IBM Hong Kong newsroom

IBM 發 《2024 年 X-Force 威脅情報指數報告》

——身 信息成網絡攻 重要目標 企業從安全漏洞恢復的時間更加緊迫

該報告重要發現包括

- *利用身 信息進行的網絡攻 激 71%*
- *當某項人工智能技術占到50% 的市場 額時 相關網絡安全威脅可能隨之而來*
- *2023 年 全球近 70% 的攻 以關鍵基礎設施為目標*
- *歐洲地區首當其衝 全球網絡攻 事件的32%*

香港2024年3月25日 /美通社/ -- IBM 近日發 了《2024 年 X-Force 威脅情報指數報告》 報告顯示網絡犯罪分子在加倍利用用 身 信息來攻 全球企業 這可能引發一場全球性「身 」危機。據 IBM Consulting 的進攻性與防禦性安全服務部門 IBM X-Force 的發現 2023 年 網絡犯罪分子看到了更多「登入」 而非侵入 有效帳 以攻 企業網絡的機會。這使得利用身 信息的策略成為網絡攻 發起者的首選武器。

《X-Force 威脅情報指數報告》是基於 天監測到的 130 多個國家/地區超過 1500 億個安全事件的洞察。此外 報告還從 IBM 部的多個來源收集和分析數據 包括 IBM X-Force 威脅情報指數 Incident Response、X-Force Red、IBM Managed Security Services 以及 Red Hat Insights 和 Intezer 提供的數據都對這 2024 年度報告做出了貢獻。

本年度報告的主要洞察包括

- **對關鍵基礎設施的攻 暴露了行業的「誤判」。** 在近 85% 的針對關鍵行業的攻 事件中 可以通過補丁、多因素身 驗證或最小權限原則來降低損失——這也意味著 安全行業長期以來所提的"基本安全"可能比印象中的更難實現。
- **勒索軟件組織傾向於採取更精簡的業務模式。** 去年 針對企業的勒索軟件攻 下降了近 12% 因為大型企業組織面對此類攻 往往拒 付贖金和尋求解密 而更傾向於重建其基礎設施。由於這種阻力與趨勢會降低攻 者基於加密勒索的收入預期 因此這 報告觀察到 以前專門從事勒索軟件的網絡犯罪團體已經更多地轉向信息竊取。
- **當前尚不能通過攻 生成式人工智能來獲得回報。** X-Force分析預測 當單一的生成式人工智能技術獲取接近50%的市場 額時 或者當市場整合到三種或更少的此類技術時 則可能會引發針對相關平台的大規模攻 。

IBM咨詢全球管理合 人、IBM X-Force主管Charles Henderson 「儘管基礎安全問題並沒有像人工智能主導的攻 那樣引人關注 但事實上 企業最大的安全挑戰仍然是一些基本且已知的問題 而不是那些新穎和未知的問題。身 信息一次又一次地被用來攻 企業。隨著攻 者通過人工智能來優化這一攻 策略 這一問題將會繼續惡化。」

一場圍繞身 信息的安全危機正蔓延全球

利用有效 進行攻 已成為網絡犯罪分子阻力最低的路徑 如今在暗網上有數十億個被洩露的身 憑證可供使用。在2023年 X-Force發現攻 者越來越多地發力於獲取用 身 ——其使用的信息竊取惡意軟件 長了266% 以竊取個人可識別信息 如電子郵件、社交媒體和通訊應用的憑據、銀行 詳細信息、數據等。

這種對攻 者而言「易如反掌」的入口難以被檢測到 給企業帶來昂貴的應對成本。據X-Force稱 對於攻 者使用有效 引起的重大安全事件 安全團隊需要採取的應對措施的複雜度比普通事件平均高出近200% 主要是因為防禦者需要區分網絡上 些是合法用 活動 些是惡意用 活動。事實上 IBM在《2023年數據洩露成本報告》中發現 由於被盜或被洩露的憑證引起的數據洩露需要大約11個月

的時間才能被檢測和恢復——這一響應週期是所有網絡感染中最長的。

2023年4月 美國和歐洲執法部門共同打 一個全球網絡犯罪論壇的行動凸顯了網絡不法分子對用 在線活動的廣泛入侵。該論壇收集了超過8000萬用 的 登 詳細信息。隨著不法分子利用生成式人工智能來優化他們的攻 基於身 信息的網絡威脅很可能會繼續 長。2023年 X-Force已經在暗網論壇上觀察到了超過80萬篇關於人工智能和GPT相關的帖子 再次 明瞭這些創新已經引起了網絡犯罪分子的關注和興趣。

直接「登 」關鍵基礎設施網絡發起攻 成趨勢

在全球範圍 X-Force應對的攻 中近70% 是針對關鍵基礎設施機構的 這一令人擔憂的發現突顯了網絡犯罪分子看准了這些高價 目標對系統正常運行的嚴格要求 借此實現其攻 目的。

X-Force在該領域應對的近85% 的攻 是通過利用面向公 的應用程式、網絡釣魚電子郵件和使用有效帳 發起的。後者給該該領域機構帶來了更大的風險 美國網絡和基礎設施安全相關部門表示 2022年針對政府機構、關鍵基礎設施組織和州級政府機構的成功攻中 大多數 及了使用有效帳 。這表明這些組織需要經常對其網絡環境進行壓力測試 以發現潛在的風險 並制定安全事件響應計劃。

生成式人工智能——下一個需要保障的重要領域

對於網絡犯罪分子來 從他們的違法活動中獲得相應回報的前提是其所針對的某項技術必須在全球範圍 大多數組織中被廣泛使用。正如過去的一些賦能性技術催生了相應網絡犯罪活動一樣 這種模式也很可能擴展到人工智能領域。這種現象在Windows Server的市場主導地位下的勒索軟件蔓延、Microsoft 365主導地位下的BEC詐騙 或基礎設施即服務的市場整合後的非法加密 礦等方面都有所體現。

X-Force認為 一旦生成式人工智能市場的主導格局明確 即當單一技術接近50% 的市場 額或者市場整合為三個或更少的技術時 就可能會促使網絡犯罪分子進一 投資新的攻 工具 並將人工智能作為攻 面。雖然生成式人工智能目前仍處於大規模市場應用之前的階段 但有關企業必須在網絡犯罪分子擴大犯罪活動規模之前保護好其人工智能模型。企業還應認識到 網絡犯罪分子並不需要什麼新的戰術或技術 就能通過它們現有的基礎設施入侵其人工智能模型。這也印證了IBM生成式人工智能安全框架 IBM Framework for Securing Generative AI 所強調的 **在生成式人工智能時代採取全局的安全防護非常必要。**

其它發現包括

- **歐洲已成攻 者的首選目標** 全球範圍 觀察到的攻 中 近三分之一的目標是針對歐洲的 該地區也經 了全球最多的勒索軟件攻 26% 。
- **網絡釣魚攻 都去 了** 儘管網絡釣魚攻 仍然是一個主要的感染途徑 但從2022年開始 其數量減少了44%。然而 這一攻 方式將隨著人工智能得以優化 X-Force的研究表明人工智能可以將其攻 速度提升近兩天 因此這種感染途徑仍將是網絡犯罪分子的優先選項。
- **人人都有風險** Red Hat Insights發現 在掃描中 92%的客 環境中至少有一個已知漏洞未被修復 而2023年檢測到的十大漏洞中有80%被賦予了"高風險"或"危急"的通用漏洞評分系統 CVSS 基礎嚴重性評分。
- **「Kerberoasting」攻 有利可圖** X-Force觀察到「Kerberoasting」攻 加了100% 在這一過程中攻 者試圖通過妄用Microsoft 活動目 Microsoft Active Directory 憑證來冒充用 以提升權限。
- **安全配置不當** X-Force Red的滲透測試結果顯示 安全配置不當 到了已識別總漏洞的30% 觀察到可被攻 者利用的140多種配置不當的方式。

其它資源

- **下載**2024年**《X-Force威脅情報指數報告》**。
- 在**IBM安全情報博客**中瞭解更多關於本報告的主要發現。
- 與IBM X-Force團隊**聯** 以獲取個性化的報告洞察解讀。

關於 IBM

IBM 是全球領先的混合雲與人工智能、以及企業服務提供商 為全球175個國家和地區的客 服務 助企業把握其數據洞察、簡化業務流程、降本 效 獲得行業競爭優勢。 IBM 混合雲平台和紅帽OpenShift 為全球超過4,000家政府和企業機構的關鍵性基礎設施提供有力支 例如來自金融服務、電訊和醫療健康等行業的客 助他們快速、高效、安全地實現數碼轉型。 IBM 在人工智能、量子運算、特定行業的雲解決方案以及企業服務等方面的突破性創新 使其可以為客 提供開放和靈活的選擇。 IBM 對信任、透明、責任、包容和服務的 久彌新的承諾 是我們業務發展的基石。 詢更多資料 請瀏覽 www.ibm.com/

關於 IBM 香港 請登入Facebook 頁面 www.facebook.com/IBMHongKong

傳媒 詢

郭韜 gguotao@cn.ibm.com

SOURCE IBM Hong Kong

Additional assets available online: Photos

https://hongkong.newsroom.ibm.com/2024-03-25-IBM-2024-X-Force