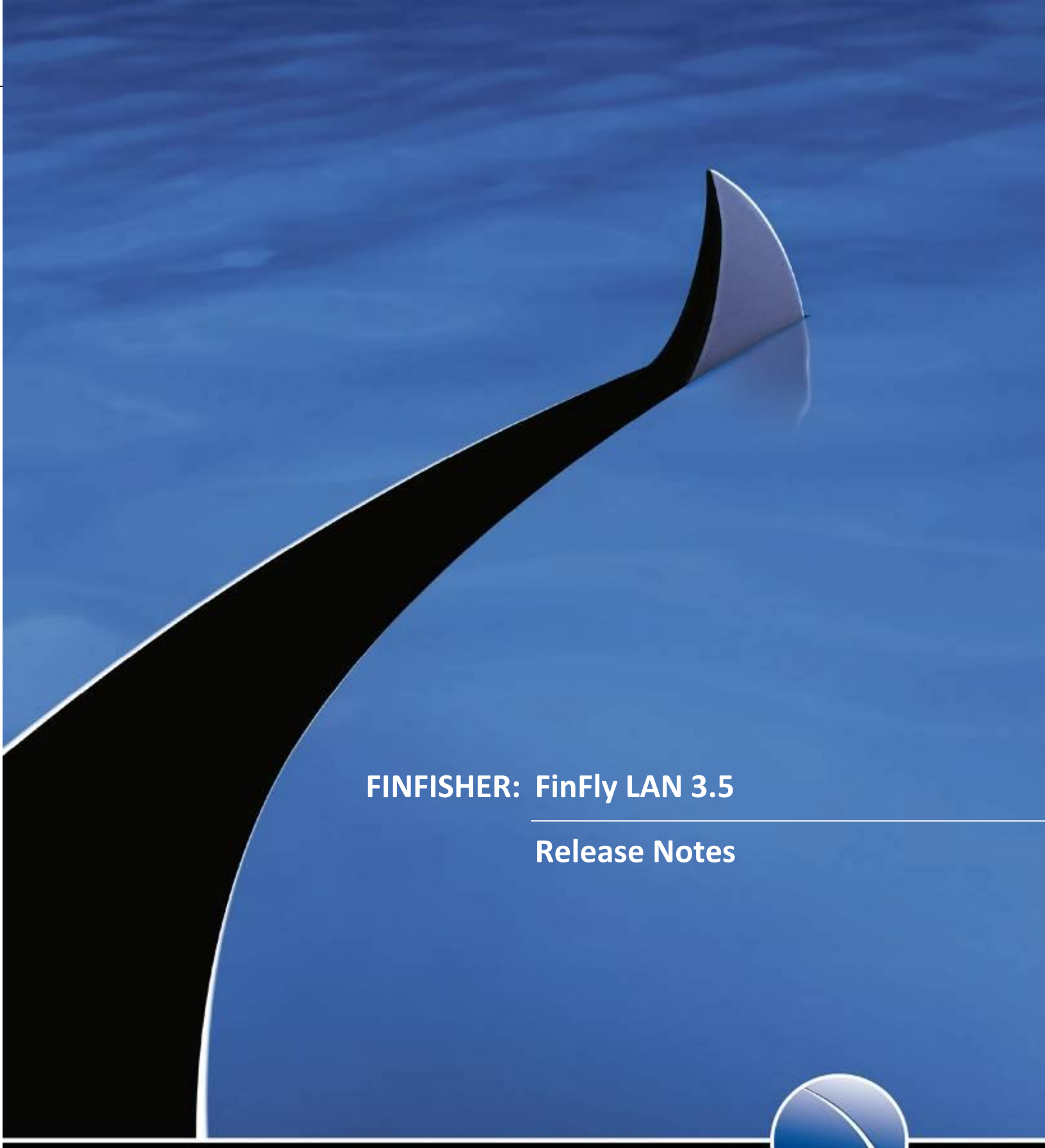


FINFISHER: FinFly LAN 3.5

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
1.2	2011-10-11	am	V3.2 release notes
1.3	2012-03-19	am	V3.5 release notes

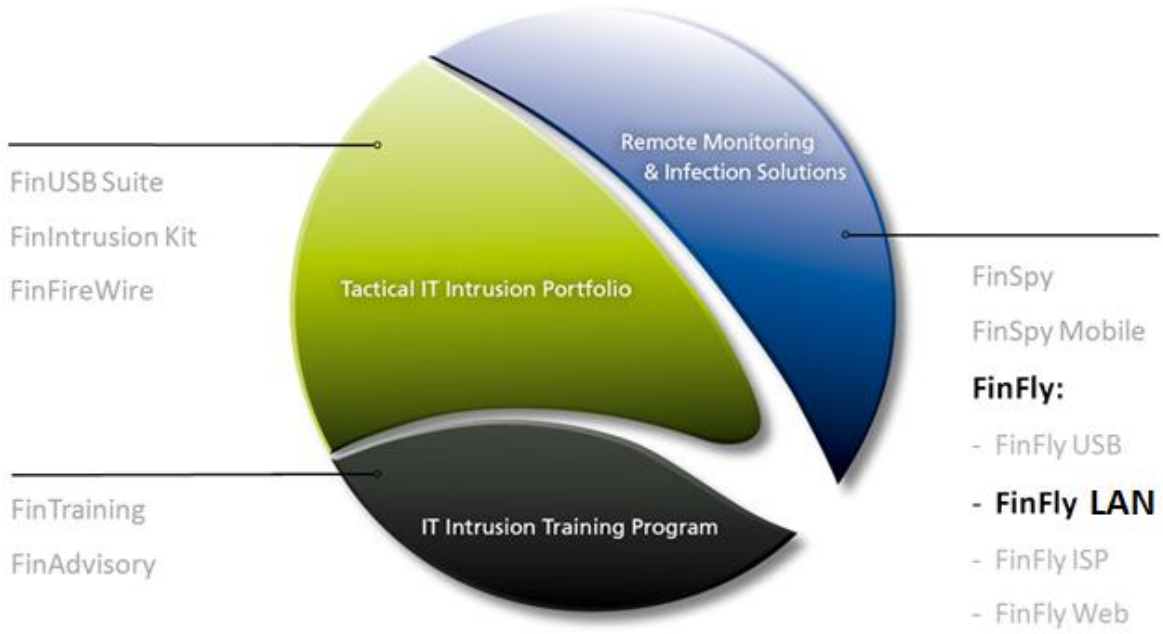
Table of Content

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: 3.5		
Component	**Change**	**Description**
Infection Techniques	Emulator Updates	Support for newer versions of CCleaner, Defraggler, Miranda, Notepad++, OpenOffice
Infection Techniques	Website Infection	Full compatibility to Finfly Web 2.0 payloads. Supports OS recognition.
Generic	Start network scanner on demand	The network scanner will be now started by pressing the 'Start' button in the GUI
	ARP cache restore	The ARP cache of a infected target will be now restored right after the payload was delivered.
	GUI payload selection	The payload selection was changed. Only one web payload can be selected.
	Select all/ Deselect all buttons	This two buttons improves the operability of the GUI

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. 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: a) The Target never executes the file on the Target System b) The configured Payload did not function on the Target System 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. Therefore it cannot be guaranteed that only the target or the target at all is infected during the operation.
MAC OSX Infection	For the MAC OS X Infection a dmg file has to be created with the included payload.

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM