# Background Info

About Java Applets: Java applets are executed in a sandbox by most web browsers, preventing them from accessing local data like the clipboard or file system. If the code rquires those rights, the user has to allow it (manually by clicking "run"). The code of the applet is downloaded from a web server, after which the browser either embeds the applet into a web page or opens a new window showing the applet's user interface.

About Java Exploits: Java exploits represent a common attack vector used by the bad guys to infiltrate vulnerable computers via the web browser. The default security level for Java applets and web start applications has been increased from "Medium" to "High". This affects the conditions under which Java web applications can run. Previously, as long as you had the latest secure Java release installed applets and web start applications would continue to run as always. With the "High" setting the user is always warned before any unsigned application is run to prevent silent exploitation. This security enhancement eliminates the risk of silent exploitation using drive-by attacks via unsigned applets, which were possible before Java 7 update 11. This leaves attackers with no choice but to use social engineering techniques to convince users to click the Run button on the security warning dialog.

Signed Applet

LUCY uses a signed Java Applet with its own company name. This is what users will see when they open a page that has an Applet Dropper activated:
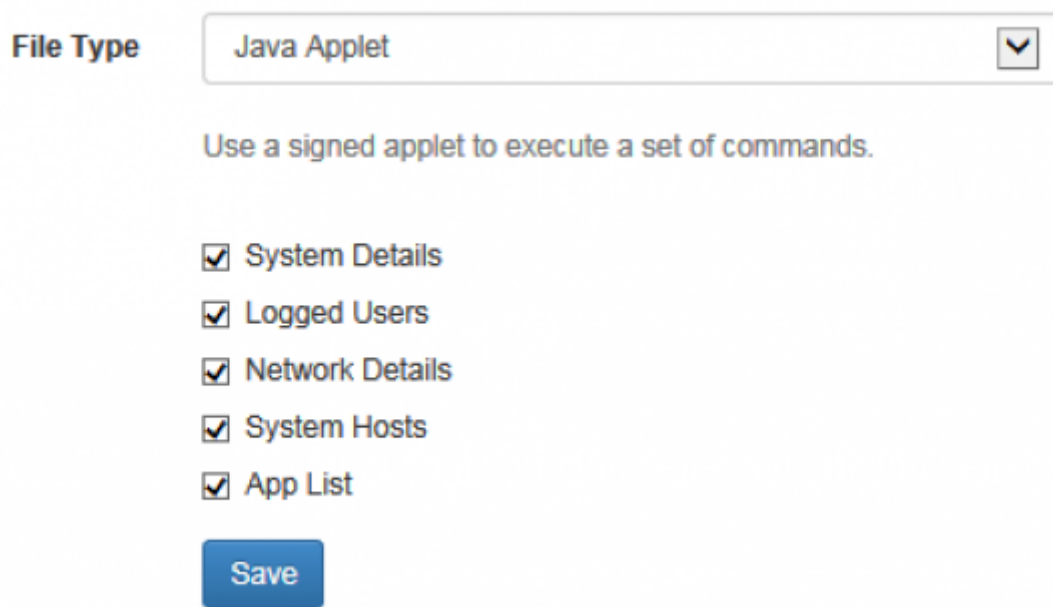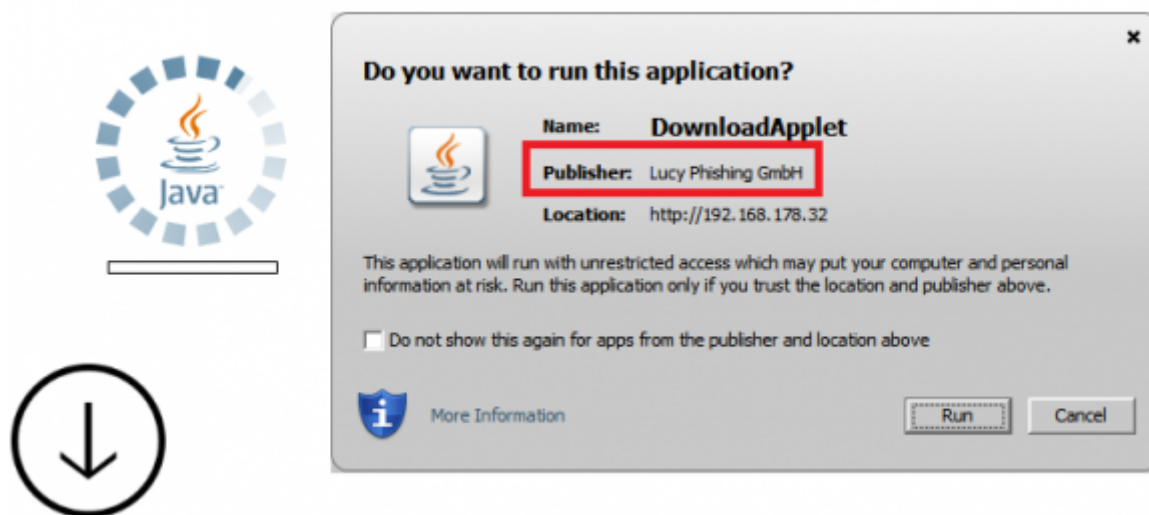

Types of Applets available in LUCY

Starting with 3.3 there are two types of applets available:

- a) **Two Stage Dropper :**: Our applet just acts as a dropper. A dropper is usually a program that has been designed to "install/run/load" some sort of malware (virus, backdoor, etc.) to a target system. The malware code can be contained within the dropper (single-stage) in such a

way as to avoid detection by virus scanners or the dropper may download the malware to the target machine once activated (two stage). In our case we use a two stage dropper: once activated, the applet will load the selected malware simulation from the LUCY campaign page (e.g. consolepost) and place it in the desired directory. Once it has been copied into that directory, the applet executes the file automatically and reports back to LUCY.

- b) **Java "Exploiter"**: The JavaExploiter is a signed applet that will execute one or multiple commands and report back to LUCY:

File Type   Java Applet

Use a signed applet to execute a set of commands.

☑ System Details
☑ Logged Users
☑ Network Details
☑ System Hosts
☑ App List

Save

Configuration

- **Step 1 - choose a file based template or a mixed template**: In order to use the Java Applet Dropper or Exploiter you should pick a file based or mixed scenario type (if you choose a mixed scenario the applet will only be placed automatically on the second page like account.html; it won't work in a mixed scenario with just one webpage). This allows you to download and run any code that is compiled on LUCY using the Java Dropper. Please use the file based attack tutorial to create your campaign.

- **Step 2 -Select the appropriate file type** within the scenario settings. "Tunnel Executable" is the java dropper and "java applet" is the applet that gathers system information:

- **Step 3 - Fine-tune the settings**: If you get to the scenario settings page please choose as a compression type "Java Applet":

In case you picked the java dropper, please make sure you pick a path where the browser is allowed to write & execute files (like /temp folder):

In case you selected the java dropper, you still need to select the malware simulation that should be loaded & executed when the applet on landing page template is activated.

- **Step 4 - Test your scenario:**: If everything is configured correctly, the user who opens the link to the landing page should now see a popup that will ask him to run an applet. If he accepts to run the applet, the selected malware simulation is loaded into the specified directory and executed OR the system commands are getting executed (depening on which applet you picked in Step 2):

Restrictions

- The applet requires the browser to have the java plugin installed and activated
- Only executables can be transmitted from LUCY to the client (no word files)
- The applet can only run on file based & mixed template types (if mixed: it will only run on the second page like account.html)

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=create_a_phishing_campaign_with_a_java_dropper_applet

Last update: **2019/07/25 12:49**