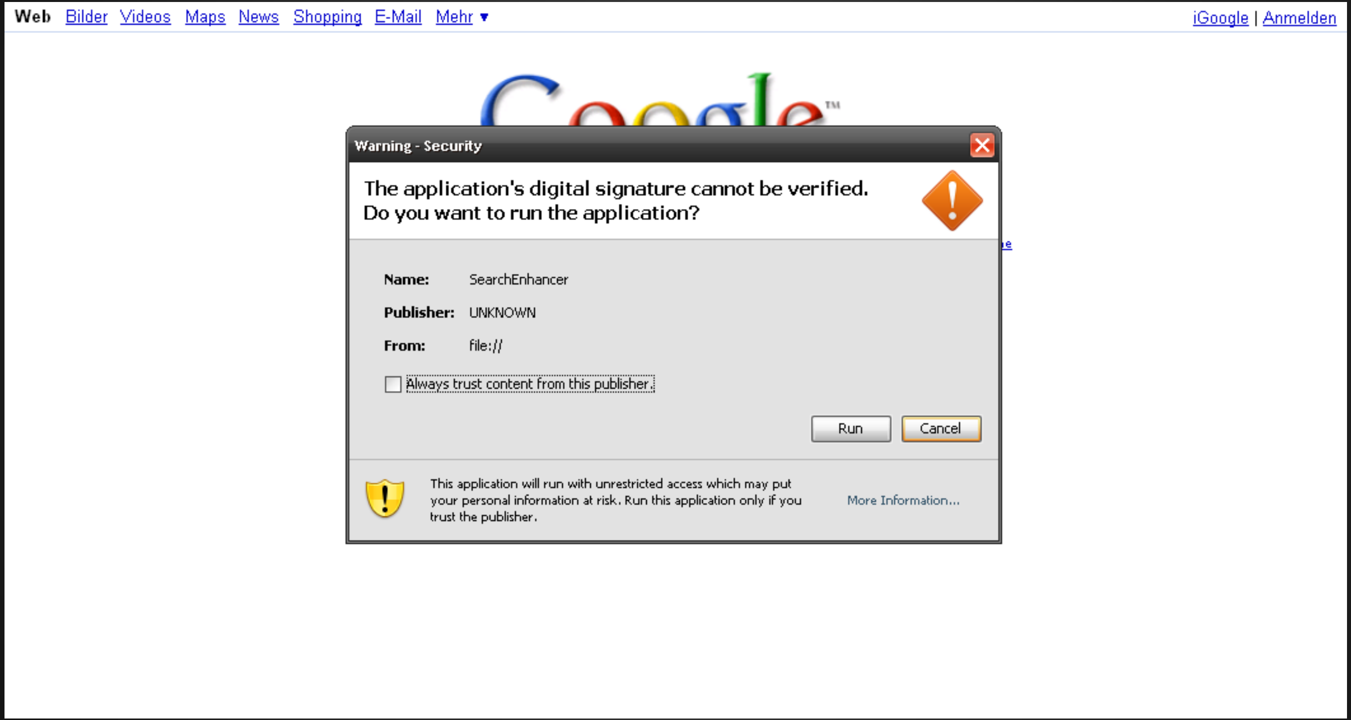
FinFisher Dummy Infection Examples

Created by Alexander Hanel

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



The application's digital signature cannot be verified.
Do you want to run the application?

