Mutlu Yıllar

written by Mert SARICA | 1 January 2014

İyisiyle, kötüsüyle, zararlısıyla, hackerıyla, uzun bir yılı geride bırakıyoruz. Siber güvenlik adına son 1 yılda ülkemizde ciddi çalışmalar yapıldı, adımlar atıldı.

Belki de bunlardan en önemlisi, resmi gazetede Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın yayınlanması oldu.
Bu eylem planı sayesinde siber güvenlik uzmanlarının yetiştirilmesine daha çok önem verilmeye başlandı. Üniversitelerde siber güvenlik eğitimleri yaygınlaştırılmaya başlandı. Siber güvenlik tatbikatlarına, yarışmalarına hız verildi. Ulusal Siber Olaylara Müdahale Merkezi (USOM) kuruldu kısaca saya saya bitiremeyeceğimiz birçok adım atıldı, gelişme yaşandı.

Yumurta kapı misali, hacking haberleri ve zararlı yazılım salgınları ile kurumların bilgi güvenliği farkındalığı artmaya başladı. Geçtiğimiz yıllara oranla sızma testi uzmanlarına talep daha da arttı. Bugüne kadar başımıza ne geldi, 10 işi yapıyorsun, sızma testi de 11. işin olsun, IPS & AV & Web & E-posta Ağ Geçidi çözümü kullanıyorum, bana birşey olmaz diyen zihniyetin yavaş yavaş işin ciddiyetini kavradığı, müşteri güvenliği ve regülasyon bir yana, zedelenen kurumsal itibarın yedekten dönülemeyeceği net olarak anlaşılmaya başlandı.

Yukarda da belirttiğim üzere geçtiğimiz yıllara oranla sızma testi uzmanlarına talep daha da arttı. Fakat buradan siber güvenlik uzmanlarını, sızma testi uzmanlarını kurnaz insan kaynakları danışmanlık firmalarına karşı uyarmakta fayda var. Kimi danışmanlık firmaları, Linkedin üzerinden grep CEH, grep CISSP yaparak sizinle iletişime geçiyorlar ve güvenlik uzmanı arayışı içinde olduklarını ve hemen yüz yüze görüşmek istediklerini iletiyorlar. Bunun nedeni ise kimi danışmanlık firmalarının her görüşme için, arayışta bulundukları firmadan komisyon almaları oluyor dolayısıyla sizi zaman zaman alakasız pozisyonlar için dahi görüşmeye davet etmekten çekinmiyorlar. Buna karşı, karşı tarafa 3 soru sormakta fayda var; 1- Pozisyon nedir ? 2- İş tanımı nedir ? 3- Düşünülen ücret aralığı nedir ? Bu 3 soru karşısında mavi ekran vermiyorlarsa görüşmeye gönül rahatlığıyla devam edebilirsiniz :)

2013 yılı benim için bol bol sızma testi, zararlı yazılım analizi, blog yazısı, sunum, teknik çalışma ve Güvenlik TV ile geçti. Hacking haberleri sayesinde sızma testinin kurumlar için önemine dikkat çekmenin artık anlamsız

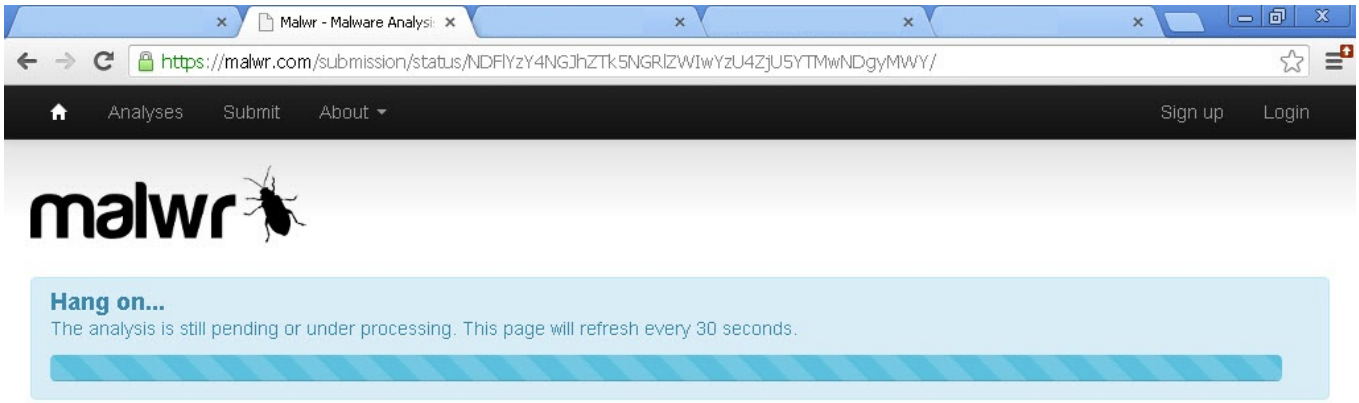
olduğu şu günlerde, zararlı yazılım analizinin kurumlar için (özellikle bankacılık sektörü) ne kadar önemli olduğu, yıl içinde gerçekleşen ve sadece Türkiye'yi hedef alan Fatmal, Hesperbot gibi salgınlarda daha çok anlaşıldı. Özellikle FatMal salgınında, komuta kontrol merkezinden cep telefonuna zararlı yazılım bulaşmış müşterileri tespit edebilmenin, müşteri güvenliği adına ne kadar önemli olduğunu kendi adıma tecrübe etmiş oldum. Yıl içinde yazdığım teknik yazılardan aldığım olumlu geri dönüşler sayesinde motivasyonumu yüksek tutabildim ve her ay en az 1 yazı yazmaya özen gösterdim. Halil ÖZTÜRKCİ ile gerçekleştirdiğimiz, birbirinden değerli konuklarımız ile güvenlik dünyasında olup bitene yer verdiğimiz Güvenlik TV ile bir yılı geride bıraktım. Üniversitelerden gelen konuşma davetlerini elimden geldiğince kabul etmeye çalıştım. Mesafelerin engel olduğu zamanlarda, Skype imdadımıza yetişerek yine siber güvenliğe meraklı, ilgi duyan öğrenci arkadaşlarla görüşmeler gerçekleştirebildim. Yıl içinde bol bol "nereden, nasıl