Iran’s Real Life Cyberwar

Phillip Hallam-Baker
Comodo Group Inc.

[Some images from Wikimedia commons]
Be Very Afraid...
The Real Problem
Gwapo's HF Money Making
WANTED
BY U.S. MARSHALS

NOTE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshal Service NCIC entry number: (NCIC N721460021)

NAME: MUTILIK, KEVIN DAVID
AKS-ID: MUTILIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: MALE
Race: WHITE
Place of Birth: VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: 5'11"
Weight: 190
Eyes: BLUE
Hair: BROWN
Skin Color: LIGHT
Scar, Marks, Tatoo: NONE KNOWN
Social Security Number (if): 550-39-5695
NCIC Fingerprint Classification: DOPM40012E10M199M09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C
DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-3316)
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone: 800-374-3538 (24 hour telephone contact) NLETS access code is VAUSM0000.

November 1992
THE CUCKOO'S EGG

Clifford Stoll

Tracking a Spy Through the Maze of Computer Espionage
What Has Changed?
Motive
Capabilities
Targets
19th August 1953
4th November 1979
Immediate Director Int. PRIORITY TEKAN, TOYO, BANGKOK.

RE: M-1125-Z/S/P STAFF

Hong Kong, June 29

Immediate Director Int.

In the GADJA Intel.

A. Director SPS 138

B. Tokyo, O.S. 63

I regret the confusion on location. The place name in the map as subject report indicated area to be avoided by ground troops is subject classified. See that ground assault is not to be confused with the ground force instruction to take place north of the river. Most of the troops are in the river

End

[Signature]
2009 Protests
Media cycle
8th April 2011
Medium
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
Comodo Certificate Mis-Issue

• Reseller Breached March 15 2011
  – Vector unkown
  – Located API used to request certs
  – Requested issue of certs for 7 domains

• Breach detected March 15 2011
  – Reseller received email saying certificates ready
  – Reseller knew that request had not been made
  – Notified Comodo
Immediate Response

• Certificates Revoked
  – But browsers don’t check this properly
• Browser Providers notified
  – Development of patches begun
• Certificate Subjects notified
• All reseller issue authority suspended
• FBI notified
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
Disclosure

• Testing browser patches takes time
  – One requires 8 days
• Jacob Appelbaum discovers new CRL entries
  – Agrees not to disclose until patches complete
• Public Announcement 28\textsuperscript{th} March
  – Reveals Iranian connection
  – Response: “You are just saying that to cover up”
Pastebin Spin:

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](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.
Response
Consequences
Action

- Browsers agree to enable faster response
- Sharing of data on attacks amongst CAs
- Resellers
DigiNotar Breach

• Total Compromise
  – Lost control of signing unit (but not the key)
  – Machines with the audit logs
  – Unknown number of certificates issued

• Detected
  – Not reported

• CA liquidated
  – Public trust anchors (roots) revoked
But they had an audit!
Flame
Collateral Damage
Cryptanalysis of MD5

• Sophisticated
• Novel
“Olympic Games”
Situation Today

You are here

[Images of flags: United States, Israel, Iran]
Changing the Infrastructure

- Perspectives, Convergence
- Sovereign Keys
- Certificate Transparency
The Problem

User

Browser

Server

CA
Conclusions

• It isn’t about the money
  – Can’t defend by making attacks uneconomic

• State actors are now a threat
  – May be hit by either side
  – Motives likely political, *not* national security

• Work on reinforcing the trust infrastructure
  – Will take time

• Have a response plan