Investigation of group 1
By group 14 (_undefined)
4/23/16

Preface

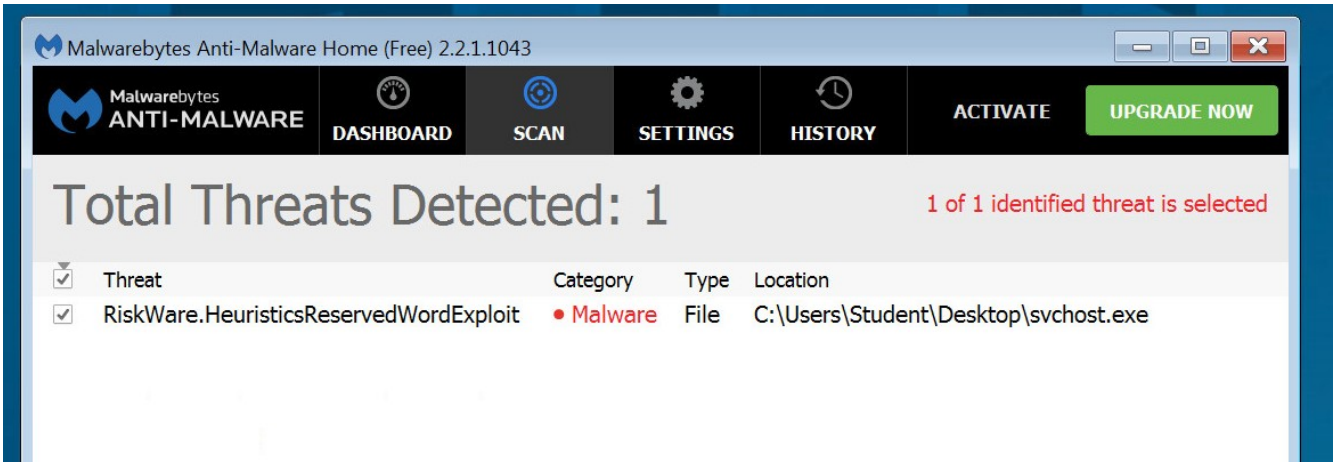
We were given given a VM with instructions to start a key logger when we logged in. Group 1 said that this was for our benefit and that if they wanted to they could schedule the program so it would start on start up. So it was our job to find traces of the key logger.

Our approach

Now that we knew that we were dealing with a key logger we decided to split this investigation into 2 parts. The First part is if we where average users, we would just do some security scans and try to see if anything was off during normal activity. The second part of the investigation was if we couldn't find anything with the scan we where to dive deeper into the system to see if we could find it manually. In this step we assumed that we the users where just overly paranoid. In the first step we were to use the following tools, Malwarebytes, Super AntiSpyware, AVG anti virus, and Spybot Search & Destroy. If we had to go to the second step we would use the Microsoft system internals utilities to dive deep into the system. Some of the tools in this suit are Auto Runs, Process Explorer, and Process Monitor.

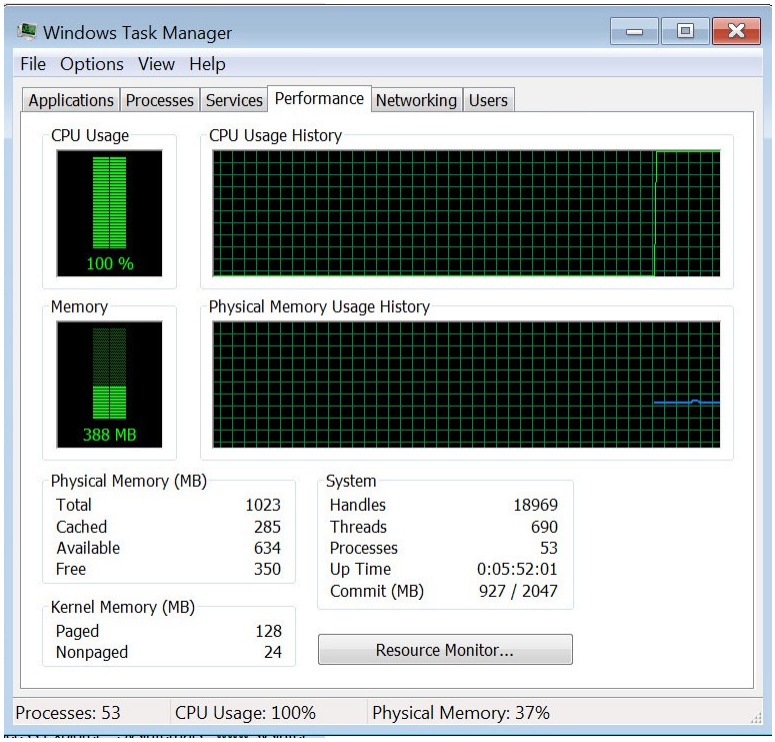
Phase 1 Results

The first tool we installed was Malwarebytes. Then we ran a computer wide scan and it found the key logger! Wanting to know if the others would catch the key logger we then installed the others and ran computer wide scans and they all found nothing! So we decided to investigate a little as to why only Malwarebytes found the key logger. From what we could find (which wasn't much because the internals on how this software works is secret) all of theses scans use a definition based search. This means that a definition needs to exist before the scan can actually pick of the key logger and because this key logger is brand new no definition has been made for it yet. Then why did Malwarebytes find the key logger? Malwarebytes it turns out not only uses this approach to finding malware but also does what they call a “heuristic analysis”. This looks for suspicious behavior from programs and flags possible dangerous ones. This is how Malwarebytes found the key logger.

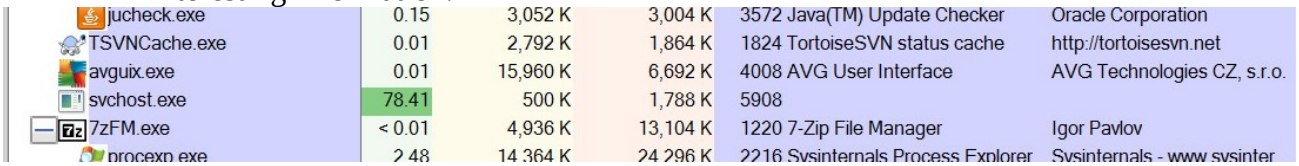


Phase 2 Results

With the first phase done we decide to continue the investigation and see what else we could find. Using the default process explorer we were flipping through the tabs and something was off. The CPU was at 100%!



Clearly something was off. So using the system internals: Process explorer we get some interesting information.



First of all there is no publisher or program description. On top of all of this that 78.41 refers to the amount of CPU usage. The key logger is using anywhere between 50 and 80 percent of the CPU on average. This clearly indicates something is wrong with this process.

Our Thoughts

Given the evidence there are a few things we would advise to better this key logger. First would be modify the program properties to give it a description and publisher. This might even allow the key logger to evade the scans. The last thing is clearly the program is structured in a way that makes its CPU usage really large. We recommend restructuring the program to lower this usage because the average user “should” know that something is wrong if their CPU is at 100% all the time