Now We Have Fileless Malware; How to Fight It

Excerpts from Ask Bob Rankin

Traditional malware consists of one or more files stored on a hard disk. At least one of these files must be executable, and the malware cannot do any harm until that file is executed. Fileless malware, in contrast, resides in RAM memory and is never written to your hard drive as a file.

Files leave traces as they are read or written to disk. A file has a pattern that can be reduced to a static signature that can be compared to known signatures in antivirus databases. These and other traits of files make it easier to figure out where a file-based malware package came from and what it is.

Instead of tricking the user to download and run an executable file, fileless malware uses legitimate, trusted tools that are part of the operating system to do its dirty work. That means there are no “suspicious” programs on the hard drive, or active in memory. Just the “ghost” lurking in system memory space.

Fileless malware is fluid. It perfectly fits itself into unused gaps in RAM, all linked together by beginning and ending memory addresses. Traditional antivirus software looks in vain for the wrong thing – a signature – and in the wrong place – the hard disk – ignoring what is in main memory.

Fileless attacks are said to be ten times more likely to succeed than file-based attacks. Fileless malware played a role in the devastating Equifax breach that exposed the personal information of over 100 million consumers.

Traditional anti-virus programs that rely on file-based scanning will not stop these attacks. Avast, Avira and Bitdefender do claim to protect against this threat, but barely mentions it on their websites. MalwareBytes has done a lot of research on this type of malware and seems to understand mitigation strategies well. PC-Matic differentiates itself by focusing on emerging polymorphic threats and fileless ransomware detection.

It's important to keep yourself aware of emerging threats and take action where you can to protect yourself, your computer, and your important data. Keeping your operating system, application software and anti-malware defenses updated is an important first step.

And since some of these fileless malware attacks rely on Windows PowerShell, experts recommend disabling that as well. To do so, follow these steps:

- **a.** Type *windows features* in the Windows 10/11 search box, and press ENTER.
- **b.** Scroll down to the Windows PowerShell 2.0 line item.
- **c.** Uncheck the box next to it, and click OK
- **d.** Wait for the prompt to restart your computer.