Local administrator is not just with Razer.. it is possible for ALL

Generated By 0xsp.com

Recently a Security researcher @jonhat discovered a zero-day vulnerability in the plug-and-play Razer Synapse installation that allows users to gain SYSTEM privileges on a Windows device quickly. by plugging the Razer mouse into the system, windows 10 will download the suitable software and start the process of driver installation. Since the process wrapper of this software is running with SYSTEM privileges, the attacker could abuse the installation path to lunch a prompt command with the same permission.

There is more?

After that disclosure, I have tried to conduct a test against another gamming keyboard “SteelSeries” which I have recently bought and started to play a litter bit with it. and was able to find another privilege escalation vulnerability, tried to contact https://support.steelseries.com/ but wasn't able to find any channel to report about their product's security issue.

Process investigation walkthrough

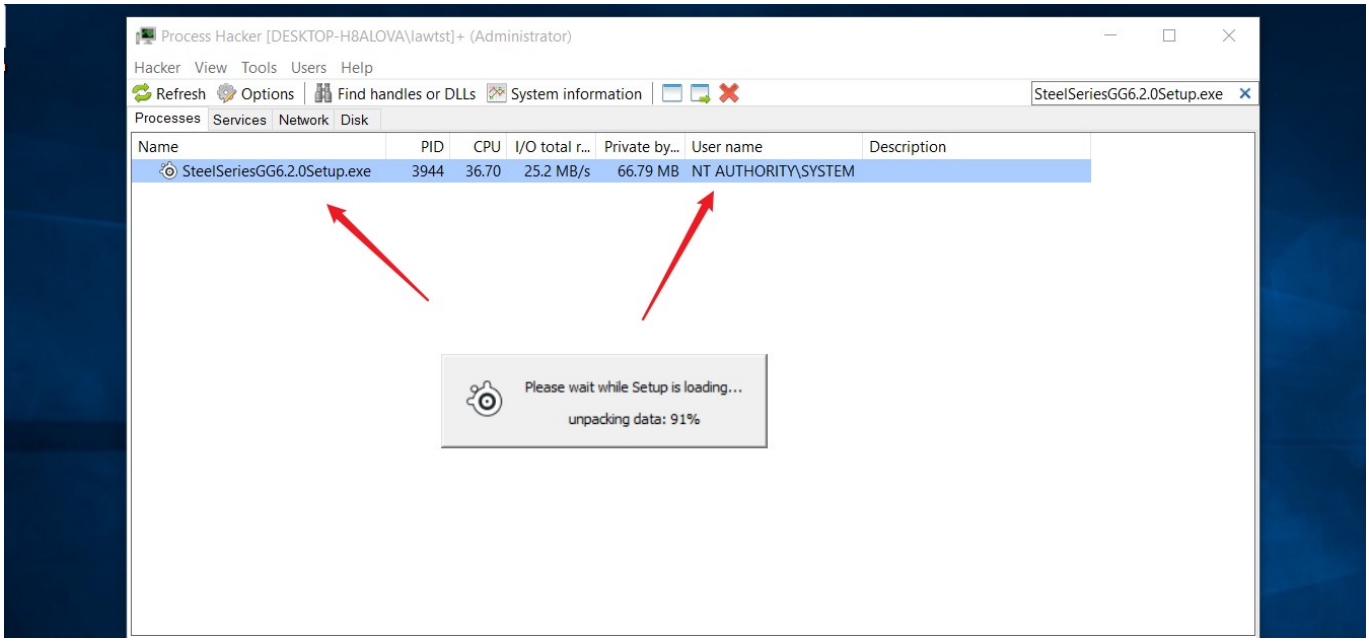
After plugging the keyboard, windows 10 start the process of installation and then immediately popped up the software installer as the following figure below In order to get insightful process information, the best way is by using Sysinternals toolkits such as Procmon or you can use process hacker portable version.

What have to understand from the installation process is that the software will first download another setup file “SteelSeriesGG6.2.0Setup.exe” and place the whole content into C:\windows\temp folder which means that the user cannot select a folder to save.

By using Procmon, I have applied some query filters to inspect if the application is loading any possible missing DLL/EXE from user folders that normal users have access to, but with no successful result.

```
#PROCMON FILTER
application name contains SteelSeries
path       endswith .dll or .exe
result   contains NOT
```

After finishing the downloading process, another setup process starts from the following path C:\windows\Temp\ with the same SYSTEM level.

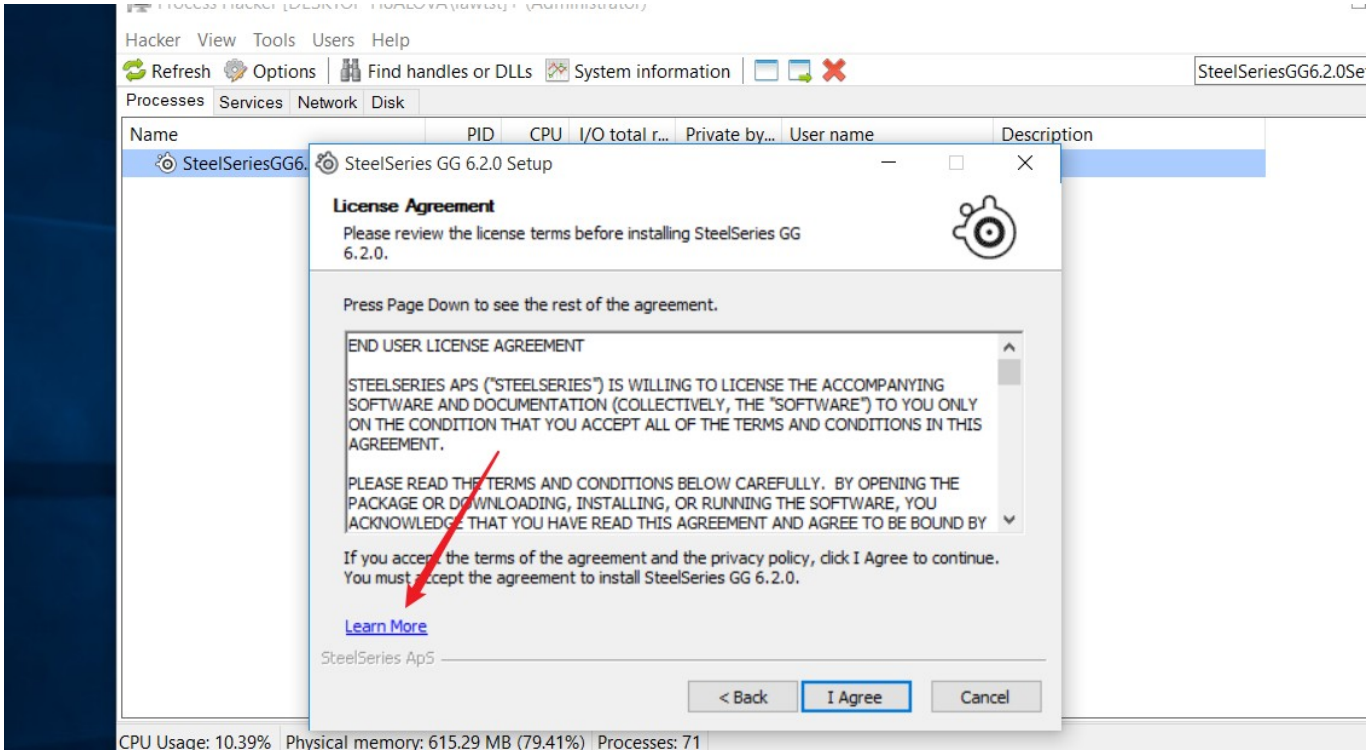


Attack chain

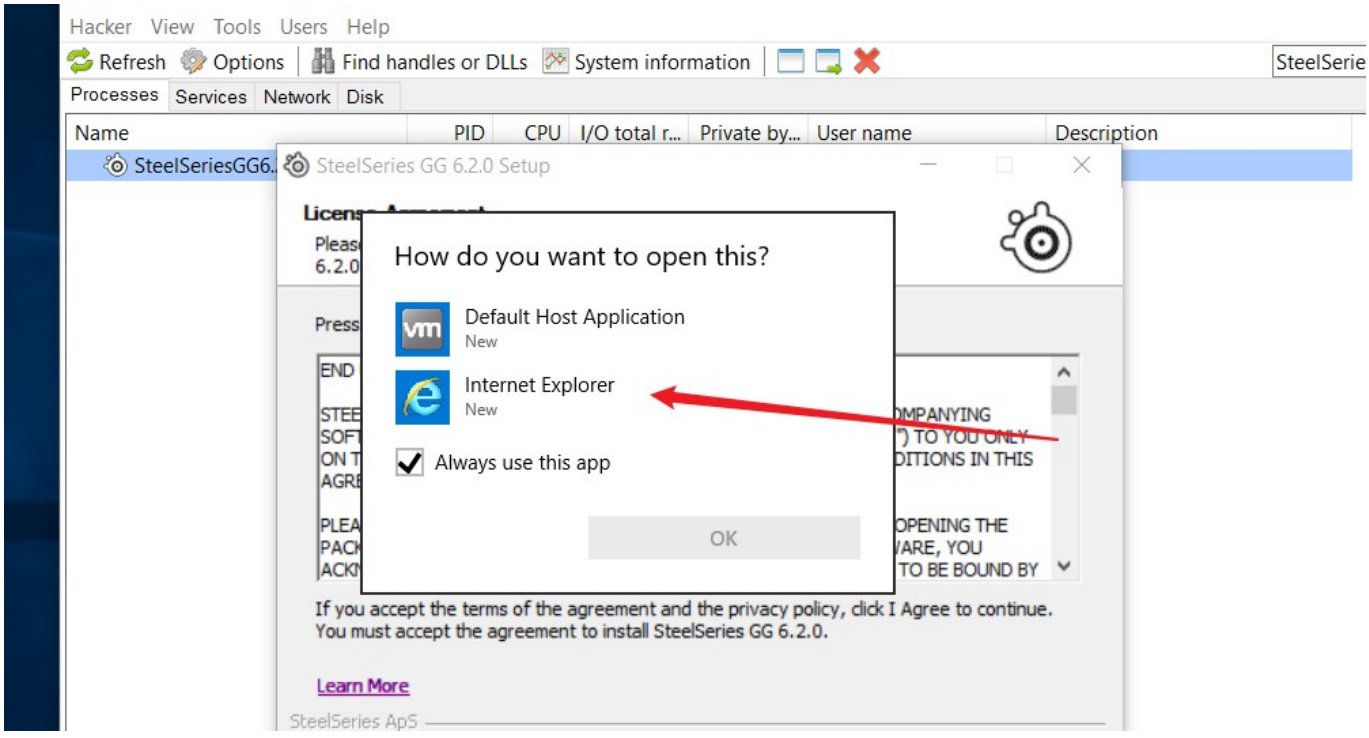
Since I have now another process running under SYSTEM privileges that gives another possibility to abuse it or find another way to escalate, I tried to find if there is any trick to choose the path to install, so from there, I can spawn a CMD. But I wasn't able to conduct such an attack similar to Razer's zero-day case, because the installation wizard chooses the default folder location and starts installation without user interaction. Also Tried to debug and monitor the setup process with Procmon but didn't find any possible way to exploit it.

Links are juicy

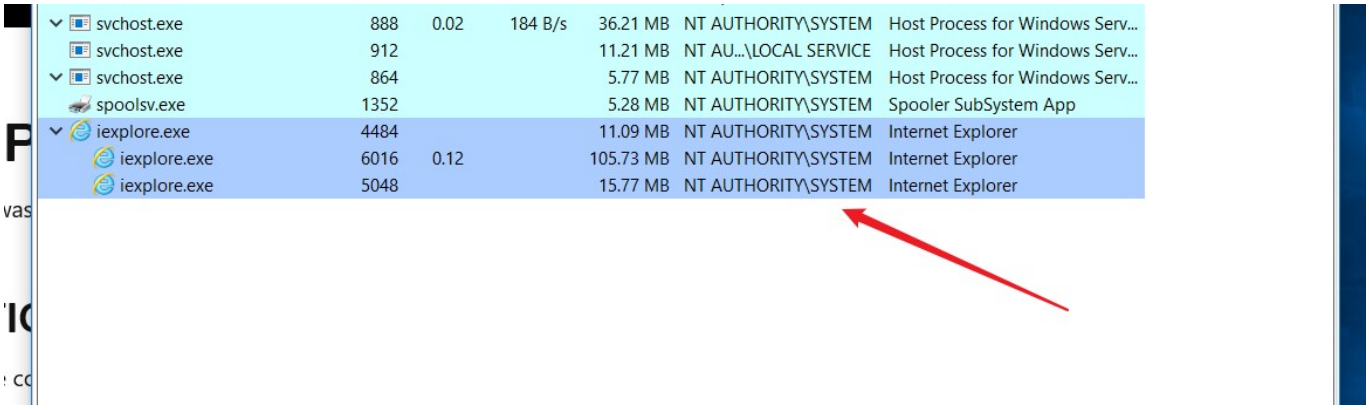
In any setup process, there is a user agreement that needs users' approval to proceed, by looking into the dialog I have spotted a learn more link is clickable and could allow me to abuse it to lunch another process with the same SYSTEM level.



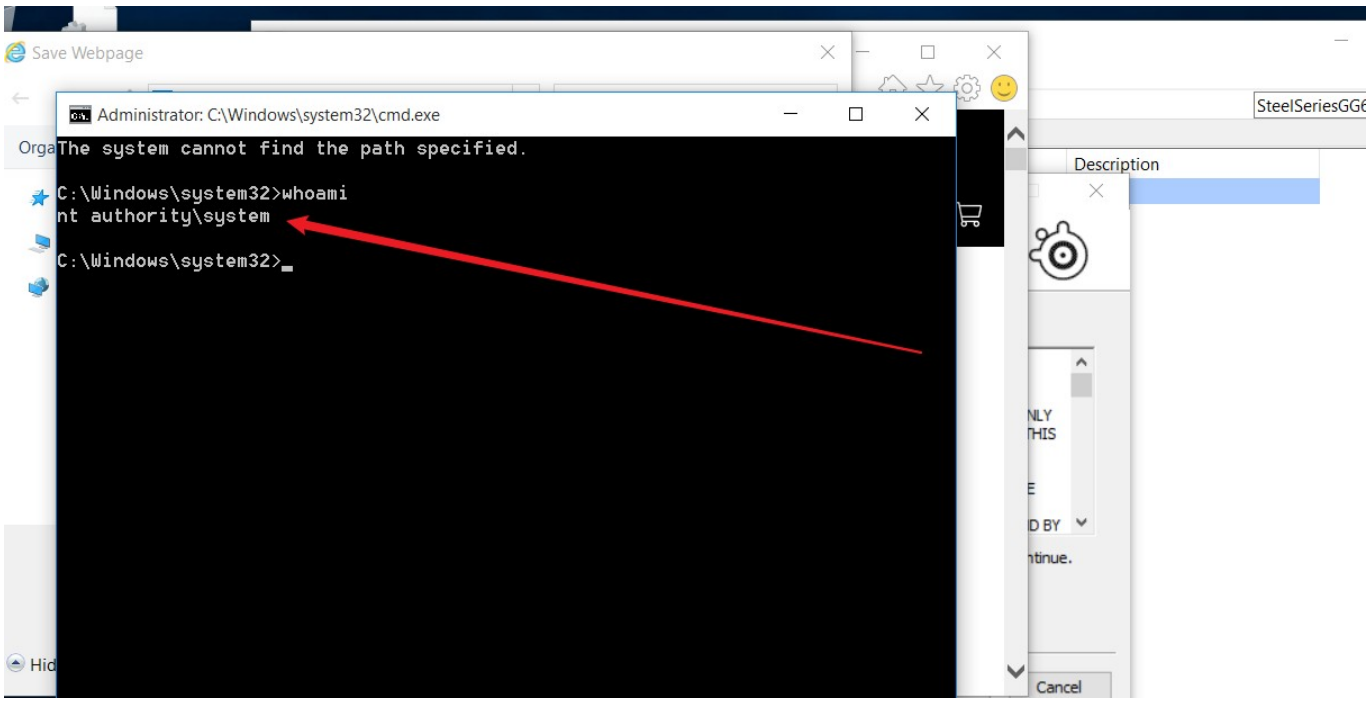
After clicking on the selected label, another dialog appeared with possible to choose a launcher application.



As the setup forbade to choose any process to open the link, while it is only by the default browser to proceed. After opening with internet explorer, the process is still running as SYSTEM.



And that's actually what all I need; I can use IE to save the web page into computer disk and inside the dialog, I can hold SHIFT hotkey and then spawn CMD and finally getting SYSTEM level.



Conclusion

as Summery since the vendors don't force proper access control against the downloadable firmware, we may still be working to conduct a test against multiple hardware products.