FINFLY EXPLOIT PORTAL

Standard Deployment methods for Remote Monitoring Solutions can **often not be applied** when dealing **with well-trained and extremely careful Targets** as they are familiar with common Deployment techniques and tools.

In most scenarios, **0-Day Exploits** provide an extremely powerful and **reliable way to deploy Remote Monitoring Solutions** by exploiting **unpatched vulnerabilities** in Software the Target is using.

The FinFly Exploit Portal offers access to **a large library** of 0-Day and 1-Day Exploits for popular software like **Microsoft® Office, Internet Explorer, Adobe Acrobat Reader, and many more**.

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through Files and Server
Content:	· Web Portal

Usage Example 1: High-Tech Crime Unit

A High-Tech Crime Unit was **investigating a Cyber-Crime** and needed to deploy a Remote Monitoring Solution on a Target System. They used an Adobe Acrobat Reader 0-Day Exploit and sent a prepared PDF file via Email to the Target. The Remote Monitoring Solution was automatically deployed once the Target opened the file.

Usage Example 2: Intelligence Agency

A Target was identified **within a Discussion Board** but no direct or Email contact was possible. The Agency created a Webserver containing an **Internet Explorer 0-day Exploit** which deployed the Payload on the Target System **once the Target opened the URL** that was sent to him through a private message in the Discussion Board.

Feature Overview

- Full Access to **Web Portal and Exploit Generator**
- **Government-Grade 0-Day Exploits** which function on multiple Systems and Patch-levels **without further modification**
- At least **4 major Exploits** (common Browser/Mail/File-Viewer Software) permanently available
- **30 day warranty** for every Exploit within the Portal
- Permanently updated **1-Day Exploits** for various Software

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

FINFLY EXPLOIT PORTAL

Product Components

FinFly Exploit Portal

- Web Interface Exploit Library

FinFly Exploit Portal Sample

Microsoft Internet Explorer 9-8-7-6 Remote Code Execution Exploit

A use-after-free vulnerability exists in Microsoft Internet Explorer when processing certain JavaScript and HTML data, which could be exploited to compromise a vulnerable system via a specially crafted web page.

The vulnerability affects Microsoft Internet Explorer 9, 8, 7 and 6, on Windows 7 SP1 and prior, Windows Vista SP2 and prior, and Windows XP SP3 and prior.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

• More Information and Details *(Exploit updated on 2011-10-14. Exploit first released on 2011-08-06)*

Microsoft Internet Explorer 9-8 Remote Sandbox Bypass Exploit

A vulnerability exists in Microsoft Internet Explorer's sandbox (Protected Mode) when processin certain data from a Low integrity process, which could be exploited to achieve code execution a Medium integrity and bypass Protected Mode.

The vulnerability affects Microsoft Internet Explorer 9 and 8 on Windows 7 SP1 and prior and Windows Vista SP2 and prior (Windows XP SP3 and prior do not include a sandbox).

The provided exploit must be combined to another IE code and must be used as a second stage shellcode.

• More Information and Details *(Exploit updated on 2011-10-14. Exploit first released on 2011-03-02)*

Adobe Acrobat & Reader 9.x PDF Processing Code Execution Exploit

A buffer overflow vulnerability exists in Adobe Acrobat and Reader when processing certain data within a PDF document, which could be exploited to compromise a vulnerable system by tricking a user into opening a malicious PDF file.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

• More Information and Details *(Exploit updated on 2011-09-02. Exploit first released on 2011-07-15)*

WWW.FINFISHER.COM

The information contained herein is confidential and subject to change without notice. Gamma Group International shall not be liable for technical or editorial errors or omissions contained herein.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422