Experiencing the Changing Course of Cybercrime
網絡犯罪的演變

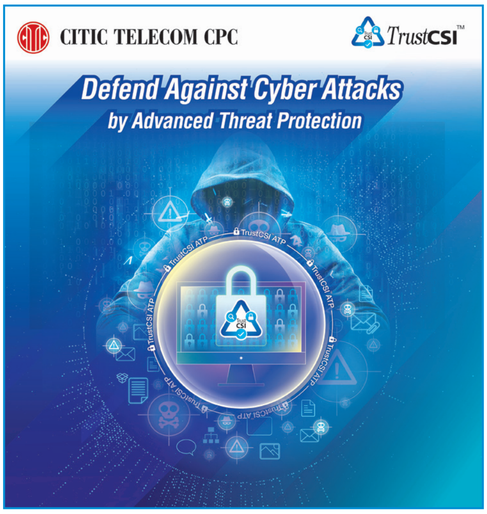
Interviewed by : Mr. Gilbert Chan
採訪者：陳錦成先生

Mr. Stephen Ho
Chief Executive Officer
CITIC Telecom International CPC Limited

何偉中先生
行政總裁
中信國際電訊（信息技術）有限公司

CITIC Telecom CPC has been delivering innovative ICT solutions to its enterprise customers since Day One. Through the efforts of Mr. Stephen Ho and his growing team of ICT professionals, the company's impressive track record began in 2002, when he identified the Virtual Private Network as the "next big thing" in the enterprise market. They created a compelling MPLS VPN solution for the increasing number of distributed enterprises requiring cost-effective, yet secure and reliable, linkage with geographically separated sites and staff, and truly delivered the right product to the right customers at the right time.

The company has now grown into a multi-ISO-certified global corporation, with over 1,000 staff, more than 140 points of presence across 130 countries, and an extensive carrier-class worldwide infrastructure. The company also continues to lead the market in many ways with its flagship portfolio of innovative ICT solutions, including cloud computing, enterprise connectivity, data center offerings, and highly sophisticated security solutions to thwart today's wide variety of complex and ever changing digital threats, including cybercrime.



中信國際電訊CPC自成立以來，一直致力向企業客戶提供創新ICT解決方案。自2002年起，在何偉中先生及其領導的ICT專業團隊的共同努力下，中信國際電訊CPC創下一個又一個驕人佳績。在公司成立初期，何先生已深諳虛擬專用網絡將成為企業市場的一大趨勢；事實上，企業市場上有很多分散式經營的企業，這些企業需要具有成本效益、安全可靠並備的專用網絡，藉此連繫不同地區的辦工室和員工。因此，中信國際電訊CPC早著先機，推出MPLS VPN服務，適時為企業提供合適的解決方案。

現時公司已發展成為一家業務遍及全球，並獲得多項ISO國際認證的企業，擁有超過1,000位員工及140個服務據點，覆蓋全球130多個國家和地區，而其電信級的網絡基建更已涵蓋全球廣泛地區。中信國際電訊CPC擁有全面及創新的ICT解決方案，持續領先市場同業，一系列的旗艦產品包括雲端運算方案、企業專用網絡方案、雲數據中心服務和信息安全管理服務。憑藉多元的服務，公司有助企業客戶應對現今複雜多變的數碼威脅，包括日漸盛行的網絡犯罪挑戰。

現今的網絡犯罪手法

科技發展日新月異，不法之徒乘機利用先進科技犯案，何偉中先生認為隨著科技的進步，網絡犯罪手法亦層出不窮：「今日網絡犯罪的手法與過往十年、二十年前的十分不同，早期主要涉及破解密碼入侵系統，隨著科技演進，惡意軟件、電腦病毒，甚或是零日攻擊（zero-day attack）已屢見不鮮。」

由於網絡犯罪頻生，加上傳媒的報導，都提高了公眾對網絡威脅的關注和認知，各行業也因此引入不同的強制性監管措施，首當其衝的是金融服務業。儘管如此，網絡犯罪仍然未有被遏止的跡象，其中原因是很少人能具體地理解到他們面對的是哪些威脅，以及可以選用哪些方案來加強信息安全。

Cybercrime Methods Today

"Cybercrime today is not like it was ten or twenty years ago," said Ho. "The earliest kinds of cybercrime mostly involved trying to hack passwords. Then there were malware, viruses and sophisticated advanced zero-day attacks."

