ILOVEYOU

Adrian Kosmaczewski

2022-08-19

Early in the morning of Friday, May 5th, 2000, we were starting yet another day of work at our office in the neighborhood of Olivos[1], north of Buenos Aires, Argentina.

Priorities are different for everyone. In my case, it was catching up with the tech news of the day. For others, it was opening their e-mail.

As I perused some news websites (I wasn't using RSS feeds yet) I read the news of a virulent trojan with catastrophic consequences, making the headlines in Asia and Europe, and as we were waking up, in the Americas too. I learned that it targeted Windows machines (what else?) and that it was written in VBScript[2]. That was the language we were using every day at work.

How did this worm work? The thing would automatically execute when you opened an attachment named `LOVE-LETTER-FOR-YOU.TXT.vbs` (see the double extension?) and it would immediately overwrite some files of your home directory with copies of itself (those with extensions like JPG, CSS, or MP3), finally sending itself as an attachment to all of your contacts in your address book. Outlook Express[3] and Active Scripting[4] FTW.

It was the (in)famous ILOVEYOU worm[5], also known as CA-2000-04 Love Letter Worm[6].

Precisely as I was reading that article (I swear the timing couldn't have been better) I hear one of my colleagues complain that her computer was not working properly and that all she saw was (and I quote, as I remember it vividly) "it says I love you everywhere!"

Seconds later the coin dropped in my head, jumped to her computer and unplugged its network cable. We then sent an e-mail to all our colleagues worldwide advising them not to open an e-mail with such a title and such an attachment. Thankfully nobody else (that we know of) had an issue with the worm, even though almost all of us received it in our inboxes.

I kept a copy of the file (which would trigger antivirus alerts for years to come) in some forgotten backup disk. It was so mind-bogglingly simple; start, overwrite

[1] https://en.wikipedia.org/wiki/Olivos%2C_Buenos_Aires
[2] https://en.wikipedia.org/wiki/VBScript
[3] https://en.wikipedia.org/wiki/Outlook_Express
[4] https://en.wikipedia.org/wiki/Active_Scripting
[5] https://en.wikipedia.org/wiki/ILOVEYOU
[6] https://resources.sei.cmu.edu/asset_files/WhitePaper/2000_019_001_496188.pdf

the files, open the address book, and send itself to all contacts. That's it. The whole power of ActiveX[7] and COM[8] components, the same programming language we were using in our Windows 2000[9] server-side ASP[10] applications, was used in a completely different, horrendous way.

2000 was the year I started learning about computer security[11]. I started playing with Back Orifice[12] in my free time. At that moment I discovered how fragile software was.

[7] https://en.wikipedia.org/wiki/ActiveX

[8] https://en.wikipedia.org/wiki/Component_Object_Model

[9] https://en.wikipedia.org/wiki/Windows_2000

[10] https://en.wikipedia.org/wiki/Active_Server_Pages

[11] https://deprogrammaticaipsum.com/the-weakest-link/

[12] https://en.wikipedia.org/wiki/Back_Orifice