

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 örtüştürmüştümdür 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 kadarıyla piyasada böyle bir araç yok veya ben aradığım zaman yoktu) ve yeri geldiğinde bunu adli bilişim analizlerinde

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

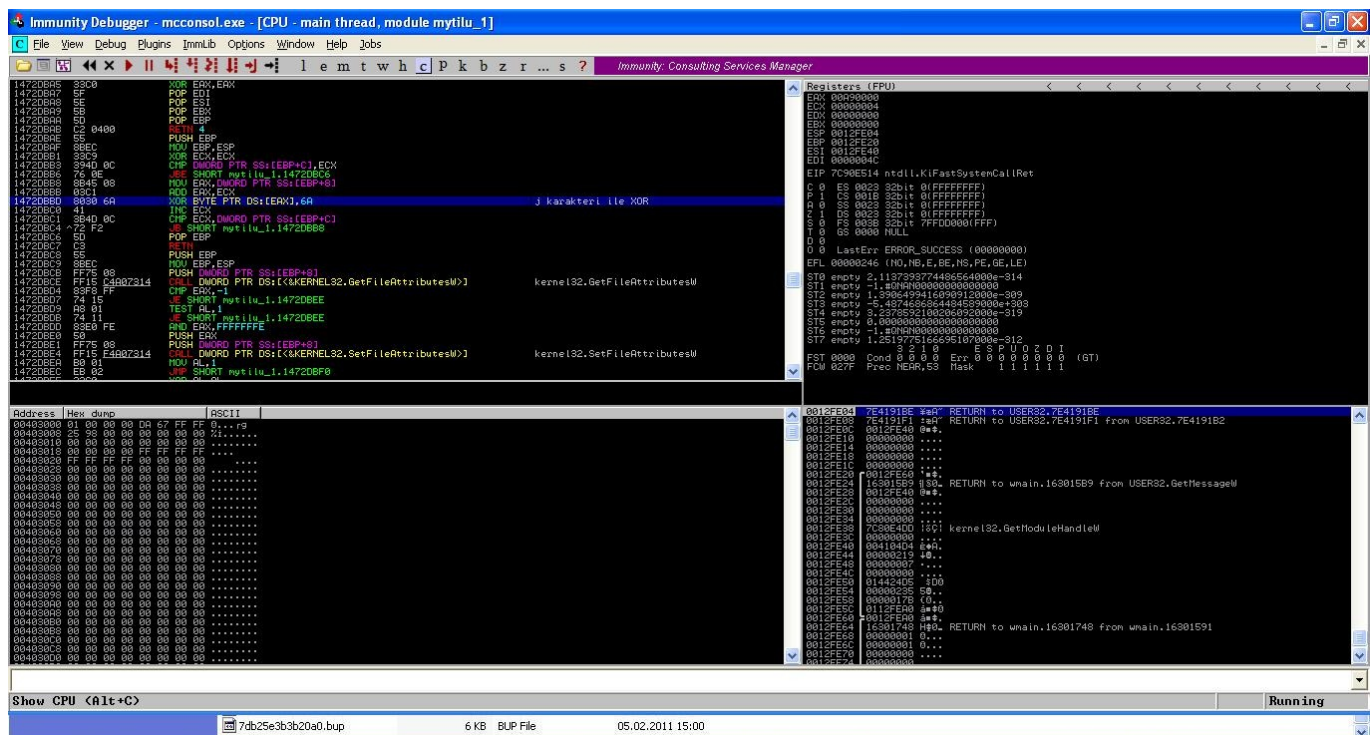
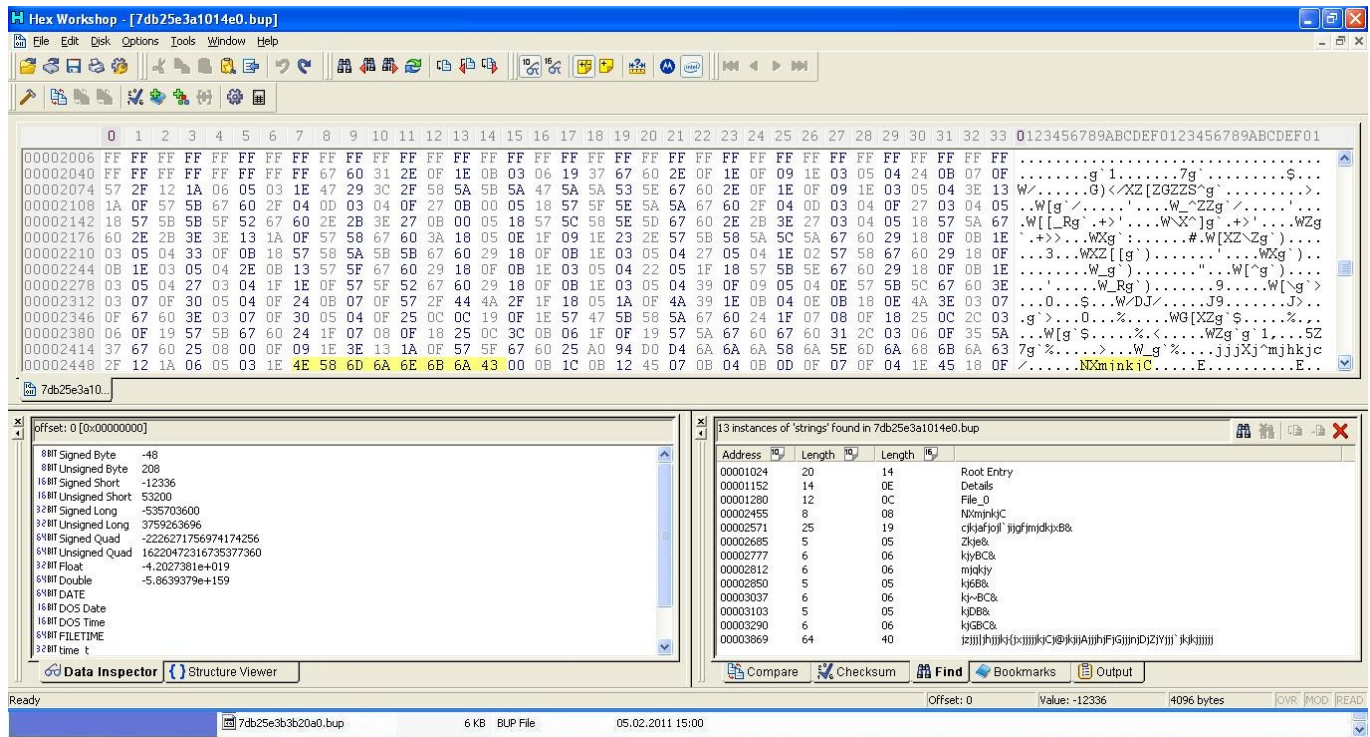
Karantina işleminin nasıl yapıldığından kısaca bahsedece olursak, Virusscan, karantinaya aldığı dosyayı C:\QUARANTINE klasörüne farklı bir ad altında kopyalamakta ve uzantı olarak BUP kullanmaktadır. (Örnek: 7db11a1031283c50.bup). Karantinaya alınan bir dosyayı herhangi bir hex editörü ile inceleyecek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

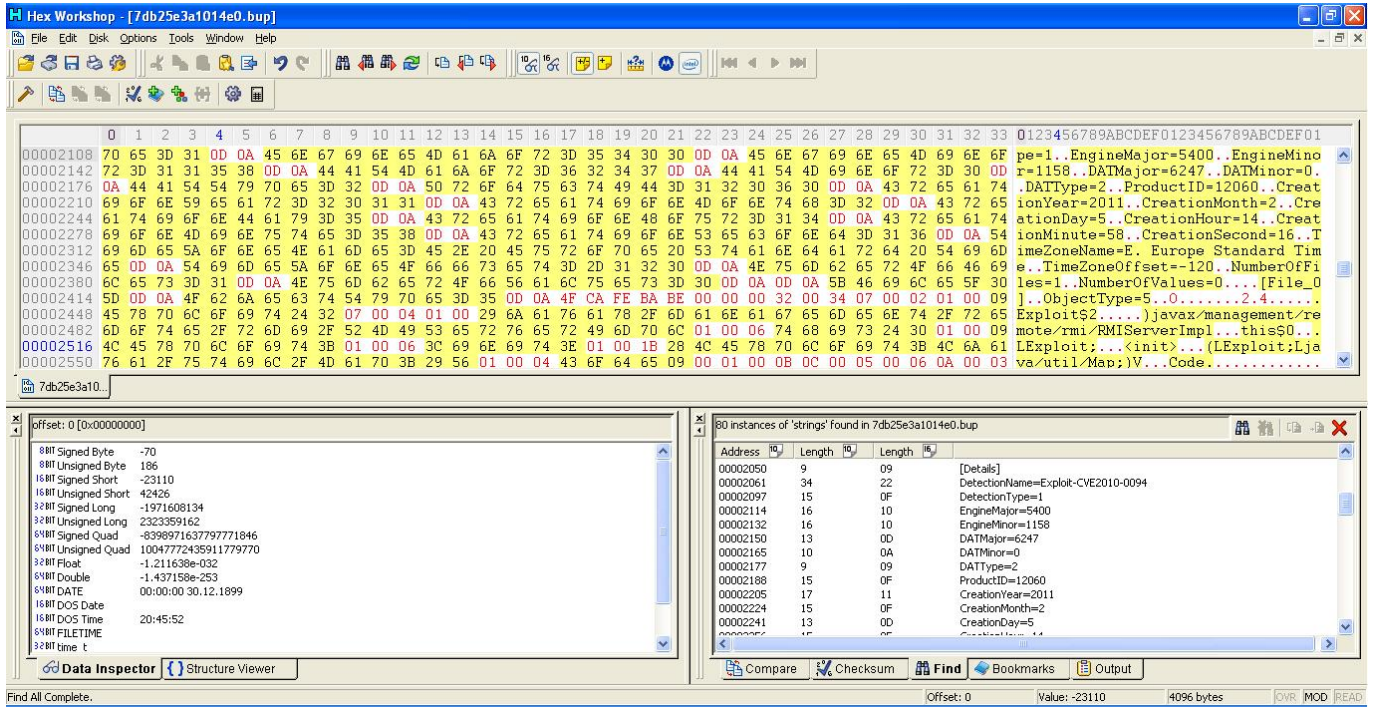
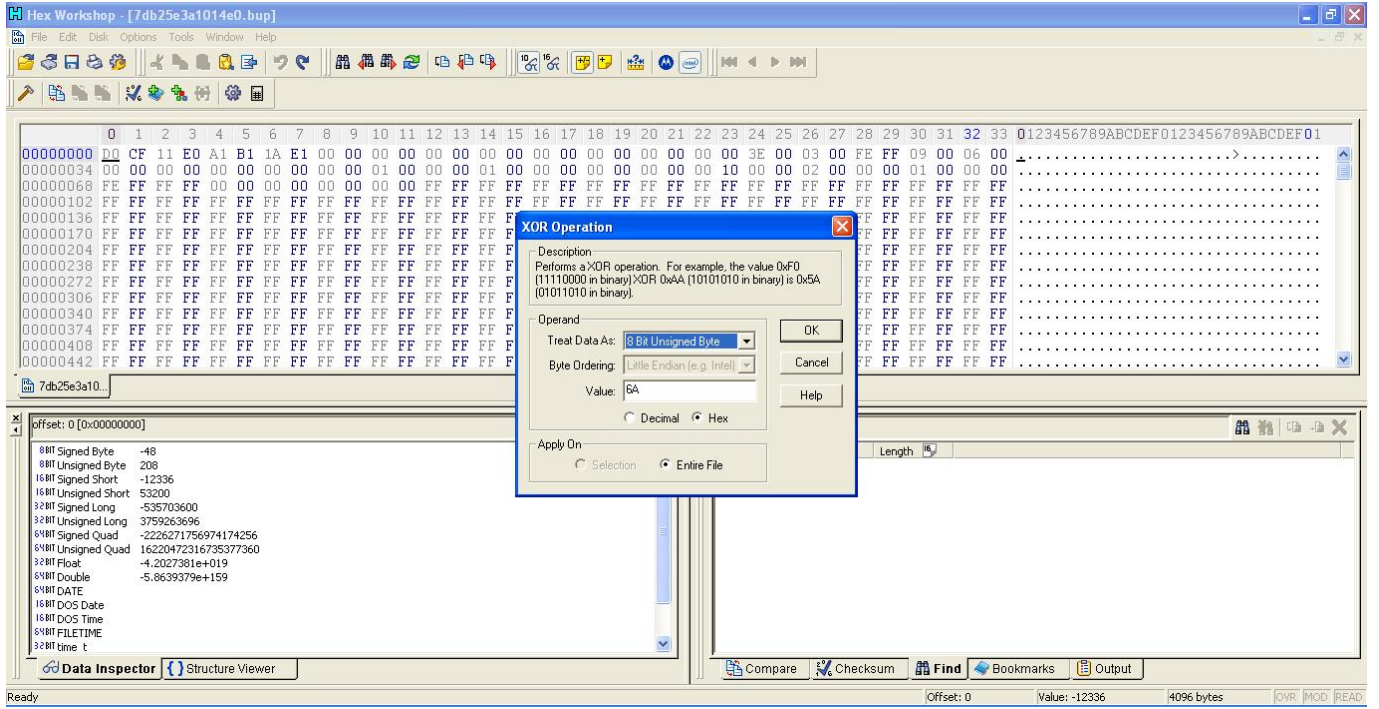
The screenshot shows a Windows Explorer window titled 'QUARANTINE' displaying the contents of the C:\QUARANTINE folder. The folder contains numerous BUP files, each with a unique identifier and a date modified. The files are listed in a table with columns for Name, Size, Type, and Date Modified. The 'Name' column shows identifiers like 7db241301f30c0.bup, 7db25e391c250.bup, etc. The 'Size' column shows file sizes in KB. The 'Type' column shows 'BUP File'. The 'Date Modified' column shows dates like 04.02.2011 01:48, 05.02.2011 14:57, etc.

Overlaid on the Explorer window is the 'Quarantine Manager Policy' dialog box. It has two tabs: 'Policy' and 'Manager'. The 'Manager' tab is active, showing a list of quarantined items. The list has columns for Time Quarantined, Detection Type, Detected as, Number of objects, DAT Version, and Engine. The list contains multiple entries for Trojan and Exploit-CVE items, all detected on 05.02.2011.

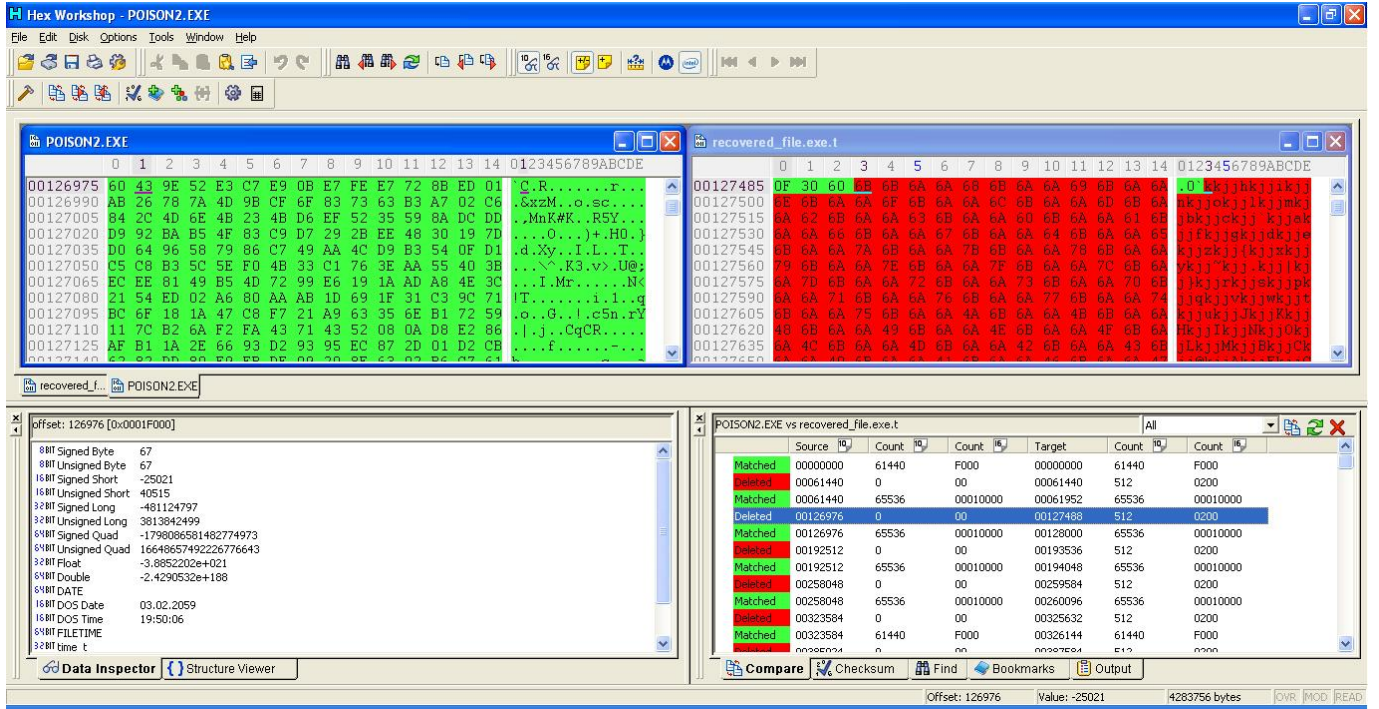
Name	Size	Type	Date Modified
7db241301f30c0.bup	3,406 KB	BUP File	04.02.2011 01:48
7db25e391c250.bup	3 KB	BUP File	05.02.2011 14:57
7db25e3933450.bup	441 KB	BUP File	05.02.2011 14:57
7db25e39319c0.bup	3 KB	BUP File	05.02.2011 14:57
7db25e3a11d10.bup	4 KB	BUP File	05.02.2011 14:58
7db25e3a11830.bup	11 KB	BUP File	05.02.2011 14:58
7db25e3a11250.bup	4 KB	BUP File	05.02.2011 14:58
7db25e3a111eb0.bup	3 KB	BUP File	05.02.2011 14:58
7db25e3a111ac0.bup	6 KB	BUP File	05.02.2011 14:58
7db25e3a111000.bup	6 KB	BUP File	05.02.2011 14:58
7db25e3a110b20.bup	4 KB	BUP File	05.02.2011 14:58
7db25e3a103620.bup	3 KB	BUP File	05.02.2011 14:58
7db25e3a1020a0.bup	6 KB	BUP File	05.02.2011 14:58
7db25e3a1019c0.bup	6 KB	BUP File	05.02.2011 14:58
7db25e3a1014e0.bup	4 KB	BUP File	05.02.2011 14:58
7db25e3a101000.bup	11 KB	BUP File	05.02.2011 14:58
7db25e3a2a3df0.bup	63 KB	BUP File	05.02.2011 14:58
