

# Secret Manuals order: Emulating an access point

- 3 Install the agent on the target device with the selected methods.  
See "[List of installation vectors](#)" on page 138 .

## List of installation vectors

### Operating systems supported by agents

Operating systems supported by the various desktop and mobile devices are listed b

<i>Device</i>	<i>Operating System</i>
<b>Desktop</b>	<ul style="list-style-type: none"><li>• Windows</li><li>• OS X</li></ul>
<b>Mobile</b>	<ul style="list-style-type: none"><li>• Android</li><li>• BlackBerry</li><li>• Windows Mobile</li><li>• Symbian</li><li>• IOS</li></ul>

[The Intercept](#): „Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide – Hacking Team manuals, dated September 2013, provide step-by-step instructions for technicians, administrators, and analysts on how to infect a device and set up spying.“

„The spyware installer might lay in wait in a hotel, or a Starbucks, and gain access to your computer by ,emulating an access point‘ – in other words, pretending to be a free wifi hotspot to which the victim connected previously.“

Ich weiß ja nicht, aber wer ist denn so blöde, darauf hereinzufallen? Ich habe mir mal einige dieser Handbücher durchgesehen, vor allem das [rcs-9-technician-final.pdf](#) ist interessant. Auf keinen Fall kann die Spionage-software zum Erfolg kommen, wenn der Nutzer sich vernünftig verhält. Und bei Linux auch nicht. Wen wollen sie also ausspionieren? Klein Fritzchen?