Topic 6: the Way of the Ninja

Social Engineering (II909)

Kaido Kikkas

Hey - ain't that a different art?

- The course is about social engineering…
- …but sometimes the best result will come from combining social skills with some physical ones
  - e.g. to create a pretext of an engineer at a project, one needs the project documentation – which happens to be locked into a drawer

Ninja craft

- *Ninja Hacking* by Thomas Wilhelm and Jason Andress
- A surprisingly good take in adapting several aspects of medieval Japanese ninjutsu to modern times, including
  - exploitation of current events
  - disguise and impersonation
  - infiltration (timing, weak points, distraction)
  - tools (entry, concealment, covert listening)

Using current events

- Water cooler politics: especially effective in difficult/ hectic times (economic low, layoffs, mergers etc); finding pretexts vs direct manipulation (playing on fears and curiosity)
- Attack vectors
  - generic or spear phishing
  - “poisoned” ads (via search engines)
  - fan/hate sites or blogs

Disguise

- Once upon a time, in the Land of Rising Sun…
- Hensōjutsu (art of disguise), *Gisojutsu* (art of impersonation) and *Shichi ho de* (7 ways of going):
  - *akindo* (merchant or tradesman)
  - *hokashi* (musician)
  - *komuso* (itinerant priest)
  - *sarugaku* (entertainer, showman)
  - *shukke* (Buddhist monk)
  - *tsunegata* or *rōnin* (wandering samurai for hire)
  - *yamabushi* (mountain warrior ascetic)

Necessary skillset

- *Hengen kasha no jutsu* (immersion in the illusion):
  - Appearance
  - Knowledge
  - Language
  - Geography
  - Psychology

A little task

- Meanwhile, in another time and place…
- What could be the counterpart of *Shichi ho de* in the West today?

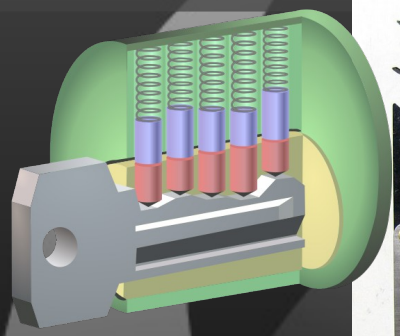
...

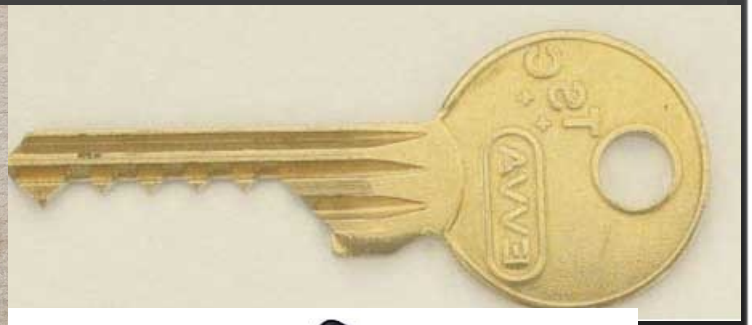
- Stephen K. Hayes:
  - Scholastic
  - Business
  - Rural
  - Religious
  - Public figures
  - Labor
  - Uniformed

...

- My take:
  - Professional (lawyer, doctor, businessperson)
  - Government official/clerk
  - Emergency worker (rescue/medic/police/security)
  - Media person (journalist, writer, TV host)
  - Student/intern
  - Support staff (technician, repairman, driver, janitor)
  - Delivery (courier, pizzaboy)

Infiltration: lockpicking





https://en.wikipedia.org/wiki/Pin_tumbler_lock#/media/File:Pin_tumbler_with_key.svg
https://en.wikipedia.org/wiki/Lock_picking#/media/File:Lockpicking-Set.jpg
https://en.wikipedia.org/wiki/Lock_picking#/media/File:Padlock_Skeleton_Keys.jpg
https://en.wikipedia.org/wiki/Lock_picking#/media/File:Bumping_key.jpg
https://en.wikipedia.org/wiki/Lock_picking#/media/File:Snap_gun.jpg

Infiltration: alarms and cameras

- False positives
- Impersonation (Tom Cruise in MI:2)
- *Metsubishi* (sight removing) – works on both guards and cameras; the latter can be physical (blinding) or networked (DDoS on control systems)

Infiltration: timing

- Daily routines
- Weak points in environment (slow doors)
- Maintenance times (repairs, upgrades)
- Tailgating
  - Two tested pretexts: smoking and fake injuries
  - Also possible in cyber-forms (session hijack, logging in at high-traffic times etc)

Infiltration: weak points in infra

- Dumpster diving
- Surplus/discarded hardware
- Cyber-versions: phishing, Google hacking

SE, ninja style

Five elements	Five weaknesses	Five needs
Earth (chi) - stable	laziness	security
Water (sui) - emotional	anger	sex
Fire (ka) - agressive	fear	wealth
Wind (fu) – wise, kind	sympathy	pride
Void (ku) - creative	vanity	pleasure

Distractions

- Large events
  - holidays and festivals
  - sporting events
  - business/company events
- Natural events (force majeure – fires, floods, outages)
- Panic rousers (fake news, identity theft etc)
- Malware

Surveillance and communication

- Smartphones – 2 cameras, mic, GPS
- Burner (throwaway) phones – either physical or app-simulated (https://www.burnerapp.com)
- Wearables (http://www.spyshops.ca/ButtonCamera.html, http://www.spyshops.ca/PenCam&MonitorDVR.html etc)
- GPS tracking devices

Some software for checking out

- Obligatory disclaimer: these are purely for reference :D
  - Maltego
  - Metasploit
  - SET (Social Engineer's Toolkit)

- NB! Most of those are readily available in Kali Linux

Conclusion

- While SE is mostly about humans, various tools can be handy
- Equally high and low tech
- “There is no problem that cannot be solved with a proper amount of high explosive” (on a bomb squad car)
- (and although pirates might be cooler than ninjas, the latter are way better social engineers)

Thanks!

- Next time, examples and cases