TLP:WHITE

網頁置換事件的背後隱憂

Announcement Advisory Report（ANAR）

2017-12-12

TWCERTCC-ANAR-2017012

Summary

- 網頁置換(Defacement)攻擊行為是受害網頁之外觀遭竄改，TWCERT/CC關注 zone-h 平台有關台灣遭駭部分並通報相關單位，截至 106 年 12 月已有三萬多筆網頁遭置換紀錄。
- 一般企業的網站若遭網頁置換時，企業的修補方式經常只是移除或修訂該網頁的安全弱點，並未檢視該系統或主機是否存在其它漏洞，或是否已遭植入惡意程式。
- 根據 TWCERT/CC 分析，有部分網站當網頁遭置換並公布於 zone-h 時，也被其他單位(PhishLabs、Netcraft 等)通報為釣魚網頁，企業在發現網頁遭置換時，不該僅排除遭置換頁面的安全問題，應該全面檢視網站全系統是否有其它安全問題，並強化防護作為。

Description

網頁置換(Defacement)是一種網頁攻擊，一般攻擊方式為駭客入侵受害網頁伺服器並將受害設備之原網頁替換成其它駭客自製的網頁，常見於有政治動機的「網路抗議者」、激進駭客用來傳播訊息[1]或是用以炫耀技術、戰績，例如知名的網頁置換揭露平台 zone-h，擁有大量國際駭客所分享之成功攻陷並置換的網頁快照資料庫，遭到網頁置換之主因通常為網站或伺服器設備出現漏洞，因此遭駭客侵入與控制。

台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC)，於 2017 年初即開始關注台灣地區遭公布於 zone-h 上受駭網頁的情資，並將結果通報相關負責單位修訂，至 2017 年 12 月 22 日，zone-h 網頁置換揭露平台資料庫中遭置換網頁之受害網域屬「.tw」者，總計有 39,264 組，其中不重複之 IP 計有 16,575 組，且有 22,689 組為單一伺服器上之其他網頁被入侵，這常發生在虛擬網站伺服器上，只要單一的服務出現漏洞，整個伺服器上之網頁都可能受害[2][3]，如下圖 1。

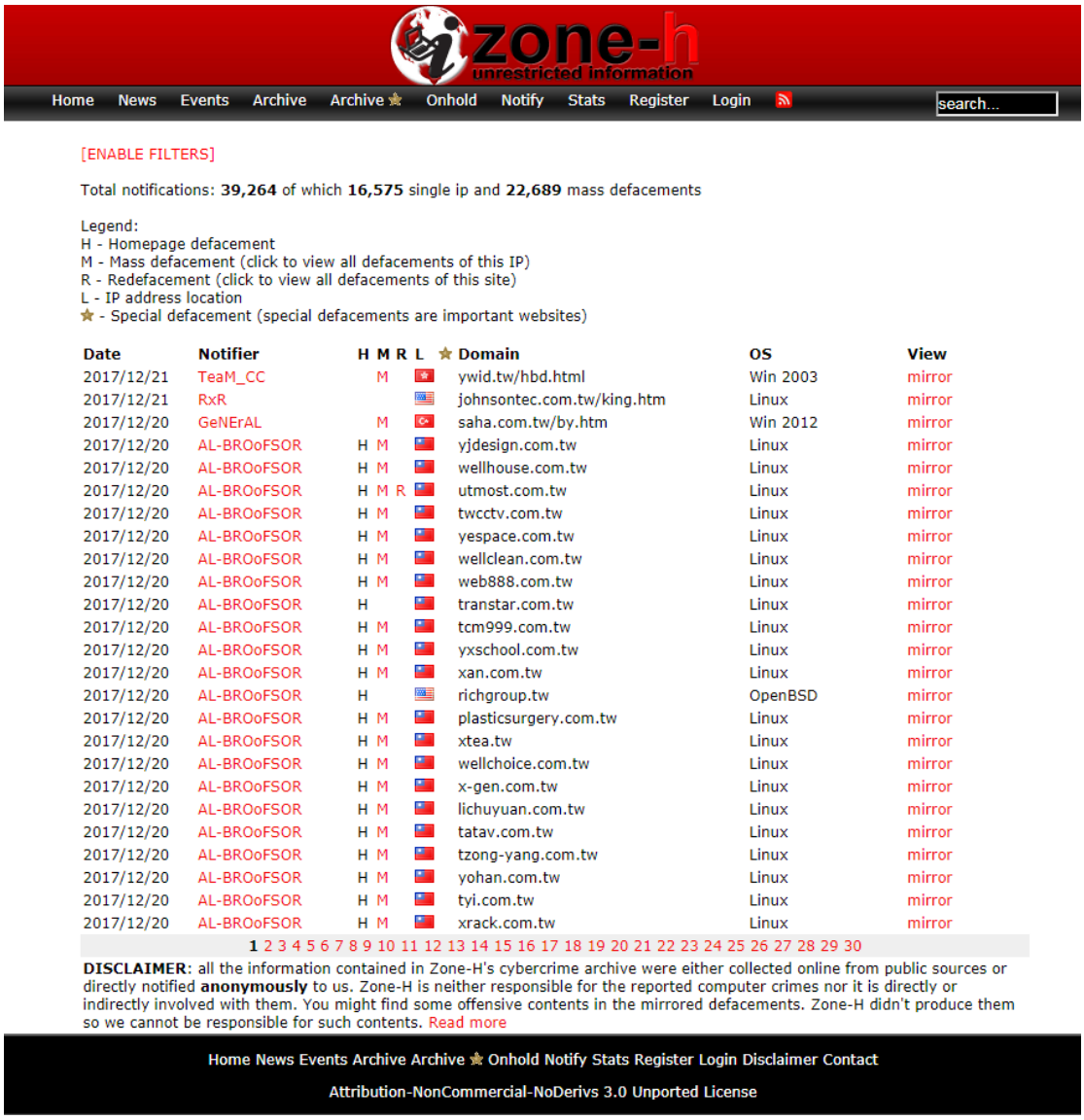

圖 1. zone-h 網頁置換揭露平台以「.tw」搜尋條件結果畫面(2017/12/22)

依據 TWCERT/CC 以往通報經驗，常見到當企業接到網頁遭置換通報時，只是移除或修訂該網頁的安全弱點，更有媒體在報導上表示此類攻擊通常不會造成受害者的金錢損失或是資料外洩，只會因網頁遭置換的狀況曝光於網路，而造成受害者的名譽損失[4]。

然而網頁置換攻擊表面上看來只是駭客單純的惡意行為，但背後真正的問題在於網頁伺服器既然能被駭客侵入，就有可能被置換成為釣魚網頁、植入後門或惡意跳轉程式，駭客可以透過釣魚網頁連結，引誘一般使用者訪問看起來和受害網站相仿，或甚至看似為其他網路服務的特製網頁，並要求他們提供私人資訊，導致使用者受騙或遭利用，而一旦受害網站被認定為具有網路釣魚的網站，便可能遭防毒軟體或防火牆系統將其列入黑名單，致使受害單位網站遭受牽連，造成

單位業務推展不利甚至信譽受損進而影響商業利益等情事[5]。

TWCERT/CC 彙整 2017 年 1 月至 11 月通報紀錄，分析流程示意圖如下圖。

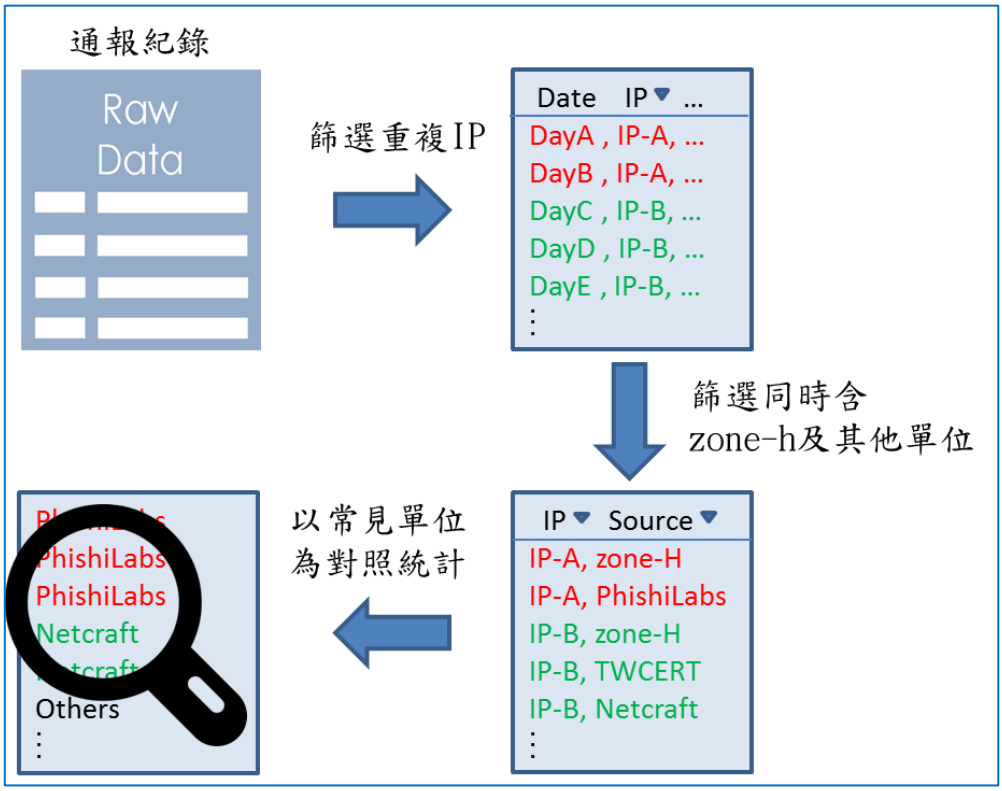

圖 2. 通報紀錄中 zone-h 分析流程示意圖

分析紀錄中通報 IP 重複出現一次以上之資料，並篩選出該資料之通報來源同時包含 zone-h 揭露平台及其他單位之紀錄共計 18 組，並與通報紀錄中常見的釣魚網站通報單位 Phishlabs 及 Netcraft 對照分析統計如下表 1 及下圖 3 所示：

1. 通報來源同時包含 Phishlabs 共計 10 組(6 組為 Phishlabs 通報，加上 2 組同時包含 Netcraft、2 組同時包含其他通報單位：法國 CERT 及美國某資安公司)。

2. 通報來源同時包含 Netcraft 共計 8 組(4 組為 Netcraft 通報，加上 2 組同時包含 Phishlabs、2 組同時包含其他通報單位：法國 CERT 及美國某資安公司)。

3. 綜上所述，通報來源同時包含 Phishlabs 及 Netcraft 共計 4 組，2 組同時為 Phishlabs 及 Netcraft，2 組為其他通報單位(法國 CERT 及美國某資安公司)，其網路所有者為民間 ISP 業者及學術網路。

4. 排除 Phishlabs 和 Netcraft 等常見釣魚網站通報單位之其他單位通報紀錄共 4 組，1 組為 HITCON ZeroDay 通報網頁有弱點，其餘 3 組分別為芬蘭、巴西 CERT 通報為釣魚網站以及由 TWCERT/CC 通報人員發現網頁資料洩漏。

表 1. 重複通報 IP 包含 zone-h 及其他通報單位統計表

重複通報 IP 包含 zone-h 及其他通報單位統計表			
	單位	IP 組數	事由
常見通報單位	Phishlabs	6	釣魚網頁
	Netcraft	4	釣魚網頁
同時包含 Phishlabs 及 Netcraft	Phishlabs 及 Netcraft	2	釣魚網頁
			釣魚網頁
	法國 CERT	2	釣魚網頁
	美國資安公司		釣魚網頁
其他	HITCON ZeroDay	4	網頁弱點
	芬蘭 CERT		釣魚網頁
	巴西 CERT		釣魚網頁
	TWCERT/CC		網頁資料洩漏

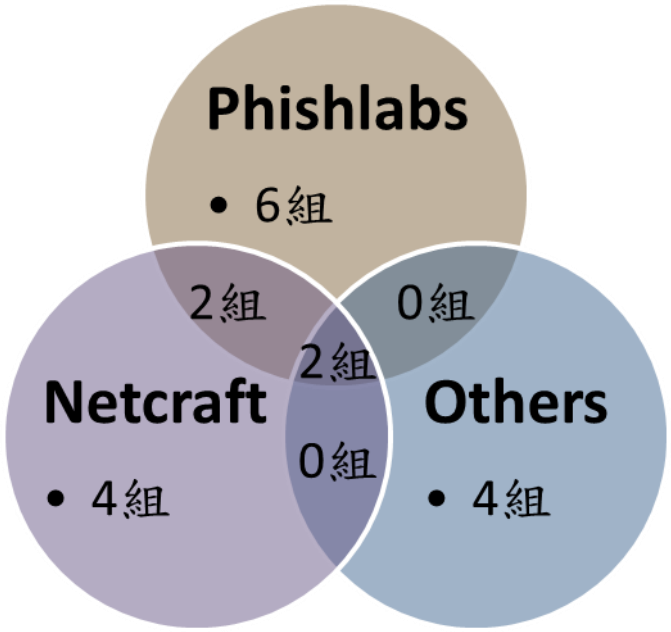

圖 3. 重複通報 IP 包含 zone-h 及其他通報單位統計

經分析發現，重複通報之 IP 有出現在 zone-h 且有其他單位通報之紀錄者，皆為網頁問題類型之通報，如網頁出現弱點遭 HITCON ZeroDay 揭露、TWCERT/CC 通報應變小組人員發現網頁機敏資訊外洩，以及 TWCERT/CC 國外固定合作夥伴 Phishlabs 和 Netcraft 及其他國家 CERT 或資安公司所通報之釣魚網頁。

由此證明，當網頁遭揭露於 zone-h 網頁置換平台時，確實有可能發生前述之背後隱憂，因此網站擁有者或維護者應將網頁置換攻擊視為警鐘，系統可能存在允許駭客變更網站資料的嚴重漏洞，若引發其他更多或更嚴重之入侵攻擊之情事，損失將會更大，企業如發現網頁遭置換應全盤檢視系統安全，並強化防護作為，否則如置之不理而遭植入惡意程式或連結而成為釣魚網頁，將會成為網路犯罪的共犯。

網站擁有者或維護者往往認為網站系統已經安裝最新的修補程式不會有弱點，然而系統漏洞與 Web 應用程式漏洞是不同層面[6]，網頁的安全性僅僅只是整體系統安全的其中一環，因此針對網站安全防護，TWCERT/CC 區分系統防護以及網頁應用安全部分提出以下建議。

I. 系統防護建議：

1. 網站伺服器的作業系統及應用程式務必安裝最新版的安全更新，並定期進行弱點掃瞄。
2. 安裝防火牆以及防毒軟體，並正確設定防火牆規則，保持防毒軟體掃毒引擎與病毒碼更新至最新。
3. 關閉不必要之網路服務，建立密碼時使用複雜度高之強密碼規則。

II. 網頁應用安全建議：

1. 網站開發時，應要求開發商納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)。
2. 網站上線後，應定期檢視網站建置環境及所使用之套件以及外掛程式等所屬廠商之更新支援狀況，並保持最新；如發現廠商公布不再支援更新修補，應即檢討可用性以及替換方案。
3. 當上線的網頁發生問題時(如遭置換網頁或被通報有弱點)，應即時修補相關弱點，全面檢視全系統的安全，並監控相關活動紀錄，以確認無其它的攻擊或惡意程式植入情事。

TWCERT/CC 將持續觀察網路上各資安情資平台，挖掘與台灣相關之攻擊或受害資訊並通報受害或權責單位即時進行應變處理，透過蒐整之情資分析研判資安趨勢，達到可向國際相關單位發布威脅預警情資之目標。平時則肩負國內民間資安意識與素養的宣導推廣之責任，除在官方網站、官方臉書粉絲專頁發布資安資訊外，亦積極透過舉辦研討會、說明會及設攤位方式，向民間及企業推廣資安的重要性，以期提升台灣民間整體資安意識。

References

[1] Wikipedia, Nov. 7, 2017, "Website defacement", Retrieved Dec. 11, 2017, from the World Wide Web: https://en.wikipedia.org/wiki/Website_defacement

[2] zone-h.org, Dec. 22, 2017 "Unrestricted information | Defacements archive", Retrieved Dec. 22, 2017, from the World Wide Web: http://www.zone-h.org/archive/domain=.tw

[3] nutsfactory, Apr. 7, 2006 "國際駭客發動網路戰", Retrieved Dec. 11, 2017, from the World Wide Web: http://blog.nutsfactory.net/2006/04/07/the-un-root-crew/

[4] 中時電子報, Apr. 5, 2017 "駭客攻陷台灣上百網站 上網刊登炫耀", Retrieved Dec. 11, 2017, from the World Wide Web: http://www.chinatimes.com/realtimenews/20170405002696-260412

[5] Cloudbric, Dec. 22, 2015 "Website Defacement: Suspicious Changes On Your Website", Retrieved Dec. 11, 2017, from the World Wide Web: https://www.cloudbric.com/blog/2015/12/website-defacement-suspicious-changes-on-your-website/

[6] 行政院國家資通安全會報, Mar. 30, 2006 "駭客攻擊手法分析與基本安全防護", Retrieved Dec. 22, 2017, from the World Wide Web: http://download.nccst.nat.gov.tw/attachfileold/366520060330164332.pdf

聯繫資訊

台灣電腦網路危機處理暨協調中心

- 免付費專線：0800-885-066
- 資安事件通報：03-4115387 或 02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站：https://twcert.org.tw/
- Facebook：https://www.facebook.com/twcertcc