ISE331: Snowden Attack
Outline of Topics Covered

- Snowden’s background and how he got to the position of being able to leak confidential information from the CIA
- How Snowden planned and performed the attack
- The method used to release the confidential information and what happened to Snowden afterwards
- What post-leakage effects were present in the United States and in other parts of the world such as the European Union
Who is Edward Snowden?

- Born June 21st, 1983
- High school dropout
- Enlisted in the army in 2004.
- In 2005, he was working as a security officer at the University of Maryland’s Center of Advanced Language Study which is sponsored by the NSA
The transition from high school dropout to the CIA

- Snowden despite no formative teaching managed to get a job with the Central Intelligence Agency (CIA) in the department of global communications.
- The CIA was impressed with his skills and he was sent to a CIA “secret” school for technology specialists in March of 2007.
- After some rigorous learning, he was brought abroad to work in Switzerland to investigate their banking system.
Snowden’s Time in Switzerland

- During this time Snowden saw first hand what the effects of the war on terrorism in the United States was having abroad.
- He considered whistleblowing at this point but held off knowing at this point Obama would be the next president.
- Unfortunately, Snowden’s hopes of Obama changing the way intelligence was being gathered never came true.
Motivations

- Snowden said to the Washington Post “It was more of a slow realization that presidents could openly lie to secure the office and then break public promises without consequence”
- Snowden was also at odds with the CIA in general. During his time in Switzerland he witnessed some terrible things the CIA would do to acquire sources
Snowden’s First NSA Job

- 2010 - Snowden transferred from the CIA to NSA
- Technical expert for Dell located in Japan
- Helped Dell of Japan secure their networks
- After Japan, was placed back in Hawaii, again for Dell
- After Hawaii, Snowden was placed in Virginia for a short period
- Snowden had climbed up in the chain of command during this time
The Final Straw

- After many years in security, Snowden wanted to expose the methods that the government was using
- Last government job as an Infrastructure Analyst at Booz Allen Hamilton
- March 12th, 2013, Snowden releases the information
- In response to his release, James Clapper states that the NSA does “not wittingly” collect information on millions of Americans
Accessing the data

● An original report stated that Snowden asked fellow staff members for their logins as it was “required” for his position
● Later contradicted by General Keith Alexander, stating that Snowden had “fabricated digital keys” to gain access
● A third party security firm, Venafi, determined the most probable method of access
Venafi and the Investigation of the Attack

- Not much info released to public
- We do know that:
  - Snowden had a Common Access Card (CAC)
  - Snowden used Secure Shell (SSH) keys in his work as a systems administrator
  - Snowden had access to NSA servers using a thin client or basic terminal
- Cyber security company Venafi wrote article on how Snowden may have breached NSA
  - At least partially revealed correct from declassified documents
Phases of the Intrusion Kill Chain

1. Reconnaissance
   - Research, identification, and selection of targets

2. Weaponization
   - Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

3. Delivery
   - Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

4. Exploitation
   - Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems

5. Installation
   - The weapon installs a backdoor on a target’s system allowing persistent access

6. Command & Control
   - Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.

7. Actions on Objective
   - The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target
Reconnaissance

- Snowden used methods of access provided by NSA to find out what information was being stored and where
- Snowden used social engineering to persuade some of his colleagues to give up their credentials
  - Systems Admin
  - Keylogger
Infiltration

- Snowden got access to and made his own fabricated administrative SSH keys to gain access to information
- NSA completely failed at keeping their systems secure and monitoring for this type of activity
  - Time difference
  - Too many privileged access users (least privilege)
  - Access to both NSAnet and British GCWiki
- Several week venture of downloading data while keeping appearances
Exfiltration

- NSA failed to make use of Insider Threat Management software
- Snowden used Command and Control servers to encrypt his data transfer sessions to other networks which kept the transfer hidden from the NSA
- Had plausible excuse for having flash drives and such
- Snowden also altered system log files to camouflage his actions
Information Obtained

- Snowden found out about hundreds of secret NSA activities and agendas
- Major leaks include:
  - NSA collected telephone records of millions of Verizon customers
  - NSA Prism program accessed and collected data through back doors into Google and Facebook
  - NSA EvilOlive program collected and stored large quantities of Americans' internet metadata
  - NSA scoops up personal data mined from smartphone apps such as Angry Birds
  - NSA strategy document revealed the agency's goal to acquire data from "anyone, anytime, anywhere"
Information Obtained Continued

- US government spies on at least 38 foreign embassies and missions
- NSA siphons billions of foreign cell phone location records into its database
- NSA infected more than 50,000 computer networks worldwide with malware designed to steal sensitive information
- Working with Canadian intelligence, NSA spied on foreign diplomats at G8 and G20 summits in Toronto in 2010
- Widespread spying revealed in Italy, NSA spied on Italian citizens including diplomats and political leaders
How was the information released to the public?

- Made contact with Guardian journalist Glenn Greenwald in 2012, promising unprecedented scoop
- Greenwald dismissed him at first, Snowden then contacts documentary filmmaker Laura Poitras who brings the three together
- Within months of their meeting, documents were published by popular media outlets worldwide
  - The Guardian (Britain),
  - Der Spiegel (Germany),
- Communicated with journalists through encrypted email and using the persona “Verax”
  - Verax in Latin stands for “truth teller”
Escape and Seeking Asylum

- A few weeks before the first leaked documents were published, Snowden took a leave of absence from the NSA and flew to Hong Kong
- Snowden then boarded a flight to Moscow, was not stopped by Hong Kong authorities
- Several countries offered Snowden asylum, could not get out of Moscow
- Snowden granted temporary asylum in Russia
- Snowden's asylum, which expired in 2017, was extended until 2020
Public Opinion

- Terms used to describe Snowden: hero, whistleblower, dissident, patriot, traitor
- Huffington Post poll shows:
  - 38% Support Snowden
  - 33% Disapprove of Snowden
  - 29% Unsure
- Differing opinion on Snowden seems to be most significant when looking at younger and older generations
- Sparked global debate on privacy and consent by bringing the US’s illegal mass surveillance to light
-Leaks led to distrust of the United States by not only Americans but by other targeted nations
Resulting Lawsuits

- The Electronic Frontier Foundation filed a formal lawsuit based on information from leaks
- Ongoing case known as Jewel vs. NSA
- ACLU (American Civil Liberties Union) filed lawsuit against James Clapper, Director of National Intelligence
  - Alleged NSA’s phone record program was unconstitutional
  - Ruled that NSA’s phone recordings were legal
What have been the long term effects?

● Americans became more critical of government and stopped being as compliant
● Escalated tensions between users and private tech companies
  ○ Google, Facebook, YouTube, Apple, Microsoft, etc.
● People support NSA surveillance
  ○ 50/50 say it is acceptable in certain circumstances or unacceptable in all circumstances
● Section 215 of Patriot Act also brought into question
Sources

https://www.wired.com/2014/08/edward-snowden/

https://www.washingtonpost.com/world/national-security/investigators-looking-at-how-snowden-gained-access-at-nsa/2013/06/10/83b4841a-d209-11e2-8cbe-1bcbee06f8f8_story.html?noredirect=on&utm_term=.5777c3eab301


https://www.darkreading.com/attacks-breaches/how-did-snowden-do-it/d/d-id/1140877

https://www.venafi.com/blog/deciphering-how-edward-snowden-breached-the-nsa

http://investigations.nbcnews.com/_news/2013/08/26/20197183-how-snowden-did-it

https://www.venafi.com/blog/venafi-analysis-of-snowden-nsa-breach-confirmed-2-years-later


https://www.huffpost.com/entry/edward-snowden-poll_n_3542931
Sources cont.


Picture sources

Slide 3 - https://www.biography.com/activist/edward-snowden

Slide 8 - https://www.flickr.com/photos/medilldc/6797228431

Slide 9 - https://fcw.com/~/media/GIG/FCWNow/People/A/Alexander_Keith_370.jpg


