ARSENAL CONSULTING

— ARM YOURSELF —

ÇYDD / 2010/633

Preliminary ÇYDD Hard Drive Report

August 30, 2013

I. Introduction

I am President of Arsenal Consulting ("Arsenal"), where I lead engagements involving digital forensics for law firms, corporations, and government agencies. I am also President of Arsenal Recon, where I guide development of digital forensics tools. I have more than fifteen years of law-enforcement and private-sector digital forensics experience. I have taught at both the Computer Security Institute and Bunker Hill Community College in Boston, Massachusetts. A true and accurate copy of my CV is attached as Exhibit A to this report.

Arsenal Consulting, Inc. ("Arsenal") was retained on August 1, 2013 by Attorney Hüseyin Ersöz to provide computer forensics consulting services in connection with his representation of Çağdaş Yaşamı Destekleme Derneği ("ÇYDD"), a Turkish non-governmental organization, in a criminal matter. More specifically, Attorney Ersöz requested Arsenal's assistance in identifying anything suspicious regarding a hard drive known as the "ÇYDD Hard Drive."

Computer forensics practitioners obtain forensic images from electronic media to preserve all the data on that media, including "deleted space." Forensic images can be authenticated at any time in the future by calculating hash values (also known as digital fingerprints) which are associated with each forensic image. Arsenal's analysis of the ÇYDD Hard Drive[1] is based on a forensic image[2] obtained by "Dijital Veri Ýnceleme Büro Amirliði" on March 15, 2009[3] using Guidance Software's EnCase[4]. It should be noted that it is impossible for the forensic image to have been obtained on March 15, 2009, as file activity on the ÇYDD Hard Drive occurs through April 10, 2009 and Arsenal has been advised by Attorney Ersöz that the computer it came from was not seized by the Turkish Police until April 13, 2009. Arsenal finds this date discrepancy unusual as forensic images are normally obtained on equipment dedicated to computer forensics, where maintaining correct dates and times is very important.

II. Executive Summary

Arsenal has concluded that the ÇYDD Hard Drive was tampered with after April 10, 2009 at 8:48 PM (when its Windows operating system was last shut down) and before it was forensically imaged on an unknown date. The tampering included copying files and folders, manipulating their dates and times, and finally deleting them while the ÇYDD Hard Drive was connected to another computer. Attorney Ersöz has advised Arsenal that all the documents mentioned in the ÇYDD indictment are

[1] Arsenal authenticated this forensic image using FTK Imager v3.1.3.2

[2] Named "Kadikoy_CYDD_Maxtor_25B6201H10T7IY_40GB"

[3] According to both metadata internal to the forensic image and external file system metadata

[4] Version 4.20

among these files. Arsenal has never before encountered such an extreme volume of file system tampering and our analysis is ongoing.

III. Suspicious File System Activity

Microsoft Windows XP ("Windows") "System Events"[5] on the ÇYDD Hard Drive (particularly the last event involving the Event Log service shutting down) indicate that Windows was last shut down on April 10, 2009 at approximately 8:48 PM[6]. The latest file system activity related to the modification, access, or creation of system files[7] on the ÇYDD Hard Drive confirms this shut down time.

Arsenal found "Entry Modified[8]" file system activity involving 171 deleted files on the ÇYDD Hard Drive which occurred between 9:03:48 PM and 11:55:16 PM on April 10, 2009 - after Windows was shut down for the last time at 8:48 PM. Arsenal found this file activity[9] suspicious and proceeded to perform more aggressive analysis of the ÇYDD Hard Drive.

A. File System Analysis

The ÇYDD Hard Drive contained Windows running on top of the NTFS file system. NTFS uses a variety of metafiles (e.g. $MFT and $LogFile) to keep track of its files and folders. Windows hides these metafiles but they can be accessed[10] and parsed[11] by computer forensics tools. These metafiles contain a significant volume of information related to files and folders such as their names, locations, and associated times.

Arsenal's analysis of NTFS metafiles on the ÇYDD Hard Drive has been focused, for purposes of this preliminary report, on file system activity that occurred after Windows was last shut down on April 10, 2009. Arsenal's primary method of identifying file activity which occurred after Windows was last shut down relied upon analysis of the $LogFile metafile. The $LogFile metafile is a transaction log that provides NTFS with redo and undo functionality by using unique identifiers called log sequence

[5] Per http://technet.microsoft.com/en-us/library/dd315601(v=ws.10).aspx, "The Event Log service maintains a set of event logs that the system, system components, and applications use to record events."

[6] See Exhibit B for details on all Windows system events from the ÇYDD Hard Drive

[7] Registry files which include system, software, SECURITY, etc. modified on April 10, 2009 at 8:48:17 PM

[8] A date and time value normally hidden by Windows related to when a particular MFT record was last changed

[9] See Exhibit C for details

[10] AccessData's Forensic Imager, Guidance Software's EnCase, etc.

[11] analyzeMFT, mft2csv, LogFileParser, G-C Partners Advanced NTFS Journal Parser, etc.

numbers (“LSNs”). LSNs occur in the order in which changes to files and folders happen, regardless of what the date and time settings of the operating system are.

The final transaction related to system files as Windows was shutting down for the last time is LSN 103816224[12]. Arsenal found a transaction (LSN 103816248) following LSN 103816224 particularly suspicious because it reflected the creation of a Windows restore point[13] when the ÇYDD Hard Drive was expected to be powered off. Arsenal considers all 41,467 transactions from LSN 103816248 onward to be extremely suspicious, as the creation of this restore point is consistent with the ÇYDD Hard Drive having been connected to another computer after Windows was last shut down. Among these 41,467 extremely suspicious transactions, 627 unique Office documents[14] were created on and then deleted from the ÇYDD Hard Drive. See Exhibit D for a full accounting of all 41,467 transactions.

Arsenal found additional evidence that the ÇYDD Hard Drive was attached to another computer after Windows was last shut down. This evidence includes a log[15] within the restore point mentioned above that refers to the ÇYDD Hard Drive as “HarddiskVolume6”, which only another computer would have done[16], and a Windows Recycler folder[17] that refers to a SID (Security Identifier) unrelated to either current or former installations of Windows[18] on the ÇYDD Hard Drive.

Attorney Ersöz has advised Arsenal that all the documents mentioned in the ÇYDD indictment were created and deleted within the 41,467 extremely suspicious transactions. Details on five of these documents (“sample documents”) are below:

[12] C:\WINDOWS\system32\config\system.LOG

[13] C:\System Volume Information_restore{068EFAD7-9E24-4D5F-8301-49D3FEBF4F39}

[14] 175 Excel, 446 Word, and 6 PowerPoint documents unique per filenames

[15] C:\System Volume Information_restore{068EFAD7-9E24-4D5F-8301-49D3FEBF4F39}\RP46\change.log

[16] See Exhibits E and F which show “MountedDevices” and “Disk Devices” Registry information over time

[17] C:\RECYCLER\S-1-5-21-1547161642-1644491937-682003330-500

[18] Registry Recon was used to rebuild Registries from 6 unique Windows installations on the ÇYDD Hard Drive

Full Path	Entry Modified
GENEL\Türkan SAYLAN\okan amiral\MEKTUP(Türkan SAYLAN).doc	04/10/09 11:55:16 PM

File Modified	File Accessed	File Created
12/25/08 11:18:52 PM	12/25/08 11:42:23 PM	12/25/08 11:42:23 PM

$LogFile LSN (File Creation)	$LogFile LSN (File Deletion)
105385237	106307207

Full Path	Entry Modified
GENEL\Türkan SAYLAN\tükansaylan-1\a ortabaşı\Türkan SAYLAN 1.doc	04/10/09 11:55:16 PM

File Modified	File Accessed	File Created
07/24/08 02:36:46 PM	07/24/08 11:38:57 PM	07/24/08 11:38:57 PM

$LogFile LSN (File Creation)	$LogFile LSN (File Deletion)
105356370	106306302

Full Path	Entry Modified
GENEL\Türkan SAYLAN\tükansaylan-1\a ortabaşı\Türkan SAYLAN 2.doc	04/10/09 11:55:16 PM

File Modified	File Accessed	File Created
10/18/08 03:42:40 PM	10/18/08 02:39:12 PM	10/18/08 02:39:12 PM

$LogFile LSN (File Creation)	$LogFile LSN (File Deletion)
105361340	106306403

Full Path	Entry Modified
GENEL\Türkan SAYLAN\tükansaylan-1\a ortabaşı\Türkan SAYLAN 3.doc	04/10/09 11:55:16 PM

File Modified	File Accessed	File Created
12/07/08 09:22:30 AM	12/07/08 01:39:22 PM	12/07/08 01:39:22 PM

$LogFile LSN (File Creation)	$LogFile LSN (File Deletion)
105364977	106306537

Full Path	Entry Modified
GENEL\listeler2\2008 toplantıözeti.doc	01/12/09 05:04:17 PM

File Modified	File Accessed	File Created
01/12/09 05:04:17 PM	01/12/09 05:04:35 PM	01/12/09 05:04:35 PM

$LogFile LSN (File Creation)	$LogFile LSN (File Deletion)
106144904	106426411

As the sample documents above were created on and deleted from the ÇYDD Hard Drive after Windows was last shut down (see their LSNs), it is obvious that the ÇYDD Hard Drive was connected to another computer from which these files were copied, manipulated, and finally deleted.

B. User Activity Analysis

When Microsoft Office ("Office") documents are opened, shortcuts to those documents are created (or modified if they already exist) by both Windows and Office. Opening Office documents also results in updates to Windows Registry ("Registry") MRU (Most Recently Used) lists maintained by both Windows and Office.

Arsenal has reviewed shortcut and Registry information from both the current and previous installations of Windows on the ÇYDD Hard Drive and found no evidence that the sample documents were interacted with in any way while Windows was running. In fact, Arsenal has not found references of any kind to the sample documents other than file system remnants which would be consistent with the ÇYDD Hard Drive having been connected to another computer after Windows was shut down for the last time on April 10, 2009 at 8:48 PM.

IV. Conclusion

Arsenal has concluded that the ÇYDD Hard Drive was tampered with after April 10, 2009 at 8:48 PM (when its Windows operating system was last shut down) and before it was forensically imaged by the Turkish Police on an unknown date. Arsenal identified 41,467 transactions on the ÇYDD Hard Drive's file system which are extremely suspicious because they occurred after Windows was last shut down. The tampering included copying files and folders, manipulating their dates and times, and finally deleting them while the ÇYDD Hard Drive was connected to another computer. Attorney Ersöz has advised Arsenal that all the documents mentioned in the ÇYDD indictment are among these files. Arsenal has never before encountered such an extreme volume of file system tampering and our analysis is ongoing.

Mark G. Spencer

Digitally signed by Mark G. Spencer
DN: cn=Mark G. Spencer, o=Arsenal Consulting, Inc., st=MA, c=US, l=Chelsea, email=mspencer@ArsenalExperts.com
Date: 2013.08.30 13:36:03 -04'00'