Antivirüsler günümüzün vazgeçilmez güvenlik katmanlarından birini oluşturmaktadır. Bilgi güvenliği mimarisinde Derinlemesine Savunma (Defense in Depth) ilkesinin bir parçasını oluşturan antivirüslerin; başlı başına bir koruma değil, aslında diğer bütün güvenlik önlemleri gibi "bir zorlaştırıcı faktör" olduğu unutulmamalıdır. Temel prensiplerden de bilindiği üzere %100 güvenlik şeklinde bir yaklaşım yoktur ve her katmanı aşmak için çeşitli yöntemler bulunmaktadır. Antivirüslerin imza kontrolünü aşmak için ise "imza tespiti" ve "imza manipülasyonu" gibi yöntemler de kullanılmaktadır.

Atlatma yöntemini incelemeden önce antivirüslerin imza kontrolünde kullandığı genel yaklaşıma kısaca değinmek yerinde olacaktır. Temel olarak imza yaratma yöntemi; "Byte-Signature", "Hash-Signature" ve "Heuristic" olarak üç başlık altında toplanabilmektedir. Byte-Signature yönteminde, ard arda gelen binary (ikilik) kodun bir kısmı kullanılmaktadır. Bu kod parçacığı, zararlı yazılımın varyantlarında değişmeyecek türden bir noktadan seçilir. Bazen de zararlı yazılımın içindeki text (string) alanlarından seçilir. Böylece kodun işlevi değişse bile değişmeyen text, label, title, caption gibi string formatındaki öğeler sayesinde tespit gerçekleştirilebilir.

Hash-Signature yönteminde zararlı yazılımın HASH'I (kriptografik özeti) alınır. Ve imza olarak kullanılır. Bu yöntemde zararlı yazılımın 1 byte kodu değişse dahi tespit işlemi gerçekleştirilemez. Heuristic yöntemde ise kodun içeriğinden çok dosyanın davranışları tespit edilmeye çalışılır. Hatalı tespitlere (false positive) neden olabilecek bir yöntemdir ancak kodun içeriğinden mümkün olduğunca bağımsız olması önemli avantajlar da sağlamaktadır.

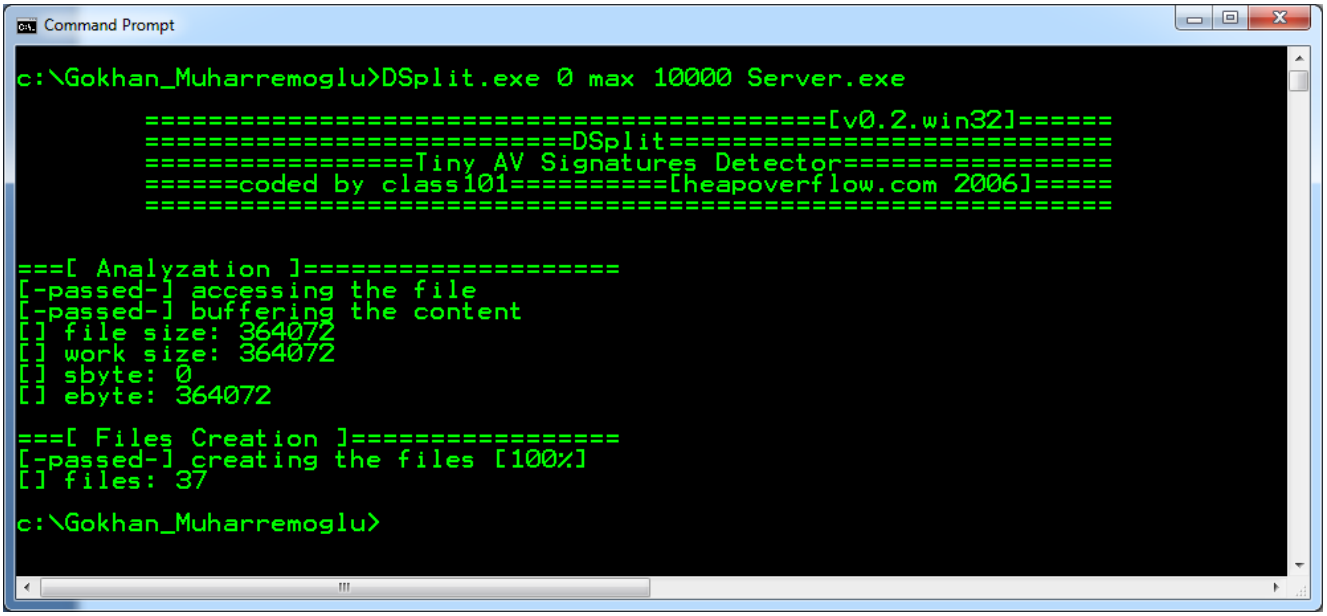
Yukarıdaki yöntemler hakkında fikir sahibi olmak ve atlatılmaya çalışılan antivirüsün nasıl bir imza yönetimini kullandığını bilmek, kısaca bilgi toplamak, her penetrasyon testi çalışmasında olduğu gibi yine ilk adım olacaktır. Bunun için seçilen zararlı yazılımın türü ve atlatılacak antivirüsün o türdeki dosyalar için uyguladığı genel imza alma yöntemini tespit etmek gereklidir.

Antivirüs tarafından tespit edilmemesini sağlamak için dünyadaki ilk FTP Truva atı konseptlerinden biri olan ve bu nedenle çoğu imza veritabanına "FirstTime.b" gibi bir imza adıyla kayıtlı olan SpyMasterSnake FTP Trojan Server.exe dosyası örnek olarak seçilmiştir. Bir trojan olması ve kendi kodunu manipüle ederek sistemde yavrulama yöntemine gitmemesi, bu türdeki zararlı yazılımları daha statik ve antivirüsler için tespit edilmesi kolay hale getirmektedir. Bu nedenle çoğu antivirüs yazılımı bu tarz yazılımlara "Hash-Signature" yöntemi ile yaklaşmaktadır. Ancak saldırgan tarafından bakıldığında, bu durum antivirüsleri atlatmak için bir fırsat olarak değerlendirilebilir.

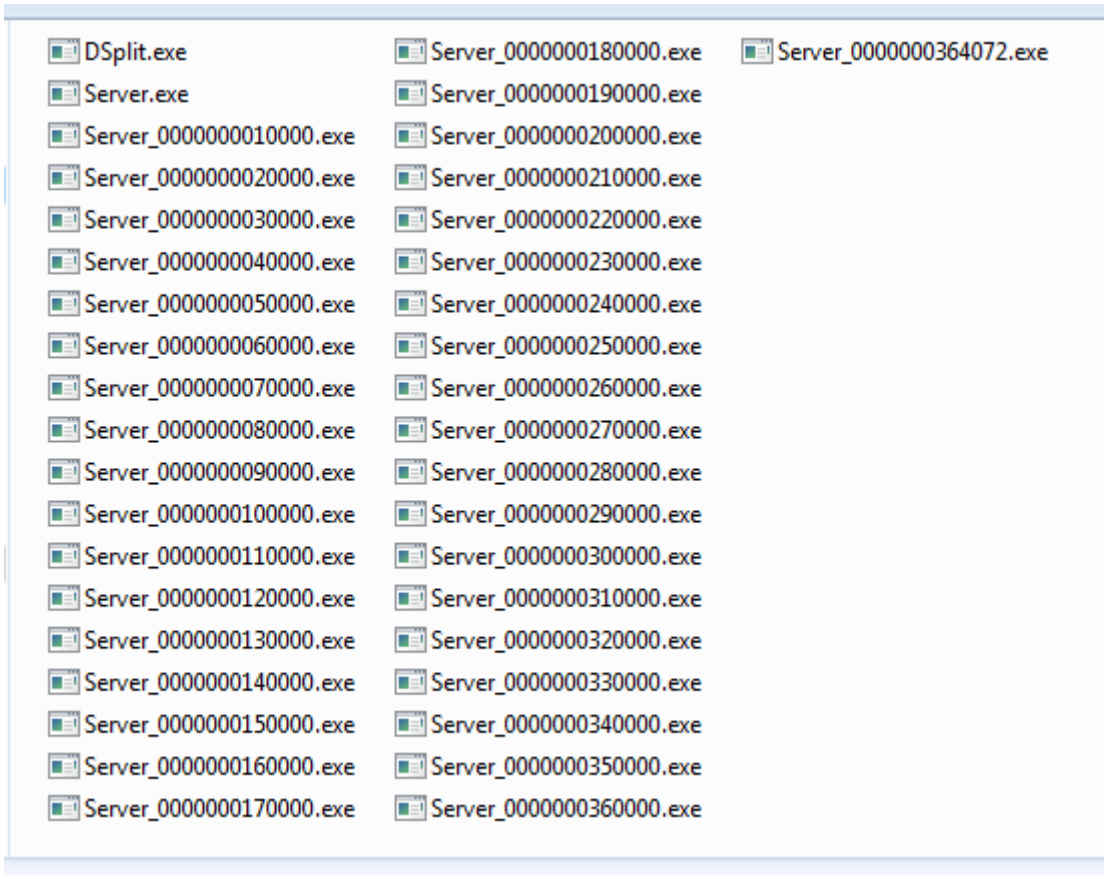
Yukarıdaki öngörüye rağmen bir imza analizi yapmak yerinde olacaktır. Bunun için DSplit isimli dosyaları parçalara bölerek imza tespitine olanak sağlayan bir araç kullanılacaktır. Yapılacak olan analizin mantığı şu şekildedir:

- Exe dosyası ilk byte'ından son byte'ına kadar bölünür
- Her dosyanın bir önceki dosyadan büyük olması ve bir önceki dosyayı da içermesi sağlanır
- Her bir dosya arasındaki boyut farkı sabit tutulur
- Antivirüs tarafından tespit edilen ilk dosya parçası imzanın olduğu bölüm olarak seçilir
- Bu parça daha ufak parçalara ayrılarak manipüle edilebilecek kod parçacığına ulaşılır
- Kod parçacığına ulaşılır ve kod Hex Editor ile manipüle edilir

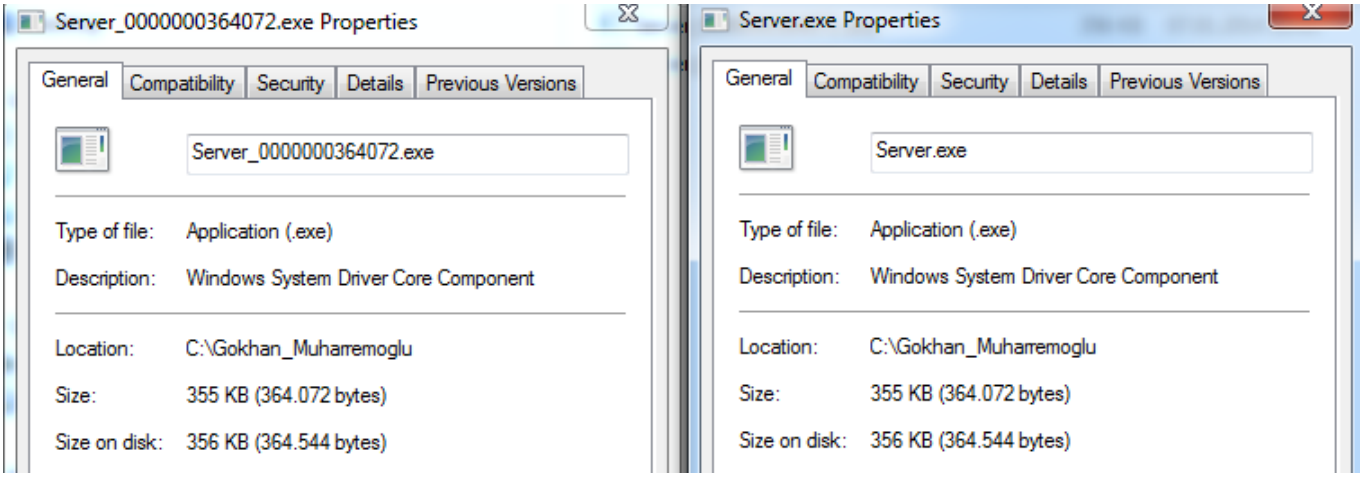
Seçilen zararlı yazılım (Server.exe) ilk byte'ından (0) son byte'ına kadar (max) 10000 byte'lık artan bölümler halinde parçalara ayrılmıştır.

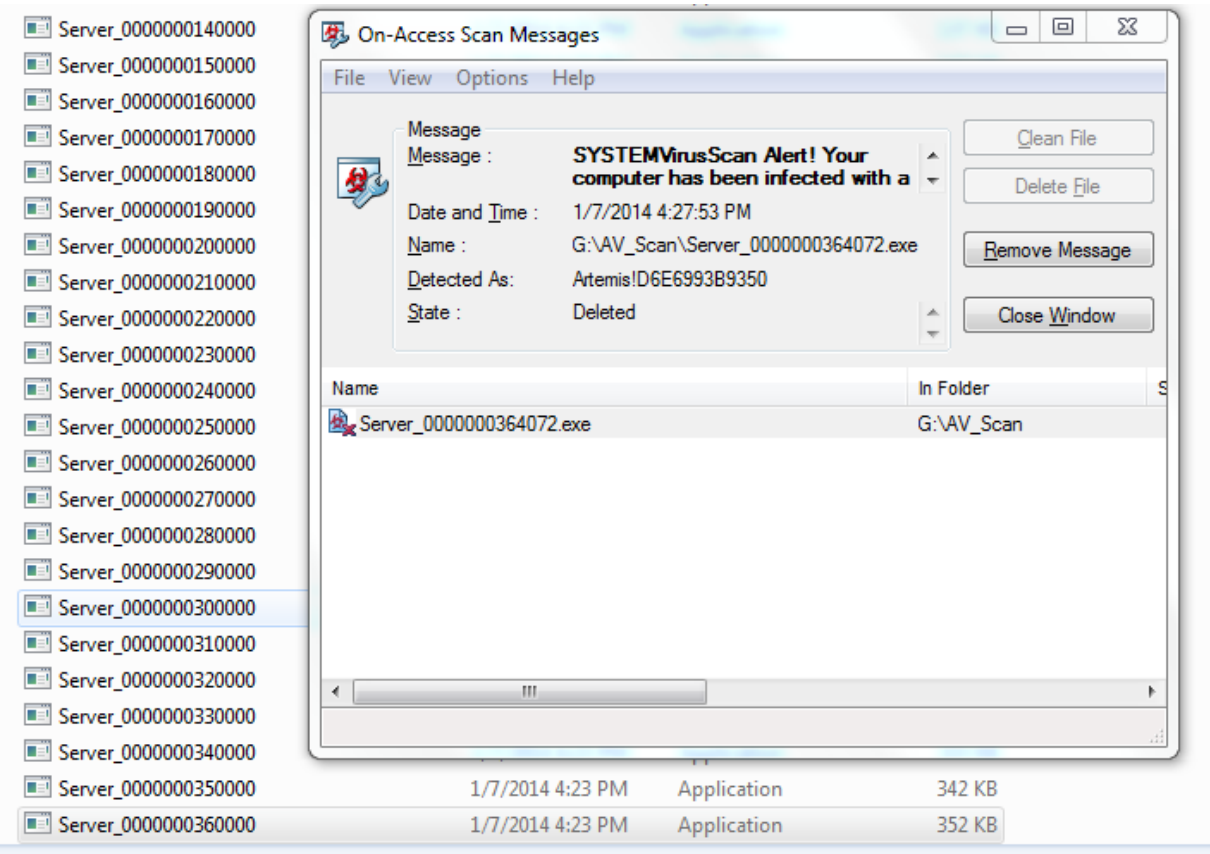


Toplamda 37 tane dosya oluşmuştur. Her dosya adı aynı zamanda dosyanın büyüklüğünü ve gelinen Offset'in byte cinsinden değerini vermektedir.

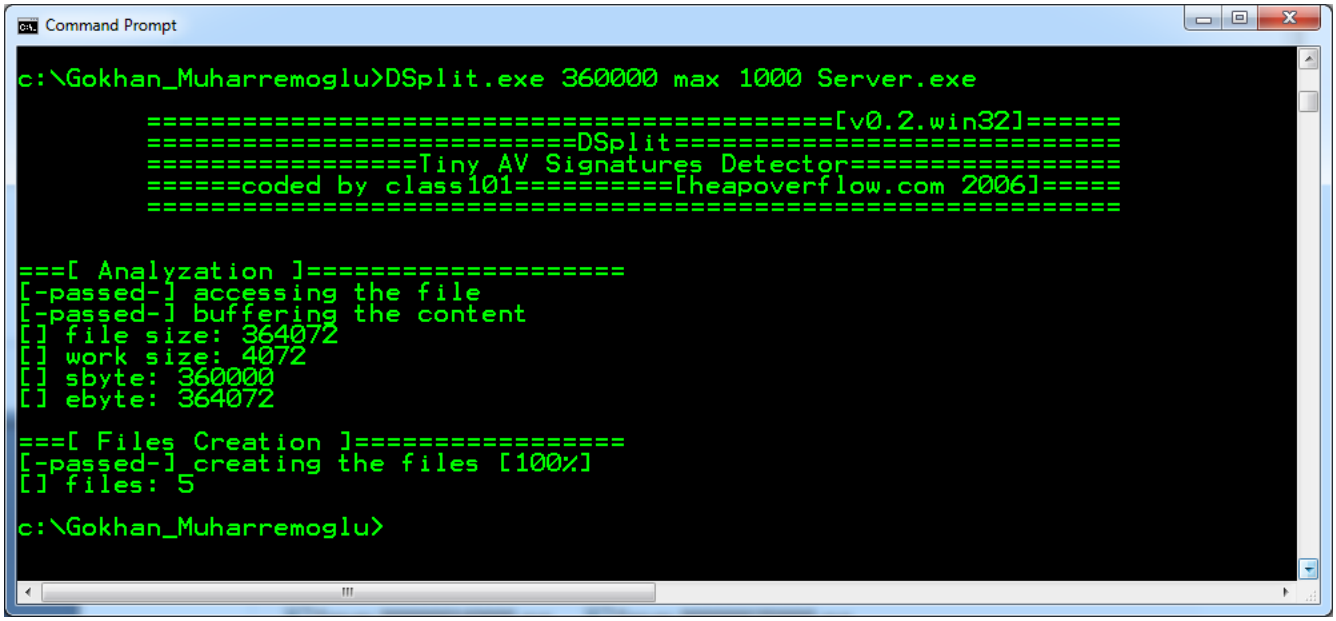


Oluşan son dosya diğerlerinden farklı olarak “364072” ile adlandırılmıştır. Çünkü bu bütün programın tam uzunluğu ve exe dosyasının kendisine denk gelmektedir. “360000” olarak adlandırılan dosya, orijinal exe dosyasından “4072” byte daha eksiktir.

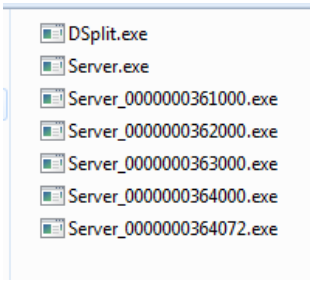




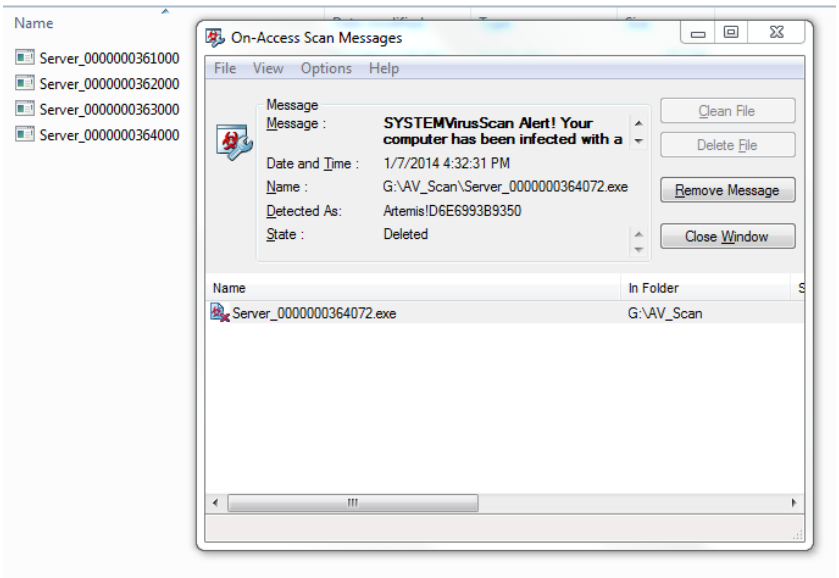
Antivirüs orijinal “Server.exe” dosyasının aynısı olan “364072” olarak adlandırılmış dosyayı zararlı yazılım olarak tespit etmiş, diğer parçalar için uyarı vermemiştir.



Başlama noktası olarak "360000" byte alınarak geri kalan kısım bu sefer 1000 byte'lık artan değerlerde bölünmüştür ve imza bu kısımda aranmaya başlanmıştır.

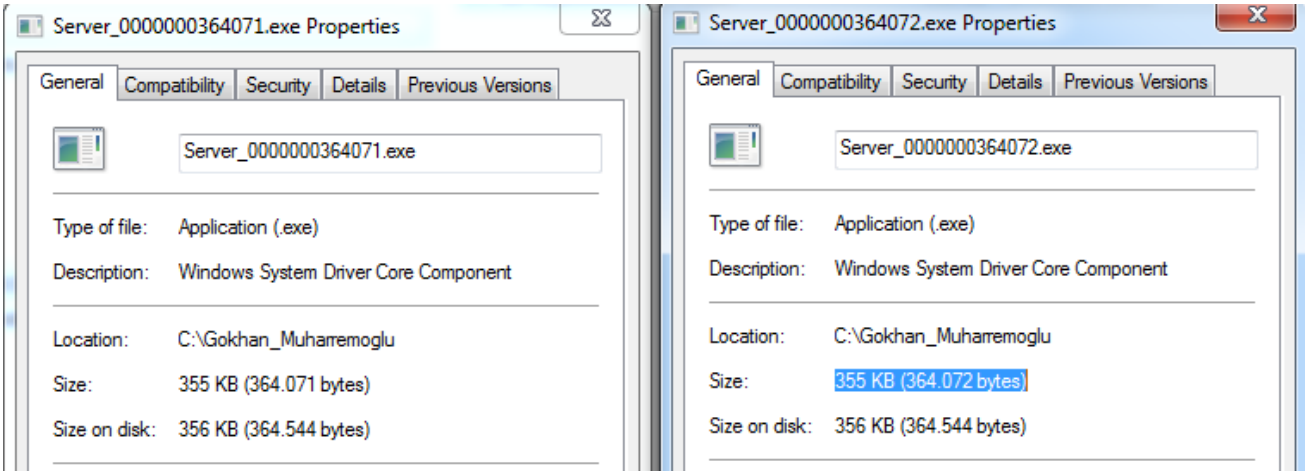


Bu sefer oluşan dosya sayısı "5" olmuştur.

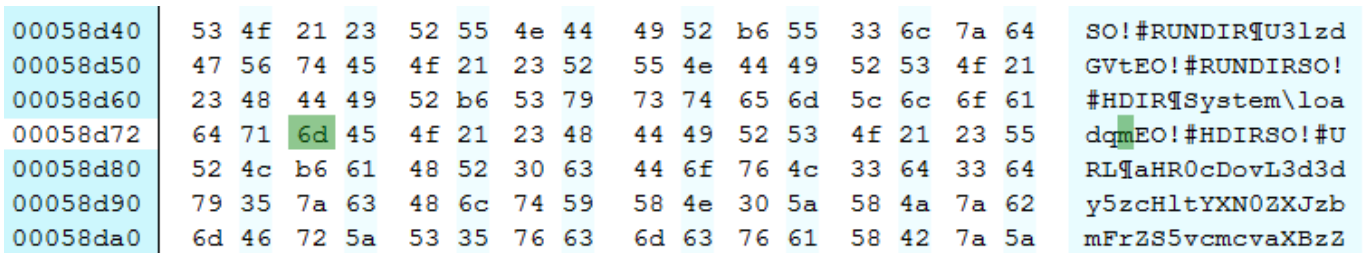


Antivirüs "364072" isimli tam boyutlu dosyayı yine zararlı olarak tespit etmiştir.

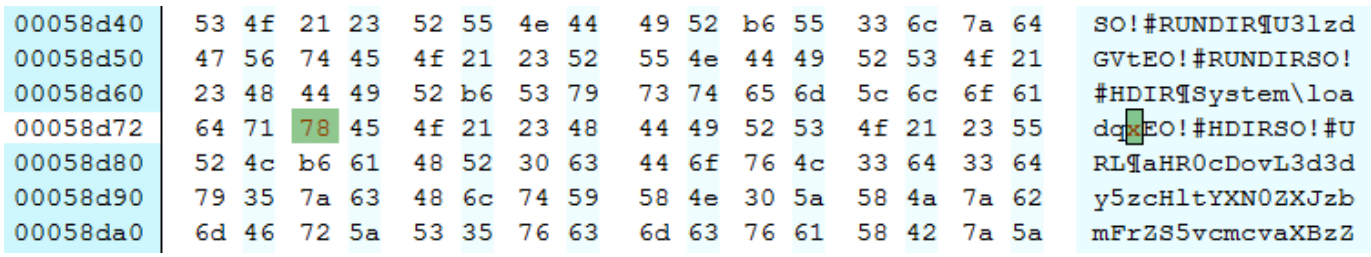
Son iki deneme de son parçanın zararlı yazılım olarak tespit edilmesi bu antivirüsün imza yöntemi olarak Hash-Signature yöntemini kullandığına işaret etmektedir. Bunun doğrulaması için dosya 1 byte farklı iki ayrı dosyaya bölünebilir. Ve antivirüsün "364071" dosyasını tespit etmediği görülebilir.

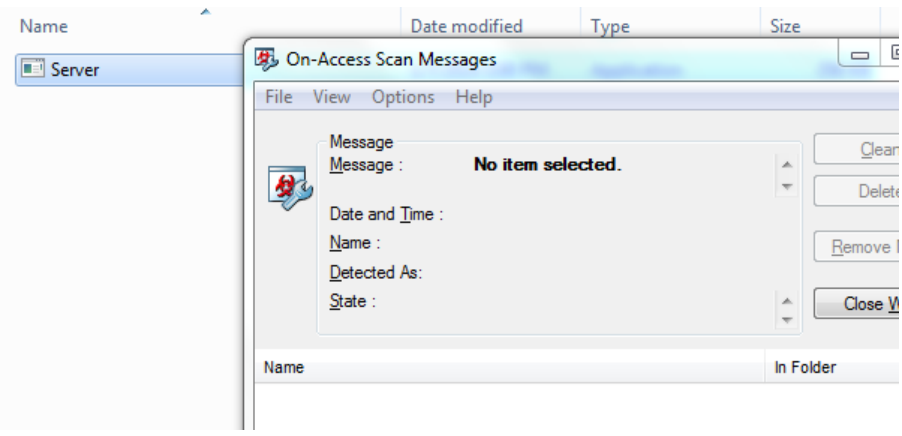


Bundan sonra atılacak adım ise zararlı yazılımın HASH değerinin değişmesini sağlamak olacaktır. Hex Editor ile açılan zararlı yazılımın, yazılımını işleyişi bozmayacak bir değerini değiştirmek (text, vb.) ya da Resource Editor türevi bir araç ile resim, dialog kutusu ve benzeri bir alanı değiştirmek, HASH değerinin değişmesi için yeterli olacaktır.



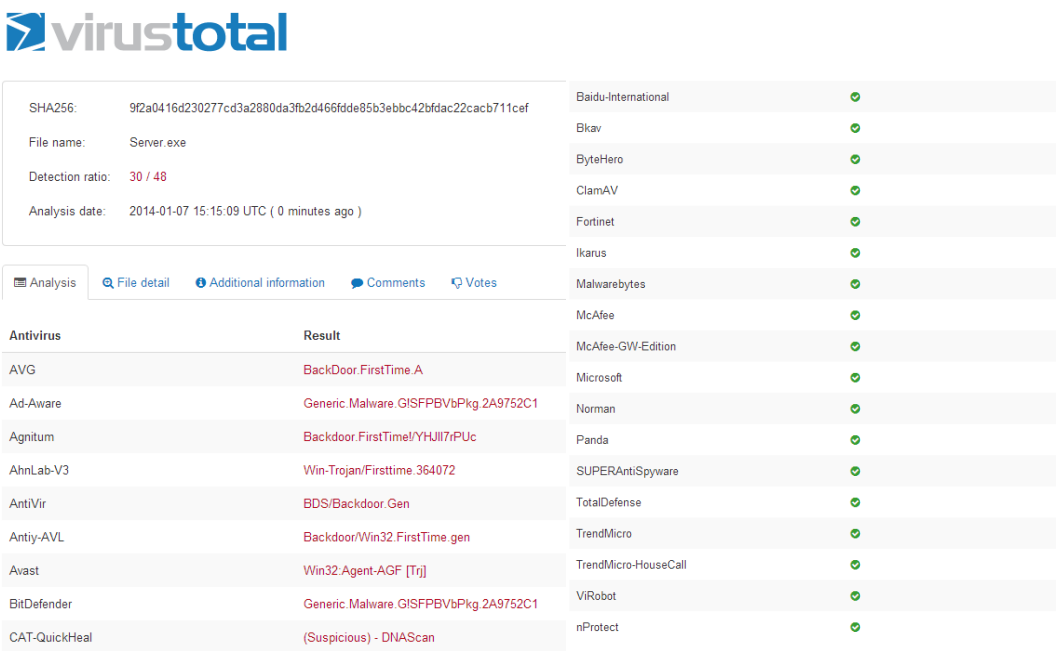
Yazılım içindeki bir text değeri Hex Editor ile değiştirilmiştir.





Artık “Server.exe” dosyasının antivirüs tarafından tespit edilemediği görülmektedir.

Virustotal web sitesi aracılığıyla yapılan testte, HASH değeri değiştirilen dosyanın tespit edilme oranı 48'de 30 olarak belirlenmiştir. Bu değer, dosya manipüle edilmeden önce 48'de 40'dır. Hash-Signature yöntemini kullanan 10 antivirüs, sadece 1 byte kodun değiştirilmesiyle atlatılabilmiştir.

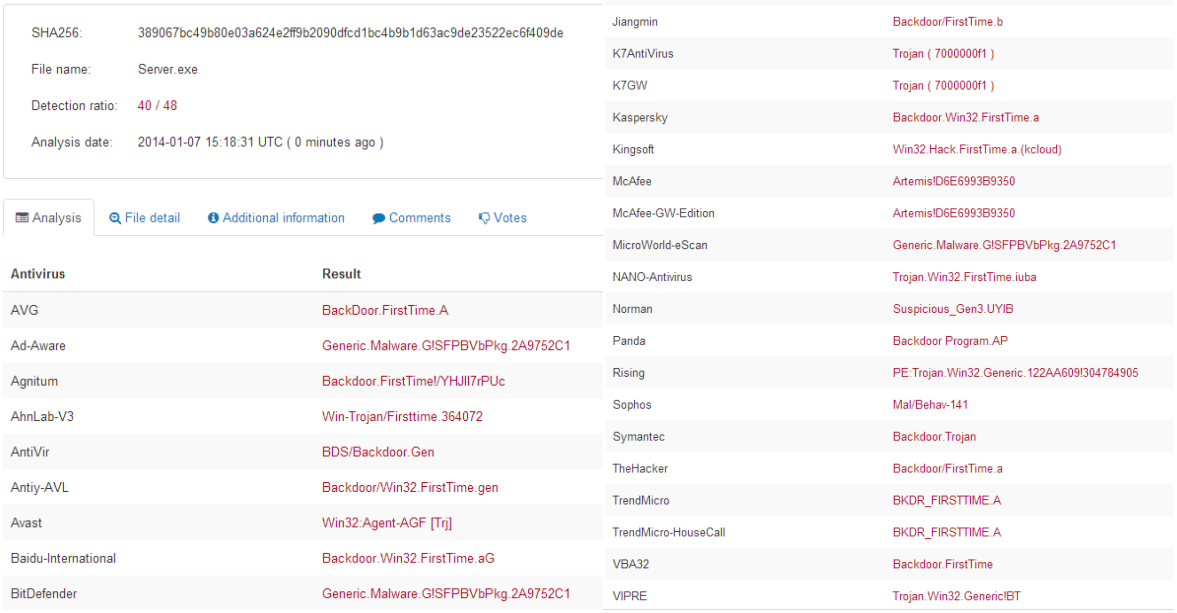


virustotal

SHA256: 9f2a0416d230277cd3a2880da3fb2d466fdde85b3ebbc42bfdac22cacb711cef
File name: Server.exe
Detection ratio: 30 / 48
Analysis date: 2014-01-07 15:15:09 UTC (0 minutes ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result
AVG	BackDoor.FirstTime.A
Ad-Aware	Generic.Malware.G!SFPBVbPkg.2A9752C1
Agnitum	Backdoor.FirstTime!/YHJll7rPUc
AhnLab-V3	Win-Trojan/Firsttime.364072
AntiVir	BDS/Backdoor.Gen
Antiy-AVL	Backdoor/Win32.FirstTime.gen
Avast	Win32:Agent-AGF [Trj]
BitDefender	Generic.Malware.G!SFPBVbPkg.2A9752C1
CAT-QuickHeal	(Suspicious) - DNAScan
Baidu-International	✓
Bkav	✓
ByteHero	✓
ClamAV	✓
Fortinet	✓
Ikarus	✓
Malwarebytes	✓
McAfee	✓
McAfee-GW-Edition	✓
Microsoft	✓
Norman	✓
Panda	✓
SUPERAntiSpyware	✓
TotalDefense	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
ViRobot	✓
nProtect	✓



SHA256: 389067bc49b80e03a624e2ff9b2090dfcd1bc4b9b1d63ac9de23522ec6f409de
File name: Server.exe
Detection ratio: 40 / 48
Analysis date: 2014-01-07 15:18:31 UTC (0 minutes ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result
AVG	BackDoor.FirstTime.A
Ad-Aware	Generic.Malware.G!SFPBVbPkg.2A9752C1
Agnitum	Backdoor.FirstTime!/YHJll7rPUc
AhnLab-V3	Win-Trojan/Firsttime.364072
AntiVir	BDS/Backdoor.Gen
Antiy-AVL	Backdoor/Win32.FirstTime.gen
Avast	Win32:Agent-AGF [Trj]
Baidu-International	Backdoor.Win32.FirstTime.aG
BitDefender	Generic.Malware.G!SFPBVbPkg.2A9752C1
Jiangmin	Backdoor/FirstTime.b
K7AntiVirus	Trojan (7000000f1)
K7GW	Trojan (7000000f1)
Kaspersky	Backdoor.Win32.FirstTime.a
Kingsoft	Win32.Hack.FirstTime.a.(kcloud)
McAfee	Artemis!D6E6993B9350
McAfee-GW-Edition	Artemis!D6E6993B9350
MicroWorld-eScan	Generic.Malware.G!SFPBVbPkg.2A9752C1
NANO-Antivirus	Trojan.Win32.FirstTime.iuba
Norman	Suspicious_Gen3.UYIB
Panda	Backdoor Program.AP
Rising	PE:Trojan.Win32.Generic.122AA609!304784905
Sophos	Mal/Behav-141
Symantec	Backdoor.Trojan
TheHacker	Backdoor/FirstTime.a
TrendMicro	BKDR_FIRSTTIME.A
TrendMicro-HouseCall	BKDR_FIRSTTIME.A
VBA32	Backdoor.FirstTime
VIPRE	Trojan.Win32.Generic!BT

Diğer antivirüsleri atlatmak için de alınan imza ve imza yönteminin tespit edilmesi gereklidir. Bu sayede tespit edilme oranı yapılacak olan sızma testi çalışması için makul bir seviyeye çekilebilir. Dosyanın farklı bir bölümünde alınan bir imza da bu yöntemle manipüle edilebilir.

Antivirüs veritabanında imzası **"H"** olarak kaydedilmiş 12 Byte büyüklüğündeki bir dosyasının 3 Byte, 2 Byte ve 1 Byte gözlem aralıklarıyla incelenmesi ile imzanın tespit edilmesi işleminin temsili görseli aşağıdaki şekilde gösterilmiştir. Dosya isimleri dosya uzunlukları ile aynıdır.

1. Gözlem aralığı 3 Byte

3.exe	6.exe	9.exe	12.exe (Tam Dosya)
A	A	A	A
B	B	B	B
C	C	C	C
	D	D	D
	E	E	E
	F	F	F
		G	G
		H	H
		I	I
			J
			K
			L

2. Gözlem aralığı 2 Byte

6.exe	8.exe	10.exe	12.exe (Tam Dosya)
A	A	A	A
B	B	B	B
C	C	C	C
D	D	D	D
E	E	E	E
F	F	F	F
	G	G	G
	H	H	H
		I	I
		J	J
			K
			L

3. Gözlem aralığı 1 Byte

6.exe	7.exe	8.exe	9.exe
A	A	A	A
B	B	B	B
C	C	C	C
D	D	D	D
E	E	E	E
F	F	F	F
	G	G	G
		H	H
			I

Sızma testleri sırasında kurumlar tarafından "başlı başına güvenlik" çözümü olarak görülen antivirüslerin aslında 1 byte farkla geçilebileceği gerçeğini göz ardı etmemek için kurumsal güvenliği bütün yönleri ile temel prensip ve ilkeler doğrultusunda hayata geçirmek ve katmanlı mimariyi, derinlemesine savunmayı bir alışkanlık haline getirmek gereklidir.

İletişim:
Gökhan MUHARREMOĞLU
Bilgi Güvenliği Uzmanı/Danışman

gokhan.muharremoglu@iosec.org
http://www.linkedin.com/in/gokhanmuharremoglu

Referanslar

[1]-An Intro to Creating Anti-Virus Signatures - **http://hooked-on-mnemonics.blogspot.com/2011/01/intro-to-creating-anti-virus-signatures.html**
[2]-Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı Ve Savunma Öğelerinin İncelenmesi - YL Tezi, İstanbul Üniversitesi, Muharremoğlu, G. 2013 - **http://kutuphane.istanbul.edu.tr/**
[3]-IOSEC.ORG-**http://www.iosec.org**
[4]-Olası Zafiyetlerin Tahmininde Temel Bilgi Güvenliği Prensiplerinin Kullanılması - **https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/olasi-zafiyetlerin-tahmininde-temel-bilgi-guvenligi-prensiplerinin-kullanilmasi.html**
[5]-Megasecurity-**http://www.megasecurity.org/trojans/s/spymastersnake/Spymastersnake_ftptrojan.html**