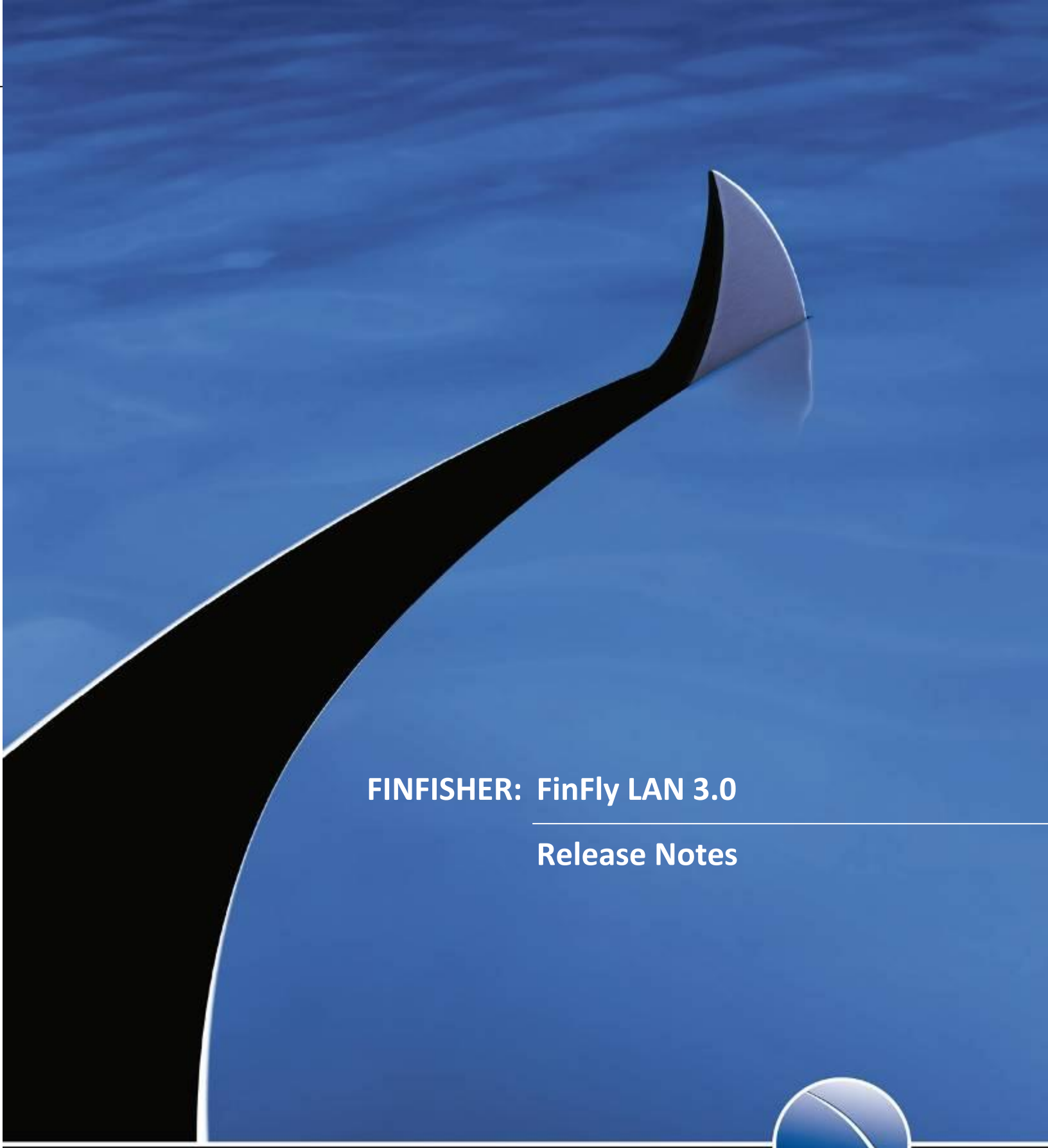


# FINFISHER: FinFly LAN 3.0

## Release Notes

FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM

Date 2010-06-29

**Release information**

| Version | Date | Author | Remarks |
|---|---|---|---|
| 1.0 | 2010-06-29 | ht | Initial version |
| 1.1 | 2011-06-28 | am | V3.0 release notes |
| | | | |

