Module 9.2: stuxnet and zero day attacks

cybersecurity notes: first massive "kinetic attack" impacting machinery

https://elab.hpa.edu/cs/videos/zero%20days.mp4

- 00-21:00 cyber background
- 21:00-38:00 what are centrifuges, how the code will be used
- 38:00- 57:00 cyber command, NSA, governments
- 57:00- NSA hackers

terms:

- airgap
- C2
- SCADA
- PLC
- zero day exploit
- DLL

questions:

1. what is a zero day exploit?
2. how did they know the code was from a nation state not a hacker?
3. what is a digital certificate?
4. why is learning about PLCs so important? (Arduinos are PLCs)
5. was there a C2 element in Stuxnet?
6. why were gas centrifuges so important?
7. did they just destroy these, or was it more complex?

8. did the operators know what was going on?
9. why was this important to the malware attack?
10. what is yellowcake uranium?
11. what is it turned into, and for what?
12. if you have seen Top Gun: Maverick, what is similar?
13. How did the PR film the Iranians made help to identify the code?
14. Look at the “balloon code”-do you see anything like the arduino code?
15. Why is it so scary to link code to “real world physical destruction”?
16. What is a DLL in the windows operating system?
17. What is the 4th dimension of warfare, according to the film?
18. What is the NSA?
19. What was buckshot yankee?
20. Compare the NSA use of remote computers with botnets
21. Why are password lists that have not been used before also known as "zero day" lists?

Migrated from Apple Server Wiki. Original page ID: 0115t5h3

Revision #2
Created 2026-09-29 15:59:56 UTC by Admin
Updated 2026-09-29 16:22:58 UTC by Admin