VeriSign®

Incident Response to Social Engineering Attacks: Domain Hijacking

Ramses Martinez
Director of Information Security
Date: June 22, 2010

Where it all comes together.™

Background

More and more attacks are exploiting business logic using social engineering attacks.

- Low tech in nature
- Leverage existing processes or systems
- Target the weakest link in the security stack, the human

Why?

- Social Engineering attacks are difficult to detect and guard against
- Training helps, but is not the only solution

Incident Response Process

1. Preparation
2. Detection
3. Containment
4. Eradication
5. Recovery
6. Follow Up

Incident Overview

Not so much a domain hijacking as an attempt to hijack a Registrar

Normally the registrant is the target, in this case the primary target were the registrars and registries.

Initial scope

- Two registrars
- Final objective:
  - Control of registrars registry account

Case Study

Target:

- Registry account for two large registrars, this could have placed hundreds of thousands, if not millions of domains under the control of the attacker

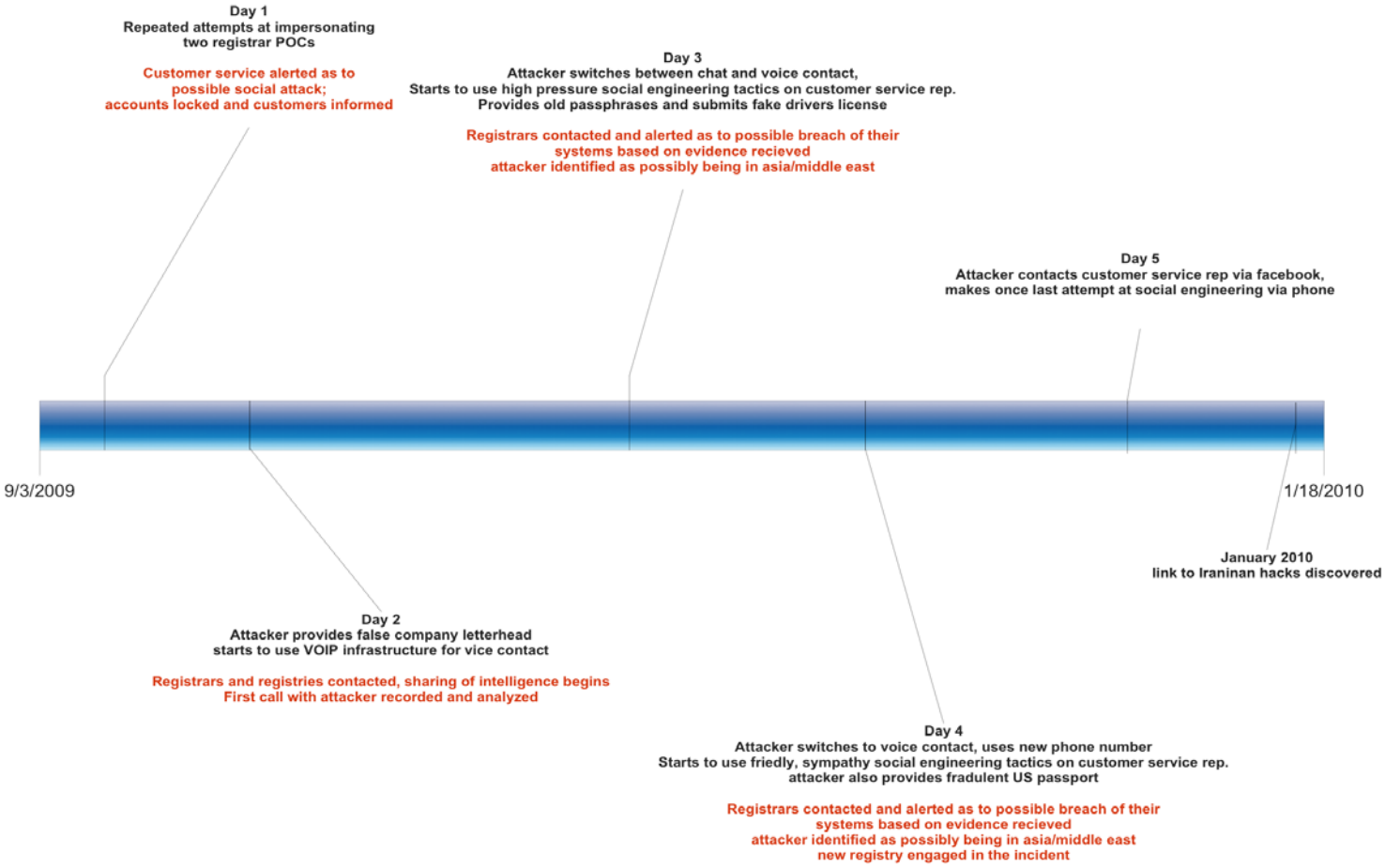
Duration: 5 days

Highlights:

- Attacker engaged multiple times in the course of attack
- Multiple false documents provided:
  - Fake company letter head
  - Fake US passport
- Attacker used multiple means of communication with customer service representatives:
  - Online Chat
  - Phone
  - Email
  - Social networks

- Great example of industry collaboration on a security issue
- Connection to nation state sponsored attacks

Attack Chronology



The Attack in Summary

Final scope of attack

- Two registrars, three registries targeted
- Objective believed to be control of registrars registry account, not just a simple domain hijacking
- Believed to be linked to the Iranian governments attack against dissident protesters

Analysis of attack (not performed by an amateur)

- Knew the process for the registry transactions in detail
  - How to contact: Where to call, chat, etc.
  - What credentials would be needed for the changes requested
  - What proof of identity would be requested by the registry
  - Name and types of applications used for transactions
  - Created hard to trace infrastructure for the attack:
    - Compromised systems
    - VoiP lines

The Attack in Summary

- Attacker had in-depth knowledge of process business processes at registrar and registry
  - Names of all points of contact
  - Points of contact location, time zone
  - Pictures of points of contacts
  - Obtained fraudulent credentials for points of contact

Attacker profile (joint research conducted with registrars and registries affected)

- Iranian male in his late twenties/early thirties involved in domain attacks since 2007 (confirmed) unconfirmed as far back as 2005.
- Initially involved in unauthorized domain reselling, briefly ran a fake registrar, attempted and successfully conducted several domain hijacks
- Involved in several system and account compromises in the last three years.
- Has been known to threaten and conduct defamation campaigns against his targets.
- Well known for the intricacy of his attacks and doing heavy reconnaissance of his targets prior to the attack.

Lessons Learned: Preparation Phase

1. Train, train.. then train some more
2. Test your people, conduct social engineering penetration tests
3. Spend time with the business, got to know it
4. Build trust and communication with all stakeholders

Information security is as much about personal relationships as it is about dealing with attacks

Lessons Learned: Detection

Fraudulent Documentation

- Parts of the text appear in different font type and size, indicating that the document has been altered
- Spelling errors
- Photographs on ID documents are scanned
- Discrepancies in the information (e.g. Date of Birth appears differently in different places on doc)
- A portion of the document has been visibly altered or obliterated (excluding phone numbers on telephone bills that have been removed for privacy purposes)
- Signature on the document does not match the printed name.
- The signature on the document has been disguised and it is not legible

Lessons Learned: Detection

Behavioral

Verbal:

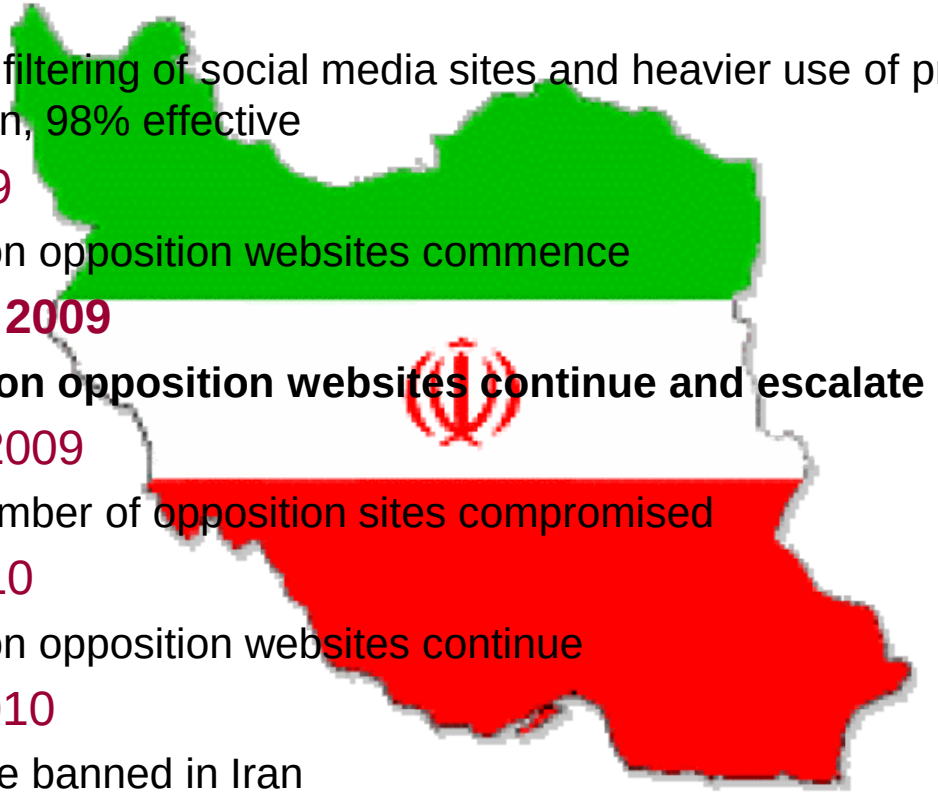
- Aggressive behavior such as shouting, constant interrupting, abusive language
- Name ‘dropping’

Written:

- Excessive use of capital letters
- Claiming that their order is extremely urgent
- Frequent references to the incompetence of staff
- References to payment and demanding that their money be refunded

The Iranian Connection: Chronology of Iranian attacks

- June 2009
  - Initial response to twitter and Facebook postings with filtering
- July 2009
  - Stronger filtering of social media sites and heavier use of proxies by opposition, 98% effective
- August 2009
  - Attacks on opposition websites commence
- **September 2009**
  - **Attacks on opposition websites continue and escalate**
- November 2009
  - Large number of opposition sites compromised
- January 2010
  - Attacks on opposition websites continue
- February 2010
  - Gmail use banned in Iran
  - Large number of opposition sites attacked and compromised



The Iranian Connection

+ The attacker against registry is identified as Omid J.
  - Facebook account
  - Previous attack data
  - Attack data f sition sites
    - Application
    - OS and web
    - Domain hijac

The attacks appear to have ucted by an entity affiliated with the Iranian gov t to compromise the infrastructure of their opposition.

Conclusion

- The human being is the most important aspect of the security process
- Defenses against social engineering attacks are hard to build, even harder to measure
- The same tried and true methods are being used for these type of attacks, only the level of complexity, the size of the targets and the tenacity of the attacks seems to be increasing.
- The true intent of an attack may not be obvious, at least not initially

VeriSign®

Thank You
Q & A

Where it all comes together.™