CS593: Digital Forensics

Lecture 3: Real-World Case Studies

D. Kevin McGrath

Thursday, June 29, 2023

Outline

- Real-world cases that involved digital evidence.

Suspicious Web Browsing

- Justin Ross Harris was charged with murder of his toddler son, who died after being left in a hot car.
  - Internet browsing history on Justin's work computer showed he had searched for information on how child deaths occur in cars and how hot it needs to be to kill them.
  - He was eventually found guilty.

Serial Killer Caught after 30 Years

- “BTK” serial killer Dennis Rader murdered 10 people in Kansas across 3 decades.
- He sometimes sent mocking messages to the police.
- In 2005 he sent a message asking the police if they could trace the source of documents on a floppy disk; via a newspaper ad, they told him no.
- He sent a message on a floppy disk, which also included a deleted Word document whose metadata referred to the Christ Lutheran Church in Wichita (where he was president of the church council) and named “Dennis” as the last person to modify the file.
- Within 10 days of mailing the disk, he was arrested.

Some Snapshots

- Dozens of New York City gang members were indicted in 2014 after posting extensive self-incriminating text and photographs on Facebook.
- In 2014, Johns Hopkins Health System paid a $190 million settlement to over 7,000 patients after photos taken during their exams were found on a gynecologist’s home computer.
- In April 2014, 3 Swedish schoolchildren were accused of hacking into their school to change grades and redirect text messages about truancy.

Industrial Espionage at Ford Motor Co.

- In 2006, Ford engineer Xiang Dong “Mike” Yu copied 4,000 Ford design documents onto an external hard drive, flew to China, and resigned from his job via e-mail.
- In 2008, Yu started a job at the Beijing Automotive Company.
- In October 2009, he returned to the U.S., where he was arrested at the airport with his Beijing Automotive Company laptop.
- It contained 41 Ford design documents, all of which had been opened by Yu since he started working at the Beijing Automotive Company.

Sloppy Digital Forensics

- In October 2008, Brad Cooper of North Carolina was charged with the murder of his wife Nancy.
- An investigator who was trying to unlock the victim’s cell phone accidentally deleted data; e.g., the SIM card was wiped clean.
- At trial, prosecutors testified that Brad had performed a certain Google Maps search that was found in the browsing history on his laptop—although they presented no evidence showing that he was the person using the laptop at the time.
- He was found guilty but granted a re-trial because of the inappropriate presentation of digital evidence. He eventually confessed—after almost wiggling off the hook because of poor digital forensics practices.

Gameover Zeus and CryptoLocker

- Gameover Zeus is a massive peer-to-peer botnet that emerged in late 2011.
- Has infected between 500,000 and 1,000,000 Windows computers around the world.
- It intercepts online browsing sessions, and when users visit their banks’ website, it displays fraudulent messages requesting answers to the bank accounts’ security questions.
- Has resulted in the theft of over $100 million from the U.S. alone.

Gameover ZeuS and CryptoLocker, 2

- Another thing Gameover ZeuS does is distribute the CryptoLocker malware.
- CryptoLocker encrypts files on infected machines. Victims are forced to pay “ransom” money, typically several hundred dollars, for the decryption key to regain access to their files.
- It infected over 234,000 machines in its first 8 months; over $27 million in ransom payments were made in the first 2 months alone.

Gameover ZeuS and CryptoLocker, 3

- Law enforcement agencies from at least 11 countries, plus some universities and tech companies, collaborated in the investigation.
- Authorities were able to locate and seize servers that were operating as control hubs.
- In June 2014, the U.S. Department of Justice indicted a 30-year-old Russian citizen on a range of charges, alleging he was the leader of a gang of Russian and Ukrainian cyber criminals behind Gameover ZeuS and CryptoLocker.

World Cup Corruption?

- In 2010, Qatar was surprisingly named host of the 2022 FIFA World Cup of soccer, despite major shortcomings such as summer daytime temps over 120°F.
- In 2011, an ex-employee of their delegation claimed they won by bribing officials, but she withdrew the claim.
- In June 2014, *The Sunday Times* published a report on a trove of millions of e-mails and bank transfer records leaked by a whistleblower.
- The data showed that a top Qatari soccer official had funneled payments of over $5 million to various people to gather support for Qatar’s World Cup bid.
- The scandal widened and as of late 2016 is still ongoing.

Attack on NASDAQ

- In October 2010, the FBI’s Internet monitoring systems detected malware on the central servers of NASDAQ (the world’s 2nd largest stock exchange).
- The attack turned out to be a new version of previously known malware created by the Federal Security Service of the Russian Federation.
- It was extremely sophisticated (e.g., included two zero-day exploits).

Attack on NASDAQ, 2

- The malware seemed to have been designed to steal data, but had the destructive capacity to wipe out the entire NASDAQ exchange.
- The investigation revealed shoddy security practices at NASDAQ, and uncovered multiple other ongoing malware attacks.
- Details have not been made public. Investigators believe the main goal was to steal NASDAQ technologies for use in Russian financial systems.

Stuxnet: Nation-State-Funded Malware?

- Stuxnet is a remarkable worm that surfaced in mid-2010.
- It exploited 4 zero-day Windows vulnerabilities and appears to have been developed by a large group of programmers working for months (at a likely cost of millions of dollars).
- It was designed to spread aggressively but become inert on any machine that isn’t a particular kind of Siemens system running certain very specific industrial processes.
  - I.e., the exact kind of systems used by Iran to run its nuclear enrichment facilities.

Stuxnet, 2

- If the victim system is attached to a particular kind of motor, the malware changes the frequency of the motor’s rotation so that it runs far too fast, then far too slow, then normally.
  - E.g., Iran’s nuclear facilities had delicate nuclear centrifuges whose rotation would have been affected if they were infected by Stuxnet.
- The malware also installs a man-in-the-middle attack that generates normal-looking data about the motor rotation, so that monitoring systems do not detect the unusual rotation.

Stuxnet, 3

- Mysterious major technical problems afflicted Iran’s nuclear program in 2009, reducing their number of centrifuges from ~4,700 to ~3,900.
- Stuxnet may have destroyed the centrifuges by causing fluctuations in the rotational frequency, causing damaging vibrations.
- Iran’s nuclear program quickly bounced back, probably disappointing the attackers.
- In 2013, Edward Snowden leaked classified documents showing that the U.S. & Israeli governments collaborated to create Stuxnet.

Questions?