Virusscan BUP Restore Utility

written by Mert SARICA | 12 February 2011

Bana göre korsanların (konumuz her zamanki gibi etik olanlar) başarılı olabilmeleri için yüksek hayal gücüne ve yaratıcı zekaya sahip olmaları gerekmektedir. Karşılaştıkları engelleri aşmak ve başarıya ulaşmak için üretecekleri senaryolar hayal güçleri ile, bu senaryoları hayata geçirmeleri ise yaratıcılıkları ile mümkün olabilmektedir. Nedense hayal gücü ile zafiyet keşfetme becerisini, yaratıcılık ile ise programlama becerisini örtüştürmüşümdür ve bu yüzden etik bir korsan olarak bu becerilerimi geliştirmek için zaman zaman senaryolar üreti zaman zamanda karşıma çıkan fırsatları değerlendirmeye çalışırım.

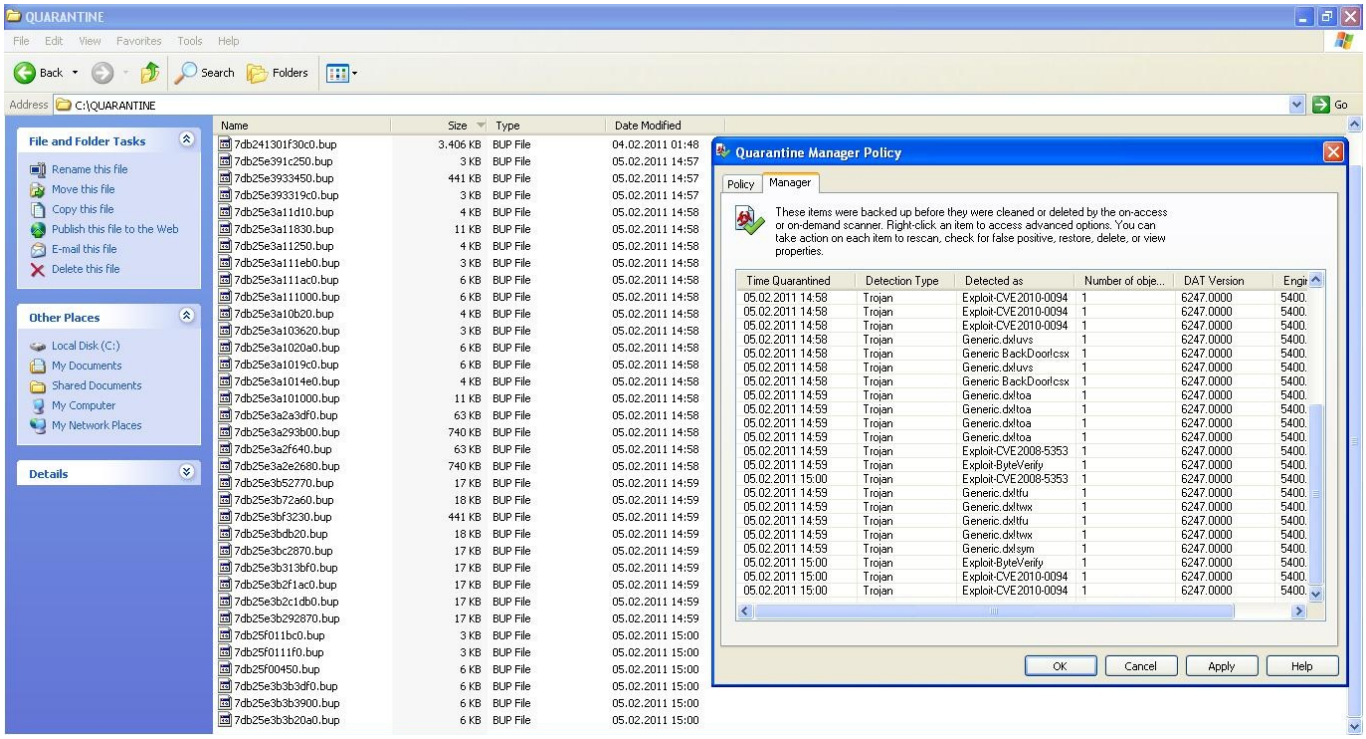
Yine günlerden bir gün, şüpheli bir duruma karşı kullanıcılardan gelen antivirus alarmlarına göz atarken kullanıcılardan gelen fazla sayıda alarm dikkatimi çekti. Zararlı yazılım analizinden oldukça keyif alan kahramanımız Mert, fırsat bu fırsat Jedi duyuları ile hareket ederek alarmların kaynağını aramaya koyuldu ve alarmların arkasında bu kullanıcıların ortak olarak ziyaret ettiği bir web sitesi olduğu anlaşıldı. Web sitesini ziyaret eden kahramanımızın antivirus programı da aynı alarmı verince dosya üzerinde detaylı bir analiz yaptıktan durumun yanlış alarmdan (false positive) ibaret olduğunu anladı ve adli bilişim analizi yapma hevesi kursağında kaldı.

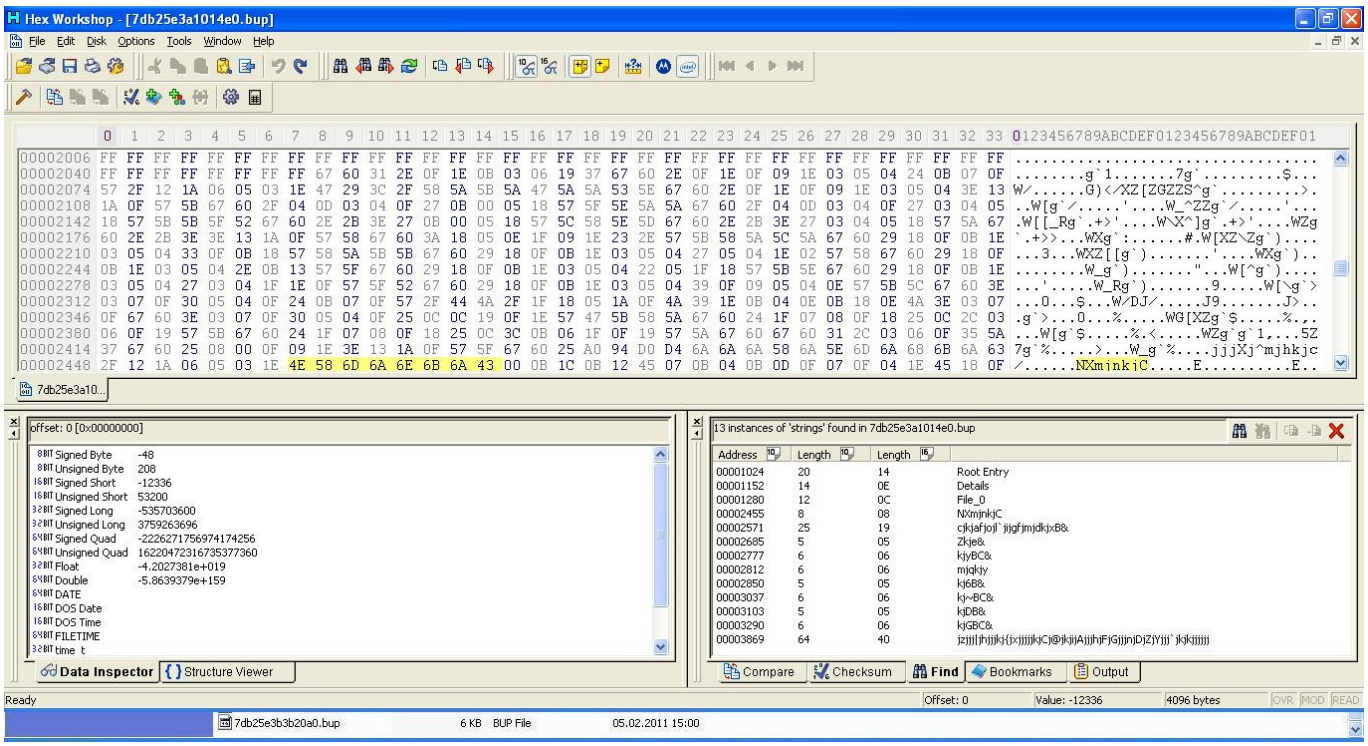
Peki ya durum biraz daha farklı olsaydı. Kahramanımızın kullandığı antivirus yazılımı Mcafee Virusscan olsaydı ve Virusscan tespit ettiği zararlı yazılımları karantinaya alıyor olsaydı ayrıca kahramanımızın antivirus üzerindeki yetkileri (dosyayı karantinadan çıkarma yetkisi) kısıtlı olsaydı bu durumda ne yapması gerekirdi ?

Antivirus sistemini yöneten kişiden ilgili dosyayı restore etmesini ve analiz için kendisine iletmesini talep edebilir (e-posta ve telefon trafiği) veya sanal makine içindeki işletim sistemine Virusscan kurabilir ve onun üzerinde restore edebilir (ölme eşeğim ölme) veya karantina mekanizmasının nasıl çalıştığını tersine mühendislik ile çözerek bunu otomatize hale getiren bir araç hazırlayabilir (bildiğim kararıyla piyasada böyle bir araç yok veya ben aradığım zaman yoktu) ve yeri geldiğinde bunu adli bilişim analizlerinde

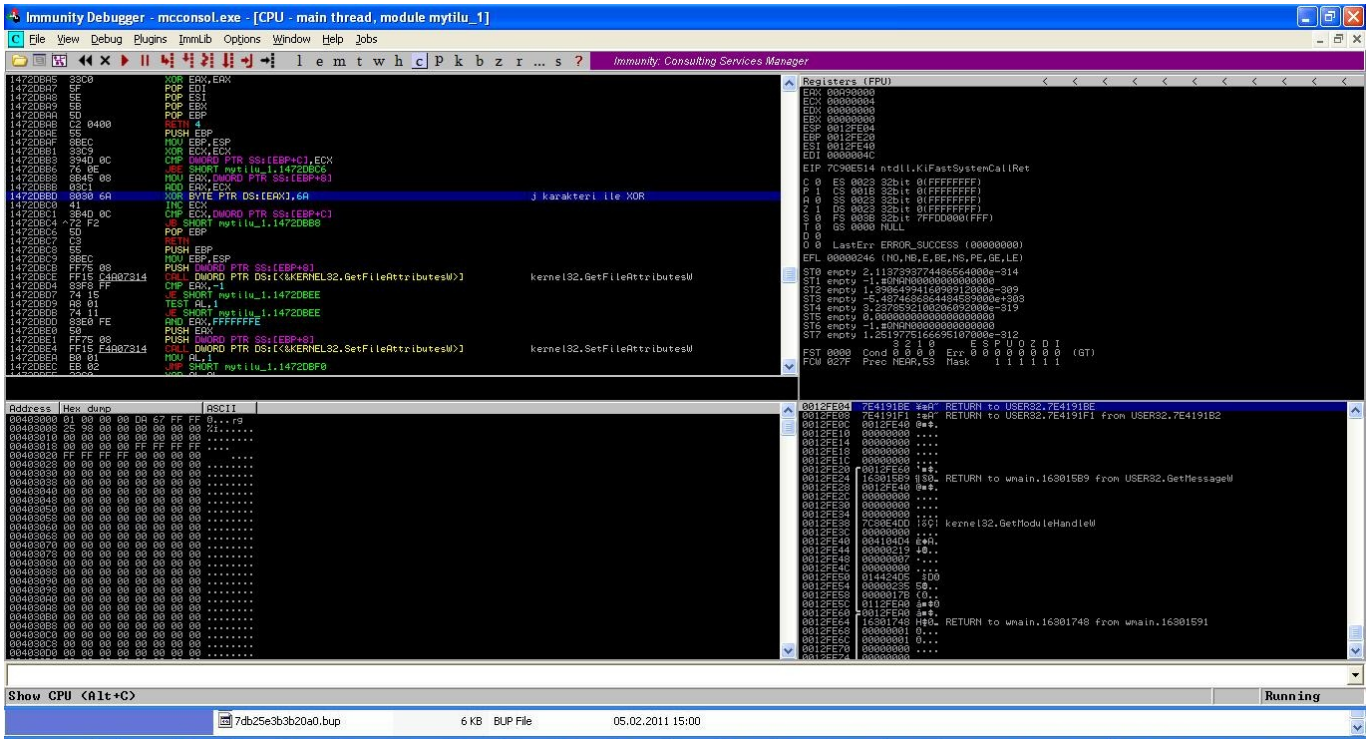
kullanılabilirdi. (hedef diskten karantinaya alınmış dosyaları kopyalamak ve incelemek size güzel ipuçları verebilir şayet analize elverişli biçimde diskle saklanmış ise)

Karantina işleminin nasıl yapıldığından kısaca bahsedece olursak, Virusscan, karantinaya aldığı dosyayı C:\QUARANTINE klasörüne farklı bir ad altında kopyalamakta ve uzantı olarak BUP kullanmaktadır. (Örnek: 7db11a1031283c50.bup). Karantinaya alınan bir dosyayı herhangi bir hex editörü ile inceleyecek olursanız içeriğin ve dosya boyutunun orjinalinden farklı olduğunu, anlamlı karakterlerden oluşan diziler (string) ortadan kaybolmuş olduğunu görebilirsiniz.

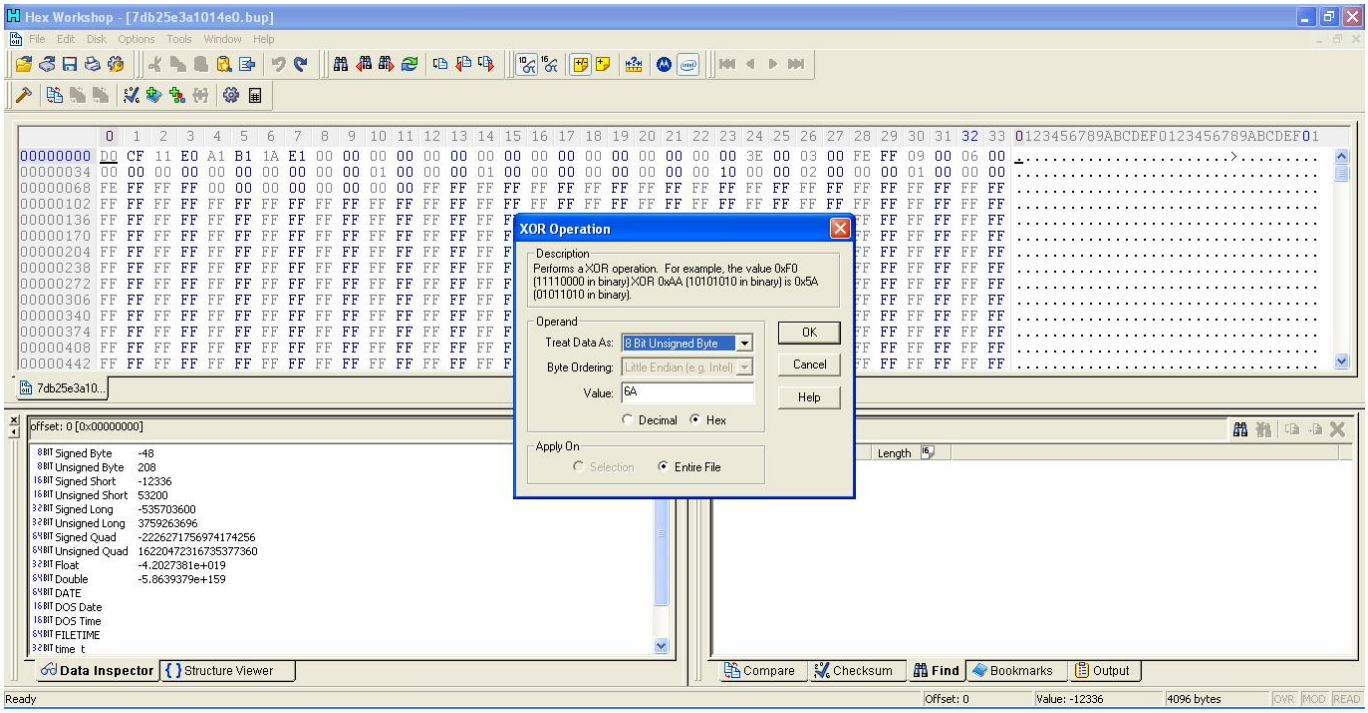


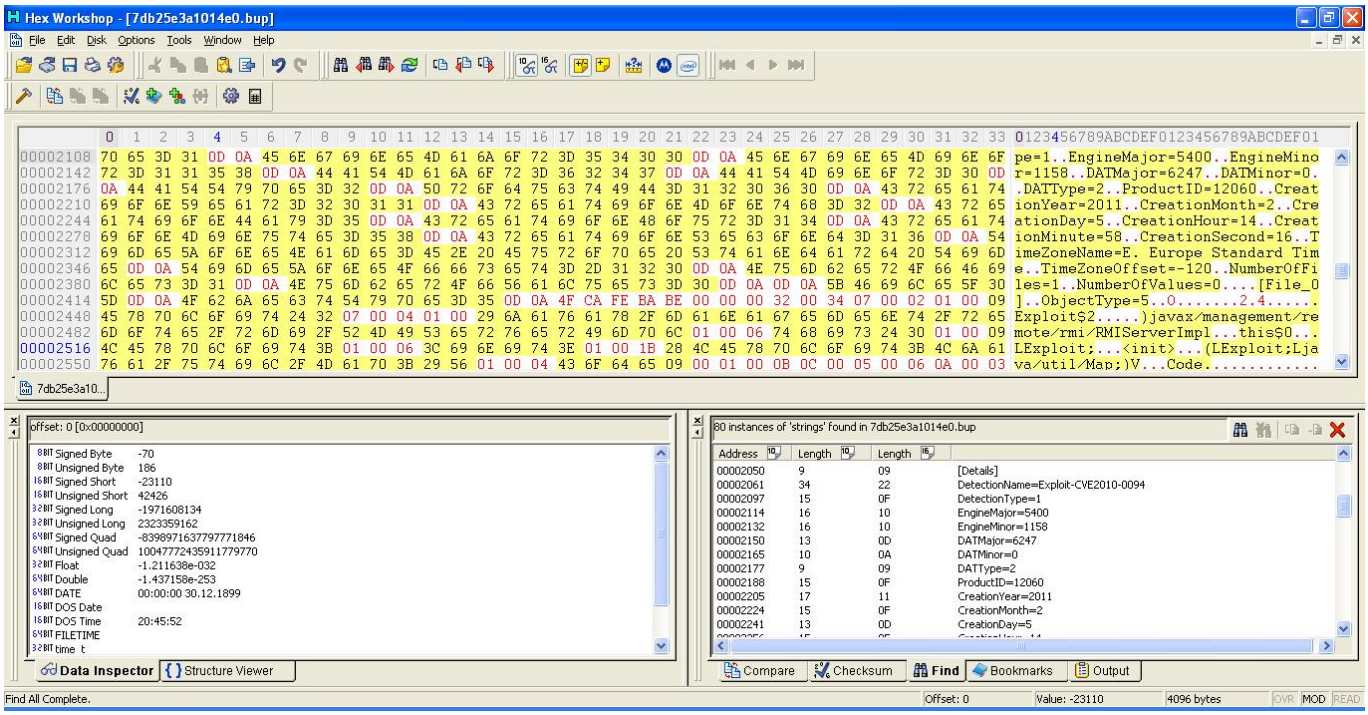


Karantina mekanizmasının nasıl çalıştığını hızlıca anlamaya çalıştığımda karantinaya alınan ve BUP uzantısı ile saklanan dosyanın j (hex: 6A) karakteri ile XOR işleminden geçirildiğini anlamam çok zor olmadı.

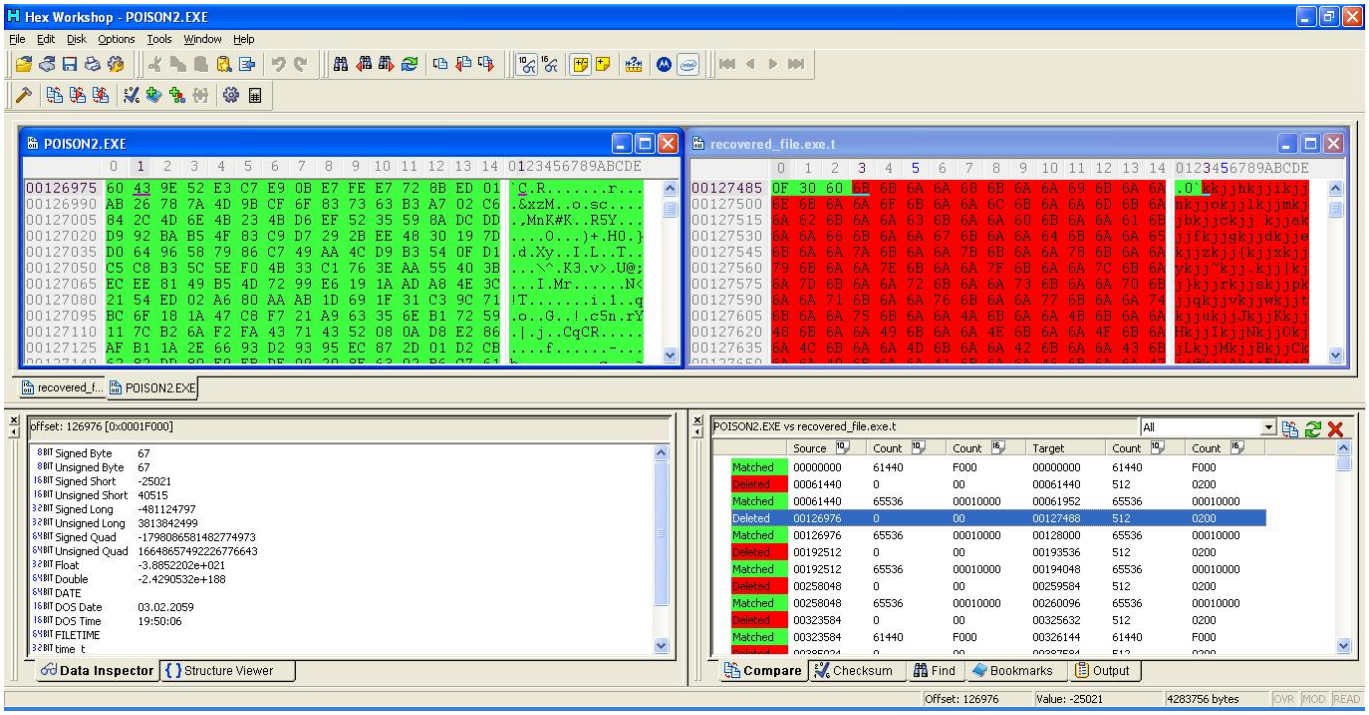


Hex Workshop ile karantinaya alınmış dosyayı 6A ile XOR işleminden geçirdikten sonra ortaya anlamlı karakterler oluşan diziler çıkıverdi.

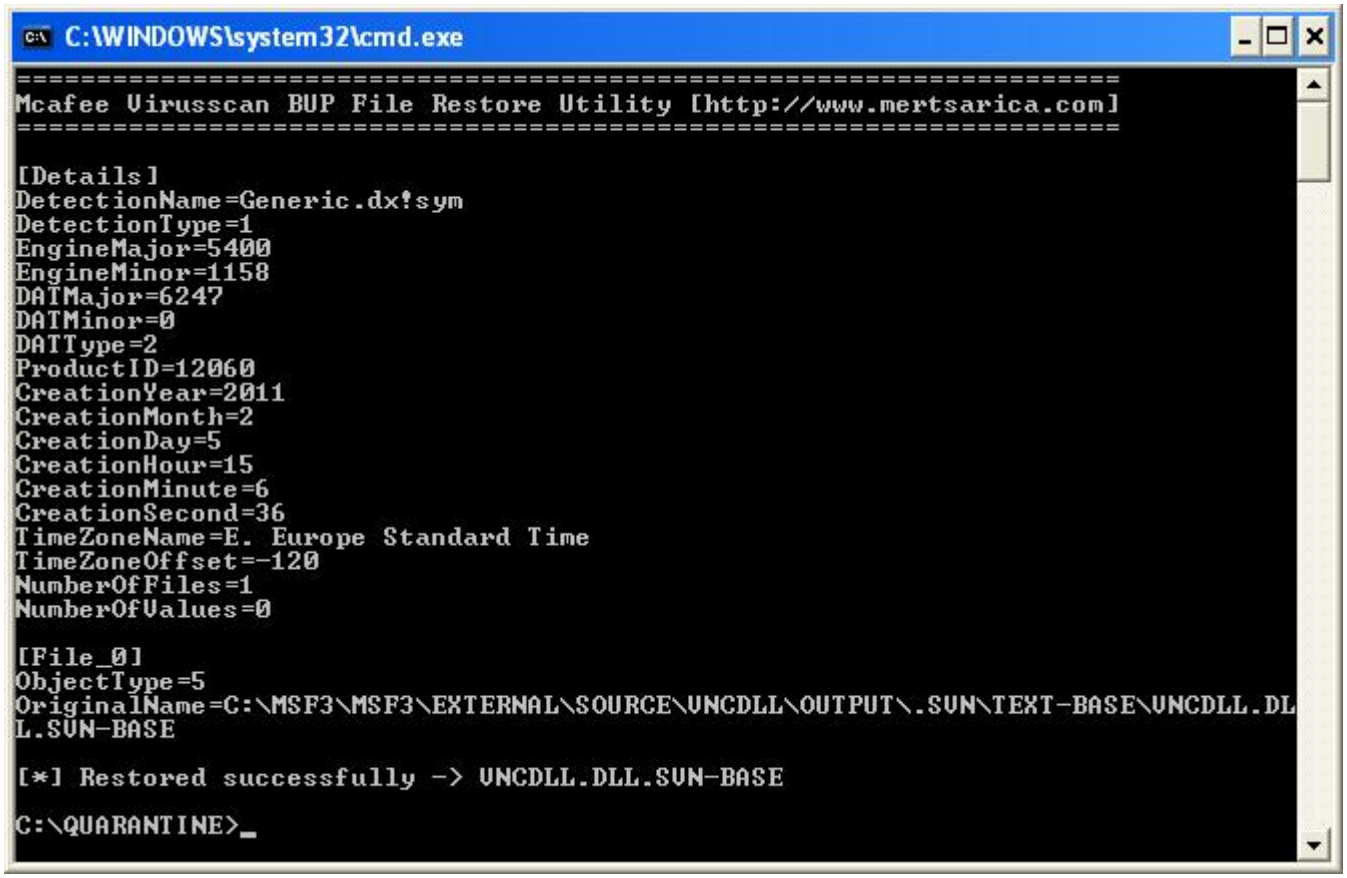




Orjinal dosya ile XOR işleminden geçirilmiş dosyayı karşılaştırdığımda XOR'lanmış dosyanın ilk 2560 baytında detaylı bilgiler (orjinal dosyanın adı, karantinaya alınma tarihi, virusun adı vs.) saklandığını gördüm. Daha sonrasında ise programın orjinali saklanıyordu. (Tam olarak orjinali diyemiyorum çünkü her 65536 baytta bir 512 bayt büyüklüğünde çöp veri araya (junk) sokuşturulmuş ve bunları ayıklamam gerekti)



Hem detaylı bilgileri gösteren hem de karantinaya alınmış olan dosyayı orjinal haline çeviren bir program hazırlamak için işe koyulduğumda ortaya bup_recovery.py aracı çıktı.



Program iki komut (restore ve view) ile çalışıyor ve kullanımı yine çok basit. İlk olarak yapmanız gereken karantinaya alınmış dosya ile bup_recovery.py programını aynı klasöre kopyalamanız. Restore komutu ile hem

detaylı bilgileri görebilir hem de karantinaya alınmış programı orjinal haline çevirebilirsiniz. View komutu ile sadece detaylı bilgileri görebilirsiniz.

Örnek: bup_recovery.py restore 7db11a1031283c50.bup

Programı buradan indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese iyi hafta sonları dilerim.

Not: Zaman zaman senaryolarımda Mcafee antivirus yazılımına yer veriyor olmamın nedeni uzun yıllarca kullanmış olmamdır başka bir nedeni yoktur :)