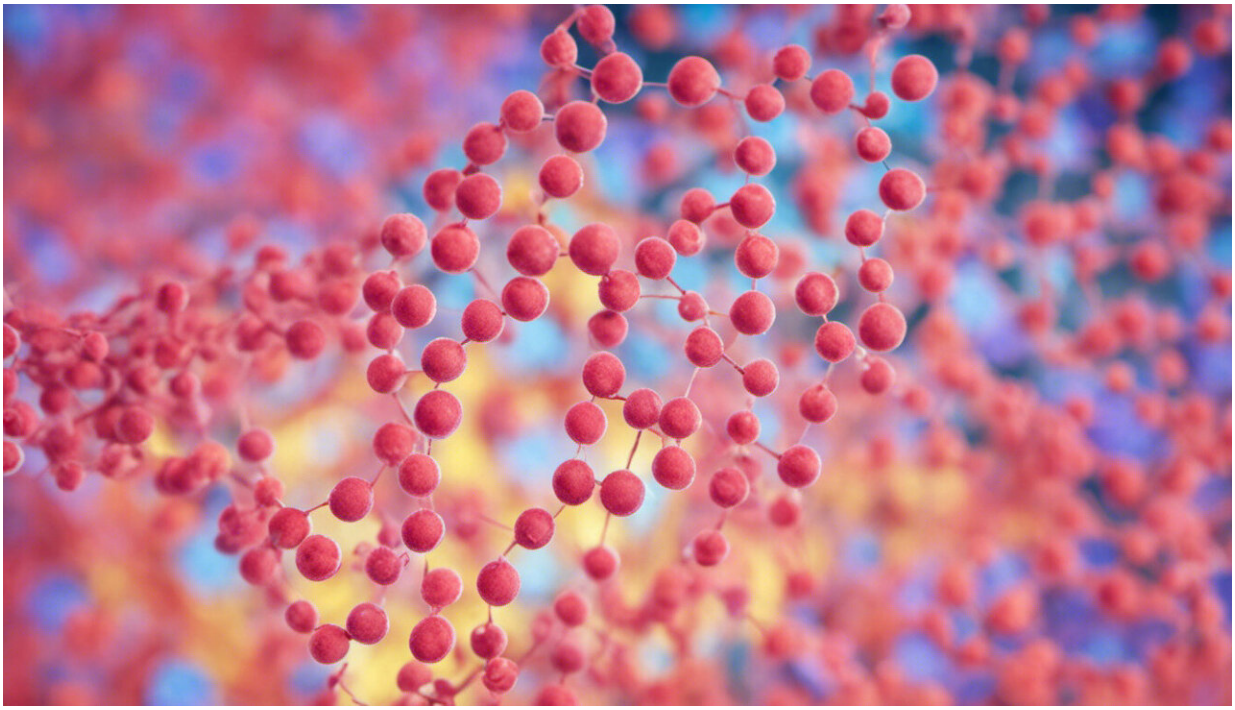
Viruses and malware—are we protecting ourselves adequately?

November 30 2017, by Hervé Debar



Credit: AI-generated image (disclaimer)

Cybersecurity incidents are increasingly gaining public attention. They are frequently mentioned in the media and discussed by specialists, such as Guillame Poupard, Director General of the French Information Security Agency. This attests to the fact that these digital incidents have an increasingly significant impact on our daily lives. Questions therefore

arise about how we are protecting our digital activities, and if this protection is adequate. The publicity surrounding security incidents may, at first glance, lead us to believe that we are not doing enough.

A look at the current situation

Let us first take a look at the progression of software vulnerabilities since 2001, as illustrated by the National Vulnerability Database (NVD), the reference site of the American National Institute of Standards and Technology (NIST).

Upon an analysis of the distribution of vulnerabilities to computer-related attacks, as published by the American National Institute of Standards and Technology (NIST) in visualizations on the National Vulnerability Database, we observe that since 2005, there has not been a significant increase in the number of vulnerabilities published each year. The distribution of risk levels (high, medium, low) has also remained relatively steady. Nevertheless, it is possible that the situation may be different in 2017, since, just halfway through the year, we have already reached publication levels similar to those of 2012.

