Yara ile Tehdit Avı

written by Mert SARICA | 1 September 2017
If you are looking for an English version of this article, please visit here.

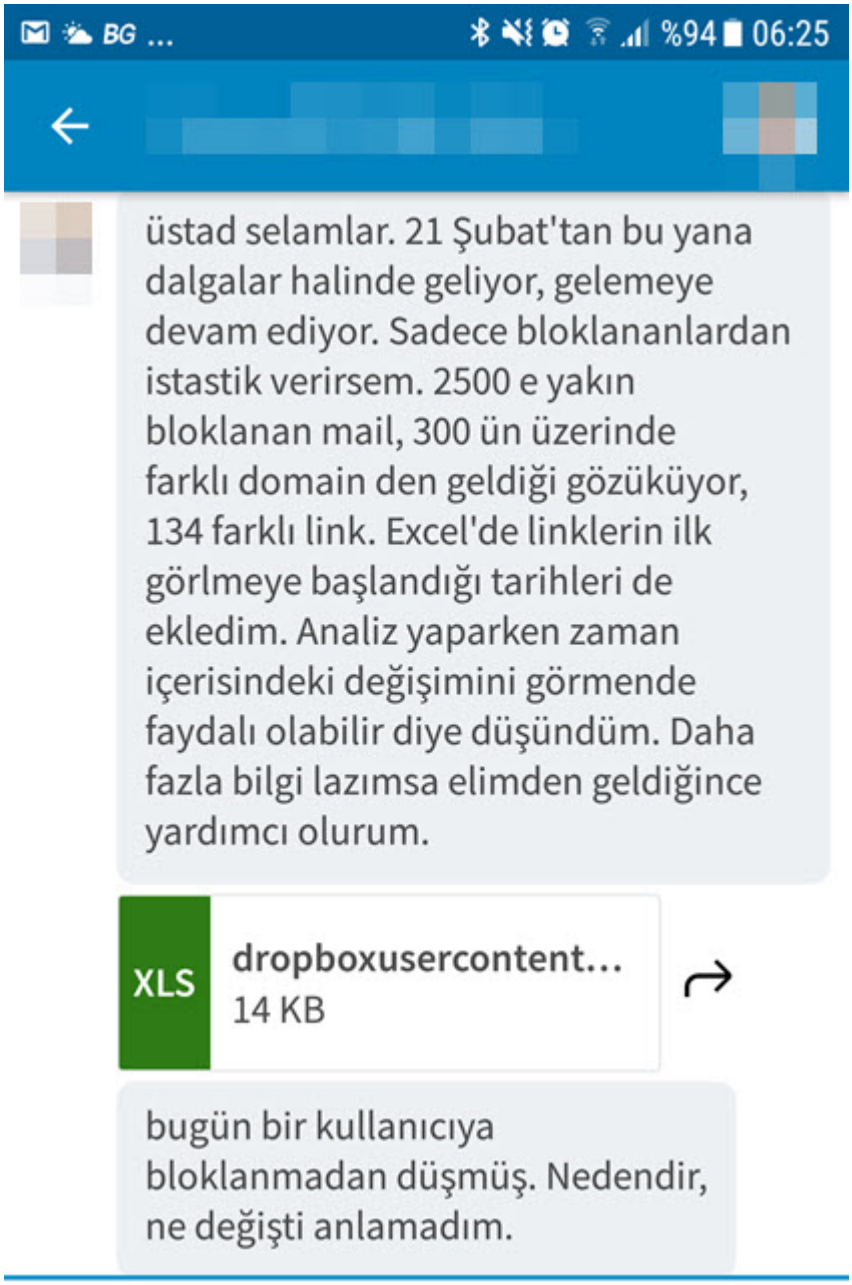
Dünya genelinde, son kullanıcı sistemlerindeki verileri zararlı yazılımlarla (cryptolocker vb.) şifreledikten sonra dosyaların şifresiz halini silip ardından da şifre çözme anahtarını kullanıcılara satmaya çalışarak bundan kazanç sağlama furyası hız kesmeden devam ediyor. Zaman zaman güvenlik araştırmacıları tarafından şifreleme algoritmalarının hatalı kullanımına bağlı olarak zararlı yazılımlar tarafından şifrelenen veri çözülebilse de, çoğu vakada kullanıcılar çoğunlukla art niyetli kişilere talep edilen yüksek miktarlı çözme bedelini ödemek zorunda kalıyorlar. Her vaka sonrasında veri yedeklemenin kıymeti daha net anlaşılsa da, 1000 nasihat yerine 1 musibet ile hareket eden kullanıcılar olduğu sürece art niyeli kişilerin bu kazanç kapısından yakın gelecekte kolay kolay vazgeçmeyecekler gibi görünüyor.

Siber saldırıların hızla arttığı günümüzde, tehditleri tespit edip en kısa sürede müdahale edebilme kurumlar için büyük önem kazanmaya başladı. Öyle ki vizyoner kurumlar artık mevcut güvenlik teknolojilerini atlatan tehditleri kurum ağ ve sistemlerinde arayabilme adına siber tehdit avcılığına başladılar. Tehdit avcılığına imkan tanıyan teknolojilere baktığınızda, çoğunun kendi imzanızı yazmaya imkan tanıyan Yara aracını ve imzalarını desteklediğini görebiliyorsunuz.

Sevgili Halil ÖZTÜRKCİ'nin 2014 yılında Yara ile ilgili olarak yayınlamış olduğu blog yazısına baktığınızda, Yara'nın o yıllarda yoğunluklu olarak adli bilişim analizinde ve bellek analizinde kullanılan Volatility aracı özelinde kullanıldığını görebiliyorsunuz. Bugün ise Yara'nın tehdit avcılığından zararlı yazılım analizine, FireEye NX gibi ticari ürünlerden, x64dbg gibi açık kaynak kodlu ve ücretsiz araçlara, paket kaydı yapan (full packet capture) teknolojilere kadar geniş bir alanda kullanılabildiğini görebiliyorsunuz. Bu da güvenlik uzmanlarına, güvenlik üreticilerinden bağımsız olarak kurum içinde kullanılan ve Yara desteği olan güvenlik sistemlerine, cihazlara tespit ve müdahaleye imkan tanıyan kendi yazdıkları imzalarını tanımlama imkanı tanıyor. İmza yazma, geçmiş yıllarda farklı güvenlik teknolojileri ile zor tecrübeler yaşamış olan güvenlik uzmanlarının kulağına nahoş gelse de, mevzu bahis Yara olduğunda işin rengi değişiyor çünkü Yara ile kural yazmanın oldukça basit, katma değerinin ise oldukça

yüksek olduğunu tecrübe ile sabit olarak söyleyebilirim.

Cryptolocker salgınının tekrar zirve yaptığı geçtiğimiz aylarda, sosyal ağlarda ve NetSec e-posta listesinde, kimi güvenlik sistemlerinin, teknolojilerinin bu salgınları tespit etmede ve engellemede yetersiz olduğunu gördüm. Ben de böyle bir durum ile karşı karşıya kalındığında, özellikle defansif güvenlik uzmanlarının Yara ile yazabilecekleri basit bir imza ile içeriği değişen benzer tehditleri nasıl tespit edebileceklerine dikkat çekmek istedim.



