

Sızma Testlerinde İmza Manipülasyonu Yöntemiyle Antivirüslerin Kolay Yoldan Atlatılması

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 incelemeye başlamadan önce antivirüslerin imza kontrolünde kullandığı genel yaklaşıma kısaca değinmek yerinde olacaktır. Temel olarak imza yaratma yöntemi; “Byte-Signature”, “HashSignature” 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 (o) son byte’ına kadar (max) 10000 byte’lık artan bölümler halinde parçalara ayrılmıştır.

```
Command Prompt
c:\Gokhan_Muharremoglu>DSplit.exe 0 max 10000 Server.exe

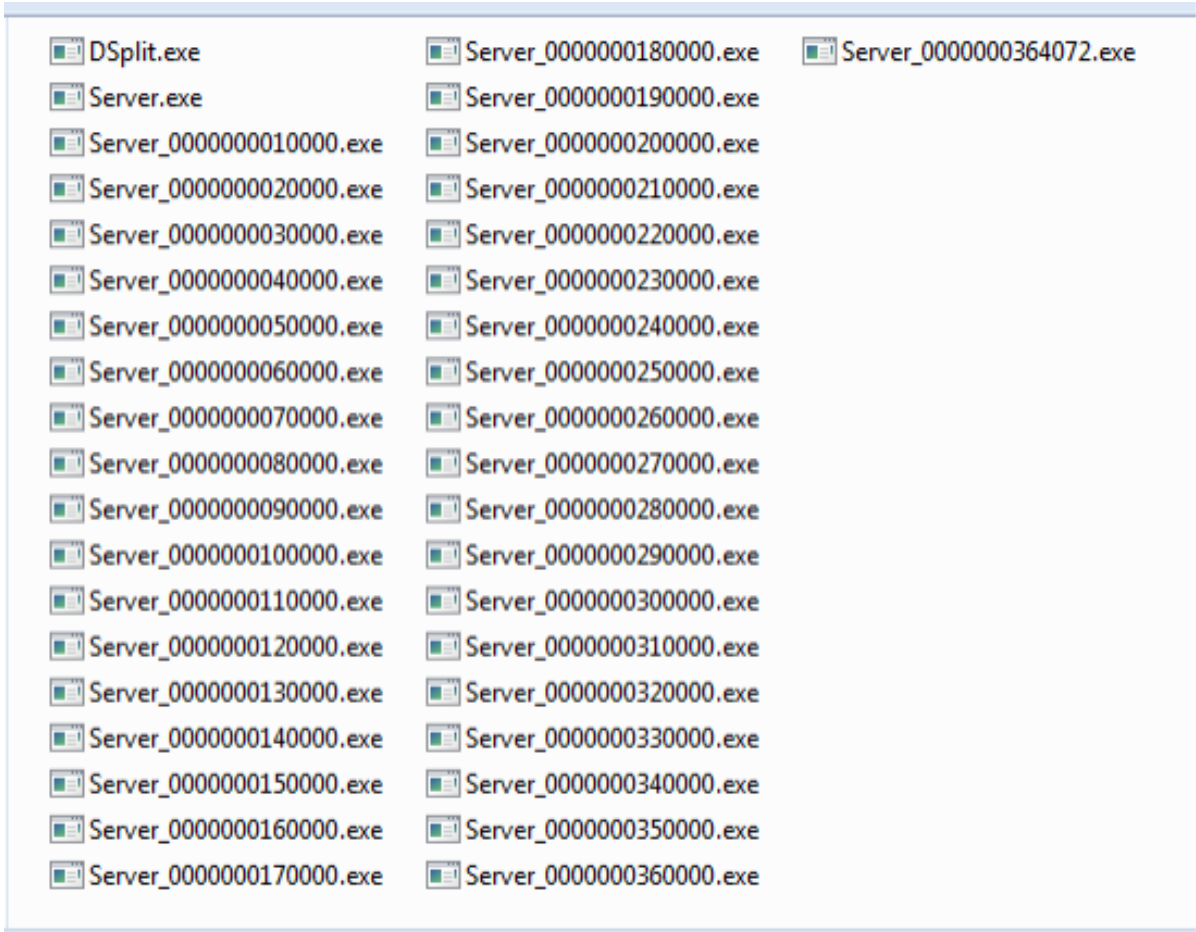
=====DSplit=====
=====Tiny AV Signatures Detector=====
=====coded by class101=====
=====

===[ Analyzation ]=====
[-passed-] accessing the file
[-passed-] buffering the content
[] file size: 364072
[] work size: 364072
[] sbyte: 0
[] ebyte: 364072

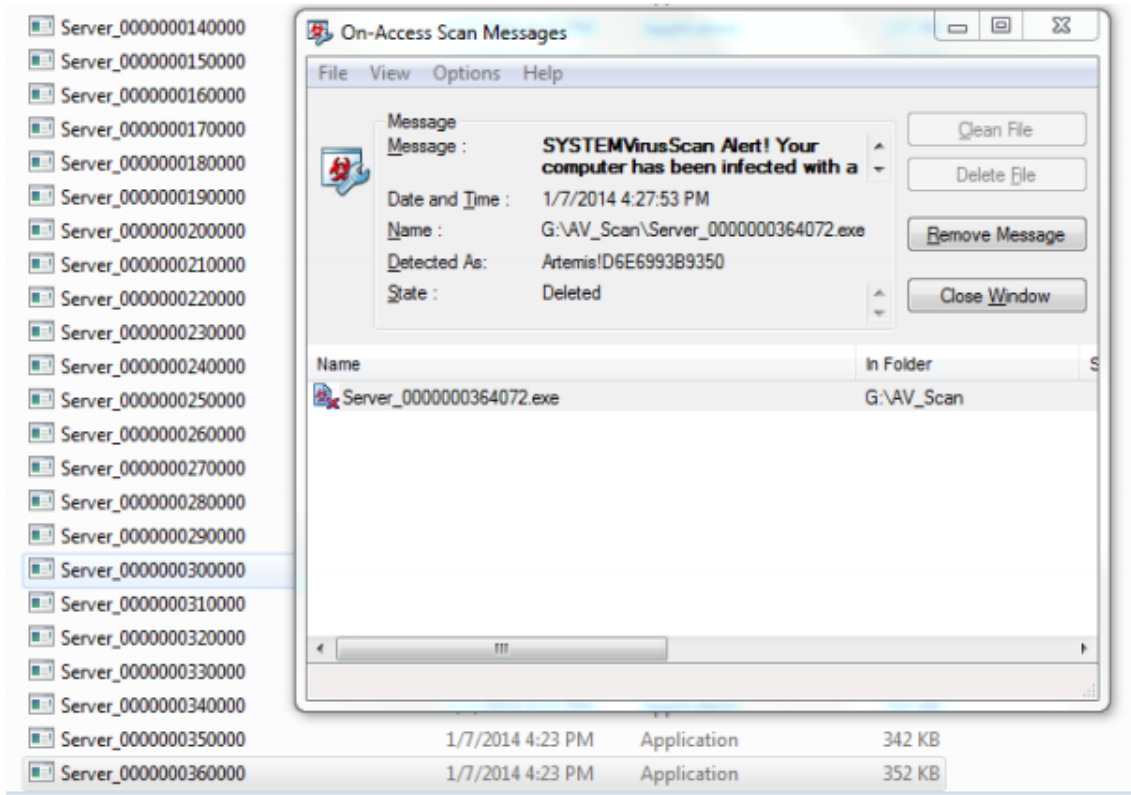
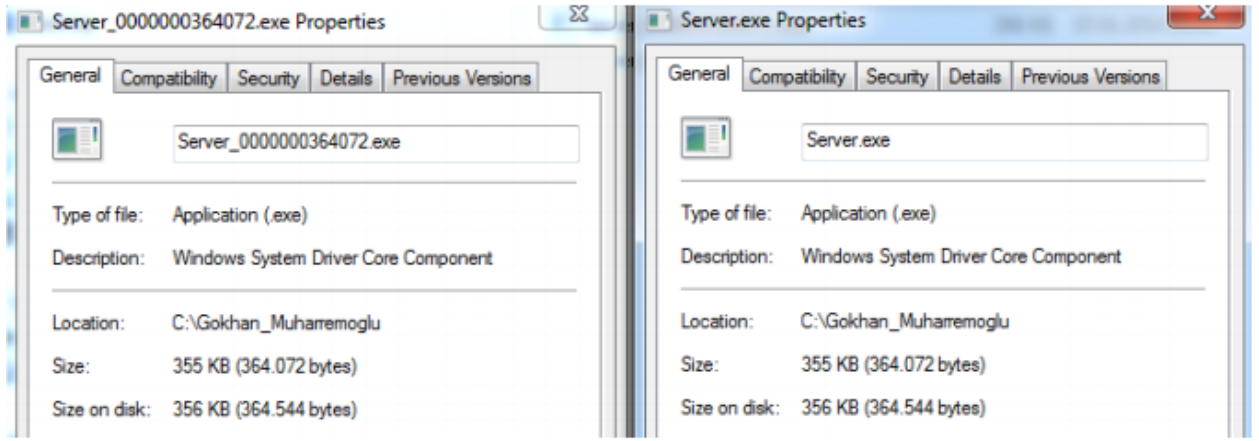
===[ Files Creation ]=====
[-passed-] creating the files [100%]
[] files: 37

c:\Gokhan_Muharremoglu>
```

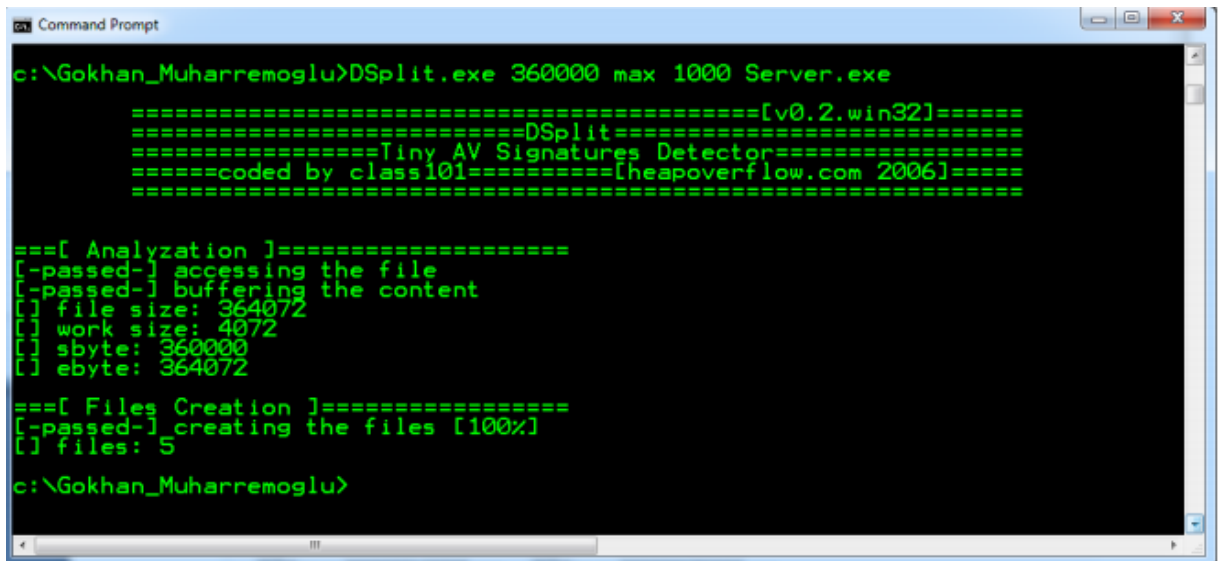
Toplamda 37 tane dosya oluşmuştur. Her dosya adı aynı zamanda dosyanın büyüklüğünü ve gelenin Offset'in byte cinsinden değerini vermektedir



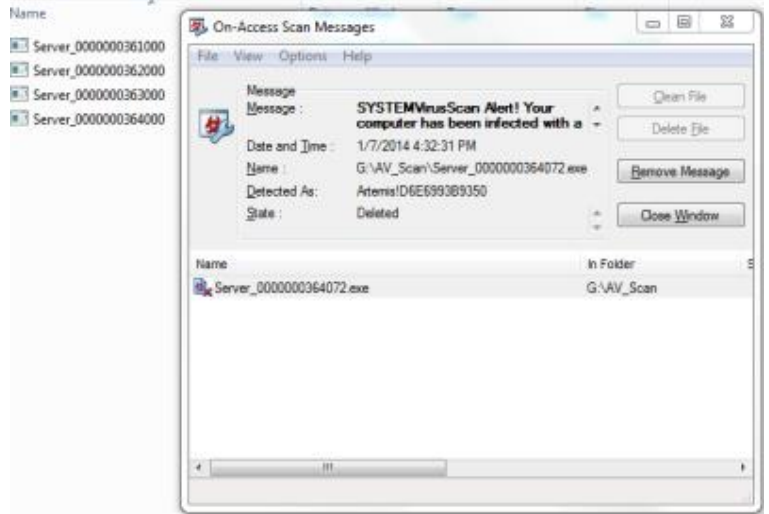
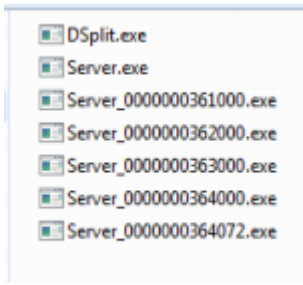
Oluşan son dosya diğerlerinden farklı olarak “364072” ile adlandırılmıştır. Çünkü bu bütün programın tam uzunluğu ve exe dosyasının kendisine denk gelmektedir. “360000” olarak adlandırılan dosya, orijinal exe dosyasından “4072” byte daha eksiktir.



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



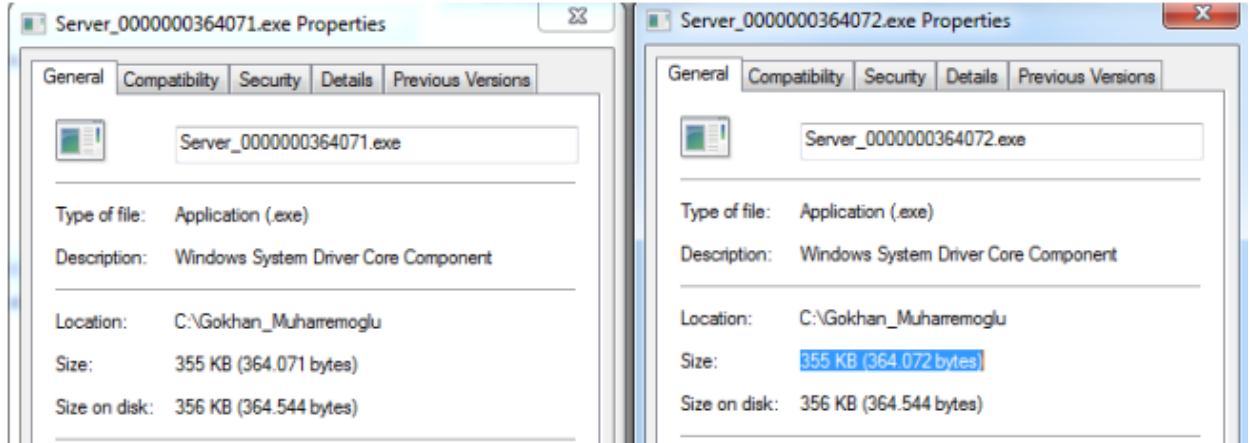
Başlama noktası olarak “360000” byte alınarak geri kalan kısım bu sefer 1000 byte’lık artan değerlerde bölünmüştür ve imza bu kısımda aranmaya başlanmıştır.



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.

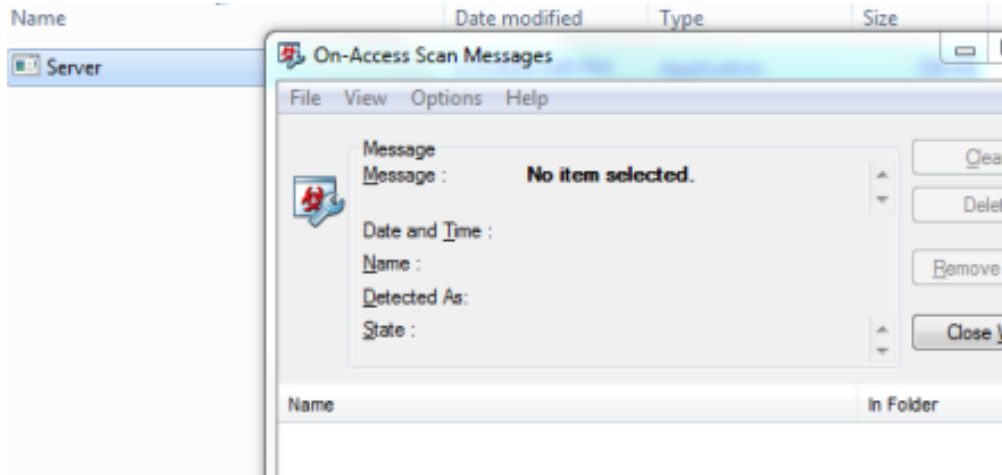


Bundan sonra atılacak adım ise zararlı yazılımın HASH değerinin değişmesini sağlamak olacaktır. Hex Editor ile açılan zararlı yazılımın, yazılımını işleyişi bozmayacak bir değerini değiştirmek (text, vb.) ya da Resource Editor türevi bir araç ile resim, dialog kutusu ve benzeri bir alanı değiştirmek,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

00058d40	53	4f	21	23	52	55	4e	44	49	52	b6	55	33	6c	7a	64	SO!#RUNDIRU31zd
00058d50	47	56	74	45	4f	21	23	52	55	4e	44	49	52	53	4f	21	GVtEO!#RUNDIRSO!
00058d60	23	48	44	49	52	b6	53	79	73	74	65	6d	5c	6c	6f	61	#HDIRSystem\loa
00058d72	64	71	6d	45	4f	21	23	48	44	49	52	53	4f	21	23	55	dcmEO!#HDIRSO!#U
00058d80	52	4c	b6	61	48	52	30	63	44	6f	76	4c	33	64	33	64	RLaHR0cDovL3d3d
00058d90	79	35	7a	63	48	6c	74	59	58	4e	30	5a	58	4a	7a	62	y5zcHltYXN0ZXJzb
00058da0	6d	46	72	5a	53	35	76	63	6d	63	76	61	58	42	7a	5a	mFrZS5vcmcvaXBzZ

Yazılım içindeki bir text değeri Hex Editor ile değiştirilmiştir.

00058d40	53	4f	21	23	52	55	4e	44	49	52	b6	55	33	6c	7a	64	SO!#RUNDIRU31zd
00058d50	47	56	74	45	4f	21	23	52	55	4e	44	49	52	53	4f	21	GVtEO!#RUNDIRSO!
00058d60	23	48	44	49	52	b6	53	79	73	74	65	6d	5c	6c	6f	61	#HDIRSystem\loa
00058d72	64	71	78	45	4f	21	23	48	44	49	52	53	4f	21	23	55	dcmEO!#HDIRSO!#U
00058d80	52	4c	b6	61	48	52	30	63	44	6f	76	4c	33	64	33	64	RLaHR0cDovL3d3d
00058d90	79	35	7a	63	48	6c	74	59	58	4e	30	5a	58	4a	7a	62	y5zcHltYXN0ZXJzb
00058da0	6d	46	72	5a	53	35	76	63	6d	63	76	61	58	42	7a	5a	mFrZS5vcmcvaXBzZ



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. HashSignature yöntemini kullanan 10 antivirüs, sadece 1 byte kodun değiştirilmesiyle atlatılabilmektedir.

SHA256:	9Qa0416d230277cd3a2890da3b2d469d8e85b3ebbc42b6dac22cacb711cef	Baidu-International	✓
File name:	Server.exe	Blav	✓
Detection ratio:	30 / 48	ByteHerc	✓
Analysis date:	2014-01-07 15:15:09 UTC (0 minutes ago)	ClamAV	✓
		Fortinet	✓
		Ikarus	✓
		Malwarebytes	✓
		McAfee	✓
		McAfee-GW-Edition	✓
		Microsoft	✓
		Norman	✓
		Panda	✓
		SUPERAntiSpyware	✓
		TotalDefense	✓
		TrendMicro	✓
		TrendMicro-HouseCall	✓
		VRBot	✓
		nProtect	✓

Analysis File detail Additional information Comments Votes

Antivirus	Result
AVG	BackDoor.FirstTime.A
Ad-Aware	Generic.Malware.GISFPBVbPkg.2A9752C1
Agnitum	Backdoor.FirstTime/YHJIT/PUC
AhriLab-V3	Win-Trojan/FirstTime.364072
AntiVir	BDS/Backdoor.Gen
Antiy-AVL	Backdoor/Win32.FirstTime.gen
Avast	Win32.Agent-AGF [Trj]
BitDefender	Generic.Malware.GISFPBVbPkg.2A9752C1
CAT-QuickHeal	(Suspicious) - DNAScan

SHA256:	389067bc49b80e03a624e2f9b2090dfcd1bc4b9b1d63ac9de23522ec6409de	Jiangmin	Backdoor/FirstTime.b
File name:	Server.exe	KTAntiVirus	Trojan (70880001)
Detection ratio:	40 / 48	KTGW	Trojan (70880001)
Analysis date:	2014-01-07 15:18:31 UTC (0 minutes ago)	Kaspersky	Backdoor.Win32.FirstTime.a
		Kingsoft	Win32.Hack.FirstTime.a (kcleud)
		McAfee	Artemis/D6E693B9350
		McAfee-GW-Edition	Artemis/D6E693B9350
		MicroWorld-eScan	Generic.Malware.GISFPBVbPkg.2A9752C1
		NANO-Antivirus	Trojan.Win32.FirstTime.luba
		Norman	Suspicious.Gen3.UYIB
		Panda	Backdoor.Program.AP
		Rising	PE.Trojan.Win32.Generic.122AA609347B4905
		Sophos	Mal/Behav-141
		Symantec	Backdoor.Trojan
		TheHacker	Backdoor/FirstTime.a
		TrendMicro	BACKR_FIRSTTIME.A
		TrendMicro-HouseCall	BACKR_FIRSTTIME.A
		VBA32	Backdoor.FirstTime
		ViPRE	Trojan.Win32.Generic/ST

Analysis File detail Additional information Comments Votes

Antivirus	Result
AVG	BackDoor.FirstTime.A
Ad-Aware	Generic.Malware.GISFPBVbPkg.2A9752C1
Agnitum	Backdoor.FirstTime/YHJIT/PUC
AhriLab-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.GISFPBVbPkg.2A9752C1

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 dosyanın 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	G
	H	H	H
	I	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.

(Dünya, 30.10.2018)

Gökhan Muharremoğlu

Siber Güvenlik Hizmetleri, Kıdemli Müdür

Email: gokhan.muharremoglu@pwc.com

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/>
- [4]-Olası Zafiyetlerin Tahmininde Temel Bilgi Güvenliği Prensiplerinin Kullanılması - <https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/olasi-zafiyetlerin-tahmininde-temel-bilgi-guvenligiprensiplerinin-kullanilmasi.html>
- [5]-Megasecurity http://www.megasecurity.org/trojans/s/spymastersnake/Spymastersnake_ftptrojan.html