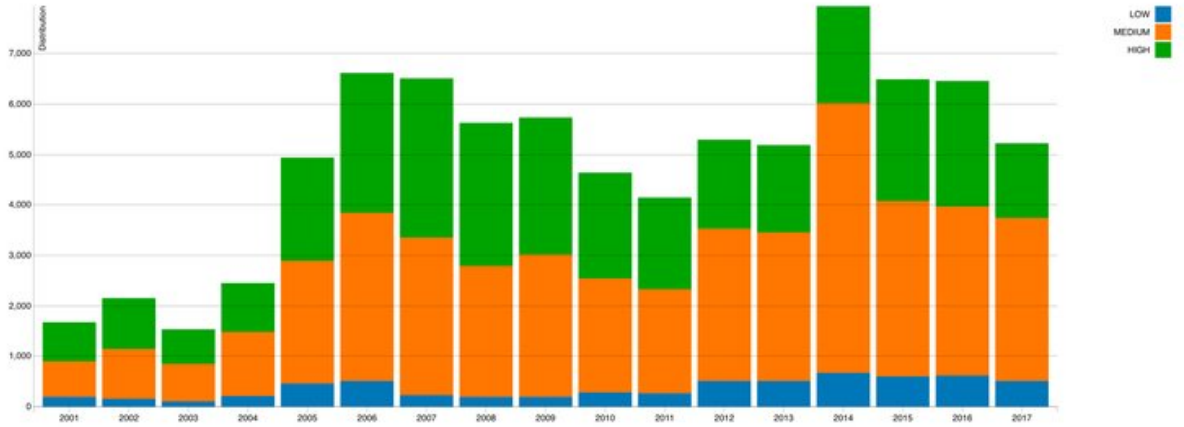
It should be noted, however, that the growing number of vulnerabilities published in comparison to before 2005 is also partially due to a greater exposure of systems and software to attempts to compromise and external audits. For example, Google has implemented Google Project Zero, which specifically searches for vulnerabilities in programs and makes them public. It is therefore natural that more discoveries are made.

There is also an increasing number of objects, the much-discussed Internet of things, which use embedded software, and therefore present vulnerabilities. The recent example of the "Mirai" network demonstrates the vulnerability of these environments which account for a growing

portion of our digital activities. Therefore, the rise in the number of vulnerabilities published simply represents the increase in our digital activities.

What about the attacks?

The publicity surrounding attacks is not directly connected to the number of vulnerabilities, even if it is involved. The notion of vulnerability does not directly express the impact that this vulnerability may have on our lives. Indeed, the effect of the malicious code, WannaCry, which affected the British health system by disabling certain hospitals and emergency services, can be viewed as a significant step in the harmfulness of malicious codes. This attack led to either deaths or delayed care on an unprecedented scale.



Distribution of vulnerabilities to attacks, rated by severity of vulnerability over a period of time. https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time, CC BY

It is always easy to say, in hindsight, that an event was foreseeable. And yet, it must be acknowledged that the use of "old" tools (Windows XP, SMBv1) in these vital systems is problematic. In the digital world, fifteen years represents three or even four generations of operating systems, unlike in the physical world, where we can have equipment dating from 20 or 30 years ago, if not even longer. Who could imagine a car being obsolete (to the point of no longer being usable) after five years? This major difference in evaluating time, which is deeply engrained in our current way of life, is largely responsible for the success and impact of the attacks we are experiencing today.

It should also be noted that in terms of both scale and impact, digital attacks are not new. In the past, worms such as CodeRed in 2001 and Slammer in 2003, also infected a number of important machines, making the Internet unusable for some time. The only difference was that at the time of these attacks, critical infrastructures were less dependent on a permanent Internet connection, therefore limiting the impact to the digital world alone.

The most critical attacks, however, are not those in which the attackers benefit the most. In the Canadian Bitcoin Highjack in 2014, for example, attackers hijacked this virtual currency for a direct financial gain without disturbing the bitcoin network, while other similar attacks on routing in 2008 made the network largely unavailable without any financial gain.

So where does all this leave us in terms of the adequacy of our digital protection?

There is no question that outstanding progress has been made in protecting information systems over the past several years. The detection of an increasing number of vulnerabilities, combined with progressively shorter periods between updates, is continually strengthening the

reliability of digital services. The automation of the update process for individuals, which concerns operating systems as well as browsers, applications, telephones and tablets, has helped limit exposure to vulnerabilities.

At the same time, in the business world we have witnessed a shift towards a real understanding of the risks involved in digital uses. This, along with the introduction of technical tools and resources for training and certification, could help increase all users' general awareness of both the risks and opportunities presented by digital technology.

How can we continue to reduce the risks?

After working in this field for 25 years, and though we must remain humble in response to the risks we face and will continue to face, I remain optimistic about the possibilities of strengthening our confidence in the digital world. Nevertheless, it appears necessary to support users in their digital activities in order to help them understand how these services work and the associated risks. ANSSI's publication of measures for a healthy network for personal and business use is an important example of this need for information and training which will help all individuals make conscious, appropriate choices when it comes to digital use.

Another aspect, which is more oriented towards developers and service providers, is increasing the modularity of our systems. This will allow us to control access to our digital systems, make them simple to configure, and easier to update. In this way, we will continue to reduce our exposure to the risk of a computer-related attack while using our digital tools to an ever-greater extent.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation