Ferrier Hodgson

Ferrier Hodgson

Introduction – Who Am I

- Stared working in Data Recovery and Data Conversion in 1992 with Doctor Disk.
- Begun working in Computer Forensics in 1998 with Forensic Data Services.
- Worked for Deloitte and Ernst and Young in their forensic and eDiscovery divisions for a number of years.
- Original Ruxcon crew (Did the 1st talk at the 1st rux in 2003).
- Now a Manager with Ferrier Hodgson Forensic IT.

Ferrier Hodgson

Computer Forensic Tools – A Brief History

Direct Disk and Binary/Hex editors

- Nortons Disk Edit
- Winhex
- Acronis
- Media Tools
- Linux Binary Editors\Custom Recovery Tools

Capabilities

- Direct Disk Access
- Media data surface analysis in hex.
- File system analysis (Partition tables, FAT tables, MFT).
- Simple keyword searching (no indexing).
- Data recovery and extraction (File system repair, simple carving)

Ferrier Hodgson

Computer Forensic Tools – A Brief History

Dedicated Forensic Analysis tools.

- Encase (Expert Witness)
- Forensic Tool Kit (FTK)
- Xways (Winhex)
- FEX – Forensic Explorer (Just released)

Capabilities

- Media data surface analysis in hex.
- File system analysis.
- Artefact Analysis.
- Compound file support.
- Advanced keyword searching (indexing in FTK, bookmarks).
- File viewers.
- Galley Viewer
- Data Carving, Data recovery.
- Advanced Scripting (Enscript)
- Advanced categorisation (FTK)

Ferrier Hodgson

Computer Forensic Tools – A Brief History

Advanced File Analysis and legal review.

- NUIX
- Intella
- Legal review platforms (Relativity, Ringtail, EDT)

Capabilities

- Advanced meta data extraction.
- Compound file support.
- Advanced keyword searching (Complex Queries).
- Text Analytics, Visual Analytics.
- File format support.
- Data Carving, Data recovery.
- Advanced Scripting (Nuix).
- Advanced legal review functionality

Computer Forensic Tools – A Brief History

Artefact Analysis and Timeline Generation.

(Point and Click scriptkiddy forensics?)

- Log2timeline
- Internet Evidence Finder
- Various individual tools, scripts, parsers.

Capabilities

- Individual Artefact analysis modules
- Visual Timeline generation (IEF)
- Non-standard artefact modules
- Centralised reporting
- Expanding support for new analysis techniques (Shellbags, Cloud storage)
- Data offsets, contextual data provided.

Ferrier Hodgson

Forensic Artefacts –Time Line Analysis

File System
- MTF, File Entries, FAT, Log, Journal

Registry
- MU lists, USB Analysis, Proprietary software entries

Link Files
- Recent Files, Most Used, Shortcuts

Jump Lists
- Recent Files, Most Used, Shortcuts

Internet History
- Searches, Web history, Recent files, Webmail, Cloud

Email
- Sent, Received, Recipient Lists, address books, calendar, Web mail

Instant messenger
- Discussions, files sent, system access

System Restore Points
- Registry Backups, File backs, Links files etc

Prefetch
- Software Access

Shell Bags
- File access, Software Access

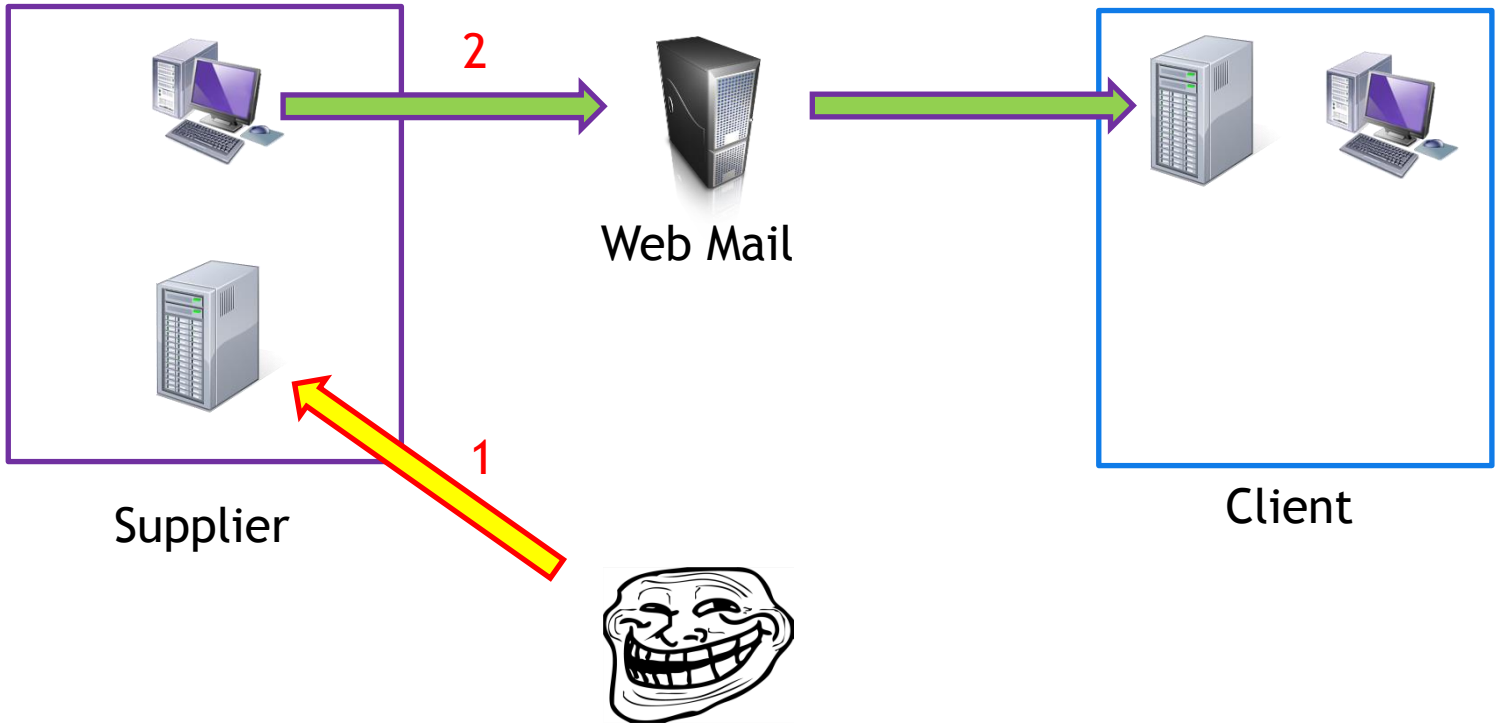
Ferrier Hodgson

Time Line Case Study – Online Fraud

- Australian Manufacturing organisation
- Numerous Asia-Pac suppliers
- Approximately $1 million fraud
- Attacker utilised a weak point in the business process (supplier IT security, payment process)
- “Man-in-the-middle” style deception
- Analysis Tools Used – Nuix, LibPDF, ExifTool
- Time Line Analysis

Ferrier Hodgson

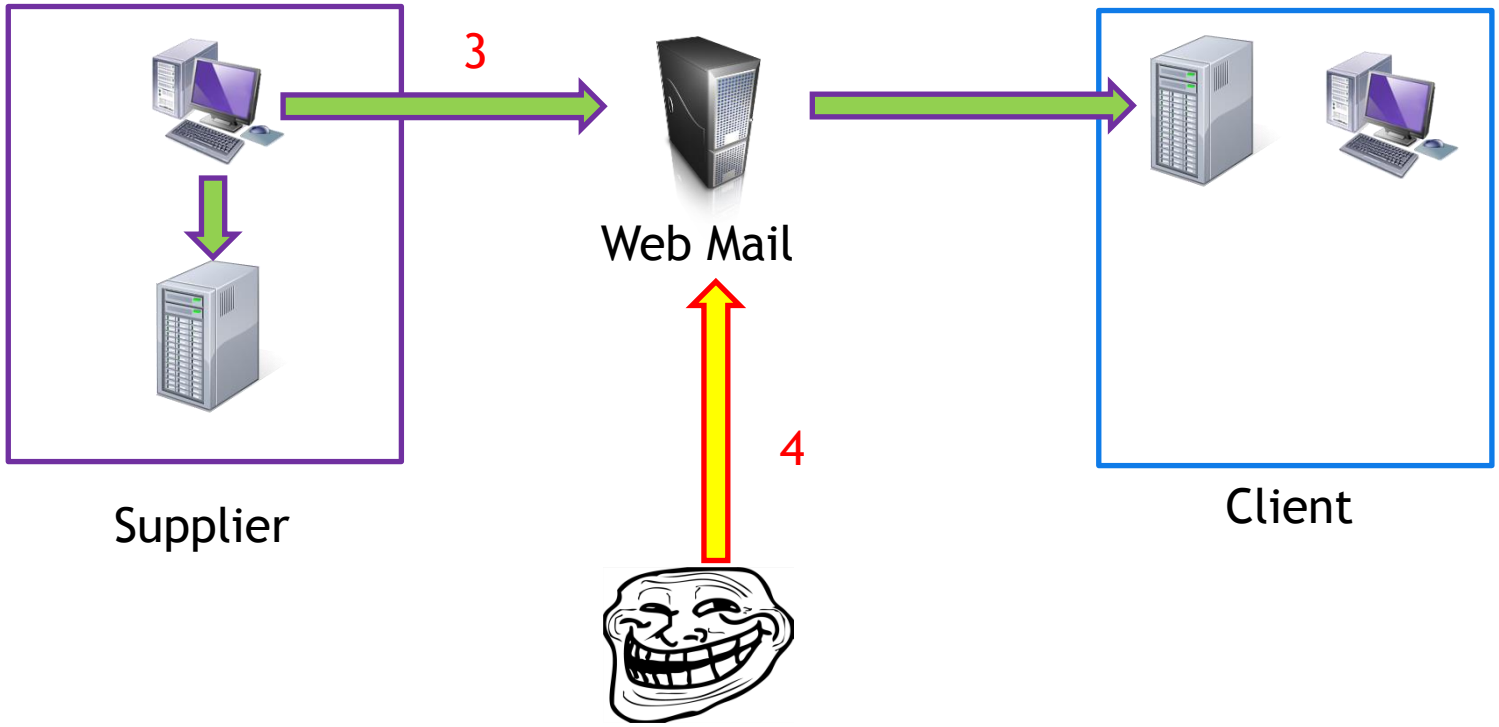
Time Line Case Study – Online Fraud



- **Early September 2013**
  - Supplier “hacked” by unknown group (1)
  - Causes minor interruption in business processes between supplier and client
  - Hacking incident is mentioned to the client in an informal email. (2)
  - Supplier contact utilises a account for communications with client
  - Attacker begins monitoring supplier operations

Ferrier Hodgson

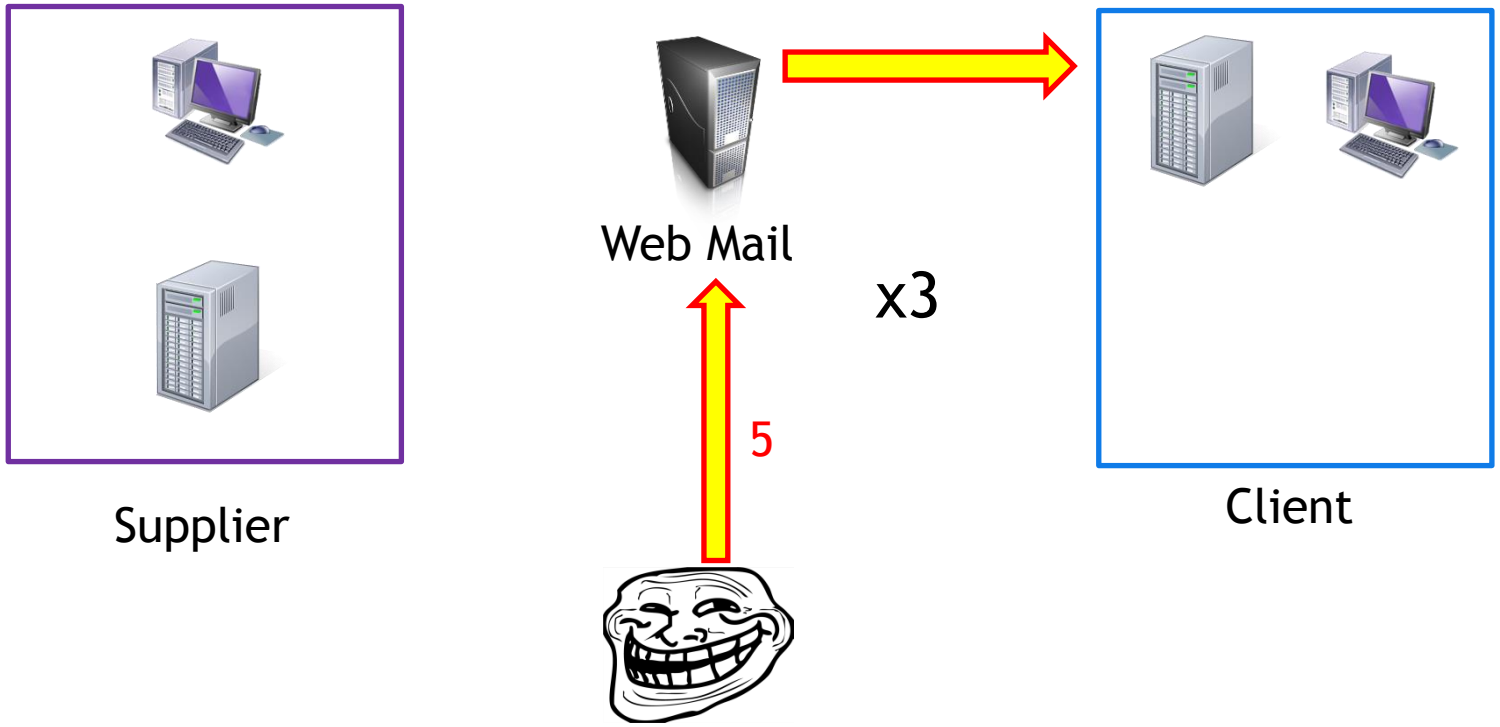
Time Line Case Study – Online Fraud



- **Late September 2013**
  - Supplier sends a payment reminder email to client ($1 million) (3)
  - Attacker observes outgoing email. Creates a web based account with a name very similar to the supplier's personal account (4)

Ferrier Hodgson

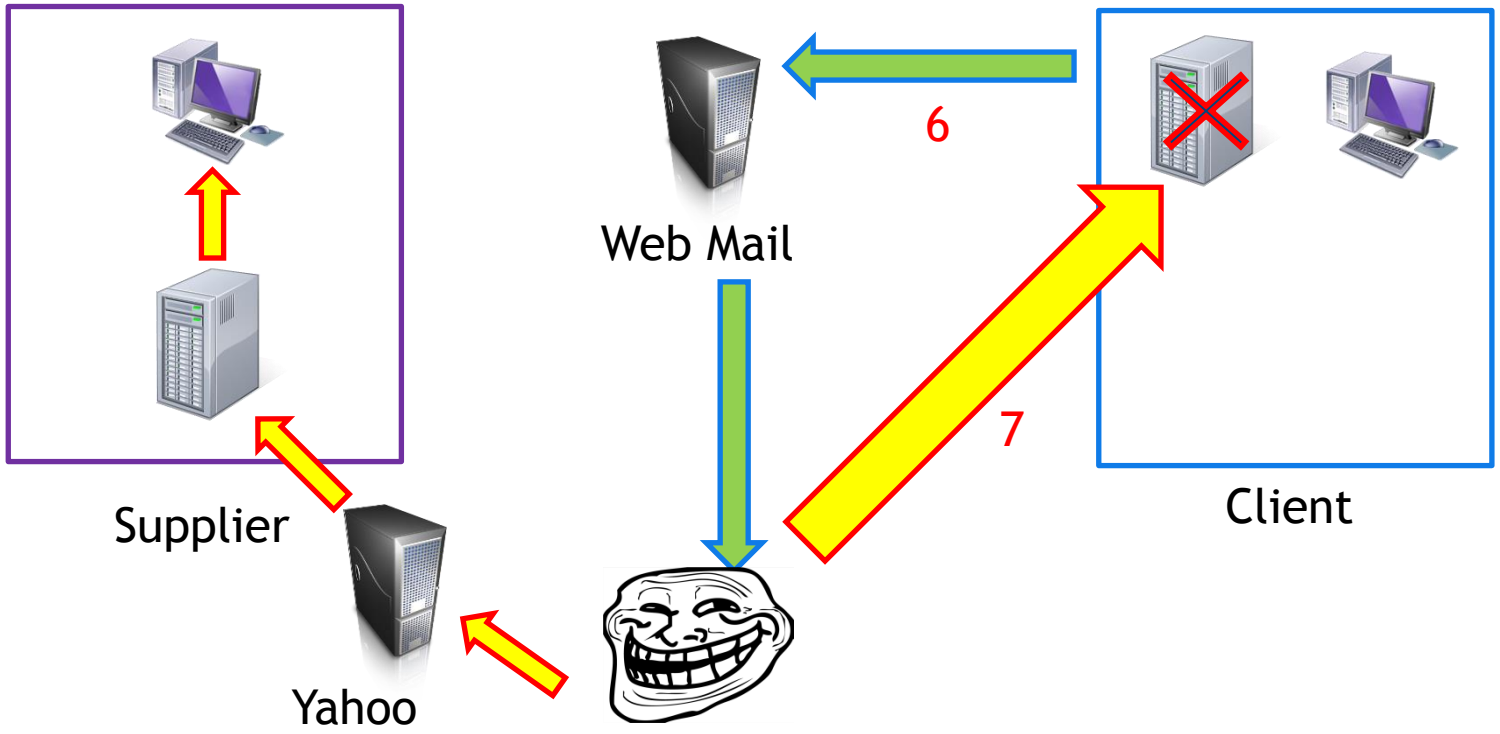
Time Line Case Study – Online Fraud



- **Late September 2013**
  - Attacker sends an email from the fake account to the client providing new banking details. States need to change the account due to an audit. (5)
  - Over the course of the next three days the attacker resends this three times

Ferrier Hodgson

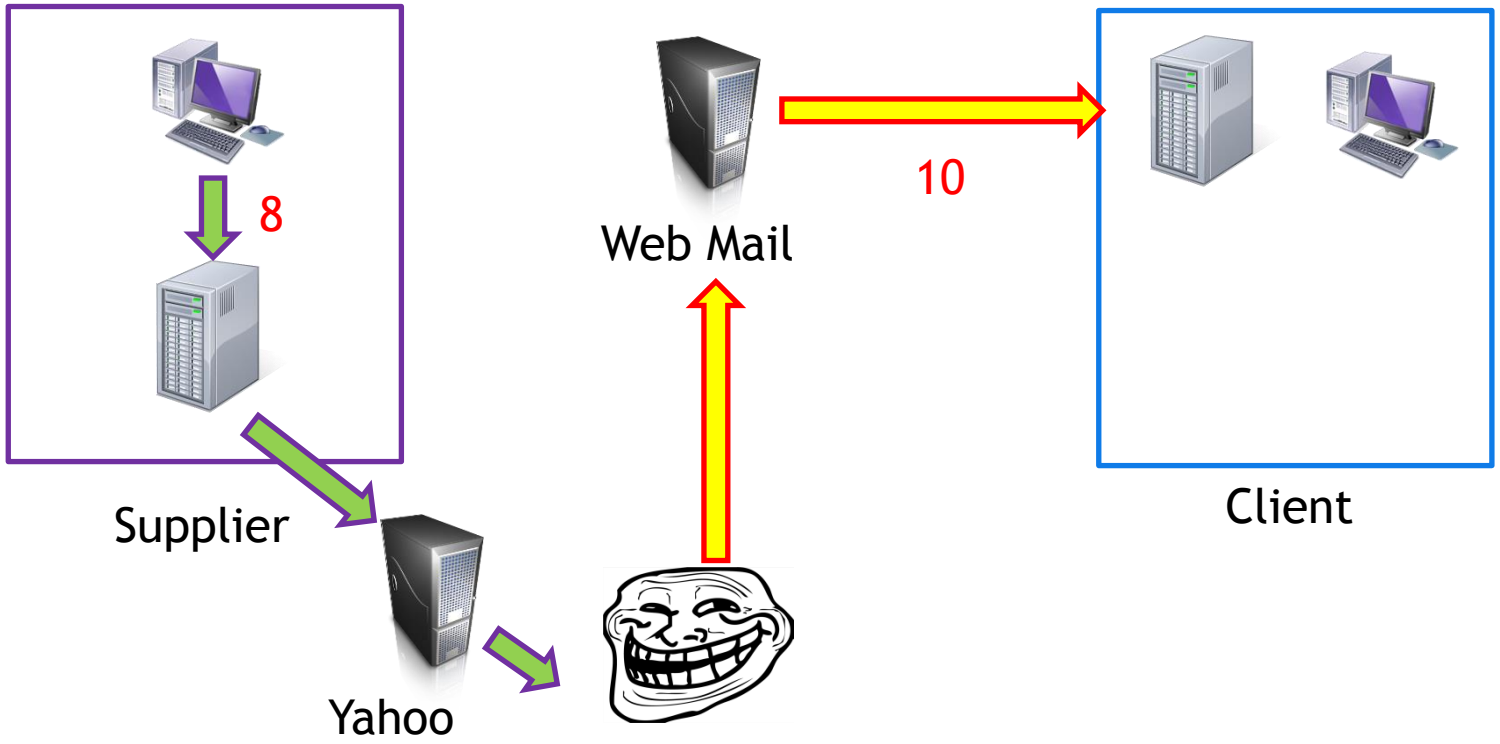
Time Line Case Study – Online Fraud



- **Late September 2013**
  - Client (following standard policies) requests that the change is verified via a formal letter signed by Supplier MD on company letterhead. (6)
  - Attacker disables the client's email server with a Denial of Service attack (7)
  - Creates a Yahoo email account under the name of the client account manager Sends a request to supplier for a document signed by MD "for their records".

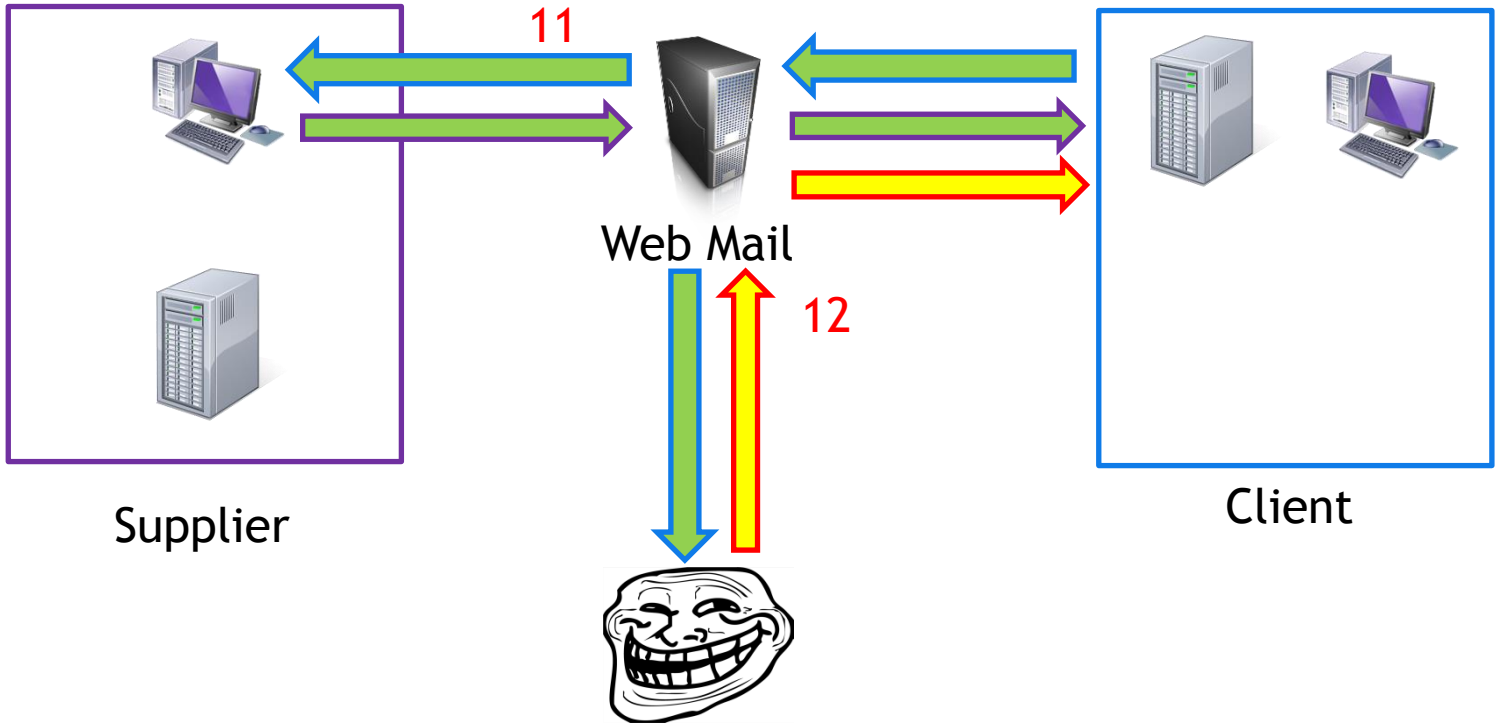
Ferrier Hodgson

Case Study – Recent Online Fraud



- **Early October 2013**
  - Email to the Supplier uses the same tactics (previous text, sig block etc).
  - Supplier sends a PDF'd letterhead document and sends to the attacker (8)
  - Attacker edits the PDF to reflect the desired bank account changes (9)
  - Attacker sends the altered PDF to the Client. The client now has a formal, signed request to alter the bank account details on Supplier letterhead (10)

