nccgroup
freedom from doubt

Dissecting Social Engineering Attacks

Robert Ray, Security Consultant, CHECK Team Member

Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

"A trend reported during the first half of 2012 is the increase of targeted attacks. These attacks need time (in some cases a few years) to be detected and are rather hard to avoid."

"Spearphishing and social engineering techniques are on the rise."

"Spearphishing is increasing, mainly due to the increased use of social networking for private and business purposes."

enisa
European Network and Information Security Agency

ENISA Threat Landscape report 2013

Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

"Loss or theft of mobile devices and other equipment by staff is a major internal threat for organisations.

Loss or theft of mobile devices and hardware are a major external threat for corporations."

"Corporations having experienced a data breach reported that one of top 3 causes is physical theft of devices containing sensitive data."

enisa
European Network and Information Security Agency

ENISA Threat Landscape report 2013

Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

January 25, 2010 11:47 pm

Hackers target friends of Google workers

By Joseph Menn in San Francisco

Personal friends of employees at Google, Adobe and other companies were targeted by hackers in a string of recently disclosed cyberattacks, raising privacy concerns and pointing to a highly sophisticated operation, security experts said.

Cybersecurity experts analysing the attacks said the hackers spied on individuals and used other sophisticated techniques, making them extremely difficult to stop. The disclosures come amid renewed alarm over cybersecurity after Google said it had been the target of a series of cyberattacks from China.

More

ON THIS STORY

Cyberattack threat to US groups

In depth Google vs China

The most significant discovery is that the attackers had selected employees at the companies with access to proprietary data, then learnt who their friends were. The hackers compromised the social network accounts of those friends, hoping to enhance the probability that their final targets would click on the links they sent.

Agenda

- **Social engineering attack methodology**
- **Dissecting a social engineer**
- **Dissecting social engineering attacks**
- **Demonstration of some tools of the trade**
- **Prevention and mitigation advice**

Social engineering methodology

Social engineering methodology

- **Information Gathering**
  - Corporate & personal websites, blogs etc.
  - Document metadata
  - Search engines
  - Whois & domain registration records
  - DNS records
  - Social media
  - Public records

Social engineering methodology

- **Reconnaissance**
  - Google Street View
  - Google Maps – Satellite View
  - Physical walk or driveby
  - Telephone reconnaissance
  - Rubbish bins (A.K.A dumpster diving)

Social engineering methodology

- **Reconnaissance**
  - CCTV location, security guards, door entry systems etc
  - Unprotected entrances, fire exits, unmanned receptions etc.
  - Weak entry points such as open windows (usually out of scope for breach)
  - Times of busy or quiet periods, lunch breaks etc.
  - Location of smoking areas, car parking etc.
  - Surveillance will be mostly covert. Taking pictures of buildings, staff ID badges, delivery points etc.

Social engineering methodology

- **Reconnaissance**

Social engineering methodology

- **Breach**
  - Deemed successful by reaching a set of pre-defined agreed goals
    - Gain network access (level of attack to be agreed)
    - Work at a staff unattended desk
    - Install a rogue access point
    - Remove specific equipment
    - Make external calls from office equipment
    - Reach sensitive areas of the building, server room, mail room etc.
    - Phish credentials or perform client exploits

Social engineering methodology

- **Post Breach**
  - Verbal debrief
  - Detailed Report
    - Detailed analysis of what we gained
    - How we gained it
    - Why it helped us
    - What we used it for
    - Which goals did we achieve
    - Our recommendations for mitigation

Dissecting a social engineer

- So who are the social engineers?

Dissecting a social engineer

nccgroup
freedom from doubt

Dissecting a social engineer

nccgroup
freedom from doubt

Dissecting a social engineer

nccgroup
freedom from doubt

Dissecting a social engineer

nccgroup
freedom from doubt

Dissecting a social engineer

- **Key Characteristics**
  - Great research skills for building solid pretexts
  - Great at building instant rapport
  - Great communication skills to allow elicitation of useful or sensitive information
  - Great at adopting another role or persona
  - Very persuasive
  - Very adaptable
  - May be a technical specialist or at least working with technical specialists

Social engineering attacks

Social engineering attacks

- **A note on scoping simulated attacks**
  - Social engineering engagements are usually very carefully scoped
  - Decisions on what types of attacks are in scope
  - Decisions on which targets are allowed to be attacked, employees, offices, buildings and so on.
  - Goals to determine a successful breach to be defined
  - Any specific items out of scope clearly defined within rules of engagement such as forcing open doors or using particular fire exits due to alarms.

Social engineering attacks

- **Client Side Attacks**
  - Exploiting browser related vulnerabilities
  - Phishing for credentials
  - Malicious attachments
  - Instructing users to install or run malicious software
  - Malicious USB sticks etc.
  - Screenshot evidence of successful attacks

Social engineering attacks

- **Physical Intrusions**
  - Unprotected entrances, fire exits, unmanned receptions etc.
  - Gain entry under pretext situation, i.e. electricity meter reader, health and safety officer, important client etc.
  - Tailgating staff
  - Use of fake ID badges or uniforms etc.
  - Use of obtained door entry fobs or access cards
  - Photos taken to record goals reached.

Social engineering attacks

- **Telephone Attacks**
  - Eliciting useful information, i.e. internal building layout, names or job titles of staff, additional telephone numbers for further attacks etc.
  - Calls into organisation under relevant pretext, i.e. impersonate staff member calling IT helpdesk for password reset or setup a site visit.
  - Off-site wingman, providing off-site standby cover should the need arise. i.e. to provide confirmation of the legitimacy of a pretext

Social engineering attacks

- **Shaun Jones of NCC, kindly provided us with a recent real world example:**

Social engineering attacks

Attack Objectives

- Gain physical access to customer premises and gain access to corporate network
- Test customer user's susceptibility to phishing attacks

Attack Plan

- Steal user credentials
    - Launch a phishing attack against Outlook Web Access
- Use compromised accounts to allow for physical breach
    - Create a pretext to gain access to building
    - Obtain physical passes and door entry fobs
    - Gain access to internal network point
    - Log into systems with stolen credentials

Social engineering attacks

nccgroup
freedom from doubt

Outlook migration

support@[redacted]

Sent: Tue 22/04/2014 14:17

To: Shaun Jones

All,

As part of [redacted]'s migration to a new IT infrastructure we request that all users confirm that they are able to login to the email portal by 29/04/2014. Any accounts that have been dormant for over 2 months will be disabled.

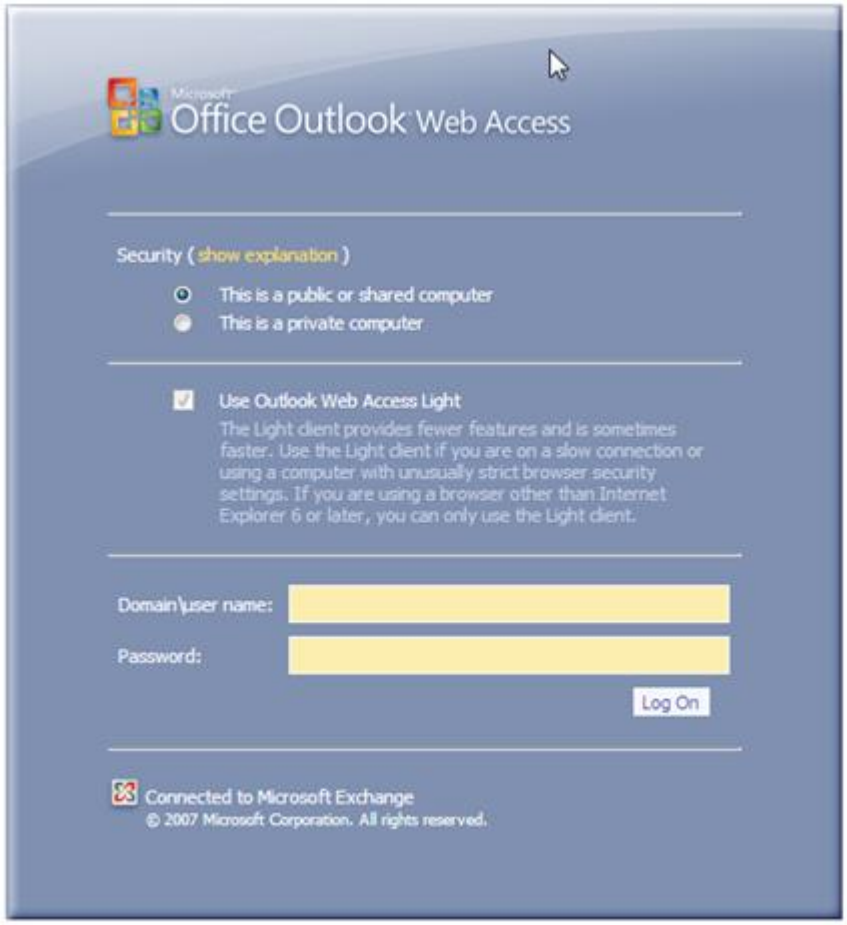
Go to http://[redacted]/owa/auth/logon.aspx?logon=[redacted] and enter your username and password. These will be the same as your regular Windows credentials.

Thanks in advance for your assistance regarding this matter.
Kind Regards,

IT Helpdesk

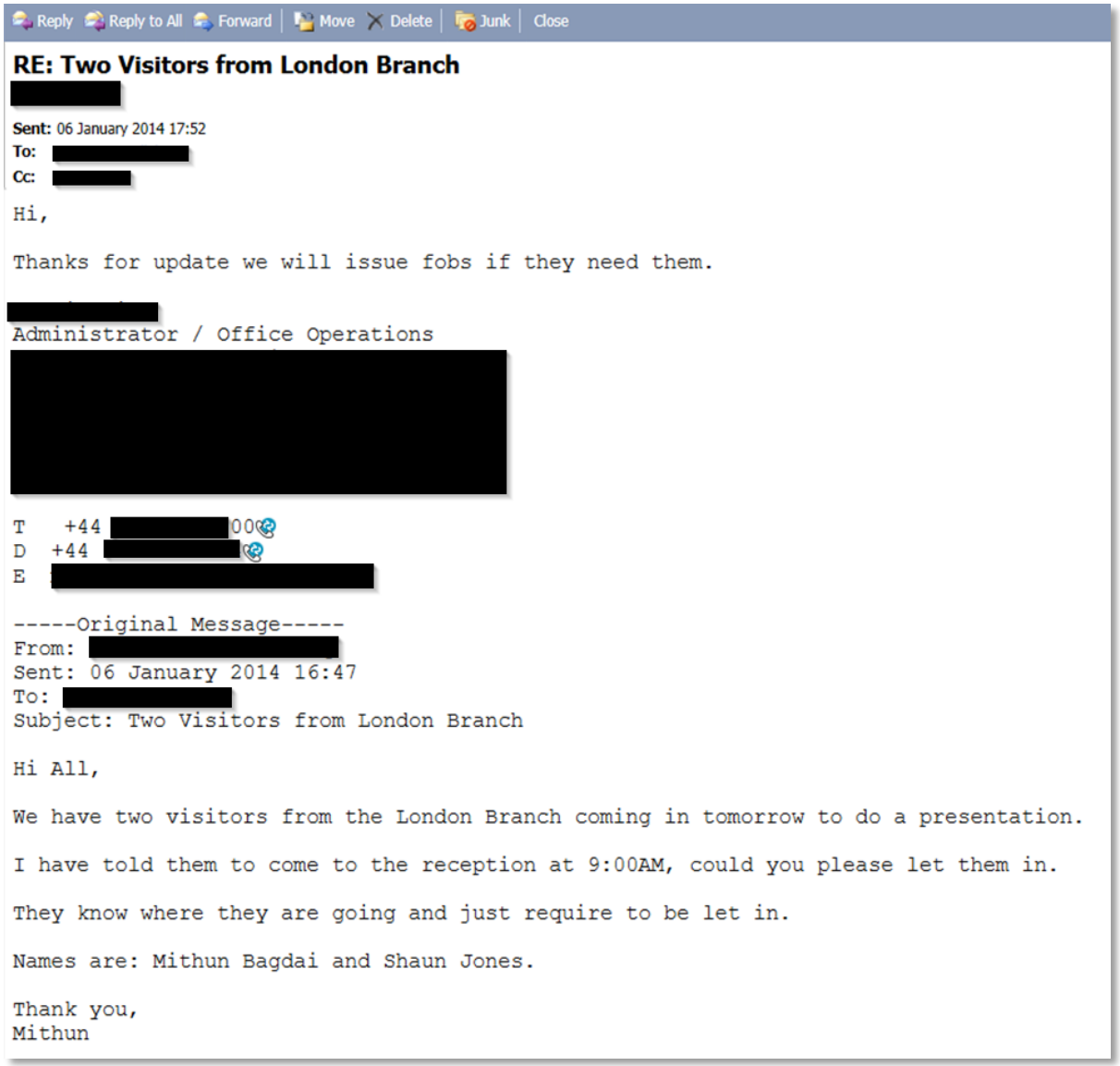
Social engineering attacks

nccgroup
freedom from doubt



Social engineering attacks

nccgroup
freedom from doubt



Reply | Reply to All | Forward | Move | Delete | Junk | Close

RE: Two Visitors from London Branch

[redacted]

Sent: 06 January 2014 17:52
To: [redacted]
Cc: [redacted]

Hi,

Thanks for update we will issue fobs if they need them.

[redacted]
Administrator / Office Operations
[redacted]

T +44 [redacted]00
D +44 [redacted]
E [redacted]

-----Original Message-----
From: [redacted]
Sent: 06 January 2014 16:47
To: [redacted]
Subject: Two Visitors from London Branch

Hi All,

We have two visitors from the London Branch coming in tomorrow to do a presentation.

I have told them to come to the reception at 9:00AM, could you please let them in.

They know where they are going and just require to be let in.

Names are: Mithun Bagdai and Shaun Jones.

Thank you,
Mithun

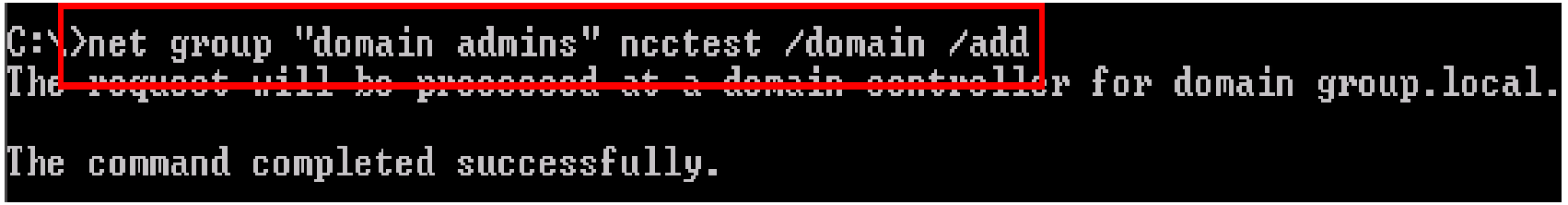
Social engineering attacks

nccgroup
freedom from doubt

Social engineering attacks

nccgroup
freedom from doubt

Social engineering attacks



Dissecting Social Engineering Attacks

nccgroup
freedom from doubt

- **Data Protection Act**
  - Guiding Principle 7 – Information Security
  - Design and organise security to fit the nature of personal data you hold and the harm that may result from a breach
  - Be clear who is responsible for ensuring information security
  - **Make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well trained staff**
  - Be ready to respond to any breach of security swiftly and effectively

Prevention and Mitigation Advice

Adopt a security culture from the top down

- Top down leadership is vital
- Everyone has to be encouraged to be security conscious

Ensure security policies and procedures include cover for social engineering vectors

- Implement & enforce clear desk policies
- Implement & enforce visible staff ID badges (to be removed outwith buildings)
- Report detected social engineering attempts to security officer
- Report mistakes or suspected mistakes to security officer
- Regularly audit policies and procedures
- Regularly assess your controls

Prevention and Mitigation Advice

Training Staff

- Train staff to increase awareness
- Training to include phishing attack techniques, how to spot them, how to handle and report attempts
- Training on physical security, tailgating and social engineering etc.

Assess Staff

- Assess staff through simulated social engineering attacks on a regular basis

nccgroup
freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland