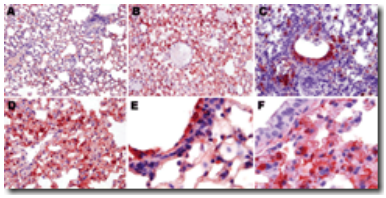
Most Human Viruses are obvious.

Don MacVittie, 2010-30-11

We spent the US Holiday Thanksgiving at my Mothers' house some 500 miles away. We love when we get the chance to see her, and there's always someone else there. This year one of my wonderful nieces was there with husband and baby in tow. And the baby was sick. Now this is my grand-niece, so of course I wanted to spoil her a bit, but she was out of sorts with a cold and ear infection, so it was tough. The Toddler is at the age where he wants to play with little girls, but beyond tag isn't certain how to play with them. Sharing toys is one way, but then they don't want to do it ***his way.*** So lots of "irritate the little girl, apologize, then go for a hug and a kiss." With a sick child. It didn't take long before nearly everyone in the house was sick, compliments of one of the two kids. The thing is, we all saw it coming. One sick child amongst two playing, in a house with ten people in it… You ***knew*** how this was going to end up, and no amount of handwashing was going to prevent it.

If only computer viruses were so obvious. Oh, most of them eventually use too many resources, or cause the machine to GPF, giving astute IT pros a chance to start remedial action, but by that point it's too late, the virus has spread all over the place. To be sure there are human viruses that stay hidden until they're well entrenched in a community, but the common ones don't. I guess that could be said about most enterprise level viruses too though – the common ones are stopped early because they have obvious symptoms or a detectable fingerprint (either in-flight or on-disk), while the really nasty ones stay hidden away until they're well propagated.

And it is unfortunate that at first our treatment for viruses is often the same as that for human viruses – treat the symptoms, not the problem. My advice of the day, when there is something odd on one of your systems, track it down remorselessly. Don't excuse it or make excuses for it, or throw more disk/memory/CPU at it, track it down. I can think of several instances where I brought up anomalies with systems I didn't own, the owner dismissed them and assured me there was no problem, only to find catastrophically at a later date that there was indeed a problem of the viral kind. I've even done it myself, thankfully only at home, but I'm guilty of "this machine is getting old" or "needs a reinstall"… Which of course is not finding the root cause and resolving it, but just a less painful (because it was a home machine) version of the same issue in the enterprise.



And infections come from the oddest places, your network is actually in contact with a lot more machines than you think – I'm writing this from a work provided machine over a VPN to corporate HQ. But this machine is also on our local network, and every other Saturday people bring their laptops and put them on our network to game… I have no idea how many other machines they're exposed to, but I do know that two of them go on Sundays to log in at another person's house to game, and there are a ton of people there… I think I'll blog about that later – look for a blog on Thursday titled 'Vector is no longer adequate". The point for this blog is that you are open to infection, and a really good infection will go a good long while without detection. Putting in active firewalls is a good idea – both traditional and app firewalls, a VPN with authentication and solid logging, so at least you can track down the source of the infection, and regular reviews of policy, procedure, and active processes on boxes is a good idea.

Image Compliments of Centers for Disease Control

Like some of the more virulent human viruses, you can of course quarantine infected machines, but like with humans this only works if you have a way to identify all infected machines on your network, which can be difficult, but is a big help to containing an outbreak. The other issue with quarantine is what, ultimately, to do with machines in quarantine. If you can't clean them safely (and most of the time you can't), the ultimate solution is generally to wipe them clean and reinstall. But depending upon the machine in question, the quality and age of your backups, and idiosyncrasies in software installed, this can create very real issues both political and in terms of lost productivity.

Do I have the golden answer? No, I'd be both wealthy and famous if I did. At least for the fifteen minutes until the next wave of intelligent viruses came along and avoided my golden answer. Put quality tools in place, as automated as possible that you build a plan to keep up-to-date, and then keep diligent in watching your systems. Respond to every anomaly that is not readily explained as if it was an infection – or at least as if it was a threat – and keep your security staff focused on just that – securing the organization. Finally, I can't stress enough the value of an external penetration test by a really great company. You miss things you see every day because they're part of the scenery. They're looking for problems and will likely find some. Better a pentest company than a virus or a hacker.

In short, don't forget the basics. Life is easier with tear-down and restart VMs, but you still need to be diligent.


F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com