Cryptolocker salgınına baktığımızda, 24 saatte çok sayıda farklı e-posta

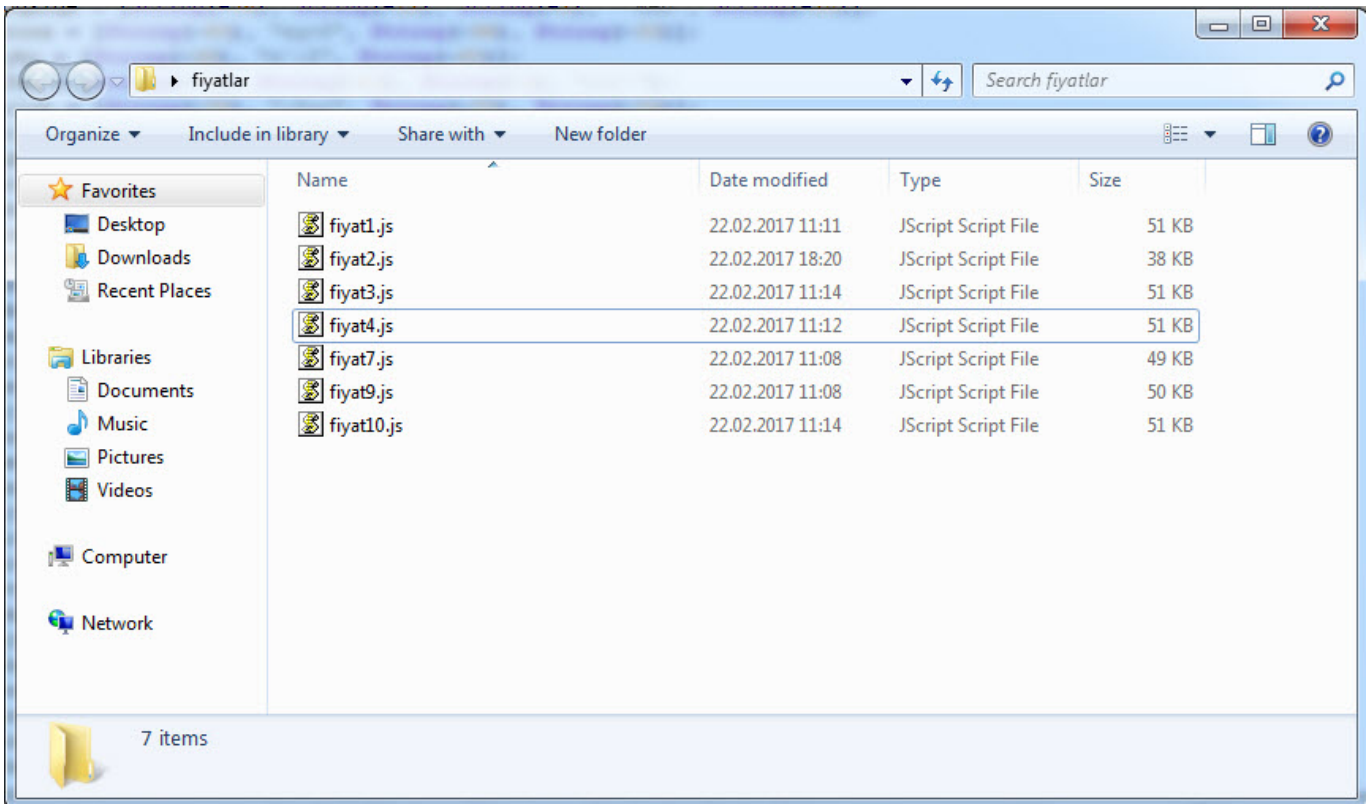
adresinden fiyatX.zip adı altında Cryptolocker varyantı gönderiliyordu. Her bir zip dosyası içinde karmaşıklaştırılmış (obfuscated) JavaScript koduna sahip bir indirici (downloader) bulunuyor ve çalıştırıldıktan hemen sonra şifreleme zararlı yazılımını indirip sistemde çalıştırıyordu.

Doruk Tekin rammer@tele2.at

Ekte gönderilen mallar için birim fiyat ve teslim süresi rica ederim.

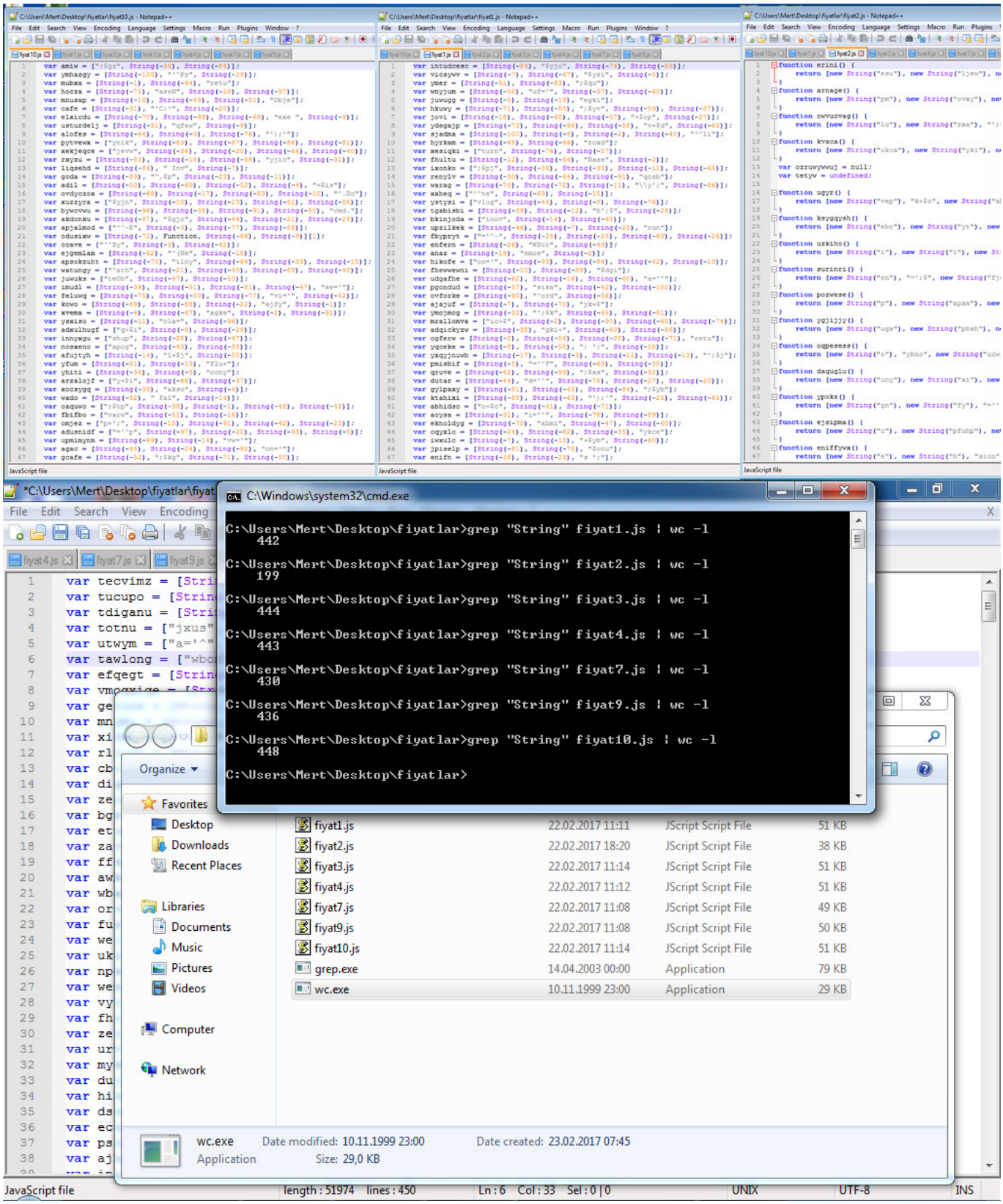
https://dl.dropboxusercontent.com/s/be9kvoym3hwjk69/fiyat3.zip

Iyi günler.

