電子郵件社交工程與防護

計算機與通訊中心
網路系統組 陳怡碩
E-mail：yschen@cc.nthu.edu.tw
分機：31234

新聞事件

- 國安局被駭？木馬竄立院—03/27/2011聯合報
- 行政院社交工程演練擴及工友—08/24/2010 iThome
- 駭客偽冒行政院院長室發送社交工程攻擊信件 — 08/05/2010國家資通安全會報 技術服務中心
- 大陸駭客以台灣企業電腦當跳板，入侵Google與數十家美國企業；教育部品德教育網被大陸駭客入侵；中央健保局遭疑似植入木馬程式 – 08/2010 天下雜誌「大陸駭客 台灣練兵」
- Twitter、Facebook遭駭客攻擊（「阻斷服務式攻擊」denial-of-service）— 工商時報08/08/2009

新聞事件

- 社交網站成為網路犯罪目標 — 08/09/2009 大紀元新聞網
- 美國FBI遭中國社交工程攻擊 技術始終不敵人性— 資安人6/22/2009
- Fortinet 7月網路威脅報告 電子賀卡垃圾郵件充斥網路世界
  - 電子賀卡垃圾郵件主要是利用直接連結、Google 網上論壇和 Tinypic 相片分享服務做為散佈工具
  - MS ActiveX Video 控制項弱點，微軟於 7 月 14 日發佈了修補程式 MS09-032
- Flash 0day漏洞攻擊首現中國網際網路— 鉅亨網新聞中心 07/30/2009

校內常見詐騙郵件主旨

- Dear EDU.TW Webmail account owner
- Dear Webmail Subscriber
- Dear MX WebMail User
- Important Notice From Help Desk
- …

社交工程介紹

社交工程

- 社交工程的定義
  - 利用人性弱點或利用人際之信任關係來進行詐騙，是一種非“全面”技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。
  - 網路世界的數位安全(Secrets & Lies: Digital Security in a Networked World)的作者Bruce Schneier曾提到所謂社交工程，全都是由人性方面，也就是利用所謂的「信任」來進行。
  - 欺騙的藝術(The Art of Deception)的作者（Kevin Mitnick），更進一步的解釋到人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。
  - 以人為本、騙術為主
  - 技術門檻低
  - 貪心、好奇
  - 缺乏警覺性：有那麼嚴重嗎？

社交工程攻擊的定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法。
- 早期社交工程是藉由電話或假扮身份問些看似無關緊要的問題等各種方法來獲取所需資訊。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

應用社交工程的各種攻擊方法

- 電子郵件隱藏電腦病毒
- 網路釣魚
- 圖片中的惡意程式
- 偽裝修補程式
- 即時通也是社交工程的新途徑

常見網路攻擊（一）

常見網路攻擊（二）

現在網路攻擊模式

電子郵件社交工程的攻擊步驟

- 有心人設計陷阱或後門程式
- 在電子郵件內放置有害程式或連結
- 將信件寄給特定或不特定對象
- 使用者開啟信件
- 啟動或下載有害程式
- 反向輸出使用者資料（轉眼變成受害者）

軟體弱點與零時差攻擊

- 只要是軟體就可能存在有弱點，未能及修補的話，就可能遭利用被入侵成功。
- 針對軟體弱點未修補前，出現針對弱點的攻擊行為，及稱為「零時差攻擊」。

常見被利用的軟體弱點

- 微軟的作業系統和文書軟體
  - Microsoft office（word）
- 常見的應用軟體
  - Winrar、adobe reader、flash player等軟體

電子郵件社交工程的手法

- 網路釣魚(Phishing)
  - 常見的社交工程，特別是利用email來欺騙，Phishing並不是一個新的攻擊手法，然而發生的頻率卻在過去幾年中逐漸增加。
  - 偽造網址：http://www.hinet.net ←→ http://www.hinet1.net
  - 偽造網頁：製作與原來完全一樣的頁面，以騙取重要的相關資訊。
- 利用郵件夾帶惡意程式或惡意連結進行攻擊。
- 運用各種人性弱點吸引使用者開啟有問題信件
  - 興趣、貪心、關心的時事、最美獸醫…

99年下半年度教育部電子郵件社交工程演練結果（一）

組別	信件類別	信件標題
Letter 1	生活類_台電帳單_教育部	台電烏龍帳單頻傳！你有注意過你家的電費是否合理嗎?
Letter 2	知識類_雞與蛋_教育部	到底是先有雞還是先有蛋！？答案公佈了！
Letter 3	科技類_透明手機_教育部	全世界第一支全透明手機！未來的新趨勢~
Letter 4	美女類_世足_教育部	世足正妹比一比！你最喜歡哪位！
Letter 5	美容類_夏日四大困擾_教育部	女生不可不知的夏日四大困擾
Letter 6	旅遊類_金門_教育部	【HiNet旅遊網】開學旅遊團 超低價好康!!
Letter 7	旅遊類_鐵道_教育部	鐵道迷的麥加！　國定古蹟－下淡水溪鐵橋
Letter 8	時事類_公務員制度_教育部	公務員退休制度超級比一比！
Letter 9	健康類_飲料_教育部	炎炎夏日，喝杯清涼的飲料最爽快！但是你知道什麼飲料會讓你越喝越肥嗎?
Letter 10	教育類_指考_教育部	明年指考 單選題可望取消倒扣
Letter 11	趣味類_睡相_教育部	睡要有睡相！你沒看過的精采睡相....

99年下半年度教育部電子郵件社交工程演練結果（二）

99年下半年度教育部電子郵件社交工程演練結果（三）

100年上半年度教育部電子郵件社交工程演練結果（一）

編號	信件類別	信件標題
Letter 1	旅遊圖片類	【HiNet 旅遊網】深度旅遊團　超低價好康！！
Letter 2	生活類	五月報稅天　網路報稅讓麻煩省一半！
Letter 3	知識類	超重要！不要再相信網路謠言「生命三角」
Letter 4	科技類	台灣之光！日內瓦展 我發明奪42金 世界第一！
Letter 5	美女類	大陸美女-范冰冰 為了拍MV露點也願意！
Letter 6	美容類	完美牙齒整型　五大注意事項
Letter 7	旅遊類	騎鐵馬逛八里 便道成車道 車友爭相樂活
Letter 8	時事類	從日本核災看輻射線對眼球的影響！
Letter 9	財經類	凍漲七年 軍公教終於要加薪了！
Letter 10	健康類	外食族 如何吃得更健康？超商減肥法！
Letter 11	新奇類	巨無霸高麗菜　重30臺斤超吸睛

100年上半年度教育部電子郵件社交工程演練結果（二）

100年上半年度教育部電子郵件社交工程演練結果（三）

100年上半年度教育部電子郵件社交工程演練結果（四）

行政單位

單位	人數
總務處	28
研究發展處	19
圖書館	12
教務處	10
共同教育委員會	8
秘書處	7
會計室	7
學生事務處	5
國際事務處	3
清華學院	1
計算機與通訊中心	1

教學單位

單位	人數
材料科學工程學系	4
化學工程學系	3
動力機械工程學系	3
物理學系	3
生命科學院	3
電機工程學系	3
EMBA	2
MBA	2
人文社會學院	2
工程與系統科學系	2
生醫工程與環境科學系	2
工業工程與工程管理學系	2
資訊工程學系	2
中國文學系	1
核子工程與科學研究所	1
工學院學士班/工學院	1
理學院	1
化學系	1
生命科學系	1
資訊系統與應用研究所	1
電子工程研究所	1

電子郵件社交工程的防護

電子郵件社交工程的防護

- 基本的防護
  - 作業系統更新
  - 應用軟體更新
  - 防毒軟體、個人防火牆
- 再多一點的防護
  - 調整收信軟體的部分設定（outlook 2007、outlook express、live mail）
  - 熟悉所使用軟體基本設定
- 近乎完美的防護
  - 改變使用習慣

基本的防護

- 作業軟體更新
  - 設定自動更新 microsoft update
- 應用軟體更新
  - Adobe reader…等軟體
- 安裝防毒軟體、個人防火牆並更新病毒碼
  - 卡巴斯基、賽門鐵克、趨勢（學校授權）

再多一點的防護

- 變更看信軟體的設定，提高安全性
  - 不自動下載圖檔
    - outlook2010
    - outlook 2007
    - live mail
    - outlook express
  - 關閉信件預覽功能
    - outlook2010
    - outlook 2007
    - live mail
    - outlook express
  - 以純文字開啟信件
    - outlook2010
    - outlook 2007
    - live mail
    - outlook express

Outlook 2010

- 開啟outlook 2010
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選取【自動下載】
- 將【不自動下載HTML電子郵件訊息或RSS項目中的圖片】打勾

Outlook 2007

- 開啟outlook 2007
- 選取【工具】
- 選取【信任中心】
- 選擇【自動下載】
- 將【不自動下載HTML電子郵件訊息或RSS項目中的圖片】打勾

Outlook express

- 開啟 outlook express
- 選取【工具】
- 選取【選項】
- 選取【安全性】
- 將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾

live mail

- 開啟 live mail
- 選取【工具】
- 選取【安全性選項】
- 選取【安全性】
- 將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾

outlook 2010

- 開啟outlook 2010
- 選取【檢視】
- 選取【讀取窗格】
- 選擇【關閉】

outlook 2007

- 開啟outlook 2007
- 選取【檢視】
- 選取【讀取窗格】
- 選擇【關】

Outlook express

- 開啟 outlook express
- 選取【檢視】
- 選取【版面配置】
- 【顯示預覽窗格】不打勾

live mail

- 開啟 live mail
- 選取【檢視】
- 選取【版面配置】
- 【顯示預覽窗格】不打勾

Outlook 2010

- 開啟outlook 2010
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選擇【電子郵件安全性】
- 將【以純文字讀取所有標準郵件】打勾

Outlook 2007

- 開啟outlook 2007
- 選取【工具】
- 選取【信任中心】
- 選擇【電子郵件安全性】
- 將【以純文字讀取所有標準郵件】打勾

Outlook express

- 開啟 outlook express
- 選取【工具】
- 選取【選項】
- 選取【讀取】
- 將【在純文字中讀取所有郵件】打勾

live mail

- 開啟 live mail
- 選取【工具】
- 選取【選項】
- 選取【讀取】
- 將【在純文字中讀取所有郵件】打勾

近乎完美的防護

- 改變使用電子郵件的習慣
  - 查明信件的來源
    - 信件可由mail header查出所經的伺服器
  - 釐清寄件者身分
    - 以電話向寄件者確認
    - 郵件驗證機制
    - 附件加密
    - …

Mail header

Retu
X-Or
Deliv
Rece

Rece

Rece

From
To: Y

Return-Path: <vipmember@infoarray.tw>
X-Original-To: OOO@mx.nthu.edu.tw
Delivered-To: OOO@mx.nthu.edu.tw
Received: from cp1.oz.nthu.edu.tw (cp1.oz.nthu.edu.tw [140.114.63.141])
by cc.nthu.edu.tw (Postfix) with ESMTP id AA6BA56C76
for <ptlin@cc.nthu.edu.tw>; Thu, 2 Jul 2009 13:56:42 +0800 (CST)
parts
Received: from mail.communicatearea.tw [(210.67.251.27)] by cp6.oz.nthu.edu.tw
(envelope-from <vipmember@infoarray.tw>)
(NTHUCCC AntiSPAM Mail Server with TLS)
with ESMTP id 577192816; Mon, 18 May 2009 06:55:06 +0800
Received: from mailsystem ([192.168.255.100])
by mail.communicatearea.tw (8.13.8/8.13.8) with ESMTP id n4HMs4w7018426
for <OOO@mx.nthu.edu.tw>; Mon, 18 May 2009 06:54:06 +0800
X-ssage-ID: <7141115.1242600903628.JavaMail.SYSTEM@mailsystem>
Date: Mon, 18 May 2009 06:55:03 +0800 (CST)

結論

- 兩不看
  - 來源不明的信不看
  - 不認識寄件者不看
- 不衝動
  - 對於自己有興趣、有吸引力....等信件

- Q & A