ECONOMY

Cyberattacks send a wakeup call to Asia

Region's vulnerability exacerbated by belligerent states

Sreeram Chaulia

May 23, 2017 19:50 JST

Half of the computers systems infected by the "WannaCry" ransomware in the first two days of the attack were in China, according to the country's authorities.

The WannaCry malware unleashed on May 12 that locked up over 300,000 computer systems in 150 countries for ransom payment signified the mother of all cyberattacks in its geographic sway and sophistication. It unveiled a new era of hyper-globalized threats to information security and critical infrastructure that respect few national or regional boundaries, and that claim victims from all walks of life.

Yet, although the scale and magnitude of the spread of this cyber worm was worldwide, it is in Asia that the most serious alarm bells should be sounded with regard to internet security and the region's ability to meet such a challenge. Among the nations worst affected by WannaCry were China, India, Taiwan, Vietnam, Tajikistan and Kazakhstan.

According to China's National Computer Network Emergency Response Center, half of the infected systems globally in the initial two days of the attack were found to be in China. A staggering 30,000 or more educational, commercial and governmental institutions in China were paralyzed by the hostile freezing of their computer networks. Just as essential services in Europe ground to a halt, several Asian countries caught unawares suffered the same kind of severe disruption.

Research by American cybersecurity company Mandiant shows that the Asia-Pacific region is the most vulnerable to online attacks. Asia is 80% more likely to be targeted by hacking than other continents due to a variety of technical and political factors, it concluded.

Fast-growing Asian nations have forged integrated information platforms with cutting-edge web-based features like cloud computing, the internet of things and the merging of financial services with online management tools. The denser the networked nature of Asian economies, the greater the chances that they can be absolutely torn apart by determined hackers like the wielders of WannaCry.

Another reason why Asian countries have been taken hostage by ransomware is their tolerance for pirated software that lacks the safeguards inbuilt in official versions. Rapid computerization and digitization without concomitant respect for intellectual property have left Asian IT systems severely prone to pulverizing attacks such as WannaCry.

The fact that authentic Microsoft operating systems equipped with up-to-date anti-virus programs were spared while pirated versions were crippled by WannaCry speaks volumes about the typical Asian habit of looking for shortcuts, savings and cheap deals while ignoring fundamental quality issues. The WannaCry blitzkrieg is a stern reminder to Asians to alter this mindset, invest more in copyright and be more vigilant about data protection.

Politics of cybercrime

But over and above these economic and technological flaws, WannaCry is also a reflection of weakened Asian defenses to cyberattacks due to internecine geopolitical ambitions and rivalries. According to Mediant's owner, FireEye, most of the hacking that takes place in Asia is state-sponsored and aimed at scoring nationalistic points over perceived foes.

Chinese hackers, in particular, seem to be refocusing from targets in the U.S. and Europe to other parts of Asia in light of friction over competing claims in the South China Sea and rising competition for spheres of influence. Persistent Chinese penetration of computer systems in India, Indonesia, the Philippines, Vietnam, Hong Kong and Macau were reported by analysts after the 2015 U.S.-China deal on electronic spying. In that landmark agreement, the two governments committed to preventing internet-enabled theft of each other's intellectual property for commercial gain.

Having already secured access to hi-tech Western scientific and industrial secrets through both human and cyber intelligence means, China is now at a stage of using cyberattacks to complement conventional warfare to bring its opponents to their knees. FireEye says that China's hackers these days are motivated by a clear political objective of "understanding the adversary and understanding their tactics." In other words, their mandate is to gain an advantage over perceived foes by infiltrating their communications and governance infrastructure.

It is of course a supreme irony that WannaCry actually took down so much of China's own computer network while sparing that of the U.S. Nonetheless, the repeated Chinese hacking of IT systems of Asian countries has softened up the latter's immunity to blackmail by non-state, transnational actors like those which might be behind WannaCry.

Another Asian player that has emerged as a disproportionate threat in the cyber security domain is North Korea. In spite of its technological backwardness and isolation, Pyongyang has staged some audacious online attacks including those on South Korea's news media, Sony Pictures in Hollywood and the central bank of Bangladesh. A hacking group called "Lazarus," which Western intelligence identified as North Korean in origin, has raided financial information systems in a bewilderingly large number of countries worldwide in search of cash for illegal transfers.

Since WannaCry is a gigantic extortion racket with randomized global targets, the possibility that it is another daring sanctions-busting maneuver by a financially starved North Korea is plausible, though unproven. Given that China is a major victim of the havoc unleashed by WannaCry, one might even speculate that the worm is a nasty surprise from North Korean dictator Kim Jong Un to a Beijing that is likely to keep tightening the economic screws on Pyongyang as punishment for its nuclear and missile tests.

Hybrid war

The manner in which ransomware was stolen from the U.S. National Security Agency's arsenal of cyber weapons by a yet-to-be-unmasked hacking group called "Shadow Brokers," and then sold online to the highest bidder, indicates that WannaCry is more than just a global heist with commercial motives.

This episode provides a rare window into how the intelligence agencies of big powers are stockpiling internet vulnerabilities for potential use against their competitors, and how these same nations are being embarrassed by leaks about their secret weapons by anarchistic whistleblowers or by other states masquerading behind the smokescreen of ransomware.

The advent of WannaCry is something of a second "Edward Snowden moment" for the U.S. government, which has much to explain about the provenance and purpose of the worm, which has attacked Russia with particular vehemence. Snowden, a National Security Agency contractor, is still on the run from U.S. authorities after he leaked classified information about Western global surveillance programs in 2013.

The key takeaway for Asia from the globalization of ransomware is that we are living in a mixed, hybrid stage of cyber insecurity. WannaCry is not mere cybercrime with pecuniary aims, but a symptom of a complex cyberwarfare matrix with political roots.

As the most geopolitically contentious continent with multiple fault lines of conflict, Asia is the theater where ordinary cyber criminals and sophisticated intelligence agencies with massive budgets merge into a fearsome combination. From the very beginning of cyberwarfare, governments have been known to use ordinary online criminals to pilfer information and engage in virtual wars. The unprecedented scope of WannaCry will whet the appetite for such hybrid warfare.

From the mightiest of Asian powers to the lowliest and scariest, everyone now knows there are ways to access foreign-designed cyber weapons and deploy them to wreak maximum damage. Tech analysts have predicted that an even more destructive attack than WannaCry is on the cards. The game has just begun.

Sreeram Chaulia is a professor and dean at the Jindal School of International Affairs in Sonipat, India. His latest book is"Modi Doctrine: The Foreign Policy of India's Prime Minister."