Stuxnet Worm Attack

Timmy Jenkins

CSCI 405 Principles of Cybersecurity

Charleston Southern University

Professor Patrick Hill

2/23/2025

What happened?

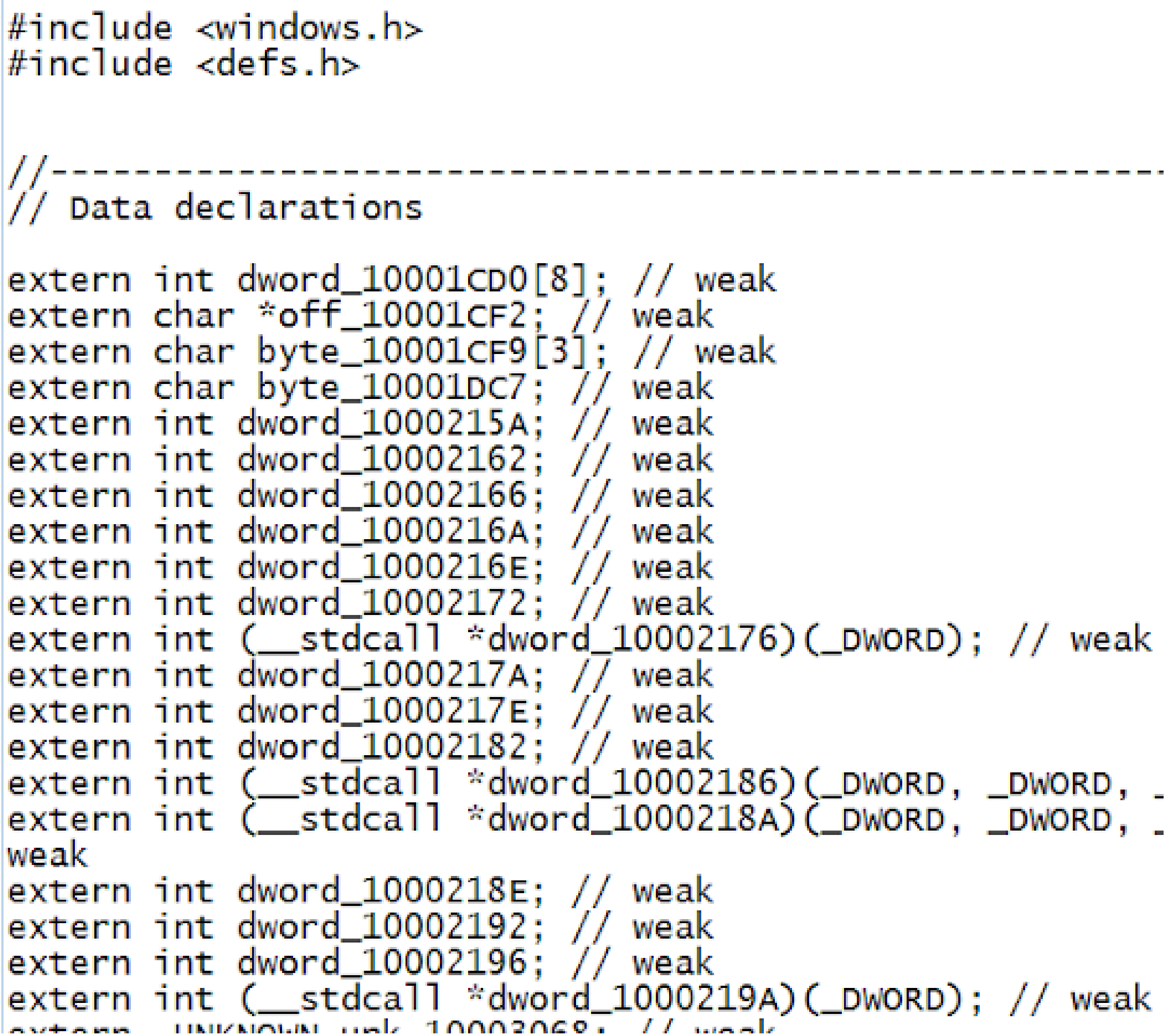
- The Natanz nuclear enrichment complex in Natanz, Iran, was hit by a sophisticated cyber attack between 2007 and 2010. This multi-national attack, allegedly carried out by the United States, Germany, France, Denmark, Israel, and Great Britain, caused catastrophic damage to the facility’s centrifuges (Reuters, 2021).
- The ultimate goal was to stall the enrichment process for diplomatic reasons, resulting in the destruction of about a fifth of Iran’s uranium enrichment capabilities.

Where did the attack take place?

- The Bushehr power plant was initially believed to be a primary target, but the Natanz Enrichment Facility was ultimately the main focus (Iran Watch, 2002).
- Operated by members of the Atomic Energy of Iran and the Islamic Revolutionary Guard, Natanz is Iran’s primary location for nuclear material enrichment (Wikipedia, 2020).
- Personal computers of workers at the Bushehr power plant were also infected during the attack.

What is the Stuxnet Worm?

- Cyberweapon allegedly developed by the United States and Israel.
- Originally thought to be developed around 2005.
- It was designed to target SCADA systems (Supervisory Control and Data Acquisition systems) (Zetter, 2015).
- It has widely believed that this is the worm that is responsible for the cyber attack that caused extreme damage to the Iranian nuclear program.



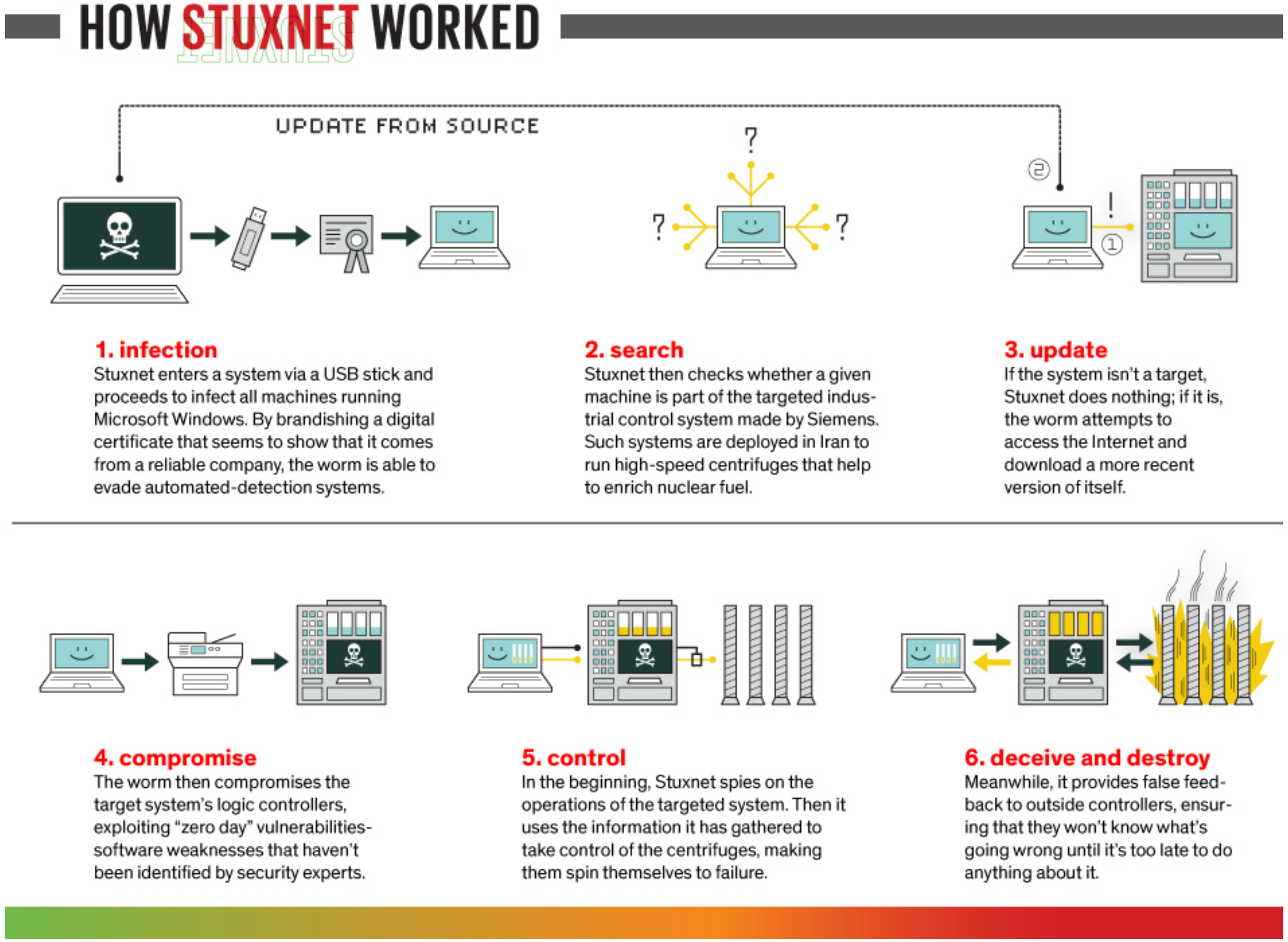
```
#include <windows.h>
#include <defs.h>


//--------------------------------------------------------------
// Data declarations

extern int dword_10001CD0[8]; // weak
extern char *off_10001CF2; // weak
extern char byte_10001CF9[3]; // weak
extern char byte_10001DC7; // weak
extern int dword_1000215A; // weak
extern int dword_10002162; // weak
extern int dword_10002166; // weak
extern int dword_1000216A; // weak
extern int dword_1000216E; // weak
extern int dword_10002172; // weak
extern int (__stdcall *dword_10002176)(_DWORD); // weak
extern int dword_1000217A; // weak
extern int dword_1000217E; // weak
extern int dword_10002182; // weak
extern int (__stdcall *dword_10002186)(_DWORD, _DWORD, _
extern int (__stdcall *dword_1000218A)(_DWORD, _DWORD, _
weak
extern int dword_1000218E; // weak
extern int dword_10002192; // weak
extern int dword_10002196; // weak
extern int (__stdcall *dword_1000219A)(_DWORD); // weak
extern UNKNOWN unk_10003068; // weak
```

How does it work?

- The worm is an unusually complex program.
- Likely took a team of very experienced individuals to develop such a complicated program.
- It specifically targets programmable logic controllers using zero-day flaws and focuses on Microsoft operating systems and Siemens Step 7 software (Zetter, 2015).
- Programmed to remain undetected by traditional means.



HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Who was involved?

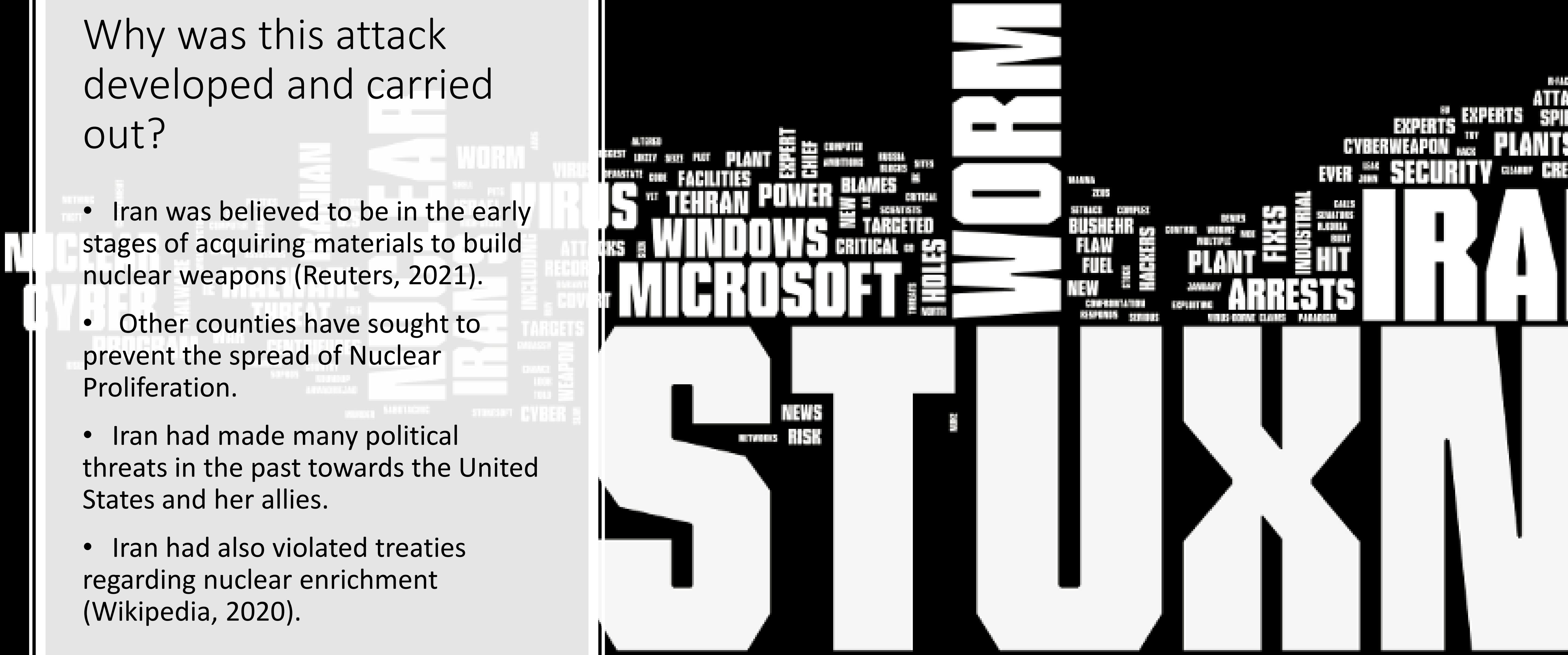
- No one has openly admitted to being involved in the attack or development of the worm.

- However, it is widely accepted that Stuxnet was developed by the United States and Israel (Zetter, 2015).

- Developed under the code name “Operation Olympic Games”. Development took place between at least two US presidents.

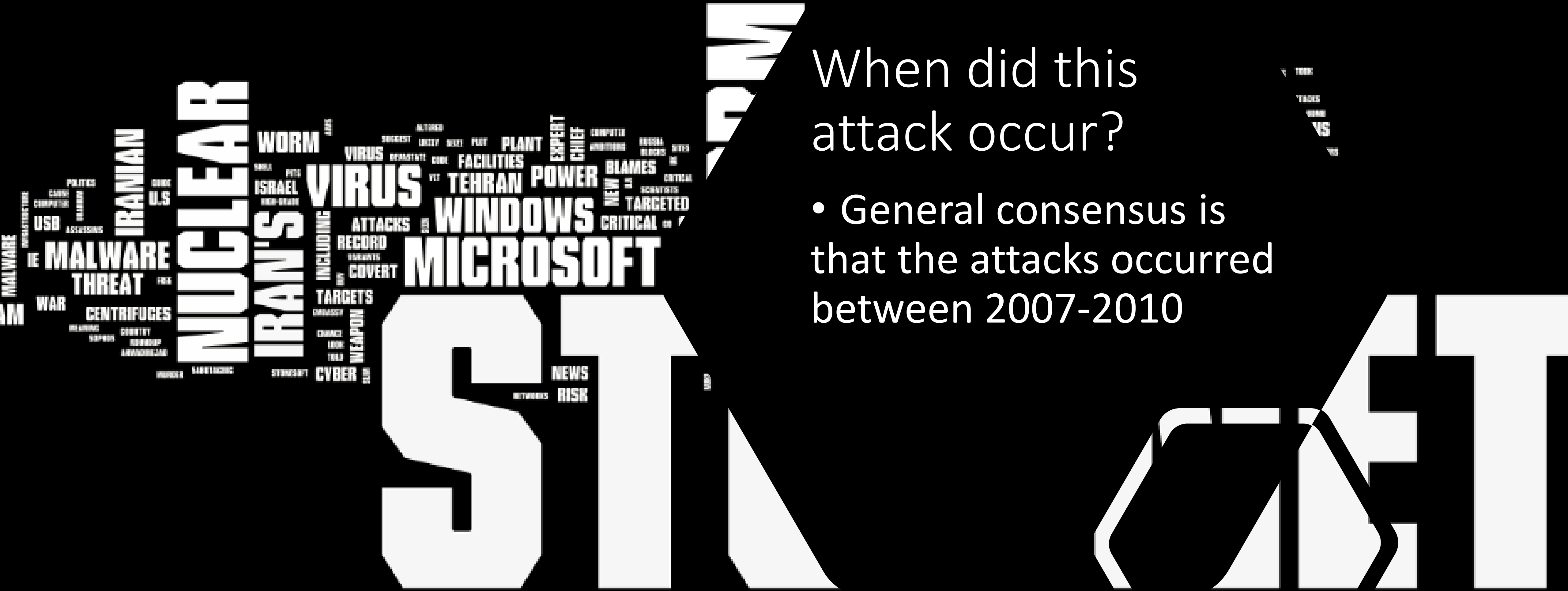
- Individual software engineers have never been identified. Although many believe it was at least a small group.

- Involvement of intelligence agencies such as the NSA and Israel's Unit 8200 has been suggested (Wired, 2011).



Why was this attack developed and carried out?

- Iran was believed to be in the early stages of acquiring materials to build nuclear weapons (Reuters, 2021).
- Other counties have sought to prevent the spread of Nuclear Proliferation.
- Iran had made many political threats in the past towards the United States and her allies.
- Iran had also violated treaties regarding nuclear enrichment (Wikipedia, 2020).



When did this attack occur?

- General consensus is that the attacks occurred between 2007-2010

How was the attack carried out?

- The attack was introduced using USB devices due to the facility’s air gap, which prevented typical network infections (The Hacker News, 2011).
- This meant that the attack had to be carried out by a person. Either willing to do it or doing it unknowingly.
- Once inside, the Stuxnet worm infected the internal control network and used a man-in-the-middle attack to deceive monitoring systems (Hacker Noon, 2019).
- It was never meant to spread to the internet but it did.

How was the attack carried out? –cont.

- After the Stuxnet worm successfully breached the air gap, the internal control network for the centrifuges became infected.
- The Stuxnet used a man-in-the-middle style attack to trick the operation systems from realizing that there was a problem. When the system tried to send the warning messages, the Stuxnet used a loop back capability to display false information thus avoiding detection.
- Stuxnet manipulated the speed of the centrifuges, causing them to spin at dangerous rates before slowing down suddenly. This cycle of acceleration and deceleration caused stress fractures, leading to mechanical failures (Hacker Noon, 2019).
- There was no way to diagnose why the centrifuges were breaking down.

Unintended Consequences.

- Stuxnet eventually spread beyond its intended target. It is believed that an infected USB or laptop left the facility, unintentionally releasing the worm into the wild (Wired, 2011).
- It is speculated that this occurred the same way the original attack did. There was an infected laptop or USB device that left the facility and connected to an outside network somewhere else.
- Affected countries include, Iran, Indonesia, India, Azerbaijan, United States, Pakistan and more.
- More advanced Malware was created in the aftermath after Stuxnet was studied in-depth.

Further actions taken and reactions to Stuxnet

- Iran publicly condemned the attack as an act of cyber warfare and intensified its focus on cybersecurity, establishing a dedicated team to prevent future incidents (Cryptome, 2010).
- Iran had since then built a team of cyber security experts tasked with training and preventing future attacks. Possibly even being able to launch attacks in the future.

Conclusion.

- Stuxnet is easily one of the most powerful cyber attacks to date. It was designed by some of the most knowledgeable programming experts in the world. The planning and execution that went into this operation is shrouded in so much secrecy, the world may never know who had a hand in it.
- Even though the worm has been heavily scrutinized by experts across the world now, they still don’t know who made it. That is the most important piece of the puzzle. This kind of cyber attack could be weaponized again, against other targets if necessary, so long as the same kind of people are working on the operation. This operation highlights just how important the future of Cyber Security really is.

Works Cited

Cryptome. (2010). *Natanz uranium enrichment complex, Iran, 2002–2010*.
http://cryptome.org/eyeball/natanz/natanz.html

FAS. (ca. 2005). *Bushehr nuclear power plant*. Federation of American Scientists.
https://nuke.fas.org/guide/iran/facility/siemens_pwr_bilbis_a.jpg

Hacker Noon. (2019, July 31). *Stuxnet, or how to destroy a centrifuge with a small piece of code*.
https://hackernoon.com/stuxnet-or-how-to-destroy-a-centrifuge-with-a-small-piece-of-code-66se283f

The Hacker News. (2011, July 19). *Stuxnet source code released online - download now*.
https://thehackernews.com/2011/07/stuxnet-source-code-released-online.html

IEEE Spectrum. (2015, February 26). *The real story of Stuxnet*.
https://spectrum.ieee.org/the-real-story-of-stuxnet

Iran Watch. (2002, September). *Natanz enrichment facility 2*.
https://www.iranwatch.org/sites/default/files/Natanz-092002.jpg

Reuters. (2021, October 25). *Iran feeds highly enriched uranium into more machines at Natanz, IAEA says*.
https://www.reuters.com/world/middle-east/iran-feeds-highly-enriched-uranium-into-more-machines-natanz-iaea-2021-10-25

Wikipedia. (2020, April 3). *Natanz*. Wikimedia Foundation.
https://en.wikipedia.org/wiki/Natanz

Wired. (2011, February 11). *Stuxnet: Five main targets*.
https://www.wired.com/2011/02/stuxnet-five-main-target/

Zetter, K. (2015). *Countdown to Zero Day: Stuxnet and the launch of the world’s first digital weapon*. Broadway Books.