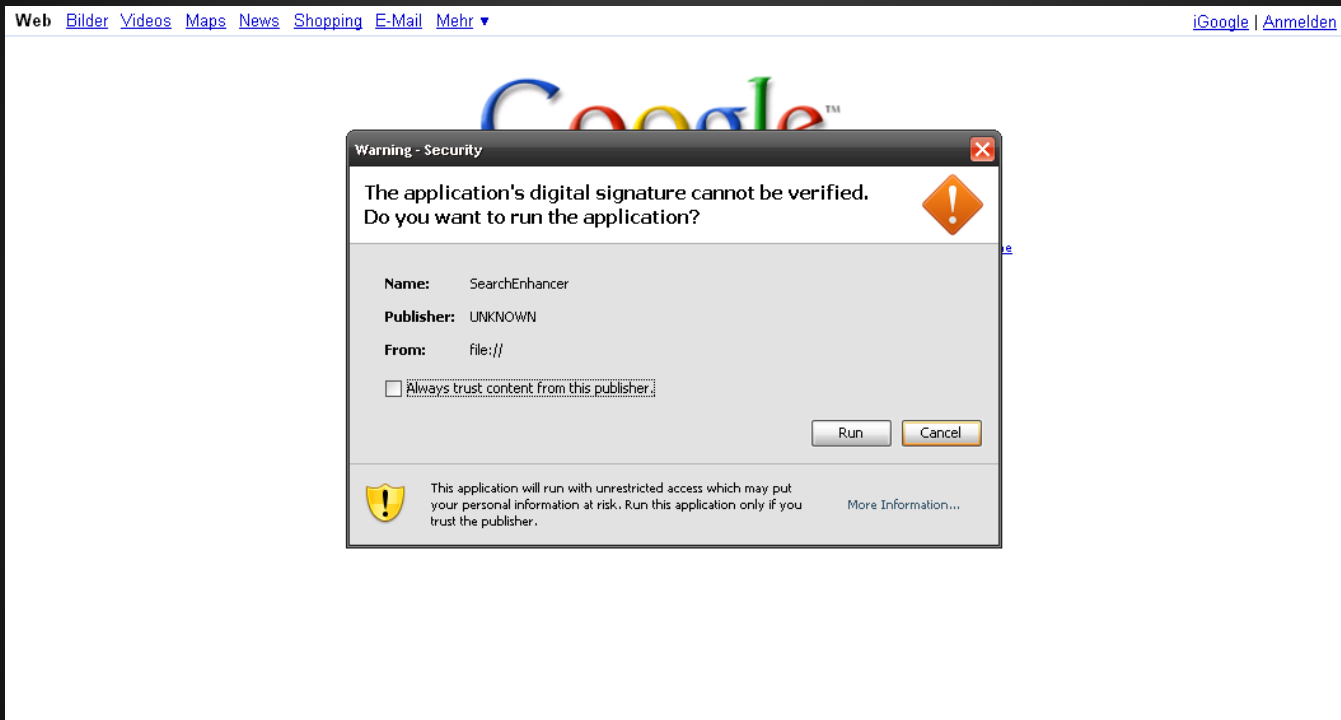


# FinFisher Dummy Infection Examples

# Summary

Within the FinFisher leak is an interesting folder labeled "ffw". The directory contains "Dummy Infection" pages that the Gamma group created to show how their backdoor can get installed on victims machines. The examples do not rely on exploitation but social engineering. These slides were created to show how attackers use social engineering to install software without sending an executable in a zip. Some tips were added to prevent infections for users.

