Deloitte.

Deloitte Financial Reporting Conference

Rising to the challenge

Tuesday 22 September 2015
Convention Centre Dublin

Cyber security

Colm McDonnell

Introduction

Stories of organisations getting hacked are becoming so frequent that it would be easy to believe that there's no real way to avoid being the next target.

Why does hacking occur?

Time invested in identifying why someone might want to hack you is worthwhile. If you work in Finance then your job description alone suggests that you have access to funds and makes you an attractive target for cybercriminals.

Some of the more common reasons are:

Access to/theft of sensitive data such as intellectual property or credit card/bank account details

Access to one of your business associates

Cash transfer

Free use of your facilities

To disrupt your day to day business

To embarrass an organisation and discourage clients from using your services

Why does hacking occur?

There are multiple ways for an external person to gain unauthorised access into a system, the most common being exploiting a known vulnerability, the introduction of malware or some combination of the two.

A hacker goes through a similar process to a house burglar; they case out the joint, test to see if there are any obvious points of entry and then attempt to break in. Hacking can be easy there are three main stages involved in targeted hacking:

Cyber scams and attacks

There are a huge variety of cyber scams and attacks that can be inflicted on an organisation. Some of the more disruptive and damaging events that we are seeing in Ireland at the moment are banking Trojans, ransomware, DDos (Distributed Denial of Service) and fund diversion by social engineering.

So, how can you try to avoid being the next victim of the Cyber crimewave?

- Install anti-malware software and keep it up-to-date.
- Don't click on email links from unknown or atypical sources
- Use complex passwords or passphrases, keep them safe and don’t use the same password across multiple systems.
- Encrypt data that you don't want stolen and safeguard the decryption keys
- Get your systems checked for known vulnerabilities
- Operate good patch (software updates) management practices
- Monitor patterns of system usage and payments
- Avoid visiting suspect websites
- Use two factor authentication for sensitive transactions
- Keep good backups of your important data
- Train your system users in safe online practices

Case #1
Ashley Madison – The Attack

This was a “**PRINCIPLED**” attack

The attack was first disclosed in July 2015.

The group behind the breach (Impact Team) said their goal was to destroy Ashley Madison's parent company as they objected to Ashley Madison's morally dubious business model.

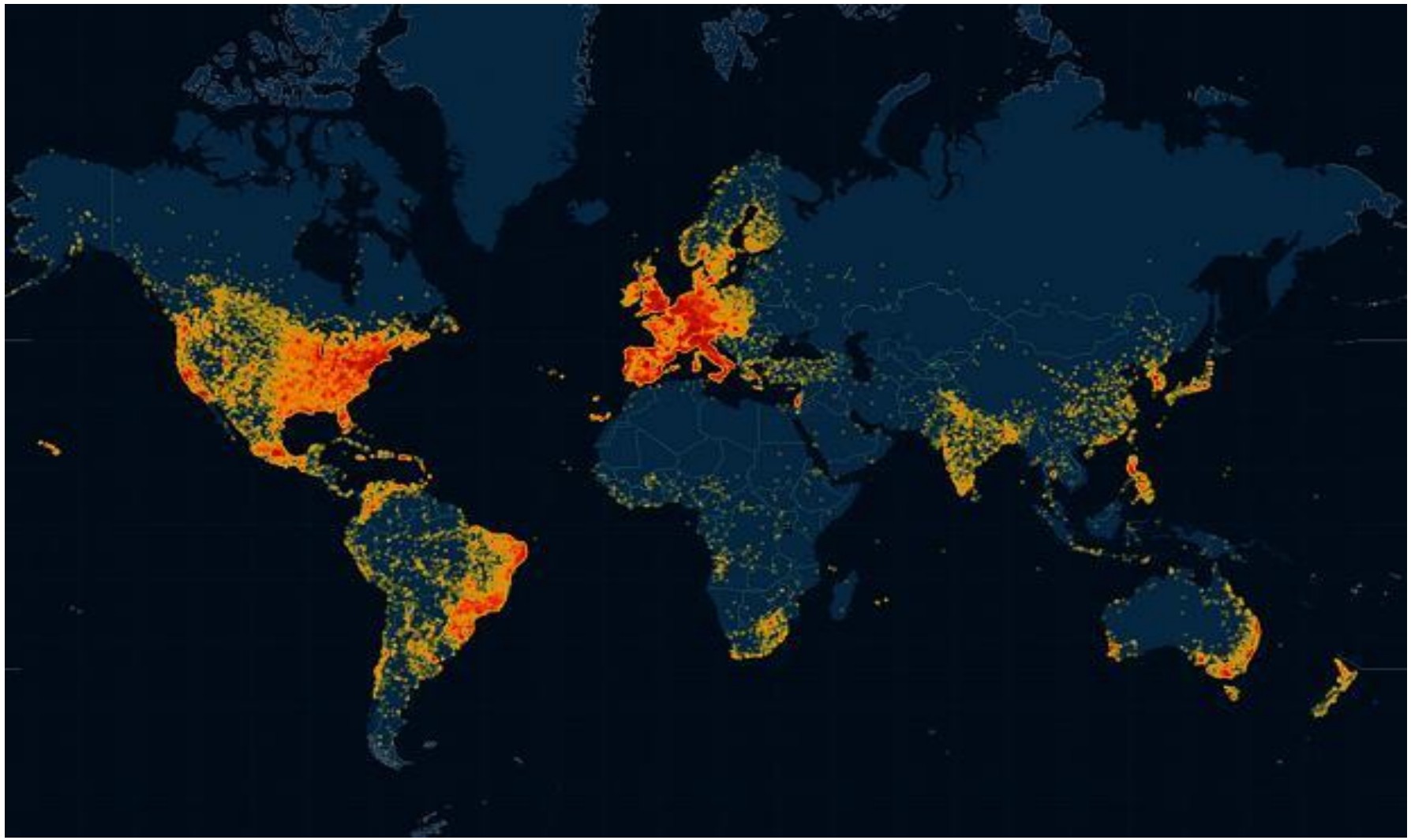
In mid August, data from 37 million of users began to appear online.

9.96GB of internal data released online including:

- ✓ *User Databases*
- ✓ *Financial Records (9 million individual credit card transactions)*
- ✓ *Private details of the service’s owners*
- ✓ *The distribution was 13.9% women versus 86.1% men*
- ✓ *12,736 unique .ie addresses*

Case #1

Heat Map Of User Access



Case #2
Sony Pictures – The Attack

The attack was discovered on the 24th November 2014 by users seeing defacement of their login screens.

The network was compromised for an unknown length of time prior to being detected.

The group responsible claims to have stolen over 100 Terabytes of data.

After copying data, the Destover malware wiped the infected systems

Over 40GB of internal data released online including:

- ✓ *Intellectual Property (5 films)*
- ✓ *Corporate data including salaries and performance reviews*
- ✓ *Confidential emails*
- ✓ Suggestion of insider (we have experienced this – bounty)

Case #3
Nortel – The Attack

Using spyware, attackers stole the passwords of the Nortel CEO and 6 other senior executives.

Nortel security staff detected unusual downloading patterns from these account and changed the passwords a couple of years later. They also began monitoring for further suspicious activity, but stopped shortly after.

It was 2010, believed to be a decade since the initial attack, that it was realised that attackers had access to:

- ✓ *Technical documents*
- ✓ *Business plans*
- ✓ *Emails*
- ✓ *Research reports*

It was too late

Case #4
Confidential – ERP Gone

Client arrived on Monday morning and could not access financial information on their ERP system

All of the system configuration had been corrupted

Back up process had been corrupted

Email received requesting significant payment for return of ERP

Week later we found data hidden on network

Case #5

Confidential – Funds Transfer

Client transferred €Xm to Cypriot bank in error

Fob had been used to approve transfer

Large single transfer

Call back from bank had not seemed to occur

Transfer did not complete through sheer luck

Cyber scams and attacks

From our security lab in Dublin we have investigated a number of cases involving malware that attempts to collect banking credentials or encrypt data for a ransom fee in the past year.

Variants of banking Trojans:

Install some kind of keylogger on your system to record your keystrokes

+

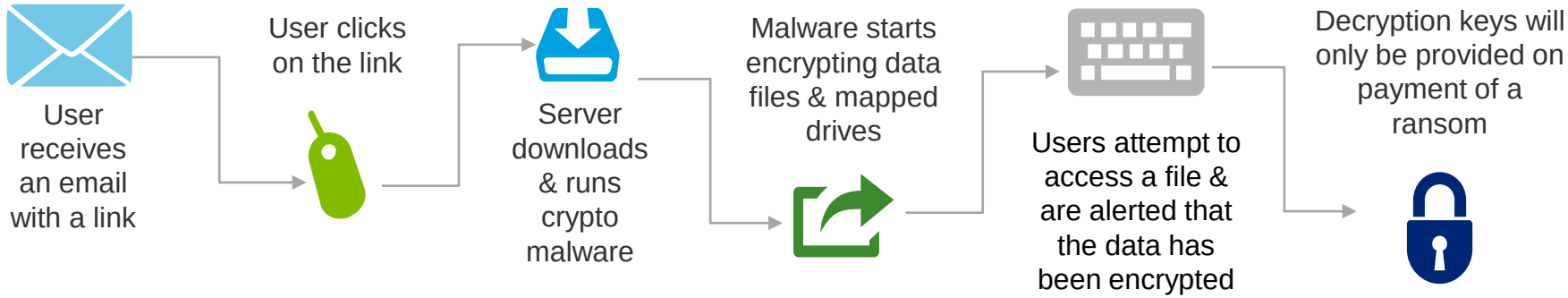
Capture your banking credentials

=

The credentials can be used by an attacker to transfer funds from your account

Example of crypto ransom attack

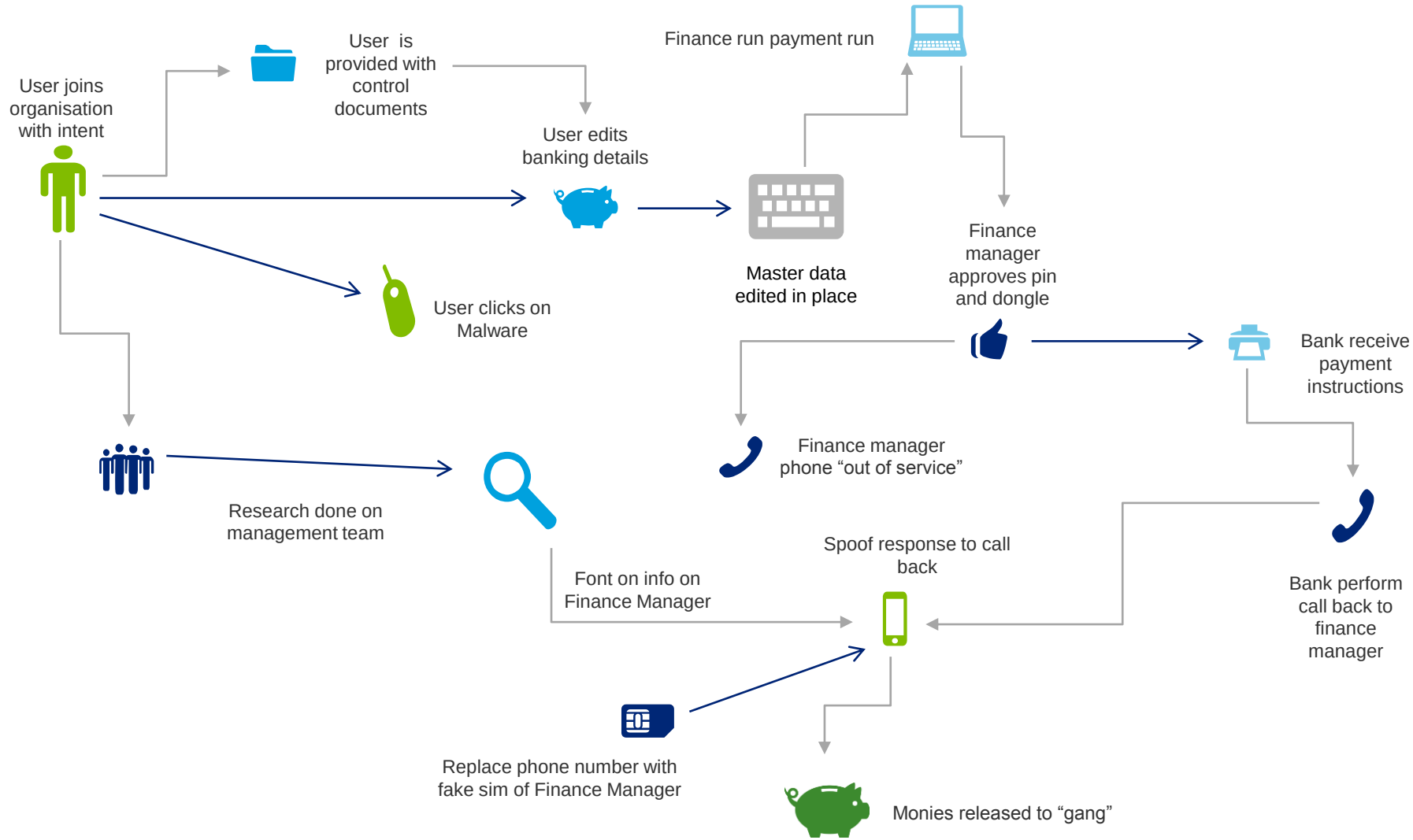
A particularly nasty crypto ransom attack has been doing the rounds globally and we have spent a couple of late nights helping our clients deal with its aftermath. This malware is typically targeted at an organisation and introduced via a phishing email.



It can be quite some time before anyone becomes aware of this. The payment is typically requested in bitcoin, an online currency which is much more difficult to track than traditional bank transfers or credit card payments. Sadly, if you don't have a good file backup strategy in place then you could be in real trouble with this attack, particularly if your backups are held on a mapped drive and also become encrypted.

Example of SIM spoof attack

A particularly nasty crypto ransom attack has been doing the rounds globally and we have spent a couple of late nights helping our clients deal with its aftermath. This malware is typically targeted at an organisation and introduced via a phishing email.



So, how can you try to avoid being the next victim of the Cyber crimewave?

- Install anti-malware software and keep it up-to-date.
- Don't click on email links from unknown or atypical sources
- Use complex passwords or passphrases, keep them safe and don’t use the same password across multiple systems.
- Encrypt data that you don't want stolen and safeguard the decryption keys
- Get your systems checked for known vulnerabilities
- Operate good patch (software updates) management practices
- Monitor patterns of system usage and payments
- Avoid visiting suspect websites
- Use two factor authentication for sensitive transactions
- Keep good backups of your important data
- Train your system users in safe online practices

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ie/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

With nearly 2,000 people in Ireland, Deloitte provide audit, tax, consulting, and corporate finance to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. With over 210,000 professionals globally, Deloitte is committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, the Deloitte Touche Tohmatsu Verein, any of their member firms, or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.