Virus\_Machine\_CleanUP

I was scanning the Slack logs and saw that the two guys who were spamming us made contact. YEAH!

That means they do want to continue in our program, and it’s not an intentional or known attack, which is good.

I will be happy to work with either these students directly or in combination with Rick & Steve as their instructors. This is a bit of over kill. Two thoughts on that, YES I am the king of it. However because these two machines have consumed a lot of your precious time, I’m going to be very cautious.

This is a long email, I’m the king of troubleshooting. I have learned to masterfully peal back the layers of the digital onion and make a reasonable assumption at the causes. May not know a solution but if I can say, “Doing X changed the behavior.” That becomes a data point and part of the puzzle of what’s wrong.

Most people don’t want to take the time to do this kind of troubleshooting. It’s even harder to take the 40+ years of practice and put it into an email. So this is broken into two parts. A kind of **Slash and Burn** technique and a more of a **Surgical** approach.

Of particular note here, if this was my computer. I would erase everything and start over. I have spent weeks of my life trying to remove obscure viruses or unwanted code, and in the end my best solution has always been, Fdisk, Format, Reload. Slash and burn will take about a weekend to rebuild a machine. Where as the more surgical approach could take a lot longer and in the end it still may be failing.

**Slash** and **Burn**:

* As it suggests, FDisk the computer and reload all operating system and software.
  + BACKUP ~ ALL DATA! I can’t stress this enough.
  + Erase everything and reload the OS.
  + Bring the OS up to the latest version of patches.
  + Load only one Browser, FireFox or Chrome
  + Try logging in and moving on with our lessons.
  + If no attack is recorded by our systems we know it’s been resolved.
  + Warning to student, Slowly re-install their software. Paying particular attention to what was “Free” software of any type. One of the pieces of software they loaded was performing a DDOS type of attack on our systems.

**Surgical** approach to troubleshooting.

My approach would be this. Let them know their accounts work and rebuild their faith in our LMS.

* Get them to agree to use a different machine even from a different network for the first test.
* First test is re-enable their account; get them to log in, move through a lesson log off and back on.
* By eliminating the failing machines all we are testing is to prove to them that our LMS is functional, and the issue was localized.

Next Virus Detection Plan

* Back to their troubled machines. Step one they have to promise me they used at least 2 different anti-virus tools.
  + From my history I have found that when the infestation (IF it’s a virus) is missed by 1 brand it is sometimes caught by a second scan from a different virus manufacturer. My humble recommendations would be NOT Kaspersky or McAfee. But use AVG and an odd one called F-PROT or F-Secure. If these students have a paid for version of anything, just try another scan.
  + Kaspersky ~ not allowed in any US government facility we are a school
  + McAfee ~ Free versions are too prolific and quite possibly an older one could miss something.
  + AVG 🡺 HERE [ https : / / w w w .avg.com/en-us/homepage#pc ]
  + F-PROT 🡺 HERE [ http : / / w ww.f-prot.com/ ]
  + F-Secure 🡺 HERE [ https : / / w ww.f-secure.com/en\_US/welcome/ ]

NO Virus detected

* Clear all cached data from all browsers using the CTL-SHIFT-DEL method.
* If Win ~ Record version and update to the latest security updates.
* If Mac ~ I need guidance from you Kevin, how do we update a MAC.
* Understand a little about their network. If it’s a home network can we shut down all machines on it except the one we are testing? Because of NAT all systems in their home network will have the same IP that we are blocking. (IF that’s how we are blocking them? )
* Start their system while we are monitoring our network activity.
  + At this point they haven’t logged on, they haven’t opened a browsers. Their system is just sitting there doing nothing. It’s been virus scanned, it’s been updated and it should not be causing any issues for our network.

Let’s get them back online locally

* Next we ask them which browser and version they like to use (It of course is up to date as well.)
* Ask how many Browser Add on’s or Extensions they have and which are they.
  + If they just turn them all off, everything is fine, then turn back on. The issue could return.
* Open browser and only that have them log in while monitoring our servers.
  + If no spike is noticed have them continue to work for a while as we monitor.

What to do if the attack re-starts.

A lot of that is predicated upon when the attack restarts.

* As soon as the virus scanning has finished and their systems are in the process of updating patches the OS requires.
  + That would indicate there is something very wrong with their systems and it’s out of our hands.
* When their browser is opened but before they attempt to log in or authenticate to our systems.
  + This would tell me a BHO or Extension has been added that is clearly not helpful.
  + Troubleshooting from this stand point
    - My preference would be to remove all traces of that browser and re install it.
    - If FF or CH look for maybe the beta versions.
    - Alternatively the student could go extension by extension removing them. I don’t believe this would be helpful. If it’s a nefarious bit of code, just removing the extension will probably not solve the issue.
* If the attack re-starts when they attempt to authenticate to our system. This indicates a much deeper issue.
  + Start by the same steps as before, remove & replace browser. The difference is we now know it’s not something that happens when the browser is idle, but only when it starts to make https connections.
* S



Scott B. Stemen | Automation QA Engineer (SDE/T)   
C: 480.298.9036 | [Scott.Stemen@Woz-U.Com](mailto:Scott.Stemen@Woz-U.Com)

[https://WOZ-U.Com](https://woz-u.com/)