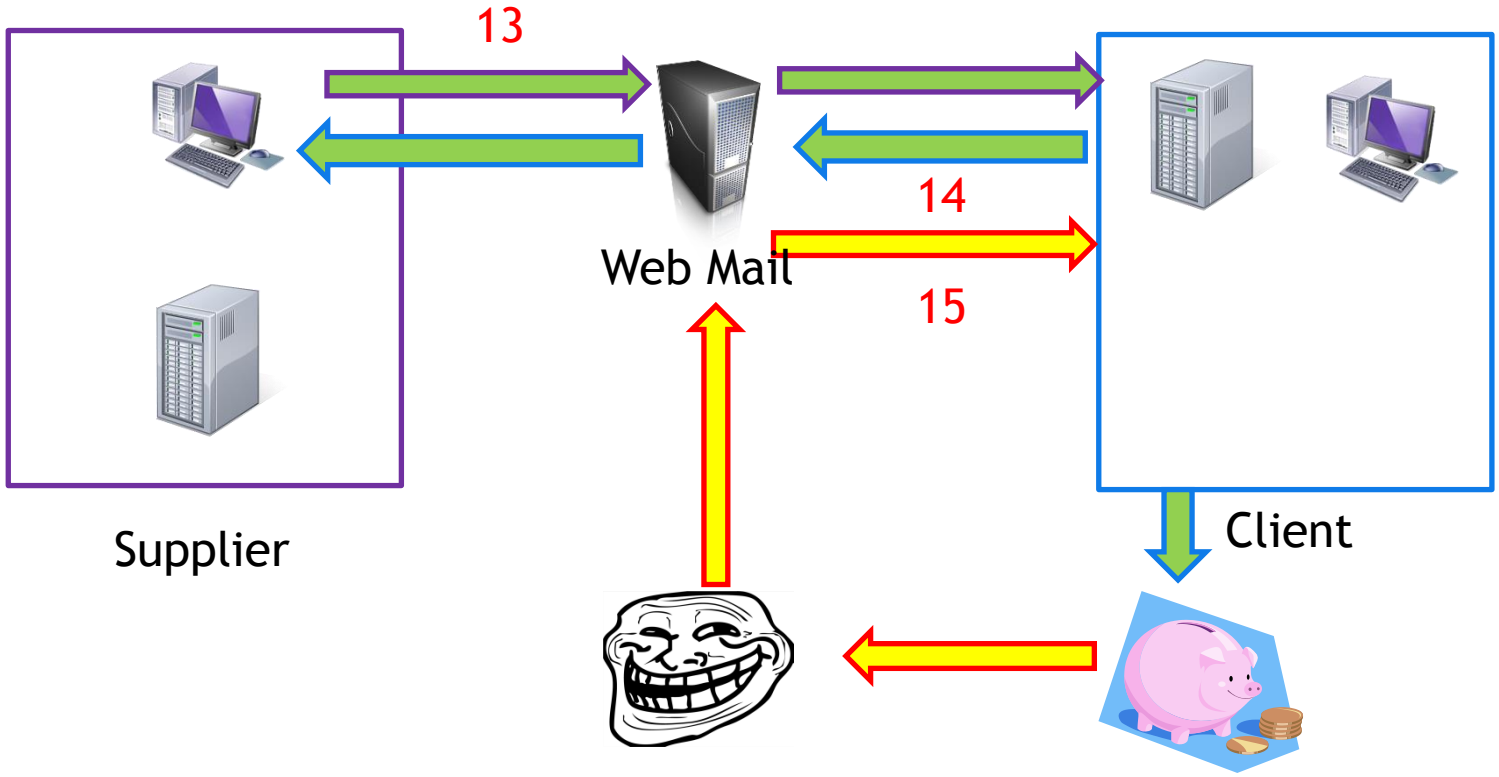
Case Study – A Complex Attack



- **Early October 2013**
  - Supplier had been trying to send a follow up email to the legit client during the email server downtime. When the server is repaired this email arrives.
  - Client responds that the payment is going through soon (11)
  - Attacker sends an email to the client reinforcing the changed bank account details.

Ferrier Hodgson

Time Line Case Study – Online Fraud



- **Early October 2013**
  - Client makes payment into attackers bank account.
  - Supplier informs Client that payment has not been received (13)
  - Client replies stating that payment should have gone through (14)
  - Attacker replies to this email stating that there have been problems with their accounts and not to worry about it for a few days (15)

Ferrier Hodgson

Questions or Comments?

Adam.daniel@fh.com.au

DON’T LET THE ALIENS PROBE YOUR BUM!
JOIN THE RESISTANCE!