Name: SearchEnhancer

Publisher: UNKNOWN

From: file://

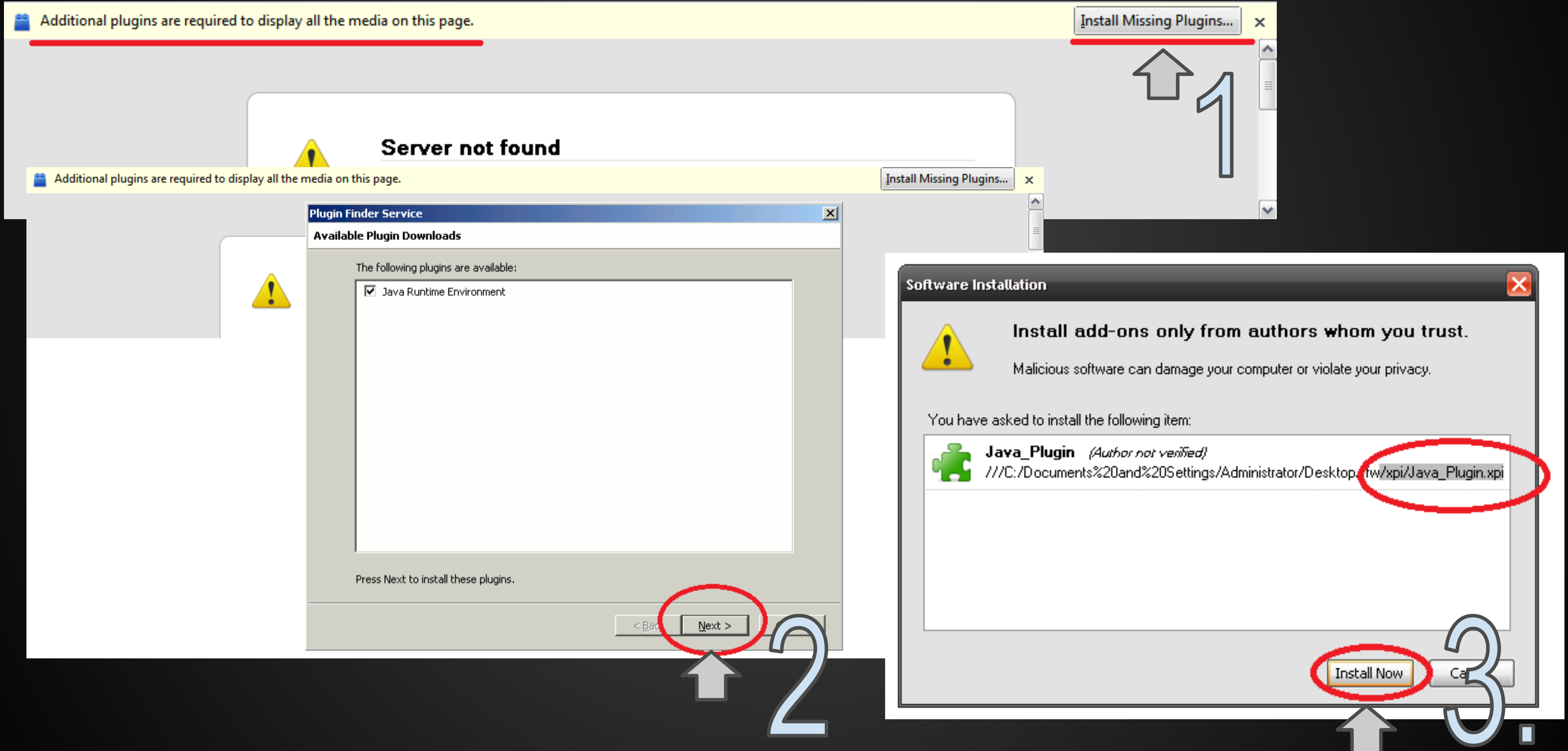
□ Always trust content from this publisher.

This application will run with unrestricted access which may put your personal information at risk. Run this application only if you trust the publisher.

Tips

- 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/Addon



Additional plugins are required to display all the media on this page.

Server not found

Additional plugins are required to display all the media on this page.

Plugin Finder Service

Available Plugin Downloads

The following plugins are available:

☑ Java Runtime Environment

Press Next to install these plugins.

Software Installation

Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

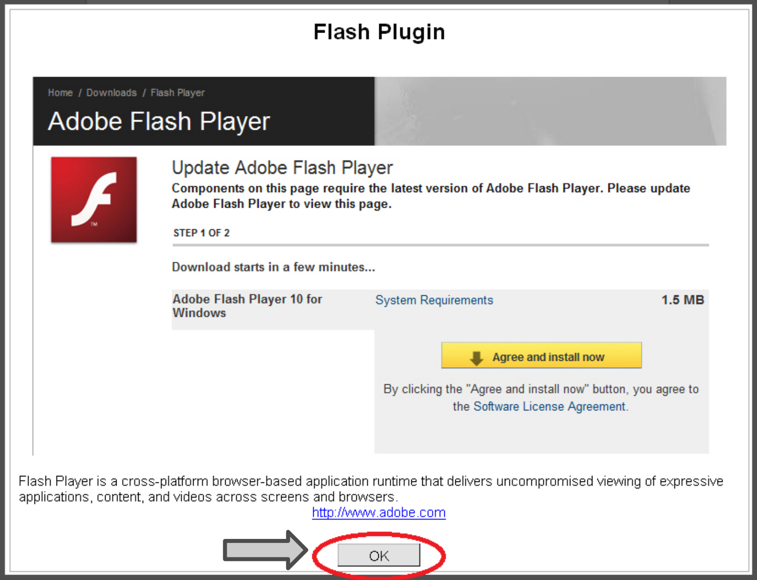
You have asked to install the following item:

