2012 National Gallery DC Attack

NGDC

The 2012 National Gallery DC scenario spans approximately 10 days and encompasses two distinct yet intertwined story arcs. The scenario is centered around an employee at the National Gallery DC Art Gallery. Criminal plans for both theft and defacement are discussed amongst actors during the scenario, and evidence may remain across the digital devices they used. The scenario is terminated upon suspicious activity being reported to law enforcement at which point certain devices are seized and network traffic logs are requested. The scenario materials can be used as both teaching material and for forensics research. Like the 2009-M57-Patents scenario, images were taken at the end of every day of the scenario. The materials include disk images of hard drives and both logical and physical images of mobile devices. Network captures were performed using the SSLstrip tool, allowing for capture files to be available with and without encrypted SSL traffic. Alex, a wealthy businessman with Krasnovian ties contacts Carry, a Krasnovian supporter in the US. Alex is seeking to embarrass America and damage public relations by defacing Foreign Art, belonging to Majavia and currently on display in the National Gallery during the month of July. Alex knows Carry through her Krasnovian parents, who also have strong anti-American sentiment. Alex contacts Carry through her father and recruits her to assist with his cause. He is sending some "tourists", Krasnovian militants, to Washington, DC to do the deed. Carry is to develop the plan to get them into the museum with the tools they need to damage the artwork. Tracy works as a supervisor at the National Gallery and is an acquaintance of Carry. Carry contacts Tracy and starts communicating small data as a back and forth under the auspices that

Carry wants to organize a Flash mob at the gallery and needs a little help. Carry will give money to Tracy for this help. Items transferred are suspicious in nature but not outright illegal. Tracy's money troubles help her overlook the suspicious nature of the requests. Subsequently, Tracy has been having an ongoing dialog with her brother about stealing specific items (Stamps) from the National Gallery. Tracy will have correspondence on her work computer, personal phone, and home computer relating to her conspiracy to have some valuable items stolen. Carry is technically savvy in that she knows about steganography tools and encryption. She hides many of her correspondence in steg files and encrypted files. She purchases a tablet computer and sets it up to use her catsumtwelve email account dealings with Alex, setting up the the flash mob, Carry is interested in security, schedules, events, and locations where art will be displayed. Unfortunately for everyone involved, Joe, Tracy's ex-husband, installed a key logger onto her computer prior to the divorce to monitor Terry, discovers the conspiracy to commit theft and turns her into the police. This reveals the contact between Tracy and Carry leading to Carry's Tablet and phone being seized as well revealing the separate defacing plot.

Persona Descriptions

Tracy

Tracy is a recently divorced mother in the middle of a child custody battle. Unfortunately, Tracy's daughter is in an expensive private school, which Tracy can no longer afford on her salary. Her ex-husband will only pay for the school if Tracy will give over custody of their daughter to him. Worse, Tracy's daughter, Terry, age 15, has stated that she would rather live with her dad if it comes to staying in school. "After all, you ran Dad off in the first place."

Pat

Pat is Tracy's brother. He is a police officer of the D.C. Enforcers Bureau. He holds the status of detective. He is very devoted to his sister and niece Terry, to this point he isn't an outright criminal, but walks the line very closely. He busted King with some items that were against his parole, but hasn't arrested him on the promise of a future "favor."

Joe

Joe is the father of Terry and is currently going through the divorce with Tracy. Joe is financially well-off, and still bitter about the relationship problems. He previously installed a key logger on the MacBook Air in an attempt to keep track of Terry's online behavior. Now that Joe and Tracy are going through a divorce, he has motivation to utilize the key logger to spy on both Tracy and Terry. Joe used to have an account on the family MacBook Air however it was deleted. The home folder may have been preserved.

Alex

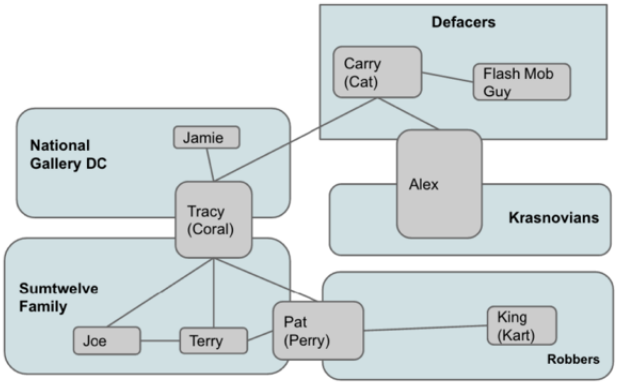
Alex is a Krasnovian supporter who wishes to embarrass the United States. He is a foreigner and lives outside the country presumably in a region called Krasnovia. He knows Carry through extended family connections and contacts her as both having similar family ties and a fellow Krasnovian. He plans to deface foreign works that are on exhibit in the National Gallery DC. Defacing said artwork will embarrass the United States and possibly degrade the reputation between the United States and the foreign country providing the foreign exhibit to America. (In some documentation this is referred to as 'Majavia', a second pseudo-nation)

Carry

Carry is a somewhat criminally involved individual that shares family ties with Alex. She is a Krasnovian supporter. Carry is both technologically savvy and an occasional social media user. She is contacted by Alex in the beginning of the scenario and asked to orchestrate the defacing of the artwork because she is both aligned with Krasnovia and because she has 'Connections'. She has a slight familiarity as friends/acquaintances with Tracy.

Terry

Terry is the daughter of Tracy and Joe. Terry attends an expensive private school. (Prufrock Preparatory School). She wants to stay in school to avoid having to start over and so that she can keep her current friends, despite the fact that her mother can no longer afford to pay the tuition.



Evidence

The seized evidence has been processed for you by the ingest team of the crime laboratory. You have been provided with the following data:

- Carry's phone on 2012-07-15 [ZIP] [FTK Logical Dump]
- Carry's tablet on 2012-07-16 [E01] [TAR]

- Email messages generated by the spyware installed on Tracy's Macbook Air and that were periodically emailed to Joe [ZIP]
- Tracy's phone on 2012-07-15 (encase) [L01] [ZIP]
- Tracy's phone on 2012-07-15 (other extraction tools) [EO1] [tar]
- Tracy's external hard drive [E01]
- Tracy's home computer [E01] [E02]
- Exterior Network Packet Dumps
  - exterior 2012-07-06 exterior-2012-07-06.pcap
  - exterior 2012-07-09 exterior-2012-07-09.pcap
  - exterior 2012-07-10 exterior-2012-07-10.pcap
  - exterior 2012-07-12 exterior-2012-07-12.txt
- Interior Network Packet Dumps
  - interior 2012-07-06 interior-2012-07-06.pcap
  - interior 2012-07-09 interior-2012-07-09.pcap
  - interior 2012-07-10 interior-2012-07-10.pcap
  - interior 2012-07-12 interior-2012-07-12.txt

Acknowledgements

The scenario was created during the summer of 2012 as part of a joint collaboration between the U.S. Naval Postgraduate School and the U.S. Military Academy at West Point. Those who worked on the project include:

- Greg Tarancon, USMA '2013
- Alex Eubanks, https://github.com/endeav0r/
- Jacob Cox, now a Research Scientist with Soar Technology, Inc.
- Mark DeYoung, now at the Air Force Institute of Technology in Dayton, OH.
- Christian Sharpstein, U.S. Army

Following that summer, this scenario lay dormant until September

2015, when Joseph Greenfield at USC picked it up and worked with a number of students to create a teacher's guide. Those creating the teaching guides include:

- Instructor Packet (introduction): Joseph Greenfield
- Tracy's MacBook Air: Parthasarathy Mysore Alwar and Sean Straw
- Tracy's iPhone [DFDR07-17]: Pratim Kar
- Tracy's External Hard Drive [DFDR05-17]: Christopher Holmes and Heather Romero
- Network Logs: Sean Straw
- Email (.eml) Files [DFDR03-1 to DFDR03-12]: Sean Straw
- Carry's Tablet [DFDR02-06]: Kshitij Kumar and COle Manaster
- Carry's Phone [DFDR01-06]: Amanda Sulistyo and Yiwei Song

(Or you can download all teaching guides as a single zip file. Please note: the teaching guides are *encrypted*. To obtain the the decryption key, which can be used for all digitalcorpora.org teaching guides, please see our page on obtaining solutions. Finally, for those interested in doing digital forensics research, please browse the entire 2012 National Gallery DC scenario archives. You will find daily images of each device, and lots more materials.