ILOVEYOU

ILOVEYOU, sometimes referred to as **Love Bug** or **Love Letter for you**, is a computer worm that infected over ten million Windows personal computers on and after 5 May 2000 when it started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". The latter file extension ('vbs', a type of interpreted file) was most often hidden by default on Windows computers of the time (as it is an extension for a file type that is known by Windows), leading unwitting users to think it was a normal text file. Opening the attachment activates the Visual Basic script. The worm inflicts damage on the local machine, overwriting random types of files (including Office files, image files, and audio files; however after overwriting MP3 files the virus hides the file), and sends a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. This made it spread much faster than any other previous email worm.

The malware was created by Onel de Guzman, a then-24-year-old resident of Manila, Philippines. Because there were no laws in the Philippines against creating malware at the time, the Philippine Congress enacted Republic Act No. 8792, otherwise known as the E-Commerce Law, in July 2000, in order to discourage future iterations of such activity.[1]

ILOVEYOU

Common name	ILOVEYOU
Aliases	Love Bug, Love Letter
Type	Computer worm
Point of origin	Manila, Philippines
Author(s)	Onel de Guzman
Operating system(s) affected	Windows 9x, Windows NT 4.0, Windows 2000
Written in	VBScript

Contents

- Creation
- Description
- Spread
- Impact
- Architecture
- Investigation
- Aftermath
- See also
- References
- External links

Creation

ILOVEYOU was created by Onel de Guzman, a college student in Manila, Philippines, who was 24 years old at the time. De Guzman, who was poor and struggling to pay for Internet access at the time, created the computer worm intending to steal other users' passwords, which he could use to log in to their Internet accounts without needing to pay for the service. He justified his actions on his belief that Internet access is a human right, and that he was not actually stealing.[2]

The worm used the same principles that de Guzman had described in his undergraduate thesis at AMA Computer College. He stated that the worm was very easy to create, thanks to a bug in Windows 95 that would run code in email attachments when the user clicked on them. Originally designing the worm to only work in Manila, he

removed this geographic restriction out of curiosity, which allowed the worm to spread worldwide. De Guzman did not expect this worldwide spread.[2]

Description

On the machine system level, ILOVEYOU relied on the scripting engine system setting (which runs scripting language files such as .vbs files) being enabled, and took advantage of a feature in Windows that hid file extensions by default, which malware authors would use as an exploit. Windows would parse file names from right to left, stopping at the first period character, showing only those elements to the left of this. The attachment, which had two periods, could thus display the inner fake "txt" file extension. True text files are considered to be innocuous as they are incapable of running executable code. The worm used social engineering to entice users to open the attachment (out of actual desire to connect or simple curiosity) to ensure continued propagation.[3] Systemic weaknesses in the design of Microsoft Outlook and Microsoft Windows were exploited that allowed malicious code capable of complete access to the operating system, secondary storage, and system and user data simply by unwitting users clicking on an icon.

Spread

Messages generated in the Philippines began to spread westwards through corporate email systems. Because the worm used mailing lists as its source of targets, the messages often appeared to come from acquaintances and were therefore often regarded as "safe" by their victims, providing further incentive to open them. Only a few users at each site had to access the attachment to generate millions more messages that crippled mail systems and overwrote millions of files on computers in each successive network.

Impact

The worm originated in the Pandacan neighborhood of Manila in the Philippines on May 4, 2000,[4] thereafter following daybreak westward across the world as employees began their workday that Friday morning, moving first to Hong Kong, then to Europe, and finally the United States.[5][6]The outbreak was later estimated to have caused US$5.5–8.7 billion in damages worldwide,[7][8] and estimated to cost US$15 billion to remove the worm.[9] Within ten days, over fifty million infections had been reported,[10] and it is estimated that 10% of Internet-connected computers in the world had been affected.[8] Damage cited was mostly the time and effort spent getting rid of the infection and recovering files from backups. To protect themselves, The Pentagon, CIA, the British Parliament and most large corporations decided to completely shut down their mail systems.[11] At the time, it was one of the world's most destructive computer related disasters ever.

The events inspired the song "E-mail" on the Pet Shop Boys' UK top-ten album of 2002, *Release*, the lyrics of which play thematically on the human desires which enabled the mass destruction of this computer infection.

Architecture

The ILOVEYOU Script (the attachment) was written in Microsoft Visual Basic Scripting (VBS) which runs in Microsoft Outlook and was enabled by default. The script adds Windows Registry data for automatic startup on system boot.

The worm searches connected drives and replaces files with extensions JPG, JPEG, VBS, VBE, JS, JSE, CSS, WSH, SCT, DOC, HTA, MP2, and MP3 with copies of itself, while appending the additional file extension VBS, making the user's computer unbootable. However, MP3s and other sound-related files would be hidden rather than overwritten.

The worm propagates itself by sending out one copy of the payload to each entry in the Microsoft Outlook address book (Windows Address Book). It also downloads the Barok trojan renamed for the occasion as "WIN-BUGSFIX.EXE".

The fact that the worm was written in VBS provided users a way to modify it. A user could easily modify the worm to replace important files in the system, and destroy it. This allowed more than twenty five variations of ILOVEYOU to spread across the Internet, each one doing different kinds of damage.[12] Most of the variations had to do with what file extensions were affected by the worm. Others simply modified the email subject in order to make it targeted towards a specific audience, like the variant "Cartolina" in Italian, or the variant "BabyPic" for adults. Some others only modified the credits to the author, which were originally included in the standard version of the virus, removing them completely or referencing false authors.[12]

Some mail messages sent by ILOVEYOU:

- VIRUS ALERT!![13]
- Important! Read Carefully!![13]

Investigation

On 5 May 2000, two young Filipino programmers named Reonel Ramones and Onel de Guzman became targets of a criminal investigation by agents of the Philippines' National Bureau of Investigation (NBI).[14] Local Internet service provider Sky Internet had reported receiving numerous contacts from European computer users alleging that malware (in the form of the "ILOVEYOU" worm) had been sent via the ISP's servers.

De Guzman attempted to hide the evidence by removing his computer from his apartment, but he accidentally left some disks behind that contained the worm, as well as information that implicated Michael Buen as a possible co-conspirator.[2]

After surveillance and investigation by Darwin Bawasanta of Sky Internet, the NBI traced a frequently appearing telephone number to Ramones' apartment in Manila. His residence was searched and Ramones was arrested and placed under investigation by the Department of Justice (DOJ). Onel de Guzman was also charged *in absentia*.

At that point, the NBI were unsure what felony or crime would apply.[14] It was suggested they be charged with violating Republic Act 8484 (the Access Device Regulation Act), a law designed mainly to penalise credit card fraud, since both used pre-paid (if not stolen) Internet cards to purchase access to ISPs. Another idea was that they be charged with malicious mischief, a felony (under the Philippines Revised Penal Code of 1932) involving damage to property. The drawback here was that one of its elements, aside from damage to property, was intent to damage, and de Guzman had claimed during custodial investigations that he might have unwittingly released the worm.[15] At a press conference organised by his lawyer on 11 May, he said "It is possible" when asked whether he might have done so.

To show intent, the NBI investigated AMA Computer College, where de Guzman had dropped out at the very end of his final year.[14] They found that, for his undergraduate thesis, de Guzman had proposed the implementation of a trojan to steal Internet login passwords.[16] This way, he proposed, users would finally be able to afford an Internet connection. The proposal was rejected by the College of Computer Studies board,[15] prompting de Guzman to cancel his studies the day before graduation.

Aftermath

Since there were no laws in the Philippines against writing malware at the time, both Ramones and de Guzman were released with all charges dropped by state prosecutors.[17] To address this legislative deficiency,[14] the Philippine Congress enacted Republic Act No. 8792,[18] otherwise known as the E-Commerce Law, in July 2000, months after the worm outbreak.

In 2012, the Smithsonian Institution named ILOVEYOU the tenth-most virulent computer virus in history.[3]

De Guzman did not want public attention. His last known public appearance was at the 2000 press conference, where he obscured his face and allowed his lawyer to answer most questions; his whereabouts remained unknown for 20 years afterward. In May 2020, it was revealed that while researching his cybercrime book Crime Dot Com, investigative journalist Geoff White had found Onel de Guzman working at a mobile phone repair stall in Manila. De Guzman admitted creating and releasing the virus. He claimed he had initially developed it to steal Internet access passwords, since he could not afford to pay for access. He also stated that he created it alone, clearing the two others who had been accused of co-writing the worm.[19][20]

See also

- Christmas Tree EXEC
- Code Red worm
- Computer virus
- Nimda (computer worm)
- Timeline of notable computer viruses and worms

References

1. Caña, Paul John (5 May 2020). "Filipino Creator of the 'I Love You' Virus Just Did It So He Could Get Free Internet" (https://web.archive.org/web/20200607094321/https://www.esquiremag.ph/culture/tech/filipino-creator-of-the-i-love-you-virus-free-internet-a00289-20200504). *Esquire Philippines*. Archived from the original (https://www.esquiremag.ph/culture/tech/filipino-creator-of-the-i-love-you-virus-free-internet-a00289-20200504) on 7 June 2020. Retrieved 19 January 2021.
2. "The 20-Year Hunt for the Man Behind the Love Bug Virus" (https://www.wired.com/story/the-20-year-hunt-for-the-man-behind-the-love-bug-virus/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Retrieved 2020-09-15.
3. "Top Ten Most-Destructive Computer Viruses" (http://www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html?c=y&page=2). *The Smithsonian*. 2012-03-20. Retrieved 2013-10-25.
4. "No excuse for virus toll, warns MessageLabs" (https://web.archive.org/web/20001214221100/http://www.messagelabs.com/news/PressReleases/nws-TakingToll.htm). MessageLabs. 10 May 2000. Archived from the original (http://www.messagelabs.com/news/PressReleases/nws-TakingToll.htm) on 2000-12-14.
5. Kane, Margaret (4 May 2000). "'ILOVEYOU' e-mail worm invades PCs" (https://web.archive.org/web/20081227123742/http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn). *ZDNet News*. Archived from the original (https://www.zdnet.com/news/iloveyou-e-mail-worm-invades-pcs/107318) on 2008-12-27.
6. "'Love bug' hacker is Pandacan man, 23" (https://www.philstar.com/networks/83717/love-bug-hacker-pandacan-man-23). *The Philippine Star*.
7. Garza, George. "Top 10 worst computer viruses" (http://www.catalogs.com/info/travel-vacations/top-10-worst-computer-viruses.html). *Catalogs.com*. Retrieved 2008-05-26.
8. http://bi.gazeta.pl/im/7/5140/m5140197.pdf
9. Buckland, Jason. "The 'love' bug — 10 worst cybercrimes of the decade" (https://web.archive.org/web/20111027131918/http://tech.ca.msn.com/photogallery.aspx?cp-documentid=27611570&page=1). *tech.ca.msn.com*. Archived from the original (http://tech.ca.msn.com/photogallery.aspx?cp-documentid=27611570&page=1) on 2011-10-27.
10. Barker, Gary (14 May 2000). "Microsoft May Have Been Target of Lovebug". *The Age*.
11. Kane, Margaret (May 4, 2000). "British parliament shut down their mail systems to prevent damage" (https://web.archive.org/web/20070923005429/http://news.zdnet.com/2100-9595_22-520435.html). *ZDNet News*. Archived from the original (http://news.zdnet.com/2100-9595_22-520435.html) on September 23, 2007.
12. "I LOVE YOU Virus Help" (https://www.computerhope.com/vinfo/iloveyou.htm). *Computer Hope*. Retrieved 11 February 2013.

13. "Symantec detects all known new variants of VBS.LoveLetter.A worm" (https://web.archive.org/web/20140316002324/http://www.symantec.com/region/reg_ap/press/my_000506.html). Symantec. May 6, 2000. Archived from the original (http://www.symantec.com/region/reg_ap/press/my_000506.html) on March 16, 2014. Retrieved 8 February 2013.
14. Gana, Severino H. Jr. "Prosecution Of Cyber Crimes Through Appropriate Cyber Legislation In The Republic Of The Philippines" (https://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana%2CPhillipine.html). Asian Criminal Administration Foundation. Archived from the original (http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html) on 2008-02-06.
15. Landler, Mark (2000-10-21). "A Filipino Linked to 'Love Bug' Talks About His License to Hack" (https://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html). *The New York Times*. Retrieved 2010-05-05.
16. "Onel de Guzman's rejected thesis proposal at AMA Computer College" (https://web.archive.org/web/20100426162413/http://www.computerbytesman.com/lovebug/thesis.htm). *ComputerBytesMan.com*. Archived from the original (http://www.computerbytesman.com/lovebug/thesis.htm) on 2010-04-26. Retrieved 2010-12-05.
17. Arnold, Wayne (2000-08-22). "Technology; Philippines to Drop Charges on E-Mail Virus" (https://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html). *The New York Times*. Retrieved 2010-05-05.
18. "Republic Act No. 8792 — An Act Providing For The Recognition And Use Of Electronic Commercial And Non-Commercial Transactions And Documents, Penalties For Unlawful Use Thereof And For Other Purposes" (http://www.chanrobles.com/republicactno8792.htm). 2001-08-01. Retrieved 2010-12-05 – via ChanRobles.com.
19. White, Geoff (2 May 2020). "Love Bug's creator tracked down to repair shop in Manila" (https://www.bbc.com/news/technology-52458765). BBC News.
20. White, Geoff (21 April 2020). "Revealed: The man behind the first major computer virus pandemic" (https://www.computerweekly.com/news/252481937/Revealed-The-man-behind-the-first-major-computer-virus-pandemic). *Computer Weekly*.

External links

- The Love Bug - A Retrospect (http://rixstep.com/1/20040504,00.shtml)
- ILOVEYOU Virus Lessons Learned Report, Army Forces Command (http://handle.dtic.mil/100.2/ADA415104)
- Radsoft: The ILOVEYOU Roundup (http://radsoft.net/news/roundups/luv/)
- "No 'sorry' from Love Bug author (https://www.theregister.co.uk/2005/05/11/love_bug_author/)" at The Register
- CERT Advisory CA-2000-04 Love Letter Worm (http://www.cert.org/advisories/CA-2000-04.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=ILOVEYOU&oldid=1005590752"

This page was last edited on 8 February 2021, at 13:22 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.