FIRST BASE technologies

Advanced Threat Protection

Lessons from a Red Team Exercise

Peter Wood
Chief Executive Officer
First Base Technologies LLP

Who is Peter Wood?

Worked in computers & electronics for 45 years

Founded First Base in 1989 (the first ethical hackers in UK)

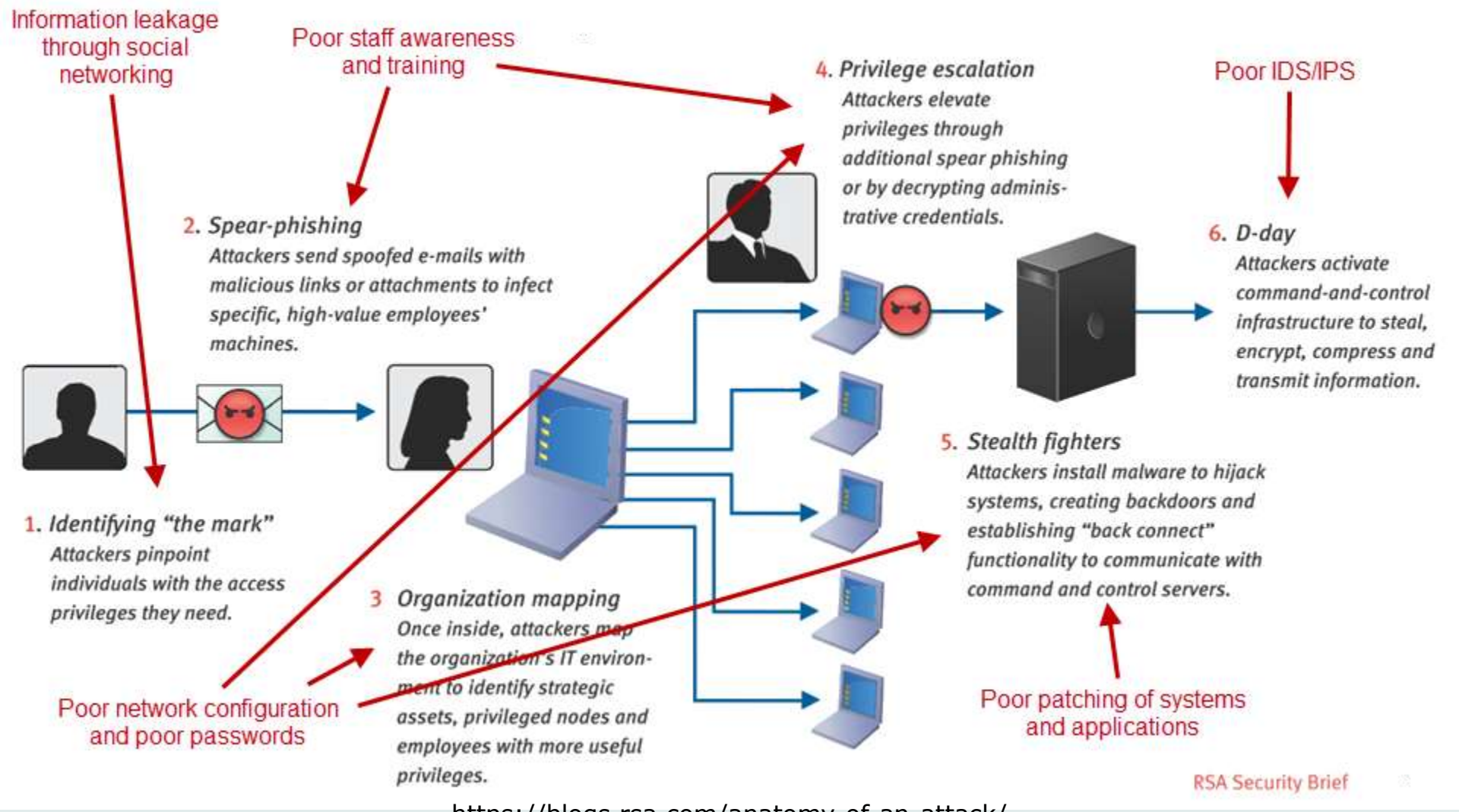
Ethical hacker, security evangelist and public speaker

- Fellow of the BCS, the Chartered Institute for IT
- Chartered IT Professional
- CISSP
- Senior Member of the Information Systems Security Association (ISSA)
- 15 Year+ Member of ISACA, Member of the ISACA Security Advisory Group
- Member of the Institute of Information Security Professionals
- Member of the BCS Register of Security Specialists
- Deputy Chair of the BCS Information Risk Management and Audit Group
- UK Programme Chair for the Corporate Executive Programme
- Member of ACM, IEEE, First Forensic Forum (F3), Institute of Directors
- Member of Mensa

Who are First Base Technologies?

