Great post on Antivirus and how it may be a layer of protection but should not be the ultimate solution. There are large number of vendors that provide antivirus solutions however many of them are not strong enough to detect advanced threats and some are. Antivirus vendors rely on information being sent back to them so they can update definitions to know what to look for when a threat immerges.

Hackers are becoming smarter and are deploying malware through phishing emails and the payloads they are delivering are not being detected by the antivirus software, this is also known as fileless malware (Mcafee, 2021) This makes it more difficult to trace.

Having worked with a client back in 2017 where all operating systems were infected by a machine that had Remote Desktop (RDP) drive sharing enabled, allowed the malware to implement itself on all Windows Servers and by means of encrypting data in the WMI database in the operating system, it remained undetected until its scheduled processes started running. PowerShell instances were launched and ran in the background and because it called a legitimate process, the antivirus solution that was running on the systems did not alert of anything suspicious.

This shows that companies should not rely on antivirus products alone but need to protect the internal network (LAN) from external threats and implement policies that stop end user sessions from connecting local drives to servers. This is the quickest way for an infection to happen and allows attackers to deploy malware using the bot which will eventually result in ransomware on the systems.

References

Anon. (2021) What is Filess Malware. Available from: <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html> [Accessed 20 September 2021].