PERSPECTIVE: BIOLOGICAL/DIGITAL VIRUS

A biological perspective on the cryptic malicious code.

When I was 10 years old (believe it or not!) I remember wondering why my PC (Personal Computer) wasn't subject to any bacterial infection as I actually thought that computers were infected by actual viruses. Since cyber intrusions are on the forefront of many news outlets I am convinced it would be interesting to investigate if malware viruses are related in some way to biological viruses beyond any nomenclature. Understanding the biological relationship provides us with a stronger conceptualization on **what a Virus actually is,** therefore enabling us to find stronger solutions to virtual infections.

First, it should be pointed-out that the term malware (malicious software) regroups many forms of software [a] and is not necessarily a virus which is subcategory of that term [b]. At its essence a computer virus has 1) a replicative nature and 2) an ability to spread a code. On that premise I will try to distinguish similarities and differences between a biological virus and malware virus.

Organic Virus

To start organic viruses are categorized in two ways which help identify the virus, the Baltimore classification and the ICTV [c] system each contributing their own informative attributes. The ICTV system has a more traditional approach of identification and is based on the morphology of the virus and whom it infects (archaea, bacteria, eukaryotic). It is the common way to identify a virus (ex: Herpes) The Baltimore classification compartmentalize the virus based on its structure. Viruses would for example be viewed as simple-stranded (1 line of code), double stranded (2 lines of code facing each other), DNA or RNA [d] built. Biological viruses are unique by their ability to use the cellular environment to their advantage. By only a small amount of code they can use the cell’s cellular machines to their benefit.

Infectious mechanism for the virus to enter the cell:

--> insert its code (by using the cell’s mechanism) --> replicate --> spread

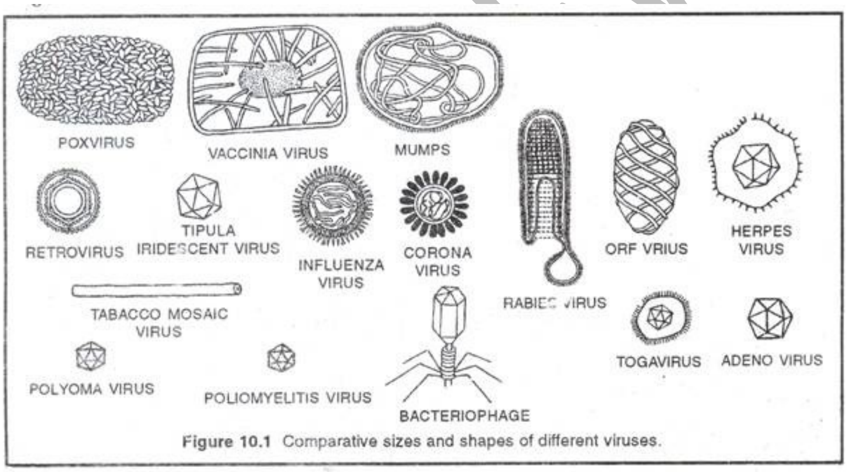

Figure 10.1 Comparative sizes and shapes of different viruses.

On this link (https://youtu.be/Rpj0emEGShQ) there is an example of an Flu virus (*Orthomyxoviridae virus).* A RNA Virus using the cells RNA polymerase [e] to replicate. Viruses come on all shapes and forms and their only purpose is to replicate a malicious code.

Malware Virus

First appearing with “Brain boot sector” in MS-DOS (1986) malware viruses are on the other hand **man-made** programs written in languages such as C++ meant to exploit operational systems (ex: Windows, iOS) or programs vulnerabilities. You could argue that they have specific purposes (ear-dropping, stealing information or destroying your files) a difference from biological viruses which whom has none apart from spreading.

So what are the Commonalities?

From what I have gathered, both are made of **short code**

- ~10 coding genes for an biological virus (vs. 21’000 genes for humans)
- 125 LOC (lines of code) for an malware (vs. 50 million lines of code [Microsoft Windows])

Both require a **robust defense system**

The human body has an intricate network of innate (ex: inflammation) and adaptive immune system involving many different cell types (B cells, T-cells, macrophages, …) both taxing in terms of resources and sophistication.

- For malwares a vast amount of code (~10 millions LOC [f]) is necessary for the creation of modern defense products.

Use of the **host’s infrastructure**

- Similar to an organic virus whom hijacks the cell’s own molecular machines, malware viruses can use codes libraries (ex: as an .dll file) pre-existing within a program of OS.

Various **vectors of entry**

- Both types of viruses have different methods of infecting the targeted host. Biologically a virus can be transmitted orally, sexually, by direct or indirect contact.
- Malware viruses can propagate via emails, web-browsers, USB’s or file-sharing.

Can be **dormant** within the system

- A case example would be the HIV virus which can be inactive for many years in humans before a random awakening.
- Malware virus may on the other hand remain hidden many years (zero-day virus) until detection!

Possibility of a **crossover**

- Stuxnet, one of the most sophisticated malware viruses ever created made headlines by its ability to cross platforms. From a Windows based operating system to a SCADA [g]
- The Avian flu virus which was in the center of headlines in 2005 created much hysteria by its potential to cross transmission from birds to humans.

And Differences ?

Detection and quarantine

- Virtual viruses are difficult to detect as due to their cheer quantity [h] and hidden mechanisms [i].
- In contrast most organic viruses aren't in general that challenging to detect but can be tough to quarantine (ex: Ebola).

Benefice and Harm

- Our own DNA is made in part of viral code and has lead to some evolutionary beneficial adaptations (ex: intestinal flora).
- Malware viruses don't have any real benefices apart maybe illustrating weakness in some coding areas.

Natural selection

Natural selection is a on-going process where random mutations are subjected to an code which in turn can lead to some physical changes. These changes if better suited to the environment will lead to an increase rate of replication.

- Most (if not all) virtual viruses have yet to reach the stage where they are subject to natural selection.
- Biological viruses main defense mechanism is natural selection and it is a reason why they are so difficult to eliminate.

Conclusion

The natural world is always a great source of inspiration as much of our understanding of the world derives from it. As malware viruses incorporate elements of its biological counterpart virtual code seems to evermore reach an ultimate stage of incorporating elements of natural selection. As this merger will likely gradually occur cyber-security experts will soon enough need to increase biological solutions in an interesting but scary arms-race.

Works Cited

[1] M. S. a. A. Honig, Practical Malware Analysis.

[2] Cell biology by the numbers, "How many genes are in a genome?,"

[3] "What Is the Difference: Viruses, Worms, Trojans, and Bots?,"

[4] D. s. Goodsell, The Machinery of Life.

[5] biologydiscussion.com, "Properties of Viruses (with Digram),"

[a] Key loggers, Trojans, worms, ransomware, adware, …

[b] Fluid term as each category is not clear cut.

[c] International Committee on Taxonomy of Viruses

[d] RNA is a temporary code sequence the cell makes to be used by molecular machines (ribosomes)

[e] Polymerase = cellular photocopy machine

[f] Based on a comparative study

[g] Control system used in industrial activities

[h] Est. of 1 Million malwares released daily

[i] Some hackers are very ingenious on hiding their malicious code