Peter W. Dudziak
10/17/2022

The Impact of Virtual Viruses

With the sudden appearance of widespread communication across a vast network of wirelessly controlled robots, there's a near infinite number of problems that could invariably happen. Things break all the time, though in the case of viruses and malware, one may call these sorts of breakings 'sabotage' rather than a minor accident that occurs because of poor planning. The history of viruses is interesting enough, but it's the virility of these viruses that is particularly interesting. Some can multiply without human interaction at all while others prey on the time period they were based upon to expose themselves out to the world. Others had pre-set commands built into them in order to tell computers and servers to enable the viruses directly. And a select few of them were admittedly somewhat harmless.

On the turn of the millennia, the year 2000, malware and viruses were literally considered to be mythical. The idea that someone was capable of sending these viruses out into the internet was unheard of. And yet, one of the fastest-growing virus in history managed to make its breakout debut across emails.[1] The virus, named 'ILOVEYOU' as per its method of transmission, was sent via a download link given in an email. Normally, these sorts of viruses would find it impossible to gain traction as people don't click on random links or download unknown files, but in the early 2000's, that sort of self-preservation wasn't quite so widespread.

When downloaded, instead of giving people a love letter, the virus installed a worm onto the computer and overwrote both personal files and internal system files, spreading itself over and over again before using the computer's own email account to send itself off to people's contacts and chat rooms. The two individuals who made the virus- Reonel Ramones and Onel de Guzman- were found guilty of making and sending the virus out in the first place, however because there were no laws put in place against the creation and distribution of this sort of malware, they were let off with no punishments, though this case laid the groundwork for protections against these sorts of malware attacks in the future.

[1] Kleinbard, David. "'I Love You' Virus Sweeps the U.S." *CNNMoney*, Cable News Network, 5 May 2000, https://money.cnn.com/2000/05/05/technology/loveyou/.

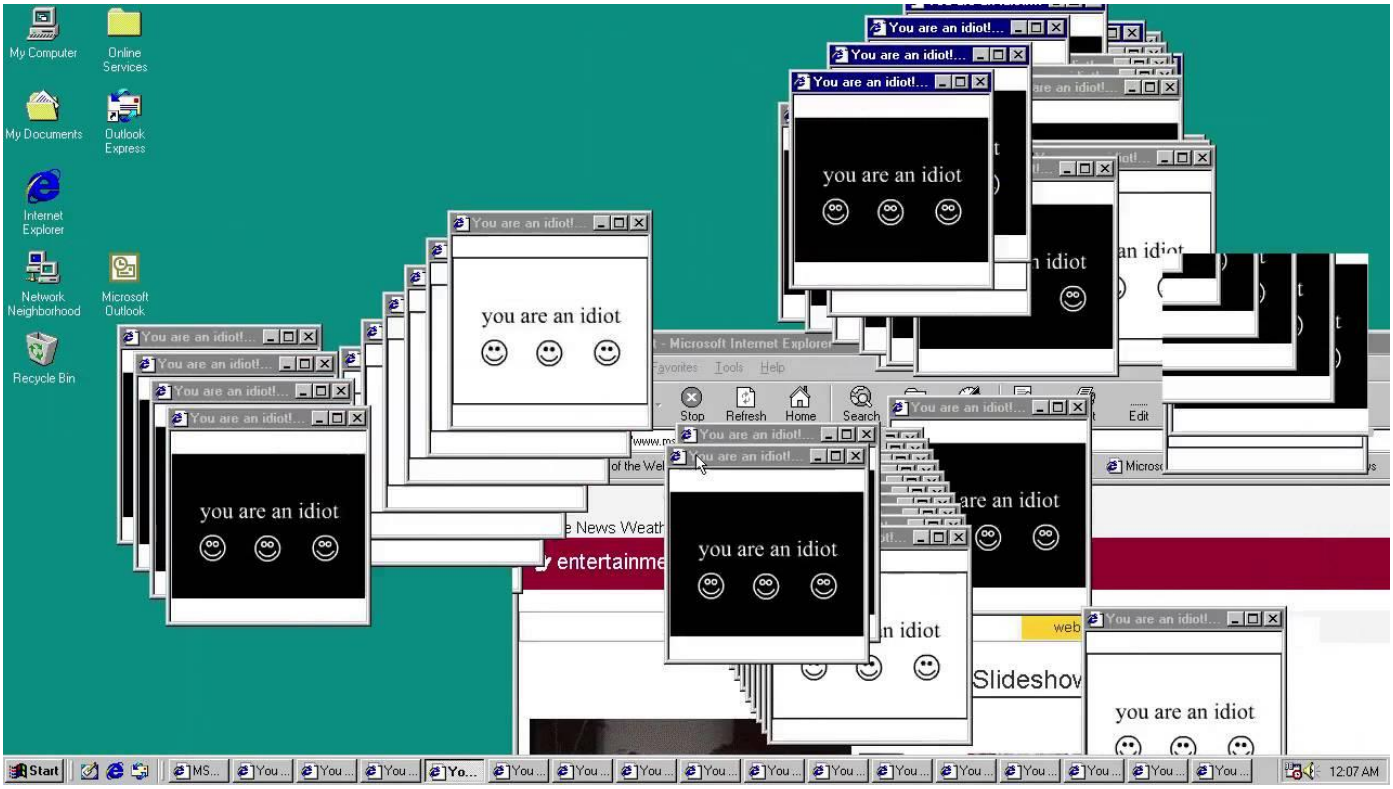
A significantly more potent and destructive virus was created only four short years later, with 2004 bringing about the rise of the infamous MyDoom. Its name is only indicative of how powerfully destructive it was. Similarly to ILOVEYOU, MyDoom sent itself through emails and contacts, but unlike the manual download that ILOVEYOU required, MyDoom automatically downloaded itself by sending a command to the server it was being hosted on, getting the server to download MyDoom. MyDoom appeared to be a fairly simple email, containing the message 'andy; I'm just doing my job, nothing personal, sorry'. The worm would then go on to access the local files in order to search for contacts and send itself to them. Curiously enough, the virus was hard coded with instructions to ignore specific contacts, including Microsoft, MIT, and Stanford. It was theorized that MyDoom ignored all .edu addresses, but this was eventually proven to be false.

While MyDoom was the fastest spreading virus in history, the real danger comes with its second wave of data. MyDoom was made up of two worms, each named A and B. MyDoom.A was the one that transmitted the both of them and created such a massive spread, while MyDoom.B overloaded the computer with what would be known as a DDoS attack, or a distributed denial of service attack. Instead of taking out specific parts of a computer in order to break it like deleting personal or internal files, MyDoom.B instead overflowed the computer with information and data that it had to process, massively slowing down response time with exponentially larger packages.

These DDoS attacks were so bad that after a single day of the virus being released to the world, the FBI and the Secret Service both offered bounties for information regarding the individual who created the two strains of the virus. To this day, nobody knows who created the virus, but it continued until midway through February, when the virus was hard coded to stop. Even with the virus having stopped, there was still a backdoor opened through both MyDoom.A and MyDoom.B, allowing for a secondary attack to come months later in July. Both of the attacks were crippling and led to the further development of strains of MyDoom, up to and including MyDoom.AO, which was used in July 2009's cyber attacks against both South Korea and the United States.

While both MyDoom and ILOVEYOU are both incredibly virulent and hazardous, there's other viruses that seem to lean a bit more into the humorous side. One virus in particular named 'You are an idiot' follows this very trend, acting not as a particularly violent trojan that destroys files, but something that pops up and plays loud noises, more akin to a prank than a proper virus. Even still, this trojan was incredibly popular back in 2002, being hidden inside all manner of links and download files.

The way You Are An Idiot worked was simply by way of being manually downloaded, similarly to ILOVEYOU. Unlike ILOVEYOU, however, the trojan wasn't capable of automatically sending itself across the user's contact list. Instead, these viruses were passed along by hand to different individuals, and upon being executed, would immediately load itself and open up six different browsers. All of these browsers showed three smiley faces, as well as the words "You are an idiot" in big bold letters, flashing black and white as it called out the same sentence through a rather loud mp4 file. If the user attempted to close one of the browsers, the virus would open two more browsers. And in the event that the user would try to open up task manager to force close it, the virus would replace it with yet another browser of its kind. The only way to get the virus to stop is by restarting the computer.



2

[2] Octavio, Dano. "Trojan.js.youareanidiot." *YouTube*, YouTube, 19 Oct. 2015, https://www.youtube.com/watch?v=LSgk7ctw1HY.

The virus was so popular, in fact, that it spawned its own community to try and create different versions of the virus, one of which eventually spawned its own internal text-based game about deciding whether or not the user was an idiot. Regardless of the method, the result ended up being the same trojan that locked off most browser access. In 2013, the virus was revived as "You Are An Idiot 2", though this time instead of a prank, the virus was created as a way to show the different problems that come with certain security systems.

In a similar fashion, the Anna Kournikova virus was more of a practical joke than a problem. In the mid to late nineties, a concerning number of people searched up Anna on the internet, leading to an idea borne of one Jan De Wit. The virus was rather simple, and acted in the same vein as the ILOVEYOU and MyDoom viruses in that it was sent via an email. The virus gained traction and started to spread by taking different people from the contacts and sending the virus along the list. The only thing about it that may consider it to be a virus was the fact that it was capable of passing itself from account to account, but it didn't actually do anything bad.

Quite the contrary, in fact. The virus only carried pictures of Anna Kournikova, the tennis star. Something of a pleasant surprise, if anything. Jan De Wit turned himself into police custody not long after the virus was made public, though because it hadn't done any severe damage, the man was let out without any charges.[3] The mayor of his town even offered him a job as a techie as a result of his work on the virus showcasing his aptitude with computers.

The worst virus out of all of them, however, is a notorious virus known as CryptoLock. One of the most advanced viruses currently known, CryptoLock was created and distributed in 2013 as a means of making money. Hence the virus coining the term 'ransomware', as it literally held the user's software and personal files for ransom. Of note, while CryptoLock made use of the numerous holes and bugs in the Windows OS, it also used backdoors created by other viruses that came before it, including the aforementioned MyDoom, though it primarily used a Gameover ZeuS botnet, which housed a separate virus.

When CryptoLock was activated, it searched through the user's computer and encrypted specific files stored in local and mounted networks, with the encryption key stored in a private server

[3] Alcouth, Jess. "Confession by Author of Anna Kournikova Virus." *Pinsent Masons*, Pinsent Masons, 20 May 2019, https://www.pinsentmasons.com/out-law/news/confession-by-author-of-anna-kournikova-virus.

separate from the user. At this point, a popup would appear stating that the user had 72 hours to pay them before the encryption key is permanently deleted. Furthermore, CryptoLock, true to its name, asked for people to pay in bitcoin, though an option was open for card-based payments as well. If 72 hours passed with no response, there would be an additional offer made following the key's destruction, but the only way to pay for the access key would be with a substantially higher amount of bitcoin.

4

[4] Cannell, Joshua. "Cryptolocker Ransomware: What You Need to Know: Malwarebytes Labs." *Cryptolocker Ransomware: What You Need to Know*, Malwarebytes , 2 June 2014, https://www.malwarebytes.com/blog/news/2013/10/cryptolocker-ransomware-what-you-need-to-know.

While the virus itself was rather easy to remove, the damage it dealt in encrypting the files was not and could not be easily undone. On top of this, there was no written guarantee that CryptoLock would give back any encrpytion key if payment was made, essentially getting users to buy into an empty promise. Over the course of 100 days, CryptoLock managed to gain upwards of 30 million dollars leading into 2014. The problem came from how easy it was for the virus to hide itself from most users, as Windows' default behavior was to hide the file extensions on most files. By simply changing the icon and making the virus look somewhat professional, people would click on it in order to see what it was before downloading the virus and getting scammed out of their money.

In June of 2014, the United Stated Department of Justice, partnering with numerous colleges and tech firms, created Operation Tovar in order to take down CryptoLock.[5] In order to stop CryptoLock's spread, the operation targetted the Gameover ZeuS botnet that it primarily worked through, isolating it and cutting off the spread on June 2nd. Additionally, an IT firm known as Fox-IT managed to produce a private bank of encryption keys which could be used to decrypt all of the files that CryptoLock had locked down. Due to the length of the keys, it was impossible to properly brute force any of the decryptions. In fact, they were so long that it was computationally infeasible to break without a concerted effort or the abuse of some flaw in the key itself.

With the entirety of the internet acting as one large 'body' of sorts, it's no surprise that the body of the internet would be prone to different problems. Parts of the body not working quite correctly, or even entire segments of the internet failing as a result of some mismanaged problem or a bug in the system. But while the human body contracts viruses from biology outside of our control, computer viruses are hand-crafted and made for the specific purpose of infecting and spreading for some cause or another. Whether it be to make money, pull a practical joke, or cause the systematic crashing of nearly every major internet-based infrastructure on the planet, these viruses are hand made.

It's precisely because of that reason that viruses are so inherently interesting. Their complete basis in human origin makes them the perfect case study in how people act and react to such a

[5] June, Dour Scot, and Hayton June. "'Operation Tovar' Targets 'Gameover' Zeus Botnet, Cryptolocker Scourge." *'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge*, Krebson Security, 2 June 2014, https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.

massive interconnected web of communication. There is never anyone who is quite so complacent as to take the internet at face value. There will always be people who want to try and mess with something that someone else has created, for better or for worse. In some cases, especially in the case of 'You Are An Idiot', these viruses can be an example of how to make the internet better. A warning to everyone else to not download unknown links. Or in the case of MyDoom, an act of literal terrorism. Computer viruses are enthralling, not because of what they do or how they do it, but because of what it is they stand for in the context of a wider internet.

Bibliography

Kleinbard, David. "'I Love You' Virus Sweeps the U.S." *CNNMoney*, Cable News Network, 5 May 2000, https://money.cnn.com/2000/05/05/technology/loveyou/.

Octavio, Dano. "Trojan.js.youareanidiot." *YouTube*, YouTube, 19 Oct. 2015, https://www.youtube.com/watch?v=LSgk7ctw1HY.

Alcouth, Jess. "Confession by Author of Anna Kournikova Virus." *Pinsent Masons*, Pinsent Masons, 20 May 2019, https://www.pinsentmasons.com/out-law/news/confession-by-author-of-anna-kournikova-virus.

Cannell, Joshua. "Cryptolocker Ransomware: What You Need to Know: Malwarebytes Labs." *Cryptolocker Ransomware: What You Need to Know*, Malwarebytes , 2 June 2014, https://www.malwarebytes.com/blog/news/2013/10/cryptolocker-ransomware-what-you-need-to-know.

June, Dour Scot, and Hayton June. "'Operation Tovar' Targets 'Gameover' Zeus Botnet, Cryptolocker Scourge." *'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge*, Krebson Security, 2 June 2014, https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.