ODA-TV HDD#6

Joshua Marpet, ACE

12/21/2011

Özet

DataDevastation , Soner Yalçın'ı temsilen Avukat Dr. Duygun Yarsuvat ve Avulat Hüseyin Ersöz'ün yapmış olduğu talep üzerine, ODA-TV'den kaldırılan sabit sürücü üzerinde, varsa, ne tür bir kurcalama yapıldığını belirlemek için disk görüntüsünü incelemiştir. Sabit disk kurcalanmadan önce diskin üzerinde yer almadığı öne sürülen birtakım kötü amaçlı yazılımların, yemleme (phishing) e-postalarının ve belgelerin oraya "yerleştirilmiş olması" nedeni ile, söz konusu sabit disk üzerinde kurcalama yapıldığı iddia edilmektedir. Burada yapılan adli soruşturma, makul bir kesinlik derecesi dahilinde, bu iddialarda herhangi bir geçek payı olup olmadığını ve bu sabit diskin ODA-TV'nin zimmeti, tasarrufu ve kullanımında iken kurcalanıp kurcalanmadığını ve öyle ise ne dereye dek kurcalandığını belirlemeyi amaçlamaktadır.

1 Delil Teşkil Eden İşlemler

1.1 Paket

DataDevastation, CyberDiligence'dan bir Fedex paketi almıştır. Bu pakette, içinde tekli 3.5" SATA hard diski bulunan bir yazılım sürücüsü bulunmaktadır. Paket içinde bulunan bu sürücü, "ODA-TV HDD6" olarak etiketlenmiş bir Western Digital sürücüsüdür.

Paket, baş tetkikçi Joshua Marpet tarafından açılmış ve incelenmiştir. Paket, tarafımızdan açılmadan önce açılmamış görünmektedir.

1.2 Disk

Disk incelenmiş ve normal bir 3.5" SATA hard disk sürücüsü olarak görünmüştür. Bir disk kızağına yerleştirildiğinde, fiziksel olarak takıldığı bilgisayara başarılı bir şekilde bağlanmıştır. Diskte, 61 pakete veya dosyaya bölünmüş olan 1 adet resim dosyası bulunmaktadır. Bu dosyalar IMAGE.001 ila IMAGE.061 olarak adlandırılmıştır. Diskte ayrıca adı 2011-02-14 12-26-56 00044 D2F.LOG olan bir dosya daha vardır. Bu dosya, bir Dosya Loguna Tablo Diski dosyasıdır ve orijinal diski görüntülemek için bir Tablo sisteminin kullanılmasına dair ayrıntıları içermektedir.

Bu dosyada, disk özütleri (hash) listelenmektedir:

SHA1: d09a547f2ae2714ecaf7e365695c7d36bd98f5d8
MD5: 5d533c43c70eccd368539c5107c63439

Bu özütler Autopsy ve Sleuth Kit tarafından raporlanan özütlerle karşılaştırılmıştır. Bunlar mükemmel şekilde eşleşmiştir.

Bu, DataDevastation'ın incelediği görüntü dosyalarının görüntülendikleri anda disk içeriğindekilerle aynı olduğu anlamına gelmektedir.

2 Belgeler

Birçok kişisel bilgisayarda olduğu gibi, söz konusu sabit disk üzerinde çeşitli formatlarda birçok belge vardır. Bu belgeler çoğunlukla basit Microsoft Word Belgeleri, E-postalar, Excel Çalışma Sayfaları, Adobe PDF dosyaları ve benzer türdeki belgelerdir. Ancak bunlardan bazıları adli açıdan ilginçtir.

2.1 Dosya Zaman Çizelgeleri

Bir dosya zaman çizelgesi oluşturulması üzerine, tarihi olmayan dosyaların var olduğu belirlenmiştir. Bunların bazıları, başta orada olan dosyaların artıklarıdır, ancak bazıları değildir.

Muhtemelen zararsız olan bir çifte örnek:

Cuma 17 Ağu 2001 15:02:20 9600 m... r/rrwxrwxrwx 0 0 12361-128-3 C:/WINDOWS/system32/drivers/hidusb.sys

9600 m... r/rrwxrwxrwx 0 0 12365-128-1 C:/WINDOWS/system32/dllcache/hidusb.sys – Tarihi yok, ancak muhtemelen sadece yukarıdakinin bir artık dosyası.

2.1.1 Silinen Komut Dosyaları

212480 m... r/rrwxrwxrwx 0 0 13499-128-3 C:/WINDOWS/SWXCACLS.exe

136704 m... r/rrwxrwxrwx 0 0 13507-128-3 C:/WINDOWS/SWSC.exe

98816 m... r/rrwxrwxrwx 0 0 13566-128-3 C:/WINDOWS/sed.exe

80412 m... r/rrwxrwxrwx 0 0 13568-128-3 C:/WINDOWS/grep.exe

68096 m... r/rrwxrwxrwx 0 0 13570-128-3 C:/WINDOWS/zip.exe

161792 m... r/rrwxrwxrwx 0 0 13578-128-3 C:/WINDOWS/SWREG.exe

Bu dosyalardan bazıları bir Windows makinesinde yaygın ve potansiyel olarak zararsızken, bir Microsoft Windows makinesinde sed ve grep görülmesi olağan bir şey değildir. Bunlar, veriler üzerinde karmaşık bir şekilde işlem yapılması için kullanılan Unix veya Linux komutlarıdır. Bunları virüs veya virüs sahibi tarafından yerleştirilmiş veya kullanılmış olması muhtemeldir.

3 Kötü Amaçlı Yazılımlar (KAY)

3.1 KAY Listesi

Bazı dosyalar, diğer araçlarla birlikte hex editörleri kullanılarak incelenmiştir. Bu belgelerin birçoğunun üzerinde veya içinde virüs, Trojan ve diğer KAY çeşitleri vardır.

Çok fazla sayıda KAY sorunu tespit edilmiştir, diskte basit bir anti-virüs/anti-KAY taraması yapılması 4 saatten fazla sürmüştür. Bulunanlara dair bir örnek aşağıda gösterilmektedir. Bu bilgisayarda o kadar çok virüs, Trojan ve solucan bulunmuştur ki, yerimiz sadece bunlarda dair bir örnek göstermeye yetmektedir. Aşağıdaki örnek özellikle ilginçtir.

3.1.1 Civil Defense-6672

Listedeki ilk virüs olan "Civil Defense-6672", Symantec'e göre az rastlanır bir virüstür."Wild Seviyesi: Düşük Virüs Bulaşma Sayısı: 0 - 49 Site Sayısı: 0 - 2 Coğrafi Dağılım: Düşük".

Diğer bir deyişle, bunu bir sistemin üzerinde bulmak çok alışılmamış bir durumdur. Bu, çalışma sırasında saptanamayan, gizli bir virüstür.

3.1.2 Autorun-BJ

İkinci kötücül program olan "Autorun-BJ", sistemi virüs bulaşmış halde tutmanın bir yoludur. Bir yapılandırma dosyasını taklit eder ancak ihtiyacı olduğu taktirde başka virüs programlarını ve kabuk komutları başlatır. Yapılandırma dosyalarının taranması teknik nedenlerden dolayı zor olduğundan, birçok antivirüs programı bunların alarmını vermez.

3.1.3 Win32:Malware-gen

Üç çeşit virüsün sonuncusu genel amaçlı bir KAYdır. Virüs yazarı sadece bir görev kümesi içinde programlama yapmak durumundadır ve Kay bunları yerine getirir. Bu, saptaması ve kaldırması son derece zor olan, inatçı bir yazılımdır.

Bu KAY kombinasyonunun silinmesi bir yana, orada olduğunun bile belirlenmesi son derece zordur.

3.2 KAY Kullanımı

Bu liste trojanları, gizli kapı (backdoor) uygulamalarını ve virüsleri içermektedir. Esasen, bu çeşit KAY programları, hem makineyi kontrol etmek hem de makinenin bulaşan bu virüslerden hiçbir zaman başarılı bir şekilde temizlenememesini sağlayacak birden fazla erişim yolu vermeyi amaçlayan bir birim şeklinde tasarlanır. Diğer her şey temizlenmiş olsa bile sisteme yeniden virüs bulaştırabilecek korumalı bir solucanın ve genel amaçlı bir virüsün ve komut kabuğunun oluşturduğu gizlenmiş virüslerin kombinasyonunun bulunduğu bu bilgisayarın, uygulamada hiçbir zaman temizlenememesi, veya temizlenmesinin mümkün olamaması garanti edilmiştir.

ODA-TV makinesine el konmuş ve asıl sahiplerinin makineyi geri almasına izin verilmemiştir.

Makinenin yeni sahipleri (KAYları sağlayan kişiler), makineden ne fayda elde etmişlerdir?

Tipik olarak, üzerlerinde KAY, bilhassa da bu makinede bulunanlar gibi trojan virüsleri bulunan bilgisayarlar, ya bir arama motoru ağı içinde "zombi" makine olarak, veya başka bazı belli amaçlar için kullanılırlar.

Ancak, zombi bilgisayarların çoğu, bir web sitesi ziyaretinin bilgisayarınıza bir virüs veya çalışma indirdiği, web sitesi "kontrolündeki" virüsler aracılığıyla elde edilirler. Bu bilgisayarlar bir arama motoru ağına indirilir ve daha sonra yaramaz (spam) posta gönderilmesinden DDoS (Dağıtık Hizmet Aksatma) saldırılarına dek her şey için kullanılabilirler. Kötücül aktör özellikle o bilgisayarın veya o kullanıcının peşine düşmez. Bunlar basit olarak, sadece yanlış zamanda yanlış yerde bulunmuş olurlar.

Bu bilgisayar bu anlatılan şekilde virüs kapmamıştır. Bu makinedeki e-posta virüsleri, dikkate alınması gereken bir faktördür. Bu bilgisayar hedeflenmiştir. Bu bilgisayara saldırıda bulunmak için, bu kullanıcı hedeflenmiştir.

4 E-posta

Bu, bizi başlangıca götürmektedir. Virüs bulaşmasının vektörü (yöntemi) e-posta aracılığı ile gerçekleşmiştir. Virüs bulaşmış ve üzerlerine birden fazla sömürücü (exploit) kurulmuş, Attaturk Ekrankoruma.scr adında bir ekran koruyucu ve Duyuru.pdf adlı bir PDF dosyası vardır. Söz konusu toplu virüs bulaşmasına bu iki dosya neden olmuş gibi görünmektedir..

Bahsi geçen, ilgilendiğimiz e-postaların ikisi de ODA-TV'nin (Barışt'nin) gelen kutusundandır. Aşağıdaki bunlara bir örnektir.

Yanıt-Yolu: <winnerr51@jangomail.com>
Teslim Edilen: 1017-barist@odatv.com
Teslim Zamanı: (ağdan çağrılan qmail 26029); 5 Şub 2011 22:51:16 +0200
Teslim Alan: monet.jangomail.com'dan (199.237.53.220) naturelreklam.com.tr tarafından SMTP ile; 5 Feb 2011 22:50:37 +0200
Mesaj Kimliği: <538297208567811@jngomktg.net>
Konu: =?utf-8?Q?Bas=C4=B1n_Duyurusu?=
Kimden: "=?UTF-8?Q?CHP_Bas=C4=B1n_Birimi?=" <basinbirimi@chp.org.tr>
Tarih: Ctsi, 05 Şub 2011 20:50:07 +0000
Kime: bilgilendirme@chp.org.tr
X-Öncelik: 3
MIME-Versiyonu: 1.0
X-Gönderici: N/A
Listele-Abonelikten Çık(ar): <http://x.jmxded133.net/u.z?4d0aa6a0b30f43a8bc6968a772d03ca8>, <mailto:winnerr51@jangomail.com?Subject=Unsubscribe>
X-Kullanıcı Kimliği: 538297.208567811T137420 X-VConfig: T.208567811
İçerik-Tür: Çık kısımlı/karışık; sınır="----=_Part_8_17649447.1296938892140" X-EsetKimliği: AA907127F2D44E32F0DC
-

Duyuru.pdf bu e-postanın ekinde yer almaktadır. İçerik ve Kay diğer mesajda farklıdır ancak alınan veri yolu üç aşağı beş yukarı aynıdır.

Yanıt veri yolunun Jangomail.com olduğuna dikkat edin. Jangomail meşru bir posta sunucusudur ancak oldukça çok sayıda yaramaz posta ve Teklifsiz Ticari E-posta için kullanılmaktadır. Buraya geri dönen rastgele postalar fark edilmeyecektir. Ayrıca, buradan, yani meşru bir e-posta sunucusundan gelen postalara da birçok veri alanında ve posta sunucusunda izin verilecektir. Bu e-posta meşru mudur? Hayır. chp.org.tr ile ilgisi bulunmayan e-posta sunucuları kullanmaktadır. Jangomail, chp.org.tr'nin kullandığı bir posta sunucusu değildir. Dolayısı ile bu, birçok ülkede cezaya tâbi bir suç teşkil eden, aldatma amaçlı bir e-postadır. Bunun da ötesinde, söz konusu iki e-postaya KAY yüklenmiştir ve bu da, Türkiye'nin de imzalamış olduğu Avrupa Konseyi Sibersuçlar Antlaşması kanunlarını ihlal etmektedir. Elbette ki işin bu kısmı yargı sistemine ve hakime kalmıştır.

5 Sonuç

DataDevastation'nin ve Baş Tetkikçi Joshua Marpet'in profesyonel görüşüne göre, söz konusu sabit diski barındıran ODA-TV bilgisayarı, bir yemleme veya hedefli yemleme saldırısı tarafından hedef alınmıştır. Bu saldırı, kandırma amaçlı e-posta adreslerine sahip 2 veya daha fazla e-posta ile gerçekleştirilmiştir. Bu e-postalarda hem PDF hem de SCR (ekran koruyucu) uzantılı dosyalar olan ekler bulunmaktadır. Bu dosyalar, yukarıda da gösterildiği gibi, envai çeşit KAY ile yüklüdür. Bunlar bir kez bulaştığında, bilgisayara yeniden virüs bulaştırabilmek için birden fazla gizlenmiş yollara sahip olduğundan, bilgisayar ve bilgisayar sahibinin bu virüsleri temizleme veya yok etme şansı çok düşüktür. Bir kez bu yolla virüs bulaştıktan sonra, artık bu bilgisayarın ODA-TV kullanıcılarının kontrolünde olamayacağı, ancak bu virüsün yaratıcısının/sahibinin kontrolü altında olacağı açıktır. Virüs yaratıcısının/sahibinin emri ile her şey değiştirilebileceği, yok edilebileceği, oluşturulabileceği, makineden kaldırılabileceği veya makineye konabileceği için, bu noktada makinenin üzerinde bulunan hiçbir şeye güvenilemez.

23 Aralık 2011 tarihinde tarafımca imzalanmıştır.

J Marpet

Bölüm I

Kullanılan Araçlar

- Sleuth Kit
- Autopsy
- Macintosh OS X Lion
- Windows XP
- VirtualBox
- Carbon Copy Cloner
- Wiebetech USB Write Blocker
- Avast Anti-Virus
- Malwarebytes Anti-Malware

Bölüm II

Tek e-posta üzerinde yapılan virüs taramasının tam raporu (karşılaştırma amaçlı)

VirusTotal kullanılarak E-posta Üzerinde Yapılan Virüs Taramasının Sonuçları:

Antivirüs	Versiyon	Son Güncelleme	Sonuç
AhnLab-V3	2011.12.19.03	2011.12.19	-
AntiVir	7.11.19.162	2011.12.19	TR/Dropper.Gen
Antiy-AVL	2.0.3.7	2011.12.19	-
Avast	6.0.1289.0	2011.12.19	Win32:VB-REA [Drp]
AVG	10.0.0.1190	2011.12.19	-
BitDefender	7.2	2011.12.20	Gen:Heur.Spesr.VB.1
ByteHero	1.0.0.1	2011.12.07	-
CAT-QuickHeal	12.00	2011.12.18	-
ClamAV	0.97.3.0	2011.12.20	-
Commtouch	5.3.2.6	2011.12.19	W32/VBInject.BF.gen!Eldorado
Comodo	11017	2011.12.19	-
DrWeb	5.0.2.03300	2011.12.20	Trojan.PWS.Panda.490
Emsisoft	5.1.0.11	2011.12.19	Backdoor. Win32. Turkojan! IK
eSafe	7.0.17.0	2011.12.18	-
eTrust-Vet	37.0.9631	2011.12.19	-
F-Prot	4.6.5.141	2011.12.19	W32/VBInject.BF.gen!Eldorado
F-Secure	9.0.16440.0	2011.12.19	Gen:Heur.Spesr.VB.1
Fortinet	4.3.388.0	2011.12.19	W32/VB.WLJr
GData	22	2011.12.19	Gen:Heur.Spesr.VB.1
Ikarus	T3.1.1.109.0	2011.12.19	Backdoor. Win32. Turkojan
Jiangmin	13.0.900	2011.12.19	-
K7Antivirus	9.119.5720	2011.12.19	Riskli Yazılım
Kaspersky	9.0.0.837	2011.12.19	Backdoor. Win32. Turko jan. lvp
McAfee	5.400.0.1158	2011.12.19	-
McAfee GW Edition	2010.1E	2011.12.19	-
Microsoft	1.7903	2011.12.19	VirTool:Win32/VBInject.PB
NOD32	6725	2011.12.19	Bir Win32/Injector.KNX varyantı
Norman	6.07.13	2011.12.19	-
nProtect	2011-12-19.01	2011.12.19	-
Panda	10.0.3.5	2011.12.19	Şüpheli dosya

Bölüm III
Birinci tetkikçinin Vasıfları

Joshua Marpet, AccessData Onaylı Tetkikçisidir (ACE). Ayrıca, NSA (Ulusal Güvenlik Ajansı) ve DHS'nin (Ülke Güvenlik Departmanı) onaylı bir Akademik Mükemmeliyet Merkezi olan Wilmington Üniversitesi'nde Adli Bilişim dersleri vermektedir.

Joshua, St. Tammany Parish, Louisiana'da St. Tammany Parish Bölge Şerif Ofisinde görev yapmış olan, eski bir kanun uygulayıcısıdır.

Konuşma geçmişi mükemmeldir. Joshua, Dojocon, Shmoocon, Black Hat DC, Defcon, BsidesLV, BsidesDE'de ve ayrıca birçok başka topluluk önünce konuşmalar yapmıştır. Joshua, bir FBI Resmi-Özel Kurum Ortaklık organizasyonu olan Infragard'a hitap etmiş ve ABD Gizli Servisiyle yapılan ECTF (Elektronik Suçlar Görev Ekibi) toplantılarına konuşmacı olarak katılmıştır.

Araştırma alanında ise Joshua, kişilerin küçük bir idari giderle dijital bir adli bilişim laboratuarı kurma kapasitelerini güçlendirmek için tasarlanmış araştırmalar yapmaktadır.

ODA-TV HDD#6

Joshua Marpet, ACE

12/21/2011

Abstract

By the request of the Attornies, Dr. Duygun Yarsuvat and Attorney Huseyin Ersoz, who represent Soner Yalcin, DataDevastation examined a drive image to determine what, if any, tampering was performed on the hard drive that was removed from ODA-TV. There is alleged to be tampering, due to malware, phishing emails, and documents "placed" on the hard drive which were allegedly not there before the hard drive was tampered with. The forensic investigation performed here will attempt to determine, within a reasonable degree of certainty, if there is any truth to these claims, and to what extent this hard drive was tampered with or not, while still in the custody and possession and use of ODA-TV.

1 Evidentiary Procedures

1.1 Package

DataDevastation received a Fedex package, from CyberDiligence. The package contained a soft drive enclosure, with a single 3.5" SATA hard drive within it. The drive contained within the package is a blah blah type of drive, labeled "ODA-TV HDD6".

The package was examined and opened by Joshua Marpet, lead examiner. The package appeared unopened, prior to receiving it.

1.2 Drive

The drive was examined, and appeared to be a normal 3.5" SATA hard disk drive. Upon being placed in a drive dock, it connected successfully to the computer hooked up to it. The drive contained 1 image file, broken down into 61 packages, or files. Each file was named IMAGE.001 to IMAGE.061. There was also a file on the drive named 2011-02-14 12-26-56 00044 D2F.LOG. This file is a Tableau Disk to File Log file, detailing the use of a Tableau system to image the original disk.

In this file, it lists the disk hashes: SHA1: d09a547f2ae2714ccaf7c365695e7d36bd98f5d8
MD5 : 5d533c43c70cccd368539c5107c63439

Those hashes were compared to the hashes reported by Autopsy and The Sleuth Kit. They matched perfectly.

What that means is that the image files that DataDevastation examined are identical to the contents of the drive, at the time it was imaged.

2 Documents

As on many personal computers, there are many documents in several formats on the hard drive in question. These documents are mostly simple Microsoft Word Documents, Emails, Excel spreadsheets, Adobe PDFs., and similar types of documents. However, some of them are forensically interesting.

2.1 File Timelines

Upon creating a file timeline, it was found that there are files with no dates. Some of these are remnants of files that were there originally, but some were not.

Example of a probably harmless pair:

Fri Aug 17 2001 15:02:20 9600 m... r/rrwxrwxrwx 0 0 12361-128-3 C:/WINDOWS/system32/drivers/hidusb.sys

9600 m... r/rrwxrwxrwx 0 0 12365-128-1 C:/WINDOWS/system32/dllcache/hidusb.sys - Without a date, but probably just a remnant of the one above.

2.1.1 Deleted Command files

212480 m... r/rrwxrwxrwx 0 0 13499-128-3 C:/WINDOWS/SWXCACLS.exe

136704 m... r/rrwxrwxrwx 0 0 13507-128-3 C:/WINDOWS/SWSC.exe

98816 m... r/rrwxrwxrwx 0 0 13566-128-3 C:/WINDOWS/sed.exe

80412 m... r/rrwxrwxrwx 0 0 13568-128-3 C:/WINDOWS/grep.exe

68096 m... r/rrwxrwxrwx 0 0 13570-128-3 C:/WINDOWS/zip.exe

161792 m... r/rrwxrwxrwx 0 0 13578-128-3 C:/WINDOWS/SWREG.exe

While some of these files are common and potentially even harmless on a windows machine, it's unusual to see Sed and Grep on a Microsoft Windows machine. These are Unix or Linux commands used for sophisticated processing of data. It is possible they were placed or used by the virus or virus owner.

3 Malware

3.1 Malware List

Several documents were examined, using hex editors, among other tools. Many of these documents have viruses, Trojans, and other malware variants on or in

them. Such a significant number of malware issues were detected, it took more than 4 hours to run a simple Anti-virus/Anti-malware scan on the drive. Here is a sample of what was found. There are so many viruses, trojans, and worms on this computer, a sampling is all there is space to show. This sampling is particularly interesting.

G:\IMAGE 001\Partition @ 63\Root\WINDOWS\pchealth\ERRORREP\UserDumps\elrn.exe 20101123-071125-00.hdmp	High	Threat: Civil Defense-6672
G:\IMAGE 001\Partition @ 63\Root\WINDOWS\pchealth\ERRORREP\UserDumps\elrn.exe 20101013-070229-00.hdmp	High	Threat: Civil Defense-6672
G:\IMAGE 001\Partition @ 63\Root\WINDOWS\pchealth\ERRORREP\UserDumps\elrn.exe 20100819-065027-00.hdmp	High	Threat: Civil Defense-6672
G:\IMAGE 001\Partition @ 121081905\Root\LogFile	High	Threat: INF.AutoRun-BJ [Wrm]
G:\IMAGE 001\Partition @ 121081905\Root\LI3ROMDriver.exe	High	Threat: Win32.Malware-gen
G:\IMAGE 001\Partition @ 63\Root\Documents and Settings\Turker\Start Menu\Programlar\Başlangıç\MSN Messenger.exe	High	Threat: Win32.Malware-gen
G:\IMAGE 001\Partition @ 63\Root\Documents and Settings\All Users\Start Menu\Programlar\Başlangıç\MSN Messenger.exe	High	Threat: Win32.Malware-gen

3.1.1 Civil Defense-6672

The first virus listed, Civil Defense-6672 is a rare virus, according to Symantec. "Wild Level: Low Number of Infections: 0 - 49 Number of Sites: 0 - 2 Geographical Distribution: Low"

In other words, it would be very unusual to find this on a system. It is a stealthed (hidden) virus, undetectable while running.

3.1.2 Autorun-BJ

The second malicious program, "Autorun-BJ", is a way to keep the system infected. It masquerades as a configuration file, but starts other virus programs and command shells if it needs to. Many antivirus programs will not alert on these, as configuration files are difficult to scan, for technical reasons.

3.1.3 Win32:Malware-gen

The last of the three types of infections is a general purpose Malware. The virus author has merely to program in a set of tasks, and the malware will perform them. It is a tenacious (tough) piece of software, extremely difficult to detect and remove.

This combination of malware is extremely tough to determine it is even there, much less to remove it.

3.2 Use of Malware:

This list includes trojans, back door applications, and viruses. Essentially, this suite of malware was designed as a unit, to give multiple pathways to both control the machine, and to make sure the machine was never able to be successfully uninfected. With a combination of stealthed viruses, a protected worm that could re-infect the system, even if everything else was cleaned out, and a general purpose virus and command shell, this computer was practically guaranteed not to ever be cleaned, or to be possible to be cleaned.

The ODA-TV machine was taken over, and not allowed to be re-taken by its original owners.

What use did the new owners (the malware providers) have for the machine?

Typically, computers with malware on them, especially trojans such as found on this machine, are used for either "zombie" machines, in a botnet, or for some specific purpose.

However, most zombie computers are obtained through website "drive by" infections, where simply visiting a website will download a virus or work to your computer. These computers are added to a botnet, and used for anything from spam emailing, to DDoS (Distributed Denial of Service) attacks. The malicious actor is not specifically going after that computer, or that user. They simply happen to be at the wrong place at the wrong time.

This computer was not infected in that fashion. The email infection of this machine is a factor that must be taken into account. This computer was targeted. This user was targeted, to attack this computer.

4 Email

Which brings us to the beginning. The vector (method) of infection was through email. There was an infected screensaver, Attaturk Ekrankoruma.scr, and a PDF file, Duyuru.pdf, that had multiple exploits built into them. These appear to be the files that caused the entire massive infection.

The specific emails in question are both from odatv (Barist)'s inbox. An example is this one.

Return-Path: <winnerr51@jangomail.com>
Delivered-To: 1017-barist@odatv.com
Received: (qmail 26029 invoked from network); 5 Feb 2011 22:51:16 −0200
Received: from monet.jangomail.com (199.237.53.220) by naturelreklam.com.tr with SMTP; 5 Feb 2011 22:50:37 −0200
Message-ID: <538297208567811@jngomktg.net>
Subject: =?utf-8?Q?Bas=C4=B1n_Duyurusu?=
From: "=?UTF-8?Q?CHP_Bas=C4=B1n_Birimi?=" <basinbirimi@chp.org.tr>
Date: Sat, 05 Feb 2011 20:50:07 −0000
To: bilgilendirme@chp.org.tr
X-Priority: 3
MIME-Version: 1.0
X-Mailer: N/A
List-Unsubscribe: <http://x.jmxded133.net/u.z?4d0aa6a0b30f43a8bc6968a772d03ca8>, <mailto:winnerr51@jangomail.com?Subject=Unsubscribe>
X-UserID: 538297.208567811T137420 X-VConfig: T.208567811
Content-Type: multipart/mixed;
boundary "—=_Part_8_17649447.1296938892140" X-
EsetId: AA907127F2D44E32F0DC
-

Duyuru.pdf is the attachment to this email. The content and malware is different in the other one, but the path it took is much the same.

Notice that the return path is to Jangomail.com. Jangomail is a legitimate mail server, but it is used for quite a lot of spam, Unsolicited Commercial Email. Random mail returning to there would not be noticed. As well, mail coming from there, a legitimate email server, would be allowed into most domains, and mail servers. Is this mail legitimate? No. It uses mail servers unrelated to chp.org.tr. Jangomail is not the mail server that chp.org.tr uses. Therefore, it is spoofed email, which is a punishable offense in many countries. More than that, the two emails in question are loaded with malware, which breaks The Council of Europe Convention on Cybercrime laws, which Turkey is a signatory of. Of course, this is more properly left to the trier of fact (the judge and justice system).

5 Conclusion

It is the professional opinion of DataDevastation, and the Primary Examiner, Joshua Marpet, that the ODA-TV computer this hard disk drive came from was targeted by a phishing or spear phishing attack. This attack was put in place with 2 or more emails, with spoofed email addresses. The emails were carrying attachments, both a PDF and a SCR (screensaver) file. These files were loaded with malware of all kinds, as demonstrated above. Once infected, the computer and computer owner would have little chance to clear or clean the infection, as the malware had multiple stealthed and hidden ways to re-infect the computer. Once infected in this way, the computer can no longer be clearly in control of the ODA-TV users, and is effectively under the control of the virus creator/owner. At that point, nothing on the machine can be trusted, as anything can be modified, destroyed, created, moved off, or moved onto the machine, at the order of the virus creator/owner.

Signed by me this day, the 23rd of December, 2011

J Marpet

Part I
Tools Used

- The Sleuth Kit
- Autopsy
- Macintosh OS X Lion
- Windows XP
- VirtualBox
- Carbon Copy Cloner
- Wiebetech USB Write Blocker
- Avast Anti-Virus
- Malwarebytes Anti-Malware

Part II
Virus Scan full report on single email (for comparison purposes)

Antivirus Scan of Email using VirusTotal:

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.12.19.03	2011.12.19	-
AntiVir	7.11.18.162	2011.12.19	TR/Dropper.Gen
Antiy-AVL	2.0.3.7	2011.12.19	-
Avast	6.0.1289.0	2011.12.19	Win32:VB-BEX [Drp]
AVG	10.0.0.1190	2011.12.19	-
BitDefender	7.2	2011.12.20	Gen:Heur.Spear.VB.1
ByteHero	1.0.0.1	2011.12.07	-
CAT-QuickHeal	12.00	2011.12.18	-
ClamAV	0.97.3.0	2011.12.20	-
Comodo	11017	2011.12.19	-
DrWeb	5.0.2.03300	2011.12.20	Trojan.PWS.Panda.490
Emsisoft	5.1.0.11	2011.12.19	Backdoor.Win32.Turkojan!IK
eSafe	7.0.17.0	2011.12.18	-
eTrust-Vet	37.0.9631	2011.12.19	-
F-Prot	4.6.5.141	2011.12.19	W32/VBInject.BF.gen!Eldorado
F-Secure	9.0.16440.0	2011.12.19	Gen:Heur.Spear.VB.1
Fortinet	4.3.388.0	2011.12.19	W32/VB.WL!tr
GData	22	2011.12.19	Gen:Heur.Spear.VB.1
Ikarus	T3.1.1.109.0	2011.12.19	Backdoor.Win32.Turkojan
Jiangmin	13.0.900	2011.12.19	-
K7AntiVirus	9.119.5720	2011.12.19	Riskware
Kaspersky	9.0.0.837	2011.12.19	Backdoor.Win32.Turkojan.ivp
McAfee	5.400.0.1158	2011.12.19	-
McAfee-GW-Edition	2010.1E	2011.12.19	-
Microsoft	1.7903	2011.12.19	VirTool:Win32/VBInject.PB
NOD32	6725	2011.12.19	a variant of Win32/Injector.XXX
Norman	6.07.13	2011.12.19	-
nProtect	2011-12-19.01	2011.12.19	-
Panda	10.0.3.5	2011.12.19	Suspicious file

Part III
Primary Examiner Qualifications

Joshua Marpet is an AccessData Certified Examiner (ACE). He also teaches Forensics at Wilmington University, an NSA (National Security Agency) and DHS (Department of Homeland Security) certified Center of Academic Excellence.