Java_Plugin *(Author not verified)*
///C:/Documents%20and%20Settings/Administrator/Desktop/fw/xpi/Java_Plugin.xpi

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/Addon



Flash Plugin

Home / Downloads / Flash Player

Adobe Flash Player

Update Adobe Flash Player

Components on this page require the latest version of Adobe Flash Player. Please update Adobe Flash Player to view this page.

STEP 1 OF 2

Download starts in a few minutes...

Adobe Flash Player 10 for Windows	System Requirements	1.5 MB

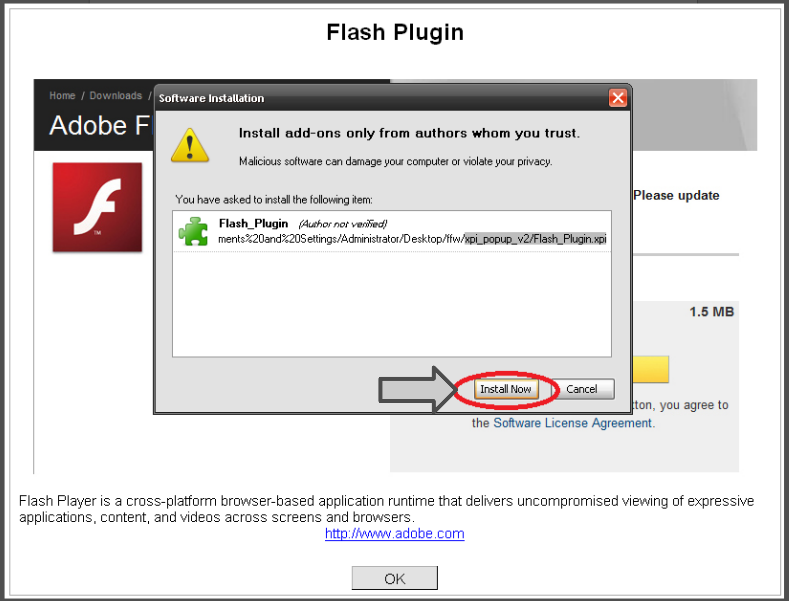
Agree and install now

By clicking the "Agree and install now" button, you agree to the Software License Agreement.

Flash Player is a cross-platform browser-based application runtime that delivers uncompromised viewing of expressive applications, content, and videos across screens and browsers.

http://www.adobe.com

OK



Flash Plugin

Home / Downloads /

Adobe F

Software Installation

Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Flash_Plugin *(Author not verified)*
ments%20and%20Settings/Administrator/Desktop/ffw/xpi_popup_v2/Flash_Plugin.xpi

