SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.03.18 (六) —— 2023.03.24 (五)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

知名駭客論壇 BreachForums 擔心遭到 FBI 盯上而關閉

自從其中一名管理員遭到逮補後，臭名昭著的 Breached 黑客論壇已經關閉，由於擔心遭到逮捕的管理員所擁有的設備遭到扣押並破解，因此將整個論壇網站下架，但目前該組織創立的Telegram 頻道暫時保留，可能會東山再起。

【資料來源：BLEEPINGCOMPUTER, 2023.03.21】

Python 撰寫的竊密惡意程式使用 Unicode 來逃避檢測

PyPI 套件庫中上架了一個惡意 Python 套件使用 Unicode 作為混淆技術來逃避檢測，同時竊取和洩露開發人員的帳戶憑證以及來自受感染設備的其他機敏資訊，利用Unicode 對於一個字母擁有多種變體的特性，撰寫視覺能夠辨識但編譯器無法解析的惡意程式來繞過檢測，請開發人員須小心注意。

【資料來源：BLEEPINGCOMPUTER, 2023.03.23】

Veeam 最新嚴重漏洞 CVE-2023-27532 POC深入探討

Veeam最新的漏洞被爆出能允許未經身份驗證的用戶存取 Veeam 備份服務（默認為 TCP 9401），並能發送請求來獲得明文存取的帳號密碼，由於認證憑證的機制可被繞過，進而可以任意請求存取資料導致該漏洞產生，呼籲大家須儘速更新。

【資料來源：HORIZON3.AI, 2023.03.23】

MITRE 推出供應鏈安全的信任系統平台

MITRE 已為其新的信任系統 (SoT) 框架悄悄發布了一個基於雲的原型平台，該框架定義並量化了供應鏈的風險和網絡安全問題，該平台會將每個風險項目都使用數據測量進行評分，然後將其應用於評分算法。由此產生的分數確定了供應商的優勢和劣勢，各大公司機關可利用該平台來對公司內部進行健檢。

【資料來源：DARKREADING, 2023.03.24】