7db25e3a293b00.bup	740 KB	BUP File	05.02.2011 14:58
7db25e3a2f640.bup	63 KB	BUP File	05.02.2011 14:58
7db25e3a2e2680.bup	740 KB	BUP File	05.02.2011 14:58
7db25e3b52770.bup	17 KB	BUP File	05.02.2011 14:59
7db25e3b72a60.bup	18 KB	BUP File	05.02.2011 14:59
7db25e3b73230.bup	441 KB	BUP File	05.02.2011 14:59
7db25e3b7db20.bup	18 KB	BUP File	05.02.2011 14:59
7db25e3b7c2870.bup	17 KB	BUP File	05.02.2011 14:59
7db25e3b713bf0.bup	17 KB	BUP File	05.02.2011 14:59
7db25e3b721ac0.bup	17 KB	BUP File	05.02.2011 14:59
7db25e3b7c1db0.bup	17 KB	BUP File	05.02.2011 14:59
7db25e3b7292870.bup	17 KB	BUP File	05.02.2011 14:59
7db25f0111bc0.bup	3 KB	BUP File	05.02.2011 15:00
7db25f01111f0.bup	3 KB	BUP File	05.02.2011 15:00
7db25f00450.bup	6 KB	BUP File	05.02.2011 15:00
7db25e3b7b3df0.bup	6 KB	BUP File	05.02.2011 15:00
7db25e3b7b3900.bup	6 KB	BUP File	05.02.2011 15:00
7db25e3b7b20a0.bup	6 KB	BUP File	05.02.2011 15:00

Time Quarantined	Detection Type	Detected as	Number of objects	DAT Version	Engine
05.02.2011 14:58	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400
05.02.2011 14:58	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400
05.02.2011 14:58	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400
05.02.2011 14:58	Trojan	Generic.dcluvx	1	6247.0000	5400
05.02.2011 14:58	Trojan	Generic.BackDoor.cxx	1	6247.0000	5400
05.02.2011 14:58	Trojan	Generic.dcluvx	1	6247.0000	5400
05.02.2011 14:58	Trojan	Generic.BackDoor.cxx	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltoa	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltoa	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltoa	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltoa	1	6247.0000	5400
05.02.2011 14:59	Trojan	Exploit-CVE-2008-5353	1	6247.0000	5400
05.02.2011 14:59	Trojan	Exploit-CVE-2008-5353	1	6247.0000	5400
05.02.2011 15:00	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltfx	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltfx	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltfx	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltfx	1	6247.0000	5400
05.02.2011 14:59	Trojan	Generic.dcltfx	1	6247.0000	5400
05.02.2011 15:00	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400
05.02.2011 15:00	Trojan	Exploit-CVE-2010-0094	1	6247.0000	5400

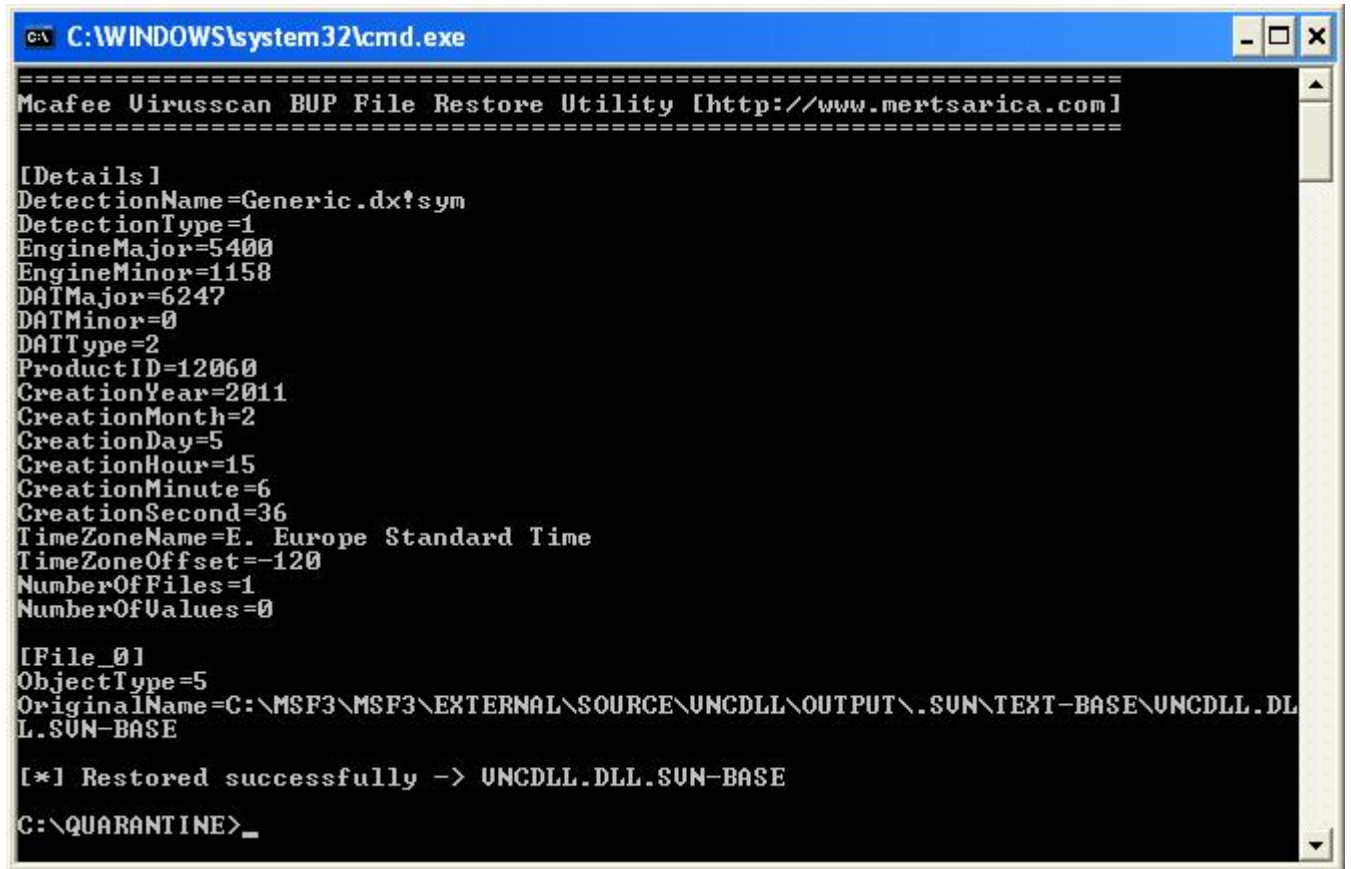




Orjinal dosya ile XOR işleminden geçirilmiş dosyayı karşılaştırdığımda XOR'lanmış dosyanın ilk 2560 baytında detaylı bilgiler (orjinal dosyanın adı, karantinaya alınma tarihi, virusun adı vs.) saklandığını gördüm. Daha sonrasında ise programın orijinali saklanıyordu. (Tam olarak orijinali diyemiyorum 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 :)