資訊處
National Chung Cheng University
Office of Information Technology

資安事件宣導

SSH 暴力攻擊案例介紹

1. 本校實際案例
2. SSH 暴力攻擊簡介
3. 一般使用者防範方式
4. 伺服端防範方式

本校實際案例(一)

案例一：某日，校方收到學生反映之 E-mail

> 您好：
>
> 不知道我做了什麼，現在點中正大學的網頁都只會顯示 Blocked because of IPS attack，我使用的ip位置似乎被列為黑名單，我的ip位置為 x-xxx-xx-xx.dynamic-ip.hinet.net 麻煩您們處理了，謝謝！

本校實際案例(一)

經資訊處透過 IPS LOG 查證，該電腦疑似被植入木馬程式，透過SSH攻擊本校的網站。因此遭到本校網路安全系統識別為惡意攻擊，並進行封鎖。

#	▼Date/Time	Device ID	Severity	Source	Destination IP	Action	Service
1	08-02 11:00	FG1K5D3I17800884	high	[redacted]	140.123.35.5	dropped	SSH

本校實際案例(二)

案例二：資訊處收到學生反映無法連上學校的網頁

您好：

我是中正大學學生○○○，在近日租屋處的網路無法連上學校的任何網頁，原因顯示為：

An attack was detected, originating from your system.
Please contact the system administrator.

想請問您該如何解決這類問題？如有需要，這是我的IP位置：
XXX.XXX.XXX.XXX

學生：○○○

聯絡電話：XXXX-XXXXXX

本校實際案例(二)

經查詢防火牆紀錄，確認使用者電腦疑似被植入後門程式，透過SSH暴力攻擊本校的網站，因此被防火牆攔阻下來。

#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		09-09 19:23		[redacted]	tcp		dropped		SSH.Connection.Brute.Force

IP Address	Source	Created	Expires
[redacted]	IPS	2018-09-09 19:23:21	2018-09-10 19:23:21

什麼是SSH暴力攻擊

什麼是SSH暴力攻擊?

SSH是以帳號密碼登入遠端電腦主機進行工作的一種方式，SSH暴力攻擊是指駭客利用程式和字典檔，不斷地自動嘗試登入主機，直到成功取得登入權限。

由於SSH暴力攻擊持續大量丟出嘗試登入的封包，因此會對被攻擊的主機及相關的網路設備造成一定程度的負荷。

一般使用者防範方式

一般使用者可以利用以下方式，以防止在不知情的情況下，被植入惡意軟體而成為駭客利用作為SSH暴力攻擊的跳板：

1. 避免安裝來路不明的軟體。
2. 不使用來路不明的外接裝置。
3. 不隨意點擊未知來源的超連結。
4. 經常使用惡意軟體掃描程式保護電腦，
   例如：windows defender、防毒軟體……
5. 保持作業系統為最新版本。

伺服端防範方式

- 設定防火牆白名單

  設置防火牆白名單，限制可登入的網段，藉以避免攻擊者從外部或未知網域進行攻擊。

- 修改預設登入方式

  關閉 SSH 連線。
  關閉 root 外部連線功能，並新增其他帳號。
  修改 SSH 連接埠。

- 限制登入次數

  限制登入次數，可避免攻擊者進行大量猜測，大幅降低被攻擊的可能性。

資料參考來源

- SSH資安防護建議
  http://blog.pulipuli.info/2011/11/ssh.html