellemesi yayımlandı ve uygulandıktan sonra bir saldırı vakasına rastlanmadığı açıklandı. Buna ilaveten ATM'lerin para dağıtım ünitelerinin kara kutu saldırılarından korunması maksadıyla iç iletişimlerinin şifrelenmesinin gerektiği belirtildi. Bu sayede saldırganlar tarafından doğrudan para dağıtım ünitesine gönderilen komutların geçersiz olarak algılanması ve sadece ATM yazılımı üzerinden gelen komutların kimlik denetiminden geçeceği ve işleme konulacağı ifade ediliyor.

Tarayıcı ve Yazıcılar Üzerinden Siber Saldırılar

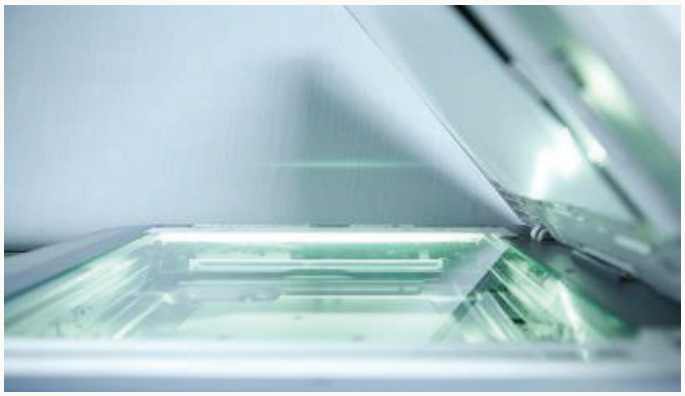
Siber suçlular ağ yazıcısından geliyor gibi gözüken zararlı ekleri milyonlarca tarayıcı ve yazıcıyı taklit ederek saldırılar gerçekleştiriyorlar[11].

2017 Kasım ayının sonlarına doğru keşfedilen ilk saldırıda kullanılan zararlı eklenti, saldırganlara hedef bilgisayarda gizli bir gözetleme başlatma veya hedef bilgisayara arka kapıdan yetkisiz erişim imkânı sağlıyor[12].

İlk tespiti müteakip şüphe duymayacak kullanıcılara zararlı eklentiyi bulaştırmak maksadıyla milyonlarca girişim tespit edilmiş durumda. Saldırı Canon, HP ve Epson marka yazıcı/tarayıcı gibi davranarak kullanıcının güvenini kazanıyor. Araştırmacılar yazıcı tarafından gönderilen PDF

[11] https://www.scmagazine.com/criminals-spoof-scanners-and-printers-to-infect-office-networks-with-malware/article/720774/?DCMP=EMCSCUS_Newswire_20171228&email_hash=0BC55706889119A98DEDEEF45AEC5598&spMailingID=18741976&spUserID=MjQ3NzE5MjgwODQ0S0&spJobID=1162272761&spReportId=MTE2MjI3Mjc2MQS2

[12] https://blog.barracuda.com/2017/12/21/threat-spotlight-clever-cybercriminals-spoof-scanners-by-the-millions/#more-20309



dosyası çok geleneksel bir durum olduğundan, kullanıcılar tarafından dokümanın tamamen emniyetli olduğunun düşünüldüğünü belirtiyorlar. Sosyal mühendislik perspektifinden bakıldığında bu davranışın tamamen siber suçluların isteyeceği bir cevap olduğu ifade ediliyor.

PDF dosyaları zararlı aktif içerikleri dağıtmak için kullanılabileceğinden ve kaynak düşünüldüğünde kullanıcılar tarafından emniyetli olarak farz edileceğinden dolayı saldırganlar özellikle PDF dosya üreten araçlar seçmektedir.

Kurbanlara gönderilen e-postanın konu bölümünün "Scanned from HP", "Scanned from Epson" ya da "Scanned from Canon" olarak yazılması ve ilişikte bulunan zararlı ekin uzantısı ve dosya isminin tespit mekanizmalarını aşmak için ".jpg", ".txt" gibi bilinen formatları taklit edilerek gizlenmesi zararlı dokümanının açılma potansiyelini artırmaktadır.

Zararlı ek, bulaştığı cihazda kurbanın hareketlerini izleme, bilgisayar ayarlarını değiştirme, dosyalarını görme ve kopyalama ve bant genişliğini kullanma gibi kabiliyetlere sahip olabilmek üzere tasarlanmış bir zararlı yazılım olarak çalışıyor.

Bu tip atakları önlemek için araştırmacılar tarafından kullanıcılara, beklenmedikleri bir dosya aldıklarında gönderen ile karşılıklı kontrol sağlanması ya da dosyanın silinmesi, fare imlecini dosyanın üzerine getirerek bağlantıların gözlemlemeye çalışılması, şüpheliyse tıklanmaması tavsiye ediliyor. Ayrıca, kullanıcıların ileri tehditlerden korunma üzerine eğitilmelerinin ve yüksek farkındalık seviyesine sahip olmalarının önemi vurgulanıyor.

Team Viewer

Kullanıcılarına bilgisayarlar arasında çevrimiçi toplantılar, masaüstü paylaşımı, uzaktan kontrol, dosya transferi vb. imkânı tanıyan "Team Viewer" uygulamasını kullanan bir milyardan fazla cihaz bulunuyor. Tabii ki böylesine geniş kullanım alanı olan bir uygulamada zafiyet söz konusu olduğunda, büyük önemi oluyor.

2017 Aralık ayı başında "Gellin" adını kullanan bir GitHub kullanıcısı tarafından Team Viewer'da kritik bir zafiyet tespit edildi. Zafiyet; saldırganın, sahibinin rızası olmadan bilgisayarını uzaktan kontrol altına alabilmesini sağlıyor[13].

Gellin bu konuda GitHub'a kavram kanıtı (proof of concept - PoC) kodu olarak enjekte edilebilir

[13] https://www.hackread.com/teamviewer-vulnerability-full-pc-control/

bir C++ dll yükledi ve kurbanın Team Viewer izinleri değiştirilirken haberi olmayacak şekilde kullanılabildiğini gösterdi.

Zafiyet ilk olarak "xpl0yt" adlı bir Reddit kullanıcısı tarafından duyuruldu ve Gellin'in GitHub'taki kavram kanıtına referans verildi. Team Viewer'ın kendisinin de zafiyetin varlığından bu şekilde haberi olduğu ifade ediliyor[14].

Zafiyet macOS, Linux ve Windows işletim sistemlerini etkiliyor ve işletim sistemlerine ait yamalar 2017 Aralık ayı içerisinde yayımlanmış durumda.

Team Viewer kullanıcılarına ilk fırsatta uygulamanın yamalanmış sürümünü yüklemeleri tavsiye ediliyor, otomatik güncellemeyi seçmiş olan kullanıcılara ise yamalar otomatik olarak yayımlanıyor.

SSH Anahtarların Rotasyonunda İhmal

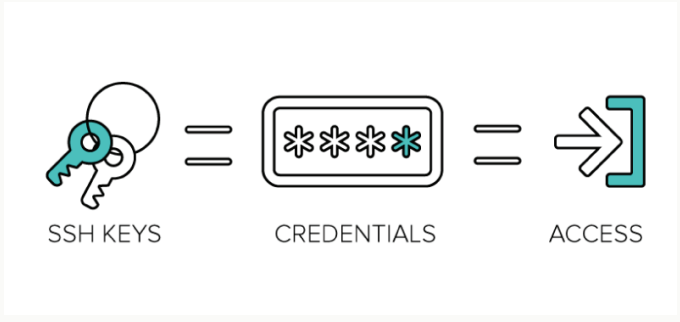
2017 Aralık ayında yapılan yeni bir araştırmaya göre, SSH anahtarları en yüksek seviyede yönetici erişim hakkı sağlasa bile rutin bir şekilde takip edilmiyor, yönetilmiyor ve güvenlik altına alınmıyor[15].

Örneğin, finans sektöründen gelen cevapların %69'u aktif bir şekilde anahtarları rotasyon yapmadığını (hatta bir sistem yöneticisinin kurumdan ayrılması durumunda bile) kabul ediyorlar. Araştırma, bu şartlarda eski çalışanın kritik ve hassas sistemlere erişiminde hâlihazırda yetkisinin devam ettiğini gösteriyor.

Uzmanlar, siber suçluların bu şekilde risk oluşturan SSH anahtarları kullanarak sunucularda tespit edilemeyecek şekilde yüksek yetki kazanıp zararlı aktiviteler gerçekleştirebileceğini ifade ediyorlar. Tehlikeye düşmüş tek bir SSH anahtarının binlerce sistemde kopyalanmış olabileceği hususu

sorunu daha da büyütüyor. Siber suçluların bu tür anahtarları kullanarak bir finansal kurumun tüm sistemlerine ek arka kapılar ve güvenli noktalar oluşturmak suretiyle nüfuz edebilme ihtimali bulunuyor.

Yılın ilk aylarında yapılan bu araştırmaya ABD, Birleşik Krallık ve Almanya'dan finans sektöründe çalışan SSH konusunda derin bilgiye sahip olan bilişim teknolojileri ve güvenlik profesyonellerinden oluşan 100 kişi katılmış.



Araştırmanın önemli bulguları şu şekilde:

- Araştırmaya katılanların %85'i tarafından tam ve eksiksiz şekilde tüm SSH anahtarı envanterine sahip olmadıkları belirtilmiş. Tam kapsamlı bir envanter olmadan finans endüstrisindeki kurumların anahtarların çalınıp çalınmadığını, amacı dışında kullanılıp kullanılmadığını ya da

[14] https://www.techworm.net/2017/12/teamviewer-vulnerability-allows-users-sharing-desktop-session-gain-control-others-pc.html

[15] https://www.securitymagazine.com/articles/88565-percent-of-financial-services-organizations-do-not-rotate-ssh-keys-after-employees-leave

güvenilip güvenilmeyeceğini saptamaları mümkün görünmüyor.

- Katılımcıların %61'i tarafından birçok sistemde SSH anahtarı üretmeye izin veren SSH yöneticilerinin sayısının kısıtlanmadığı ve bu yöneticilerin kurumları SSH güven ilişkilerinin envanterinden ya da rutin gözden geçirilmesinden mahrum bırakan tutarsız güvenlik kontrolü kullanma eğiliminde olduğu belirtilmiş.

- Katılımcıların sadece %29'u tarafından anahtarları 3'er aylık veya daha sık aralıklarla rotasyona tabi tuttukları, %36'sı tarafından hiç anahtar rotasyonu yapmadıkları veya ara sıra yaptıkları belirtilmiş. SSH anahtarlarına sahip olan saldırganların, o anahtarlara rotasyon uygulanıncaya kadar ayrıcalıklı erişim hakları devam etmektedir.

- Katılımcıların %39'u tarafından SSH port yönlendirmeyi kapatmadıkları söylenmiş. Port yönlendirme, kullanıcıların sistemler arasındaki güvenlik duvarlarını rahatça baypas edebilmesini sağladığından dolayı, bu durum SSH erişimine sahip siber suçluların çok hızlı bir şekilde kurumdaki farklı ağlar arasında atlama yapabilmelerine yol açmaktadır.

- Katılımcıların %31'e yakını tarafından SSH ayarlarının kurumun Yetkilendirilmiş Erişim Yönetimi (Privileged Access Management-PAM) ilkelerinde işlenmediği ve nadiren denetlendiği belirtilmiş. Düzenli denetlenmeden ve etkili SSH güvenlik politikasına sahip olmadan SSH anahtar zayıflıkları tespit edilememekte ve finans sektöründeki kurumları geniş yelpazede siber saldırılara karşı savunmasız bırakmaktadır.

Veri İhlalleri

Uber

2017 Ekim ayında gerçekleşen yoğun veri sızıntısı sonucunda dünya genelinde yaklaşık 57 milyon sürücü ve yolcusuna ait e-posta adresi ve telefon numarası bilgileri ile yaklaşık ABD'de çalışan 600 bin sürücüye ait ehliyet numaralarının çalındığına yönelik açıklama yapıldı. Bu konuda yayımlanan bir raporda da bilgilerin çalındığının ifşa edilmesi yerine şirketin, verileri çalan iki siber korsana olayı gizli tutmaları ve bilgilerin silinmesi karşılığında 100.000 $ fidye ödediğinin de iddia edilmesi dikkat çekti[16].

Uber'in açıklamasında hiçbir sistemlerinin ele geçirilmediği, sadece şirket dışı iki kişi tarafından üçüncü parti bir bulut bilişim hizmeti kapsamında tutulan verilere erişim sağlanarak indirildiği ifade edildi. Ayrıca seyahatin güzergâhı, kredi kartı numaraları, banka hesap numaraları, sosyal güvenlik numaraları, doğum tarihleri gibi kişisel bilgilerin saldırıdan etkilenmediği vurgulandı.

Bloomberg'de yayımlanan raporda da Uber mühendislerinin kullandığı bir GitHub kod deposuna erişim sağlayarak Amazon bulut bilişim hizmeti için gerekli özel oturum kimlik bilgilerini elde eden siber korsanların bu şekilde sürücü ve yolcu bilgilerini çaldıkları ifade ediliyor[17].

[16] https://thehackernews.com/2017/11/uber-hack-data-breach.html

[17] https://www.theverge.com/2017/11/21/16687796/uber-cyberattack-data-breach-exposed-users-57-million

Şirketin siber korsanlara fidye ödeyerek gerçekleşen veri sızıntısını gizli tutmak istemesi güvenlik yöneticilerinin işlerini kaybetmesine sebep oldu. Şirketin yeni CEO'su yaptığı bir açıklamasında olmaması gereken bir olayın yaşandığını, bununla ilgili bir bahane üretmeyeceğini, ancak her Uber çalışanı adına hatalardan ders çıkarılacağı sözünü verebileceğini belirtti. Şirketin, olaydan etkilenen sürücülere ücretsiz kredi izleme ve kimlik hırsızlığı koruma hizmeti önerdiği, aynı zamanda etkilenen hesapların dolandırıcılığa karşı takip ettiği ifade ediliyor.

Saldırıdan sonra Uber'in bu saldırıyı engellemesi için değişik yöntemlerin kullanılabileceği açıklandı[18]:

- İki faktörlü kimlik doğrulama ile ilave bir güvenlik katmanı oluşturarak saldırganların Uber hesaplarına girişinin engellenmesi,

- SSH anahtarları kullanımı ve oturum detayları ile yazılım kodlarının ayrımının sağlanarak riskin düşürülmesi,

- Verinin kendisine bir Software-Defined Perimeter (SDP) mimari yaklaşımı sağlanarak saldırı yüzeyinin azaltılması.

Tabii ki bulut bilişim, bilgi teknolojisinin modern yüzü olarak şirketlere daha fazla çeviklik sağlamakta ve uygulamalarını maliyet ve zaman dengesine göre sunma imkânı vermektedir; ancak bununla birlikte bulut bilişimin paylaşılmış sorumluluk modeli, müşteri bilgilerinin bulutta güvenli olarak saklanmasına yönelik politikanın hem bulut sağlayıcısı hem de onu kullanan organizasyon tarafından benimsenmesini gerektirmektedir.

Karaborsada 1.9 Milyar Kullanıcı Adı ve Parola

2017 Kasım ayında gerçekleştirilen bir araştırma karaborsada 1.9 milyar kullanıcı adı ve parolası bulunduğunu ortaya koydu. Daha da ötesi bu çalıntı ad ve parolaların %25'i geçerli bir Google hesabı ile kullanılabilir durumda[19].

Hazırlanan raporda Google'ın mülkiyetinde bulunan verilerin, siber korsanlarca ele geçirilen ve siber korsanlık sitelerinde ve Dark Web'de pazarlanan kullanıcı adı ve parolaların gerçek hesaplarla uyuşup uyuşmadığına yönelik çalışmada

kullanıldığı ifade edildi.

Çalışma sonucunda birçok kullanıcının değişik uygulamalarda aynı parolaları kullandığı, ne zaman ki bir uygulamaya ait veriler ele geçirilse siber korsanların aynı parolaları diğer uygulamalarda da çalışacağını umarak denedikleri vurgulanıyor[20].

Araştırmacılar tarafından ayrıca oltalama maksatlı ve kullanıcı tiplerini gizlice kayıt etme maksatlı zararlı yazılımları da incelenmiş.

Kullanıcıları sahte oturum açma sayfalarına kimlik bilgilerini göndermeye zorlayan oltalama araçları bu zararlı yazılımlara bir örnek. Bu sahte giriş sayfaları genellikle kullanıcı adları, parolalar, kurtarma soruları, telefon numaraları, cihaz tanımlayıcıları ve coğrafi konumlar gibi kullanıcı kimlik bilgilerini alıyor.

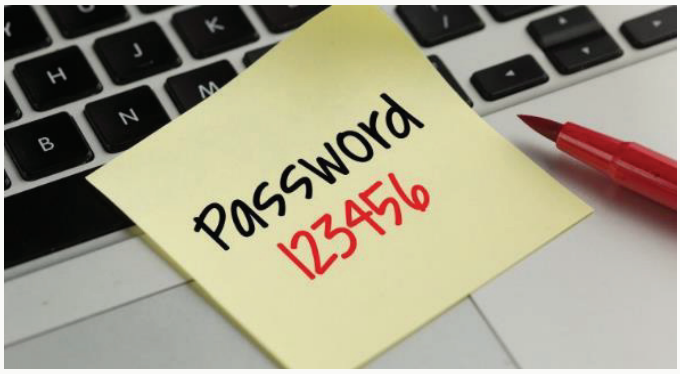
[18] https://blog.checkpoint.com/2017/11/24/uber-takes-cloud-security-ride/

[19] https://www.digitaltrends.com/computing/google-berkeley-study-billion-passwords-black-market/

[20] http://www.businessinsider.sg/google-research-report-on-phishing-keyloggers-and-stolen-passwords-2017-11/

Ayrıca binlerce farklı "keylogger"lar bulunuyor. Bu yazılımlar kurbanın bilgisayarında arka planda çalışıyor ve yazılan her şeyi kötü niyetli kişilere gönderiyor. Bu tip keyloggerlar 'HawkEye' ya da 'Cyborg Logger' gibi isimlerle adlandırılıyor.

Ortaya çıkan gerçek, bu tür zararlı yazılımların dayandıkları teknolojiye ait herhangi bir güncelleme yapılmadan yıllardır birçok geliştirici tarafından satılıp dağıtıldığı. Yaklaşık on yıldır tespit edilen oltalama araçlarının hâlâ aynı PHP çatıya ve çalınan giriş bilgilerine dayalı yaklaşıma dayalı olduğu vurgulanıyor.



Araştırmacılar Google gibi firmalara ve kullanıcılara kendilerini bu tür zararlı yazılımlardan korumak için;

- Hesaba giriş yaparken bir kullanıcının özel bir güvenlik anahtarına ihtiyacı olduğu ya da bir hesabına tam erişim için mesajla gönderilen bir kod yazmasını gerektirecek şekilde iki faktörlü kimlik doğrulamayı,

- Bir site ihlal edildiğinde, bilgisayar korsanlarının diğer hesaplara erişememelerini sağlayacak şekilde her site için yeni bir rastgele şifre oluşturan bir şifre yöneticisi kullanılmasını,

- Özellikle en yaygın kullanılan "123456" veya "abc123" gibi güvensiz bir şifre kullanılmamasını tavsiye ediyorlar.

Siber Casusluk/İstihbarat

Kaspersky Hakkında İddialar

2017 Ekim ayı başında bir Amerikan medya ajansı Wall Street Journal'de Kaspersky karşıtı yayımlanan bir makalede, Rus Hükümeti'nin Kaspersky'ın desteğiyle yüksek gizlilik derecesine sahip NSA dokümanlarını ve siber istismar araçlarını çaldığına yönelik bir iddia yayımlandı.

Amerikan istihbarat kaynaklarından yapılan alıntılarla hazırlanan Wall Street Journal makalesinde Kaspersky'ın Rus ajanları ile bilinçli olarak ilişki içinde olduğuna veya bazı siber korsanların Kaspersky antivirüs ürününe ait sıfırıncı gün zafiyetlerini istismar ettiklerine yönelik herhangi bir sağlam dayanak bulunamadı.

Müteakiben New York Times'ta İsrail İstihbarat Ajanslığı'ndan bir kaynağa dayanılarak yayımlanan bir makalede de İsrail devlet destekli siber saldırganlarının 2015 yılında Kaspersky ağına girerek Rus Hükümeti'nin Kaspersky'ın desteğiyle ABD Hükümeti'ne yönelik siber korsanlık faaliyetlerini suçüstü yakaladığı iddia edildi. Bu da Wall Street Journal'de yayımlanan iddiaları doğrulama maksatlı bir girişim olarak dikkati çekti.

Makalede 2015 yılında olası bir veri sızıntısına yönelik olarak İsrail yetkilileri tarafından NSA'nın uyarılmasının üzerine, ABD yetkilileri tarafından ivedi bir araştırma başlatıldığı ifade ediliyor.

2015 yılının ortalarında Moskova merkezli Kaspersky Lab'ın, kendi kurumsal ağında gelişmiş bir siber casusluk arka kapısı tespit ettiği ve ihlâl hakkında detaylı bir rapor hazırladığı ve aynı dönemde Kaspersky tarafından tespit ettikleri bazı saldırı kodları ile İran'ın nükleer programını sabote etmek üzere 2010 yılında ABD ve İsrail tarafından geliştirilen Stuxnet solucanına ait dijital parmak izlerinde benzerlikler olduğu yönünde de açıklama yapıldığı biliniyor. Bu süreçte Kaspersky'ın tutumuna bağlı olarak hakkında oluşan şüpheler, sonunda ABD Anayurt Güvenlik Departmanı'nı tüm devlet bilgisayarlarındaki Kaspersky antivirüs yazılımlarının kaldırılması ve yasaklanması kararına götürmüş durumda.

İlaveten, 2017 Eylül ayında ABD Ulusal İstihbarat Konseyi'nin NATO üyeleriyle, Rus FSB istihbarat ajanslığının Kaspersky'ın veri tabanlarına ve hatta kaynak koduna erişim sağladığı sonucuna varıldığını ifade eden gizli bir rapor paylaşmış durumda.

Buna karşılık Kaspersky Lab herhangi bir siber casusluk harekâtı hakkında bilgisi olduğu veya karıştığı yönündeki haberleri reddediyor.

Kaspersky'nin herhangi bir suça iştirak edip etmediği yönünde bir hüküm vermek oldukça zor. Şu aşamada top, yüksek gizlilik dereceli İsrail karşı istihbarat operasyonu ile ilgili gerçek bulguları dünya kamuoyuna sunması gereken Amerikan mahkemesinde görünüyor.

Özel Ek

STM Capture The Flag'17

29 takım, 119 yarışmacı, 9 farklı kategoride 42 adet birbirinden zor soru, 8 saat süre, yoğun stres ve yüksek sesli müzik... STM CTF'17 bu sene böyle geçti.

STM olarak ilk CTF yarışmamızı 27 Ekim 2015 yılında Bilkent Üniversitesinde gerçekleştirmiştik. 21 takım 73 yarışmacı ve gün boyu süren maraton sonrasında[21] 2016 yılında daha iyisini yapma fikirleri oluşmaya başlamıştı. STM Capture The Flag'16 ise müthiş bir görsel sunum ile 20 Ekim 2016'da Wyndham Hotel Ankara'da bir yıl önceki yılda olduğu gibi büyük bir coşku ile başladı[22].

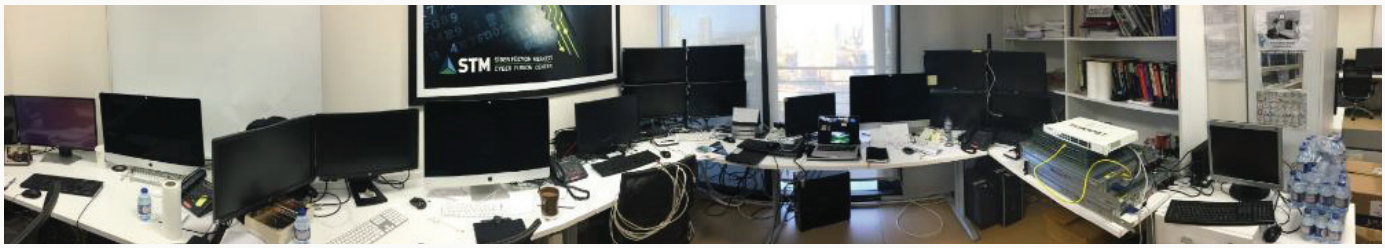
STM CTF'17 çalışmalarına 6 ay önce başladık. İşte bu, 6 ay süren bir maratonun sonunda ortaya çıkan bir yarışmanın öyküsüdür.

6 kişi ile toplamda 22 soru hazırlama planı ile başlayan süreç 10 kişi ve 42 soru ile tamamlandı. Biraz abartarak diyebiliriz ki biraz daha zamanımız olsaydı 100 sorulu CTF hazırlayan ilk ekip olacaktık. Soruları kimse birbiri ile paylaşmadı. Soru sayısını ve içeriğini gizli tutuyorduk. Tüm sorular bir kişide toplanıyordu ve kontroller yapılıyordu. Yarışma panelinin konfigürasyonu, sunucu ve switch'lerin güvenlik sıkılaştırmaları ve yaşanan her aksilikte tekrarlanan test süreçleri ile çalışma ofisimizin bilgisayarlar tarafından fethedildiğini de fark etmemiz fazla zamanımızı almadı.

Yaz sıcağında deniz kenarında yazılan sorular olduğu gibi, sıcak Ankara günlerinde(!) hazırlanan sorular da vardı. Hal böyle olunca STMCTF {Ş3KİL_Y4pm4K_İÇİn_N3_K4Dar_uĞr4ştığımı_GöRÜy0rsUn_DEğİl_mİ?} veya STMCTF {CTF_icin_ne_guzel_bir_gun} gibi bayraklar bizlerin ruh halini yarışmaya yansıtıyordu. STMCTF {GIT_TATIL_YAP_ISI_BOSVER} bayrağı ise son anda kendisinin tatilde olduğunu hatırlayan birisinin hazırladığını düşünebilirsiniz.

Panelde güvenliği arttırmak için bu sene yarışmada bulunan bayrakların MD5 değerlerinin girilmesini istemiştik. 2016 yılında Panele SQL Injection deneyecek kadar cesur olan yarışmacılar olunca 2017'de karakter sayısını kısıtlamak en kolay çözüm oldu.

Sorular toplanmaya başlayınca çok tehlikeli bir dosya oluşmaya başlıyordu. Bu dosya da soru ve bayrak bilgilerinin bulunduğu Excel dosyası idi. Toplam dağıtılacak ödülün 32.000 TL olması, cevapların bulunduğu bu dosyanın yarışma sonuna

