Maneuvering Around Clouds: Bypassing Cloud-based Security Providers

✧ Summary

DDoS 攻擊的氾濫，令許多企業開始尋求與 CBSP(基於雲端的安全提供商)合作，至少約七成皆採用 DNS rerouting 方式將流量導向 scrubbing center 進行清洗，如此作法令企業**不需修改網站、購買硬體設備且可以快速啟用或停用**。然而如此做法也令企業可能存在 origin-exposing 的風險，本篇結合於 Black Hat USA 2013 的四種做法，並提出四種新做法，來繞過 CBSPs 的防護。同時，本篇亦選擇五個著名服務供應商(CloudFlare、Incapsula、DOSarrest、Prolexic、Sucuri)，結合 **CloudPiercer** 自動化原始 IP 檢測系統，評估擁有適當的 DNS 配置，並且屬於 Alexa 的前 100 萬個網站，對八種攻擊手法的影響層面，並**衡量、驗證潛在風險**。

最後在文末也提出可採用的**對策**，以及使用 CBSP 緩解服務企業所可進行的設定。

✧ Strengths

因 DDoS 可改為使用 IP 而非域名來攻擊目標伺服器，因此若能知道攻擊者目標 IP 位址，任何透過 DNS 更改 record 的 scrubbing center 皆可被繞過。八種攻擊手法包含 **IP History、Subdomains、DNS records、Temporary exposure、SSL certificates、Sensitive files、Origin in content、Outbound connections**。

透過 IP 歷史紀錄資料庫，可找出目標網站網域所可能曾經使用過的 IP，因僅更改 DNS record 為重設 IP 而仍可遭受攻擊。目標網站相關子域為了不打破特定協議，而將部分網站設置值皆解析至原始子域，而可能洩漏 IP 位址資訊，攻擊者可以直接使用，或作為跳板來猜測易受攻擊的位址。DNS 紀錄也可是攻擊之處，某些網站可能僅更改 A、CNAME record，然而 MX(電子郵件紀錄)、SPF 或其他 DNS record 可能仍會洩露網站伺服器的 IP 位址。而機敏文件，管理員可能忽略一些敏感資訊的權限控管或其他開發日誌文件的訪問，而洩漏如 php 文件訊息。Ping Backs 可以利用驗證機制觸發網站的 outbound connection，而可連結上原始伺服器。其他尚如 SSL 證書，可利用 *ZMAP* 掃描所有 IP 位址並獲得所有 SSL 證書，便可從中找到 domain 與 IP 之間的關聯。

✧ Weaknesses

本篇攻擊手法基本上皆基於 **DNS rerouting**，因此若可改為使用 BGP routing 來保護整個網路便可相當程度的解決本篇問題。然而此方法有賴於企業需擁有大量自己的 IP 位址(透過硬體並擁有至少一個 class C 位址)，並且須具有足夠的財務與技術能力來安排整個網路架構服務。雖這對一般中小企業救難做到且會增加額外複雜性，但最能解決 origin-exposing 問題。

在 CBSP 服務防禦方面，企業可以調整對外防火牆的設定，僅允許來自 CBSP 的流量，同時更改原始 IP 的位址。此外，CBSP 也可以自行部署類似 CloudPiercer 的工具，主動掃描客戶域名以了解目前暴露的風險，提高警覺心並協助網站管理員修復潛在漏洞。

✧ Reflection

事實上本篇所提出的攻擊手法難度都不會太高，但若要完全解決 origin-exposing 問題實務上難度還是比較高的。管理者需要考慮到各方面，注意每個環節可能的漏洞。管理者或許可以自行進行例行性地測試 DDoS 緩解現況；時常檢查域名紀錄，查看攻擊者可能會拿來利用的內容；定期掃描伺服器上的 URL、標頭、原始碼內容等等是否會暴露伺服器的 IP 位址等等。

儘管如何處理基於 DNS 的 DDoS 攻擊防護是一件極具挑戰的事，但從實現的角度看，企業目前仍可以採取相關措施，確保透過 CBSP 能得到他們期望的防護。網站管理者需了解 origin-exposing 風險為何，對其以及 DDoS 攻擊防護服務皆進行模擬測試，並評估過濾與檢測機制，如此企業才得以在這一塊保持領先地位。