Phl 10th most attacked online in Q3 — report

By RICHMOND MERCURIO

The Philippines is the 10th most attacked country worldwide in terms of online infections in the third quarter, according to cybersecurity firm Kaspersky Lab.

For the July to September period, Kaspersky Lab said it has monitored more than eight million web threats against Filipino internet users.

"While the latest threat statistics in the Philippines are relatively lower than last quarter at 10.6 million, eight million is still alarmingly a huge leap from last year's numbers. In fact, we discovered just nearly two million online threats during the third quarter of 2017," Kaspersky Lab Southeast Asia general manager Yeo Siang Tiong said.

"In the same period last year, the Philippines ranked only 35th most attacked worldwide in terms of web threats. The young and globally known internet savvy Filipinos are fast becoming a prime target for the money hungry cybercriminals. It's high time that they get their defenses up," Tiong said.

Data from the Kaspersky Security Network showed that over three-in-10 or 33.3 percent of users in the Philippines were attacked by Internet-borne threats from the three-month period.

Globally, the top five most attacked countries during the third quarter were Algeria (45 percent), Venezuela (40.7 percent), Belarus (40.5 percent), Albania (39 percent), and Moldova (37.9 percent).

Kaspersky Lab said web-based threats or online threats are malware programs that can target someone while using on acomputer.

Kaspersky said internet-borne malware have been

the internet. These browser-based threats include a range of malicious software programs that are designed to infect victims' computers.

Web threats include drive-by download that refers to the unintentional download of malicious code to one's computer or mobile device leaving it open to a cyberattack.

A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates. This infection can also be done through social engineering which involves tricking the human mind to download a legitimate-looking but infected program

used to steal money and confdential data as well as to serve as launch pads for bigger attacks against large companies worldwide.

"These types of attacks can be avoided with a lot of common sense and vigilance. The lack of cyber-hygiene habits plays a very significant role in cybercriminals' success. Filipinos need to be cautious with the sites they visit, files they share, apps they download, and the information they divulge online through social media platforms. Add-on a solution that holistically detects and blocks malware, and you will surely give these cybercriminals a hard time stealing your data and your money," Yeo said.

Smart investment opportunity arises in Amaia Steps Altaraza

For many hardworking Filipino families and professionals who dream of purchasing their own home, a place that provides a vibrant lifestyle not far from their workplaces and urban centers is what they aspire for. This makes condominium living a smart investment to make.

Top-of-mind property developer Amaia Land Corp. makes this dream more reachable to more Filipinos by offering quality yet affordable condominiums in Mega Manila, one of which is Amaia Steps Altaraza.

Strategically located on Quirino Avenue corner Governor F. Halili Avenue in Brgy. Tungkong Mangga, San Jose Del Monte, Bulacan, Amaia Steps Altaraza is Amaia Land's first affordable mid-rise condo development in Altaraza Town Center, a 55-hectare township project where urban lifestyles complement the laidback charms of community life.

With Ayala Land's expertise in building communities, Altaraza Town Center is projected to be the next growth complex in northeastern Manila. This urban community, which is ensconced within a vast spread of residences and commercial spaces, is also set against a picturesque backdrop of the Sierra Madre mountains. Small wonder why Amaia Land has chosen it as the site of Amaia Steps Altaraza.

Amaia Steps Altaraza will rise near commercial establishments like SM City San Jose del Monte, The District by Ayala Malls, Waltermart, and Puregold Tungko; educational institutions like STI College, Colegio de San Agustin, and APEC Schools; transport hubs like the MRT; and other nearby developments like Colinas Verde Residential Estate and Country Club.

Future residents of Amaia Steps Altaraza will enjoy leisurely weekends at its first-rate amenities: a large swimming pool, pretty landscaped areas, a children's play area, and a cozy clubhouse.

With its mission to serve aspiring Filipino homeowners with affordable yet quality homes, Amaia commits in building sustainable communities that support comfortable lives today and in many years to come. Amaia cares for life, the living and the spaces around it.

Best of all, owning an affordable superior-quality condo is a dream that is now being brought closer to hard-working Filipinos through Amaia Land's easy payment options: cash, deferred cash, and bank financing.

Amaia Land remains committed to ensuring comfortable lives for them today and in many years to come. Amaia CARES for life, the living, and the spaces around it.

Amaia Steps Altaraza offers spacious and masterfully designed condo units that cater to homeowners' varying tastes and needs.

Bitcoins and blockchains: Murphy's Law waiting to happen

By MANNY GONZALEZ

Murphy's Law: Whatever can go wrong, *will*.

Bitcoins (we'll use this word to mean cryptocurrencies generally, for duosyllabic convenience and to annoy crypto-pedants) have been touted as the money of tomorrow. In the Bitcoin alternate reality, you own cryptocurrencies through a digital address (like a bank account number) and a private key (like an unforgeable signature).

Most sober observers agree that cryptocurrency could never serve as money (for one, the supply of cryptocurrencies is unlimited), but feel obliged to acknowledge that blockchain technology is somewhere between "promising" and "transformative".

Really?

To simplify a very complex mechanism: Blockchains carry information in packets; data is repeated as well as spread around. When a private key is used, its validity is "vetted" by third parties solving complex mathematical problems by trial and error.

What practical advantage do blockchains provide over conventional record-keeping? And, suspending our other reasons for disbelief, in what way is cryptocurrency better than old money like dollars and euros? The answer to both questions is invariably "security": Combined with public-private key encryption, blockchain balances and records can't be stolen or tampered with.

But it just isn't so. The blockchain process is riddled with excessive system complexity, practical vulnerabilities, and utter lack of "robustness" (the ability to recover from accidents, human errors, or unforeseen events).

Blockchain/cryptocurrency address or private key lost. With government-insured bank accounts, if you can prove your identity, your deposit is there. With blockchains, ownership or control vests solely through your address and private key. Together, that's about 100 alphanumeric characters. If you lose either, all your blockchain records, cryptocurrencies included, are forever inaccessible. Keep the address/key on your computer? It might crash or be hacked. A thumb-drive is probably your best choice, but if it's mislaid or corrupted - finito. Keep a backup? Now you have two things to guard from thieving hands. Welcome to the "security" of blockchains.

Exchange hacked. Instead of handling crypto-money directly, you might work through an exchange (like a stockbroker or bank, but almost surely less trustworthy), which issues you a "wallet" to effortlessly buy or sell various cryptocurrencies. But now your private keys are recorded somewhere in the exchange. If it's hacked, you could be cleaned out. It's already happened; Mt. Gox and Coincheck together lost about $ 1 Billion.

If your bank account is hacked, you can show it wasn't you; the bank will make good. No such "save" is possible with Bitcoins; once you lose them (through hacking, inputting an incorrect destination address, or diverse other ways) they're lost forever.

Blockchain/cryptocurrency keys compromised at source. Most people get their addresses and keys from any of several helpful websites that do this for free, just because they like you. Exactly how sure are you that the site didn't keep a record of both your address and your key?

Itchy-fingered heirs and avaricious roommates. If you manage your crypto-money directly, you need to give your heirs access to your private key, right? Hope they don't pull a midnight raid while you're still alive.

And if your lover/roommate/janitor uses spyware to determine your device password and cryptocurrency key, you could lose everything and never know whodunit.

Who will guard the guardians? Suppose that blockchains are employed to keep important records. How many people should hold the key? "One"? Better hope she's immortal and incorruptible, and lives inside the vault at Fort Knox. "Greater than One"? You are merely multiplying your vulnerabilities.

Every possible "patch" or "fail-safe" just gives rise to other risks, or puts you in the same effective data-security situation as any conventional record-keeping system. Once you work through the logic tree, there is no palatable answer to this simple question applicable to any blockchain intended for general record-keeping.

Virus infects the blockchain. Are blockchains truly immune to viruses? A lot of very smart hackers are working on the matter. Stay tuned.

The validation system collapses. Blockchain/cryptocurrency transactions must be validated by third parties, called "miners", using powerful computers guzzling electricity. The average transaction validation now consumes an estimated 800 kwh, costing about $70 in China, triple in Western Europe. That's for each transaction. Many miners work on the same transaction, but only the first to finish gets paid, in a combination of new cryptocurrency and fees charged the sender.

This framework is a scaffolding waiting to collapse. Cryptocurrency mining could become unprofitable (because there are no more free coins to issue, and people are unwilling to pay rising direct fees) and simply stop. Or governments could finally realize that 800 kwh is a lot of energy to waste, when a bank could process an old-money auto-payment or cable remittance for a penny's-worth of electricity, or a filing clerk could keep a record for not much more cost. Solution? Simply prohibit this ecologically-irresponsible activity, whose only beneficiaries, so far, are speculators and criminals. China already did exactly this. Once other subsidized-electricity countries figure out why, they might follow.

If a country or company did choose to store its vital records on a form of blockchain, who would do the mining? Since there are no free cryptocurrencies to issue, would the country or company be happy to pay whatever 800 kwh costs, each and every time it paid a bill or recorded a birth? Even if the costs were cut a hundredfold by drastic improvements in the validation procedure, 70 cents per record entry can add up fast.

The 51 percent attack. Blockchains are supposedly unhackable because multiple records are "polled". If you tamper with one's records, the others will out-vote you. But mining is increasingly investment-intensive; smaller players with weaker computers have been eliminated. Someday a small group of miners acting in collusion might be processing over 51% of the work. Then they would be able to cook the blockchain books. The crypto-faithful pooh-pooh this scenario, but do you really want to bet your life savings, vital national records, and the world economy against it?

Kidnapping 201. Don't believe the movies. To move largish amounts from your normal bank, you need to sign a check, or visit in person. The system protects you by its very slowness.

In contrast, blockchain instructions go out instantly, cannot be rescinded, and when validated/executed are non-reversible. Criminals will love it. Scenario: you own Bitcoins, or are your country's Blockchain Records-Keeper. One night thugs with masks and guns force their way into your home. Two kneecaps and five minutes later, your life savings is lost forever, or your country's most sensitive records have been exposed on social media.

Because of this immanent possibility alone, it is inconceivable that blockchains/cryptocurrencies could ever serve as money (never mind all their other failings), or for any form of sensitive record-keeping - they're just too vulnerable to simple low-tech coercion.

Blockchains are hailed by some as magical, but when you subject the prospective operating practicalities to common-sense scrutiny, they turn out to be extremely convoluted and costly ways to perform functions that are already efficiently performed, cheaply, by conventional banking and record-keeping. There are several plausible scenarios under which a blockchain system could simply collapse. Finally, anyone armed with a low-tech knife or gun can easily execute an end run around supposed high-tech blockchain security.

We ignore Murphy's Law at our peril.

A former international banker and successful entrepreneur, Gonzalez was the person principally responsible for the conceptualization, design, and construction of Plantation Bay.

Bitcoins *AND* Blockchains: Murphy's Law Waiting to Happen

By Manny Gonzalez

Murphy's Law: Whatever can go wrong, *will*.

Bitcoins (we'll use this word to mean cryptocurrencies generally, for duosyllabic convenience and to annoy crypto-pedants) have been touted as the money of tomorrow. In the Bitcoin alternate reality, you own cryptocurrencies through a digital address (like a bank account number) and a private key (like an unforgeable signature).

Most sober observers agree that cryptocurrency could never serve as money (for one, the supply of cryptocurrencies is unlimited), but feel obliged to acknowledge that blockchain technology is somewhere between "promising" and "transformative".

Really?

To simplify a very complex mechanism: Blockchains carry information in packets; data is repeated as well as spread around. When a private key is used, its validity is "vetted" by third parties solving complex mathematical problems by trial and error.

What practical advantage do blockchains provide over conventional record-keeping? And, suspending our other reasons for disbelief, in what way is cryptocurrency better than old money like dollars and euros? The answer to both questions is invariably "security": Combined with public-private key encryption, blockchain balances and records can't be stolen or tampered with.

But it just isn't so. The blockchain process is riddled with excessive system complexity, practical

vulnerabilities, and utter lack of "robustness" (the ability to recover from accidents, human errors, or unforeseen events).

Blockchain/Cryptocurrency Address or Private Key Lost. With government-insured bank accounts, if you can prove your identity, your deposit is there. With blockchains, ownership or control vests solely through your address and private key. Together, that's about 100 alphanumeric characters. If you lose either, all your blockchain records, cryptocurrencies included, are forever inaccessible. Keep the address/key on your computer? It might crash or be hacked. A thumb-drive is probably your best choice, but if it's mislaid or corrupted - *finito*. Keep a backup? Now you have two things to guard from thieving hands. Welcome to the "security" of blockchains.

Exchange Hacked. Instead of handling crypto-money directly, you might work through an exchange (like a stockbroker or bank, but almost surely less trustworthy), which issues you a "wallet" to effortlessly buy or sell various cryptocurrencies. But now your private keys are recorded somewhere in the exchange. If it's hacked, you could be cleaned out. It's already happened; Mt. Gox and Coincheck together lost about US$ 1 Billion.

If your bank account is hacked, you can show it wasn't you; the bank will make good. No such "save" is possible with Bitcoins; once you lose them (through hacking, inputting an incorrect destination address, or diverse other ways) they're lost forever.

Blockchain/Cryptocurrency Keys Compromised at Source. Most people get their addresses and keys from any of several helpful websites that do this for free, just because they like you. Exactly how sure are you that the site didn't keep a record of both your address and your key?

Itchy-fingered Heirs and Avaricious Roommates. If you manage your crypto-money directly, you need to give your heirs access to your private key, right? Hope they don't pull a midnight raid while you're still alive.

And if your lover/roommate/janitor uses spyware to determine your device password and cryptocurrency key, you could lose everything and never know whodunit.

Who Will Guard the Guardians? Suppose that blockchains are employed to keep important records. How many people should hold the key? "One"? Better hope she's immortal and incorruptible, and lives inside the vault at Fort Knox. "Greater than One"? You are merely multiplying your vulnerabilities.

Every possible "patch" or "fail-safe" just gives rise to other risks, or puts you in the same effective data-security situation as any conventional record-keeping system. Once you work through the logic tree, there is no palatable answer to this simple question applicable to any blockchain intended for general record-keeping.

Virus Infects the Blockchain. Are blockchains truly immune to viruses? A lot of very smart hackers are working on the matter. Stay tuned.

The Validation System Collapses. Blockchain/cryptocurrency transactions must be validated by third parties, called "miners", using powerful computers guzzling electricity. The average transaction validation now consumes an estimated 800 kwh, costing about US$70 in China, triple in Western Europe. That's for each transaction. Many miners work on the same transaction, but only the first to finish gets paid, in a combination of new cryptocurrency and fees charged the sender.

This framework is a scaffolding waiting to collapse. Cryptocurrency mining could become unprofitable

(because there are no more free coins to issue, and people are unwilling to pay rising direct fees) and simply stop. Or governments could finally realize that 800 kwh is a lot of energy to waste, when a bank could process an old-money auto-payment or cable remittance for a penny's-worth of electricity, or a filing clerk could keep a record for not much more cost. Solution? Simply prohibit this ecologically-irresponsible activity, whose only beneficiaries, so far, are speculators and criminals. China already did exactly this. Once other subsidized-electricity countries figure out why, they might follow.

If a country or company did choose to store its vital records on a form of blockchain, who would do the mining? Since there are no free cryptocurrencies to issue, would the country or company be happy to pay whatever 800 kwh costs, each and every time it paid a bill or recorded a birth? Even if the costs were cut a hundredfold by drastic improvements in the validation procedure, 70 cents per record entry can add up fast.

The 51% Attack. Blockchains are supposedly unhackable because multiple records are "polled". If you tamper with one's records, the others will out-vote you. But mining is increasingly investment-intensive; smaller players with weaker computers have been eliminated. Someday a small group of miners acting in collusion might be processing over 51% of the work. Then they would be able to cook the blockchain books. The crypto-faithful pooh-pooh this scenario, but do you really want to bet your life savings, vital national records, and the world economy against it?

Kidnapping 201. Don't believe the movies. To move largish amounts from your normal bank, you need to sign a check, or visit in person. The system protects you by its very slowness.

In contrast, blockchain instructions go out instantly, cannot be rescinded, and when validated/executed are non-reversible. Criminals will love it. Scenario: you own Bitcoins, or are your country's Blockchain Records-Keeper. One night thugs with masks and guns force their way into your home. Two kneecaps

and five minutes later, your life savings is lost forever, or your country's most sensitive records have been exposed on social media.

Because of this immanent possibility alone, it is inconceivable that blockchains/cryptocurrencies could ever serve as money (never mind all their other failings), or for any form of sensitive record-keeping - they're just too vulnerable to simple low-tech coercion.

Blockchains are hailed by some as magical, but when you subject the prospective operating practicalities to common-sense scrutiny, they turn out to be extremely convoluted and costly ways to perform functions that are already efficiently performed, cheaply, by conventional banking and record-keeping. There are several plausible scenarios under which a blockchain system could simply collapse. Finally, anyone armed with a low-tech knife or gun can easily execute an end run around supposed high-tech blockchain security.

We ignore Murphy's Law at our peril.

For the Editor: Whereas most persons who speak out on this subject have narrow backgrounds (academics, lawyers, bankers, touts), Mr. Gonzalez brings a unique multi-disciplinary perspective – public policy, investment evaluation, technology, and practical operations management. As an officer of the World Bank, Mr. Gonzalez advised governments and financial institutions; as an investment banker he designed financial derivatives and assessed IPOs. He has also been awarded 5 US Patents related to gathering information on the internet. He has been a successful entrepreneur for many years, giving him a healthy skepticism for complex procedures with too many moving parts. MBA Columbia University, Robert J. McKim, Jr., Fellowship, and Roswell McCrea Award winner (most outstanding first-year student). AB Ateneo de Manila, Presidential Scholarship (topped the entrance examinations).