nccgroup
freedom from doubt

Phishing Stories

Shaun Jones

Agenda

- **What is Phishing?**
- **Phishing Story I – Intranets are actually pretty useful**
- **Phishing Story II – Why do I need two factor auth**
- **Phishing Story III – Everybody gets shells!**

What is Phishing?

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

PHISHING STORY I

Intranets are actually pretty useful

STORY I

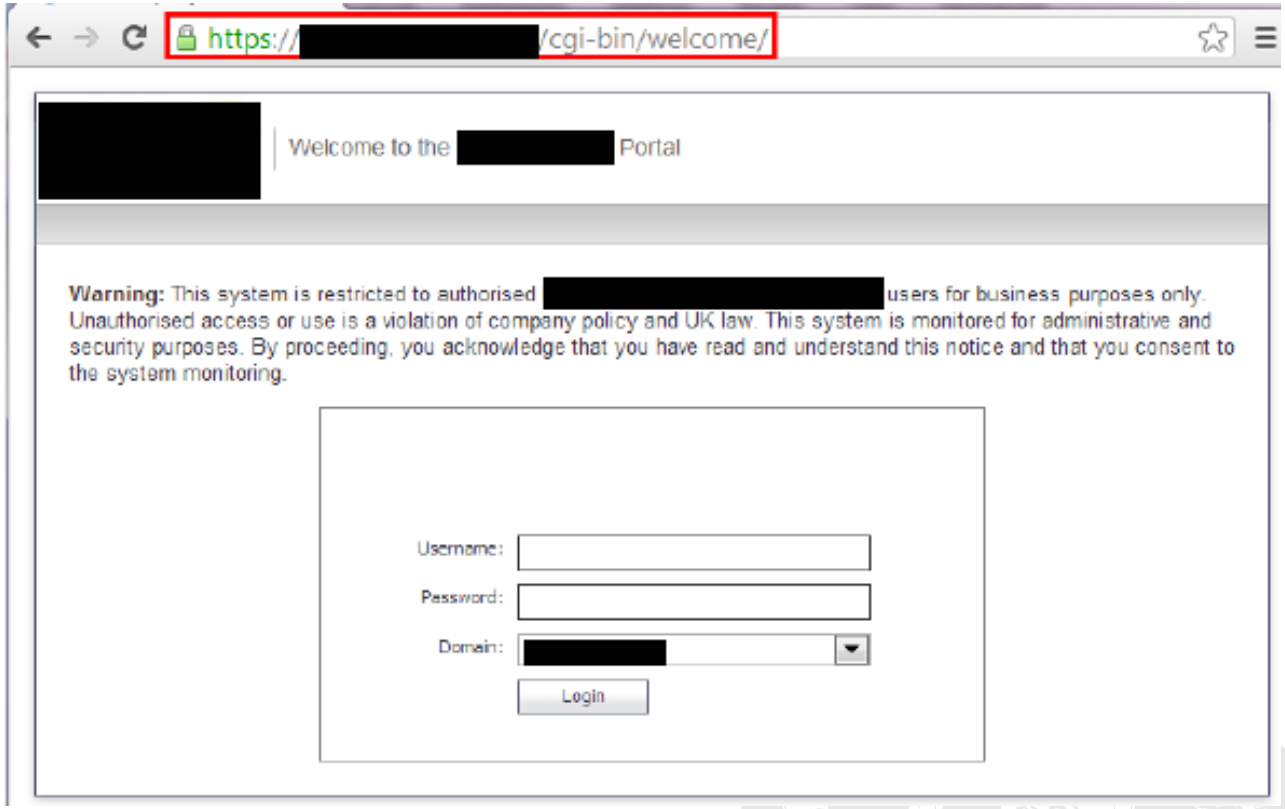
Point of the job?

- Test the client's susceptibility to phishing attacks
- Test clients IT team's ability to respond to a phishing attack
- Phishing was part of physical breach

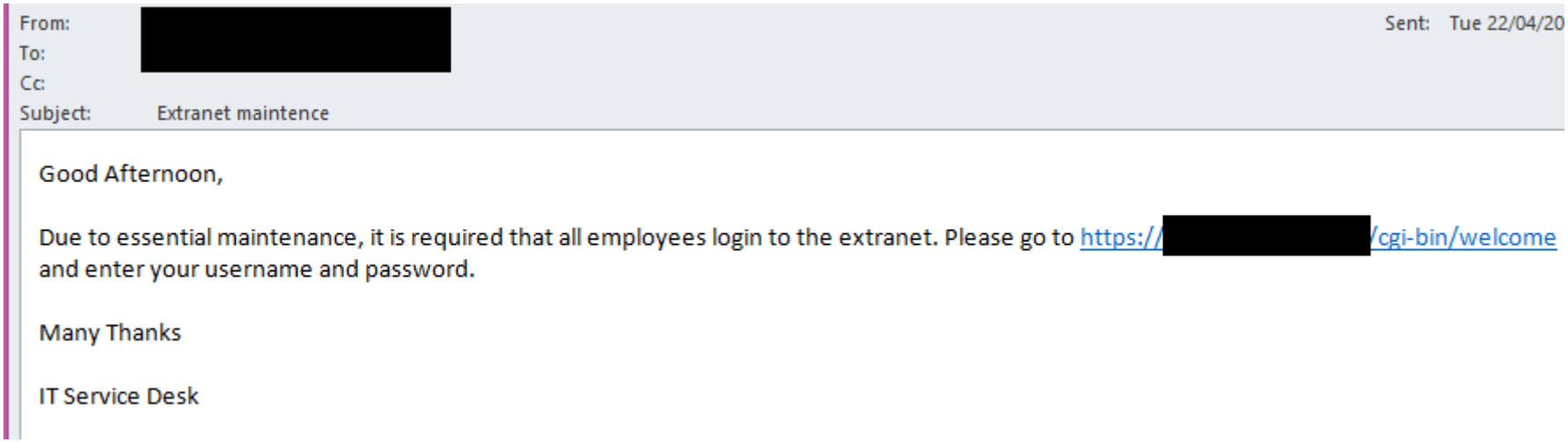
Our Plan

- Target the external login interfaces
- Launch an attack impersonating an extranet login page
- Capture creds and use them to access the SSL VPN
- Do the root dance
- Use access to aid with physical breach

STORY I – FAKE EXTRANET SITE – THE SITE



STORY I – FAKE EXTRANET SITE – THE EMAIL



From: [redacted]
To:
Cc:
Subject: Extranet maintence

Sent: Tue 22/04/20

Good Afternoon,

Due to essential maintenance, it is required that all employees login to the extranet. Please go to https://[redacted]/cgi-bin/welcome and enter your username and password.

Many Thanks

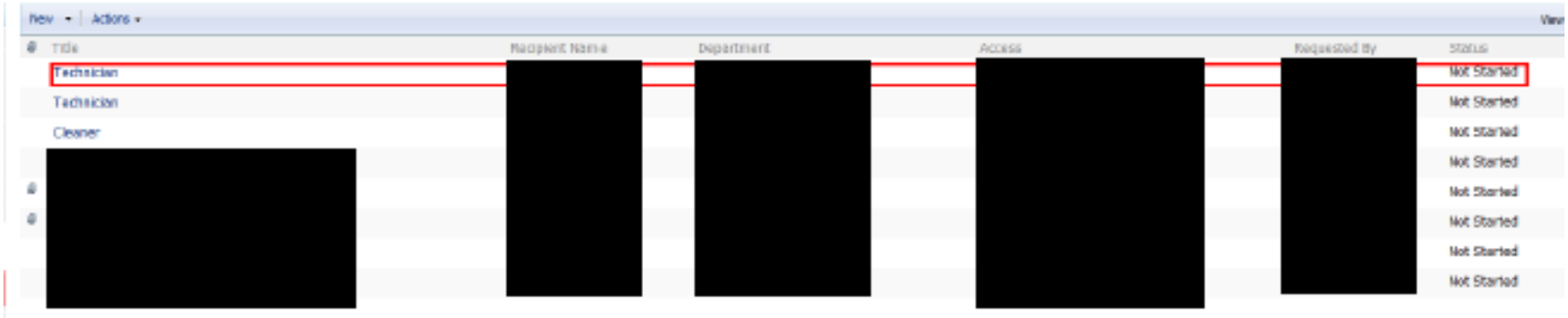
IT Service Desk

Story I – Outcome of The Phishing Attack

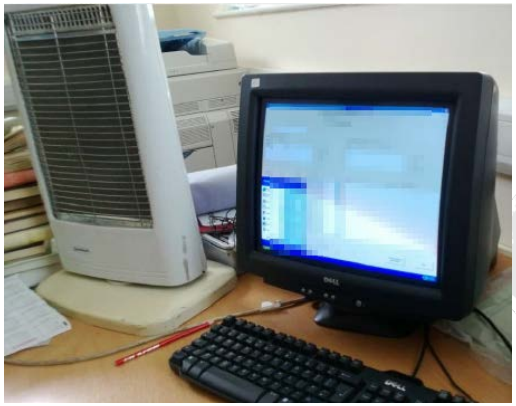
- Captured a lot of domain credentials within minutes of sending the email
- Used the captured credentials on OWA and their SSL VPN
- Found a number of credentials sets and instructions on how to connect to certain systems in mailboxes
- Scanned their internal network for common easy ports (8080, 8081 and 1433)
- Found numerous MSSQL(1433) ports open
- Default creds SA with a blank password
- MSSQL service has domain admin privs

Story I – The Intranet/Requesting an Access Card

Access Card Request



STORY I – ACCESS TO THE BUILDING



nccgroup
freedom from doubt

PHISHING STORY II

Why do I need two factor authentication

STORY II

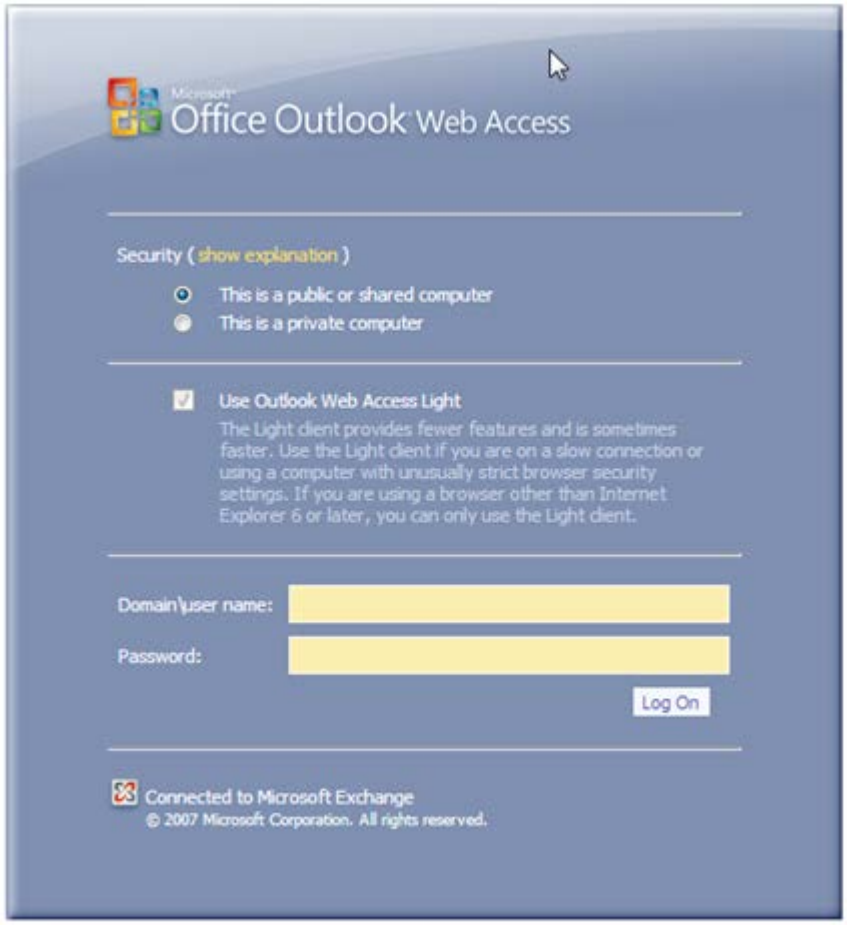
Point of the job?

- Physical breach gig with a Phishing assessment included
- Test clients user’s susceptibility to a phishing attack

Our Plan

- Steal credentials
    - Launch an attack against OWA
- Use compromised accounts in Physical breach
    - Create a back story to get access
    - To log into machines

STORY II – FAKE OWA – THE SITE



STORY II – FAKE OWA – THE EMAIL

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

STORY II – BACK STORY EMAIL

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.

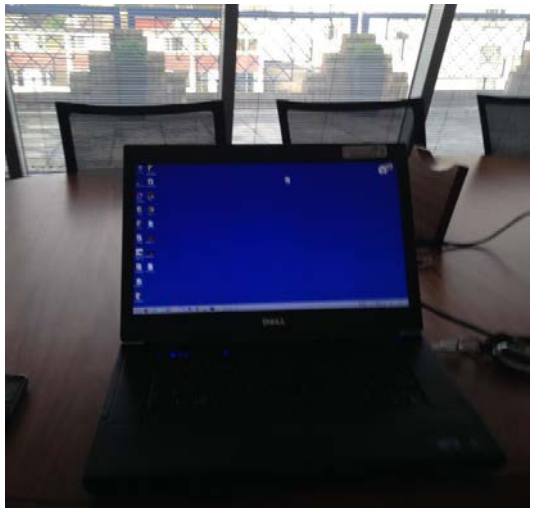
They know where they are going and just require to be let in.

Names are: Mithun Bagdai and Shaun Jones.

Thank you,
Mithun

THE NEXT DAY…

Got Fobs and visitor badges…



Went to a meeting room…

Got domain admin thanks to weak local admin creds and services running with domain admin privs…
The whole breach took 20 minutes thanks to the email

```
C:\>net group "domain admins" ncctest /domain /add
The request will be processed at a domain controller for domain group.local.

The command completed successfully.
```

PHISHING STORY III

Everybody gets shells!

STORY III

Point of the job?

- Test the users susceptibility to a Phishing attack
- White box approach was taken

Our Plan

- Steal credentials
    - Employee Benefits
    - A new OWA rollout (they actually use Lotus Notes)
- Get Shells
    - Obtain remote access & get proof of pwnage

WHY WHITE BOX?

Time limited testing

Technologies in place

- Whitelisting approach to web filtering (Websense)
- Application Whitelisting (Avecto)
- AV & Host based firewall (Sophos)
- TrendMicro's InterScan Web Security

The main goal was to test users not the technology, but where is the fun in that?

STORY III – CRED HARVESTING - SITE

STORY III – CRED HARVESTING - EMAIL

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

STORY III – CRED HARVESTING REPLIES

Sometimes users just don't want remote access to their emails.

Hi Shaun,

Why would I want to check my work emails when I'm away from work, I switch
off from work the minute I leave site and enjoy my freetime.

Regards.

Andy.

From: helpdesk[redacted]
To: andy.[redacted]
Date: 04/04/2014 11:14
Subject: Re: Email Pilot

Hi Andy,

This should work from anywhere, have you tried logging in?

Thanks,
Shaun

On 2014-04-04 11:12, andy.[redacted] wrote:

> Thanks,
>
> But I think this is a waste of time as I don't have a works device to
> read
> my emails remotely from.

STORY III – CRED HARVESTING REPLIES

Some have odd questions... And still enter their creds.

```
Shaun

to clarify, do you mean I can go into an internet cafe in Iraq and login to
my emails?

Clark
```

STORY III – CRED HARVESTING REPLIES

And others want access real bad!

Shaun,

The link took me to the [redacted] website. What am I meant to do next please
to
access my e-mails?

Darren

Darren [redacted]
Head of [redacted]

Shaun,

When are you planning to do this please?

Darren

Shaun,

Tried several times but not certain it has worked.

Darren

STORY III – CRED HARVESTING REPLIES

So we told him we would need to remotely access and that he had to go to a website and run a malicious batch script. He said it didn't work…

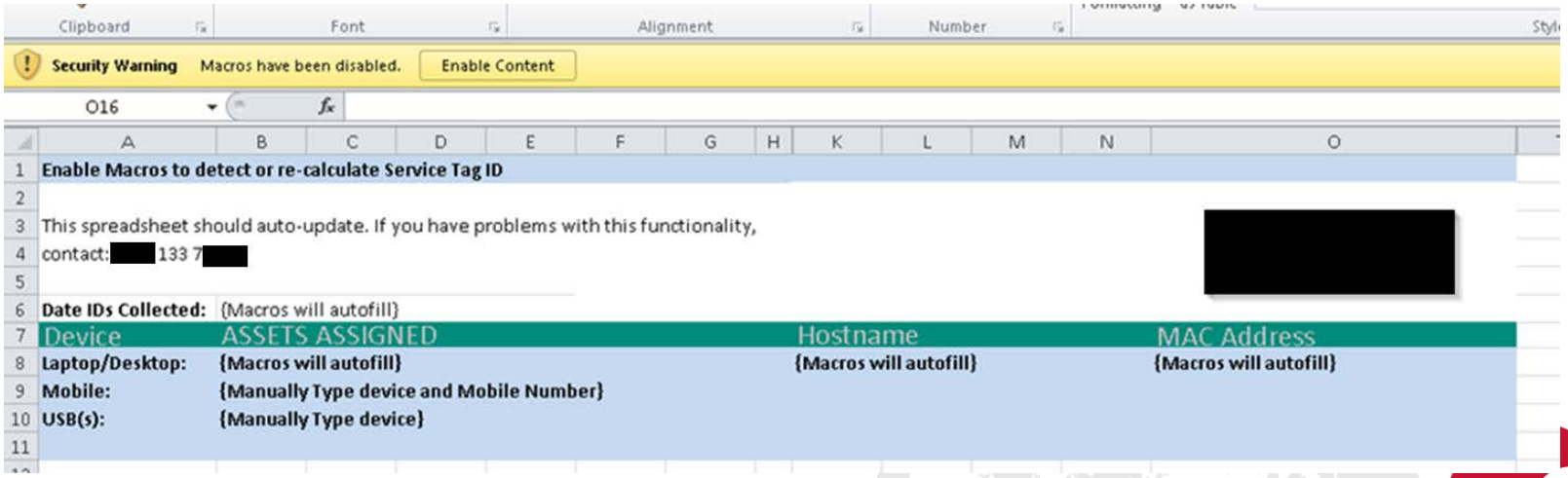
```
===============
0 - IFXXXXX4L
===============
1 - IGXXXXX6D
Please select a victim: 1
You have selected:
IGXXXXX6D

Please enter a command: whoami
DOMAIN-NAME\Darren_XXXXXXXXX

Please enter a command: net user
  User accounts for \\IGXXXXX6D
-------------------------------------------------------------------------------
Administrator            ASPNET
Guest                    SophosSXXIGXXXXX6D
The command completed successfully.

Please enter a command: systeminfo
 Host Name:                 IGXXXXX6D
 OS Name:                   Microsoft Windows 7 Professional
 OS Version:                6.1.7601 Service Pack 1 Build 7601
 OS Manufacturer:           Microsoft Corporation
```

STORY III – GETTING A SHELL

Payload = Modified version of DNSCat & custom reverse shell

Dropper = Malicious Macro

Reason to enable = Auto-fill for asset registration (everyone's lazy)



STORY III – GETTING A SHELL - EMAIL

[Action Required] - Assigned Assets Register

procurement@[redacted]

Sent: Fri 04/04/2014 09:38

To: Shaun Jones

Message | Asset-register-v0.1a.xlsm (33 KB)

Dear Shaun,

Inaccuracies within the asset register for assigned IT equipment is making it hard to track and plan ongoing IT asset procurement. The attached spreadsheet will automatically update with your currently assigned asset details; please check the entry for the assets currently tracked against you is correct and reply back to this email. A pending upgrade of laptops that are older than 2 years will be processed by 9th April ; to check your eligibility, the spreadsheet can check your Service Tag for you.

Please note – to ensure your details are updated correctly, please make sure that that you click the "enable macros" button on the attached spreadsheet.

Thank you for your cooperation.

Richard[redacted]
IT Procurement Assistant | [redacted]

Tel [redacted]
Email: richard.[redacted]

Out of Office:
Advance Notice of Leave:

ENVIRONMENT - Please consider the environment and don't print this e-mail unless you really need to.
****
Warning: This message is intended only for the use of the individual to whom it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law.
If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error please notify the sender.
Thank you.
****
For more information about [redacted] please visit our website at [redacted]

STORY III – GETTING A SHELL

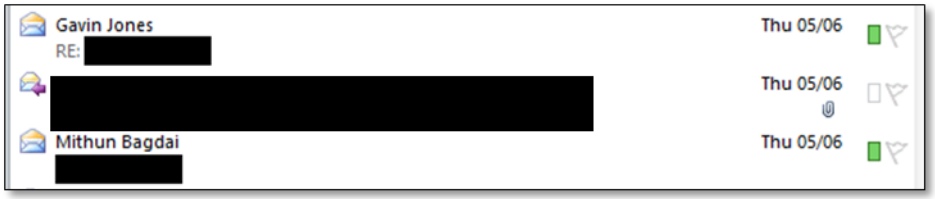
```
Waiting for DNS requests for domain '*' on 0.0.0.0:53...
Session jwnqtswq doesn't exist; accepting sequence number 1577
Creating new session jwnqtswq with sequence number 1577
jwnqtswq: Microsoft Windows [Version 6.1.7601]

jwnqtswq: Copyright (c) 2009 Microsoft Corporation.  All right
jwnqtswq: s reserved.

jwnqtswq: H:\Document>
Session timed out: jwnqtswq
Creating new session jwnqtswq with sequence number 1670
jwnqtswq: whoami
jwnqtswq: XXXXXXXXXX\Robert_XXXXXXXXX

jwnqtswq:

jwnqtswq: H:\Document>
jwnqtswq: systeminfo
jwnqtswq: systeminfo
jwnqtswq:
jwnqtswq:

jwnqtswq: Host Name:                 IGXXXXXXL

jwnqtswq: OS Name:                   Microsoft Windows 7 Pro
jwnqtswq: fessional

jwnqtswq: OS Version:                6.1.7601 Service Pack 1 Build 7601

jwnqtswq: OS Manufacturer
```

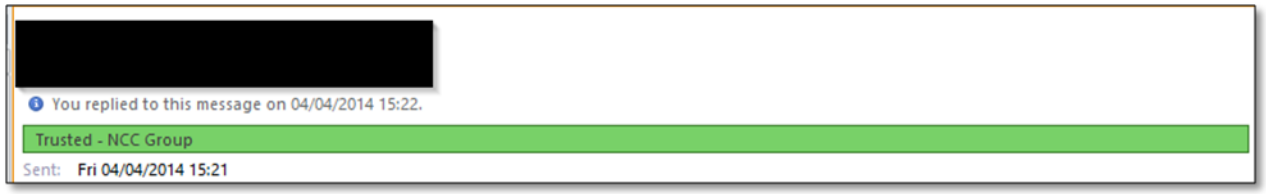
How Can You Protect Yourself?

- Ensuring regular updates are installed
  - Operating systems
  - Mail & document clients
  - Anti-virus & security packages
  - Third party software
- Implement endpoint protections and configure them correctly
  - Web & mail filtering software
  - Application whitelisting software
  - Proxy & Network traffic monitoring software
- Ensure Firewall rules are correctly configured, allowing only trusted traffic

How Can You Protect Yourself?

- Use mailbox categorisation techniques and rules
  - Microsoft's Outlook allows categorisation by colour used in conjunction with rules can aid with identifying addresses within the internal address book





How Can You Protect Yourself?

- Develop a security awareness program
  - Develop security policies
  - Conduct annual security awareness training
  - Carry out annual phishing and social engineering assessments
  - Publicise security awareness within the organisation
  - Award those who point out issues

nccgroup
freedom from doubt

Any Questions or Queries?

shaun.jones@nccgroup.com

nccgroup
freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Milton Keynes

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

North American Offices

San Francisco

Atlanta

New York

Seattle

Austin

Australian Offices

Sydney