Jefferson Lab Cyber Security Event

Brent Morris

Andy Kowalski

Winter 2012 ESCC

January 26, 2012 – Baton Rouge, LA

An Advanced Persistent Threat attacked Jefferson Lab

Attack

- Mid April 2011 → attack appears to have been initiated across multiple DOE sites
- May 24 → two externally facing Jefferson Lab webservers compromised
- Five weeks of recon by attackers
- June 28 → escalation of privilege to domain admin (root) on the Windows environment
- June 29/30 early morning → Data exfiltration

Discovery & protection

- June 30 AM→ attack detected; block Internet access to all areas with sensitive information; inform leadership and DOE; launch analysis
- June 30 PM →block everything but incoming traffic and email; enhance monitoring;
- July 1 afternoon → discover PNNL also under attack; block all Internet access except email and limited access to LQCD clusters
- Safety and physical security systems not impacted; most onsite IT systems operational

Analysis and recovery

- July 2 → develop initial understanding of event
- July 2 & 3 → turn a year and a half "shovel ready" project into a 5-8 day activity
- July 3-5 → launch recovery activities
- July 6-15 → external website; guest wireless open to Internet; new Windows "core"; new Certificate Authority; change all passwords; reissue all smartcards; general Internet access online
- July 16-mid August → bring all web services online; provide an external file transfer system

Attacker's goal: science, engineering and technology information

Key Points

- Onsite work continued
- Worked with Business Services to connect to banks, etc. as required
- Used guest network and portable media to retrieve data
- Follow up steps taken:
  - Implemented additional cyber security enhancements during the 6 month construction down
  - Two reviews in August by CSC, plus a self assessment

Lessons Learned

- Firewalls and network segmentation work, but need to segment Windows and authentication
- Email as a stand alone service is a good thing
- Bring up your web server ASAP
  - Good public relations
  - Press considers site up if they can reach a web site
  - DOE considers site up if web and email are up

Questions For Networking

- Should ESnet play a role in protecting the Labs
  - Cyber incident response
  - Network traffic monitoring
- Do labs need dedicated network access to JC3-CIRC and other Labs to conduct forensics
  - Secure exchange of information and for conducting forensics
  - Monitoring help during off-hours
- How do networking and cyber security reach consensus