Install Now Cancel

Please update

1.5 MB

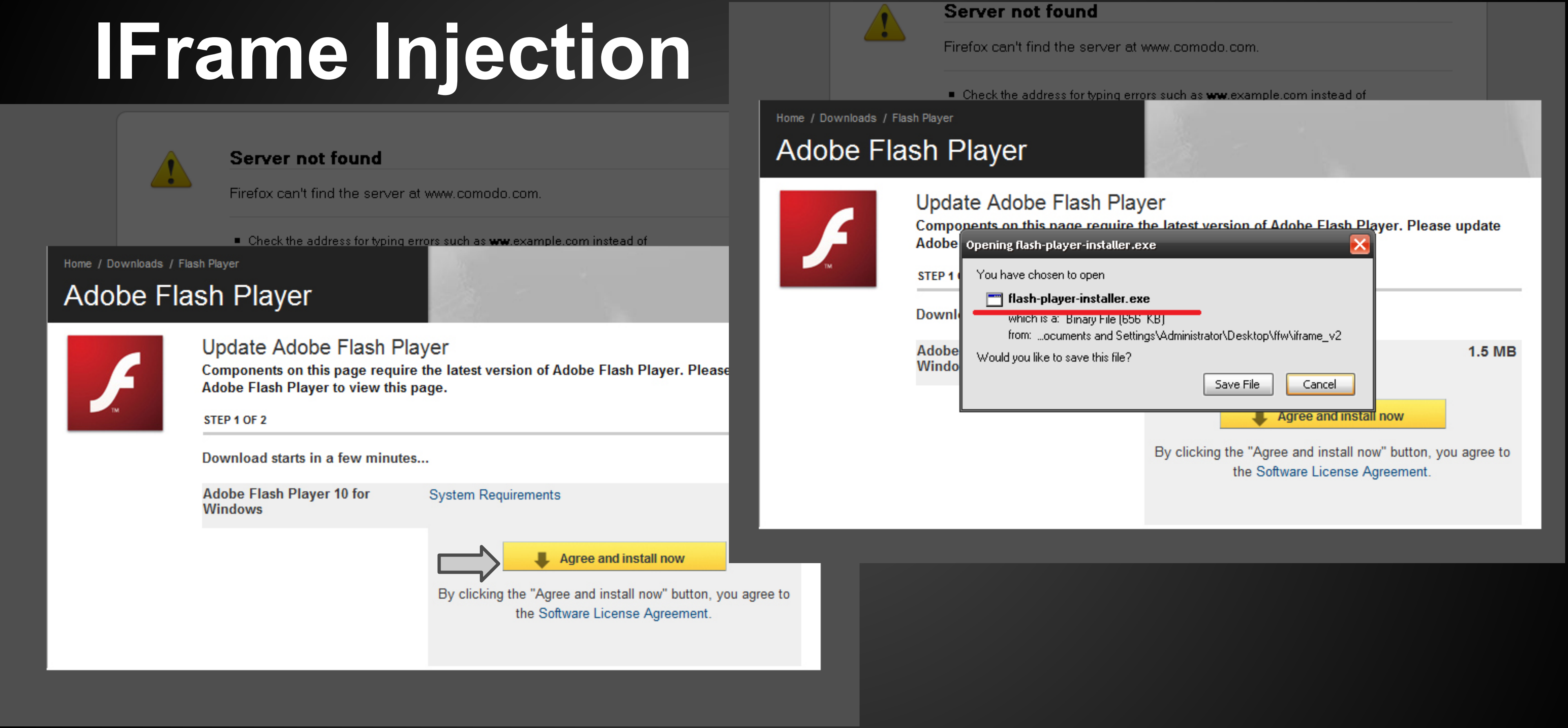
ton, you agree to the Software License Agreement.

Flash Player is a cross-platform browser-based application runtime that delivers uncompromised viewing of expressive applications, content, and videos across screens and browsers.

http://www.adobe.com

OK

IFrame Injection



Server not found

Firefox can't find the server at www.comodo.com.

- Check the address for typing errors such as **ww**.example.com instead of

Home / Downloads / Flash Player

Adobe Flash Player

Update Adobe Flash Player

Components on this page require the latest version of Adobe Flash Player. Please Adobe Flash Player to view this page.

STEP 1 OF 2

Download starts in a few minutes...

Adobe Flash Player 10 for Windows

System Requirements

By clicking the "Agree and install now" button, you agree to the Software License Agreement.

Server not found

Firefox can't find the server at www.comodo.com.

- Check the address for typing errors such as **ww**.example.com instead of

Home / Downloads / Flash Player

Adobe Flash Player

Update Adobe Flash Player

Components on this page require the latest version of Adobe Flash Player. Please update Adobe

STEP 1

Downl

Adobe Windo

1.5 MB

Opening flash-player-installer.exe

You have chosen to open

flash-player-installer.exe

which is a: Binary File (656 KB)

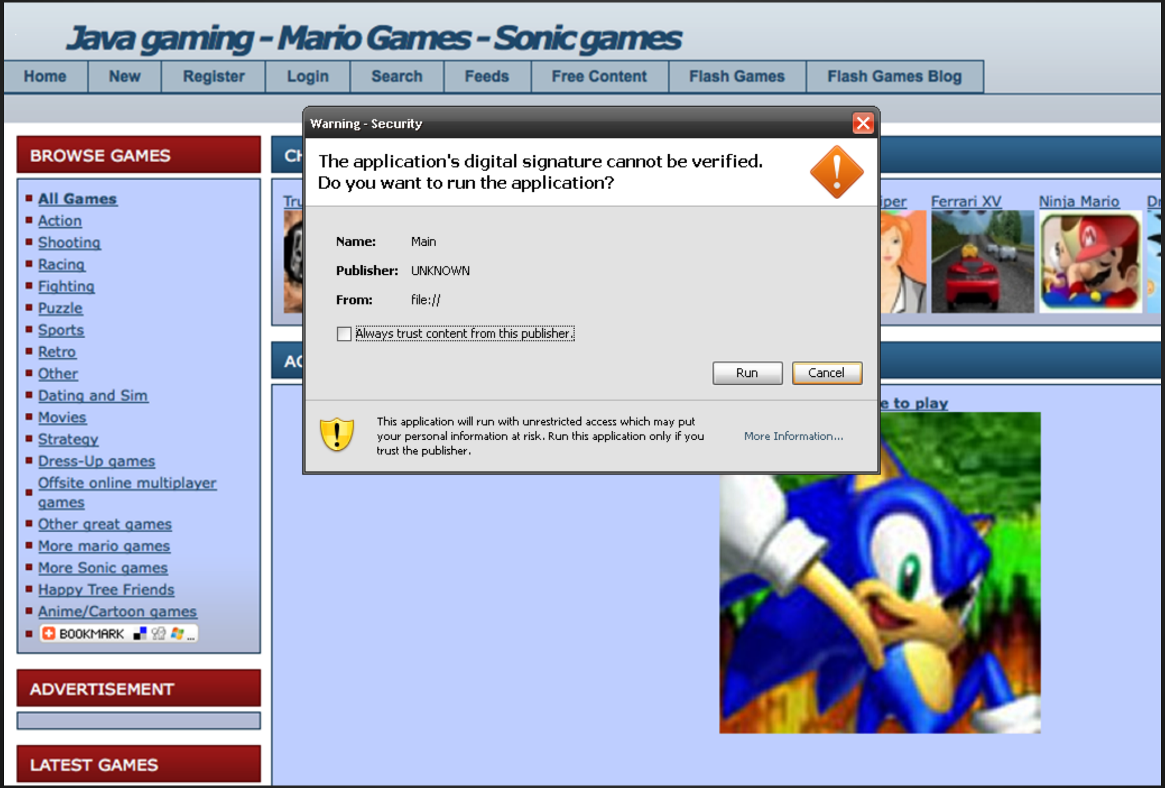
from: ...ocuments and Settings\Administrator\Desktop\ffw\iframe_v2

Would you like to save this file?

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



Warning - Security

The application's digital signature cannot be verified.
Do you want to run the application?

Name: Main

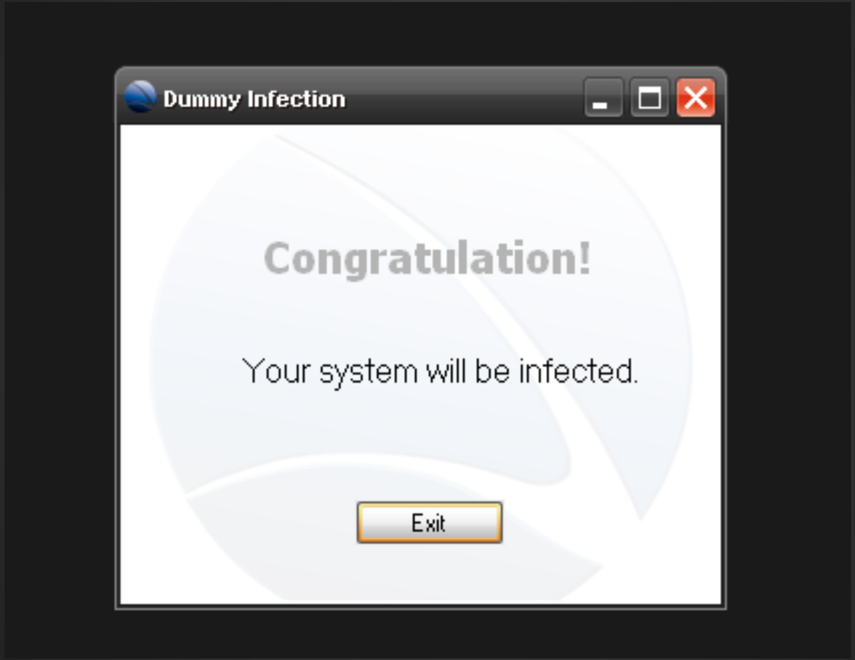
Publisher: UNKNOWN

From: file://

□ Always trust content from this publisher.

This application will run with unrestricted access which may put your personal information at risk. Run this application only if you trust the publisher.

Dummy Infection Popup



Congratulation!

Your system will be infected.

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