What to do about computer malware and viruses

Draft by Martin Clark 21/02/2023 troppo19@gmail.com

Introduction

I said I would write something about this didn't I. Yep. Then I found out that the subject is VAST.

A bit like the other subject that I have expertise in, being the REAL nature of climate. I have promised a number of people that I will try to summarise my knowledge of climate in the context of being a Bahá'í. The difficulty is, "climate goes in a thousand directions, and there are more than 100 areas of technical and scientific study that have a bearing on climate". That is a quote from my old colleague Dr Robert Carter. Did I accept that at face-value? No. I started to count the areas, and stopped counting when I got to about 84. It was the nature of climate that first prompted the development of "chaos mathematics" as a field of study.

I'll try to limit what follows to 2 x A4 pages in a reasonably compact font.

Malware and viruses

Malware is a term used to describe any program or code that is created with the intent to do harm to a computer, network or server. A virus is a type of malware, but its definition is limited to programs or code that self-replicate or copy themselves in order to spread to other devices or areas of the network. Viruses try to hide, but malware may be a component of software that is apparently, or may actually be, useful, but contains components that do something you do not know about and have not approved. [source: crowdstrike.com).

It now turns out that some types of malware may be introduced into a system as a way of benefitting the writer of software, rather than doing actual damage. An example of this is PDFsam (https://pdfsam.org/) which has a number of pdf management tools that can be useful, but the installation spreads bits of itself throughout the Windows registry and dominates the context settings, and all the bits are hard to remove. (LibreOffice Draw can reverse engineer pdfs.)

Another danger of "harmless" malware is that it can become a route for real damage to be introduced. This is also the case of software that is genuinely useful, such as AutoHotkey, which sees a key sequence such as #A and can translate that into a much longer sequence. I used to use Texter and AutoHotkey to reproduce frequently needed sequences in my professional writing. Bahá'ís may use this type of software in order to easily transliterate words and names with diacriticals such as 'Abdu'l-Baha, Bahá'í, Bahá'u'llah. The problem is, this type of software employs a scripting method that can be invaded, and used to write very damaging scripts. As a result, some virus-checking software will quarantine this type of program. The examples here are copy/pasted from a text file that has most of the common terms requiring diacriticals. (Look for "Oriental Words in Bahá'í Literature, Transliteration, and Pronunciation published in *Bahá'í World*, Vol. 18 (1979-1983), pages 893-904 Haifa: Bahá'í World Centre, 1986.)

Fonts have been created that try to make the problem of diacriticals easier for Bahá'ís, but unfortunately, the writers cannot resist the temptation to make these fonts ornate and flowery "in keeping with the context".

Vulnerability to malware and viruses

Virus and malware checking software is generally available for Windows (pc and laptops), macOS (Apple/Macintosh pcs and laptops), Android (phones), iOS (iPhones), and ChromeOS ("Chromebooks", eg Google operating system for laptops, miniature pcs).

The CVE website (https://cve.mitre.org/) lists the number of cybersecurity vulnerabilities for three of these operating systems; ChromeOS; 55, Windows; 1111, macOS; 2212.

Absent from the list of operating systems is Linux. This is said to be because there are relatively very few personal and desktop computers running Linux, but it is also the case that it is very difficult to write viruses and malware for Linux. However, there are very many network computers running Linux that provide staging and server functions, and these need protection at the enterprise level.

I cannot find a count of vulnerabilities for Android devices, but running Avast anti-virus on my phone threw up a large number of serious risks. I believe it was a virus on my phone that resulted in the attack on me. I noticed a couple of occasions when my bank sent a message with a code to enter to confirm a change of password, which had not been generated by me. I thought this was because someone out there had a bank ID similar to mine and kept typing my ID not theirs. Similar to people who ring you and expect you to be someone else because they have the number wrong, but sometimes refuse to believe it is their error. I reported two of these, got my internet banking frozen until a fresh change of password was effected by me. Initially the bank refused to change my internet ID number, which was a serious error on their part. I was lucky. The fraudulent transaction used a BPay reference to transfer a large payment to a supplier who does not trade in this area. The transfer was to an identifiable account, and the money has been paid back. It is possible that someone will now be prosecuted for this offence.

There are viruses listed by ThreatFabric [https://www.threatfabric.com/] as the "SpyNote" family that runs on mobile phones that can confirm a change of password without the account owner's knowledge. It is possible that one of these was used on me, but I recently found another risky area, being the "Spam" inbox used in most email software, where "dubious" items are dropped. I have to peruse this area every day using Gmail because it often places material that I know to be safe, written by people I know and have worked with, that triggers Google's false "fact-checking" censorship, so I have to order Google NOT to categorise it as spam. For some items in spam, it is difficult to determine from the title, so it is necessary to open the item. This has enabled me to alert clients and people I know to the fact that someone has hijacked their email account and is sending out stuff that they would not have sent themselves. There are also spam emails that have pdf attachments. If in doubt, DON'T download these. I recently accidentally downloaded a pdf file that was immediately placed in quarantine by my virus/malware checker because it contained a serious "phishing" threat that could be activated if I opened the pdf, which was capable of spying out for banking IDs and the like. Pdfs and images CAN be used to transmit malware and viruses, and it seems that Windows Defender / Windows Security will NOT detect them.

<u>What to do</u>

Do NOT rely on Windows Defender / Windows Security. It is basically useless. Windows 11 is spruiked as being more secure but is probably less secure. It has functions that try to hide things more than Windows 10, and as a result provides more hiding places for criminals.

An example of the competence of Windows programmers is the web browser, Edge. This will not allow a user (like me) to use a local html file that they have written themselves as a home page. You are supposed to find a home page on the internet !!! This is absurd, but you cannot safely uninstall Edge because there are programs that expect it to be present. Make sure you have a copy of Brave browser https://brave.com/. Make sure you have a range of choices for searching – do not rely on Google, get second opinions from Startpage, dogpile.

To start cleaning out my systems, I got a "free" copy of Avast, and GridinSoft Anti-Malware.

These give a "free" report, but don't clear up the mess until you pay for it. I don't blame them for charging. They all need to have the support of the higher tier organisations assessing cyber security, which sometimes costs thousands.

If you have few problems, then it may be possible to do screen captures to get a copy of the reported problems and delete them yourself, but if there are many issues, then it would be more cost-effective to pay for a subscription. (Watch out for McAfee. This is installed on many new computers, and you might get emails from fraudulent sources trying to get you to pay the subscription – to someone else.)

I decided to pay annual subscriptions. It is quite possible that the attack on me was a bi-product of my activities as an advocate (3-4 successful appeals to the Queensland Supreme Court written by me) and being an Assessor (judge) on the Queensland Building and Development Tribunal. I can be identified on numerous cases and could easily have a few enemies as a result.

One common finding is a program called “Advanced Windows Manager” which may be in the directory C:\Program Files (x86). This has a PUP (potentially unwanted program) virus.

Is this problem getting worse?

It has certainly been made worse by the (pointless) Covid-19 lock-downs of the past few years. People had to rely on digital communication, which exposed all of us to a greater risk than face-to-face meetings. Communication systems are being used that have questionable security. Facebook, WhatsApp and LinkedIn all now belong to individuals or agencies who support leftist oppression of humanity, and the claim that transactions are encrypted may now have little value.