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.

QUARANTINE									
ile Edit View Favorites Tools	Help								
3 Back 🔹 🕥 🕤 🏂 🔎 S	5earch 😥 Folders 🛄 🕶								
	1								✓ →
	Name	Size 🤝 Type	Date Modified						
File and Folder Tasks 🙁	📅 7db241301f30c0.bup	3.406 KB BUP File	04.02.2011 01:48	R o	and DelPase				6
	1 7db25e391c250.bup	3 KB BUP File	05.02.2011 14:57	🤏 Quarantine Manag	er Policy				ļ
Rename this hie	10 7db25e3933450.hup	441 KB BLIP File	05.02.2011 14:57	Carlo Manager					
🙀 Move this file	0 7db25e393319c0 bup	3 KB BLIP File	05.02.2011.14.57	Policy Manager					
Copy this file	T 7db25e3a11d10 bup	4 KB BLID File	05 02 2011 14:59	These items w	are backed up before i	they were cleaned or data	d but he on accord		
			05.02.2011 14:50	or on-demand a	scanner Bight-click ar	nitem to access advanced	ontions You can		
Publish this file to the Web	Em /ub25e3a1163U.BUp	II KD BUP File	05.02.2011 14:58	take action on	each item to rescan, c	check for false positive, rest	ore, delete, or view		
🔀 E-mail this file	@ /db25e3a1125U.bup	4 KB BUP File	05.02.2011 14:58	properties.		026			
🗙 Delete this file	7db25e3a111eb0.bup	3 KB BUP File	05.02.2011 14:58						
~	7db25e3a111ac0.bup	6 KB BUP File	05.02.2011 14:58	Time Quarantined	Detection Type	Detected as	Number of obje	DAT Version	Engir 🛆
	📅 7db25e3a111000.bup	6 KB BUP File	05.02.2011 14:58	05.02.2011 14:58	Trojan	Exploit-CVE2010-0094	1	6247.0000	5400.
Other Places	🔟 7db25e3a10b20.bup	4 KB BUP File	05.02.2011 14:58	05.02.2011 14:58	Trojan	Exploit-CVE2010-0094	1	6247.0000	5400.
	7db25e3a103620.bup	3 KB BUP File	05.02.2011 14:58	05.02.2011 14:58	Trojan	Exploit-CVE2010-0094	1	6247.0000	5400.
🛶 Local Disk (C:)	7db25e3a1020a0 bup	6 KB BLID File	05 02 2011 14:58	05.02.2011 14:58	Trojan	Generic.dxluvs	1	6247.0000	5400.
D H. Danmarks	7db20000102000.00p	6 KB BUD File	OF 02 2011 14-F9	05.02.2011 14:58	Trojan	Generic BackDoorlcsx	1	6247.0000	5400.
My Documents		O KD BUP FILE	05.02.2011 14:58	05.02.2011 14:58	Trojan	Generic.dxluvs	1	6247.0000	5400.
Shared Documents	III /db25e3a1014e0.bup	4 KD BUP File	05.02.2011 14:58	05.02.2011 14:56	Trojan	Generic BackDooricsx	1	6247.0000	5400.
My Computer	7db25e3a101000.bup	11 KB BUP File	05.02.2011 14:58	05.02.2011 14:59	Trojan	Generic datoa	1	6247.0000	5400
Mu Natural Discor	7db25e3a2a3df0.bup	63 KB BUP File	05.02.2011 14:58	05.02.2011 14:55	Trojan	Generic dyltoa	1	6247.0000	5400
S My Network Places	🖾 7db25e3a293b00.bup	740 KB BUP File	05.02.2011 14:58	05.02.2011 14:59	Trojan	Generic dxttoa	1	6247.0000	5400
11	🖾 7db25e3a2f640.bup	63 KB BUP File	05.02.2011 14:58	05.02.2011 14:59	Trojan	Exploit-CVE2008-5353	1	6247.0000	5400.
	📅 7db25e3a2e2680.bup	740 KB BUP File	05.02.2011 14:58	05.02.2011 14:59	Trojan	Exploit-ByteVerify	1	6247.0000	5400.
Details 📀	7db25e3b52770 bup	17 KB BLIP File	05 02 2011 14-59	05.02.2011 15:00	Trojan	Exploit-CVE2008-5353	1	6247.0000	5400.
	Tab25000000000000000000000000000000000000	19 KB BUD Elo	0E 02 2011 14/E0	05.02.2011 14:59	Trojan	Generic.dxltfu	1	6247.0000	5400.
	Tubesestor 2000.000		05.02.2011 14.39	05.02.2011 14:59	Trojan	Generic.dxltwx	1	6247.0000	5400.
	Im / db25e3br323U.bup	441 KB BUP File	05.02.2011 14:59	05.02.2011 14:59	Trojan	Generic.dxltfu	1	6247.0000	5400.
	@ /db25e3bdb20.bup	18 KB BUP File	05.02.2011 14:59	05.02.2011 14:59	l rojan	Generic.dxltwx	1	6247.0000	5400.
	7db25e3bc2870.bup	17 KB BUP File	05.02.2011 14:59	05.02.2011 14:59	Trojan	Generic.dxlsym	1	6247.0000	5400.
	🛅 7db25e3b313bf0.bup	17 KB BUP File	05.02.2011 14:59	05.02.2011 15:00	Trojan	Exploit-byteventy Evoloit-CVE2010-0094	1	6247.0000	5400
	🛅 7db25e3b2f1ac0.bup	17 KB BUP File	05.02.2011 14:59	05.02.2011 15:00	Trojan	Exploit-CVE2010-0034	1	6247.0000	5400
	7db25e3b2c1db0.bup	17 KB BUP File	05.02.2011 14:59	00.02.2011 10.00	riopan	Enplox 0+12010-0004		0241.0000	0400. V
	0 7db25e3b292870.bup	17 KB BUP File	05.02.2011 14:59	<					>
	7db25f011bc0.bup	3 KB BLIP File	05.02.2011 15:00						
	7db25f0111f0 bup	3 KB BLID File	05 02 2011 15:00						
		J KD DUP Fild	05.02.2011 15:00			OK	Cancel	Apply	Help
	10025FUU45U.DUp	5 KB BUP HIE	05.02.2011 15:00						Linih
	I 7db25e3b3b3df0.bup	6 KB BUP File	05.02.2011 15:00						
	🔟 7db25e3b3b3900.bup	6 KB BUP File	05.02.2011 15:00						
	🖾 7db25e3b3b20a0.bup	6 KB BUP File	05.02.2011 15:00						

H Hex Workshop - [7db25e3a1014e0.bup]							
Lie Edit Disk Options Iools Window Help _ 리 가							
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 32 42 5 26 27 28 29 30 31 32 33 0123456789ABCDEF0123456789ABCDEF01 00002040 FF							
00002244 08 1E 03 05 04 2E 08 13 57 5F 67 60 29 18 0F 08 1E 03 05 04 22 05 1F 18 57 58 5E 67 60 29 18 0F 08 1E							
x [13 instances of 'strings' found in 7db25e3a1014e0.bup 🏦 👬 🕼 🖓 💥							
SHI Signed Byte -46 SHI Unsigned Byte -46 SHI Unsigned Byte 208 SHI Signed Shot 1:2336 SHI Signed Shot 1:2336 SHI Signed Shot 1:2336 SHI Signed Cong -55700500 SHI Signed Cong -57500500 SHI Signed Cong -57500500 SHI Signed Cong -57500500 SHI Signed Cong -57500500 SHI Signed Cong -56593709+159 SHI Float -5.66593709+159 SHI Float -5.66593709+159 SHI Float -5.66593709+159 SHI Float -5.66593709+159 SHI Float -6.65 SHI Float -5.6659370+159 SHI Float -6.66							
ready Offset: 0 Value: -12336 (4096 bytes (OVR (MOD)READ							

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.

		_ 7 🗙
Man File Lat Lisk Options Tools Window Fielp G 日 る 後 よ ト 日 日 日 マ マ 単 晶 都 都 2	[™] ‰ [™] [™] [™] [™] [™] [™] [™]	- 0 X
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 1 0000000 00 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 0000034 00 00 00 00 00 00 00 00 00 00 00 00 00	15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 0123456789ABCDEF0123456789ABC 00	DEF01
x offset: 0 [0×0000000]	C Decimal · Hex 83 4	la a X
881 Signed Byte -48	Apply On Length 🖲	
Bill Unsigned Byte 208 Bill Unsigned Short -12336 Bill Unsigned Short 53200 Self Signed Long -53703600 Self Signed Long -375926366 Sill Unsigned Quad -222827175691174256 Sill Float -4.2027381e+019 Sill Doble -5.8639379e+159 Sill DOS Date ISBI DOS Date Sill Tiput -3281 tiput		
God Data Inspector Structure Viewer	📗 🖺 Compare 🔣 Checksum 🕅 Find 🗢 Bookmarks 📋 Output	
Ready	Offset: 0 Value: -12336 4096 bytes	OVR MOD READ
Hex Workshop - [7db25e3a1014e0.bup] Image: End Data Options Looks Window Help Image: Comparison of the two options and the two options and twooptions and two options and two options and	Sa 19 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	_ - ×
Hex Workshop - [7db25e3a1014e0.bup]	Image: Section 1 Image: Section 2 Image: Section 2 <t< td=""><td>DEF01 eMino (A) or=0. Creat 1.6T d Tim rOFFi (B) ile_0 y</td></t<>	DEF01 eMino (A) or=0. Creat 1.6T d Tim rOFFi (B) ile_0 y
Hex Workshop - [7db25e3a1014e0.bup]	Image: Image	DEF01 eMino A or-0. Creat Creat 16T d Tim rrOFFi ile_0 store
Hex Workshop - [7db25e3a1014e0.bup]	Image:	DEF01 eMino or-0. Creat 16T d Tim rOFFi ile_0
Hex Workshop - [7db25e3a1014e0.bup] Ele Edt Disk Options Icols Window Help Image: State	Image: Section 1 Image: Section 2 Image: Section 2 <t< td=""><td>DEF01 eMino or-0. Creat 16T d Tim rOFFI ile_0 </td></t<>	DEF01 eMino or-0. Creat 16T d Tim rOFFI ile_0

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)

H Hex Workshop - POISON2.EXE		- 7 🛛
Eile Edit Disk Options Iools Window Help		
B POISON2.EXE	🗙 🛱 recovered_file.exe.t	
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 012456789ABCDE 00126975 60 43 9 5 2 3 7 FE 67 7 8 9 11 12 13 14 012456789ABCDE 00126975 60 43 9 5 2 7 7 9 B 7 67 7 19 B 7 68 37 36 38 7 02 68 67 7 7 18 18 7 13 84 7 14 15 14 012 5 5 84 10 11 12 13 14 012456789ABCDE 00127005 A4 2 48 16 16 18 83 17 7 29 28 14 30 11 13 14 13 14 14 14 14 14 14 14 14 14 14 14 <	0 1 2 3 4 5 6 7 8 9 10 11 12 13 1 ■ 00127405 0F 30 60 MB 60	4 0123456789ABCDE .0 22318131833 6 38336833 83368 8 38433633 83368 8 335833633 8336 8 3358336336 8 3358336336 9 83358336 9 83358336 9 83358336 1 833583 1 833583 1 83358 1 83558 1 8355858 1 83558 1 8355858 1 83558
Image: Construction of the second s	POISON2.EXE vs recovered_file.exe.t	
9#7 Signed Byte 67 9#1 Signed Byte 67 18#1 Unsigned Shot -25021 18#1 Signed Long -81124797 32#1 Unsigned Long -81124797 32#1 Unsigned Long -81124797 32#1 Unsigned Long -81124797 32#1 Unsigned Long -81124797 32#1 Float -3.8952202e+021 6*WIT DATE -3.8952202e+188 6*WIT DATE -3.9952202+188 6*WIT DATE 19:50:06 6*WIT FLETIME 32#1 time t	Source Out Count Target Coun	Count ♥
Otata Inspector () Structure Viewer	Offset: 126976 Value: -25021	4283756 bytes OVR MOD READ

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.

C:\WINDOWS\system32\cmd.exe	- 0	×
Mcafee Virusscan BUP File Restore Utility [http://www.mertsarica.com]		
<pre>[Details] DetectionName=Generic.dx!sym DetectionType=1 EngineMajor=5400 EngineMinor=1158 DATMajor=6247 DATMinor=0 DATType=2 ProductID=12060 CreationYear=2011 CreationMonth=2 CreationMonth=2 CreationMonth=5 CreationHour=15 CreationMinute=6 CreationSecond=36 TimeZoneName=E. Europe Standard Time TimeZoneOffset=-120 NumberOfFiles=1 NumberOfValues=0</pre>		
[File_0] ObjectType=5 OriginalName=C:\MSF3\MSF3\EXTERNAL\SOURCE\VNCDLL\OUTPUT\.SUN\TEXT-BASE\VNCDL L.SVN-BASE	L.DI	
[*] Restored successfully -> UNCDLL.DLL.SUN-BASE		
C:\QUARANTINE>_		•

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 :)