Joshua is ex-law enforcement, having spent several years with the St. Tammany Parish Sheriff's Office, in St. Tammany Parish, Louisiana.

His speaking record is excellent. Joshua has spoken at Dojocon, Shmoocon, Black Hat DC, Defcon, BsidesLV, BsidesDE, and in front of many other audiences as well. Joshua has addressed Infragard, an FBI Public Private Partnership organization, and has spoken at ECTF (Electronic Crime Task Force) meetings with the US Secret Service.

In research, Joshua is conducting research designed to strengthen the ability of people to build a digital forensics lab with little overhead.

Objective: We were asked to perform a forensic analysis on what is referred to as Hard Disk Drive #6's forensic image as provided to us. Concern was expressed about the authenticity and authorship of various documents (See Exhibit A) that purportedly were found on HDD #6. As such, the following objectives of this investigation were determined:

1. Determine if any evidence exists suggesting that the files in question may have been planted by unknown individuals to frame the user of the computer.
2. Is there any evidence suggesting that the owner had knowledge that the files in question existed on the hard drive.
3. Is there any evidence that the owners/custodians of the hard drives accessed the subject files listed in (Exhibit A).

Forensic Examination Steps:

1. Perform a forensic analysis on the hard drive utilizing various state-of-the-art forensic software tools:

    a. Forensic Tool Kit (FTK) Version 3.3
    b. X-Ways Forensics
    c. Internet Evidence Finder

2. Examine the computer for artifacts of recently accessed files.
3. Perform a malware analysis to determine if there is evidence of any compromise that would facilitate the planting of incriminating files.

Findings: Using start-of-the-art forensic tools, and acceptable computer and investigative methodologies, it has been determined that the hard drive examined, hereafter called *"HDD # 6"* has been compromised as a result of a direct and targeted attack by unknown individuals. Malware which are classified as Droppers and Remote Access Trojan (RAT) was planted on the computer hard drive using a specifically targeted "spoofed" email (See Exhibit B). The malware detected showed that *"HDD # 6"* was infected numerous times and the characteristics of the malware indicates that it was Remote Access Trojan designed to give the attacker full control of the computer.

Examination of the "Recently Accessed Files" (See Exhibit C) reveals all the documents that were accessed (opened), created or modified by the user of the computer. The majority of documents in question were never opened by the owner of the computer.

The metadata file headings for these documents are conclusive; if the owner of the hard drive created, accessed or modified the document files there would be evidence of that on the computer's hard drive. That evidence is absent in many of the documents which supports the conclusions and findings written herein.

Examination of *"HDD # 6"* not only showed the existence of malware, Windows Prefetch files indicate that the malware was an executable file that was indeed executed as soon as the malware program penetrated the computer's security perimeter via an infected email, and we believe that based on the malware characteristics (SVCHOST.exe) that the malware communicated back to the external source of the malware attack in accordance with its programmed characteristics and behavior to download additional malware (See Exhibit D).

Our examination shows evidence of a *"spoofed email"* being used to allow the malware to access the computer. In other words someone other than the original owner or custodian of an email address impersonated that email address in order to induce the custodian of *"HDD # 6"* to open an email that then, unbeknown to the email recipient, downloaded an executable malware program. CHP.ORG.TR uses BMX.IS.NET.TR as its email server not JANGOMAIL. The *spoofed email* came via JANGOMAIL.com which is a known entity in the computer forensics field for this type of clandestine impersonation of email users. The spoofed email was designed to have the owner of the computer open an email that they thought was from someone they knew when in fact it was an impersonation with one intention; open an attached PDF file. Once opened the PDF file contained a Malware which took control of the owner's computer without his/her knowledge.

In conclusion, it is our expert opinion that the computer has been targeted for compromise and was in fact compromised by unknown individuals. Therefore the rightful owner of the computer lost control of the computer in question. No digital evidence that was obtained from this computer can be relied upon or used in any civil or criminal process as it was intentionally targeted and compromised. There is a high probability that the unknown attackers may have planted the evidence in question.

Amaç: Bizden, tarafımıza verilen Sabit Disk Sürücüsü (HDD) #6 olarak adlandırılan adli görüntü üzerinde bir adli bilişim analizi yapmamız istenmiştir. HDD#6 üzerinde bulunduğu ileri sürülen çeşitli belgelerin aslıyla özdeşliği ve kim tarafından yazıldığı konularında bazı kaygılar olduğu dile getirilmiştir (Bkz. Ek A). Bu durumda, bu araştırmaya ilişkin olarak aşağıda belirtilen amaçlar belirlenmiştir:

1. Söz konusu dosyaların bilgisayar kullanıcısını oyuna getirmek amacıyla bilinmeyen kişilerce makineye konmuş olabileceğine dair herhangi bir delil olup olmadığının belirlenmesi.
2. Bilgisayarın sahibinin söz konusu dosyaların sabit diskte bulunduğunu bildiğine dair herhangi bir delil olup olmadığının belirlenmesi.
3. Sabit disklerin sahiplerinin/zimmetli olduğu kişilerin (Ek A)'da listelenen söz konusu dosyalara eriştiğine dair herhangi bir delil olup olmadığının belirlenmesi.

