

# Virus outbreaks attack clients computers



John Deans

It may be clean country air, good food, or just plain luck but I have not been sick from a virus in years.

Slight colds here and there, but no fever or throwing up has hit me. Until this week I could have said the same thing about computer viruses, but no more.

Within five days two clients got hit with two different types of viruses. Today we will walk through those troubling timelines and learn how they happened, how they were fought, and what can be done differently to prevent such outbreaks again.

Let's start with Client A, who recently had some of their computer support outsourced to a Houston-based IT company that performed all their software maintenance remotely. My role was still needed to do the on-site duties, which was fine with me as long as there was good communication.

Turns out that lack of communication had already begun with them replacing my AVG antivirus with a different OEM version that appeared to be working but had actually been dysfunctional for weeks.

During that time we lost two older

computers from corruption of Microsoft Windows. Since Client A wanted to phase out those computers with new Dells anyway, we just put them aside. But when a third went down I had to jump in and investigate why.

The three computers would not even boot so it was too difficult run a virus scan. What I did was verify the virus updates were timely on the remaining PCs and that is when I discovered they were not only stale but the antivirus software was not working.

Red Flag Alert! We immediately got on the phone with the remote outsourced IT company and after some interrogation

discovered that a third person probably accidentally misconfigured it during installation which let numerous really bad viruses into the network.

After the cause was determined, the fix was quickly applied which entailed removing all OEM'd antivirus software installations and re-installing my full retail version of AVG. The remaining computers were saved and we have begun re-loading Windows on those three that died to make them usable again.

Lesson learned: Avoid too many cooks in the kitchen.

A couple of days later I was installing some new computers at Client B, which required new installations of AVG antivirus which led me to setup the latest version 8. Since the license had not expired on the other 20+ computers with version 7.5 they were left as is.

Only a small percentage of the hundreds of computer I manage had the new 8.0 and the 7.5 based PCs were all still getting the same virus signature definition updates.

During those installations, a user ran to me and said his computer was crashing with the "Blue Screen of Death." Thinking it was just a case of bad spyware I ran my favorite anti-spyware software, ComboFix, and

it found hundreds of problems. This is when I realized it was not just a spyware problem but a virus outbreak.

This user, due to his artistic and international background, was all over the Internet on various foreign sites, so he was really pushing the safeguards put in place.

I upgraded his AVG from 7.5 to 8.0 and numerous virus hits started showing up. At that same time two other users at Client B came down the hall telling me their computer was showing virus infections on the server! This made me stomach start hurting.

Those two computers also had the latest AVG 8.0 and they were seeing dozens of .EXE (executable) files located on our company server that had the Tanatos virus, which is non-destructive but it can bring in other viruses that are more damaging.

Red Flag Alert Number 2! Due to my harsh experience with three computers dying days before at Client A, I put the whole computing environment of Client B into complete lockdown and called in the Jason from Computer Helpers for backup.

It really helps to have a second pair of hands and eyes to combat a dynamic and possibly catastrophic virus attack that

could take out 25 computers in minutes.

With every virus and even every virus version being different along with not knowing if it is just a single virus or a mass infection by many hosted or imported malware entities, there is no textbook procedure to follow.

The first thing we did was disconnect all the workstations and even the server from the network that connects them all together to stop the spread of the virus. Then while Jason researched the named virus (Tanatos.m). I started running scans and trying to find a fix.

We found out that a new strain of Tanatos had recently hit and that virus signature update had just been distributed by AVG at 3 p.m. that very day!

We found a repair program on AVG's Web site and so we started applying the fix via our USB thumb drive. Then we found out that this virus was automatically and quickly infecting our USB thumb drive along with the virus fix executables!

Luckily we discovered this after the second application.

Jason just happened to have an older thumb drive with a write-protected switch so we put the virus fix along with the AVG 8.0 upgrade on that one to distribute to the other 24 computers.

With our intruder identi-

fied, its tactics learned, the fix acquired, we then were able to put together a process to decontaminate our environment using a Mac laptop to verify all remaining USB thumb drives in the company were clean.

The next 12 hours was spent running the fix (which took up to an hour) and upgrading all 7.5 AVGs to 8.0 on all computers. The infected files were removed from the server and all workstations.

The next day, after only three hours sleep, I had the systems all up, operational and clean. The chest pains were finally residing too.

Lesson learned: AVG 7.5 checks for virus signature updates once a day where as the new AVG 8.0 checks every four hours. Those golden hours between a virus being sent out and the signature definition being received from the antivirus company is critical!

Bottom line: Though I had not been sick for years, after this week I felt I just recovered from malaria caught in the computer jungle.

Next week's column: VistaPrint.

John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.