CY5210 | INFORMATION SYSTEM FORENSICS

Northeastern University

Case Study: Lone Wolf Scenario

Elton Booker | Part-Time Lecturer | e.booker@northeastern.edu

Scenario Introduction

CY5210
Information System Forensics

Scenario Background

- Jim Cloudy lives in Alexandria, VA
- J. Cloud has an online argument with his brother Paul
  - Throws his laptop on floor in anger
  - P. Cloudy lends him a sanitized laptop
- Unemployed and uses his computer at odd hours
  - Grows marijuana
  - 325K in savings
- Uploads documents to a variety of cloud services for availability
- J. Cloudy gives P. Cloudy access to storage accounts
- P. Cloudy notifies the police and J. is apprehended

Lone Wolf Planning

- Unhappy with media coverage of gun violence / gun-control
- Perceives an attack on 2nd Amendment
- Begins writing about his views and plans an attack
- Uploads documents to a variety of cloud storage services
  - Gives P. Cloudy access who reads documents and notifies police
  - A search warrant is executed
- Plan to attacked a town hall meeting to discuss gun violence
  - 7 April 2018 1230-1400
  - Cascades Library, 21030 Whitfield Pl, Sterling, VA 20165
- Depart Dulles airport to Indonesia (no extradition treaty)

Methodology - Caveats

- Laptop SSD wiped with EnCase Acquisition v7.12.01
- Windows 10 Education installed from a USB
- Actual Keylogger v3.2 was installed intentionally for grading/scenario
  - Installed on USB drive and logs when system turned on
- Live acquisition of SSD/RAM performed with FTK Imager via USB
- Three opens windows at acquisition
  - Downloads folder: installation files of the four cloud services
  - OneNote application: Jim's Notebook
  - Chrome Browser: Google Doc "Brother Chat" with chat feature

Final Scenario Facts

- Most research for the attack was planned on this system
- AWS account created on another system to preserve CC data
- Username / password stored in image – account deleted
- Public and private keys also downloaded to system
- Google account created on another computer
  - Files downloaded from another Google Drive accidentally
  - "Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/IndexedDB/https_drive.google.com_0.indexeddb.blob"
- MS Office license associated with a real university email
- Desktop synced to Google Drive (S3 using S3 Browser)

Northeastern University

Case Study Requirements

CY5210
Information System Forensics

Target Hardware – Dell Latitude E6430 ATG

Characteristic	Detail
Name	DESKTOP-PM6C56D
Timezone	Eastern Daylight Time
CPU	I5-3340M dual-core
RAM	16GB
SSD	512GB Samsung 950 Pro
OS	Windows 10 Education x64
Version	1709 (OS Build 16299.309)
Username	jcloudy
Password	Jcloudy2018!

Live Acquisition

Characteristic	Details	
FTK Imager Lite	Version	3.1.1.8
Samsung T5 portable SSD	Model	MU-500B
	SN	S3UJNK0J707805H
LoneWolf.E01	Start	Fri Apr 06 08:50:44 2018
	Finish	Fri Apr 09:42:25 2018
	MD5	7af48fa65519e84246b1729e5b68f140
	SHA1	694e26624d1ea029eb50d793b198edf85be4b4fc

Installed Software

Software	Version
Microsoft Office 365 ProPlus	1708 (Build 8431.2236)
Microsoft Edge Browser	41.16299.248.0
Microsoft OneDrive Application	18.044.0301.0006
Google Chrome Browser	65.0.3325.181, 64-bit
Google Backup and Sync	3.40.8921.5350
Box Sync Application	4.0.7900.0
Dropbox Application	47.4.74
NetSDK S3 Browser Application	7.6.9

Related Accounts

Accounts	Credentials
Microsoft Account	jimcloudy@outlook.com
Google Account	jimcloudy1@gmail.com
Dropbox Account	jimcloudy1@gmail.com
Box Account	jimcloudy1@gmail.com
AWS Account	jimcloudy1@gmail.com
AWS S3 Bucket	cloudy-thoughts
Facebook	jimcloudy1@gmail.com
Twitter	@jcloudy1 / jimcloudy1@gmail.com

Non-Target Devices

SanDisk Extreme USB 3.0 (1)	**Details**
Model and Size	SDCZ80-032G 32GB
External ID	BM170225534bB
Usage	Windows 10 installation
SanDisk Extreme USB 3.0 (2)	**Details**
Model	SDCZ80-016G 16GB
External ID	BL160624687B
Name	CloudLog
Usage	Keylogging

Windows Triage Artifacts

- Registry Hives/Files
  - SAM, SYSTEM, SECURITY, SOFTWARE
  - NTUSER, and USRCLASS
- Link Files
- Shellbags
- Jump Lists
- Log Files
- Memory (Live/Dead)
- Setupapi.dev.log
- User Profile
- Prefetch
- $MFT
- $LogFile

See Lab Assignment 1

Report Requirements

- Report Template
  - Required for all case studies
- Chain of custody document
  - Use download time OR
  - The Apr 6 2018 time and Apr 13-20 for analysis
- Cloud-based artifacts
  - Documents
  - Images
  - Internet searches
  - Keyword searches


Q&A