başlamalıyım, nasıl ilerlemeliyim ?" sorularını içeren e-postalara elimden geldiğince detaylı yanıtlar vermeye çalıştım. Eğitici ve öğretici yazıların ve sunumların yetersiz kaldığı noktaları doldurabilme adına, Zararlı Yazılım Analizi 101 dersi (2014 Şubat ayı itibariyle) vermek için Bahçeşehir Üniversitesi'nin Siber Güvenlik Yüksek Lisans Programı'na katıldım.

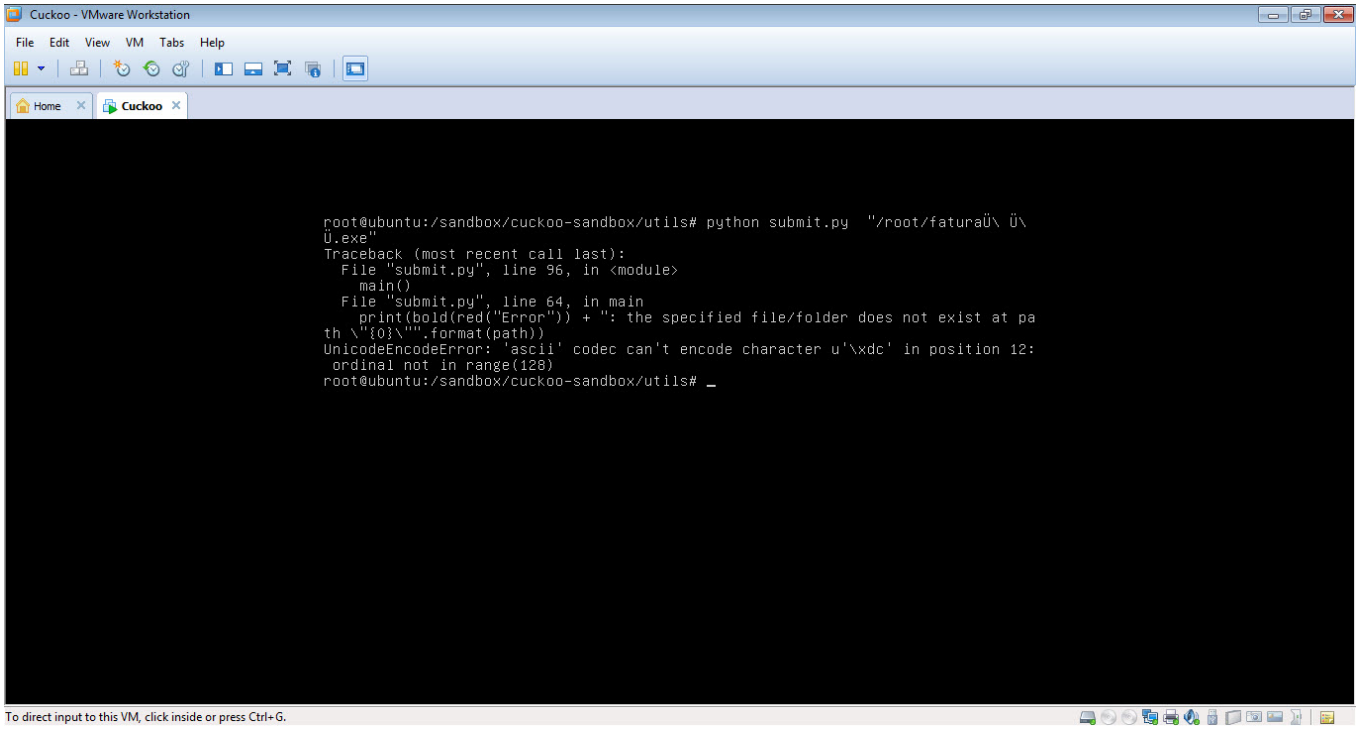
2013 yılını, geçtiğimiz günlerde keşfettiğim, çam sakızı çoban armağanı bir zafiyetle kapatmak istedim. Herkesin bildiği gibi zararlı yazılım analizinde, en kısa sürede sonuca yani zararlı yazılımın sistem, ağ üzerindeki etkisini anlamak için çeşitli dinamik, statik, kod ve bellek analiz yöntemlerinden faydalanırız. Dinamik analizde kum havuzları (sandbox), analizin olmazsa olmazlarındandır. Özellikle açık kaynak kodlu Cuckoo Sandbox, (çevrimiçi sürümü ile Malwr) bu analizin vazgeçilmezidir. Ancak her zaman söylenildiği gibi dinamik ve statik kod analizi yapılmadığı sürece sistemsel dinamik analiz ile elde edilen bilgilerin doğruluğundan tam olarak emin olamazsınız.

Bunu farklı bir örnekle ortaya koymak ve bu konuda farkındalığı arttırmaya yardımcı olabilmek adına malwr.com'da hizmet veren Cuckoo Sandbox ile biraz oynamaya başladım. Güvenlik testlerinden bugüne dek tecrübe ettiğim kadarıyla çoğunlukla çevrimiçi, çevrimdışı olsun, dışarıdan dosya kabul eden benzer uygulamalar, sistemler, Türkçe karakter içeren dosya isimlerini çözümlemede (parse) sıkıntı yaşayabiliyorlar. Hesperbot salgınından elde ettiğim örnek zararlı yazılımın adını değiştirip (fatura.exe dosyasının adını faturaÜ Ü Ü.exe olarak değiştirdim) malwr.com'a göndermeye başladıktan kısa bir süre

sonra dosya isminin sonunda Ü Ü Ü olduğu taktirde malwr.com'da gerçekleşen analizin kısır döngüye girdiğini ve analizin sonlanmadığını farkettim. Dosyayı çevrimdışı olarak Cuckoo Sandbox ile analiz etmeye çalıştığımda da bir hata ile karşılaştım.

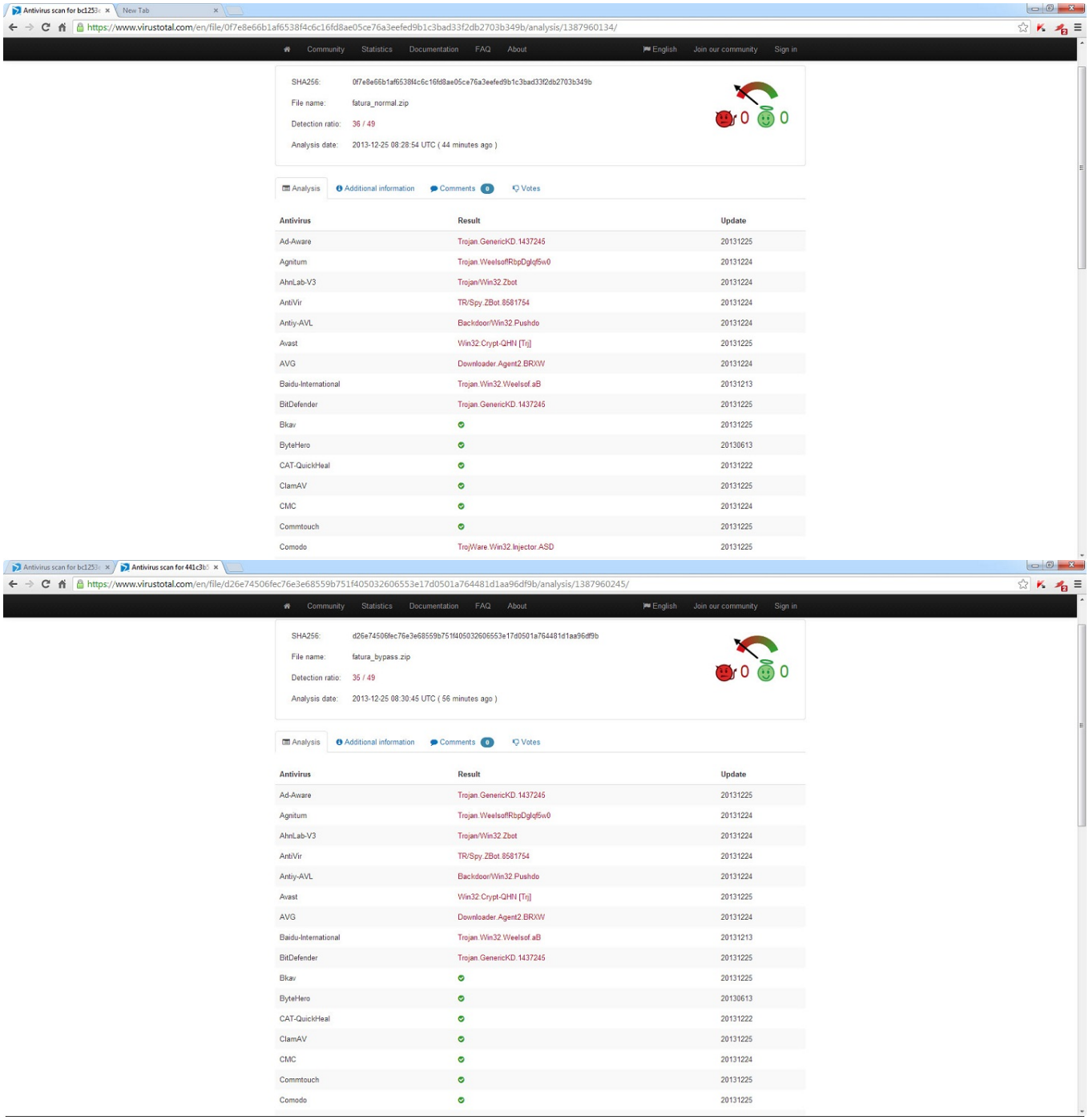
Günler önce faturaÜ Ü Ü.exe dosyasının, üzerinde Cuckoo Sandbox çalışan malwr.com adresine gönderilmiş ve hala kısır döngüde kalmış analizine buradan ulaşabilirsiniz.





Tabii diyeceksiniz ki adını fatura.exe yapıp yollasam analiz başarıyla tamamlanmayacak mı ? Tamamlanacak fakat zararlı yazılım çalıştıktan sonra hangi isim altında çalışıp ona göre zararlı fonksiyonları çağıracaksa şekilde tasarlanmış olsaydı o da çözüm olamayacaktı kısaca kod analizi yapmadan her zaman bu tür yöntemlerle analizin atlatılması, farklı sonuçlar üretmesi mümkün olabiliyor.

Cuckoo/Malwr dışında bu iki zip dosyasını VirusTotal'a da gönderip orada da ilginç bir durumla karşılaşıp karşılaşmayacağıma bakmak istedim. 2 dosyayı da ayrı ayrı VirusTotal'a gönderip rapora baktığımda, fatura_normal.zip (36/49) ile fatura_bypass.zip (35/49) için üretilen raporlarda, Comodo antivirüs yazılımın farklı sonuç ürettiğini gördüm. fatura_normal.zip dosyasını zararlı olarak tespit edebiliyorken, fatura_bypass.zip için dosyanın güvenli olduğunu raporluyordu.



Kıssadan hisse, zararlı yazılım analizi için sistemsel, davranışsal analiz evet kısa sürede size birçok ipucu verebiliyorken, kolaylıkla atlatılabileceği ve duruma göre farklı sonuçlar üretileceği hiçbir zaman unutulmamalıdır.

Bu vesileyle herkesin yeni yılını kutlar, 2014 yılını herkese sağlık, mutluluk ve başarı getirmesini dilerim :)