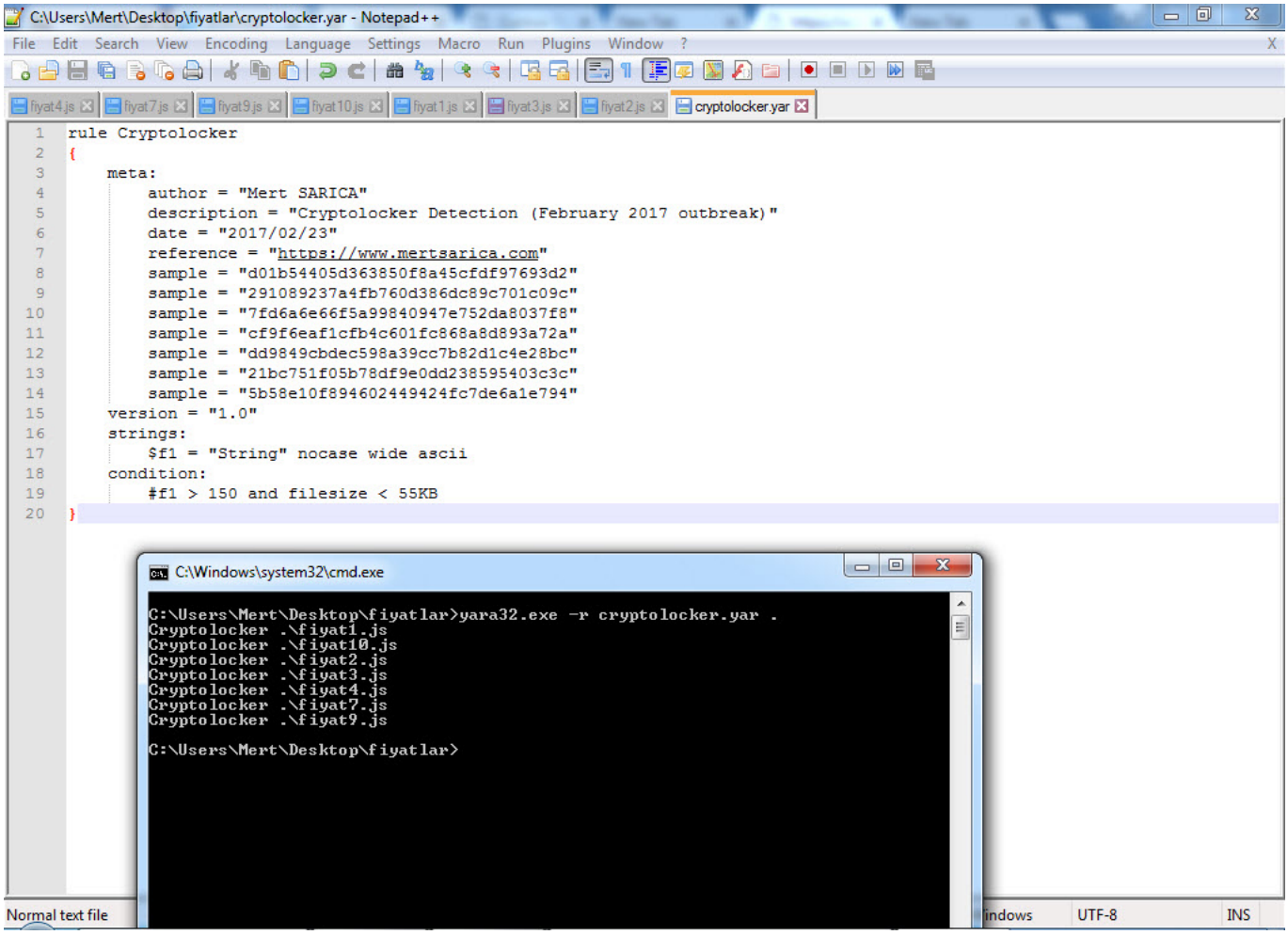


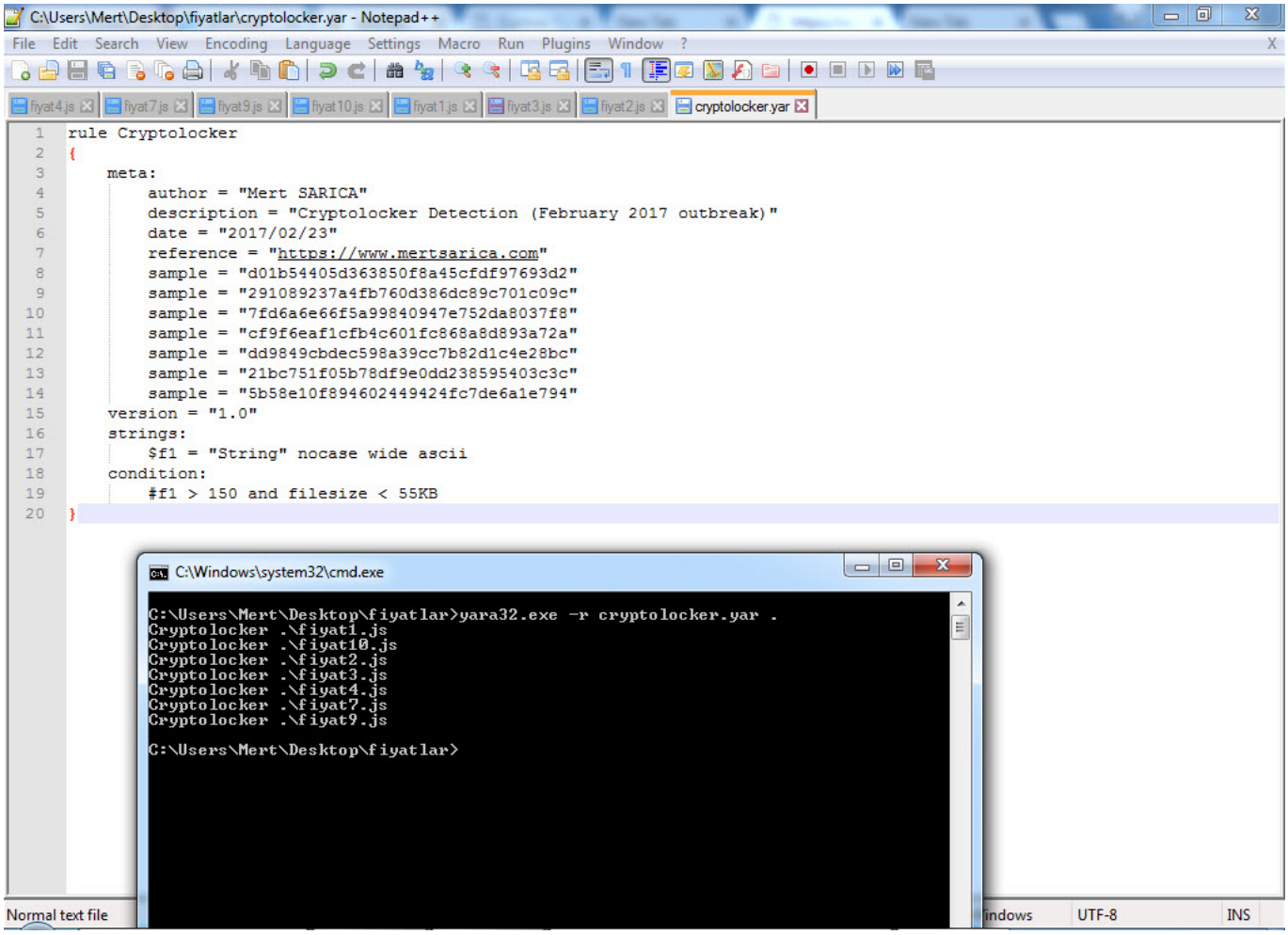
İş, boyutları ve içeriği birbirinden tamamen farklı olan varyantları tespit etmeye geldiğinde Yara ile bunu oldukça kolay bir şekilde yapabilirsiniz. İlk olarak boyutları listelediğimizde bir varyant hariç tamamının 55 KB'den ufak

olduğunu görüyoruz. Dosyaların içeriğine baktığımızda ise her ne kadar içerik tamamen farklı olsa da String fonksiyonu kullanılarak karmaşık kod çözümlenerek alan adı ve indirilecek dosya ortaya çıktığı için String fonksiyonu üzerinden ilerleyebiliriz.



Normal şartlarda 55 KB’dan küçük olan bir dosyada kullanılan String fonksiyonunun sayısının, dosya şüpheli olmadığı sürece 150‘den az olacağını varsayarak Yara anahtar kelimelerinden faydalanarak aşağıdaki gibi bir Yara imzası oluşturabiliriz. Yazmış olduğumuz cryptolocker.yar isimli imzanın doğru çalıştığını ve elimizdeki tüm varyantları tespit edebildiğini Yara aracı ile de doğruladıktan sonra imzamızı Yara destekleyen tüm güvenlik sistemlerine, teknolojilerine yükleyerek yeni bir salgını, tehdidi tespit etmede önemli bir mesafe katetmiş oluyoruz.





Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.