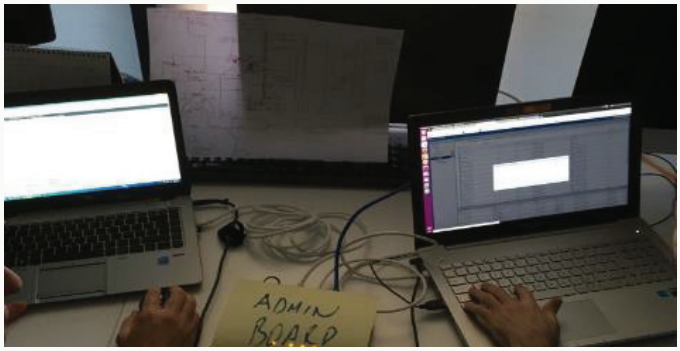


[21] https://www.youtube.com/watch?v=Rzxtwed6GbM

[22] https://www.youtube.com/watch?v=vqXQbd7iL4c

KATEGORI	KOD	PUAN	SORU ADI	DOSYA / SERVER		KEYWORDS	FLAG	
FORENSICS	**FOR200**	200	jigsaw puzzle	**b0df64ae2a7bfbfa63e9060b7fedf091.zip**	P	1.hex,2.hex,3.hex, PCAP, ZIP,	STMCTF{Damladi_dAmLaDI_GOL_oLDu}	A5F04526D725A
PWN	**PWN200**	200	PWINGME	nc 192.168.MASANO.5 7777	sn	8.8.8.8$(cat flag)	STMCTF{welld0neFLAGyoupwinged1t}	10CD7341F260C
TRIVIA	**TRIVA020**	20	Anket	https://goo.gl/	P	Anket doldurulacak	STMCTF{STM_CTF_18_de_gorusmek_uzere!}	AF44FEE817D57
MOBILE/WIRELESS	**MOB200**	200	Tombul Kuş	**6b6251894b1f2922d9860b9c4e99e7d5.zip**	Y	apk, 200Xpng	STMCTF{tombul_kus_arabaya_kos_:)}	8E363D03313B4
CRYPTOGRAPHY	**CRYPT150**	150	ATBAŞI gidiyorlardı...		Ö	ATBASH, ENIGMA	STMCTF{ENIGMAYIDAKIRDINBRAVO}	A59F8B06DD35E
MISC	**MISC175**	175	ENCODEDECODE	**01c9343bc97ccb619c191dcf5ad98f63.zip**	sn	base58	STMCTF{3ncoding1sn0tcryptin6}	FB2F1A7D82F72
CRYPTOGRAPHY	**CRYPT250**	250	LFSR64	**1368bcdb1fd305416757edbe85a35843.zip**	Ö	Berlekamp- Massey algoritması	STMCTF{CTF_icin_ne_guzel_bir_gun}	6B86E64B15DA1
CRYPTOGRAPHY	**CRYPT050**	50	ŞA the DARKNIGHT	**439eec60a5ce2520a4078dac350c6e4b.zip flag.zip**	E	binary, base64, ceaser	STMCTF{Gotham_artik_daha_guvenli!}	EEF1795A3A93F
FORENSICS	**FOR175**	175	Farkı Bul	**c214364ee8d366a4170337c5216f498c.zip**	Y	compare, AES, exif, base64	STMCTF{F4rK!_H!sS3T}	E5AD35EA82CB7
CRYPTOGRAPHY	**CRYPT175**	175	Destek istiyorum Sizden	**c460e1ea3455bbf5b4253a8a7d5f55a5.zip**	Y	DES.MODE_ECB	STMCTF{takt1k_v1tes1_1e}	18687C9E52B40
WEB	**WEB050**	50	Odie	**6b51d5a125cf6c0eca3d1df3545b7d25.zip**	nl	Grep STM	STMCTF{YARI_Kor_Kedi_ODIE_nin_HAYATI}	AF0B157C01076
REVERSE	**RE075**	75	Beni Çalıştırma	**ac78fc90b6fb7e17ec2d35e09e7b008d.zip**	nl	IDA	STMCTF{_Hold_the_DOOR__}	697410045FF8C
MISC	**MISC125**	125	NURELLA	**67b99362ffe51662399a5c2bad15e284.jpg**	P	Jpeg metadata, XOR	STMCTF{Ay_ne_K4D4r_Y3r_yAndi!?!?!?}	8FBDA0AAC22A1
CRYPTOGRAPHY	**CRYPT100**	100	Disk Yuvarlak - Kod Kare	**f93f75f8cae4a51cdd9b491a7c11c69d.zip d02f7fa78908987a9460a4decbb1a927.png**	Ö	Kare Kod, Alberti Diski	STMCTF{DEREAEDIFICATORIA}	0D6C1AEA74D30
CODING	**CODE300**	300	calculator	http://192.168.MASANO.5:4444	P	math, base58, binary file, jpg	STMCTF{Python_N3yDi?_PYTHON_muTLuLuKtU}	4C23C161CEF2E
MISC	**MISC060**	60	Ook yaşa!	**09f16d5a13fcbeeedf6d6f3e5b8824bc.zip**	Ö	ook-language	STMCTF{ook_is_a_cool_language}	2FACDA7E08562
MISC	**MISC050**	50	Zafiyeti Bul		Ş	osint, git	STMCTF{MS17-010}	AA69084AA15EF
MISC	**MISC080**	80	Adresi Bul		Ş	osint, maps	STMCTF{Center_Park_Blvd}	2A14C77547E08
CRYPTOGRAPHY	**CRYPT200**	200	Balküpü	**f0fc1bc65d283fc5c065a364de26ebaa.zip**	Ö	padding	STMCTF{Padding_ yoksa_RSA_8192_bile_kirilabiliyor}	4A66DA3D026604
FORENSICS	**FOR200**	200	Köstebek	**ac6b6864c2dc3978c0a6a8cdba239dcd.zip**	A	pcap XMPP compress	STMCTF{alice_ve_bob_mesajlasmis_kostebek_eve_degil_miydi_?}	6F6C39A2BA5B27

kadar saklanması stresi bizlere bırakılmıştı. Yarışma panelinde bile bayrakların MD5 değeri olduğu için gerçek bayraklar sadece bu dosyada yazılıydı. Hazırlanan sorular hazırlayanlar tarafından defalarca kontrol edildi ve yine soruları hazırlayanlar tarafından sistem üzerinde bir yarışmacı gibi giriş yapılarak sorular çözüldü. Hem soruların hem de bayrakların kontrolünün kaç kere yapıldığını saymayı bırakmıştık. Hazırlık boyunca sorularda yapılan en küçük değişiklik bu süreci tekrar etmemize neden oldu. Hata istemiyorduk.

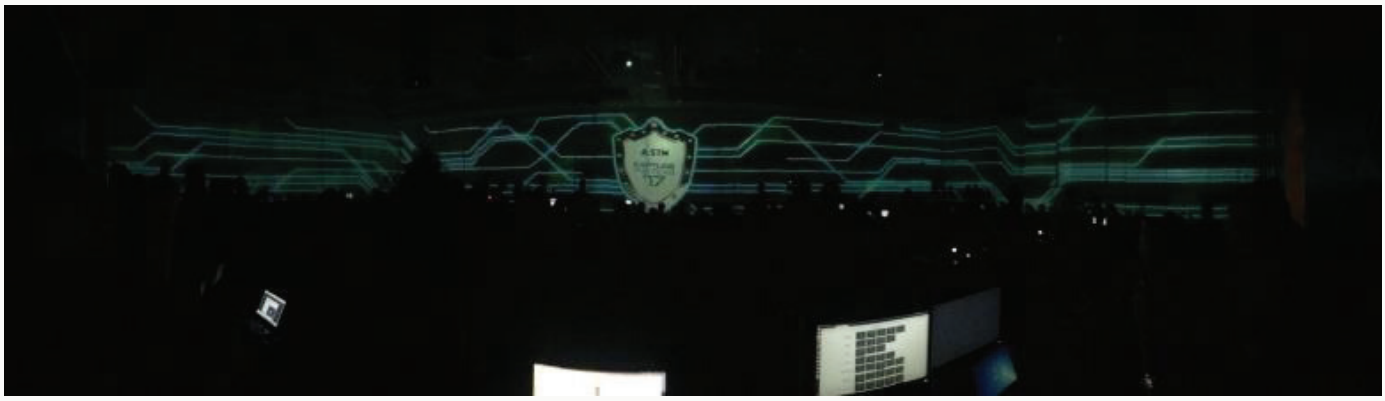


Bu sene her takıma ayrı bir sunucu vermeyi planlamıştık. Böylelikle yarışma süresince hiçbir takım başka bir takımın sunucusuna ulaşamayacak ve takımların sunucular üzerinde yapacağı işlemlerden diğer takımlar etkilenmeyecekti. Bu da bizlere yetmedi ve online soruları takımlara tahsis edilen sanal sunucu içerisinde ayrı "Docker container"ları içerisine yerleştirdik. Takımlar kendi içlerinde de farklı sorular ile uğraşırken kendi takım arkadaşını rahatsız etmeden farklı soruları çözebilecekti. Bu arada her takımın ayrı bir sanal ağda (VLAN) olması da bizim açımızdan ilave bir güvenlik önlemiydi.

Yarışma alanının hazırlanması 48 saatimizi aldı. Salonun ve altyapının kapasitesini zorlayarak 32 takım için oturma düzeni sağlayabildik. Sanallaştırma platformu, switch konfigürasyonu, masalara çekilen kablolar hepsi özenle yapıldı. Her masaya yedekli olması için ikişer CAT kablo çekildi. Asıl ve yedek switch'lere bağlandı. Acil durumda switch'ler arasında geçişlerin provası yapıldı.

Her kablonun ucunda her türlü sistemi ele geçirmeye hazır bir takım bulunacaktı ve işimizi şansa bırakmak istemiyorduk. İşi gücü bırakmış ve switch üzerinde pentest çalışmasına bile başlamıştık.

Çalıştığı zaman bir odayı ürettiği enerji ile ısıtabilen iki sunucu çalışmaya başlayınca keyfimiz yerine geldi. Hatların kontrolü, yük testi, panel kontrolü, soruların son kontrolleri derken yarışma sabahı geldi çattı.



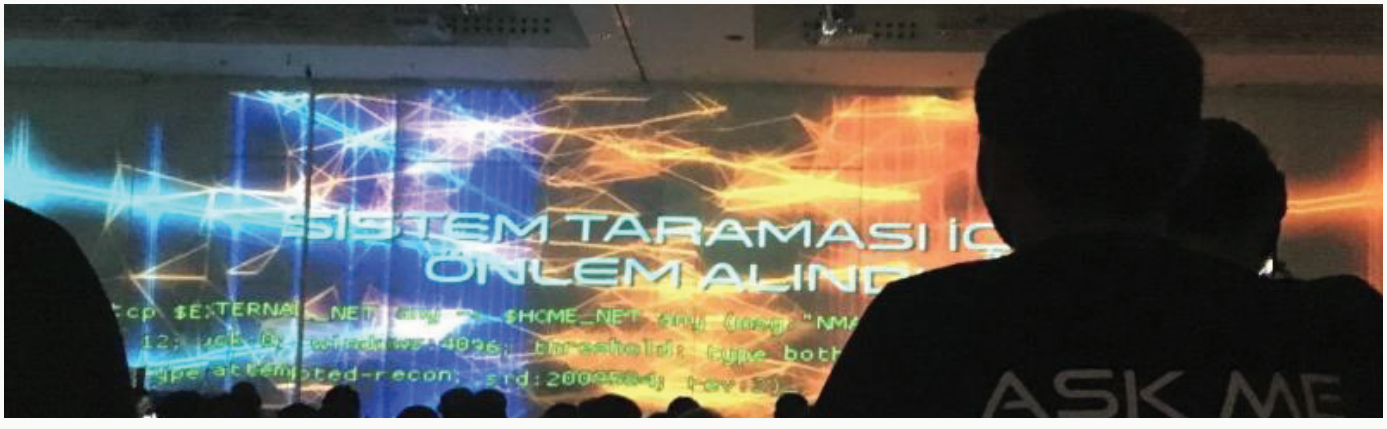
Yarışmanın 09.00'da başlayıp 17.00'de tamamlanması planlanmıştı. Saat 08.00'de takımları yarışma alanına almaya başladık. Takım olarak içeri giren takımın, bilgisayarlarını masada bulunan switch'e bağlayıp "Hoş geldin" sorusunu çözmesini bekliyorduk. Yarışma başlamadan önce en azından yaşanabilecek bağlantı sorunlarını çözerek yarışma başladığında olabildiği kadar az sorun ile karşılaşmak istiyorduk.

Hoş geldin sorusunu çözen "**KTO Siber**" ve "**noobtakim**" 08.20'de puan tablosuna 10'ar puanlarını yazdıran ilk takımlar oldu. Resmi olarak yarışma başlamamıştı ama puan tablosu ilk puanlarını alan yarışmacı takımlarının isimleri ile dolmaya başlamıştı. Hepimiz heyecanlıydık. Bu sene herkes panele yüklenince ne olacaktı, yarışmacıların sanal bilgisayarları ve Docker'lar umduğumuz gibi çalışacak mıydı? Sorularda hata var mıydı? Aklımıza gelemeyen başka bir yolla çözülen soru olacak mıydı?

Büyükşehir trafiği, yedek takımların yerleştirilmesi gibi işlemler neticesinde yarışmanın gecikmeyle saat 09:45'te başladı. İlk açılan soru, soruların babası "Faceless Flag"di. İlk açılan soru olmasına karşın yarışma sonuna kadar sadece "**Bulut**" takımı bu soruyu çözebildi ve takım olarak da bizlerin ayrıca takdirini kazandılar. İlk soruyu açtıktan sonra bir süre bekledik. Başka soru yayımlamadık. Tüm destek ekibi masalar arasında dolaşıp sorun yaşayan takımlar ile görüşüyordu. Admin masasında sunucuların yük durumları kontrol ediliyordu ve her şey yolundaydı. Soruları açmaya başlayabilirdik. Yarışma resmi olarak başlamıştı.

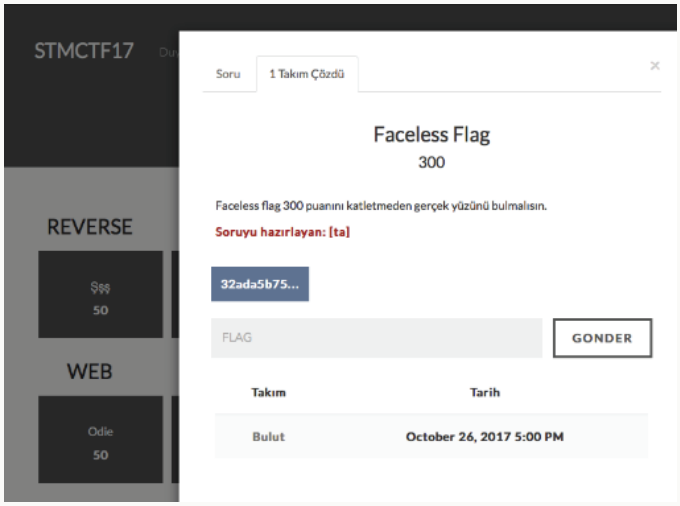
Toplamda 42 adet soru olunca tüm soruları aynı anda açmama kararı almıştık. Soruları 6 farklı gruba ayırdık. Kademeli olarak açılan sorular ile saat 12:00'de tüm sorular yarışma panelindeydi. Sorular açıldığında skorboard ekranlarında yeni soru yayınlandığı ikazı veriliyordu. Toplam soru sayısını açıklamamıştık ve yarışmada soru yağıyordu. İşte bu andan itibaren yarışma tam bir takım yarışmasına dönüşmüştü.

Şimdi de sizler ile CTF'17'de yarışan bazı takımlarımızın görüşlerini paylaşıyoruz.

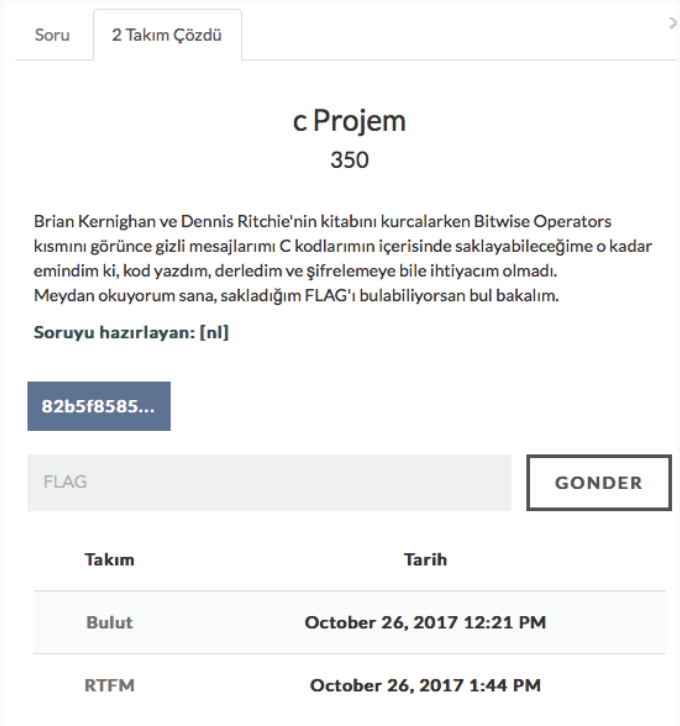


Emrah Demir, Bulut Takımı:

"Yarışmaya yedek grup olarak katıldık. O gün yarışmaya asıl olarak kabul edilip gelmeyen grup/grupların yerine girdik.



Yarışmanın öğrenci, kamu ve özel sektör fark etmeksizin ortak yapılması ne kadar zor olduğunu gösteriyordu. Grup arkadaşlarımın yaptığı sorular sayesinde sıralama olarak yukarılara çıktık. Ben kendim ilk başta "Faceless Flag" sorusunda çok vakit kaybettim. O soruyu bir kenara bırakıp bir web sorusuyla puanımıza iyi bir katkı sağladım. Web sorusunun puanı bizi yarışmaya tekrar bağladı. İyi bir motivasyon sağladıktan sonra "cProjem" adlı soruya yoğunlaştım ve çok geçmeden çözebildim. Sonra herkes kendisine uygun geldiği soruya yoğunlaştı.



Yarışmanın sonlarına doğru bizi çok heyecan sarmıştı. Sıralama çok değişkendi. Yapabileceğimizi düşündüğümüz sorulara vakit ayırdık. Panel kapandığında 5. sıradaydık. İlk üçe girmemiz için bize yüksek puanlı iki soru lazımdı, tabi 3. ve 4.'nün soru çözmemesi gerekirdi aynı anda. Düşük puanlı sorular çözüyorduk, ama panel kapatılınca tek çözüm yolumuzun "Faceless Flag" olduğunu düşündüm. Bu soruya çok vakit kaybetmiştim ve aynı zamanda her yolu denediğimi düşünüyordum. İyi odaklandıktan sonra ve tek çözüm yolumuzun bu olduğunu bilmemle beraber küçük bir şeyi gözden kaçırdığımı anladım. O an çok üzüldüm bu soruyu çok kısa sürede çözebilirmişim. Bu puan diğer grupların soru çözmediğini varsayarsak bizi 4'üncü sıraya yükseltiyordu.

Son anlarda bu yarışmaya yedek olarak katılıp yine de iyi bir sıralama yakalamanın verdiği mutluluk içerisindeydik. Başka soru çözmeden yarışma sona erdi. O an çok heyecanlıydık. Matematiksel olarak en iyi 4. sıradaydık, ama bir sürü soru vardı ve altımızdaki gruplar da soru çözmüş olabilirlerdi. Faceless Flag'i çözmenin verdiği rahatlık vardı bizde, çünkü "Faceless Flag" bu yarışmada en yüksek puanlı sorulardan biriydi. Sonuçlar gösterildiğinde 4. sıradaydık. "Faceless Flag" sorusunu çözmeseydim alt sıralara düşeceğimizi gördüm. Bu durum beni mutlu etmişti. 4. sıradaki grup başka sorular çözmüştü, ama "Faceless Flag" bizi dördüncülüğe yükseltmişti. Sorular çok güzel hazırlanmıştı. Yarışma çok iyi bir ortamda geçti.

Emre Toraman, NavSec Ekibi Adına:

"Öncelikle ülkemizde özellikle savunma sanayisi tarafında böyle bir organizasyonu yapan tek kuruluş olmanız dolayısıyla ekip arkadaşlarım adına sizleri tebrik ediyorum. Günümüzde bütün dünyanın dikkat çektiği önemli bir hususta bu işi özel sektör tekelinde bırakmak yerine devletimiz bünyesinde bulunan bir şirketin özel sektöre göre daha iyisini yapması gerçekten çok sevindirici, umarız bu çabalar daha da katlanır ve ülkemiz adına daha güzel gelişmeler sağlanır.

Yarışma süresince takım olarak yaşadığımız en güzel anlardan bir tanesi, bizlere dağıtılan su şişelerinin bir ipucu içermesi idi. Bir anlık düşünce ile baktığımız etiketin altında bulduğumuz ipucu sıralamada aşağılara düşmekte olan bizleri daha da heyecanlandırdı ve oyuna tekrardan katılmamızı sağladı.

Şahsi olarak içimin pek ısınmadığı Ankara'dan ilk defa bu kadar mutlu olarak ayrıldığımı söyleyebilirim. Yarışma, başından sonuna kadar bizleri gerçek bir mühendislik ve "Red Team" bakış açısıyla bakmamızı sağladı. Katıldığımız ilk CTF deneyimi olduğu için yarışma başlarında olan heyecanımız bizleri olumsuz etkilemesine rağmen yarışmadan mutlu ve ümit dolu ayrıldık.

Yarışmada emeği geçen herkese çok teşekkürler, seneye görüşmek dileğiyle."

scoreboard değişim sesi bizi kalp hastası yapıyordu. Playlist'ler ve sorularla coşan bedenlerimizi biraz kaldıralım eklemlerimiz açılsın diyerek aldığımız atıştırmalıklar birbirimize "bak bu da iyiymiş" dedirtirken acı ve gözyaşıyla kurutulmuş portakal ve kiviler suikast amaçlı üretilmiş gibilerdi. Yarışma sonrası ganimetleri sayarken herkesten "Benim çantamda flaş bellek yok!" çığlıkları yükseldi ve kimsede olmadığının anlaşılması hepimizi derin bir hüzne boğdu. Her şey için teşekkürler. "

Melih Tolga Şahin, Yubitsec Takımı:

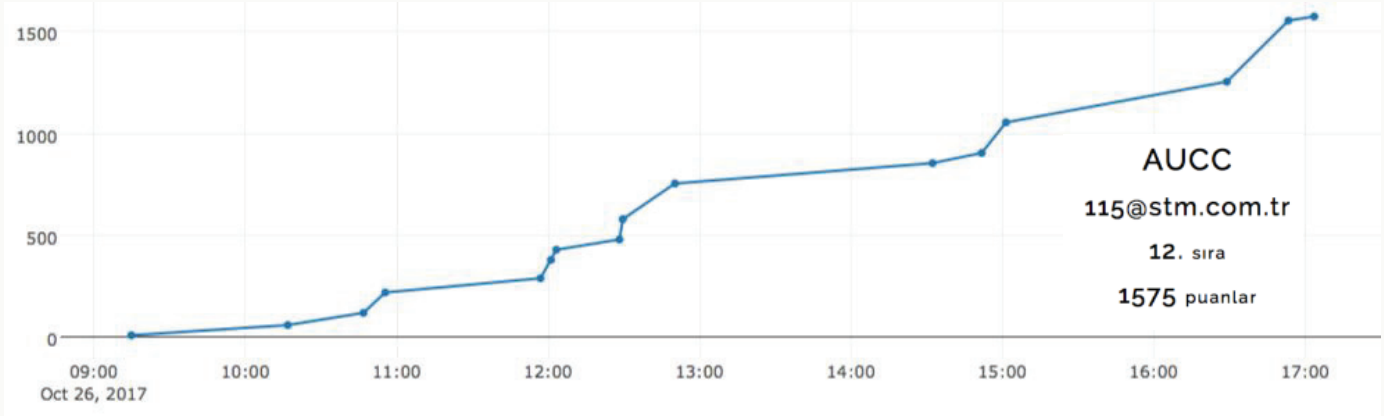
"Bizim için yarışma müthiş bir deneyim idi. Günü birlik İzmir'den geldik yarışmaya katılabilmek için. İlk kez fiziksel olarak yapılan yarışmaya katılma şansını yakaladık. Birçok grubu başka platformlardan biliyorduk, fakat rakiplerimiz ile fiziksel olarak da aynı yerde bulunmak bizi daha hırslandırdı ve keyiflendirdi.

Yarışmada ilk soru çözen takım bizdik yanlış hatırlamıyorsam, çözdükten sonra gelen "First blood!" sesi ve canlı tablo beni epeyce heyecanlandırmıştı. Bu heyecan sonrasında bir süre sıralamada ilk 3'te gidip geldik. Öğleden sonra

AUCC Takımı:

"Yarışma ortamı çok güzel, samimi ve beklentilerimizin üzerindeydi, en sakin anlarda gelen

1. sırada olduğumuz sırada insan kaynaklarından Yağmur Hanım masamıza uğradı. Tanıştık, uğramamızı istedi. O gittiğinde grupça birbirimize baktık, gülümsedik. Gurur vericiydi.



O sırada daha önce okul içinde bayrak yakalama etkinliklerinin tanıtımı için yaptığımız yarışmada kullandığımız platformun aynısı olduğunu fark ettik. Girilen bayrakların sisteme düştüğünü ve takip edildiğini biliyorduk.

Takım arkadaşım Süleyman bir sorunun cevabına "Kardeşim hint verir misin?" cümlesini girdi. Aramızda bu olaya gülerken, görevli personellerden biri gelip, "Buyrun hint istemişsiniz, noldu yahu?" diye tepkisi bizi kahkahaya boğdu.

Ben bir ara hava almaya dışarı çıkmıştım. O zaman fark ettim ki ateşim var. Sonra aşağıya gidip bu durumu diğer arkadaşlarıma söylüyordum ki diğer 2 takım arkadaşım da acayip hasta olmaya başlamış. Öksüre tıksıra soruları çözmeye çalışmaya devam ettik; fakat yarışmanın bitmesine 2 saat kala yol yorgunluğu ve hastalık bizi geri düşürdü. Öyle oldu ki kendi açımdan, bilgisayar ekranına baktığımda her şey dağılıyordu.

Her şeye rağmen çok mutlu ve keyifli ayrıldık. STM gibi başarılı firmaların İzmir'de olmamasından yakınarak ve hayıflanarak geri döndük."

Semih Demirci, RTFM Takımı:

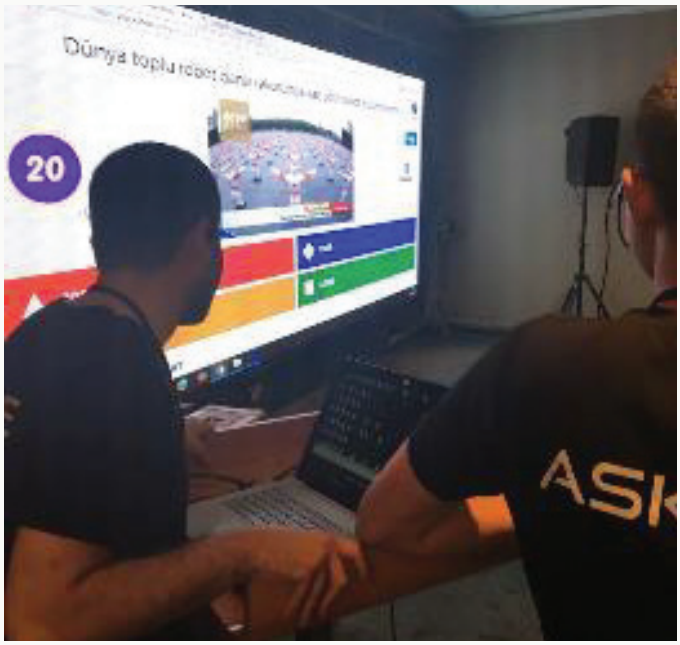
"Öncelikle gittikçe daha kaliteli bir hale gelen CTF yarışmanız için takımım adına tüm ekibinize teşekkür ederim.

Yarışmanın sonlarına doğru geldiğimizde bir taktik uyguladık ve 1'incinin 25 puan altına taşıdık kendimizi ve bu durumdan sonra çözdüğümüz soruların bulduğumuz flag'lerini sisteme girmedik.

Son yarım saat içerisinde gerçek puan değerlerinin yansıtılmaması ile birlikte daha da merak edilir bir durum oluşmuş oldu."

İzleyicilere Özel Yenilikler

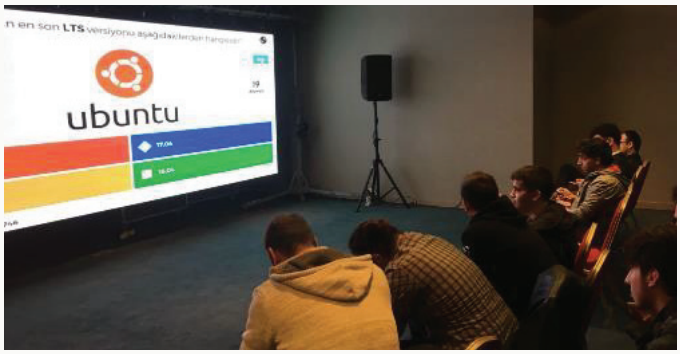
CTF yarışmalarını izlemek keyiflidir. Eğer yarışmacı değilseniz bu keyif kısa sürer. Bu sene STM CTF yarışmasına katılmayıp izleyici olarak gelenler için bir farklı aktivite arayışına girdik. CTF'ten farklı olmalı ama yine de bir yarışma havası taşımalıydı. STM İnsan Kaynakları tarafından yeni katılım yapan personel için düzenlenen temel oryantasyon eğitiminde kullanılan "Kahoot" uygulaması aklımıza gelmişti. Deneme soruları hazırladık ve Kahoot'a



yükledik. Ekipçe testini yapıyoruz, olabilecek aksaklıkları Kahoot konfigürasyonunda değişiklikler yaparak oynanabilir bir hale getirmeye çalışıyorduk.

Yarışma günü için 100'ün üzerinde soru hazırladık. Her saat başı izleyicilerin bulunduğu salonda ekrandan bilişim dünyası ağırlıklı sorular ile alternatif yarışma alanı oluşmuştu. Sorulara doğru ve en hızlı cevap veren yarışmacılar ufak da olsa ödül kazandılar.

Kahoot uygulaması üzerinden gerçekleştirdiğimiz Quiz yarışmasında izleyiciler cep telefonları ile yarışmaya katıldılar. Yarışma alanında bulunan dev ekranda beliren sorulara cep telefonundan en hızlı ve doğru cevabı vermek için çekişmeli anlar yaşandı.

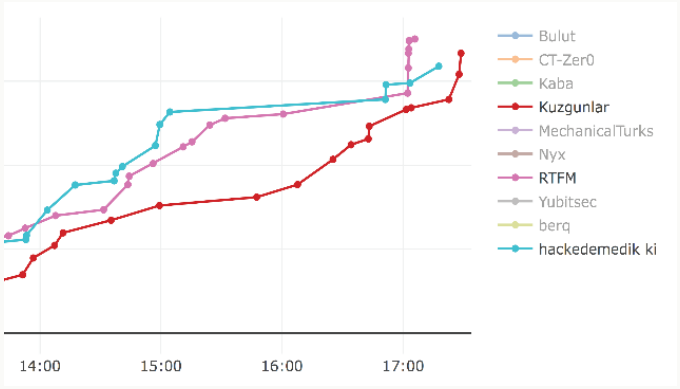


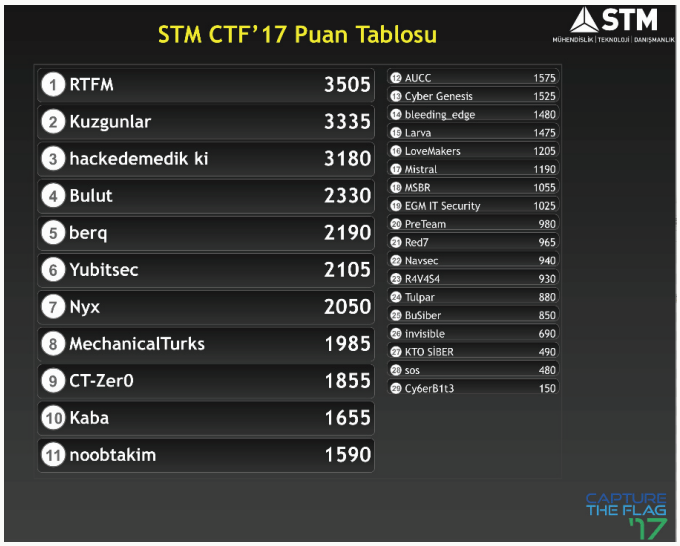
Yarışma Sonu

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 içerisinde bayrak saklayan takımlar bayrak girişlerini yaptı ve son 5 dakika içerisinde bazı takımlar son ataklarını gerçekleştirdiler ve yarışma bitti; ancak biz puan tablosunu açıklamayıp tam bir Oscar ödül töreni gibi birinciyi açıklamak istiyorduk. Yarışma sonunda konuşmalar yapılıyordu. İlk 3'e giren takımların isimlerini zarflara yazıp açıklanması için teslim ettikten sonra şöyle bir soru geldi. "Puan tablosunu Refresh yaptın değil mi ?" :) Kısa bir sessizlik, korku ve heyecandan sonra o kısa sürede bayrak girişleri dâhil bütün kontroller yapıldı ve Oscar töreninde yaşanan talihsizlik gibi bir durumla karşılaşmadık. :)

Yarışmanın son 30 dakikasında ilk 3'ün sıralaması tamamen değişmişti. "**RTFM**" takımı bayrak saklamış ve elindeki 6 bayrağı son yarım saatte girerek birinciliğe yükselmişti.

"**Kuzgunlar**" ve "**hackedemedik ki**" takımları, birbirlerini geçme çabalarındaydılar. "**Kuzgunlar**" takımı tecrübesi ile son dakikalarda çözdükleri iki soru ile ikinciliğe yükselmiş ve puan tablosu kapanmadan önce birinci olan "**hackedemedik ki**" takımı üçüncülüğü almıştı.





Ödül töreni sonrasında dereceye giremeyen bir yarışmacıya da iPad hediyemiz oldu.

Yarışmacı panelinde toplamda 44 soru gözükmesine karşın Anket ve Hoş Geldin soruları dışında 42 adet soru sorduk.

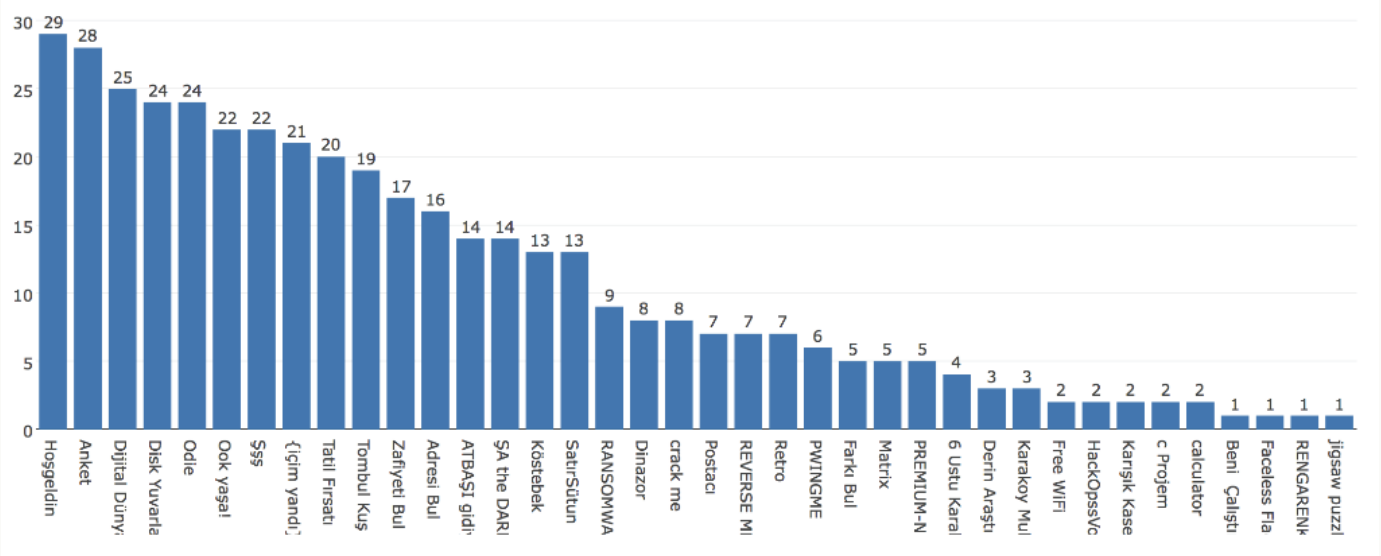
Yarışma bitimine yakın puanlı anket sorusuna verilen cevaplardan En Sevdiğiniz Soru olarak "Retro", "ATBAŞI gidiyorlardı", "Tatil Fırsatı" ve "{içim yandı}" birinciliği %8.1 oy ile paylaştılar. Soruları hazırlayan arkadaşlara buradan bizler tekrar teşekkür ediyoruz.

En sevmediğiniz soru olarak %13.1 ile "NURELLA", %8.1 ile de "Postacı" ve "Faceless Flag" yer almıştır.

En zor soru kategorisinde ise %10.8 ile "Faceless Flag" ve "Postacı" birinciliği paylaşmıştır. :)

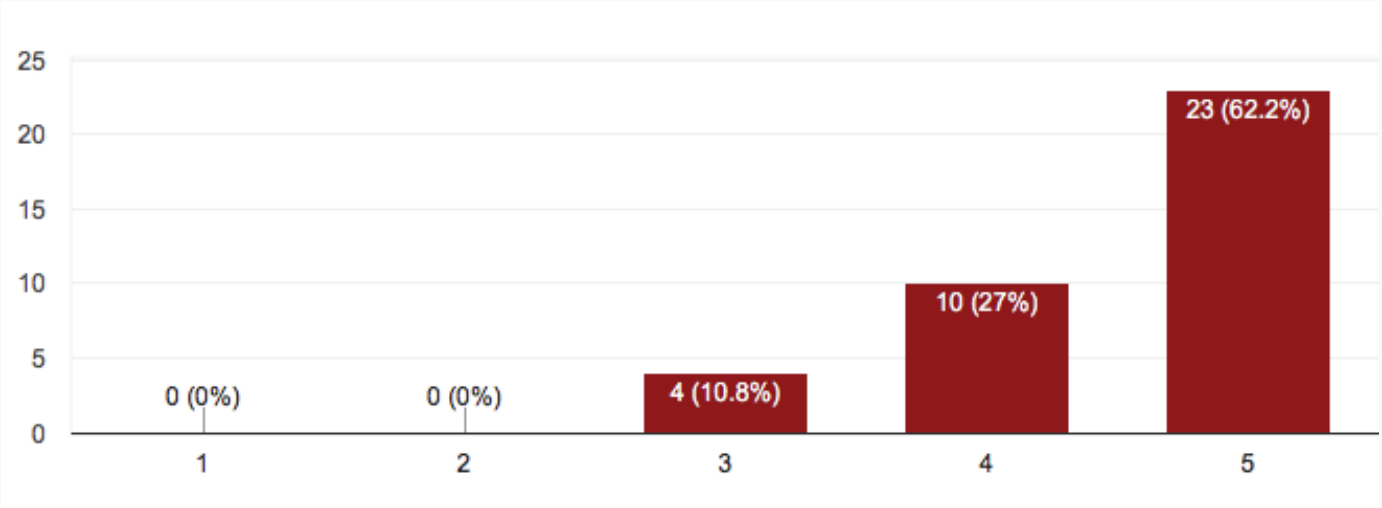
Soruları ve çözümleri https://github.com/stmctf/stmctf17 adresinden paylaştık. Google'da "STMCTF'17 Writeups" olarak da aratabilirsiniz.

Hiç çözülemeyen "NURELLA", "Destek istiyorum Sizden", "encodingLoop", "LFSR64", "Balküpü" ve "ENCODEDECODE" soruları dışındaki soruların kaç takım tarafından çözüldüğü bilgisini de sizlerle paylaşmak istiyoruz.

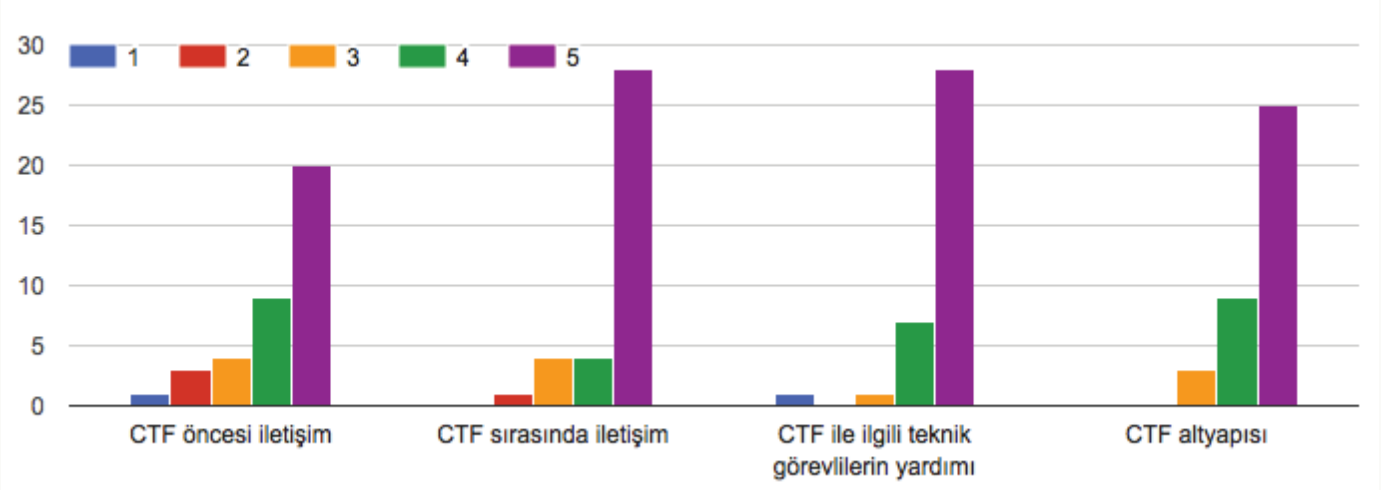


Yarışma sonuna doğru yarışmacıların doldurduğu anket için teşekkür ederiz. Anket sonuçlarını aşağıda bulabilirsiniz.

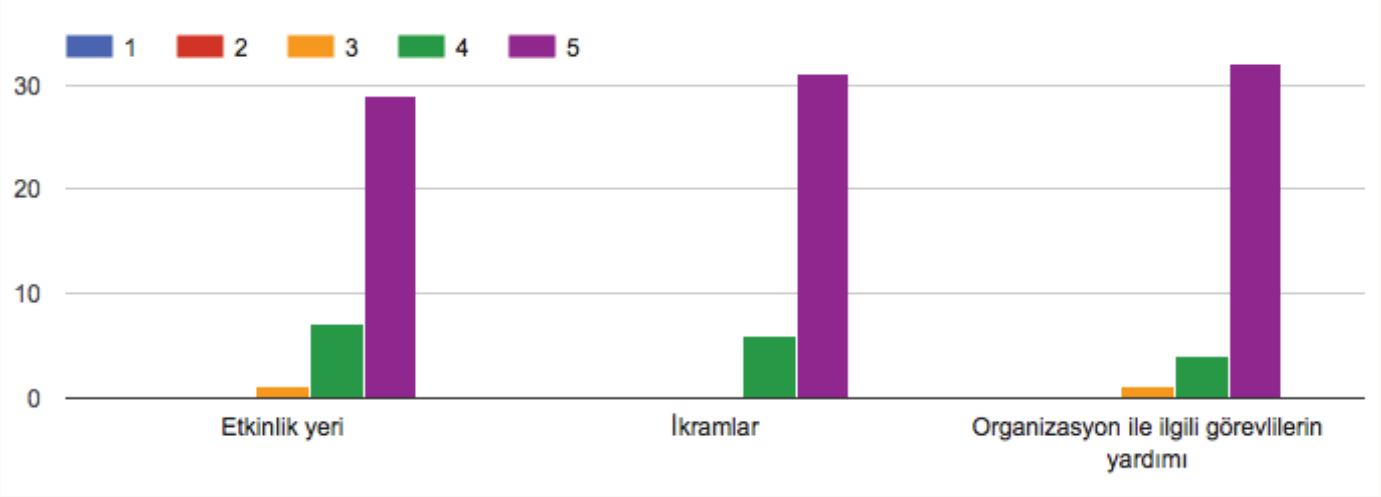
Etkinlik sizce nasıldı?



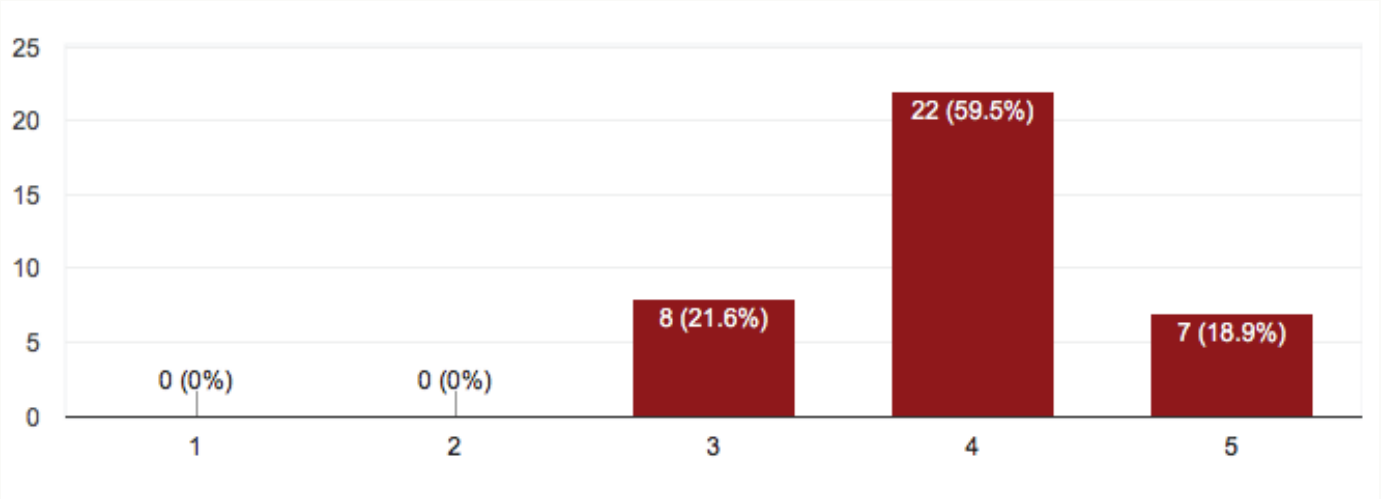
CTF'i değerlendiriniz:



Organizasyonu değerlendiriniz:



CTF sorularının zorluk derecesi?



Etkinlik hakkındaki düşünceleriniz

- Güzel (3).
- Süper.
- Süper ama İngilizce
- Çok iyiydi.
- Her şey çok güzeldi, çok iyi bir tecrübe oldu, seneye görüşmek üzere.
- Güzel bir etkinlik oldu. Tüm her şey için teşekkür ederiz.
- Gayet başarılı bir etkinlik oldu çok teşekkür ederiz.
- Fena değildi, teşekkürler.
- Very nice ;D (STM hep CTF yapsın.)
- Çok güzeldi.

• Etkinliğin daha kapsamlı ve büyük bir yarışma haline gelmesini istiyorum. Ödülleri de gittikçe artırabilirsiniz. Yarışmacıları da üniversite ve sektör olarak ayırsanız çok daha iyi olabilir, teşekkürler.

• Gayet iyiydi.

• Sorular hariç güzeldi.

• Keyifliydi.

• Emeğinize sağlık.

• Mükemmel.

• Etkinlik çok başarılıydı devamını bekliyoruz.

• Güzeldi.

• Gayet güzeldi.

• Güzel bir etkinlik.

• Bence daha sık yapılmalı.

• Güzel bir etkinlik, seneye tekrar katılacağım.

• Başarılı.

• Keyifli bir etkinlikti, ambiyans ve organizasyon gerçekten güzeldi.

• Harikaydı.

• İyi, devam etmeli.

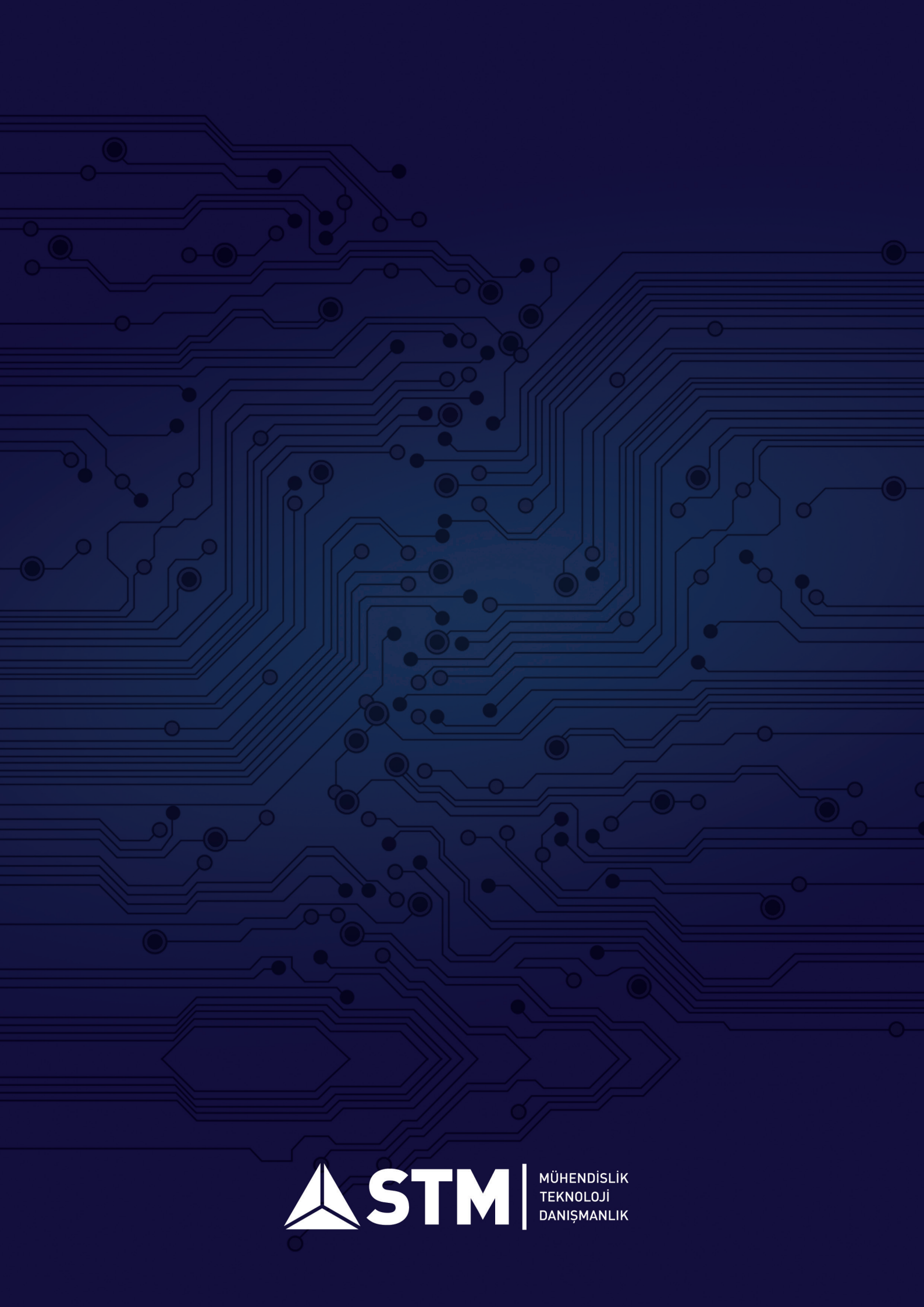
• Güzeldi bence.

• Güzeldi.

• Sevdim.

Büyük başarılar ancak uyumlu bir ekip çalışması ile kazanılabilir.

STM CTF'17 Ekibi


STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK