出國報告（出國類別：開會）

出席 Black Hat Asia 2024

出國報告書

服務機關：數位發展部

姓名職稱：周詳制度工程師

派赴國家：新加坡

出國期間：113年04月17日至21日

報告日期：113年07月17日

摘 要

Black Hat（黑帽大會）是全球最著名的資訊安全會議之一，始於1997年。它提供一個平台，讓來自世界各地的資安專家、研究人員和行業領袖聚集一堂，分享最新的安全研究、技術和趨勢。會議包括深入的技術研討會、培訓課程和現場演示，涵蓋從漏洞發現和滲透測試到惡意軟件分析和防禦策略等多個領域。Black Hat 目的為推動資訊安全技術的進步，促進知識交流和創新，並提高全球網路安全。

本次參與 Black Hat Asia 2024，除了 Asia 外，今年還有 USA、Middle East & Africa、Europe 等地的 Black Hat。Black Hat Asia 培訓課程於 4/16 至 4/19 舉行，為攻擊和防禦駭客提供直接的技術培訓機會，由專家進行授課。Black Hat Asia 網路會議於 4/18 至 4/19 舉行，在這些會議中，研究人員將分享有關信息安全風險和趨勢的最新資訊，涵蓋從漏洞開發、平台安全到惡意軟體等各種主題的研究成果，本次會議主要參與 4/18 至 4/19 之會議部分。

目錄

壹、目的

Black Hat 是一個國際資訊安全會議，尤其對政府部門的資訊安全人員而言，提供了寶貴的學習和交流機會。此會議集結全球資安專家的最新研究，並針對當前和未來的安全挑戰提供應對策略。對於從事公共安全、國防和重要基礎設施保護的政府人員來說，瞭解先進的攻擊技術和防禦方法是必要的。

Black Hat Asia 不僅增進參與者對於最新安全技術的瞭解，還激勵他們發現和創造解決方案以對抗日益複雜的網路攻擊。此外，活動為資訊安全專業人士提供一個促進合作與知識共享的環境。通過參加 Black Hat 會議，專業人士不僅能夠提升自身技能，更能在全球範圍內推動資訊安全領域的進步與創新。

本次參加 Black Hat Asia 不僅促進了技術交流，也增強了國際間在資訊安全領域的合作與對話，對於致力於提升政府資訊安全防護能力的專業人士來說，實屬不可多得的機會。

貳、會議過程

本次共整理八場會議，分別為：

1. Cloud Console Cartographer: Tapping Into Mapping > Slogging Thru Logging （Cloud Console Cartographer：從記錄中繪製地圖 > 苦苦尋找日誌）
2. The Hole in Sandbox: Escape Modern Web-Based App Sandbox From Site-Isolation Perspective（沙盒中的漏洞：從站點隔離的角度逃逸現代網路應用沙盒）
3. Breaking Managed Identity Barriers In Azure Services（在Azure服務中突破託管身份障礙）
4. A Glimpse Into The Protocol: Fuzz Windows RDP Client For Fun And Profit（瞥見協議：為樂趣和利益模糊測試Windows RDP客戶端）
5. China's Military Cyber Operations: Has the Strategic Support Force Come of Age? （中國軍事網路作戰：戰略支援力量成熟了嗎？）
6. The Dark Side of EDR: Repurpose EDR as an Offensive Tool （EDR 的陰暗面：將 EDR 重新用作進攻工具）
7. Bypassing Entra ID Conditional Access Like APT: A Deep Dive Into Device Authentication Mechanisms for Building Your Own PRT Cookie（繞過 APT 等 Entra ID 條件存取：深入研究裝置身分驗證機制以建立您自己的 PRT Cookie）
8. Chinese APT: A Master of Exploiting Edge Devices（中國APT：邊緣裝置利用大師）

圖 1：Black Hat 大會開場

圖 2：Black Hat 大會分享

一、Cloud Console Cartographer: Tapping Into Mapping > Slogging Thru Logging （Cloud Console Cartographer：從記錄中繪製地圖 > 苦苦尋找日誌）

講者：Daniel Bohannon, Andi Ahmeti | Permiso Security

時間：2024.04.18 (四) 10:20 - 11:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/index.html#cloud-console-cartographer-tapping-into-mapping--slogging-thru-logging-36450

簡報連結：

https://i.blackhat.com/Asia-24/Asia-24-Bohannon-CloudConsoleCartographer.pdf

講者詳細介紹了如何利用雲端控制台日誌進行威脅狩獵和事件回應，內容包括引言、雲端日誌對防禦者的重要性、控制台日誌的問題、解決方案以及工具演示和發佈。

雲端日誌對威脅狩獵和事件回應至關重要。雖然本地日誌和網路日誌提供詳細的事件紀錄，但雲端日誌通常更抽象且粒度較低，這使得在雲環境中檢測惡意活動變得更加困難。由於控制台日誌資訊量巨大且雜亂無章，分析和從中提取有用資訊變得非常困難。這些日誌通常包含大量無關資訊，掩蓋了潛在的威脅活動。

講者提出了一種通過對應來提高日誌清晰度的方法，即使用 Cloud Console Cartographer 工具。這個工具可以自動將大量的日誌事件呈現在互動式控制台，從而大大減少需要分析的數據量，提升分析效率。

講者展示了如何使用 Cloud Console Cartographer 工具來處理和分析雲端控制台日誌，並提供了該工具的公開發佈資訊。工具的主要功能包括標籤分配、資訊評估和生成資訊對象等，這些功能有助於對日誌進行有效的處理和分析。

講者強調了組態雲端日誌選項以便於檢測和分析可疑 Session 的重要性。建議包括保持邊緣設備的訪問或審計日誌、理解攻擊者的行為模式以及定期審查和更新日誌策略等。

講者最後強調了雲端日誌在威脅狩獵和事件回應中的重要性，提出了利用對應技術來解決噪雜日誌問題的解決方案，並介紹了 Cloud Console Cartographer 工具的使用方法和效果。通過這些方法，安全專業人員可以更有效地管理和分析雲端環境中的日誌，提升整體安全防護能力。

二、The Hole in Sandbox: Escape Modern Web-Based App Sandbox From Site-Isolation Perspective（沙盒中的漏洞：從站點隔離的角度逃逸現代網路應用沙盒）

講者：Bohan Liu, Haibin Shi | 騰訊安全玄武實驗室

時間：2024.04.18 (四) 11:20 - 12:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#the-hole-in-sandbox-escape-modern-web-based-app-sandbox-from-site-isolation-perspective-37166

簡報連結：

https://i.blackhat.com/Asia-24/Presentations/Asia-24-Liu-The-Hole-in-Sandbox.pdf

本次會議主要探討了現代網路應用程式沙盒的安全性及其從站點隔離的角度逃逸的技術。首先，講者介紹了其研究領域，包括瀏覽器安全和 Android 安全。接著，詳細描述了 Chrome 瀏覽器的多執行緒架構和沙盒機制，這些機制旨在限制資源訪問和隔離進程。

接下來，講者探討了攻擊者如何利用渲染器遠端代碼執行（RCE）攻擊來突破沙盒，並介紹了Universal Cross Site Scripting（UXSS）攻擊，即在瀏覽器層面注入惡意代碼，繞過站點隔離政策。

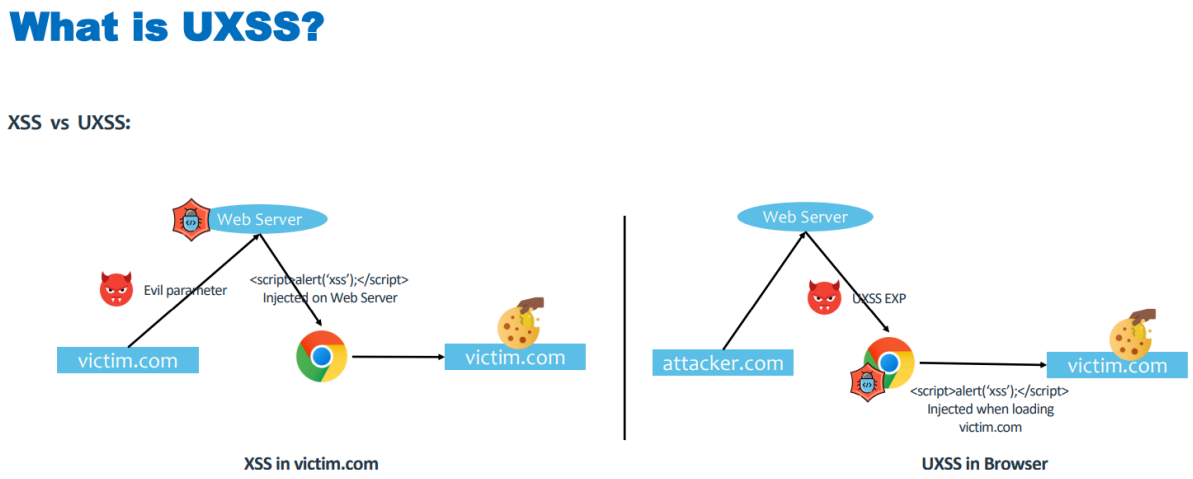


圖 3：XSS vs UXSS

講者還通過具體案例展示了如何利用 Safari 瀏覽器中的漏洞來繞過站點隔離，進行跨域資料訪問和代碼注入。此外，詳細解釋了 Chrome 的站點隔離機制，包括跨執行緒導航和跨域讀取阻塞，分析了技術挑戰和解決方案。之後，講者探討了基於網頁的應用程式中存在的安全隱患，特別是在多平台設計和特權 API 使用方面的漏洞，提出了針對 WebView 應用程式的攻擊方法，並展示了實際攻擊演示。

最後，講者提供了建議和未來研究方向，強調了加強特權API訪問控制和使用不可變代碼的重要性，並指出了持續改進站點隔離機制以增強網頁應用程式安全的必要性。通過這些分析和建議，為安全研究人員提供了寶貴的見解和實踐經驗。

三、Breaking Managed Identity Barriers In Azure Services（在Azure服務中突破託管身份障礙）

講者：Nitesh Surana, David Fiser | 趨勢科技

時間：2024.04.18 (四) 13:30 - 14:10

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#breaking-managed-identity-barriers-in-azure-services-37998

簡報連結：

https://i.blackhat.com/Asia-24/Presentations/Asia-24-Fiser-Breaking-Managed-Identity-Barriers-in-Azure.pdf

本次會議探討了在 Azure 服務中利用託管身份進行攻擊的方法以及如何防範這些攻擊。首先，講者介紹其研究領域，包括雲端安全和威脅研究，強調了託管身份在Azure服務中的重要性及其應用範圍。

接著，講者詳細研究了 Azure Functions，這是一個無伺服器平台，允許運行用戶代碼。講者分析了其身份驗證和觸發機制，並探討了環境變數在這些功能中的使用情況，指出這些變數經常儲存敏感資訊如憑證和身份令牌，存在安全風險。

在身份管理問題部分，講者詳細介紹了如何通過分析 Azure Functions 的環境變數來獲取託管身份代理設置和有效的 JWT 令牌，強調了在雲端環境中，環境變數的普遍使用可能帶來的風險，特別是當這些變數包含敏感資訊時。然後，演示了如何利用未

經妥善保護的環境變數進行攻擊，詳細說明了攻擊者如何利用這些變數繞過 Azure 的安全控制，取得系統的訪問權限。

講者接下來探討了Azure Machine Learning 服務中的安全性問題，分析了機器學習工作區中的網路流量和運行過程，並逆向工程了雲服務提供商的代理，說明了如何利用預設日誌和環境變數來發現並利用漏洞。講者提供了一些真實的攻擊案例，展示了攻擊者如何利用這些漏洞來進行惡意活動，強調了攻擊者能夠通過這些方法取得存儲帳戶的訪問密鑰、環境變數中的憑證以及託管身份的令牌。

在防範建議部分，講者建議使用環境變數時應謹慎，並限制其包含敏感資訊，對雲服務的威脅模型進行審查和改進，採取最小權限原則管理身份，並強調了對雲API進行測試和安全驗證的重要性，提出了可行的日誌記錄方法以便檢測異常活動。

最後，講者強調了未來需要持續改進 Azure 服務的安全性，包括 API 管理、容器實例和機器學習等多個方面，呼籲研究人員進一步探索和挑戰官方文件中的假設，以發現更多潛在漏洞。講者全面分析了 Azure 託管身份在現代雲服務中的應用和安全挑戰，並提出了具體的防範措施，為安全研究人員和雲端服務使用者提供了寶貴的見解。

四、A Glimpse Into The Protocol: Fuzz Windows RDP Client For Fun And Profit（瞥見協議：為樂趣和利益模糊測試Windows RDP客戶端）

講者：Quan Jin, Yingqi Shi, Mingjia Liu, Siyuan Liu, Guoxian Zhong | 安恒信息

時間：2024.04.18 (四) 14:30 - 15:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#a-glimpse-into-the-protocol-fuzz-windows-rdp-client-for-fun-and-profit-37629

簡報連結：

https://i.blackhat.com/Asia-24/Asia-24-Shi-A-Glimpse-Into-The-Protocol.pdf

本次會議深入探討了針對 Windows RDP 客戶端的模糊測試技術。講者強調了遠端桌面協議（RDP）的流行和長期存在的重要性，以及過去一年中RDP的漏洞情況。

RDP提供了多種功能，包括剪貼簿、列印機、儲存裝置、憑證卡、麥克風、喇叭的支援。講者分析了 RDP 客戶端和伺服器的攻擊，並聚焦於 Microsoft RDP 客戶端，理由包括其清晰性、可操作性和簡單性。講者討論了 RDP 的虛擬通道，包括靜態虛擬通道和動態虛擬通道，並提到了相關研究和資源，如 SSTIC 2022 的文章和以前的黑帽會議演示。

- **Proxy**

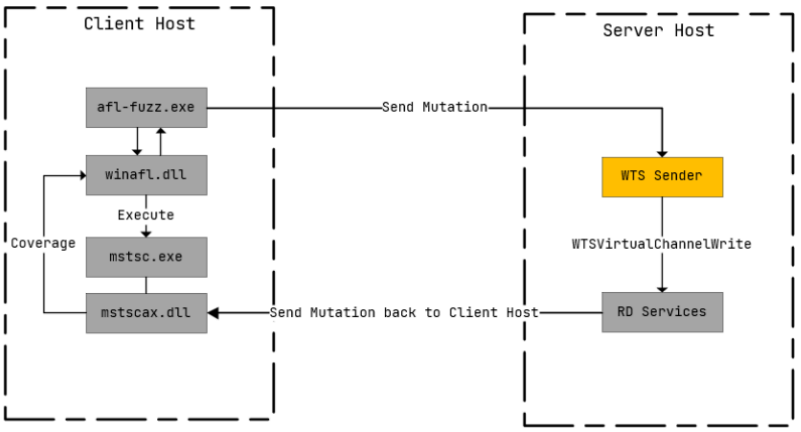


圖 4：RDP Fuzzing 架構示意圖

講者詳細介紹了開源 RDP 模糊測試工具，包括 rdpfuzz 和 WinAFL-RDP，並介紹了模糊測試的架構，分為循環模式和代理模式，最終選擇使用 WinAFL-RDP 進行測試。模糊測試的環境準備包括使用兩台虛擬機或一台虛擬機和 RDPWrap 進行設置，確保測試環境的穩定和準確。

講者演示了模糊測試的開始和批次部署，並分享了一些增強模糊測試的方法，如轉移honggfuzz 的變異策略和覆蓋可視化，說明了如何處理模糊測試過程中發現的崩潰和競爭條件。並提供了兩個具體的案例，說明在列印機功能中的 UAF（Use-After-Free）漏洞和 XPS 列印機中的競爭條件漏洞，詳細說明了每個案例的技術細節，包括觸發漏洞的過程和修補方法。

最後，講者介紹了未來的研究方向，包括 RDP 伺服器、更多的虛擬通道和其他協議的安全性研究，為未來的安全研究提供了寶貴的方向和方法。這份簡報通過詳細的技術分析和實例演示，展示了模糊測試在發現和利用 Windows RDP 客戶端漏洞中的重

要性。講者分享了他們的最新研究成果和工具，並強調了競爭條件在漏洞發現中的意義，提升了對 RDP 安全性的理解。

五、China's Military Cyber Operations: Has the Strategic Support Force Come of Age?（中國軍事網路作戰：戰略支援力量成熟了嗎？）

講者：Pukhraj Singh | Director, Centre for Epistemic Security

時間：2024.04.19 (五) 10:20 - 11:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#chinas-military-cyber-operations-has-the-strategic-support-force-come-of-age-36831

簡報連結：

https://i.blackhat.com/Asia-24/Asia-24-Singh-ChinasMilitaryCyberOperationsHas.pdf

本次演講呈現了一場關於中國軍事和資訊戰策略的演講的日程安排，內容包括下列六項：探討中國最近的網路預置行動如 Volt Typhoon 和 RedEcho；深入分析人民解放軍的戰略支援部隊（SSF）；討論中共的資訊戰指揮控制（C2）體系；解析解放軍的軍民融合策略；總結中國如何利用網路攻擊作為首次打擊手段，對敵方關鍵基礎設施進行打擊；以及評估中國網路戰略對印太地區地線政治的影響。這場演講提供了對中國如何通過網路手段塑造其國際地位和區域權力平衡的深刻洞察。

會議中提到涉及中國的軍事網路作戰策略，特別是在其地緣政治敏感的近海區域。中國通過戰略資訊戰強化了對南中國海和台灣海峽的空中及海上控制，目的是為了保護其地緣經濟利益。這包括干擾美國的後勤支援和航行自由，以調整該地區的權

力平衡。此外，中國軍事網路作戰的組織架構顯示了對戰時資訊作戰群體（IOG）的動員，這些群體在民用領域中的參與突顯了軍民融合策略的實施。這次會議的討論有助於深入理解中國如何利用網路空間操作來塑造區域內的政治和軍事動態。

講者強調了戰術和基礎設施在威脅活動群組中的重疊，指出授權力量已被納入戰時的 IOG。此外，這些操作直接由中央軍事委員會授權，顯示了嚴格的指揮和控制結構。從政治軍事目標的角度來看，資訊和網路作戰被視為首次打擊手段，隨後是電子戰和動能作戰，旨在破壞敵方的系統體系。這種策略的目標是削弱敵方的意志並達到威懾效果，從而在戰略層面上達成其目標。這種分析有助於深入瞭解中國如何整合其網路戰能力，以強化其軍事和政治影響力。

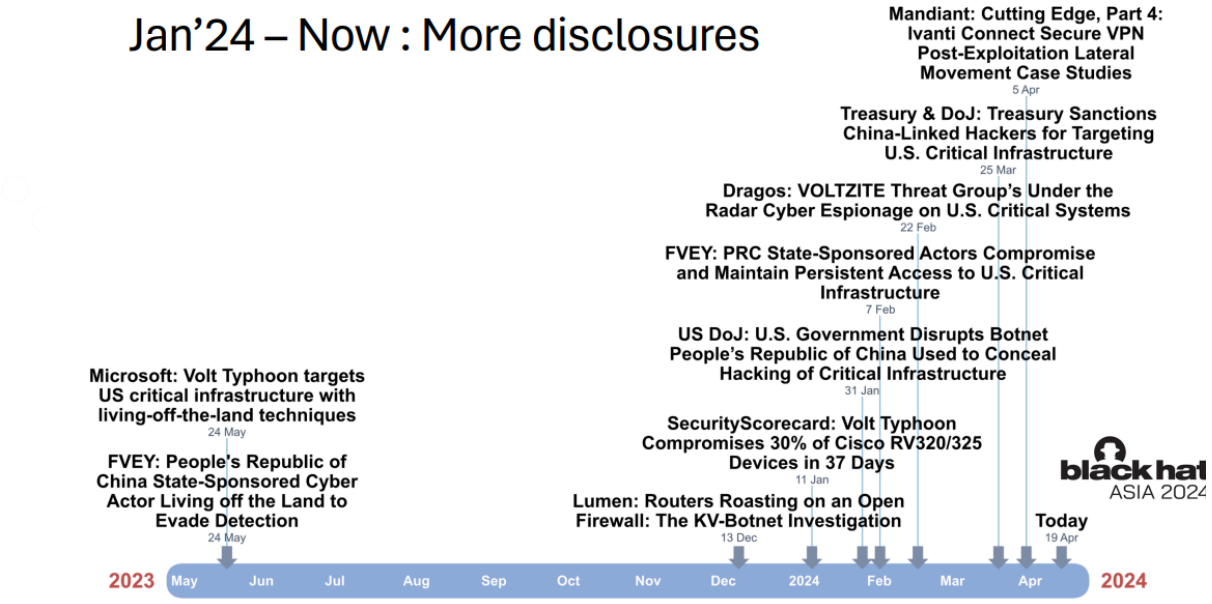


圖 5：網路攻擊事件，涉及美國關鍵基礎設施

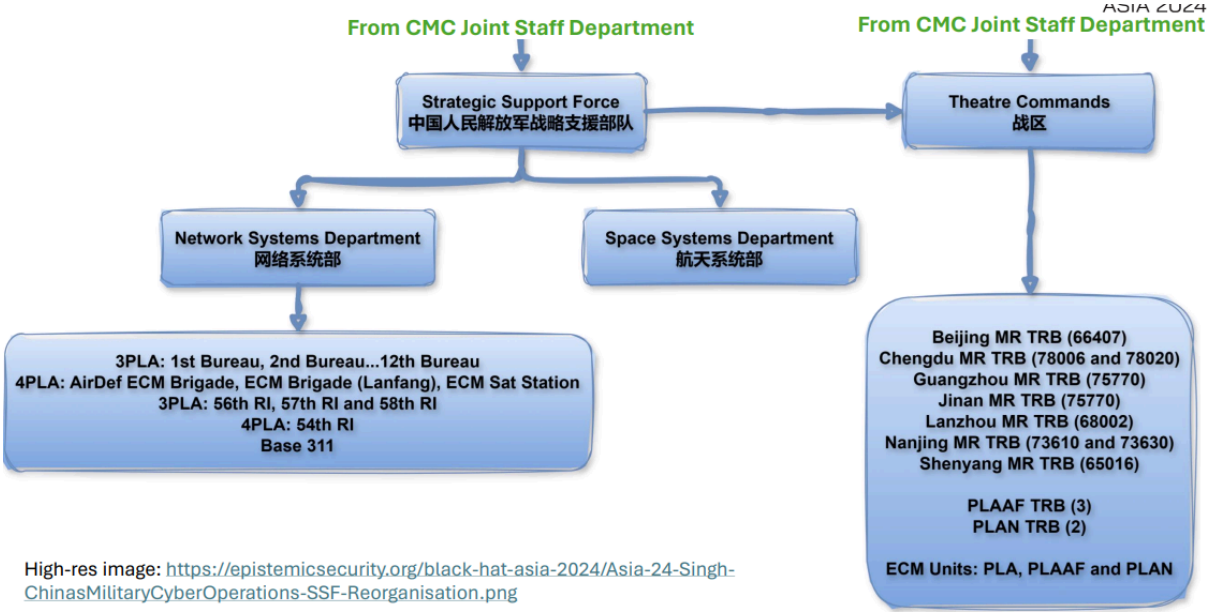
上圖概述了 2023 年 5 月至今，有關網路安全和網路攻擊的多項重要披露事件，特別是針對美國的關鍵基礎設施。主要內容包括：

1. 2023.05.24 Microsoft 報告稱 Volt Typhoon 針對美國的關鍵基礎設施，使用了多種隱蔽和持久的技術來維持對系統的存取。
2. 2023.05.24 五眼聯盟揭露中國的國家支援的網路行動者利用隱蔽技術進行操作，以避開檢測。
3. 2023.12.13 Lumen 進行了一次開放調查，揭露了駭客如何利用 KV-botnet 進行攻擊。
4. 2024.01.11 SecurityScorecard 發現 Volt Typhoon 在 30 天內入侵了 30% 的 Cisco RV320/325 設備。
5. 2024.01.31 美國司法部瓦解了一個由中國支援的用於隱藏對美國關鍵基礎設施攻擊的僵屍網路。
6. 2024.02.07 五眼聯盟揭露中國的國家支援的網路行動者利用隱蔽技術進行操作，以避開檢測。
7. 2024.02.22 Dragos 發現 VOLTZITE 威脅組織在美國關鍵系統上進行雷達網路間諜活動。
8. 2024.03.25 美國財政部和司法部對涉及針對美國關鍵基礎設施的中國駭客實施了制裁。
9. 2024.04.05 Mandiant 在其系列報告的第四部分中，揭示了 Volt Typhoon 使用 Ivanti Connect Secure VPN 進行後門操作和橫向移動。

Volt Typhoon 網路攻擊行動已經活躍至少五年，其主要的地理目標包括美國、亞太地區和非洲。此行動針對的關鍵基礎設施涵蓋交通、自來水、電力、衛星網路、通訊、緊急管理系統、國防工業基地以及地理資訊系統。此外，Volt Typhoon 的行動展示了與其

他威脅行動者如Kostovite（Dragos）、APT31、Mirai 僵屍網路和UTA0178（2024 Ivanti Oday）的潛在重疊。它們使用的技術和程序（TTPs）雖然不顯眼，但效果顯著，包括廣泛的預先妥協偵察、手動鍵盤活動和利用現有環境技術。這些資訊提供了對該網路威脅行動深入的洞察，顯示了其對全球多個關鍵領域的潛在影響。

講者另外展示了幾個主要的網路威脅行動者 RedEcho, RedFoxtrot, TAG-38, 以及與APT41和Tonto Team有結構性重疊的 APT31。這些組織的攻擊目標符合Volt Typhoon的定位標準，針對的是地區或州級的負荷調度中心、高壓輸電站、熱電廠、多國物流公司、國家緊急反應系統，以及為英國公用事業提供運營技術（OT）服務的管理服務提供商（MSP）。此外，這些行動在戰術上與 Volt Typhoon有相似之處，例如利用被侵佔的邊緣或物聯網設備如IP攝像機進行指揮與控制（C2），以及使用快速反向代理技術。這些資訊揭示了一系列複雜且協調的網路攻擊活動，展示了這些威脅行動者在全球範圍內如何操作以及他們的技術手段。



High-res image: https://epistemicsecurity.org/black-hat-asia-2024/Asia-24-Singh-ChinasMilitaryCyberOperations-SSF-Reorganisation.png

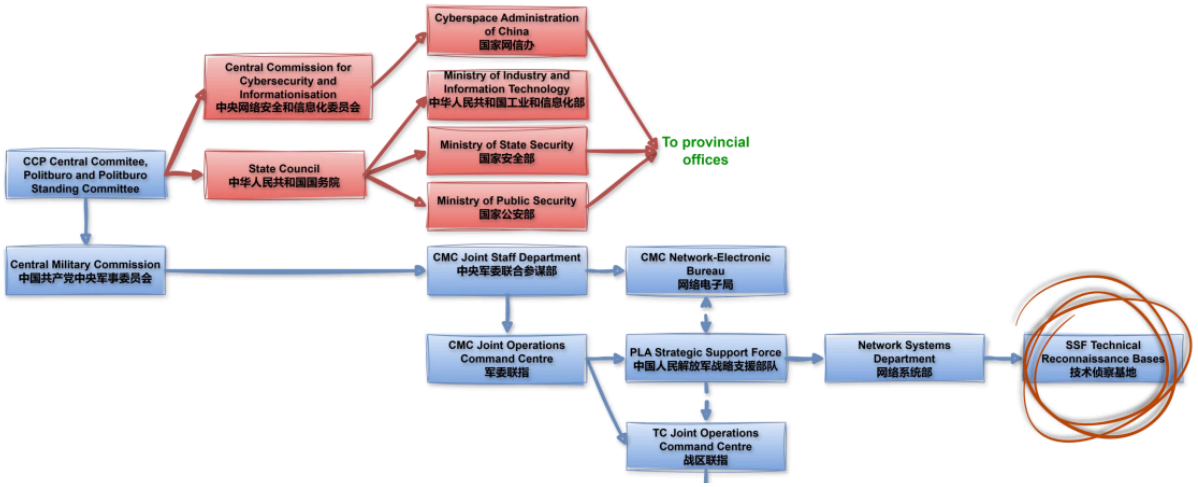


圖 6：中國網路部隊組織架構

上圖展示了中國人民解放軍戰略支援部隊（SSF）的組織架構，該部隊直接受中央軍事委員會聯合參謀部的指揮。這些單位涵蓋了電子戰、網路攻擊和防禦等多個方面，顯示了中國在這些高技術領域的組織深度和專業性。此外，圖中也顯示了指揮部的結構，指出了與網路系統部相關的多個技術偵查局（TRB）和電子對抗單位。

最後講者提到，為何「Volt Typhoon」網路行動可能將非洲作為目標，這被稱為「多邊威懾」。即使在與美國或日本的緊張關係中，中國領導層可能不僅僅從事威懾活動，而是進行有針對性的攻擊或限制性資訊操作，旨在威懾第三方國家。這些行動目的在於展示中國的能力和決心，增強其在全球範圍內的戰略影響力。這種策略是為了在關鍵時刻展示力量，對主要對手造成心理上的壓迫和實際上的牽制。

六、The Dark Side of EDR: Repurpose EDR as an Offensive Tool（EDR 的陰暗面：將 EDR 重新用作進攻工具）

講者：Shmuel Cohen | Security Researcher, SafeBreach

時間：2024.04.19 (五) 11:20 - 12:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#the-dark-side-of-edr-repurpose-edr-as-an-offensive-tool-37846

講者探討了端點偵測和回應（EDR）系統可能存在的漏洞，特別針對 Palo Alto Networks 的 Cortex XDR 系統。不同於傳統的避開或停用EDR系統的攻擊方式，此研究展示了如何控制 EDR 系統並在其內部執行程式碼，使之成為隱蔽且持續的惡意軟體。

這項研究突顯了如果 EDR 部署不當，可能會被惡意行為者利用來執行高級持久威脅（APT）攻擊。研究指出，攻擊者可以繞過 Cortex XDR 的重要安全特性，包括機器學習檢測模組、行為模組，並能夠進行資料外洩、建立持久性控制，甚至對整個機器進行加密而不被檢測到。

針對上述 Palo Alto 漏洞官方進行回應，回應指出，「安全是我們最高的優先事項。SafeBreach 在十個月前通知我們其研究結果，我們當時通過對客戶自動更新內容來解決了功能繞過的問題。」這表明 Palo Alto Network s已經對報告的安全漏洞進行了迅速的反應和修復，強調他們對保護客戶安全的承諾和努力。這種快速和透明的回應是建立用戶信任和保護企業品牌的重要方面。

此次也將探討這一新型攻擊向量的含義，揭示攻擊者與 XDR 之間複雜的關係，並討論到目前為止在 EDR 安全方面尚未被充分探索的重要方面。這強調了即便是被廣泛依賴的高級工具如 EDR，也需要嚴格的安全措施以應對不斷演變的網路威脅。

講者針對一些攻擊手法進行分享，包含LSASS記憶體轉儲和硬連結的安全風險。LSASS是 Windows 系統中負責處理使用者驗證的過程。透過使用 procdump 這一工具，攻擊者能夠從 LSASS 提取認證資訊，這些資訊可能被用來進行網路內橫向移動，即利用這些認證訪問網路中的其他系統。另一方面，硬連結在 Windows 中被用作檔案緊密連接，可能被惡意利用以提升系統權限。講者並指出如何利用這些連結來開發漏洞利用程式，同時強調了作業系統更新在防止此類攻擊中的重要性。這兩種技術示例突出了系統管理員在保護關鍵系統資源面臨的安全挑戰及防護策略的重要性。

最後講者強調了端點安全產品在研究安全風險時的重要性，指出應深入理解這些系統的內部運作以增強保護。它批評了僅基於名稱或命令列正規表達式來設定允許列表的方法，認為這種策略不夠全面，並呼籲需要更細致的控制和智慧檢測機制以對抗安全威脅。最後，這強調了端點安全解決方案在設計和實施時的複雜性和深度，並推動業界對現有方法進行創新和改進。

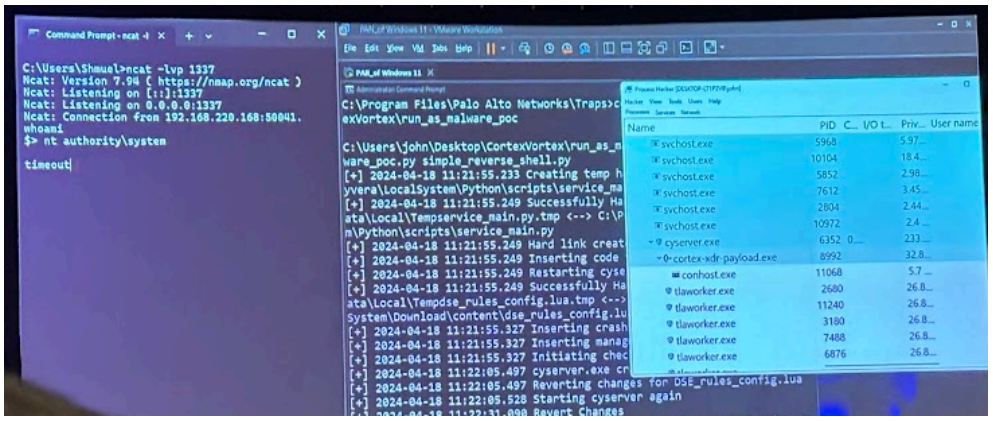


圖 7：現場說明攻擊方法

七、Bypassing Entra ID Conditional Access Like APT: A Deep Dive Into Device Authentication Mechanisms for Building Your Own PRT Cookie（繞過 APT 等 Entra ID 條件存取：深入研究裝置身分驗證機制以建立您自己的 PRT Cookie）

講者：Yuya Chudo, Takayuki Hatakeyama | Senior Advisor, Secureworks Japan K. K.

時間：2024.04.19 (五) 13:30 - 14:10

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/index.html#bypassing-entra-id-conditional-access-like-apt-a-deep-dive-into-device-authentication-mechanisms-for-building-your-own-prt-cookie-37344

簡報連結：

https://i.blackhat.com/Asia-24/Presentations/Asia-24-Chudo-Bypassing-Entra-ID-Conditional-Access-Like-APT.pdf

講者主要探討了如何繞過微軟 Entra ID 條件式存取的裝置認證。講者介紹了裝置認證機制，包括設備密鑰和傳輸密鑰的生成與註冊，以及如何使用這些密鑰進行瀏覽器單點登入（SSO）過程。他們發現了一種方法，通過逆向工程微軟的認證庫，不需要管理員權限就能假冒裝置，從而繞過裝置基礎的存取控制策略。此外，還說明了如何利用未記錄的API與儲存在TPM（可信平台模組）中的密鑰進行互動。

為了防範和檢測可能繞過裝置認證的攻擊，講者建議監控可疑的遠端程序呼叫（RPC）活動和特定加密函數調用。此外，建議調查來自同一裝置的多個帳戶的Microsoft Entra ID登錄記錄。最終，強烈建議為所有使用者設定多因素認證（MFA），

而不僅僅是要求企業裝置，以增強對抗此類攻擊的安全防護。這些措施有助於增加攻擊者橫向移動和進入雲環境的難度。

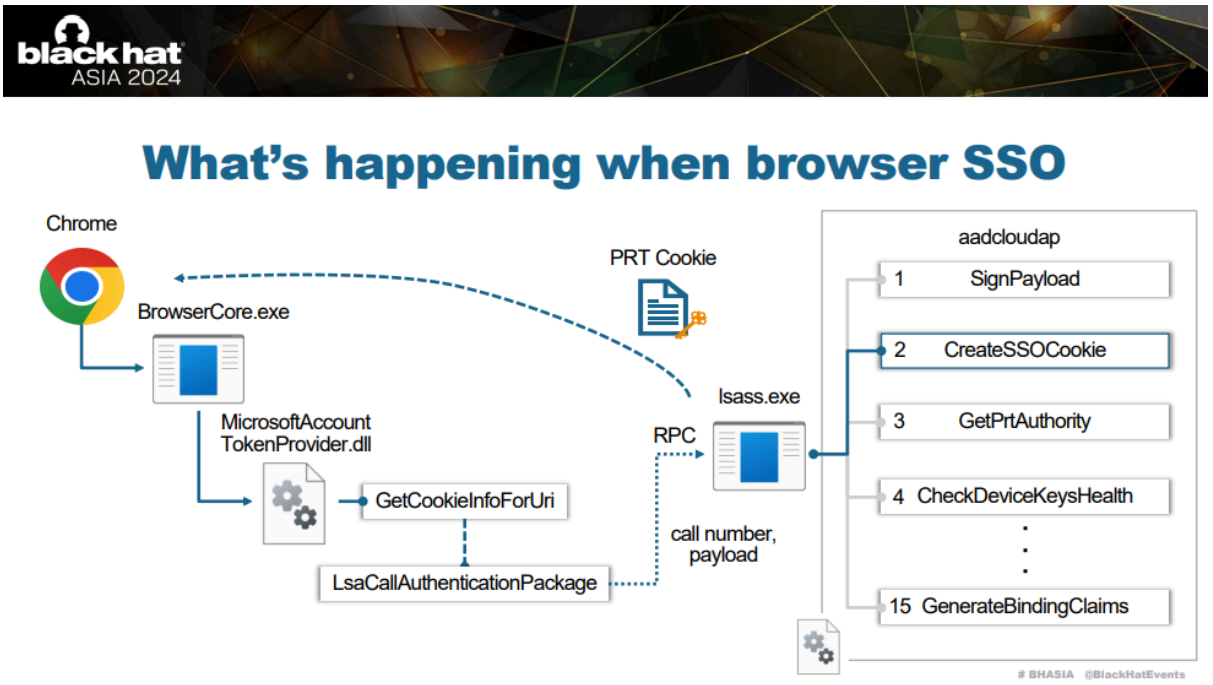


圖 8：說明瀏覽器帳號驗證原理

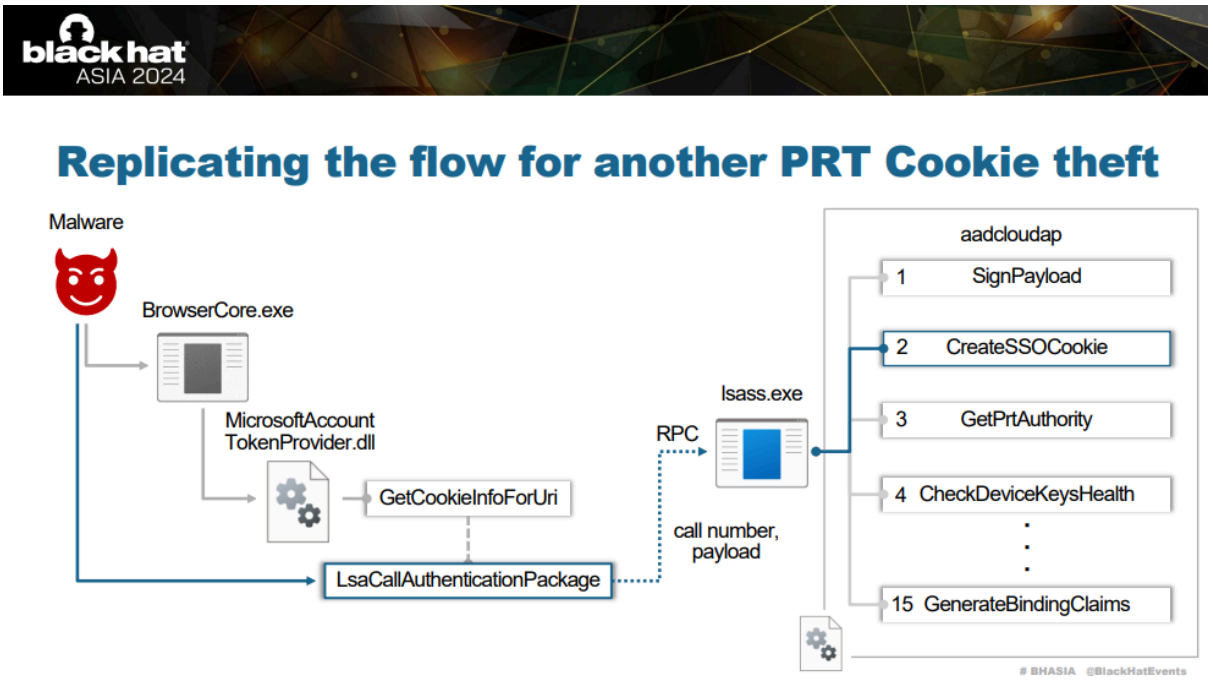


圖 9：說明攻擊原理與方法

八、Chinese APT: A Master of Exploiting Edge Devices（中國APT：邊緣裝置利用大師）

講者：Greg Chen, Charles Li, Che Chang | TeamT5

時間：2024.04.19 (五) 14:30 - 15:00

議程連結：

https://www.blackhat.com/asia-24/briefings/schedule/#chinese-apt-a-master-of-exploiting-edge-devices-37937

簡報連結：

https://i.blackhat.com/Asia-24/Presentations/Asia-24-Chen-Chinese-APT.pdf

講者詳細探討了中國APT（Advanced Persistent Threat）如何針對邊緣設備進行漏洞利用。特別關注了這些攻擊者如何利用在邊緣設備中發現的0-day漏洞來進行初始侵入。這些邊緣設備包括Sophos防火牆、Fortinet FortiOS SSLVPN、Barracuda ESG等，並詳述了攻擊者如何在這些設備上植入惡意軟體來進行遠端控制和資料竊取。

講者描述了中國駭客利用ZyXel ZyWall USG設備建立殭屍網路的過程。他們結合兩個舊漏洞來實施遠端程式碼執行，並在設備上安裝EmergeBot進行進一步的控制。由於USG20/40是終止服務的產品，其安全漏洞並未被修補。

講者說明了中國駭客如何通過利用Sophos防火牆來散佈虛假資訊。他們在2023年1月在Sophos防火牆上植入了名為EquipDoor的惡意軟體，並利用這些被攻擊的防火牆和監控路由器，在2024年1月的台灣總統大選期間散佈虛假資訊。一個特定的例子顯示，

這些虛假資訊被發佈在台灣知名的社交論壇 PTT 上，內容涉及國家個人資料被出售和政府官員的不當行為。這些行動旨在干擾台灣的選舉進程並傳播虛假資訊。

講者展示了中國 APT 組織如何利用邊緣設備進行指揮和控制（C2）以及橫向移動攻擊。APT攻擊者利用受損的 ASUS 路由器和 HikiVision DVR 來隱藏其攻擊來源，並通過ColdFusion漏洞初次進入政府伺服器。此外，MenuPass（APT10）利用Array Networks SSLVPN進行橫向移動攻擊，並發現了零日漏洞，該漏洞被中國部落格公開。MenuPass還在日本使用專有惡意軟體BigPooh進行內部網路攻擊。

講者說明了中國駭客組織SLIME57如何攻擊郵件安全網關（如Barracuda ESG），以竊取敏感資料。他們利用了多個漏洞，以命令注入方式在解壓附件時實施反向殼攻擊。此外，SLIME57 還利用 UnRAR二進制檔案中的漏洞對台灣政府和日本IT行業的郵件網關進行攻擊，實現任意檔案寫入，進一步竊取郵件內容和附件。這些攻擊強調了加強郵件安全防護和漏洞修補的重要性。

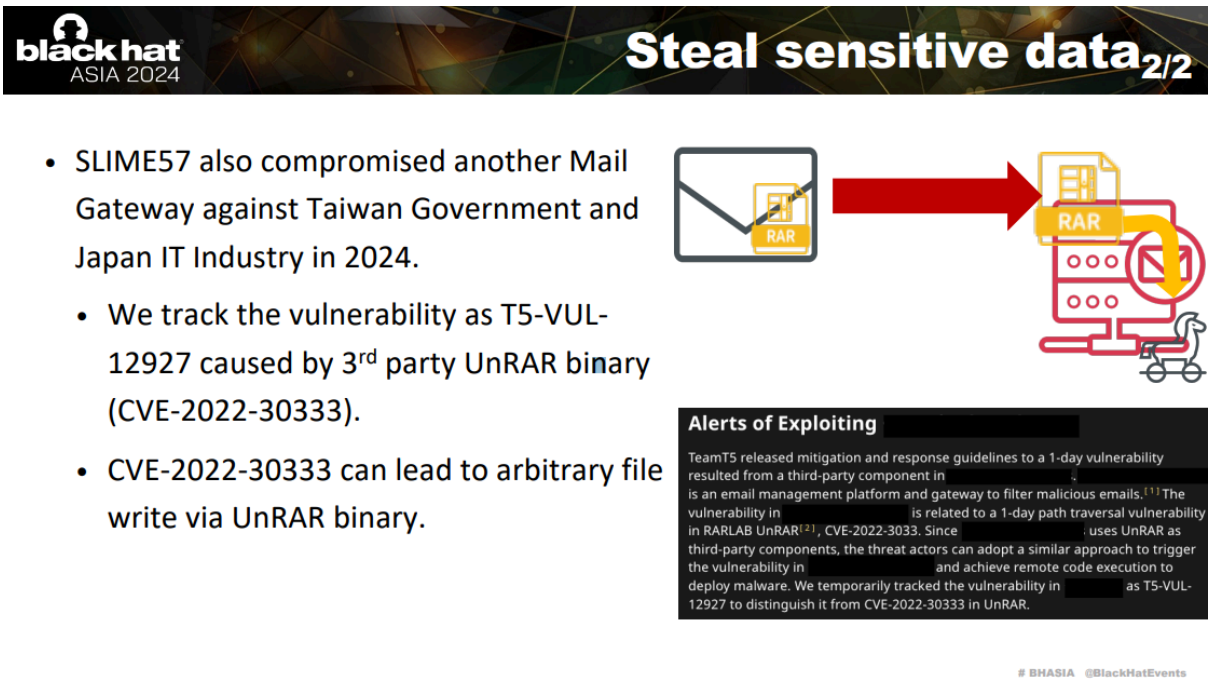


圖 10：SLIME57 攻擊台灣政府單位電子郵件

除了攻擊技術的細節，講者還討論了如何應對和緩解這些攻擊。建議包括限制邊緣設備對不必要網路服務的訪問，應用關鍵漏洞修補，以及進行有效的漏洞管理，確保使用最新的安全措施來保護組織免受這類高級持續性威脅的侵害。此外，保持邊緣設備的存取或審計日誌，並瞭解攻擊者如何理解你的設備。未來研究將聚焦於檢測和識別已被植入代理程式的邊緣設備，這些設備具有隨機連接埠、加密流量和複雜訪問限制的特點。

參、心得與建議

參加Black Hat Asia 2024是一個極具啟發性的經驗。透過多場專題演講和技術研討，對當前最先進的資安技術和威脅有了更深刻的理解。特別是在雲端資安方面，講者們展示了許多新的工具和方法，這些工具和方法不僅提升了威脅檢測和響應的效率，還揭示了現有系統中的潛在漏洞。這些知識對於我們在政府單位提升雲端環境中的安全防護能力具有重要意義。

「Breaking Managed Identity Barriers in Azure Services」是令人印象深刻的講座，講者深入探討了在Azure服務中利用託管身份進行攻擊的方法，以及如何防範這些攻擊。他們詳細介紹了如何通過分析環境變數來獲取敏感資訊，並展示了攻擊者如何利用這些變數繞過Azure的安全控制，取得系統的訪問權限。

在談及中國的網路威脅時，「China's Military Cyber Operations: Has the Strategic Support Force Come of Age?」這場演講提供了豐富的資訊。講者深入分析了中國解放軍的戰略支援部隊（SSF），並強調了其在地緣政治敏感區域的網路作戰策略，這些策略旨在破壞敵方的系統體系，達到威懾效果。這場演講揭示了中國如何通過網路手段塑造其國際地位和區域權力平衡，這些資訊對於我們理解和應對中國的網路威脅非常有幫助。

在「Bypassing Entra ID Conditional Access Like APT: A Deep Dive Into Device Authentication Mechanisms for Building Your Own PRT Cookie」的講座中，講者深入研究了如何繞過微軟Entra ID條件式存取的裝置認證。透過逆向工程微軟的認證庫，攻擊者

不需要管理員權限就能假冒裝置，從而繞過裝置基礎的存取控制策略。講者還說明了如何利用未記錄的API與儲存在TPM中的密鑰進行互動。

關於中國的網路威脅，「Chinese APT: A Master of Exploiting Edge Devices」這場演講提供了豐富的資訊。講者詳細探討了中國APT如何針對邊緣設備進行漏洞利用，特別關注了這些攻擊者如何利用在邊緣設備中發現的0-day漏洞來進行初始侵入。此外，講者還描述了中國駭客利用ZyXel ZyWall USG設備建立殭屍網路的過程，以及他們如何通過利用Sophos防火牆來散佈虛假資訊，干擾台灣的選舉進程並傳播虛假資訊。

在「The Dark Side of EDR: Repurpose EDR as an Offensive Tool」中，講者探討了EDR 系統可能存在的漏洞，特別針對Palo Alto Networks的Cortex XDR系統。研究展示了如何控制EDR系統並在其內部執行程式碼，使之成為隱蔽且持續的惡意軟體。這項研究突顯了如果EDR部署不當，可能會被惡意行為者利用來執行 APT 攻擊。

基於在會議中的學習和觀察，以加強我們機構的資訊安全防護。首先，機關可以考慮引入自動化工具來提升日誌分析的效率和準確性，確保我們能夠及時發現和應對潛在的安全威脅。這將有助於提高我們在日常的安全運營中的工作效率和準確性。

其次，我們需要加強對託管身份和環境變數的管理。在雲端服務中，託管身份和環境變數經常儲存敏感資訊，這些資訊如果被攻擊者獲取，可能會帶來嚴重的安全風險。因此，我們應該嚴格限制環境變數中包含的敏感資訊，並定期審查和更新身份管理策略，以減少潛在的安全風險。

針對中國的網路威脅，我們需要強化對關鍵基礎設施的保護。應該加強對邊緣設備的監控，確保這些設備的訪問和審計日誌得到妥善管理，並理解攻擊者的行為模式。定期審查和更新安全策略，確保我們能夠應對來自中國的各種網路攻擊。