

One of the major challenges in using a Remote Monitoring Solution is to install it onto the Target System, especially when only a little information, like an **Email-address**, is available and **no physical access** can be achieved.

FinFly Web is designed to provide **remote and covert** infection of a Target System by using a wide range of **web-based attacks**.

FinFly Web provides a **point-and-click interface**, enabling the Agent to easily **create a custom infection code** according to selected modules.

Target Systems visiting a prepared website with the implemented infection code will be **covertly infected** with the configured software.

Usage Example 1: Technical Surveillance Unit

After profiling a Target, the unit created a **website of interest** for the Target and sent him the **link through a discussion board**. Upon opening the Link to the unit's website, a Remote Monitoring Solution was installed on the Target System and the Target was **monitored from within Headquarters**.

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through Websites
Content:	· Software

Usage Example 2: Intelligence Agency

The customer deployed **FinFly ISP within the main Internet Service Provider** of their country. It was **combined with FinFly Web** to remotely **infect Targets that visited government offensive websites** by covertly injecting the FinFly Web code into the targeted websites.

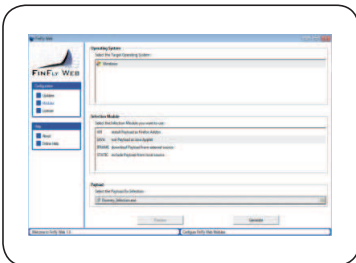
Feature Overview

- **Fully-Customizable** Web Modules
- Can be covertly **installed into every Website**
- Full integration with **FinFly LAN** and **FinFly ISP** to deploy even inside popular Websites like Webmail, Video Portals and more
- Installs Remote Monitoring Solution **even if only email address is known**
- Possibility to target every person visiting **configured Websites**

For a full feature list please refer to the Product Specifications.



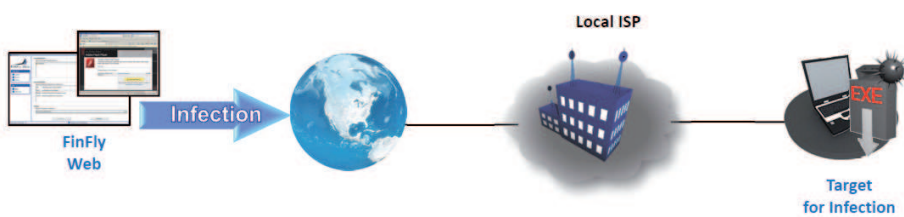
Product Components



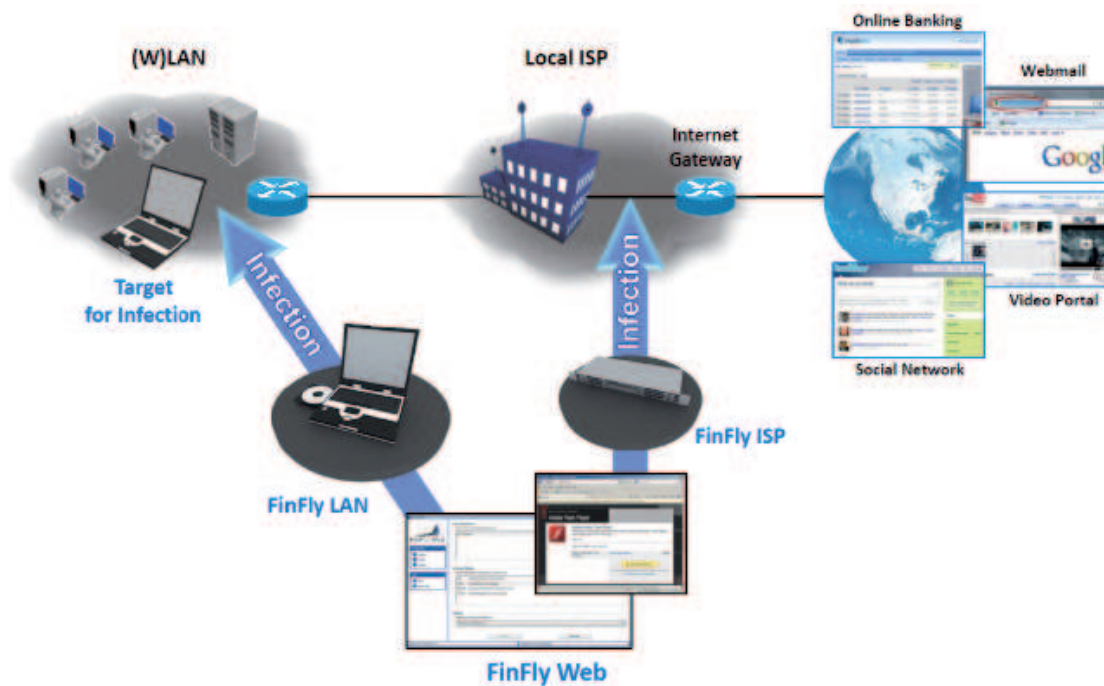
FinFly Web

- Point-and-click software to create custom infection Websites

FinFly Web direct infection

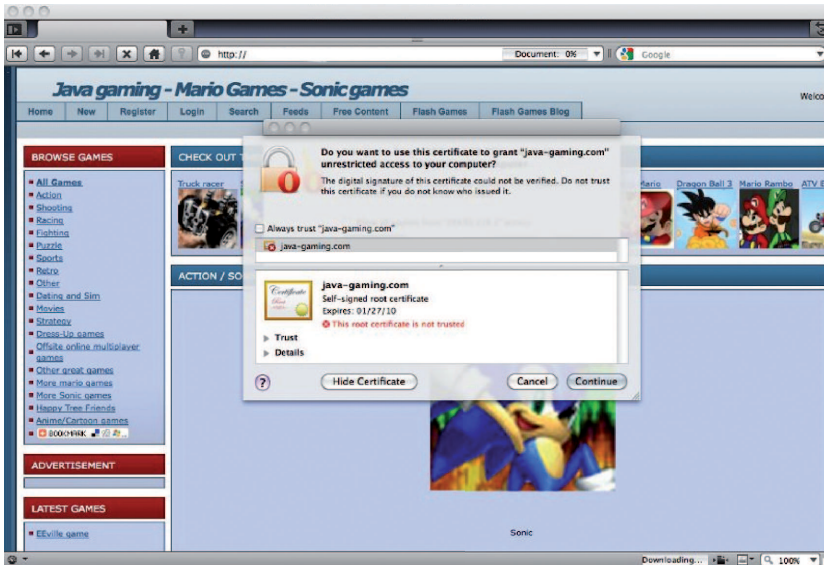


Full integration with FinFly LAN and FinFly ISP



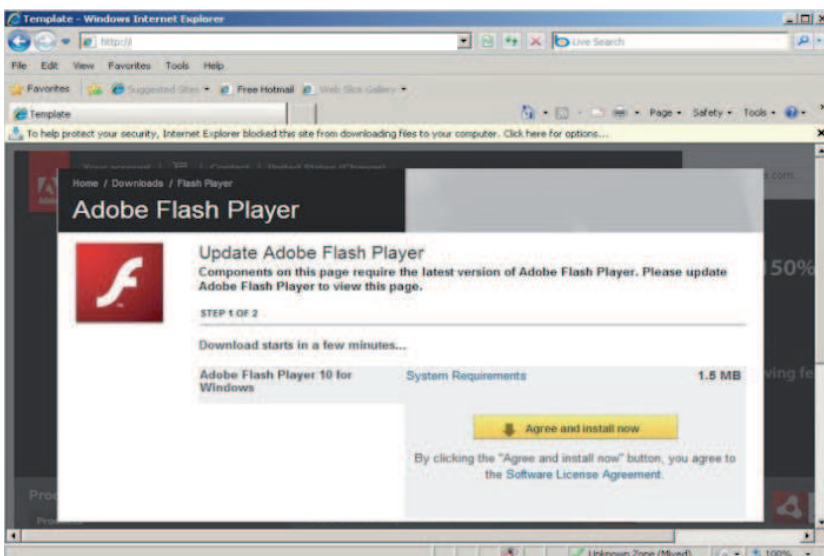
Example: Java Applet (Internet Explorer, Firefox, Opera, Safari)

The website will prompt the Target to accept a Java plug-in that can be signed with any company name (e.g. "Microsoft Corporation")



Example: Missing Component (IE, Firefox, Opera, Safari)

The website will pretend that a plug-in/codec etc. is missing on the Target System and prompt it to download and install this software



Example: Missing XPI (Firefox only, all platforms)

This module will prompt the Target to install additional plug-ins in order to be able to view the website.