Penetration Testing & Ethical Hacking	Security Consultancy & Awareness
• Web Application Testing	• Risk Assurance
• Infrastructure Testing	• Transformation Consultancy
• Network Security Testing	• Cloud Security
• Server Security Audits	• Architectural Reviews
• SCADA Security Testing	• Awareness Consultancy
• PCI Penetration Testing	• Keynote Seminars
• Endpoint Testing	• Security Evangelism
• Social Engineering	• Multimedia Training
• Red Teaming	• White-hats.co.uk User Group

RSA Advanced Attack (2011)



https://blogs.rsa.com/anatomy-of-an-attack/

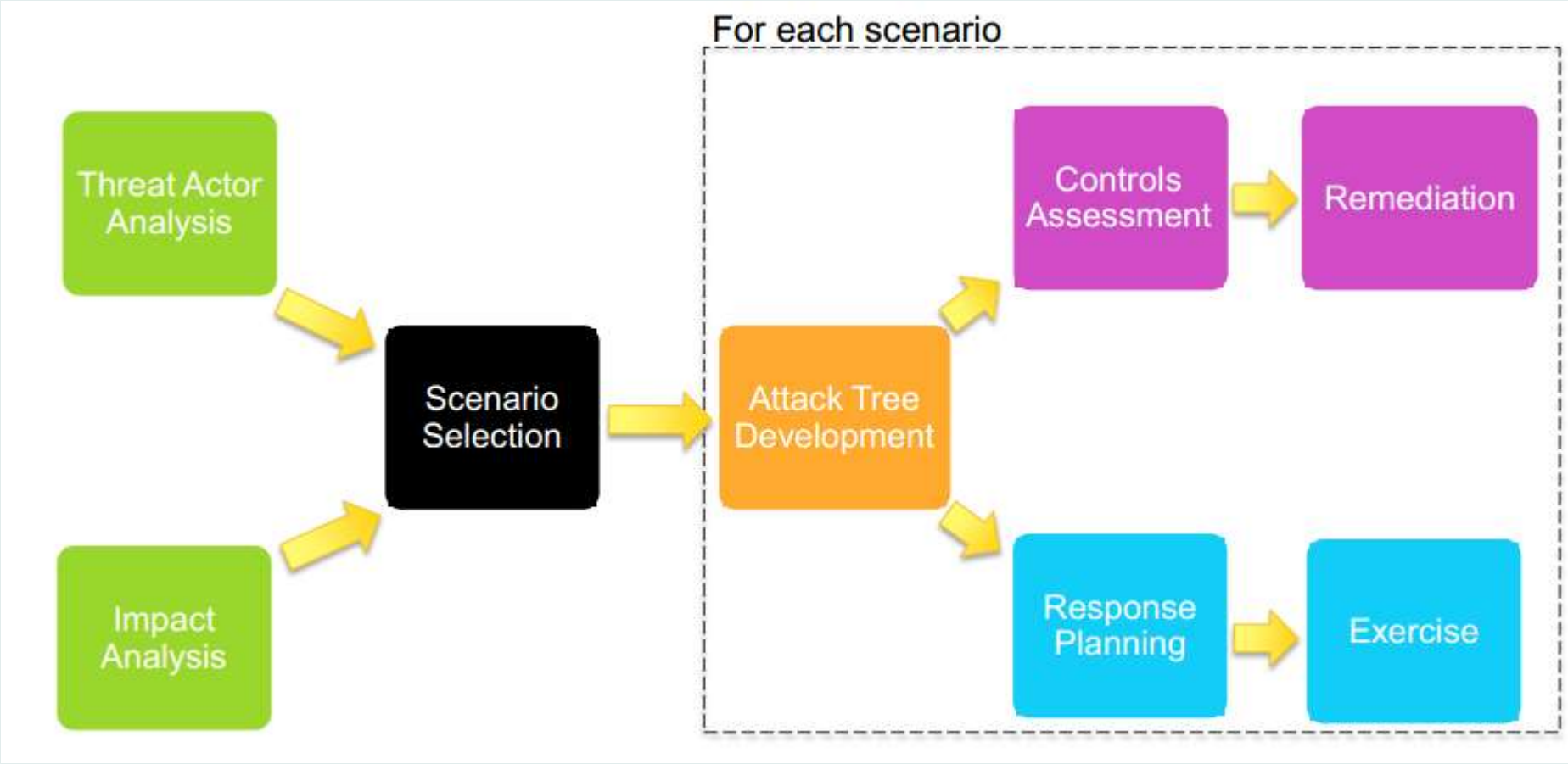
How an Advanced Attack Works

Background Research	Social Engineering	Control Your PC	Explore the Network	Take Control	Find the Data	Steal the Data
• Internet searches • Social networks • Metadata • Phone calls • 192.com	• Spear phishing • USB attacks • Phone calls • Fake staff • Service staff • Visitors	• Malware • Key logging • Physical exploits • Wireless intercepts	• Servers • Desktops • Network devices • Firewalls • Wireless	• Windows admin • Network admin • Business apps • Database	• Strategy • Intellectual property • Marketing plans • HR data • Finance • Salaries	• VPN • Wireless • Email • FTP • Extranet • Physical devices

Red Team Testing

- Use your threat analysis to pick a realistic attack scenario
- Use your asset register to identify realistic targets
- Engage a red team exercise to simulate a real attack
- Check your preventative and detective controls!
- **Learn, improve, repeat!**

Threat analysis for testing



http://csrc.nist.gov/cyberframework/rfi_comments/040813_cba_part2.pdf

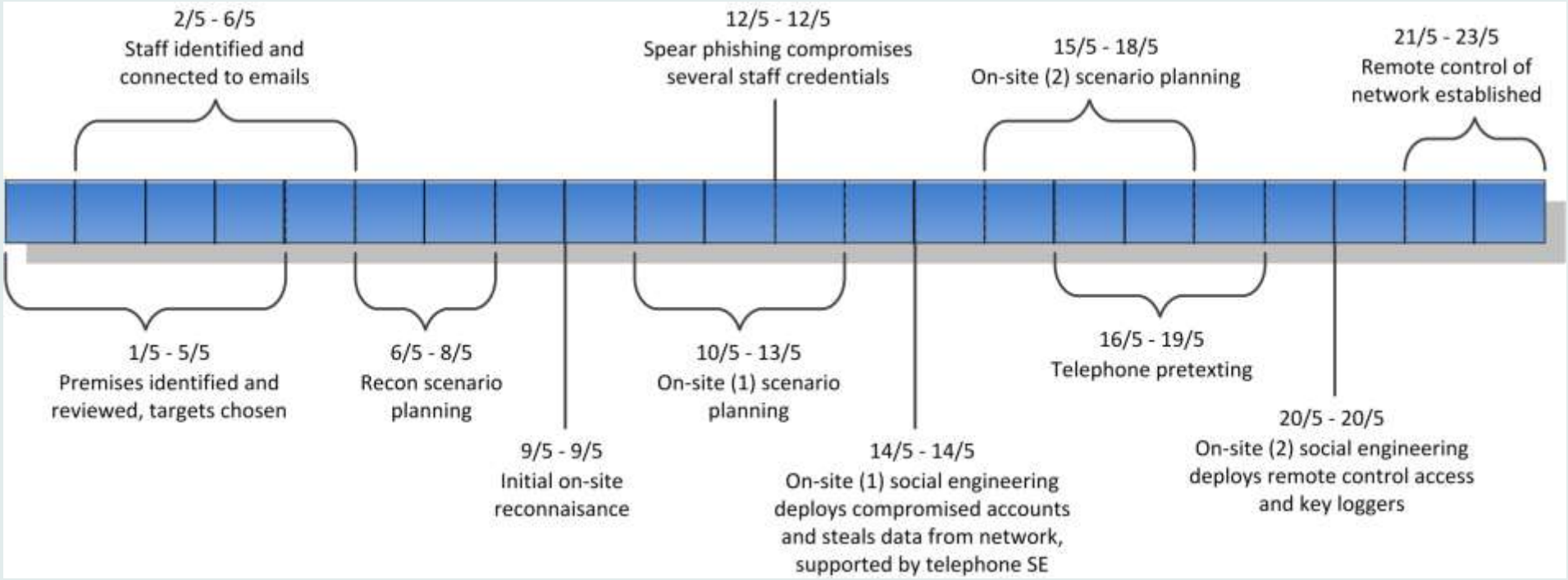
Lessons from a red team exercise

We combined real examples to tell a story

Stories are always more compelling than bald facts!

"The story you are about to hear is true; only the names have been changed to protect the ~~innocent~~ vulnerable."

Our attack timeline



Remote information gathering

- 15 premises in UK, reviewed on Google maps and street view
- 4 registered domains
- 5 IP address ranges
- 72 Internet-facing hosts
- Metadata retrieved for Adobe, Office and QuarkExpress
- Scan revealed OWA in use
- Internet search for relevant email addresses
- LinkedIn searches to construct email addresses for employees
- 400 email addresses identified
- 'Interesting' staff names and job titles from LinkedIn
- Emails sent to obtain responding email style and layout

On-site reconnaissance

- Head office:
  - Perimeter guards and external CCTV
  - Main reception manned and controlled
  - Goods entrance well controlled
  - No other access
  - Staff ID card design noted
  - Results used to plan on-site attack 2
- Branch office:
  - High street premises, no guarding
  - Small reception, one receptionist
  - Door intercom
  - Multi-tenanted building
  - Results used to plan on-site attack 1

Results of info gathering

1. Spear phishing is viable and can be used for theft of credentials
2. Head office will require legitimate appointment to gain physical access
3. Branch office may be vulnerable to ad hoc visitor with remote backup
4. Significant number of other premises available as fallback
5. Windows and Office in use, so typical network vulnerabilities will apply

Spear phishing plan

1. Convincing fake domain name available and purchased
2. OWA site cloned onto fake domain for credential theft
3. Large number of email addresses harvested as targets
4. Design of real emails copied to facilitate spear phishing
5. Names and job titles gathered as fake senders
6. Genuine OWA will be used to test stolen credentials (and gather further info)
7. Credentials will be deployed in first on-site attack

Spear phishing exercise

1. Email sent from IT manager, using fake domain address
2. OWA cloned on to tester's laptop, DNS set accordingly
3. Email sent to three groups of 100 recipients
4. Within a few minutes, 41 recipients entered credentials
5. Credentials tested on legitimate OWA site
6. Significant information gathered from each account
7. Further emails can now be sent from legitimate addresses

Branch office attack plan

1. Team member “Harry” to pose as a contractor working for a telecomms firm
2. Clothing and ID badge prepared
3. Works order fabricated
4. Engineering toolkit prepared, including laptop
5. Credentials obtained from spear phishing stored on laptop
6. Other team members on landline phones for remote verification

Branch office attack exercise (1)

1. "Harry" arrives and tells receptionist he needs to fix a network fault
2. Receptionist asks for a contact name for verification
3. Harry claims not to know and gives receptionist his works order number and a phone number to get details
4. Receptionist calls and speaks to "George" who gives the name of an IT employee (who we know is 'out of office')
5. Receptionist cannot make contact with absent IT employee, so tells Harry to call their IT Manager to resolve the problem
6. Harry calls "Charlie" and asks him to impersonate the IT Manager
7. Charlie (impersonating the IT Manager) calls receptionist and tells them to give Harry access

Branch office attack exercise (2)

9. Harry is escorted into the office and given a desk and a network point
10. He is left unsupervised and plugs his laptop in to the network
11. He explores the network and identifies several Windows servers
12. He authenticates to a domain controller using credentials obtained during the phishing exercise
13. He explores various servers and identifies many interesting files
14. He plants several files to demonstrate full read-write access
15. He explains that he has run diagnostics and that the network connection seems ok. He is escorted to reception and signs out

Head office attack plan (1)

A number of scenarios were considered:

- Apply for a job vacancy with a suitable fake CV
- Courier delivery of a parcel
- Research and interview for newspaper or publication
- Discussion about a school tour of premises
- Tour of premises as a prospective customer

Two alternatives were selected and developed:

- Tour of premises as a prospective customer for a specific product
- Interview for a charity magazine about corporate fund raising

Head office attack plan (2)

Relevant domain names were obtained, email addresses and web pages created for both fake organisations.

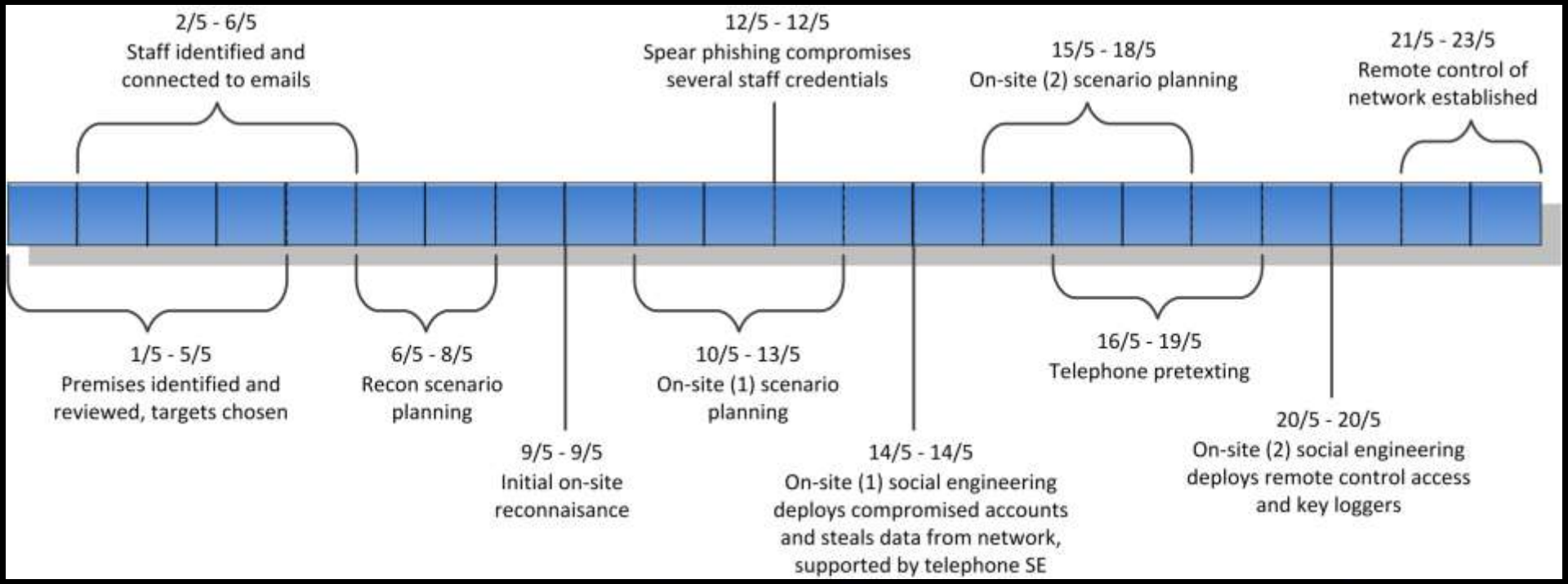
1. Tour of premises as a prospective customer for a specific product:
   - "Anne" sent an email via the company's online form
   - An exchange of emails occurred over the next few days and she obtained permission, as a new customer, to book a tour of the premises
2. Interview for a charity magazine about corporate fund raising:
   - "Anne" called the company and spoke to head of fund raising team
   - Press office called Anne and asked for more details
   - Background research proved convincing and pretext was accepted
   - Interview booked at head office

Option 2 entailed less risk of exposure, so was attempted first.

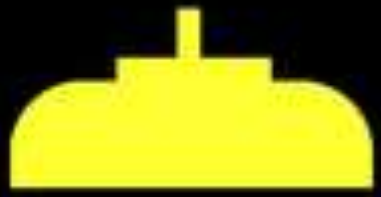
Head office attack exercise

1. "Anne" and "Harry" arrive for the press interview, are given visitor passes and escorted to a meeting room
2. Harry asks to use the bathroom and is given directions
3. A senior employee joins the meeting and asks further questions to validate their story, which are answered satisfactorily
4. Harry returns from the bathroom, but quickly exits the meeting again leaving a pack of diarrhoea medicine on the table
5. During his 'bathroom visit' Harry is able to access unattended computers, simulate installing keyloggers and remote control software and copying files on to a USB drive
6. When the interview concludes, Anne and Harry are escorted from the building

GAME OVER



LIVES 0



Lessons

1. No checks on social networking using work email addresses
2. No sanitisation of metadata in published documents
3. Insufficient staff training on spear phishing
4. Inadequate visitor validation at branch office
5. Unsupervised visitor at branch office
6. Unsupervised visitor at head office (bathroom break)
7. Unlocked computers
8. No challenging of unescorted visitors
9. Sensitive information protected only by Windows credentials

Red Team Testing

- Use your threat analysis to pick a realistic attack scenario
- Use your asset register to identify realistic targets
- Engage a red team exercise to simulate a real attack
- Check your preventative and detective controls!
- **Learn, improve, repeat!**

FIRST BASE technologies

Need more information?

peter@firstbase.co.uk

http://firstbase.co.uk
http://white-hats.co.uk
http://peterwood.com

Twitter: @peterwoodx

Peter Wood

Chief Executive Officer

First Base Technologies LLP