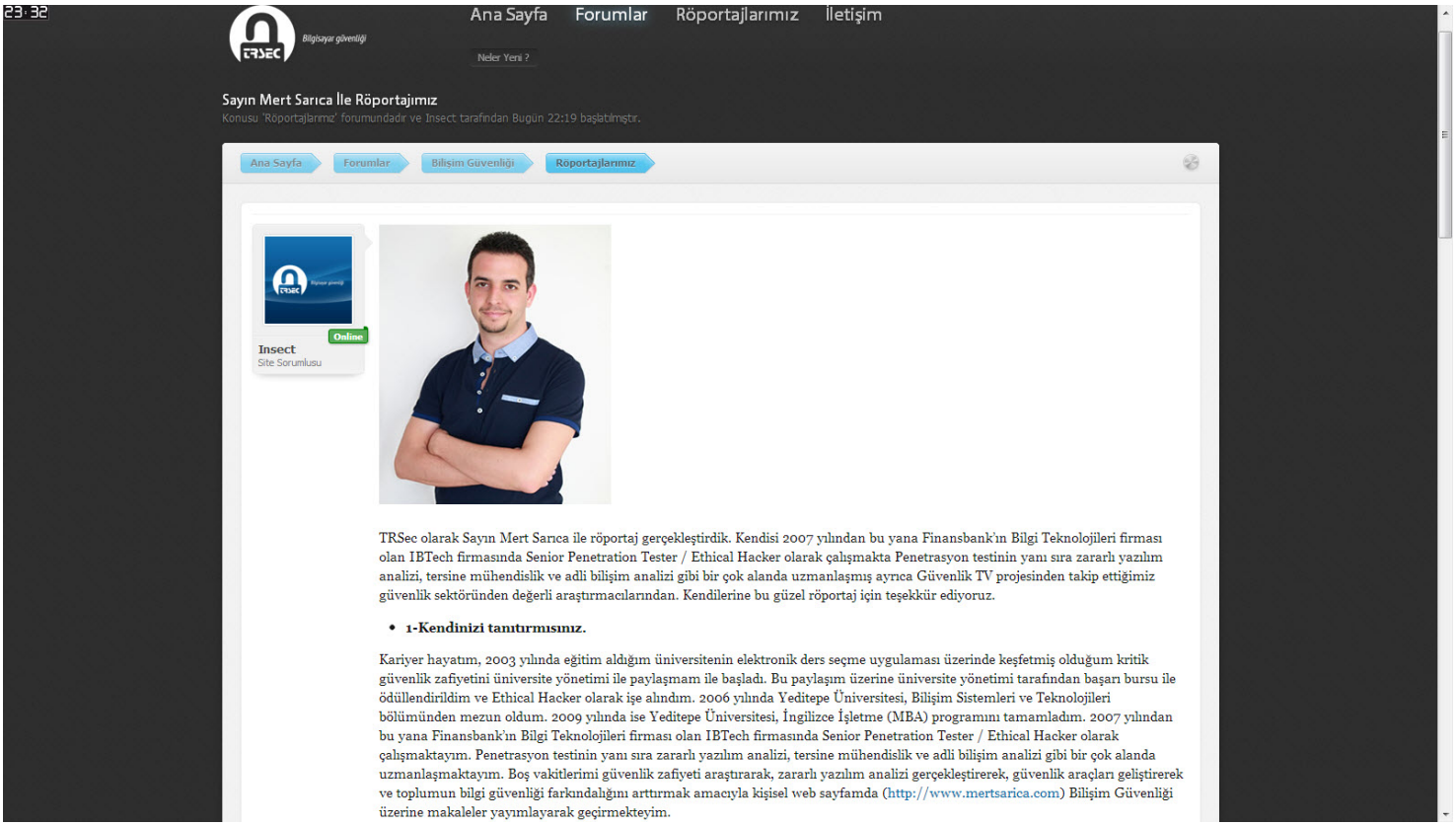

TRSec olarak Sayın Mert Sarıca ile röportaj gerçekleştirdik. Kendisi 2007 yılından bu yana Finansbank'ın Bilgi Teknolojileri firması olan IBTech firmasında Senior Penetration Tester / Ethical Hacker olarak çalışmakta Penetrasyon testinin yanı sıra zararlı yazılım analizi, tersine mühendislik ve adli bilişim analizi gibi bir çok alanda uzmanlaşmış ayrıca Güvenlik TV projesinden takip ettiğimiz güvenlik sektöründen değerli araştırmacılarından. Kendilerine bu güzel röportaj için teşekkür ediyoruz.

