LUCY allows you to create file that can be stored on removable media devices (CD, USB, DVD, SD Card etc.). The most popular is an attack using USB sticks. But keep in mind that this template works for all other variations of removable media types as well.

Background Info

At the moment, there are three popular methods that malicious applications use to infect USB flash drives:

Simple file copy method: With this method, a malicious application that is installed on an infected computer simply makes copies of itself to all storage devices that are attached to the infected computer. With this method, a malicious file is often named with a sensational filename to lure a victim into launching the file and causing malicious code to be executed. Quite often there are familiar file icons such as Microsoft Windows icons for videos and images that are used to trick unsuspecting victims into thinking that an executable file is a harmless image or video. This infection method requires that the victim manually execute the malicious file from their computer to become infected.

AutoRun.inf modification method: Microsoft Windows and some other operating systems have a functionality that is called “AutoRun” (sometimes also referred to as Autoplay). AutoRun functionality is basically designed to perform some actions that are automatically executed when removable media is inserted or removed from a computer. On Microsoft Windows platforms, “autorun.inf” is the file that contains instructions for the AutoRun functionality. The autorun.inf file can instruct AutoRun to use a certain type of icon; add menu commands; and among other things, start an executable. With this infection method, the malicious application modifies or creates an autorun.inf file on all of the network shares, local drives, and removable media (including USB flash drives) that are connected to the computer. When an infected USB flash drive is inserted into another computer, the copy of the malicious application is automatically executed. Under a default configuration of Windows, this infection method does not require any interaction from the victim other than physically attaching the media to the computer.

Reprogramming USB peripherals. To turn one device type into another, USB controller chips in peripherals need to be reprogrammed. Very widely spread USB controller chips, including those in thumb drives, have no protection from such reprogramming.

BadUSB – Turning devices evil: Once reprogrammed, benign devices can turn malicious in many ways, including:

- 1.A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.
- 2.The device can also spoof a network card and change the computer’s DNS setting to redirect traffic.
- 3.A modified thumb drive or external hard disk can – when it detects that the computer is starting up – boot a small virus, which infects the computer’s operating system prior to boot.

Our Approach

With LUCY we provide a template for the "Simple file copy method". As mentioned before this

infection method requires that the victim manually execute the malicious file from their computer to become infected. So you have to lure a victim into launching the file and causing malicious code to be executed (e.g. just copy the file with an interesting file name on an USB stick and place them in spots where they will be picked up by other users).

Setup

In order to create an USB scenario go through the following steps:

- Start a new campaign and add a scenario called "USB attack. If you don't have this scenario among your templates then please download it using the "download" button in the template section.

- Give the scenario a name and pick a domain or IP address (this is the domain or IP which is used upon execution: the malware simulation will send the data back to this host)

- Next configure the USB template. This template defines what malware simulation should be running upon execution of the file on the USB drive. Make sure you have the latest malware simulations installed in LUCY. You can download the malware simulations using the "download" button in the template section.

- Now its time to create the USB recipients. Go to "recipients", create a new group and make sure you select "USB attack". Then define how many USB sticks you plane to use.

- In the last step you need to add the recipients to the campaign and go back into the base settings of your scenario and download the according malware simulations. Once you started the campaign LUCY will wait for incoming requests from executed files.

Important Questions

- Does it need admin rights to execute the files? No - to execute the malware simulations it does not need admin rights. The standard windows user rights will do.
- Can I only place an executable on the USB? No - you can place any type of malware simulation on the USB (.exe, doc with Macro, archived format etc.)
- How can I get the users to execute the file? You could use simple social engineering techniques and just place some sticks in a public area, rename the executable to something like "decrypt_accounts.exe" (if you choose for example the malware simulation with the screenshot & webcam tool it will show you some fake decryption GUI upon execution)
- How do I know if users executed the files? The moment the files get executed and the user has internet access the data will be transferred back to LUCY using the build in browser.
- Will the tool get detected by an AV? No - this should not happen (please let us know if this occurs)
- Will the tool be able to bypass USB filters or windows security settings (like UAC)? No - if you don't allow files from an USB drive to be executed this won't work.