Security in knowledge

NATION-STATE ATTACKS ON PKI

Phillip Hallam-Baker

Comodo Group Inc.

RSA CONFERENCE 2013

Session ID: **STU-W25B**

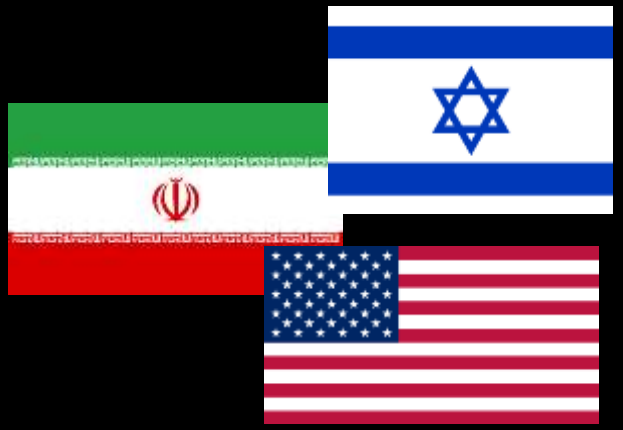
Session Classification: **Studio**

Why are state actors different?

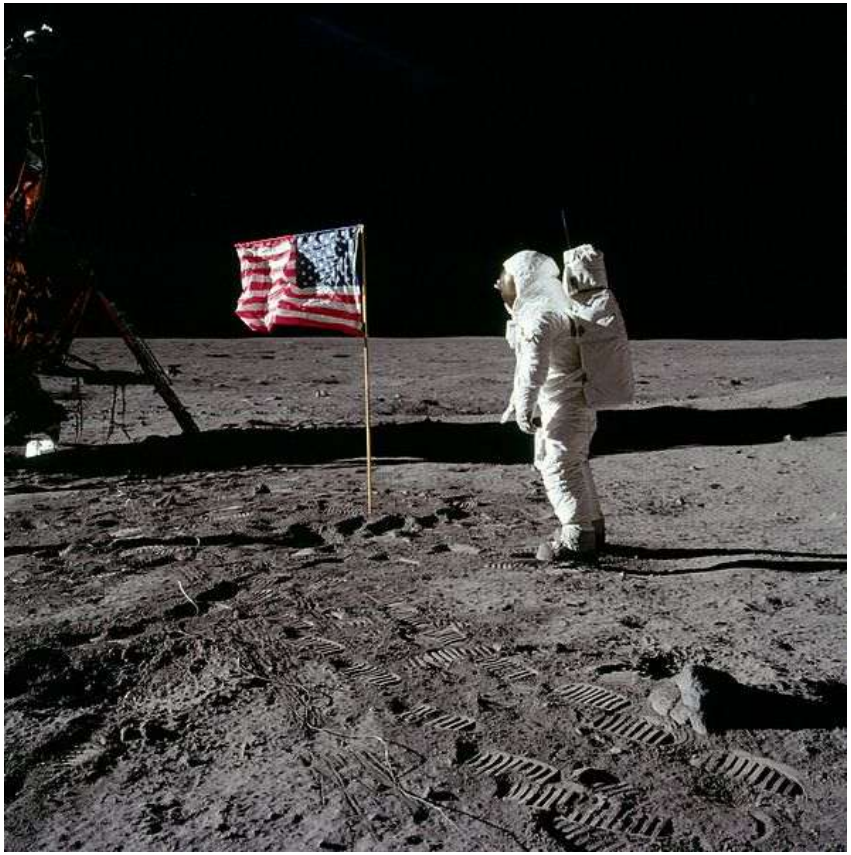
Security in knowledge

Motive


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
100
B
ONE HUNDRED DOLLARS



Capabilities



Targets


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
100
B 96195909 D
ONE HUNDRED DOLLARS


BETONDEMONTAGETE
LOVE & PEACE
IN
EAST & WEST
Test
West

Iran

Security in knowledge

2009 Protests

Media cycle

StuxNet

- Discovered July 2010
  - At least 5 Variants
  - Possibly reduced production of U-235 by 30%
- Used signed code
  - Legitimate code signing certificates
  - Stolen keys
  - Needed to sign driver code
- Estimated to cost > $1 million to write
  - [Raised to >$100 million after Olympic Games disclosure]

2011 Arab Spring

Medium

Comodo Certificate MisIssue

- Reseller Breached March 15 2011
  - Vector unkown
  - Located API used to request certs
  - Requested issue of certs for 7 domains
    - Targeting Social Media sites
- Breach detected March 15 2011
  - Reseller received email saying certificates ready
  - Reseller knew that request had not been made
  - Notified Comodo

Information Gathered

- IP Address from which request launched
  - In Iran
- Requests for cert status
  - Same Iranian address
- Email correspondence from attacker
  - IP address is in Iran
  - Company purports to be Israeli
  - Content cut and pasted from actual Israeli firms

Comodo and Industry Response

- Certificates Revoked
  - But browsers don't check this properly
- All reseller issue authority suspended
- Browser Providers notified
  - *Need to push new browser binaries (!)*
- Responder Notification
  - Certificate Subjects notified
  - FBI
- Public (gated on browser patches)
  - Revealed Iranian connection
  - Accused of being alarmist, distracting attention etc.

Iran mounts PR offensive

- 1) So counted **green movement** people in Iran isn't most of Iran, so when Obama says I'm with Iranian young community, I should say as Iranian young simply I hate you and I'm not with you, at least 90% of youngs in Iran will tell you same thing, it's not my sentence. But you have bad advisors, they report you wrong details, maybe you would think better if you have better advisors.
- 2) To Ashton and others who do their best **to stop Iranian nuclear program**, to **Israel** who send terrorist to my country to **terror my country's nuclear scientist** (http://www.**presstv**.com/detail/153576.html), these type of works would not help you, **you even can't stop me**, there is a lot of more computer scientist in Iran, when you don't hear about our works inside Iran, that's simple, we don't share our findings as there is no use for us about sharing, so don't think Iran is so simple country, behind today's technology, you are far stronger then them, etc.

PR Response

Incident comparison

Comodo

- Reseller breached
- Issue platform secure
- Mis-Issue detected in hours
- Notified browser providers
- Attacker objective failed

- **Still operational**

DigiNotar

- CA breached
- Lost control of Logs, HSM
- Mis-Issue not detected
- Discovered by targets
- Attacker succeeded

- **Liquidated**

Conclusions

Security in knowledge

Lessons learned

- State Actors matter
  - Money isn't the motive or even the enabler
  - Different objectives ⇒ different targets
  - Consequences may be life, not property
- Security basics matter
  - Separate perimeter from core
  - Deploy controls to test effectiveness of your controls
  - Security is not a competitive advantage, share your knowledge
- Disclosure matters
  - Notify responders immediately
  - Plan for public disclosure in days