2022/05/09~05/013 資安週報

Active Directory 域權限提升 (CVE-2022–26923)

#漏洞公開

描述如何透過證書認證機制漏洞，讓低權限使用者輕鬆取得DC管理員權限。

【資料來源：IFCR, 2022.05.11】

隱藏在眾目睽睽之下：通過濫用CDN服務來掩蓋C2流量

 # 網絡威脅情報

攻擊者利用域前置技術，將C2網域連線更改為pypi.python.org 使得攻擊行為隱藏並且不易受阻攔。

【資料來源：TEAMT5, 2022.05.10 】

IceApple—針對Microsoft Exchange 服務器上的新後滲透框架

 # 網絡威脅情報

一個新的基於.NET開發的後透框架被發現，並針對IIS服務進行利用，在感染主機上會盡可能地降低足跡難以發現，建議盡快更新網頁服務。

【資料來源：BLEEPINGCOMPUTER, 2022.05.11】

DCRat，一個完整的遠程訪問木馬只需 5 美元

 # 駭客工具

DCRat 是目前在暗網出售的商業RAT之一，可以作為竊取資料與C2的接口，售價非常便宜並有著不錯的效果開始受到攻擊者的青睞。

【資料來源：Security affairs, 2022.05.09】

研究人員發現一種新的網絡釣魚服務——Frappo

 # 駭客工具

Frappo透過Docker容器與自動化的服務，讓用戶可以輕鬆建立釣魚網站，並透過訂閱制度讓釣魚服務宛如企業SaaS服務平台。

【資料來源：Security affairs, 2022.05.10】