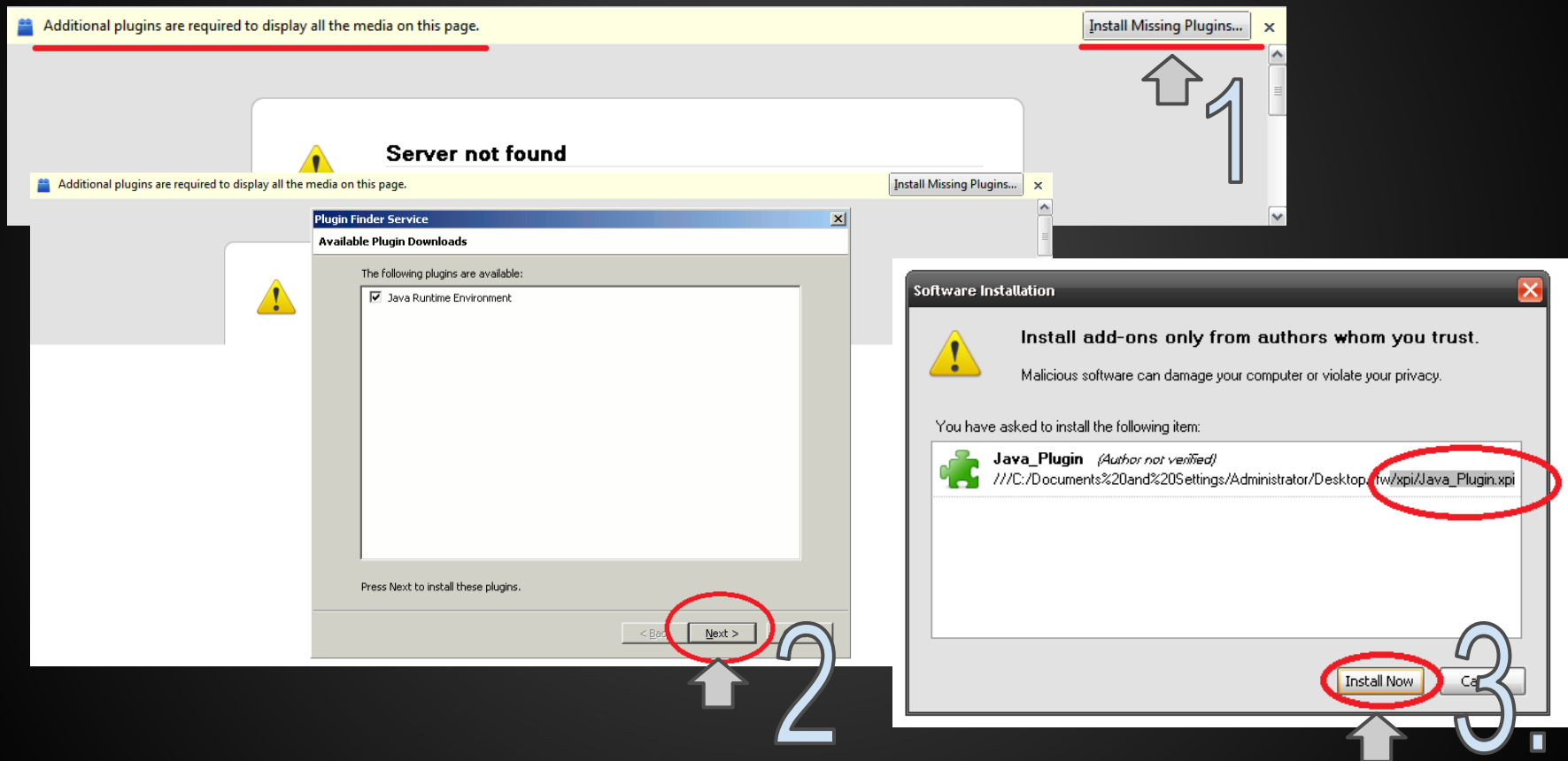
# Google with Java Prompt



# Tip

- Do not trust brand recognition when prompted to install, run software or give credentials.
- Do not run applications when prompted from websites. Always press Cancel or No.
- It is best to have Java disabled by default and only enable it if needed. [LINK](#).
- If the link was sent to you in an email it would be best to be cautious with any other links from that individual.

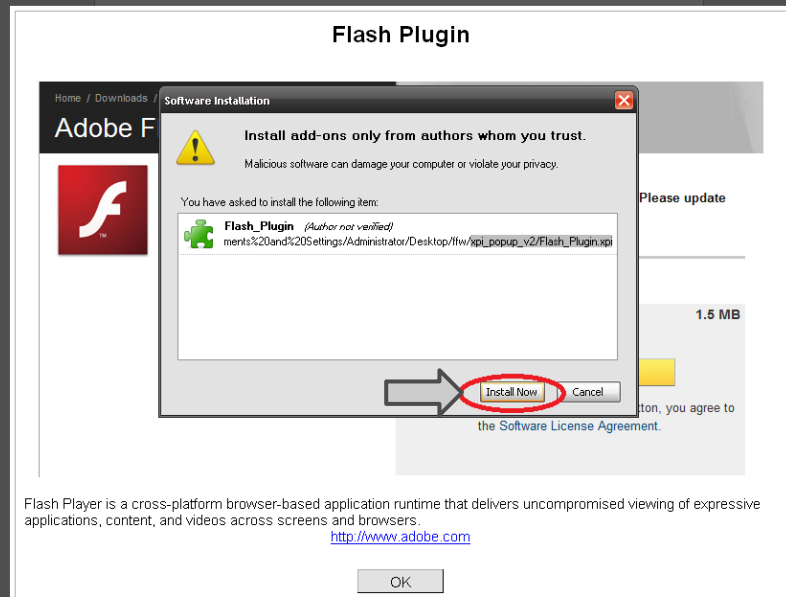
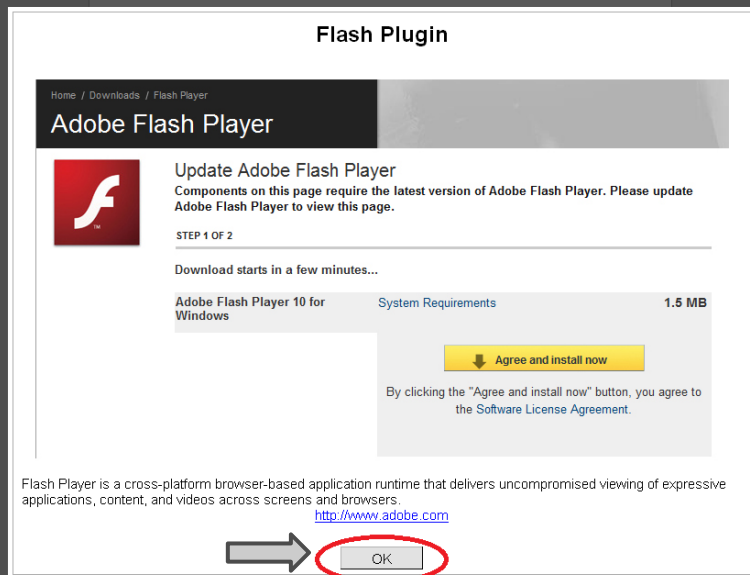
# XPI Plugin/Add-on



# Tips

- Do not install Missing Plugins from websites when prompted.
- The average user will only install new plugins when they first install Firefox.
- Plugins can be downloaded from Mozilla Add-Ons store.
- If the plugin is not present in the Add-On store and does not have reviews it is safe to assume the plugin is not needed.

# XPI Popup/Add-on



# IFrame Injection

The image is a composite of three overlapping browser window screenshots to demonstrate an IFrame injection attack.

- Top Screenshot:** A "Server not found" error message from Firefox, stating "Firefox can't find the server at www.comodo.com." It includes a warning icon and a suggestion to check the address for typing errors.
- Bottom-Left Screenshot:** The Adobe Flash Player update page. It features the Adobe logo, the heading "Update Adobe Flash Player", and a message: "Components on this page require the latest version of Adobe Flash Player. Please update Adobe Flash Player to view this page." Below this, it says "STEP 1 OF 2" and "Download starts in a few minutes...". There are links for "Adobe Flash Player 10 for Windows" and "System Requirements". A large yellow button labeled "Agree and install now" is prominent, with a grey arrow pointing to it from the text below.
- Bottom-Right Screenshot:** A Windows file installer dialog box titled "Opening flash-player-installer.exe". It shows the file name "flash-player-installer.exe" (656 KB) and its location. The dialog asks "Would you like to save this file?" with "Save File" and "Cancel" buttons. In the background, the Adobe Flash Player update page is visible, showing the "Agree and install now" button and a "1.5 MB" download size.

By clicking the "Agree and install now" button, you agree to the [Software License Agreement](#).

*Note: This is probably the most interesting technique. I can't recall seeing IFrame injection combined with brand spoofing to install malware before.*



# Java Applet



# Dummy Infection Popup



Note: The logs in `finfisher\www\GGI\Support\Attachments\A169FE42.rar` is an interesting read.