機械人世紀之戰 美版大嘸VS日本秘武

在美國舉辦的史上首場「美日巨型機械人大戰」，將於香港時間今日早上10時正式上演，由美國MegaBots製作的巨型機械人「Eagle Prime」，將會與日本水道橋重工製作的「Kuratas」展開一場格鬥戰。實況網站Twitch將全程直播這場世紀之戰。

美：高5米 成本近2000萬

總部設在三藩市的MegaBots，耗時近兩年製作出Eagle Prime，總成本達250萬美元(約1,950萬港元)，當中約1/5來自網絡眾籌。Eagle Prime身高5米，重12噸，使用430匹馬力的V8 LS3引擎驅動，並由兩名駕駛員操控。

日：性能成謎 遙控操作

至於來自巨型機械人故鄉的Kuratas，一切性能到賽前仍然是個謎，水道橋重工自今年4月以來沒有公佈過任何新消息，但日前公開的賽前準備片段顯示，Kuratas與兩年前首次亮相時相比已經有很大變化，除了機身換成紅色外，左手的設計亦與之前完全不同。兩年前公開的資料顯示，Kuratas重約4噸，有30個液壓關節，可以在駕駛艙或遙控操作。

打至斷手脫甲 倒地方休

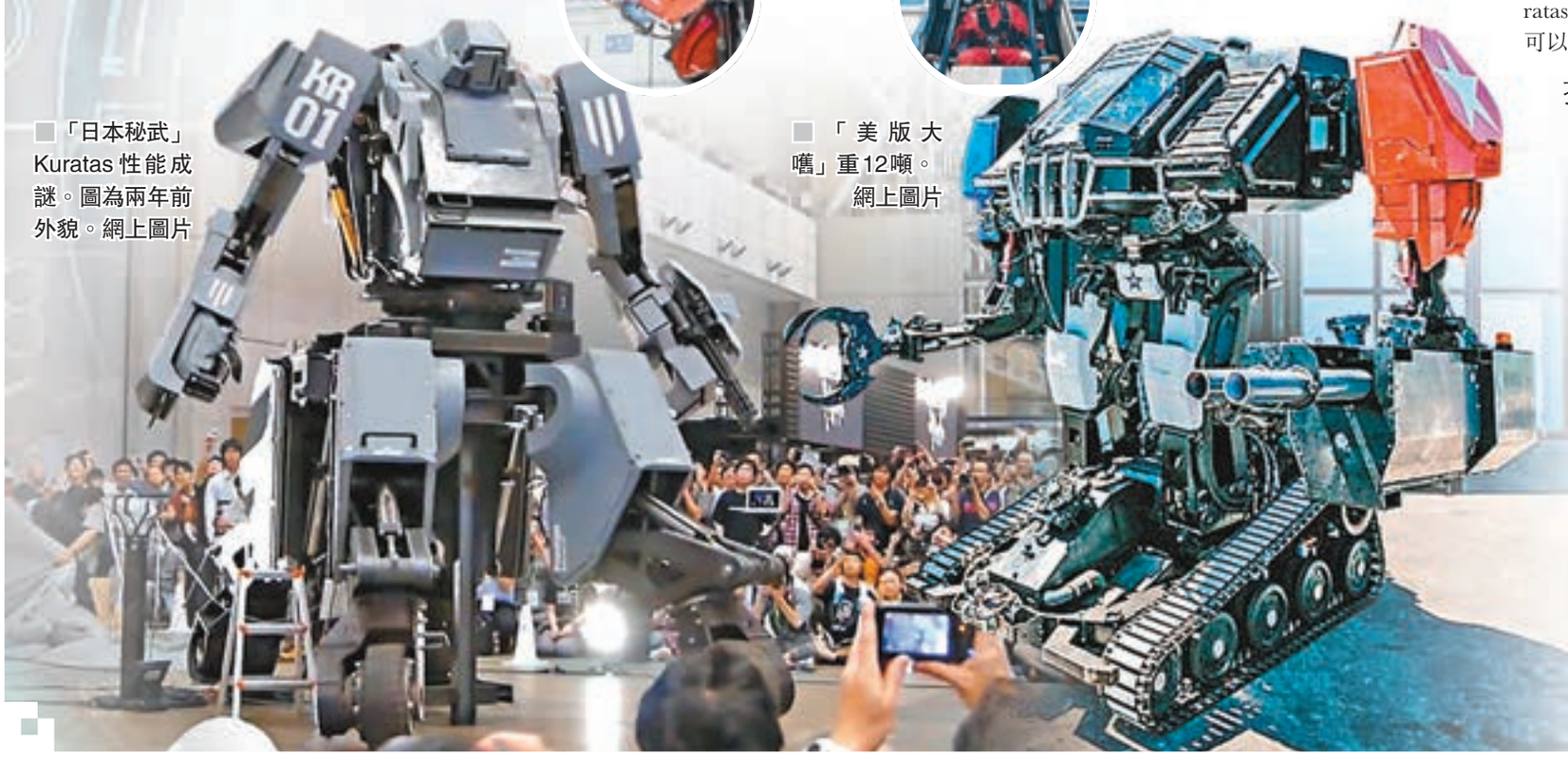
Megabots於2015年向水道橋重工下戰書，後者同意決鬥，但要求以格鬥方式進行，由於改裝機械人需時，決鬥結果遲了兩年才舉行。Megabots指，今日雙方將會打至機體冒煙、斷手脫甲，直至其中一方完全倒地不起為止。

由中國機械人藝術家孫世前領軍的「鋼鐵意志」團隊，今年初亦曾展出巨型機械人「大聖號」，並希望加入戰團，不過今日的賽事暫時沒有它的份。

■《每日郵報》/CNBC


■轉色兼強化左手


■兩名駕駛員操控


■「日本秘武」Kuratas性能成謎。圖為兩年前外貌。網上圖片

■「美版大嘸」重12噸。網上圖片

加密協議爆漏洞 41% Android裝置高危

全球Wi-Fi大危機 私隱「不設防」

全球各地廣泛使用的Wi-Fi無線網絡加密協議WPA2被揭有嚴重安全漏洞，可導致數以百萬計用戶遭攻擊，當中Android及Linux系統用家最為高危，估計有41%的Android裝置受影響。專家指，不法之徒可能利用漏洞，從Wi-Fi數據傳輸截取密碼、信用卡、電郵及其他本應加密的訊息，或者在用戶瀏覽的網站內加入惡意軟件，不論政府、企業或家用Wi-Fi網絡均有受入侵風險。專家建議用家馬上更新所有無線上網裝置及路由器，以保安全。

名為「密鑰重裝攻擊」(KRACK)的漏洞最初由比利時勒芬大學的專家發現，他們將這消息對外封鎖了數周，讓各大企業研發補救措施。

蘋果Google：數周內推更新

微軟表示，上周發佈的安全性更新修復有關漏洞，已安裝或開啟自動更新的用戶可受保護。至於蘋果公司及研發Android系統的Google則表示，將於數周內推出更新，各大網絡路由器生產商據報亦陸續發佈更新檔。

恐遭黑客勒索植木馬

勒芬大學研究員范赫夫指，KRACK並不會盜取用戶的Wi-Fi密碼，它主要針對WPA2協議的「四次握手」加密過程，強制將用家裝置的密碼設置為全部零，令所有經Wi-Fi傳輸的資料變成「不設防」，供黑客任意讀取。在個別情況下，黑客甚至可向用戶的裝置植入勒索程式或木馬程式等惡意軟件。

一般而言，用家若瀏覽經加密網站(網址前綴為HTTPS://)，所有傳輸的數據將獲額外加密，不會因為KRACK而被讀取。不過范赫夫提醒，個別網站的HTTPS協議存在漏洞，未必能夠加密資料，加上一些手機程式可能不支援HTTPS，因此仍不能掉以輕心。

專家倡安裝更新軟件

專家強調，黑客必須在用家的Wi-Fi網絡附近，才可以使用KRACK攻擊，意味家庭Wi-Fi用戶受影響的機會較小，相反政府或大企業的公用Wi-Fi則風險最高。暫時未知道黑客經KRACK發動攻擊的難度有多高，亦不知是否已發生過相關襲擊。WPA2已經有13年歷史，芬蘭網絡保安公司F-Secure指出，專家向來關注Wi-Fi能否應付21世紀網絡安全的挑戰，代表業界的Wi-Fi聯盟則強調，只要安裝軟件更新便可解決問題。■法新社/路透社/Ars Technica網站

■Wi-Fi加密協議被揭有嚴重安全漏洞，影響不少Android裝置。 網上圖片

攻「握手」加密過程 金鑰強制變零

KRACK的全名是「Key Reinstallation AttaCK」(密鑰重裝攻擊)，顧名思義，即容許黑客重設用戶的Wi-Fi加密金鑰，再直接讀取傳輸資料，攻擊的關鍵在於名為「四次握手」(4-way handshakes)的加密過程。

Wi-Fi加密協議WPA2一般使用基於AES加密技術產生的共享金鑰，保障網絡流量安全，這條金鑰會透過「四次握手」加密過程，在裝置和接入點之間分享認證。KRACK就是從「四次握手」的第3次入手，強制重設用家裝置保存的加密金鑰，即不用破解金鑰，直接將之替換成全「0」金鑰，從而將用家裝置連接到偽裝Wi-Fi網絡上，再從中偷取資料。

這個方法對於Linux系統和Android 6.0以上的系統特別有效，原因是兩者均按照電機電子工程師學會(IEEE)的要求，使用wpa_supplicant加密元件，這組元件會在首次使用加密金鑰後，將其從暫取記憶體中移除，防止金鑰被重複使用，但由於元件會把金鑰轉換成全0，結果正中KRACK的下懷。

限制多 普通黑客難仿傚

雖然微軟視窗和蘋果iOS不會受「四次握手」漏洞影響，但其金鑰仍然可能在「群組金鑰」和Fast BSS Transition握手協議中被攻擊。專家指出，KRACK攻擊方法的限制甚多，研究人員還未公佈攻擊代碼，一般黑客短期內難以仿傚。■綜合報道

簡易自保招數

更新所有無線裝置

■微軟、蘋果公司及Google等主要無線裝置系統開發商，均已經或即將發佈更新檔修復漏洞，網絡路由器的韌件亦有必要升級。

停用Wi-Fi上網

■如果路由器未能更新，可以選擇關掉Wi-Fi，直接使用LAN線連接路由器上網。至於手機等無法有線上網的裝置，則可暫時改用4G網絡，直至路由器和裝置獲得更新。

額外保安措施

■如果仍然擔心受攻擊，用家可以使用HTTPS加密協議瀏覽網站，或使用虛擬網絡(VPN)接連上網，但兩種方法各有弱點，不能過度依賴。

加密總比不加密好

■即使WPA2出現漏洞，仍是現時最安全的Wi-Fi加密方式，用家若要使用Wi-Fi上網，便應繼續以WPA2連接，否則只會讓不法之徒更易盜取資料。

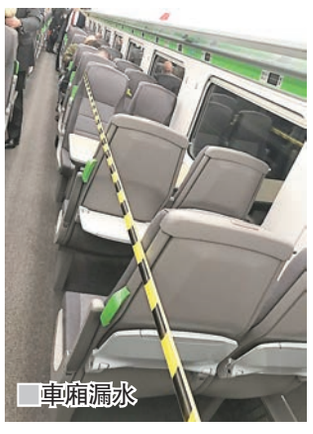
避免用公共Wi-Fi

■部分公共Wi-Fi沒有設置加密，加上任何人均可登入，風險大增。

TechCrunch網站

日立製高鐵用問題鋁 倫敦通車延誤漏水

由日本日立製作所在英國製造的城際高鐵列車，前日開始在倫敦至威爾士的線路正式運作，但列車出師不利，由於技術故障，出發時間比預定晚了近25分鐘，行駛期間更發生冷氣漏水，空調系統要關閉。日立證實列車使用了神戶製鋼所的鋁製品，但堅稱製品達英國標準。


■車廂漏水

日立表示，列車延遲出發是因為「輕微技術問題」，至於冷氣漏水則是因為原本應該排出車外的冷卻水，倒流回車廂所致。乘客在社交網站上載漏水的照片，顯示列車座位被滴濕，許多網民轉發，引起關注。結果列車最終比原定時間遲了41分鐘抵達目的地。

由英國大西方鐵路公司委託日立在英國生產的800型列車，將陸續取代1976年起服役的舊型號列車，新車據稱速度更快，載更多人。由於大西方鐵路部分路線仍然未電氣化，所以列車採用油電混合動力驅動。當局預計，待路軌改善工程明年底完結後，新列車可令早上繁忙時間的載客量增加4,000人次。

神戶製鋼擬售資產套現


■新式列車

另外，神戶製鋼所產品數據造假醜聞持續發酵，《日經新聞》昨日報道，神戶製鋼日本工廠造假時間恐長達數十年。根據投資公司Jefferies日本分公司的報告指，儘管神戶鋼鐵有足夠現金與資金應付短期所需，但正透過降低營運資金與出售資產，以籌募資金。

■《衛報》/英國廣播公司/中央社