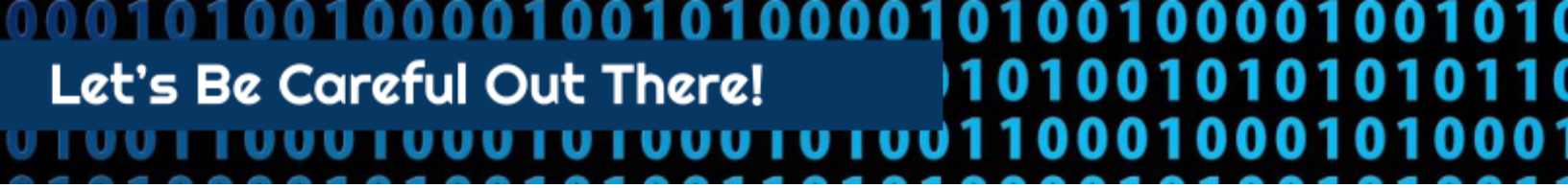


Ransomware Testing

BACKGROUND

Ransomware is one of the biggest threats to organizations today. In fact, one big target seems to be third parties that manage data for multiple organizations. In August 2019, hundreds of dentist offices were affected when the data manager DDS Safe was infected.

Contrary to popular belief, many antivirus solutions will not always catch ransomware. This exercise will provide a stress test on your Windows machine and let you know which, if any, strains of ransomware you are susceptible to.

When doing this exercise, feel free to run different AV or ransomware prevention software and see which attacks are caught and which ones are not.

REQUIREMENTS

A working installation of Windows, a web browser, and an internet connection. You can use a Windows VM. Note that you can get a free Windows 10 VM from Microsoft here:

https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

PART I: Download the RanSim software

1. The company KnowBe4 provides security training for companies of all sizes (one of their classes stars Kevin Mitnick). They also make a number of tools available to people *for free*.

   For this exercise, we will be using RanSim, which will simulate fifteen different ransomware attacks and one cryptomining attack. Don't worry--no files on your computer should be harmed during this process (although this would be a good time to fire up Windows 10 as a virtual machine--just remember to knock the processors up to 2).

2. Download the software here:

   https://www.knowbe4.com/ransomware-simulator

3. You will most likely have to provide your name and email address; use any email address you want--it does not have to be your school account, nor does it have to be a valid email (with some exceptions; for example, the form will not accept gmail.com or

test.com email addresses). You will be given access to the `.zip` file and the password to open the file.

4. Install RanSim on your Windows machine.

EVIDENCE #1

INSERT A SCREENSHOT OF RANSIM INSTALLED.

PART II: Run RanSim

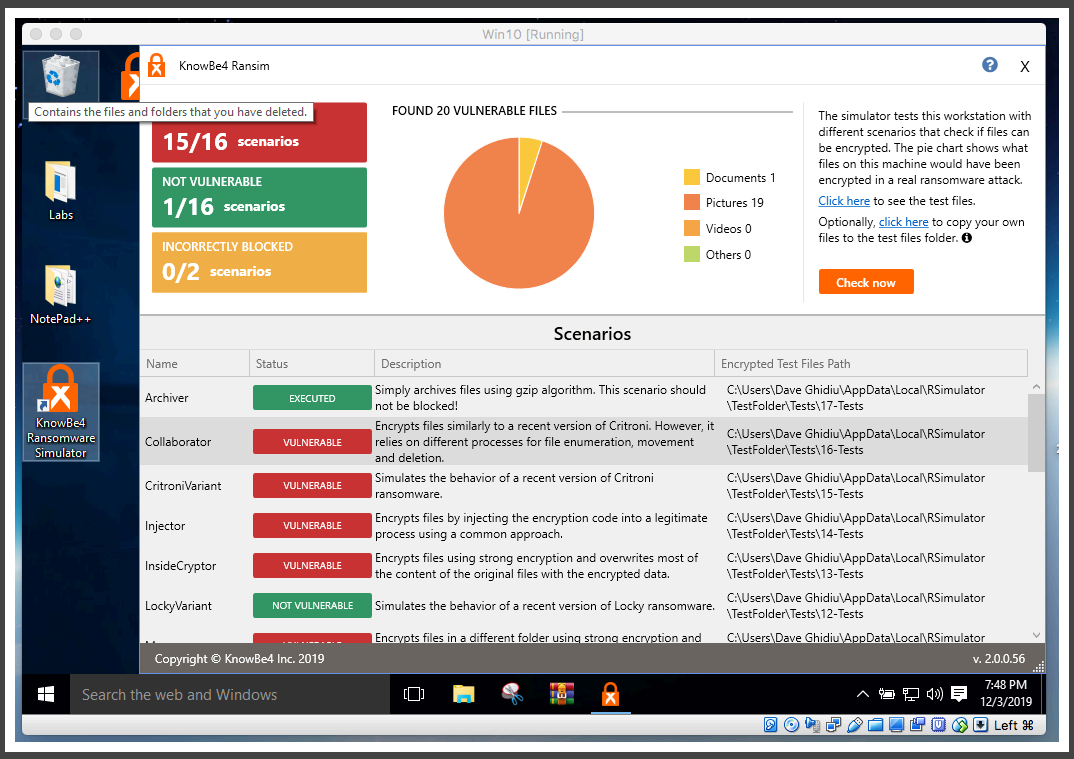
1. Double click on the software and run it. The test may take several minutes. RanSim works by actually using ransomware to lock files. Don't worry! It locks it's own files, not any of yours.

2. You'll get a report of the flavors of ransomware that were able to successfully lock files. It's possible that your system was able to ward off all the different attacks (if you have your computer locked down appropriately). Either way, you'll see which attacks you need to better prepare for.

3. In this example, I used Windows 10 out-of-the-box, just like an average consumer would.

I was susceptible to all of the attempts.

EVIDENCE #2



INSERT A SCREENSHOT OF THE RANSIM REPORT