- **1-Kendinizi tanıtırmısınız.**

Kariyer hayatım, 2003 yılında eğitim aldığım üniversitenin elektronik ders seçme uygulaması üzerinde keşfetmiş olduğum kritik güvenlik zafiyetini üniversite yönetimi ile paylaşmam ile başladı. Bu paylaşım üzerine üniversite yönetimi tarafından başarı bursu ile ödüllendirildim ve Ethical Hacker olarak işe alındım. 2006 yılında Yeditepe Üniversitesi, Bilişim Sistemleri ve Teknolojileri bölümünden mezun oldum. 2009 yılında ise Yeditepe Üniversitesi, İngilizce İşletme (MBA) programını tamamladım. 2007 yılından bu yana Finansbank'ın Bilgi Teknolojileri firması olan IBTech firmasında Senior Penetration Tester / Ethical Hacker olarak çalışmaktayım. Penetrasyon testinin yanı sıra zararlı yazılım analizi, tersine mühendislik ve adli bilişim analizi gibi bir çok alanda uzmanlaşmaktayım. Boş vakitlerimi güvenlik zafiyeti araştırarak, zararlı yazılım analizi gerçekleştirerek, güvenlik araçları geliştirerek ve toplumun bilgi güvenliği farkındalığını arttırmak amacıyla kişisel web sayfamda (http://www.mertsarica.com) Bilişim Güvenliği üzerine makaleler yayımlayarak geçirmekteyim.

- **2-Kendilerini "güvenlik uzmanı" sıfatıyla tanıtan, sektörde yer bulamadığı gibi bir takım medya kuruluşlarına demeçler veren kişiler hakkında ne düşünüyorsunuz. Sizce medya daha çok yanlış kişilere mi söz hakkı tanımakta.**

Aslında bu konuda genelleme yapmak pek doğru olmayacaktır çünkü ben de dahil olmak üzere güvenlik sektöründe yer alan birçok uzman arkadaşım, güvenlik ile ilgili konularda, yazılı, görsel ve internet medyasında zaman zaman röportajlar ve demeçler vermekteyiz. İlgili veya ilgisiz kişilere söz hakkı tanıma kısmı aslında medya kuruluşunun haber politikasına göre değişmektedir. Politikası sadece rating olan bir medya kuruluşunun "Ben Superman'im" diyen herkese mikrofon uzatması, ısmarlama haber yapması çok yadırganmamalıdır. Haberin doğruluğuna önem veren bizler için doğruluğuna, objektifliğine inandığımız medya kuruluşlarını ve uzmanları takip etmek bizler için en doğru yol olacaktır.

- **3-Güvenlik sektöründe yer alan kişiler blog adreslerinde bilgilendirici içerikler paylaşmakta, fakat bunlar daha çok temel anlamda yararlı oluyor, bu konuda araştırma yapmak için yabancı dil bilinmesinin önemi nedir ?**

Bu işin olmazsa olmazlarının başında İngilizce belki de ilk sırada yer almaktadır. Bilişim güvenliği alanında ilerlemek isteyen ve bu konuda bana e-posta gönderen birçok öğrenci arkadaşıma, herşeyi bir kenara bırakıp öncelikle İngilizce öğrenmeleri gerektiğini söylüyorum. Baktığınız zaman, bilişim güvenliği uzmanı olmanın temeli bol bol okumak ve bol bol pratik yapmaktan geçiyor ancak sizin de dikkat çektiğiniz gibi yerli kaynak sıkıntısı nedeniyle çoğumuz kendimizi yabancı kaynakları takip ederek geliştirebiliyoruz. Her ne kadar benim gibi birkaç arkadaşım, vakitleri ve imkanları el verdiği sürece, yeri geldiğinde basit, yeri geldiğinde ileri düzey yazılar yazsalar da, yazanların sayısının az olması nedeniyle kendini geliştirmek isteyenler için yabancı kitaplar, dolayısıyla İngilizce bilmek, bu alanda çok büyük bir öneme ve önceliğe sahip oluyor.

- **4-Firma ve kuruluşlara bir takım pentest ve güvenlik danışmanlığı hizmeti veren yapıların ülkemizde durumlarına baktığımız da bu hizmetlere rağbet sizce ne düzeyde ? Özel şirketler bu hizmetleri artık olmazsa olmaz boyutunda mı değerlendiriyor ?**

Bugün baktığımızda güvenlik danışmanlığı, sızma testi hizmeti, kurum içi sızma testi ekibinin oluşturulması gibi konular firmanının vizyonuna ve tabi olduğu regülasyona göre değişiklik göstermektedir. Kimi firmalar regülasyonlarla kendilerini sınırlı tutarken (yılda 1 defa sızma testi yaptırılması), müşterilerinin güvenliğine önem veren vizyoner firmalar ise bu işi çok daha ciddiye alarak yeri geldiğinde sızma testi yapan yeri geldiğinde projelerde danışmanlık veren ekipler oluşturmaktadırlar. Son yıllarda artan siber saldırılar, güncellenen regülasyonlar ile firmalar için bu ve benzer hizmetlerin alınmasının zaruri olduğu bir gerçektir.

- **5-Zararlı analizleri, blog adresinizi incelediğimiz kadarıyla sizin de ilgi alanınız, Olmazsa olmaz araçlarınız neler ? Örneğin hangi sanal makina yazılımını daha çok kullanıyorsunuz ? Kendi oluşturduğunuz lab ortamınızda hangi araçlar öne çıkmaktadır.**

Aslında boş vakitlerimde ilgilendiğim zararlı yazılım analizi, Fatmal gibi internet bankacılığı müşterilerini hedef alan zararlı yazılımların artması ile işimin de bir parçası haline gelmiştir. Zararlı yazılım analizin en önemli kısmı belki de izole bir laboratuvar kurulmasıdır. Doğru şekilde izole edilmeyen bir laboratuvar, analiz etmeye çalıştığınız zararlı yazılımın mağdurları arasında yer almanıza yol açabilir. Zararlı yazılım analizini yerine göre VMWare içinde kurulu olan Windows XP, Windows 7 ve/veya Remnux işletim sistemleri üzerinde gerçekleştiriyorum. Sıkça kullandığım araçların başında, Sysinternals'ın araçları, OllyDbg ve eklentileri, Immunity Debugger ve IDA Pro yer alıyor. Daha fazlasını merak eden okuyucular, Euroforensics, KKTC ve İstanbul Siber Güvenlik Konferansları'nda gerçekleştirdiğim Ofansif Zararlı Yazılım Analiz sunumuma göz atabilirler.
(http://www.mertsarica.com/sunumlar/Ofansif_Zararli_Yazilim_Analizi.pdf)

- **6-Ülkemizden gerçekleştirilen siber saldırılara tarih olarak bakacak olduğumuz da bundan 5-6 yıl öncesine dayanıyor. Sizce bu konunun artık bu kadar sık anılmasının nedeni sizce nedir ? Saldırılar daha mı komplike olmaya başladı yoksa bir takım gruplar sayesinde mi bu saldırılar ün kazandı.**

Bugün baktığımızda medyaya yansıyan çoğu hacking haberinin ardında SQL Injection zafiyetinin istismar edilmesi yer alıyor. SQL Injection zafiyetinin 1999 yılında keşfedildiğini ve bundan 15 sene sonra halen sistemlere sızmak ve veri çalmak amacıyla kullanıldığını düşündüğümüzde saldırıların ileri seviye olduğunu söylemek çok doğru olmayacaktır. Siber saldırıların ve tehditlerin öneminin artmasının en önemli sebebi, geçmişte yerinde yapmamız gereken işlemleri artık uzaktan yapabiliyor olmamızdır yani çoğu sistemin internet üzerinden hizmet verebilir hale gelmesi, dolayısıyla siber saldırılara açık hale gelmesidir. Sistemler internet üzerinden hizmet verdikçe, geçmiş yıllara kıyasla hacking bilgisine erişmek, bu bilgileri paylaşmak kolaylaştıkça, güvenliği farkındalığı artmadıkça, organize suç örgütleri, hacktivistler, script kiddieler, siber teröristlerden tarafından gerçekleştirilen ve başarılı olan siber saldırılar gündemimizi meşgul etmeye devam edecektir.

- **7-Bir takım gizlilik yöntemleri özellikle Türkiye'de aktif olan Phorm sonrası sıkça kullanılmaya başlandı. Genel olarak baktığımız da Tor yapısının güvensizliğinden Tor kullanıcılarının bilgilerinin kolaylıkla elde edildiğinden söz edilir. Siz bu konuda ne düşünüyorsunuz. Sizce Tor güvensiz ve gizlilik sağlamayan bir yapımıdır ?**

Bugün baktığınızda ne %100 güvenli bir uygulama, ne %100 güvenli bir işletim sistemi, ne de %100 güvenli bir ağ vardır. Dolayısıyla TOR 'un da çeşitli zafiyetleri, zayıf noktaları vardır, olmaya da devam edecektir. Internet üzerinden yapacağınız haberleşmelerin, dahil olacağınız ağların %100 anonim olması teorikte mümkünse gibi görünse de bence pratikte mümkün değildir. TOR üzerinde yapılan çeşitli güvenlik analizleri de bunu ortaya koymaktadır. Örneğin bir saldırı yönteminde, TOR Exit node üzerine kurulan bir ağ analiz aracı ile kullanıcı adı ve şifreler ele geçirilebilmiştir. Bir diğer saldırı yönteminde ise TOR ağı üzerinde yer alan Bittorrent kullanıcılarının IP Adresleri tespit edilebilmiştir. Kısaca TOR'un yerine göre gizlilik sağlayabildiği noktalar olduğu gibi sağlayamadığı noktalar da mevcuttur.

- **8-Uzun süredir Skype kullanıcılarının konuşmaları AES-256 şifreleme tekniğinle korunduğundan söz edildi. Yapılan incelemeler sonucunda Microsoft'un bir takım HTTP ve HTTPS verilerini kendi sunucularına aktardığı görüldü. Bu konu hakkında düşünceleriniz neler. Artık Jabber gibi bir takım şifrelemelerin eklentilerle kullanıcı tarafından yapıldığı ve kişisel sunucu tarafına kurabiliceğiniz daha esnek platformlara geçiş dahamı doğru mu olacaktır.**

Bence burada gözden kaçan bir nokta var o da vadedilen korumanın neye ve kime karşı olduğunun kullanıcılar tarafından yanlış anlaşılmasıdır. Burada bahsi geçen koruma (şifreleme), ağ üzerinden iletilen verinin şifrelenmesi ve yetkisiz kişiler tarafından izlenmesini engellemektedir. Bugün Microsoft firması bu sistemin sahibi, yetkilisi ise, mahkeme kararı ile iki kişi arasında geçen bir haberleşmeye ait bilgileri mahkeme tarafından talep edilmesi durumunda bu bilgileri mahkemeye iletmekle yükümlüdür. Aynı durum telefon görüşmeleri için de geçerlidir. Bugün cep telefonu ile yaptığınız görüşme de GSM operatörüne kadar şifreli olarak iletilmektedir ancak mahkeme kararı ile bu görüşmelere ait bilgiler kayıt altına alınabilmektedir. Eğer aksi durum söz konusu olsaydı telefon görüşmesi yapan, Skype üzerinden haberleşen suçlular hiçbir zaman yakalanamazdı. Eğer amacımız alıcı ile verici (kişiler veya sistemler) arasındaki haberleşmenin gizliliğini sağlamak, 3. kişilerin bu verileri izlemesini engellemek ise ise bu durumda şifreleme anahtarının sadece alıcı ve verici tarafından bilinmesini ve haberleşme esnasında kullanılan verilerin bu anahtar ile şifrelenmesini sağlamak olacaktır.

- **9-Blackmarket sitelerinin 2005 sonrası bir takım uluslararası yapılan operasyonlarla kapatıldığı, kurucularının yakalanıp yargılandığını görmekteyiz. Sizce bu yapılan operasyonlar blackmarket alanını giderek küçültüyor mu ? Deepweb kısmına bu alanın yöneldiği söz konusumudur ?**

Blackmarket sitelerine gösterilen ilgili ve bu siteler üzerinden elde edilen kazançlar yüksek olduğu sürece kapananların yerine yenilerinin açılması devam edecektir. Blackmarket'in Deepweb'deki yansısı her ne kadar anonim paylaşımlar için tercih edilebilir gibi görünse de, bu işten kazanç sağlamak isteyenler bir noktada anonimliklerinden ödün vermek zorunda kalacaklarından ötürü Blackmarket'in DeepWeb'e tamamiyle yönelmesini kısa vadede çok gerçekçi bulmuyorum.

- **10-TRSec hakkında düşüncelerinizi alabilirmiyiz.**

Forumunuzda, doğru bilgilerin düzeyli bir şekilde paylaşılmasına özen göstermenizi, gerçekleştiğiniz röportajlarda seçici davranmanızı oldukça beğeniyor ve takdir ediyorum.