My Life as a Cyber Stalker
MU, February 2017

Paul Vlissidis - Technical Director, Senior Advisor
paul.vlissidis@nccgroup.trust
About NCC Group

Making the Internet a safer place

- Software Escrow & Assurance
- Cyber Forensics Incident Response
- Technical Security Assessments
- Applied Research
- 600+ Technical Assurance Consultants
- 35 Offices Around the World
- Cyber Security Assurance
- £850 Million FTSE Listed Company

About NCC Group
NCC Group tracks fugitives in second series of Channel 4 show Hunted
Ethical Hacking Quiz

- You are using an online shop and notice some strange errors. You type 'or '1'='1'-- and it throws an error indicating there is a vulnerability. You email the administrator to tell him.

- You are in an Internet café using a public access computer and you are worried that it might be caching everything you are typing. You hit 'back' a few times and find the previous user’s bank statement as a PDF displayed on the screen. You tell the manager of your concerns.

- You are on a wifi hotspot in a pub. You see a friend across the room on his laptop. You know his password so you remotely logon to his laptop while he is at the bar and screenshot/hide all his icons.

- You are using an online shop and notice some strange errors. You type 'or '1'='1'-- and it throws an error indicating there is a vulnerability. You email the administrator to tell him.
What makes it ethical?

• Expressed (usually written) permission to probe the network and attempt to identify potential security risks.

• You respect the individual's or company's privacy.

• You close out your work, not leaving anything open for you or someone else to exploit at a later time.

• You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware if not already known by the company.
• Why any of it matters

Case Study

• How Hackers work to hack you

Stuff We Will Cover
It’s a jungle out there
Hacking or Stalking?

- Hackers usually want money
- They will take their time
- Have different motives – e.g., revenge porn

Stalkers usually don’t

- They are usually opportunists
- You have probably never met them
- Probably know you (79% of stalkers are known to victims)

- Hackers usually want money
People Are The Weakest Link – it’s you they are hacking
How Hackers Target Victims

• Trawling the Internet for 'dumps'
• Phishing
• Malvertising
• Driveby downloads (apps & software)
• Spoofing a 'free' wifi network
• Vishing
• Lost or Stolen phones/laptops
• Vishing
• 'Dodgy downloads' (apps & software)
• Phishing
• Hack his hardware
• Hack his phone
• Hack his house

#HUNTED

Peter Blackley

search his house

'Hack his hardware'

'Hack his phone'

'Hack his house'
Data Breaches – 2 Billion and rising fast

- Usernames (usually email)
- Passwords (sometimes encrypted but usually easy to crack with free tools)
- Password 'hints'
- Sometimes home addresses
- Other data

Over 2 Billion accounts are out there.

On Hunted we got an almost 100% hit rate on breached accounts.

It cannot be deleted – it's a tattoo.

Check all your family's emails.

Check if you have an account that's been compromised in data breach.

These addresses are not the only data available.
How Stalkers Target Victims

Step 1 – Get Information About You

- They may already know you, so this is easy
  - Your details may be in an online 'data dump'
  - Your accounts may help them access your accounts
  - Email address
  - Social media profile
  - Mobile
  - Home address

You may be making it too easy by having a rich digital footprint
- Anything that could help them access your accounts
- They may already know you, so this is easy
  - Your details may be in an online ‘data dump’
How it all started

Paul Vissel’s knows that I am on a pre-Christmas break in Delhi. He can hack my every move and
is planning to do it to you.

And someone, somewhere this Christmas my home... simply by hacking my e-mails.
They took my cash, my job and the keys to my life were stolen by cyber stalkers.

Claudia Joseph for Mailonline

Published: 22 Dec 2013 | Updated: 10:48, 22 December 2013

- Cyber crime is estimated to be worth up to £27 billion a year in the UK
- He was able to not just steal her home, but also steal her identity. If he wished
- An online security investigator gets all her details in just a few clicks
- Claudia Joseph had her life hacked and was shocked by the results

13
The Phone Call

Claudia: “Hello. Can you hack me?”

Me: “Er…. What?”

Claudia: “I want to do a piece in the Mail On Sunday on how much of someone’s life a hacker can get access to so I want you to hack me. Can you start straight away?”

Me: “It’s not quite that simple – we need to discuss scope and authorisation.”

Claudia: “How tiresome. What do we need to do? Basically you can do what you like but don’t delete anything and don’t reset any passwords without checking first.”

Me: “Okay, I’ll give it a go.”

Claudia: “Great.”

Me: “I’ll let you know.”

Claudia: “Thank you.”
#HUNTED

David Toddington

Online Intelligence Expert

a digital tattoo. "It’s not just a..."

Open Source Intelligence

- Website – mobile and email
- Facebook – friends viewable but not much
- Twitter – very little but followers/followed
- Linkedin – correlated connections
- Companies House – home address
- Domain names – home address and addresses
- Company and credit searches – addresses
- Linked in – correlated connections
- Company and credit searches – addresses
- Alternate email in RIPE
- Domain names – home address and addresses
What we did find

Mac.com, me.com email indicated apple mac user
Confirmed iphone user using imessage

So...

iTunes account  - almost certainly
iCloud account - probably
Iphone backups – if we are lucky……..

Time to go phishing
Phishing

• Phishing is a social engineering technique to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

• Spear phishing is like phishing, but tailored for a specific individual or organization.

