EVOLUTION OF THE PHILIPPINE CYBER THREAT LANDSCAPE

NULLFORGE
WHITEPAPER
WP0002-2025

www.nullforge.net

ABSTRACT

In May 2000, a computer worm infected millions of Windows personal computers, prompting *the Pentagon, CIA, the British Parliament, and most large companies to shut down their mail servers and systems.* The worm spread through an email with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs. This worm is known as the “I Love You Virus” or Lovebug, originating from the Philippines. This put the Philippines on the map of cyberspace despite the country's first Internet in 1994.

The rest is history and as of 2021, Kaspersky Security Network (KSN) has published some data regarding the Philippines being targeted by cybercriminals. Kaspersky has observed increasing attacks in the country including Filipino users.

INTRODUCTION

The COVID-19 pandemic in the Philippines started in January 2020 when it first recorded its first case. In March 2020, the Philippine government implemented a national lockdown that forced Filipinos to stay at home, and most Filipinos applied for jobs online that allowed them to work from home while most IT and BPO companies retained their operations in online or hybrid setups. It has also been noted that some were not lucky enough to land a job or be given monthly salaries by the companies they are connected with, especially people working in the aviation, construction, and manufacturing industries. This change, especially the hybrid setup not only increased the number of users on the Internet but also opened a lot of possibilities of Internet jobs in the Philippines.

This paper aims to present the cyber incidents, threats, and background of Philippine cyberspace through an enumeration of the history of the hacking culture in the Philippines and the threat intelligence that Nullforge has gathered regarding the local and international threat actors that have plagued the Philippine cyberspace. It also aims to help out the study conducted by cyber security groups like Kaspersky.

HISTORY

March 29, 1994, 1:15 a.m.: *Benjie Tan, who was working for ComNet, a company that supplied Cisco routers to the Philnet project, established the Philippine's first connection to the Internet at a PLDT network center in Makati City. Shortly thereafter, he posted a short message to the Usenet newsgroup soc .culture.Filipino to alert Filipinos overseas that a link had been made. His message read: "As of March 29, 199,4 at 1:15 am Philippine time, unfortunately, 2 days late due to slight technical difficulties, the Philippines was FINALLY connected to the Internet via SprintLink. The Philippine router, a Cisco 7000 router, was attached via the services of PLDT and Sprint communications to SprintLink's router at Stockton CA. The gateway to the world for the Philippines will be via NASA Ames Research Center. For now, a 64K serial link is the information highway to the rest of the Internet world."*

March 29, 1994, *10:18 a.m.: "We're in," Dr. John Brule, a Professor Emeritus in Electrical and Computer Engineering at Syracuse University, announced at The First International E-Mail Conference at the University of San Carlos in Talamban, Cebu, signifying that Philnet's 64 kbit/s connection was live.*

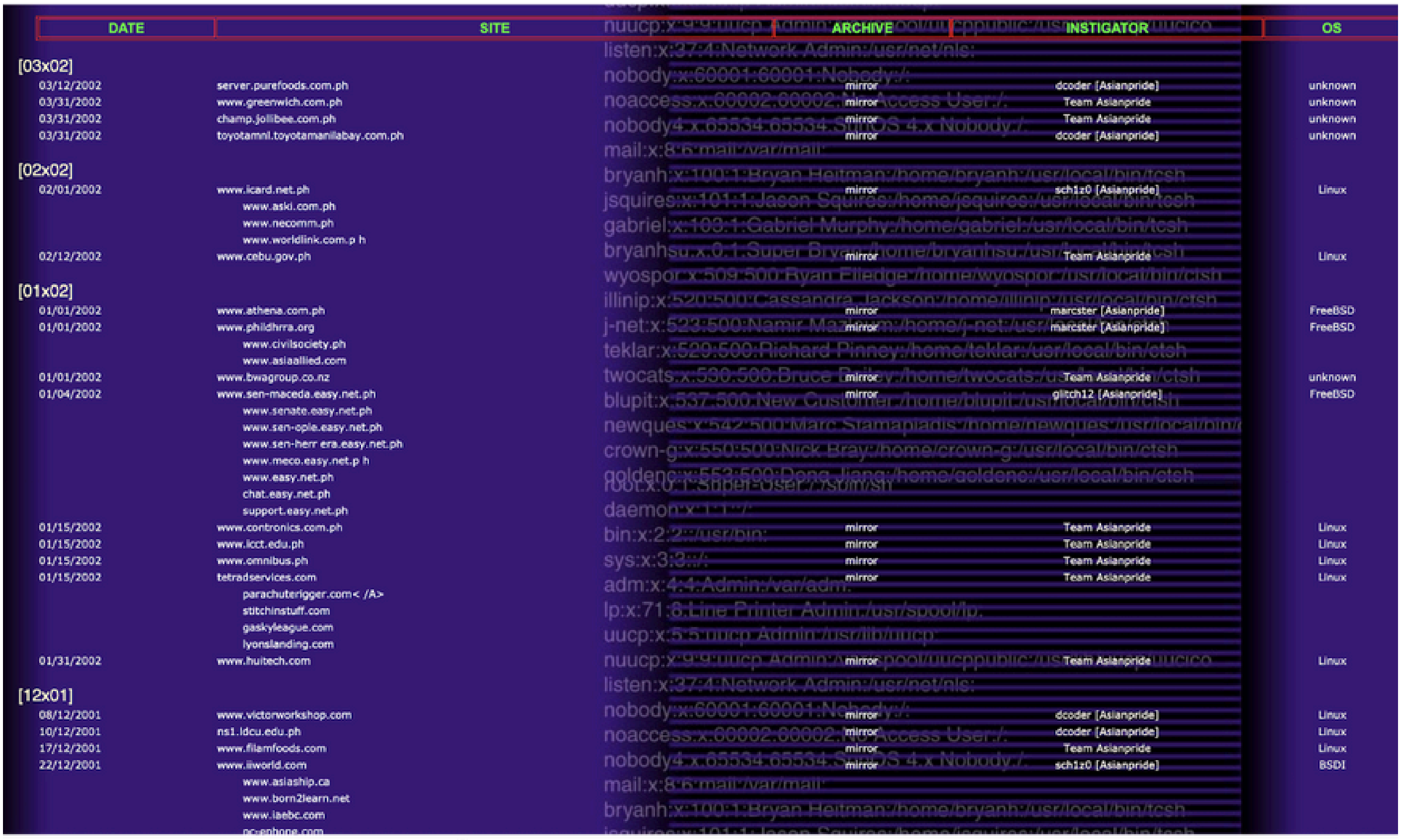
May 2000 - The I Love You Virus Incident

Since there were no laws regarding hacking in the Philippines, the alleged three suspects of the I Love You Virus were released with all charges dropped by state prosecutors.

July 2000 - The Philippine Congress enacted Republic Act No. 8792 also known as the E-Commerce Law as there were no hacking laws yet in the Philippines. This law was enacted months after the I Love You Virus outbreak.

November 2001 - The 4’ O Clock Project

A project initiated by Asianpride was launched which is the 4 o’clock Project. They aimed to publicize the flaws of Philippine websites during that time. The website contained their mass defacements and defacement mirrors or archives from the local ISP Mosaic Communications Inc (MosCom) and also popular Philippine websites like cebu.gov.ph, Globe ISP, informatics.edu.ph, ABS-CBN websites, server.purefoods.com.ph, Icct.edu.ph, etc.



DATE	SITE	ARCHIVE	INSTIGATOR	OS
[03x02]				
03/12/2002	server.purefoods.com.ph	mirror	dcoder [Asianpride]	unknown
03/31/2002	www.greenwich.com.ph	mirror	Team Asianpride	unknown
03/31/2002	champ.jollibee.com.ph	mirror	Team Asianpride	unknown
03/31/2002	toyotamnl.toyotamanilabay.com.ph	mirror	dcoder [Asianpride]	unknown
[02x02]				
02/01/2002	www.icard.net.ph www.aski.com.ph www.necomm.ph www.worldlink.com.p h	mirror	sch1z0 [Asianpride]	Linux
02/12/2002	www.cebu.gov.ph	mirror	Team Asianpride	Linux
[01x02]				
01/01/2002	www.athena.com.ph	mirror	marcster [Asianpride]	FreeBSD
01/01/2002	www.phildhrra.org www.civilsociety.ph www.asiaallied.com	mirror	marcster [Asianpride]	FreeBSD
01/01/2002	www.bwagroup.co.nz	mirror	Team Asianpride	unknown
01/04/2002	www.sen-maceda.easy.net.ph www.senate.easy.net.ph www.sen-ople.easy.net.ph www.sen-herr era.easy.net.ph www.meco.easy.net.p h www.easy.net.ph chat.easy.net.ph support.easy.net.ph	mirror	glitch12 [Asianpride]	FreeBSD
01/15/2002	www.contronics.com.ph	mirror	Team Asianpride	Linux
01/15/2002	www.icct.edu.ph	mirror	Team Asianpride	Linux
01/15/2002	www.omnibus.ph	mirror	Team Asianpride	Linux
01/15/2002	tetradservices.com parachuterigger.com< /A> stitchinstuff.com gaskyleague.com lyonslanding.com	mirror	Team Asianpride	Linux
01/31/2002	www.huitech.com	mirror	Team Asianpride	Linux
[12x01]				
08/12/2001	www.victorworkshop.com	mirror	dcoder [Asianpride]	Linux
10/12/2001	ns1.ldcu.edu.ph	mirror	dcoder [Asianpride]	Linux
17/12/2001	www.filamfoods.com	mirror	Team Asianpride	Linux
22/12/2001	www.iiworld.com www.asiaship.ca www.born2learn.net www.iaebc.com pc-ephone.com	mirror	sch1z0 [Asianpride]	BSDI

Website: fouroclockproject.iwarp.com

September 2005 - *The first Filipino to be convicted of cybercrime, particularly hacking, was JJ Maria Giner. He was convicted in September 2005 by Manila MTC Branch 14 Judge Rosalyn Mislos-Loja. Giner pleaded guilty to hacking the government portal "gov.ph" and other government websites. He was sentenced to one to two years of imprisonment and fined Php100,000. However, he immediately applied for probation, which was eventually granted by the court. The conviction is now considered a landmark case, as he is the first local hacker to be convicted under section 33a of the E-Commerce Law or Republic Act 8792.*

January 2010 - Technical Education Skills and Development Authority (Tesda) was defaced by Busabos, a Filipino hacker who then gained notoriety for defacing a lot of government websites in the Philippines like the National Disaster Coordinating Council(NDCC), Department of Labor and Employment(DOLE), Department of Health(DOH) etc. during the years 2009-2010.

He has a lot of notifications and archived defacements in Zone H. He then became one of the admins of the Facebook Fan Page "Anonymous #OccupyPhilippines".

April 2012 - Chinese hackers defaced the University of the Philippines website which is related to the dispute over Scarborough Shoal (Philippine Term: Panatag Shoal) or Huangyan Island (Chinese Term).

News spread regarding the defacement and intrusion of the hackers, who claim to be from China, and because of that a hacker who goes by the handle busabos retaliated and defaced three Chinese domains: star.chinaumu.org, v.cyol.com, and ploft.cn. He also posted the websites in a Facebook fan page called Anonymous #OccupyPhilippines, which has over 1000 likes and counting. This happened on April 21, 2012. This triggered the Philippine-China Cyber War.

Other Filipino hackers also retaliated and conducted other defacements and denial of service attacks.

Last April 23, 2012, the Presidential Spokesperson Edwin Lacierda issued an official statement saying:
"At around four o'clock in the afternoon of April 23, 2012, the Presidential Communications Development and Strategic Planning Office (PCDSPO) noticed a significant spike in traffic with malicious URL requests from forged user agents being channeled to the Official Gazette website (URL: www.gov.ph), to the PCDSPO website (URL: www.pcdspo.gov.ph), and to the Presidential Museum and Library website (URL: www.malacanang.gov.ph), causing our servers to momentarily lag. We determined that this was a denial-of-service attack. Information gathered through our data analysis indicated that the attack originated from IP addresses assigned to Chinese networks. The PCDSPO is endeavoring to maintain its websites. However, please note that we can expect temporary disruption of service while the attack is ongoing."

February 2016 - The Bangladesh Heist

The Philippines' National Bureau of Investigation (NBI) launched a probe and looked into a Chinese-Filipino who allegedly played a key role in the money laundering of the illicit funds as hackers transferred over 100 million Bangladesh Bank account dollars - executing the action from New York's Federal Reserve Bank. The funds were transferred to bank accounts across the Philippines and Sri Lanka.

2015 - The Philippine hacker group Deathnote Hackers (DNH) was formed in 2015, but officially founded in 2016 by TATAY45. They initially started as a hacking tutorial page but evolved into a hacking group. The group claimed to have conducted DDoS attacks on the Dragon Nest Sea Server and has also hacked some private and public entities in the Philippines.

March 2016 - The 2016 "Comeleak"

Two Filipino hackers defaced the Commission on Elections' website which is two months before the May 2016 elections. Lulzsec Pilipinas also claimed on Facebook that it had gotten the entire Comelec database which contains PII from 55 million registered voters.

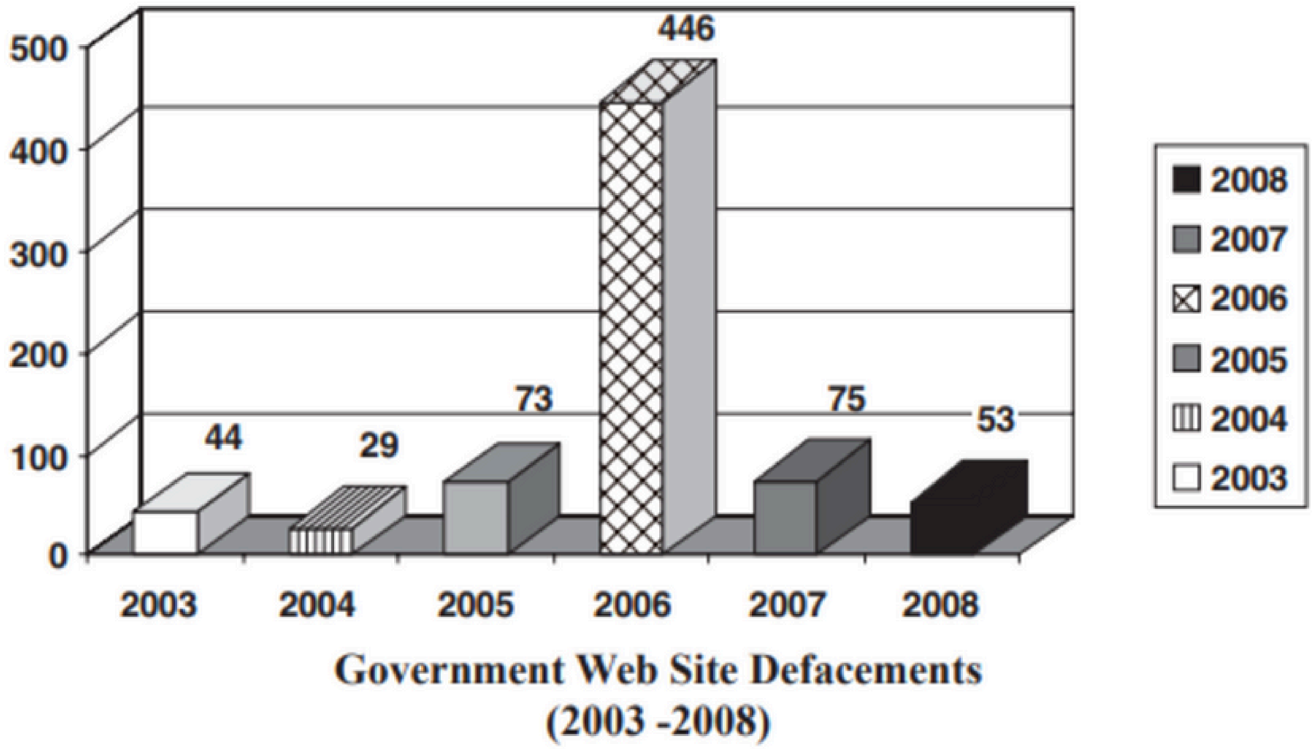
April 2017 - DeathNote Hackers ransomware discovered by Michael Gillespie. This is probably the first ransomware in the wild that originated from the Philippines.

The Aftermath

A lot of breaches have happened then and the Philippines saw a significant spike of cyber attacks in website defacements, phishing, malware attacks and data breaches throughout the year 2018.

Unisys Corp public survey reported that a staggering 90 percent of Filipinos were majorly concerned for their personal information's safety.

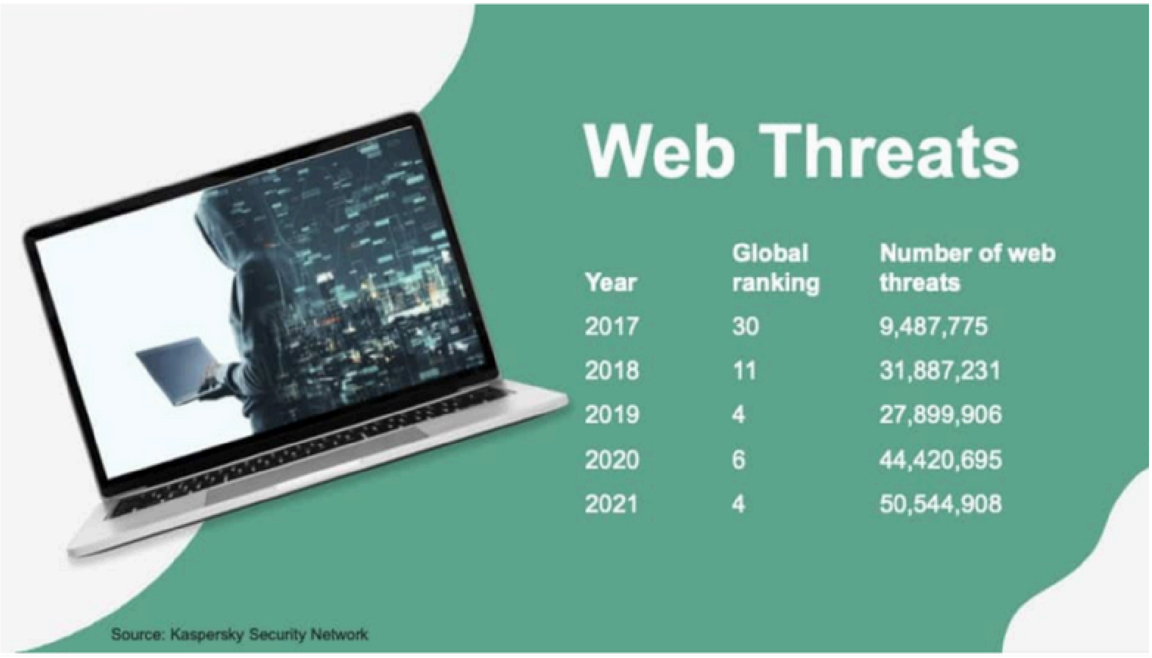
Data Background:
The Government Computer Security and Incident Response Team or the GCSIRT conducted research on Philippine CyberCrime from 2003 to 20017 and they discovered that *a total of 667 government websites were discovered defaced, or an aggregate of 133 government websites was attacked by defacers/hackers each year, an average of 11 incidents per month. Based on this research, it was found that 134 coded defacers (both local and international) attacked these government websites in those five years.*



Government Website Defacements (2003 - 2008) statistics by GCSIRT

Based on the statistics, we can understand that website defacements have been rising in the early 2000s and that hacker groups both international and local have started playing with the cyber infrastructures from the Philippines. In addition to the statistics they have presented, they also noted that of the attacked/hacked government websites, 507 of the 667 government websites were using the Linux web servers. As someone working in the penetration testing field, we can therefore deduce that most of these Linux web servers have weaknesses in their configuration systems during their time or have not patched their configurations as the year 2003 -2007, there were 0-days already.

It is also plausible that they are using CMS that are vulnerable to common web attacks like SQL Injection and Remote Code Execution. If you visit Packet Storm Security, milw0rm, and Exploit Database for that year, it is easy to see 0-day vulnerabilities that were then recorded, submitted, and archived for those years.
In 2021 and 2022, Kaspersky Security Network (KSN) released data for the top countries with the most cyber attacks. Below are summaries of their threat intelligence.



Web Threats

Year	Global ranking	Number of web threats
2017	30	9,487,775
2018	11	31,887,231
2019	4	27,899,906
2020	6	44,420,695
2021	4	50,544,908

Source: Kaspersky Security Network

The Philippines ranked 4th with the most number of web threats ranging from web attacks, remote desktop protocol (RDP) attacks, and mobile malware in 2021 according to Kaspersky.

The data show that web threat attempts against Filipino users of Kaspersky software grew 432.75% from 9,487,775 in 2017 to 50,544,908 in 2021. With the pandemic-borne shift towards remote working, the overall RDP attacks versus local businesses rose by 141% from 2019 (2,549,698) to 2021 (6,150,891). RDP enables computers running Windows on the same corporate network to be linked together and accessed remotely, even when employees are at home. In 2022, The Philippines was the second most-attacked country by web threats worldwide last year, according to a global cyber security firm's online security monitoring. Data from the Kaspersky Security Network (KSN) revealed that the country moved two places up, ranking second among countries most attacked by web threats within the period from January to December last year. The 2022 global ranking is topped by Mongolia with 51.1 percent of the attacks recorded, followed by the Philippines (49.8 percent), Ukraine (49.6 percent), Greece (49.5 percent), and Belarus (49.1 percent).

In 2022, The Philippines was the second most-attacked country by web threats worldwide last year, according to a global cyber security firm's online security monitoring. Data from the Kaspersky Security Network (KSN) revealed that the country moved two places up, ranking second among countries most attacked by web threats within the period from January to December last year. The 2022 global ranking is topped by Mongolia with 51.1 percent of the attacks recorded, followed by the Philippines (49.8 percent), Ukraine (49.6 percent), Greece (49.5 percent,) and Belarus (49.1 percent).
From their research, we can understand that the pandemic has played a large role in making Filipino users use the Internet more due to remote working.

The study of Kaspersky was also further proven or supplemented in 2023 by Palo Alto Networks wherein they noted that the primary threat vectors plaguing Filipino organizations are malware (66%), phishing and spear-phishing attacks (63%), and password-related breaches (56%). Although this is not a coop or related study, it helps the research to understand the cyber threats in the Philippines.

There are other studies and research conducted by other cyber security companies that also point to the same data about how the Philippines suffered the most cyber incidents in the APAC region. However, the data of Kaspersky and the supplemental conclusion of Palo Alto Networks should suffice to understand the cyber threat landscape in the Philippines.

CONCLUSION

The Philippines might be late in achieving global connectivity on the Internet compared to other countries. However, with its population and number of users to date - it is one of the countries suffering from cyber-attacks and data breaches. It is no stranger to the onslaught of computer viruses, website defacements, and data breaches. The I Love You Virus put the Philippines on the Internet map. The Bangladesh heist proved there are lack of security measures and validation from local banks. ComeLeak pointed out how the national government reacted to the largest data breach of its time. There are also new local underground groups that evolved from just website defacements to ransomware groups and hacktivism.

With the evolving threats growing per year and with the Philippines being the second most-attacked country by web threats worldwide, it is in the hands of both private and public sectors to come up with a solution to combat these attacks. This is an ongoing problem that the national government should try to address. There should always be ongoing risk assessments about the cyber security preparedness of both the public and private sectors. An action plan should be taken now, this is not something to be taken for granted.

REFERENCES

1. “Top Ten Most-Destructive Computer Viruses" - Smithsonian Magazine (smithsonianmag.com)

2. TIMELINE: One year of COVID-19 in the Philippines - Philippine Daily Inquirer

3. Remembering the First Internet Connection in the Philippines - iecepnegor.org

4. The Philippines E-Commerce Law – Republic Act No. 8792 by Janette Toral - digitalfilipino.com

5. Country Report on Cybercrime: The Philippines by Gilbert C. Sosa*
6. Tales from our Pinoy Hackers after the Y2K Bug - Nullforge

7. Understanding the Origins of the China - Philippine Cyber War - Infosec Institute

8 Biggest Data Privacy Breaches in the Philippines - journal.com.ph
9. The great Bangladesh cyber heist shows the truth is stranger than fiction - dhakatribune.com

10. Deathnote Hackers (DNH) group history - deathnote-hackers.blogspot.com

11. Kaspersky Security Network (KSN)

12. Palo Alto Networks: Philippines leads ASEAN in disruptive cyberattacks - Manila Bulletin