Hacking NASA

Tyler Hebenstreit

April 2, 2012

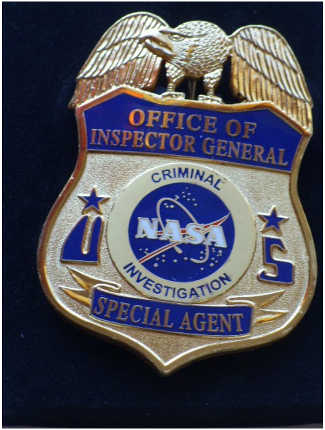
Why NASA?

- Proving l33t h4x0r 5k1ll5
- Hacking for profit
- Gathering intelligence

Why hack NASA?

Many of the technologies developed and utilized by NASA are just as useful for military purposes as they are for civil space applications, he said. While our nations defense and intelligence communities guard the front door and prevent network intrusions that could steal or corrupt sensitive information, NASA could essentially become an unlocked back door without persistent vigilance.
- Subcommittee Chairman Rep. Paul Braun

OIG Investigation



Attacks in 2011

- 5,408 incidents of installed malicious software or unauthorized access
- 47 APT attacks
  - 13 successfully compromised computers
  - One hack captured 150 emplpoyee credentials
  - Groups or organizations aiming to misbehave

Advanced State of the art intelligence technology and intrusion techniques

Persistent One goal in life...

Threat Capability and intent

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station
- China attacks!
  - Hacker from an IP in China compromised the most privileged accounts in the Jet Propulsion Laboratory
  - Gained complete network access allowing user to:

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station
- China attacks!
  - Hacker from an IP in China compromised the most privileged accounts in the Jet Propulsion Laboratory
  - Gained complete network access allowing user to:
    1. modify, copy, or delete files

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station
- China attacks!
  - Hacker from an IP in China compromised the most privileged accounts in the Jet Propulsion Laboratory
  - Gained complete network access allowing user to:
    1. modify, copy, or delete files
    2. add, modify, or delete user accounts for mission-critical JPL systems

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station
- China attacks!
  - Hacker from an IP in China compromised the most privileged accounts in the Jet Propulsion Laboratory
  - Gained complete network access allowing user to:
    1. modify, copy, or delete files
    2. add, modify, or delete user accounts for mission-critical JPL systems
    3. upload hacking tools to steal user credentials and compromise other NASA systems

Attacks in 2011

- Stolen laptop containing highly sensitive information including algorithms used to control the International Space Station
- China attacks!
  - Hacker from an IP in China compromised the most privileged accounts in the Jet Propulsion Laboratory
  - Gained complete network access allowing user to:
    1. modify, copy, or delete files
    2. add, modify, or delete user accounts for mission-critical JPL systems
    3. upload hacking tools to steal user credentials and compromise other NASA systems
    4. modify system logs to conceal their actions

Primary Causes/Vulnerabilities

Primary Causes/Vulnerabilities

- Network servers not securely configured exposing:
  - Encryption keys
  - Encrypted passwords
  - User account information

Primary Causes/Vulnerabilities

- Network servers not securely configured exposing:
  - Encryption keys
  - Encrypted passwords
  - User account information
- 24% of Flight Center computers monitored for updates
- Only 62% monitored for vulnerabilities
- Lots of moving parts

Primary Causes/Vulnerabilities

- Network servers not securely configured exposing:
  - Encryption keys
  - Encrypted passwords
  - User account information
- 24% of Flight Center computers monitored for updates
- Only 62% monitored for vulnerabilities
- Lots of moving parts
- 10 computers released with sensitive data still stored on disk
- 1% of all NASA laptops are encrypted

Sources

http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

http://gizmodo.com/5892408/how-secure-are-nasas-servers

http://www.technewsworld.com/story/science/74569.html

http://www.zmescience.com/space/nasa-hacked-06032012/

http://en.wikipedia.org/wiki/Advanced_persistent_threat

Questions?