• Website from a phish website cannot tell a legitimate 70% of employees.
The Sting (spear phish)

86.163.100.212 - - [09/Apr/2013:17:48:36 -0400] "GET /?RTWPH-PHY8-MT6B-R9X6-JFHB2 HTTP/1.1" 200 530 ""Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/536.28.10 (KHTML, like Gecko) Version/6.0.3 Safari/536.28.10"

Dear Claudia Joseph,

I am the Apple Customer Support. You have received this email in error. If you have an unauthorized person has attempted to access your account, don't worry - your account is still secure and no one has been given access to it. Temporary limitations can be removed by verifying your account below.

Thanks,
Apple Customer Support

[Verification Code]

Please verify your account.

If you believe you have received this email in error, please contact Apple Customer Support directly.
Email — still the key to everything

Trawled emails containing the word 'password' or 'welcome'

66 emails containing the word 'password' and 85 emails saying: 'Welcome.'

Backup of password vault was attached to an email

Cracked using slight variation of iCloud password
Identity Theft
Challenge 1 – Who am I staying with?

US Embassy?

Email/Facebook searches
Challenge 2 – Keys to my house

Hi Pandora, I forget that I had arranged to have someone check out my central heating. He is due around 3pm and his name is Paul. Can you let him in? I mobile account SMS - neighbour

• Narrowed down to 2.
• Search emails/facebook for correspondence
• Narrowed down to 2.
• Guessed nearest
• Searched contacts for same street

"I" Pandora, I forget that I had arranged to have someone check out my central heating. He is due around 3pm and his name is Paul. Can you let him in?"
Money transfer account number was needed for verification but this was stored in Contacts in iCloud.
Hiding the evidence
Phone restore

- iCloud backup restored to a blank phone
- Geo tagged photos
- Spoof texts “I resign”
- Access apps
- Access photo stream
Implications

- Cloud services have dramatically increased the risks for individuals. Our device backups and pictures are out there.
- Email is still much more important than we all think.
- Email is still much more important than we all think.
- Password managers work really well (but only if you use a unique password!).
- If somebody takes over your online life it can have dramatic consequences.
- Adopt two-factor authentication to protect yourself. It's not foolproof but it will thwart most hackers/stalkers.
If in doubt, seek technical help!

See https://www.linkedin.com/pulse/protecting-your-digital-self-cyberstalkers-

- Emails get marked as read or disappear.
- Friends report getting odd messages from you on social media.
- Your computer takes longer than usual to start up, restarts on its own, or doesn’t start up at all.
- The homepage set on your web browser has changed or web pages are slow to load.
- Make sure your security software is up to date and run it to check for infection.
- Check your login history and your Google search history for anything that looks odd.
- Check your security settings on email, social media.

Signs When Something Isn’t Right
10 Steps To Protect Yourself

• Do lock your computer/phone/tablet when you leave it and set a PIN
• Do regularly apply latest software updates to everything
• Do use an anti-virus tool
• Do back up your important files/photos/data
• Do use 2-factor authentication for your main email and cloud services
• Do store passwords/PINs in your contacts
• Don’t share passwords between sites
• Don’t install software/apps unless you are very sure it is genuine
• Don’t save card details on websites
• Don’t save passwords/PINs in your contacts
• Don’t save passwords/PINs in your contacts
• Do treat public Wi-Fi with suspicion – use a VPN
• Do use a password manager
• Don’t store passwords/PINs in your contacts
• Do treat public Wi-Fi with suspicion – use a VPN
• Do use a password manager
Europe

Manchester - Head Office

Middle East

Singapore

North America

Atlanta, GA

San Francisco, CA

New York, NY

Chicago, IL

Cupertino, CA

Boston, MA

Austin, TX

Aliso Viejo, CA

Toronto, ON

Sunnyvale, CA

Seattle, WA

San Francisco, CA

London

Edinburgh

Dublin

Cheltenham

Copenhagen

Cambridge

Amsterdam

Zurich

Vilnius

Munich

Milan

Madrid

Luxembourg

London

Leeds

Leatherhead

The Hague

Chicago

Campbell, CA

San Francisco, CA

Seattle, WA

Sunnyvale, CA

New York, NY

Chicago, IL

Cupertino, CA

Boston, MA

Austin, TX

Aliso Viejo, CA

Toronto, ON

Sunnyvale, CA

Seattle, WA

San Francisco, CA

London

Edinburgh

Dublin

Cheltenham

Copenhagen

Cambridge

Amsterdam

Zurich

Vilnius

Munich

Milan

Madrid

Luxembourg

London

Leeds

Leatherhead

The Hague

Chicago

Campbell, CA

San Francisco, CA

Seattle, WA

Sunnyvale, CA

New York, NY

Chicago, IL

Cupertino, CA

Boston, MA

Austin, TX

Aliso Viejo, CA

Toronto, ON

Sunnyvale, CA

Seattle, WA

San Francisco, CA

London

Edinburgh

Dublin

Cheltenham

Copenhagen

Cambridge

Amsterdam

Zurich

Vilnius

Munich

Milan

Madrid

Luxembourg

London

Leeds

Leatherhead

The Hague

Chicago

Campbell, CA

San Francisco, CA

Seattle, WA

Sunnyvale, CA

New York, NY

Chicago, IL

Cupertino, CA

Boston, MA

Austin, TX

Aliso Viejo, CA

Toronto, ON

Sunnyvale, CA

Seattle, WA

San Francisco, CA

London

Edinburgh

Dublin

Cheltenham

Copenhagen

Cambridge

Amsterdam

Zurich

Vilnius

Munich

Milan

Madrid

Luxembourg

London

Leeds

Leatherhead

The Hague

Chicago