Rubber ducky

Technology, Information Technology

The USB Rubber Ducky Introduction The USB Rubber Ducky is the device used for the purpose of damaging the particular system. It has the processor that is programmed accordingly for making the destruction of the targeted computer where it is physically plugged in. The Universal Serial Bus (USB) devices are used for transmission of Data in a safe mode from one system at physical location to another location. It is the easiest and safest solution to deliver data. The growing age of technologies in the field of Information Technology the threats against USB flash storage are also grown up and demand a high degree of protection.

Physical Protection

The administrator’s system should have enough security that no one can physically interact with it and plug the USB stick with it. The physical access to an unauthorized person is strictly prohibited in the office environment (Pajari, 2014).

Destructions USB Rubber Ducky

The program keyboard is developed in it. The Rubber Ducky can alter the settings of the system and can open the doors for illegal access. All this work is done in seconds and can make a great loss of the secret data of the concerned organization and business. It can create files, and delete files from the system and also can deliver emails. All this can make a huge loss with the data of a particular company. In such situations, the backup is essential to recover the secret information and to protect from the severe situations. The ducky can bypass many tricks and easily makes it by the system’s keyboard, like the key combination of Ctrl+Alt+Delete.

Detection and Protection methods for Rubber Ducky

There are no direct symptoms that can detect and display the existence of USB Rubber Ducky and its functions. It could be predicted from the increased speed of the keyboard. The passwords set for security and protection must meet the standard format of a high security that is harder to be matched by the USB Rubber Ducky. To make it disable, the feature of foreign HIDscan provides protection from the USB Rubber Ducky to some extent. The changes made in the group policies can lead the process to fail. Some typing performed on the user side can also stop the processing of ducky in failure mode.

Must programming that can aid in the protection from the Ducky. In the Linux, the procedure of making USB devices into black and white list can help to stop the ducky processing. If the concerned system doesn’t respond to the ducky due to different reasons like time difference, delays, and active windows can make the ducky fail to process (Hak5 Forum, 2010).

Conclusion

In this paper, protection measures are only able to protect the system in specific circumstances, but if the case where the situation is not matched, it is impossible to make protection from the ducky. These are some precautions and safety paradigms that need to address for making security against the USB Rubber Ducky. The functionality of ducky is very dangerous for the organization, so it requires special attention for its protection and handling.

References

Hak5 Forum (2010). DefencesAgainst the Ducky. Available from: https://forums. hak5. org/index. php?/topic/16233-question-defences-against-

the-ducky/Accessed on: 11/26/2014.

Pajari, G. (2014). USB Flash Storage Threats and Risk Mitigation in an Air-Gapped Network Environment. CANSECWEST VANCOUVER 20142014, P. 1-8.