Adli Bilişim İncelemesine Ait Adımlar:

1. Çeşitli son teknoloji ürünü adli bilişim yazılım araçları kullanılmak suretiyle sabit disk üzerinde bir adli bilişim analizinin gerçekleştirilmesi:
    a. Forensic Tool Kit (FTK) Versiyon 3.3
    b. X-Ways Forensics
    c. Internet Evidence Finder

2. Bilgisayarda son zamanlarda erişilen dosyalara ilişkin yapay kanıtlar açısından incelenmesi.
3. Suçlamalara neden olan dosyaların bilgisayara dışarıdan konmasını kolaylaştıracak herhangi bir taviz olduğuna dair herhangi bir kanıt olup olmadığını belirlemek amacıyla bilgisayar üzerinde bir kötü amaçlı yazılım (KAY) analizinin gerçekleştirilmesi.

Bulgular: Son teknoloji ürünü adli bilişim yazılım araçları ve kabul edilebilir bilgisayar ve araştırma yöntemleri kullanılarak, bundan böyle burada "HDD#6" olarak adlandırılacak olan sabit diskin, doğrudan ve hedeflenmiş bir saldırı sonucunda bilinmeyen kişiler tarafından zaafa uğratıldığı belirlenmiştir. Dropper ve Uzak Erişimli Trojan (RAT) olarak sınıflandırılan KAYlar, özel olarak hedeflenmiş bir "aldatıcı" e-posta kullanılarak söz konusu sabit diske "ekilmiştir" (Bkz. Ek B). Tespit edilen KAY, HDD#6'ya birçok kez virüs bulaştırıldığını ve KAYın özelliklerinin bunun saldırgana bilgisayarın tam kontrolünü vermek için tasarlanmış olan bir RAT olduğunu göstermiştir.

"Son Zamanlarda Erişilen Dosyalar"ın (Bkz. Ek C) incelenmesi, bilgisayarın kullanıcısı tarafından erişilen (açılan), yaratılan veya değiştirilen tüm dosyaları ortaya çıkarmıştır. İnceleme konusu olan belgelerin büyük çoğunluğu ise bilgisayarın sahibi tarafından hiçbir zaman açılmamıştır.

Bu belgelere ilişkin dosya başlığı metaverileri kesin ve şüpheleri ortadan kaldırıcı niteliktedir; har diskin sahibinin bu belge dosyalarını/a oluşturmuş, erişmiş veya değiştirmiş olması halinde, bilgisayarın sabit diskinde bu işlemlere ilişkin kanıt bulunması gerektiği kesindir. Bu kanıt belgelerin çoğu için yoktur ve bu durum da burada yazan sonuçları ve bulguları destekler niteliktedir.

HDD#6 üzerinde yapılan inceleme sadece KAY varlığını göstermekle kalmamış, Windows Prefetch dosyaları KAYın, KAY bilgisayarın güvenlik çevresine virüslü bir e-posta aracılığı ile nüfuz eder etmez gerçekten de çalıştırılmış olan, çalıştırılabilir bir dosya olduğunu da göstermiştir; düşüncemize göre, KAY özelliklerine dayanarak (SVCHOST.exe), söz konusu KAY, ilave KAYların da indirilmesi için programlanmış özelliklerine ve davranışına uygun şekilde kötü amaçlı yazılım saldırısının kaynağı ile iletişime geçmiştir (Bkz. Ek D).

Yaptığımız inceleme, KAYın bilgisayara erişmesine olanak sağlamak için [e-posta adresi e-postanın gerçek bir kişiden gittiğine inandıracak şekilde düzenlenmiş olan] bir "*aldatıcı e-postanın*" kullanıldığına dair kanıt olduğunu göstermektedir. Diğer bir deyişle, bir e-posta adresinin gerçek sahibinden veya koruyucusundan başka biri, HDD#6'nın sahibinin veya koruyucusunun çalıştırılabilir bir KAY programı yüklenebilmesi amacıyla o anda e-posta alıcısının tanımadığı bir e-postayı açmasını sağlamak için bu e-posta adresini taklit etmiştir. CHP.ORG.TR, e-posta sunucusu olarak JANGOMAIL'i değil, BMX.IS.NET.TR'yi kullanmaktadır. *Aldatıcı e-posta*, adli bilişim alanında e-posta kullanıcılarının bu türden gizli saklı taklit edilmeleri alanında tanınan bir kurum olan JANGOMAIL.com adresi üzerinden gelmiştir. Aldatıcı e-posta, bilgisayar kullanıcısının tanıdığı birinden geldiğini düşündüğü, ancak aslında tek bir amaçla - : ekli bir PDF dosyasını açtırmak - taklitçi olan bir e-postayı açmasını sağlamak üzere tasarlanmıştır. PDF dosyasında, dosya açıldığı anda bilgisayar sahibinin bilgisayarının kontrolünü sahibin haberi olmaksızın ele geçiren bir KAY yer almaktadır.

Sonuç olarak, uzman kanaatimize göre, söz konusu bilgisayar zaafa uğraması ve teslim olması için bilinmeyen kişilerce hedeflenmiş ve bunlar gerçekten de başarılmıştır. Bu nedenle de bilgisayarın gerçek sahibi, söz konusu bilgisayar üzerindeki kontrolünü kaybetmiştir. Bu bilgisayar kasti olarak hedef alındığı ve zaafa uğratılarak teslim alındığı için, bu bilgisayardan elde edilen hiçbir dijital kanıta güvenilemez veya bu kanıtlar herhangi bir medeni kanun veya ceza kanunu takibatında veya davasında kullanılamaz. Bilinmeyen saldırganların söz konusu kanıtları hard diske "ekmiş" olması oldukça yüksek bir olasılıktır.