SHALUN
CYBER SECURITY HUB

資安週報

2022.06.18 (六) —— 2022.06.24 (五)

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

Avos勒索軟體組織已更新惡意軟體工具

Avos是一個於2021年首次發現的勒索軟體組織，最初針對Windows主機。最近以該組織命名的新勒索軟體AvosLocker也針對Linux環境主機，由於像Avos這樣積極主動的威脅者正在積極招募附屬機構，未來這些攻擊可能會持續增加。

【資料來源： TALOS, 2022.06.21】

Adobe Acrobat 可能會阻止防毒軟體監控PDF文件

研究人員發現Adobe Acrobat 正在阻止大多數防毒軟體在啟動時掃描PDF文件，從而實質上阻止它們監視惡意活動，如此將使用戶面臨資訊安全風險。

【資料來源： BLEEPINGCOMPUTER, 2022.06.21】

嚴重的PHP漏洞使QNAP NAS設備遭受遠端執行程式碼攻擊

QNAP今天警告客戶，其部分網路附加存儲(NAS)設備容易受到攻擊，這些攻擊將利用一個存在三年之久的PHP漏洞(CVE-2019-11043)並允許遠端執行程式碼。更新以下系統版本解決該漏洞(QTS 5.0.1.2034 build 20220515或更高版本和QuTS hero h5.0.0.2069 build 20220614或更高版本)

【資料來源： BLEEPINGCOMPUTER, 2022.06.22】

Palo Alto Networks為Prisma Cloud新增應用程式安全功能

為了幫助組織管理和保護複雜的雲環境，Palo Alto Networks正在為其Prisma Cloud平台增加新功能以檢測雲環境中的漏洞和惡意活動。該版本更新重點是簡化對雲環境網路流量中違規指標的檢測。

【資料來源： siliconANGLE, 2022.06.23】