LIONIC
Security Solution Provider

鴻璟科技 資安白皮書

2023

www.lionic.com

LIONIC CORP.
Security Solution Provider

鴻璟科技 2023資安白皮書

鴻璟科技(https://www.lionic.com) 專注於 DPI (Deep Packet Inspection) 技術及其相關應用的研發，包括網路防毒、防駭客、防惡意網站、應用程式識別和裝置識別等。這些技術授權給許多國際知名企業，如 Cisco、NEC 等，並大量出貨。

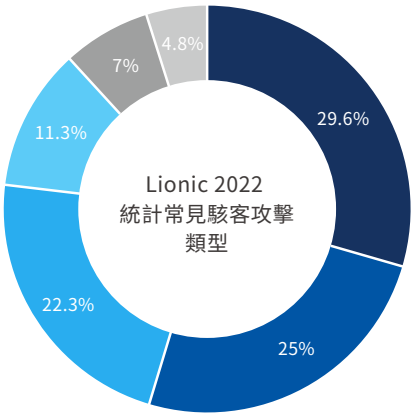
Pico-UTM 100

- IT全方位整合型網路安全過濾器
- OS系統漏洞防護有效
- 防病毒、防駭客、防惡意網站、防火牆
- 專利核心技術-深度封包檢測 (DPI)
- 多重防禦部署，內網保護、端點防護

鴻璟科技同時也以自家的DPI技術，結合多年經驗，打造了一款自有產品 Pico-UTM，這是一款具備企業級網路安全過濾功能的產品，提供網路防毒、防駭客、防惡意網站、防火牆等多種功能。

除了硬體產品外，鴻璟科技為國產品牌中，少數有自有特徵碼資料庫的公司之一。鴻璟科技的情蒐團隊收集了大量分散在世界各地委請托管 Pico-UTM 的受攻擊紀錄，此外，部分技術授權的國際網通大廠，也同意回傳其產品的受攻擊紀錄，這些資料形成了扎實的統計基礎。

根據鴻璟科技所蒐集的資料，在排除了資安風險較低的 Protocol Anomaly 和 Brute Force Attack 兩大類攻擊之後，2022年，有五大駭客攻擊類型特別突出，佔總攻擊量的95.2%。其餘攻擊類型僅佔4.8%，不在本次討論範圍內。這五大攻擊類型如下：



網路攻擊類型:

HTTP Basic Auth default password login	29.6%
Router exploit	25%
Web service exploit	22.3%
IP Cam/DVR exploit	11.3%
Trojan traffic	7%
Other	4.8%

上述攻擊類型，通常利用已知漏洞或甚至是零日漏洞，未經授權地進入計算機系統或網絡，以從中獲取或更改數據、損壞系統或進行其他不正當活動。為了保護網絡安全，使用者應該注意密碼安全、更新系統補丁、禁用不必要的服務等措施，並透過鴻璟科技 Pico-UTM 產品所提供的防駭客功能阻擋常見的網路攻擊，降低安全風險。

以下，讓我們共同探討這5大駭客攻擊類型以及相對應的防禦措施:

Default password login

弱密碼是指由短字母或數字串、常見單詞等簡單組成的密碼，容易被猜測或破解。例如 “abc”、“123456”等。預設密碼也是一種弱密碼。若使用弱密碼進行身分驗證，攻擊者可以通過猜測、字典攻擊等方式輕鬆破解密碼，從而取得敏感資訊或冒充身分，對個人或組織造成嚴重的損失。

因此，為了保護帳號密碼和敏感資訊，建議使用強密碼。強密碼應包括大小寫字母、數字和特殊符號等元素，不應使用常見單詞或字典中的詞彙。同時，應避免在多個網站上使用相同的密碼，以防萬一。

鴻璟科技的網路安全產品提供防駭客功能，可阻擋常見的預設密碼與弱密碼的登入請求，從而降低安全風險，保障個人或組織的資訊安全。

Router exploit

路由器是連接網路的重要裝置，它負責將網路封包從一個網路由到另一個網路。如果路由器受到攻擊，將對整個網路產生嚴重影響，因此攻擊路由器往往是駭客首選的目標。常見的攻擊方式是利用弱密碼或漏洞等方式進入路由器，攻擊者可能會更改路由器設置、控制網路流量，例如劫持 DNS 導致使用者訪問惡意網站，或者竊取使用者的敏感資料。

為了保護路由器的安全，使用者應該採取一系列的措施。首先，嚴格保護路由器的登入密碼，使用強密碼並定期更換，禁用不必要的遠端訪問功能。其次，定期更新路由器的韌體以獲取最新的漏洞修復和安全功能，限制不必要的網絡連接和流量，並使用安全的網路協議，如HTTPS。

鴻璟科技的網路安全產品，可以阻擋已知路由器漏洞攻擊的流量，使CVE漏洞無法被成功利用。

Web services exploits

攻擊者會利用 web 服務本身或服務使用的技術中的漏洞或弱點，對 web 服務進行攻擊，從而獲取敏感資訊、或是阻斷服務(DoS, Denial of Service)，甚至是控制主機。常見的 web 服務攻擊包括 XSS、XXE、注入攻擊 和 Remote Code Execution 等多種類型，這些攻擊方式往往是隱蔽的，難以被發現和防範。

於2021年底，Apache log4j被挖出漏洞。由於該軟體廣泛使用於Web服務，犯罪集團利用此漏洞，撰寫程式進行掃描，並成功進行Remote Code Execution入侵。之後的2022 年的網路流量中充斥著掃描log4j漏洞的行為。

為了保護 web 服務的安全，應及時修補漏洞，加強身份驗證和授權機制，實施安全的開發和測試流程，定期更新軟體和系統，並使用防火牆和入侵檢測系統等安全工具，以最大限度地減少攻擊的風險。另外，還應定期進行安全評估和測試，發現和解決潛在的風險和漏洞。

鴻璟科技的網路安全產品，可以阻擋常見的 web 服務攻擊流量，以減少弱點攻擊的影響。此外，產品還支援便捷的安全日誌功能，有助於快速發現和解決安全事件，保障 web 服務的安全和穩定運行。

IP Cam/DVR exploits

網路監控攝影機(IP Cam)和數位錄影機(DVR)廣泛用於家庭和企業的監控，但這些設備也因為容易受到攻擊而成為攻擊

者的目標。攻擊者可以利用預設密碼、漏洞或其他方式，未經授權地訪問設備並竊取數據，甚至接管設備並將其用於進一步攻擊。常見的攻擊手法包括預設密碼登入、漏洞利用和入侵等。

根據BleepingComputer 2022年8月的報導，大約仍有八萬台海康IP Camera暴露於互聯網，其韌體版本存在CVE-2021-36260漏洞，這意味著這些攝影機隨時可能會受到入侵的風險。實際上，一個以Mirai為基礎的botnet，名為Moobot，正是利用該漏洞大量繁殖。如果接收到Moobot botnet的命令，這些攝影機可以發動DDoS（分散式拒絕服務）攻擊，使某個網站癱瘓。

為了保障網路監控攝影機(IP Cam)和數位錄影機(DVR) 的安全，使用者必須更改預設密碼，並使用強密碼。同時，定期更新韌體以修正已知漏洞，並監控是否存在可疑的登入紀錄或網路活動。此外，使用者也可以採用 VPN 或其他加密方式來增強設備的安全性。

鴻璟科技的網路安全產品，可以阻擋已知網路監控攝影機(IP Cam)和數位錄影機(DVR) 漏洞攻擊的流量，進一步保護設備免受攻擊，或被利用成為DDoS攻擊的工具。

Trojan traffic

古希臘神話中的特洛伊木馬故事，成為現代電腦領域中的一個比喻，形容一種透過欺騙手段，將有害的軟件或代碼隱藏在看似無害的軟件或文件中，等待被攻擊者下載或運行後，獲得系統控制權的攻擊手法。這種攻擊通常需要使用者的不知情或疏忽，才能成功進行。

因此，"木馬"被引申為現代網路攻擊中的一種手法。攻擊者會將有害軟件或代碼藏在看似無害的軟件或文件中，例如電子郵件附件、下載的軟件、網路頁面等，誘騙使用者下載或運行，取得系統控制權，甚至竊取使用者的敏感資訊。為了防止"木馬"攻擊，使用者應該注意電子郵件來源，避免下載不明來源的軟件，安裝防毒軟體等措施。

木馬流量是指木馬程式的惡意行為所產生的網路流量，具有多樣化和隱蔽性強的特點，因此很容易繞過傳統的防火牆而不被偵測到。當木馬程式成功地感染了一台電腦，它就能夠在背景中運行，並且可以藉由存取資源和資料，來執行各種惡意行為，例如竊取敏感資訊、遠端操控被感染的設備，或者將被感染的設備轉變成僵屍網絡的一部分(Botnet)以攻擊其他設備或系統。

為了防止木馬流量攻擊，使用者應該安裝防毒軟體、定期更新系統與軟體，並且不要下載來自不明來源的檔案或點擊不明來源的連結。此外，使用者也應該注意開啟防火牆、使用強密碼來保護帳號和資料、以及避免使用公共的 Wi-Fi 網路，因為這些網路通常較不安全。

鴻璟科技的網路安全產品提供防駭客功能，可以阻擋木馬程式的流量，以降低感染木馬的影響。此外，我們的產品可以檢測和隔離感染木馬的設備，從而有效地防止木馬的擴散和傳播，保障網絡安全。

Tera-UTM 12

- OT全方位整合型網路安全過濾器
- 工業控制系統(ICS)協定防護
- Hardware Bypass維持產線網路連線
- HTTPS流量掃描偵測
- 有效防護作業系統漏洞
- 專利核心技術-深度封包檢測 (DPI)開發
- 受市場認證的病毒碼資料庫
- 防病毒、防駭客、防惡意網站、防火牆地理封鎖

鴻璟科技在DPI的延伸應用，以網路安全與內容管理為主。所以，不斷地提升自身技術水平和創新能力，以因應不斷變化的網路安全威脅。旗下產品Pico-UTM已經證明了其成本效益和高品質的網路安全功能，贏得了眾多成功案例和用戶的信任。

在2023年，鴻璟科技即將推出Tera-UTM，採用更強大的硬體設備和更加先進的技術，加入更多的高級功能，例如支援工業通信協定、威脅來源分析和地理封鎖等，相信這款產品將會有更加驚人的表現，提供更高級別的的網路安全保障。

無論是企業還是個人，都可以放心地依賴鴻璟科技的產品，保障其網路安全，防範勒索軟體、木馬、病毒、駭客、惡意網頁等各種威脅的攻擊。鴻璟科技將繼續致力於開發和提供更加優秀的產品和服務，讓用戶的網路安全更加穩定可靠。

LIONIC
Security Solution Provider

聯絡窗口
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com

LIONIC CORP.
https://www.lionic.com/
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.