SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.01.30 (五) —— 2023.02.03 (五)

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

TrickGate，自2016 年以來被惡意軟體用來逃避檢測的加殼器

TrickGate 是一種基於shellcode 的加殼工具，作為一項服務提供，至少從2016年7 月被發現開始用於幫助惡意程式來繞過防禦機制，應用於攻擊行動的惡意程式有FormBook、LokiBot 和Agent。據報導，攻擊主要發生在台灣、土耳其、德國、俄羅斯和中國。

【資料來源： SECURITYAFFAIRS, 2023.01.30】

新的Sh1mmer ChromeBook漏洞可讓設備脫離控管

一個名為 “Sh1mmer” 的新漏洞允許用戶取消企業管理的Chromebook，使他們能夠安裝他們想要的任何應用程序並繞過設備限制，不幸的是，目前沒有提供有關管理員如何防止漏洞利用或檢測被利用設備的信息。但是，當使用Sh1mmer 漏洞時，它會導致設備在管理控制台中顯示為非活動狀態。

【資料來源：BLEEPINGCOMPUTER, 2023.01.31】

網絡犯罪集團在暗網上為IT 人才提供六位數美金的薪水

研究人員發現駭客組織在暗網發佈的廣告訊息高達61%都是招聘廣告，並提供非常優渥的薪資待遇，進階攻擊專家薪資最高可達15000-20000美金/月，但研究人員也提醒為駭客組織工作可能擁有的風險，理性評估風險依然大於收益。

【資料來源： CYBERSECURITYNEWS, 2023.02.01】

幾乎所有組織都曾與受害過的供應商合作過

最新研究中調查組織的全球供應商風險發現，全球98.3%的組織至少與一家在過去兩年中遭到攻擊的第三方供應商密切合作過，其中超過50%的組織與200家第四方供應商（第三方供應商的合作夥伴）有間接關係或在過去兩年中遭到侵駭過，呼籲大眾能多重視供應鏈攻擊與其危害。

【資料來源：INFOSECURITY-MAGAZINE, 2023.02.01】