FAST Forensics

DIB-3750G-28

Howard Phan
Karter Rohrer
Raissa Engelhard
Patrick Mulvey
Kirk Hofmeister

Scope

- On March 31, 2017, Casey Kan and his team noticed suspicious network traffic coming from the corporate workstation of Mr. Munoz.
- Mr. Munoz was in a meeting at the time of the incident.
- An unknown individual attempted to badge out using what Casey Kan and his team suspect to be a fake ID badge.
- The man was detained for trespassing on private property and potential corporate espionage.

Our Task

- The CEO of Do IT Better has tasked us to perform a forensic analysis on the files provided to determine if the evidence correlates to this case or any other potential cases.

- Do IT Better created the forensic images and has instructed us to examine them for potential corporate espionage.

The Forensic Images

- Image of Corporate Workstation
  [Computed Hashes]
  MD5 checksum: 68c56a684fd2048bb60bad01ff45d11d
  SHA1 checksum: 24004b3f0ee97b36d8d11ecc915085471bfea9bd

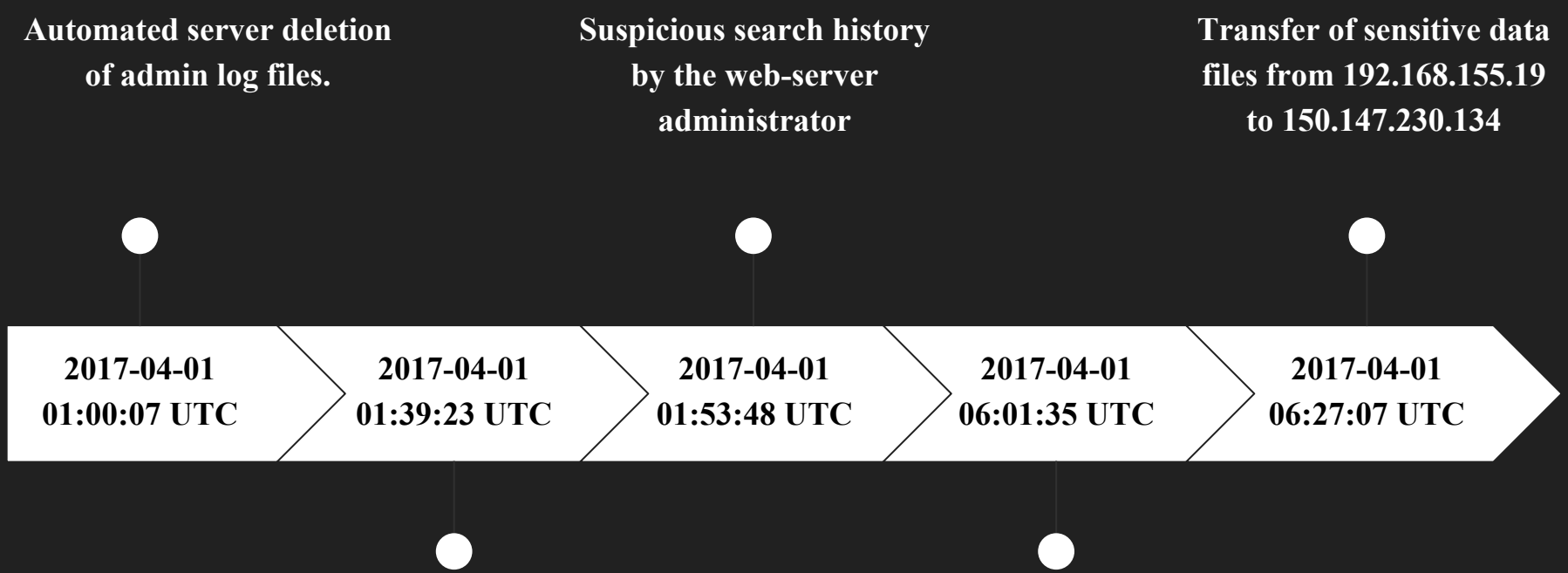
- Image of Corporate Web Server
  [Computed Hashes]
  MD5 checksum: f99a6134a3e8197e0e400a99855f6221
  SHA1 checksum: f70f58906edb1b5232b497a33957aa5d266a9302

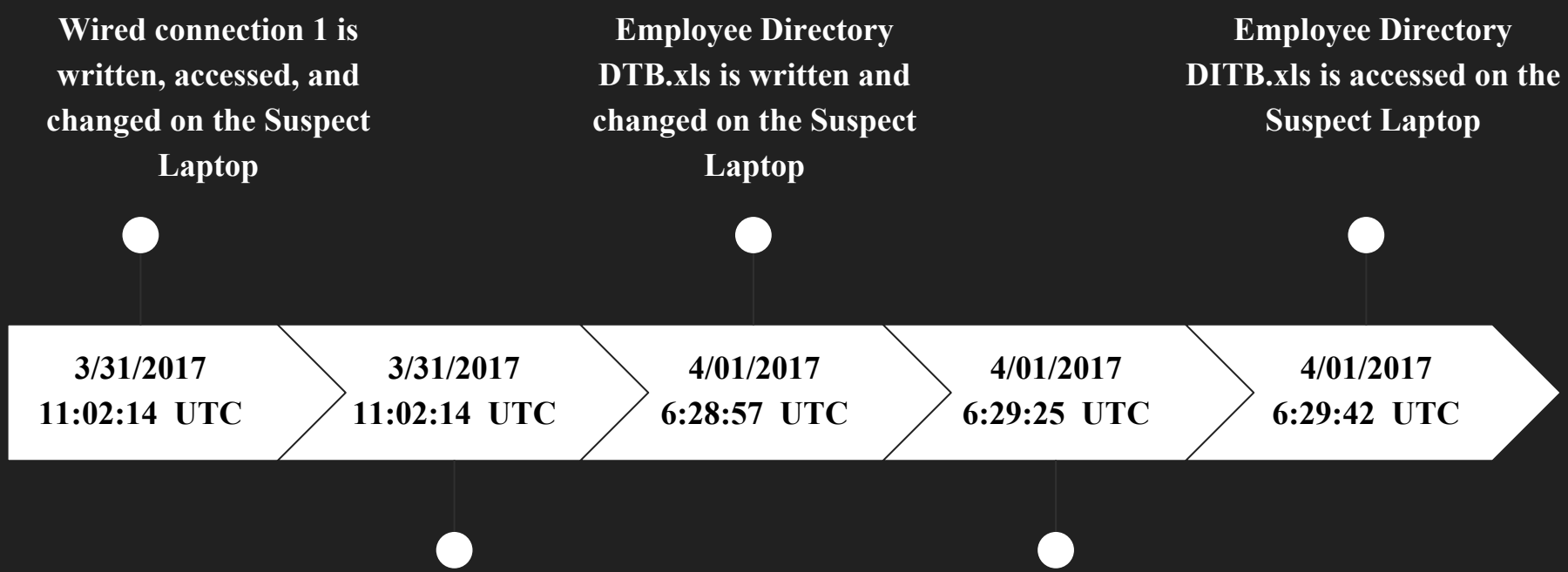
- Image of Suspect Laptop
  [Computed Hashes]
  MD5 checksum: f026053d320066961c7308fbf2c80bd9
  SHA1 checksum: 1864e1b8b632f6bcd6f0ed7fdf30eda90757f417

Tools Used

- Guidance® Software's EnCase® version 7.06.01
- AccessData® Forensic Toolkit Suite® version 6.2.0.1026
- AccessData® Registry Viewer® version 1.8.3.0
- AccessData® FTK Imager Lite version 3.1.1
- Magnet Forensics Internet Evidence Finder version 6.7.4.0771
- Autopsy version 2
- SANS Sift Workstation version 3.0

Timeline


Automated server deletion of admin log files.
Suspicious search history by the web-server administrator
Transfer of sensitive data files from 192.168.155.19 to 150.147.230.134
2017-04-01 01:00:07 UTC
2017-04-01 01:39:23 UTC
2017-04-01 01:53:48 UTC
2017-04-01 06:01:35 UTC
2017-04-01 06:27:07 UTC
Identification of corporate web-server IP address.
Identification of Employee database, Customer database, and Sales Representative database


Wired connection 1 is written, accessed, and changed on the Suspect Laptop
3/31/2017 11:02:14 UTC
Wired connection 1.GK4EXY is written, accessed, and changed on the Suspect Laptop
3/31/2017 11:02:14 UTC
Employee Directory DTB.xls is written and changed on the Suspect Laptop
4/01/2017 6:28:57 UTC
Sales Team Roster DITB.xls is written and changed on the Suspect Laptop
4/01/2017 6:29:25 UTC
Employee Directory DITB.xls is accessed on the Suspect Laptop
4/01/2017 6:29:42 UTC


Sales Team Roster DITB.xls is accessed on the Suspect Laptop
.bash_history file is written, accessed, and changed on the Suspect Laptop
4/01/2017 6:31:49 UTC
4/01/2017 6:31:50 UTC
4/01/2017 6:45:03 UTC
2017-04-01 6:35:55 UTC
Customer Directory.xls is accessed on the Suspect Laptop
Last logon time of Mr. Munoz

Findings

Corporate Workstation

Accomplishment 1

- Discovered that Mr. Munoz last login time for the workstation was 4/1/2017 at 6:35:55 UTC
- Mr. Munoz internet browser has google image searches for “Identification badge images”
- Google search for “how to make a fake security badge”
- A San-disk ultra was connected to the workstation at 4:40:00 UTC

Accomplishment 2

- The browser cache of web page instructional of “Picking New High Security Door Locks”
- Website and wordpress database login credentials were discovered on the desktop in a .txt file
- It has been discovered that the firewall had been turned off at 6:13:04 UTC.

Attention areas

Risk 1

- Potential fake security badge being used
- Physical security

Risk 2

- Login credentials for website and wordpress in plain text
- A usb device not belonging to the corporation being connected to a corporate workstation.
- Firewall turned off

Corporate Web-Server

Accomplishment 1

- Processed e01 file corporate-web-server
- Identified the web-server IP address
- Identified sensitive files

Accomplishment 2

- Provided evidence of transferring sensitive files to 150.147.230.134
- Verified document sensitivity
- Cross referenced transfer destination

Attention areas

Risk 1

- Customer Information
- Employee Information
- Sales representative information

Risk 2

- Customer credentials
- Weak customer credentials