In the news, high profile attacks have raised the public's general awareness of these threats, and various mandatory regulatory measures have been implemented, particularly in the financial industry. Yet, people and companies continue to be victimized, partly because not enough people truly understand what kinds of specific threats exist, and how to be protected against them.

Today, the most well-known attacks include phishing (sending emails to trick potential victims into clicking fake websites that look genuine and stealing their login information), malware (viruses and Trojan Horse applications that are inadvertently installed on devices), and ransomware (a special kind of malware that locks user data, or threatens to release private information, unless ransom money is paid).

The WannaCry attack is an excellent example of both malware and ransomware. This high profile 2017 worldwide attack targeted vulnerabilities in Microsoft Windows, and when a victim's computer system is infected, WannaCry would encrypt and lock up all the computer data, then request ransom payment in Bitcoin.

One of the most interesting aspects of WannaCry was its origin. It was later discovered that WannaCry was actually based on a software tool created by the NSA (National Security Agency). Criminals had stolen this information from NSA, and used it to create WannaCry.

"The lesson we can learn from WannaCry is that it's not just a malware created by criminals, but they actually stole the core hacking tools," said Ho. "So, first there was intrusion into the enterprise, then intellectual property theft, and all this later led to the malware and ransomware."

While ransomware such as WannaCry tries to directly extort money from victims (not all victims will pay), a more subtle variant is exemplified by WannaMine. Instead of alerting victims to their presence, these types of malware hide in the background and utilize the infected computer's system resources for nefarious activities. In the case of WannaMine, the infected computer's processing power is used to "mine" (or calculate) cryptocurrency, with the mined cryptocurrency automatically transferred to the attacker's digital wallet. WannaMine slowed down computer systems, and most of its victims were in Europe. Unless detected, malware such as WannaMine are a kind of digital parasite, and can cause many problems (deteriorating an e-commerce server's responsiveness, for example).

As sophisticated as they are, WannaCry and WannaMine merely represent two types of advanced attacks, and criminals have evolved other elaborate ways of conducting their operations, including leveraging zero-day vulnerability.

談到現今最流行的網絡攻擊方式，包括網絡釣魚攻擊（Phishing）— 主要透過電子郵件吸引受害者點擊虛假網站，以竊取個人登錄資料；惡意軟件（Malware）— 在受害者不為意的情況下，在其電子設備上安裝病毒或木馬程式；勒索軟件（Ransomware）— 一種特殊的惡意軟件，主要是封鎖受害人的資料及數據，甚或威脅將個人的私隱資料公開，以要脅受害機構支付「贖金」，否則不會將有關資料解封。

去年肆虐全球的「WannaCry」，便是惡意軟件和勒索軟件的一個例子。「WannaCry」在2017年針對微軟Windows系統的漏洞，對全球Windows的用戶發動攻擊，當用戶的電腦系統被「感染」時，病毒會加密和鎖定所有電腦中的檔案及數據，藉此要求用戶以比特幣繳付贖金，以冀獲取由攻擊者提供的解密金鑰。

除了所帶來的影響外，「WannaCry」的起源也是其中一個受外界關注的地方。勒索事件發生後，經過深入調查，發現原來「WannaCry」實際上是基於美國國家安全局（NSA）的一個軟件工具而開發。犯罪分子從美國國家安全局竊取了這個軟件工具的資料，再加以利用製造成「WannaCry」。

何先生指出，「『WannaCry』給全球上了寶貴的一課，它不單是由犯罪分子創造的惡意軟件，更是他們竊取了核心黑客工具的憑證。黑客首先入侵企業系統，接著盜取資訊及數據，侵犯知識產權，這一切都加深了該惡意軟件和勒索軟件對受害機構所帶來的影響。」

如果說「WannaCry」是透過封鎖受害機構所儲存的資料及數據，以公開進行勒索活動（事實上並非所有受害者都會付錢），另一款變種的「WannaMine」則是更巧妙的隱藏惡意軟件。與「WannaCry」不同，「WannaMine」不會讓受害機構知道它的存在，這類惡意軟件通常隱藏在電腦系統的後台，利用受感染的系統資源偷偷進行入侵者的目標行動。事實上，「WannaMine」是一款以開發加密貨幣為目標的惡意軟件，受感染的電腦會隱蔽地被強制利用作開發或計算加密貨幣（俗稱「挖礦」），被開發的加密貨幣會自動轉移到入侵者的電子錢包中。而在挖礦過程中，受害機構的電腦運作速度會在不明顯的情況下被減慢，使電腦的運算能力持續消耗，影響巨大。目前來說，受害機構大部分集中在歐洲地區。這類的惡意軟件可說是「數碼寄生蟲」，除非電腦被檢測到受感染，否則難以杜絕，甚至引起其他網絡安全問題，如嚴重影響電子商貿的回應能力等。

網絡犯罪手法不斷演變，「WannaCry」和「WannaMine」僅代表其中兩種先進的信息安全攻擊類型，事實上犯罪分子利用各種精密的方法，瞄準企業的網絡漏洞，推陳出新地作出攻擊，其中包括利用零日漏洞（zero-day vulnerability）。

Cutting-edge Technologies Boost Human-Machine Interaction

Artificial Intelligence is one such way. The use of AI in cybercrime is increasing. With AI, attacks can be more "productive" and easily mass target a large number of people and companies (including even small businesses, when in the past hackers only focused on large organizations). Massive email attacks and phone scams can be conducted using AI. The new AI-based attacks are also better at masquerading as genuine communications and therefore more people can be fooled into clicking to a fake website, downloading malware, or answering the phone and talking to the scammers.

Speech Recognition is another technology adopted by these criminals. Some scammers record victims' voices on the phone and use these recorded voices to authenticate voiceprint biometrics, such as with some banking systems. When attackers combine AI to call numerous phones, and use speech recognition to harvest voice signatures, within a short time they can collect a very large quantity of voice samples from potential victims.

One of the most crucial emerging areas of vulnerability in the modern age is the domain of the Internet of Things (IoT). Like many other cities, Hong Kong is moving towards the era of the Smart City, with a 5G mobile network infrastructure that will support literally billions of connected devices. Hackers are already starting to target these hardware devices. For example, duplicating the wireless key devices of automobiles to unlock cars and steal items inside them, or even drive away with the vehicles. Other criminals are targeting mobile phones, and even finding ways to steal money using contactless payment systems, including the contactless cards in victims' wallets.

With upcoming 5G and IoT, even more attention must be paid to fully secure a large number of devices, in addition to the underlying mobile infrastructure itself. The Smart City era of IoT will feature many sensor-type devices that send out signals when a predetermined stimulus is detected (such as if a room falls below a certain temperature, or when movement is detected), alongside numerous surveillance cameras. All these devices are prone to security breaches. For instance, in 2017, many surveillance cameras in Washington DC were hacked, ironically not to commandeer cameras to spy on the city, but to exploit the Internet-connected computers behind the cameras to send ransomware-laden spam emails. So while IoT has the potential to improve our lifestyles within a Smart City framework, IoT also requires a new paradigm of ICT security.

Advice for Cybercrime Prevention

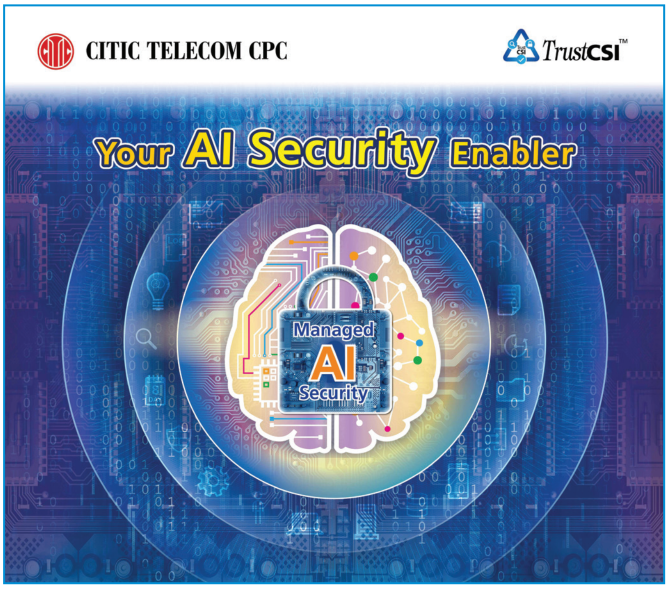
As a long time observer of the changing nature of cybercrime, and an active participant in its prevention, Stephen Ho has valuable advice: "Always double-check everything," he warns. "For example, telephone scammers can now show a Caller ID of people you know, and trick you into revealing information or authorizing transactions. Parents have been tricked by WhatsApp messages they thought were from their children, and sent money to certain accounts, thinking they were letting their children buy games and

尖端技術促進人類與機械互動

人工智能（Artificial Intelligence，AI）是其中一種被廣泛使用作網絡犯罪的手法，統計數字更顯示有上升趨勢。與傳統黑客針對少數人的入侵行為相比，利用人工智能技術，網絡攻擊可以更高效，更容易針對大量的個人和公司目標，更由過往只針對大型機構，進而將數以千萬計的小型企業也納入成為攻擊範圍。大規模的電子郵件攻擊和電話詐騙可以利用人工智能來進行，而新型的人工智能攻擊更可偽裝成「個體」跟人作「真正」的通訊交流，誘騙更多被害者到訪虛假的網站、下載惡意軟件，甚或接聽電話時與騙子「交談」，從而被盜取個人資料，遭受到財產損失。

另外，語音識別（Speech Recognition）亦是另一種不法分子常利用的技術。當他們致電受害者時，會同時記錄受害者的聲音，從而利用這些聲音來作「語音生物識別」驗證。要在短時間內從大量的潛在受害者身上取得語音樣本，不法分子會先以人工智能技術大量撥打電話號碼，撥通後再以語音識別技術來收集語音簽名（voice signature），以便進行不法的欺詐活動。例如一些銀行系統會利用「語音生物識別」技術作驗證，客戶通過驗證後方可使用銀行的特定服務；不法份子便利用這個機會，在盜取受害者的語音簽名後以此通過銀行驗證，繼而竊取金錢或作其他不法用途。

談到目前其中一個最易受攻擊的新興領域，可說是物聯網（IoT）的興起。與全球許多城市一樣，香港正逐步走向智能城市（Smart City） 的時代，透過5G流動網絡基礎設施，用作支援數以十億計的通訊設備。部分黑客已瞄準這些硬件設備，如透過複製汽車的無線匙裝置，為汽車解鎖，從中偷走車內物品，甚至運走汽車。另外，部分黑客則以流動電話為目標，他們千方百計通過非接觸式支付系統來盜取金錢，包括受害者錢包中的非接觸式信用卡。



other software. Always double-check and never assume anything nowadays."

Ho also recommends using two-factor authentication (which usually involves a physical device, along with a password) for everything, especially email and financial transactions.

For corporations, he suggests focusing on vulnerability management, including being validated with security ISO certifications, and being particularly mindful that properly trained professionals are looking after cloud services. "With cloud systems, all your sensitive information is available online, even when you are not actively using the applications," he says.

In fact, CITIC Telecom CPC is precisely helping his customers in all these areas, including round-the-clock staffing to monitor and troubleshoot cloud platforms 24x7x365, plus lock down customers' enterprise infrastructure with advanced security solutions. "We continually enhance our TrustCSI™ security product to keep on the cutting edge of information security," explains Ho. "For example, we recently added a TrustCSI™ Secure AI service, which uses User and Entity Behavior Analytics (or UEBA) to detect anomalous enterprise activity. We are helping our customers stay ahead of the tools that attackers might use."

CITIC Telecom CPC also operates dedicated Security Operations Centers (SOCs), which are all certified for ISO 27001 (Information Security Management). In fact, the company was the first IaaS provider in Hong Kong to be certified for ISO 27017 (Code of Practice for Information Security Controls for Cloud Services).

"Our security and cloud experts are always on hand to monitor systems and alert our customers in realtime of any anomalies, so prompt action can be taken," explains Ho.

The TrustCSI™ solution suite is actually a flagship family of information security solutions encompassing a plethora of security technologies, all easily interoperating with the company's other offerings.

"World-class security is available throughout all our solutions and services," clarified Ho. "We have ethical hackers to uncover infrastructure loopholes, and powerful security features in our cloud and network solutions. In fact, our latest Software Defined WAN solution, branded as TrueCONNECT™ Hybrid, uses strong security to ensure network resilience and peace of mind for our customers leveraging the benefits of flexibility and agility in this cloud era."

As a veteran of cybercrime prevention, Stephen Ho has seen a lot. Although criminals will continue to refine their methods of attack, perhaps Ho's advice of proactive prevention is the best measure against these ever changing threats.

隨著即將踏入5G和物聯網的時代，外界除了需要把注意力放在流動基礎設施外，更需要投入更大力度確保大量設備的安全。智能城市的物聯網時代，標誌著將會出現大量具感應器功能的設備。這些設備廣泛應用在日常生活，簡單如房間低於某個溫度抑或檢測到某物體移動，便會發出提示訊號，而大量的監控攝錄機也是其中一些例子。正因為被廣泛應用，這些設備都容易出現安全漏洞，如2017年美國華盛頓發生過大型網絡攻擊，區內許多監控攝錄機遭到黑客入侵。而諷刺的是黑客並沒有徵用攝錄機監視這座城市，而是利用攝錄機背後連接互聯網的電腦系統發送帶有勒索軟件的垃圾郵件。因此在智能城市的框架下，物聯網縱然具有改善社會生活方式的潛力，同時也需要一種嶄新的信息及通訊技術（ICT） 安全管理模式來保障社會的信息安全。

預防網絡犯罪的建議

多年來，何偉中先生見證著網絡犯罪性質的演變，更積極參與預防行動，對此他提出了寶貴的建議，「對每件事都進行複檢，有助減低碰到網絡犯罪的機會，如電話詐騙者來電時，來電顯示已可以調教成你認識的朋友，欺騙你洩露個人訊息或授權交易；又如父母會被來自認為是自己子女的WhatsApp訊息欺騙，把錢存到某些帳戶，以為是子女購買遊戲和軟件，造成金錢上的損失。因此，大家要時刻對每件事進行複檢，預到懷疑不要心存僥倖，要仔細檢查以免落入不法份子圈套。」

何先生還建議透過雙重身份驗證來處理各種重要事務，尤其是電子郵件及進行網上金融交易（雙重身份驗證通常包括一件硬件裝置，連同相關密碼，以核對身份是否有效及正確）。

對企業而言，何先生建議集中專注在安全漏洞管理，包括通過ISO信息安全管理認證的檢測，並確保由曾受過培訓的專業人員管理雲端服務，他提到：「一旦使用雲端系統，即代表著就算你沒有主動使用任何應用程式，所有敏感的資料依然可以在網絡上被獲取。」

事實上，中信國際電訊CPC在各項ICT領域上都一直致力協助客戶，包括提供全天候專人監控、偵測及修正客戶的雲端平台，更可透過先進的信息安全服務保護客戶的企業基礎設施。何先生解釋指「我們正不斷加強旗下的TrustCSI™ 信息安全管理服務，確保一系列的服務均由尖端科技所支持。例如我們最近推出了TrustCSI™ Secure AI服務，透過利用「使用者與實體設備行為分析」（UEBA）全面監測企業網絡異常行為。無論黑客利用什麼入侵工具，我們都希望客戶能夠受到妥善保護，使企業資產免受損失。」

此外，中信國際電訊CPC還設有數個安全運作中心（SOCs），均得到 ISO 27001 信息安全管理體系認證；而公司亦是香港第一家榮獲「ISO 27017 雲端服務資訊安全管理標準」的基建即服務供應商。

何先生解釋指，「我們的信息安全及雲端服務專業團隊時刻都在監控有關系統，可及時提醒我們的客戶任何異常情況，讓客戶可立即採取相應行動」。

中信國際電訊CPC TrustCSI™ 安全管理服務套件是公司的其中一個旗艦產品，涵蓋多項信息安全技術，並可以與中信國際電訊CPC的其他產品互相協作。

何先生強調，「我們提供的所有解決方案及服務都是由世界級的安全技術及標準所保障。公司有透過「道德黑客」（ethical hackers）來揭示基礎設施的漏洞，並於我們的雲端及網絡解決方案中配置強大的安全功能。事實上，我們最近亦推出一項名為TrueCONNECT™ Hybrid的混合式軟件定義網絡解決方案，利用強大的安全功能以確保網絡的彈性，使客戶在這個訊息萬變的雲時代，可以充分利用其帶來的靈活性。」

何偉中先生在業界擁有十分資深的經驗，曾目睹很多不同的網絡犯罪例子。雖然犯罪分子會繼續完善他們的攻擊方式，何先生的主動式預防建議，或許是對付這些不斷變化的威脅的最佳方法。