News Buddy

騙徒誘裝毒App 遙控手機盜存款

Scammers Use Fake Apps to Steal Deposit through Smart Phone

原文

摘錄自6月15日香港《文匯報》：

有詐騙集團在社交平台開設虛假網購專頁推銷食品、旅遊和包車優惠，誘使受害人下載植入木馬程式的非官方惡意手機App，暗中奪取受害人的手機控制權，從而掌握受害人網上銀行全部資料包括保安密碼，再不留痕跡地盜走受害人銀行存款。

在東南亞地區，有超過4,000人墮入該詐騙集團的陷阱，其中新加坡和香港苦主共佔近半，損失逾兩億港元。香港警方發現騙徒發送的部分木馬程式租用香港的伺服器，遂於早前聯同新加坡以及馬來西亞警方展開代號「遙嶺」的行動，三地共拘捕156人，包括在馬來西亞拘捕兩名詐騙集團骨幹。

香港警方日前公布案情指，2023年年中，香港警方和新加坡警方發現有犯罪集團以網上購物進行詐騙。該集團在不同社交平台，例如Facebook或Instagram開設虛假假商店專頁，聲稱售賣不同貨品或者提供服務，包括食品、旅遊、包車服務等等。當有市民與假店主聯絡欲網購時，騙徒就

會要求市民到WhatsApp平台繼續通訊，在WhatsApp對話中，騙徒會假冒客服，發送一個非官方的檔案或超連結，誘使受害人下載並安裝App進行網購。

該App中其實已安裝了木馬程式，騙徒會要求用家同意開放該惡意App的所有權限，目的是令騙徒可以遠端監控市民手機。騙徒又會誘使市民在App中輸入網上銀行理財登入資料，聲稱是用來支付禮費或其他雜費。

其間，騙徒會通過實時遠程監控，取得受害人的全套登入資料，繼而安裝偽冒成地圖的App以截取受害人一次性密碼短訊。

由於偽冒的程式與真正的地圖程式太相似，受害人往往未能辨識到兩者分別，未有移除偽冒地圖App。當騙徒出監取受害人銀行資料，再轉走受害人銀行存款，得手後將相關惡意程式解除安裝減燬，受害人全程都未能察覺。

調查發現，東南亞地區有逾4,000名受害人。其中，新加坡警方在2023年共錄得1,899宗相關騙案，累計損失超過1億9,700萬港元。香港則

由2023年9月至2024年4月共有41宗同類案件，受害人損失1,200萬元，其中一名88歲老翁因為貪圖購物網站有折扣，在與對方溝通後下載惡意程式，結果被轉賬600萬元。

該詐騙集團所使用的木馬程式在「暗網」購買，主要掛載在香港及馬來西亞的伺服器上。經過三地警方深入調查，發現有50個木馬程式伺服器的租用人是兩名馬來西亞籍男子，馬來

◆警方解釋詐騙集團的犯罪手法。　　資料圖片

◆香港警方聯同新加坡以及馬來西亞警方展開代號「遙嶺」的行動。　　資料圖片

西亞警方拘捕兩名犯罪集團骨幹成員，新加坡警方則由2023年至今拘捕140人，香港警方拘捕10男4女（19歲至61歲），主要為傀儡戶口持有人。他們涉嫌由2023年2月至今年4月，利用31個戶口清洗3,450萬元犯罪得益。

香港警方已對控制木馬程式的伺服器進行數碼法理鑑證，並向相關社交平台要求移除涉案的虛假專頁。

譯文

A fraud syndicate has set up fake online shopping pages on social media platforms to promote special offers on food, travel and chartered buses, inducing victims to download unofficial malicious cell phone apps implanted with Trojan horse programs, so that they can secretly seizing control of victims' cell phones, then get hold of all the information of their online banks, including their security passwords, which can be used to steal the deposits of the victims without leaving any traces. More than 4,000 people in Southeast Asia have fallen into the trap of the fraudster, with nearly half of the victims in Singapore and Hong Kong losing more than HK$200 million. The Hong Kong police found that some of the Trojan horse programs sent by the fraudsters rented servers in Hong Kong, so they launched an operation code-named "Operation DISTANTHILL" together with the Singaporean and Malaysian police earlier and arrested a total of 156 people in the three places, including two backbones of the fraud syndicate in Malaysia.

The Hong Kong Police recently announced that in mid-2023, the Hong Kong Police and the

Singapore Police discovered that a criminal syndicate was using online shopping as fraud. The syndicate set up fake store pages on social media platforms, such as Facebook or Instagram, claiming to sell other goods or provide services, including food, travel, chartered car services, etc. When a public member contacted the fake shop owner, they were told that the shop owner was not a member of the syndicate and that the shop owner was not a member of the syndicate. When a member of the public contacts the fake store owner to make an online purchase, the scammer will ask the member of the public to continue the conversation on WhatsApp. During the WhatsApp conversation, the scammer will pretend to be a "customer service agent" and send out an unofficial file or hyperlink to entice the victim to download and install the app to make an online purchase.

A Trojan horse program is installed in the app, and the scammer will ask the user to agree to open all the permissions of the malicious app so that the scammer can remotely monitor the citizen's cell phone. The fraudster will then trick the user into entering their online banking login de-

tails into the app, claiming that it is for payment of shipping or other miscellaneous fees. In the meantime, the fraudster will obtain the victim's complete set of login information through real-time remote monitoring, then install an app that pretends to be a map to intercept the victim's one-time password SMS.

As the fake program is too similar to the actual map program, the victim often fails to recognize the difference between the two and fails to remove the phoney map app. The victim remains unaware of the fraudster's actions when the fraudster steals the victim's bank details, transfers the victim's bank deposits, and then uninstalls the malicious program to destroy the victim's ID after the fraudster has gained access to the victim's bank account.

The investigation into the scam revealed a shocking number of victims in Southeast Asia, exceeding 4,000. In Singapore alone, the police recorded a staggering 1,899 fraud cases in 2023, resulting in a cumulative loss of over HK$197 million. Hong Kong also saw its share of victims, with 41 similar cases reported from September 2023 to April 2024, leading to a loss of $12 mil-

lion. These numbers are not just statistics, they represent real people, like an 88-year-old man who lost $6 million after falling for the scam while trying to get a discount on a shopping website.

The Trojan horse program used by the fraudster group was purchased on the "dark web" and was mainly hosted on servers in Hong Kong and Malaysia. After in-depth investigations by the police in the three places, it was found that the renters of 50 Trojan horse program servers were two Malaysian men. The Malaysian police arrested two key members of the crime syndicate. In contrast, the Singaporean police arrested 140 people from 2023 to the present, and the Hong Kong police arrested ten males and four females (aged between 19 and 61), who were mainly puppet account holders. They are suspected of using 31 accounts to launder $34.5 million in criminal proceeds from February 2023 to April this year.

The Hong Kong Police have conducted digital forensics on the server controlling the Trojan horse program and have requested the relevant social media platforms to remove the fake pages involved in the case.

◆琬琰

部落有盟友 島嶼出英雄

貼地英文

上期我們談到一些頗具趣味的州名，這期我們還會看到更多有趣的原住民詞：

奧克拉荷馬（Oklahoma）

A native chief suggested to called themselves as Oklahoma. Okla was translated as people. And homa is red. That's red people. 一位土著酋長建議稱他們為Oklahoma，Okla譯為人群，homa就是紅色的，加起來是「紅人」。

印第安納（Indiana）

The US Congress purchased the Indiana territory previously occupied by several tribes. Indiana was referring to the several tribes collectively in the treaty. 美國國會從幾個部落買下了他們的地，印第安納就是條約中所謂的幾個部落。

奧勒岡（Oregon）

It could be "big paw", "a mis-spelled river name", "a herb called big ear", or "hearing the water". 奧勒岡州名的起源有多種說法，並來自多種語言。它可能是「大爪子」、「拼寫錯誤的河流名稱」、「一種叫大耳朵的草藥」或「聽到水聲」。

德克薩斯（Texas）

Texas was translated from native word as friend or ally to descrive the relationship among the four tribes. 德克薩斯從從住民詞明友或盟友翻譯而來。

南、北達科他（South and North Dakota)

Before Dakotas were applying the statehood, they were two regions of people living far apart. When came to fixing the capital location, their emotions had boiled. Finally, South and North Dakota were admitted as two new states. 在達科他申請成為州之前，兩地居民住在相距甚遠的地區。因首都選址，兩地的人也沸騰起來。最終造成南和北達科他州的出現。

緬因（Maine）

Maine could be called as main or mainland，which means main is to differentiate the mainland from the islands around it. 緬因州想要是大地或大陸，這意味着它主要是將大陸與其周圍的島嶼區分開來。

阿拉斯加（Alaska）

Alaska means in Aleut-language means the mainland. In more detail, it is literally "the object towards which the action of the sea is directed". 阿拉斯加在阿留申語中的意思是大陸。更詳細地說，它的字面意思是「海洋活動所指向的一個目標」。

夏威夷（Hawaii）

Hawaii may mean homeland. Some said Hawaii was named after a Polynesian hero who discovered it. 夏威夷可能是祖國的意思。有人說夏威夷是傳說中發現玻里尼西亞的英雄的名字。

美國有五個不達到州級的領地（Territories）：

美屬薩摩亞（American Samoa）

The source is uncertain. Samoa is compounded of "Sa" meaning "tribe people" and "Moa" which means "chicken" a highest-ranking titleholder of eastern (American) Samoa. 薩摩亞由Sa（意為部落民）和Moa（意為「雞」）所組成，雞是指薩摩亞東部（即美屬部）最高頭銜持有者的「家族」。

美屬處女群島（United States Virgin Islands）

Columbus gave them the name Saint Ursula and her 11,000 Virgins, later shortened to The Virgins, after the legend of Saint Ursula. 哥倫布將群島命名為聖烏蘇拉和她的一萬一千名處女，後來縮寫為The Virgins，以紀念聖烏蘇拉的傳說。烏蘇拉因堅持信仰和純潔而被殺，她的一萬一千名同伴也全被殺了。

北馬利安納群島（Northern Mariana Islands）

The islands name was to honour Mariana of Austria, then regent of Spain. 該島的命名是為了紀念奧地利的瑪麗安娜，她後來成為西班牙王后，再之後為攝政者。

關島（Guam）

Guam means a "place that has" or" a place of resources". 關島的意思是「自給的地方」或「充滿資源之地」。

波多黎各（Puerto Rico）

In Spanish, Puerto Rico is a rich port. So ironic. It's broke. 在西班牙語中，它是富有的港口。諷刺的是它破產了。

至此五十州的州名我們已全部了解，與外國友人聊天的時候，想必不會再無話可說了吧。

◆康源 專業英語導師

木建築設計體現古人智慧

恒大清思

在古代中國，建築不僅是人們遮風避雨和安身立命的居所，更是藝術和文化的結晶。其中，木材因易於獲取、施工周期又短，加上獨特的榫卯結構賦予建築物優良的抗震性能，而成為中國古代建築的主流。

然而，木結構長期暴露於潮濕的環境中，很容易因吸收濕氣而導致木材發霉和腐爛，甚至會引來蟲蟻如白蟻等的侵害，以致降低建築物的使用壽命。因此，如何增強建築物的防潮和防蟲性能，便成為古代木建築設計和維護中不可或缺的重要環節。

古人在建築材料的選擇上，早已深知不同木材的防潮性能有所差異。他們傾向於使用抗潮能力較高的木材，例如楠木、柚木和杉木等。這些木材質地堅硬，紋理細密，不易受潮變形，甚至埋入土中也不容易腐爛損壞，更可以遠離害蟲的侵擾。

◆山西的應縣木塔是世界最古老的木塔。　　資料圖片

桐油灰泥 防火免蛀

古人還懂得以桐油為髹漆塗在木材上用以防蟲。《農政全書》引《齊民要術》記載，古人在青松上「鑿取大孔，入生桐油數斤，待其滲入，則堅久不蛀。」桐油具有特殊的性質，能夠使白蟻等害蟲遠離。

除了桐油之外，古人還採用了灰泥封護的方法，王禎《農書》就提到

「內外材木露者，悉宜灰泥塗飾，以辟火災，木又不蠹。」灰泥封護是將灰泥塗抹在木材表面，使其形成一層保護層，既有防火的作用，又能防止蟲蛀。

除了選擇優質木材和對木材進行保護處理外，古人還十分注重建築的通風設計。他們會巧妙地在建築物的牆面上設計通風口，以確保木柱能夠經常保持通風和乾燥。

例如，北京紫禁城在木柱與牆體對應的位置經常會留下一個個洞口，這樣的設計可以增加牆體內部的空氣流通，從而有效避免了木柱因潮濕而腐朽。而為了進一步提高防潮和防蟲效果，古人同時在木柱下墊上了石墩。這些柱礎使木柱與地面保持一定的距離，減少木材與地面的直接接觸，降低受潮的風險，而且柱礎凸出地面上還能夠有效防止白蟻的侵害，從而延長建築物的壽命。

古人建築設計的智慧體現在材料選擇、通風設計、柱礎設計、灰泥封護和使用桐油塗材等多個方面。這些方法不僅確保了古代建築能夠歷經歲月而長久保存，同時也為我們今天設計或修繕木建築提供很好的借鑒作用。

香港恒生大學
THE HANG SENG UNIVERSITY OF HONG KONG

◆陳鴻圖博士
香港恒生大學中文系副教授