**Table of Content**

1 Overview ..... 4

2 ChangeLog ..... 5

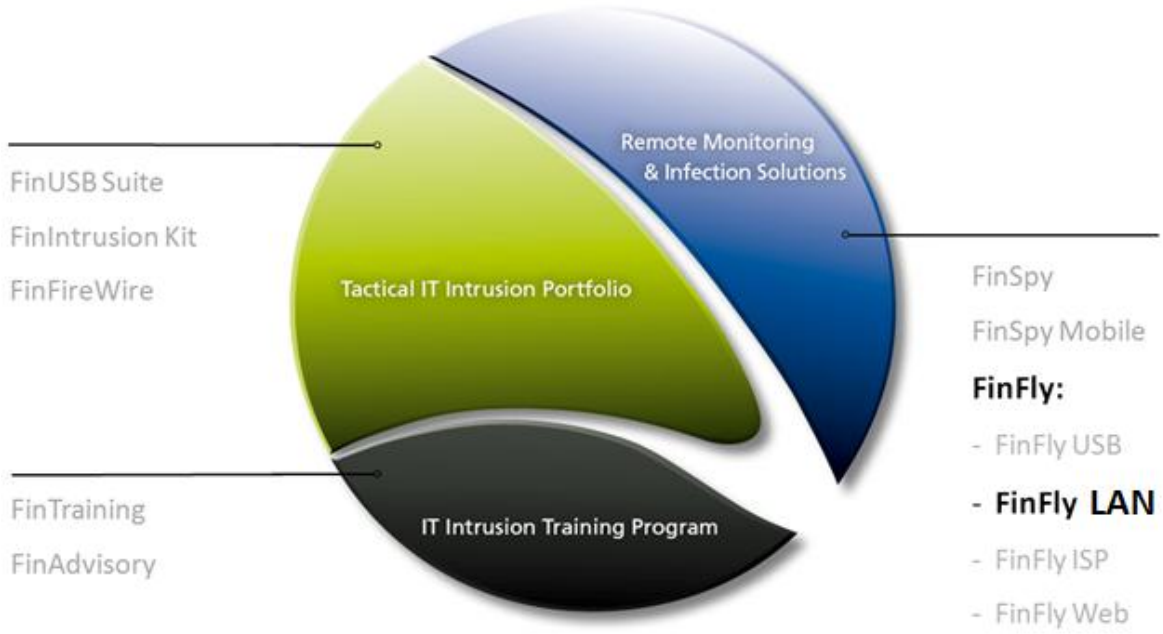
3 Limitations ..... 6

# 1 OVERVIEW

*FinFly LAN* is designed to help Law Enforcement and Intelligence Agencies to covertly install Remote Monitoring software onto Target Systems through Local Area Networks (Wired and Wireless).

The *FinFly LAN* Infection Proxy is able to automatically detect all Systems that are connected to the same logical subnet of the Local Area Network.

Using various configurable techniques, it deploys Software onto selected Target Systems through modifications of Downloads and Injections of Software Updates.



## 2 CHANGELOG

| Version: 3.0 | | |
|---|---|---|
| **Component** | **Change** | **Description** |
| **Generic** | New GUI | GUI rewrite in .NET for better usability |
| | Functionality Verification | Auto-Detect protected networks where operation is not functional |
| **Discovery** | Enhanced Display of Systems | Display MAC Address and OS of discovered systems |
| | Computer Names | Display Computer Names if possible (e.g. DHCP Requests, SMB, etc) |
| **Infection Techniques** | Multi-OS Support | Support for Mac OSX Infection |
| | Client-Software-Update | Support for more client software update infection (e.g. in research: Skype, Adobe Acrobat) |
| | Emulator Templates | Emulators can be created/modified by advanced end-users to create support for more infection techniques |
| | URL Injection | Remote URLs can be added into visited Websites to infect through Browser Plugins (e.g. using FinFly Web) |

# 3 LIMITATIONS

This chapter covers current known limitations within the FinFly LAN Software.

| Feature | Description |
|---|---|
| **SSL/TLS encrypted Traffic** | Encrypted sessions cannot be monitored and no infections can be done inside SSL/TLS encrypted connections. |
| **Compressed Files** | As the software infects downloaded files on-the-fly, it is not possible to infect files that are compressed (e.g. ZIP archives). |
| **IPv6** | IPv6 networks are currently not supported. |
| **Security Tools** | Even though permanent tests are conducted within our Quality Assurance cycles, it cannot be guaranteed that the injected Application Loader does not trigger alerts.<br><br>Also it cannot be guaranteed, that the ARP cache poisoning attack bypasses all network security tools which could detect a change of Gateway. |
| **Target Infection** | Even though a downloaded File has been infected, the actual infection of the Target System cannot be guaranteed as for example:<br><br>a) The Target never executes the file on the Target System<br><br>b) The configured Payload did not function on the Target System<br><br>Some specific exe files will be not infected by the infection proxy, but the vast majority will work as expected. |
| **Non HTTP traffic on port 80** | Some applications use the port 80 for non HTTP traffic. Targeting a System may cause these applications to malfunction and generate errors.<br><br>Therefore it cannot be guaranteed that only the target or the target at all is infected during the operation. |

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM