詐騙技術淺析

該如何抵禦進階攻擊者

白皮書

聲明：此文件由賽門鐵克 (Symantec) 統籌之後發佈，並接受下列企業的支援或間接合作而成：

作者： Ashok Banerjee、Torry Campbell
撰寫人：Balaji Prasad、Alpesh Mote、Spencer Smith、Shireen Rivera

Symantec™
A Division of **Broadcom**

目錄

背景

截至 2021 年止，網路攻擊者預估將於全球造成六兆美金的損失。另預估 2017 到 2021 年間的抵禦網路攻擊成本，也將高達一兆美金。攻擊者時間充裕且策略多變，不斷針對企業常用的靜態網路與端點防禦方式，設法找出弱點下手。詐騙技術可搭配端點與網路防護功能，根據各種環境自訂並新增動態安全機制，讓攻擊者優勢不再。

雖然端點與網路安全可保護您免於遭到入侵，但詐騙技術更能提早偵測並察覺攻擊者的意圖，降低影響之餘更能加快反應速度。端點與網路安全用於攻擊者在漏洞發生之前的技術，詐騙技術則用於攻擊者在漏洞發生之後的意圖和行動。根據安全研究中心 Ponemon Institute 發佈的最新報告，攻擊者平均躲藏 191 天後才會被偵測到；而詐騙技術就是要積極找出潛藏在您網路中的攻擊者所設計。詐騙技術可誤導攻擊者，中斷其攻擊流程與決策，快速找出攻擊者所在位置以縮短躲藏時間，進而防止他們完成攻擊目標。詐騙技術現已是 Symantec Endpoint Protection (SEP) 系列的內建功能，可為您的多層式防護機制再添動態功能。

詐騙技術之演變

詐騙技術並非新概念。綜觀歷史，你可以看到大自然和戰爭事件中的詐騙實例。有許多動物演化出自己的偽裝技巧，瞞過掠食者的眼睛而免於遭到捕食；更有許多世界聞名的戰爭策略也是透過欺騙而克敵成功 (如特洛伊木馬屠城)。若提到網路安全，詐騙技術則可誤導攻擊者進行他們原本目標以外的事情。

網路安全的詐騙技術，本由簡單的網路誘捕帳號起家。這些誘捕帳號會模擬一部分的系統功能，雖然不是所有攻擊者都會上當，但足可愚弄一些新手。但有限的功能 (例如資料庫雖然具備多個關聯式資料集，但卻無法大量上傳) 讓系統易於遭識破。企業可試著改善這種誤導，並部署更大量的誘捕帳號 (通常稱為蜜網或蜜場) 吸引攻擊者接觸，且在完全不同的隔離子網內增加了功能和互動複雜度。

假網路的可信度越高，就越有機會吸引攻擊者進入互動，進而免於真正的資訊遭到攻擊。可惜的是，這種誘捕陷阱需要極大量的時間與專業知識，才能部署、管理、維護所有的軟硬體，建立可信度高的隔離子網以及其內的假造憑證、資料庫、網路伺服器、可入侵的系統與內容。也因為如此，許多企業並無法架設並維護這類的誘捕蜜網。

為了在各個端點布置詐騙技術，企業往往依賴端點的可達性 (reachability)。這種依賴性很快就讓防火牆、代理、網路位址轉換 (NAT)，或虛擬私人網路 (VPN) 背後的端點既複雜又難以操作。由於在大型的分散式環境中，極難以在端點上部署並監控詐騙技術，因此大多數的廠商都將重點放在網路詐騙技術。

但是賽門鐵克解決了傳統詐騙技術解決方案的問題，讓端點安全機制可同時保護端點免受攻擊，並主動偵測已經在端點上的攻擊者。賽門鐵克目前已經保護超過 27 萬名客戶的 1.25 億個端點；且所有客戶都能和賽門鐵克合作啟動詐騙技術，並部署已內建於 SEP 系列中的高互動性誘捕陷阱，大幅提升攻擊偵測功能。

因為您才知道自己重要資產的所在，你更能利用此優勢來誤導攻擊者避開企業。您可以在環境中部署多樣的「誘餌」，如假檔案、假憑證、假網路共享、假快取項目，以及假端點，欺騙攻擊者進入而讓自己曝光與其攻擊目標：

- **假檔案**：您可建立假檔案引誘攻擊者開啟。試想名為「ConfidentialMerger.doc」或「FundraisingCycle.doc」的檔案，在您的桌上型電腦上有多麼誘人，或是人資伺服器上的「Salary.xls」檔案也特別吸引注意。類似的選擇無窮無盡。
- **假憑證**：您可建立假密碼並散佈到系統之中，以輕鬆找出攻擊者。任何使用假密碼的行為都能視為惡意活動。高互動性的進階詐騙技術系統，則可讓攻擊者使用假密碼登入受控制的系統，在互動之後隨即暴露自己的策略與真正意圖。
- **假網路共用**：您可在桌上型電腦上使用假的網路共用，引用攻擊者與資源互動而暴露自己的行蹤。和假網路共用的任何互動，如點擊開啟、複製檔案等都能算是攻擊行為。
- **快取項目**：您可透過如 DNS 快取、遠端存取工具快取 (RDP, VNC) 等的假快取項目，誤導攻擊者並找出其真正目標。
- **假端點**：您可在網路上設定假的可見節點，引誘攻擊者嘗試遠端存取。因為此為假端點，所以任何企圖存取的行為都是攻擊行為。

是否需要詐騙技術

一旦其他多樣的防護機制已經到位，為何仍需要詐騙技術？因為您必須兼顧所有的基礎設施。攻擊者越來越卑鄙。滲透網路的最佳方式，就是竊取使用者的憑證。此外，攻擊者也會使用已經安裝於目標電腦上的工具。這類「自給自足」策略，往往不會載入惡意軟體，也不會在裝置硬碟中建立新的檔案，而是直接於記憶體中執行。而且目前的攻擊層面不斷翻新。

為了抵禦攻擊，您必須建構多樣機制，協助您斷絕攻擊者的任何可乘之機，並封鎖某些正使用中的攻擊媒介：

1. **社交元件**
   a. 根據 2017 資料外洩調查報告 (Data Breach Investigations Report)，共 42,068 件資安事端中有 43% 是與社交工程攻擊有關。
   b. 「人」親手攻擊預估在 2020 年達到 40 億次。企業脫離不了與員工、合作夥伴、契約商、供應商、客戶之間的互動。這些人都有機會存取企業資源並滲透資料，不論有意或無意皆然。
   c. 有三分之二受訪的技術專家指出，企業面臨的最大威脅即在於網路釣魚/魚叉式網路釣魚，以及社交工程攻擊。攻擊者透過釣魚攻擊取得必要的憑證，再獲得所需的資訊，而且沒有其他可協助及早發現的攻擊手法。
   d. 56% 的電子郵件使用者，還有 40% 的 Facebook 使用者，往往會點擊由不知名寄件者所傳來的連結。

2. **技術漏洞**
   a. 99% 的電腦均有漏洞，易於遭到刺探攻擊 (未修正的作業系統或軟體)。
   b. 超過 75% 的合法網站都有未修正的漏洞。

3. **端點弱點**
   a. 可能並非所有端點均部署了端點防護 (意外狀況)。

4. **錯誤設定**
   a. 防護往往過期未更新，讓資產暴露出易於攻擊的漏洞。
   b. 專為防護設計的功能可能遭關閉。

詐騙技術可再加上一層防護，提高發現攻擊者的機會。您可迅速且輕鬆地在企業中佈下無數誘餌，如假憑證、假檔案、假可入侵端點、假重要資產等，吸引攻擊者進入並暴露自身行蹤。詐騙技術可補上其他安全技術的缺點，以防禦性的策略發現後續攻擊行為。

攻擊流程

大部分的安全技術，均是為了找出並遏止早期攻擊行為所設計，但詐騙技術則是針對後續的攻擊階段而最佳化。根據下列簡化的攻擊程序，大部分的安全技術均針對步驟 1、2、3、6；而詐騙技術則專注於步驟 1、4、5、6，期能找出已經存在於網路中的攻擊活動：

1. **偵查** – 攻擊者先發掘攻擊層面，找出建構環境所用的系統、服務、應用程式、人員、廠商等等。

2. **傳送** – 攻擊者擬定並送出攻擊。傳送行為往往透過電子郵件釣魚、電子郵件附件、惡意連結、水坑攻擊、USB 隨身碟，或其他可移除磁碟而完成。

3. **刺探攻擊** – 在網路中發動攻擊。

4. **執行** – 攻擊者完成攻擊步驟。一般可分為：
   - **建立持續性 (Persistence)** – 即使已經被發現攻擊要素，還是能讓攻擊者繼續待在網路中。例如讓後門程式 (reverse shell) 在系統重新開機之後仍留著。只要設計出應用程式的轉接介面 (application shimming)，或將之嵌入在啟動項目、登錄、Windows Authentication 封包中，就能達到此目的。
   - **提高權限** – 可能需提高權限，才能存取重要資產。所使用的技術可能包含存取 Token 操作、AppInit DLL、應用程式轉接介面、DLL 插入、啟動背景程式 (Daemon) 等。
   - **指令與控制** – 基於各環境有所不同，攻擊者必須有一般用途的遠端存取工具 (RAT) 或後門程式 (reverse shell)，先瞭解環境之後再規劃後續行動。指令與控制流量一般均經過加密，並在 HTTP 或 IRC 中建立通道，避免遭到防火牆偵測。

5. **橫向移動** – 攻擊者漫遊在內部網路中，尋找重要資產。同時可能會使用所取得的憑證 (透過權限提升)。

6. **洩漏** – 一旦取得重要資料，均會先加密過再傳送出去。攻擊者使用的加密機制，通常會跟著企業的加密偏好和使用的工具。洩漏時，往往同樣將資料上傳至企業所用的雲端服務，如 Box、Dropbox、Google Drive 等。

藝術性質多於科學性質

詐騙技術的藝術性質高於科學性質，可說是規避與反規避的遊戲。重點就是讓誘餌綁在您的環境之中，讓攻擊者和其互動並暴露自己的行蹤。支援賽門鐵克詐騙技術的 Symantec Cyber Security Services (CSS)，極適於持續監控威脅與資安事端應變專業知識；另可透過 Symantec Consulting Services 為您自訂詐騙技術部署方式，以找出最適合您環境的戰術、技術、流程 (TTP)。兩者可一同支援：

- 部署並自訂初始誘餌，嵌入在您的環境中。
- 橫跨您的內部部署與雲端環境，全年無休地監控由 SEP Deception 及其他裝置所觸發的警示 – 若確認發生重要資安事端，隨即由 CSS SOC 分析師聯絡您 (10 分鐘 SLA)，並提供攻擊細節、受影響的資產，及任何建議採取的行動。
- 資安事端應變一般會封鎖整個侵入路徑，因此往往必須進行鑑識與 EDR 分析。
- 關閉反饋迴圈，以持續改良誘餌並最佳化部署。

總結：賽門鐵克為您帶來最現代的詐騙技術

詐騙技術可填補常用安全技術的缺漏，健全您的企業防禦工事，讓攻擊者無所遁形。透過 Symantec Endpoint Protection Manager，賽門鐵克讓您能自訂誘餌，輕鬆部署於環境之中，找出躲藏於網路中的攻擊者，並在其達到目的之前就阻止他們。且由於詐騙技術使用相同的單一 Symantec Endpoint Protection 代理程式與管理主控台，因此解決方案已完成最佳化，不致對既有效能產生實質影響。賽門鐵克的詐騙技術，可解決困擾廠商已久的端點可達性 (reachability) 問題。有了賽門鐵克，您不需鬆綁防火牆的規則，或使用易遭入侵的端點服務，更不需處理、管理、監控其他附加硬體。只要啟動詐騙技術，為大型分散式環境中的端點添加誘餌即可。只要在端點上置放實際的誘餌，即可大幅提高攻擊者上鉤的可能。因為是誘餌，任何人只要嘗試假遠端連線、假憑證、假檔案、假網路共享等的誘惑，就沒有任何合法的理由，而且您也能確認有了攻擊者。誘餌均經過 Symantec Cyber Security Services 的專業微調、監控、改善。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號
電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw