SECURITY NEXUS
A free, open access, international, peer-reviewed, online publication for the Daniel K. Inouye Asia-Pacific Center for Security Studies faculty and alumni.
apcss.org/nexus

Security Nexus Perspectives

COLLECTIVE INTELLIGENCE AND INTERNATIONAL COORDINATION: ANTIDOTE FOR THE NOVEL BIOLOGICAL ZERO-DAY EXPLOIT #COVID-19

By Dr. Rajib Subba [*]

Just as computer malware Duqu - using a zero-day vulnerability - had catastrophic impacts on computer systems and cyberspace, the novel coronavirus is causing the global economy to grind to a halt, debilitating our health systems and hampering the lives of those most vulnerable to the pandemic. It is a biological zero-day exploit that has infiltrated almost every aspect of our planet, one that seems to understand the world's vulnerabilities.

Conventionally zero-day exploit is a familiar term for computer professionals or technology savvy security professionals. Zero-day vulnerabilities are computer security vulnerabilities which are not well understood and for which no patch is available to defend against them (Chen, 2015). "Knowledge of new vulnerabilities gives cyber criminals a free pass to exploit and attack any target of their choosing while remaining undetected" (Bilge and Dumitras, 2012, p1). A zero-day attack is a cyber-attack exploiting a vulnerability that has not been disclosed publicly.

There are many examples of zero-day exploits in the digital sphere. For example, attacks on Sony Entertainment in 2014 or Microsoft in 2017 (Trojan named Dridex[2] or CVE-2016-0167[3]) were zero-day exploits. However, zero-day exploits like STUXNET and its offshoots Duqu, Flame, and Triton have gone one step further. Such malware spreads via USB drives and infects as many computers as it comes in contact with. The virus typically remains dormant if it doesn't reach the target but once it does, the results are disastrous. Some of these malwares could manipulate the frequency of programming logic circuits which means attackers, from a remote place, can alter flight routes, manipulate security surveillance systems at a defense headquarters or shutdown emergency

[*] Dr.Rajib Subba is DKI APCSS alumni of CCM13-1. The views expressed in this article are the author's alone, and do not necessarily reflect the official position of the DKI APCSS or the United States Government.

[2] https://www.phishprotection.com/content/zero-day-protection/zero-day-attack-example/

[3] https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

centers after an attack. With zero-day exploit capabilities cyber terrorism "may not have occurred yet" (Chen, 2014, p38) but "real and extant" (Noor, 2011, p59).

For emergency and security professionals, zero-day attacks by cyber criminals and terrorists pose many-fold challenges: they are not aware of the virus, the virus is spreading fast, they have no antidote and it takes a long time to develop one. By the time security professionals come up with a solution, the damage will have been done. With the advent of a new biological virus called coronavirus disease (COVID-19), such situations parallel the physical world as well.

Like when malware affects a computer system, COVID-19 has impacted almost every aspect of today's world. According to the World Health Organization (WHO), COVID-19 is an infectious disease caused by a novel coronavirus. As of now, there are no specific vaccines or treatments for COVID-19.

This biological virus has exposed zero-day vulnerabilities that we hadn't yet witnessed in recent times. The main carriers of COVID-19 are humans. It spreads primarily through droplets of saliva or discharge from the nose when an infected person coughs or sneezes. The WHO declared COVID-19 a pandemic in March and by the mid of first week of April, the world saw more than a half-million people infected and more than 56,000 dead. With the rising death toll, United Nations Secretary-General Antonio Guterres sounded an alarm on what he said was humanity's worst crisis since World War II.[4] On 2nd April, the UN General Assembly unanimously adopted a resolution (*Global solidarity to fight the coronavirus disease 2019 (COVID-19)*) [5] urging for increased global solidarity and international cooperation.

In a bid to flatten the curve, countries - in their silos - are frantically testing several methods including finding, isolating, and testing cases, quarantine, contact tracing, location finding, facial recognition and surveillance applications, restricted travel, physical and social distancing or lockdowns. Ironically, in this crisis, formal and informal in-person contacts between international actors are limited thus affecting joint efforts.

Such incidents highlight the challenges in awareness, prevention, mitigation as well as integrated coordination and cooperation among different countries across the world. However, effective international coordination among various actors during such a crisis is a challenging task. For example, the post-STUXNET period illustrates a very poor coordination among actors who were working to decipher the malware in different parts of the world. They worked independently without informing the other of their progress or failures (Zetter, 2014). Their work, which should have been "coordination by feedback" - coordination that involves transmission of new information - (March and Simon,1958), would've helped not only accelerate the deciphering of the malware, but

[4] https://www.japantimes.co.jp/news/2020/04/01/world/un-coronavirus-worst-crisis-since-world-war-ii/#.XodPZxczagQ

[5] https://www.un.org/pga/74/wp-content/uploads/sites/99/2020/03/A-74-L.52.pdf

also help create a more effective collaborative solution. There was not only a communication lapse between the actors, but also, lack of motivation to make one (Zetter, 2014).

Eventually, these actors from Belarus, Germany, France and the USA were able to decipher the malware and develop the antidote. But had they worked together; they would have been able to finish the work faster. This case study indicates fighting alone against the zero-day attacks is not sufficient due to the lack of knowledge and calls for collective intelligence. Collective intelligence is defined as "groups of individuals active collectively in ways that seem intelligent" (Malone, Laubacher and Dellarocas, 2009, p2). Collective intelligence emerges from collaboration which "involves combining knowledge (for example ideas) from a group of people to produce novel information or insight" (Segaran, 2007) as mentioned in Vivacqua and Borges (2010).

Therefore, agile and integrated international coordination among stakeholders is our best weapon against the deadly COVID-19 for which an antidote is yet to be discovered. As the rapid spread of the COVID-19 represents a global threat, joint cooperation between countries is our best defense against possible global security and economic collapse. The head of the United Nations warns that with rising health threats as well as possible economic recessions, COVID-19 may cause "enhanced instability, enhanced unrest, and enhanced conflict" in the world.[6] With the rise of COVID-19 we are witnessing a spike of fake news, misinformation and disinformation, cyber-criminal activities, racial hatred, out casting [of sick people], profiling of travelers (flagging their houses), food supply crisis, countries banning their nationals to return home from neighboring countries – creating ill equipped quarantine camps across the borders which may create national as well as regional conflicts. Moreover, COVID-19 vulnerabilities may become a tool for terrorist outfits like the Islamic State (Lumbaca, 2020).

Therefore, we must join forces in the region to respond to the current zero-day exploits which might threaten not only our national security, but also the world's stability. In such unimaginable crisis adept public leadership and communication is must to limit the consequences as well as build public trust (Canyon, 2020). At present, there may be some "confusion about what works best, and how to balance what is necessary with what is reasonable, especially for an extended period" (Cohen and Kupferschmidt, 2020). Approaches against COVID-19 that have been taken by Hong Kong, South Korea, Singapore, Taiwan and Vietnam may offer best practices to the Indo-Pacific region. Unless we work post-haste together to neutralize the 'black swan' we will perish in our own silos.

[6] https://www.japantimes.co.jp/news/2020/04/01/world/un-coronavirus-worst-crisis-since-world-war-ii/#.XodPZxczagQ

References:

1. Chen, Thomas M. Cyberterrorism after Stuxnet. Didactic Press. Kindle Edition, 2015
2. Bilge, L. and Dumitras T. CCS '12: Proceedings of the 2012 ACM conference on computer and communications security October 2012:833–844
3. Noor, E. The problem with cyberterrorism. SEARCCT's Selection of Articles, 2011;2:51-63
4. Zetter, K., Countdown to zero day: Stuxnet and the launch of the world's first digital weapon, Broadway Books, New York, 2014
5. March, J. G. and Simon, H. A., Organizations, Wiley, New York, 1958
6. Malone, Thomas W., Laubacher, Robert and Dellarocas, Chrysanthos N., Harnessing crowds: mapping the genome of collective intelligence, MIT Sloan Research Paper 2009:4732-09 dx.doi.org/10.2139/ssrn.1381502
7. Segaran, T., Programming collective intelligence: building Smart Web 2.0 applications. O'Reilly, Califoria, 2007
8. Vivacqua, A. S. and Borges, M. R. S., Collective intelligence for the design of emergency response in Proceedings of the 14th International Conference on Computer Supported Cooperative Work in Design, CSCWD, IEEE, 2010:623–628.
9. Lumbaca, J. L., Coronavirus, terrorism, and illicit activity in the Indo-Pacific, Security Nexus, 2020. https://apcss.org/nexus_authors/j-lumpy-lumbaca/
10. Canyon, D., Strategic crisis leadership in COVID-19, Security Nexus, 2020. https://apcss.org/nexus_articles/strategic-crisis-leadership-in-covid-19/
11. Cohen, J. and Kupferschmidt, K., Mass testing, school closings, lockdowns: Countries pick tactics in 'war' against coronavirus, Science, 18 March, 2020. doi:10.1126/science.abb7733 https://science.sciencemag.org/content/367/6484/1287.full

April 2020