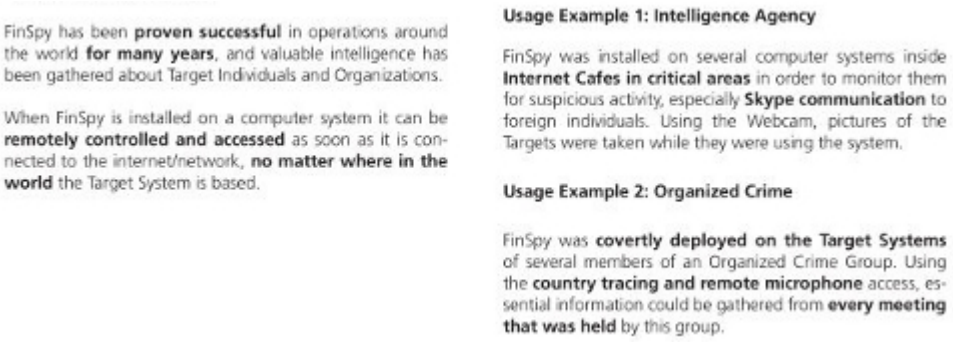
# FinSpy



FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

**Usage Example 1: Intelligence Agency**

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

**Usage Example 2: Organized Crime**

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Netzpolitik.org: „Seit ein paar Tagen werden auf dem Twitter-Account @GammaGroupPR interne Dokumente der Trojaner-Produktfamilie FinFisher/FinSpy aus dem Hause Gamma veröffentlicht.“

By the way: Es heisst „Trojanisches Pferd“ und *nicht* Trojaner“ – die Trojaner saßen eben *in Troja* und nicht im Pferd.

Jetzt schauen wir mal genau hin. (Die Links gehen zu den Werbe-pdfs der Firma Gamma International GmbH bzw. FinFisher.)

*Die Software-Suite umfasst unter anderem:*
*1. FinSpy: Eine Trojaner-Software, die Fernzugriff auf einen bereits infizierten Rechner ermöglicht. Diese läuft unter Windows, Mac OS X sowie Linux.*
*2. FinFireWire: Software durch welche mithilfe von Firewire und DMA ein komplettes Abbild des Arbeitsspeichers heruntergeladen werden kann.*
*3. FinFly USB: Installation von zuvor gewählter Software nur durch Einstecken eines zuvor präparierten USB-Sticks.*
*4. FinFly ISP: Eine auf Internet-Provider-Ebene installierte Software, die unter anderem gezielt momentan geladene Dateien mit Überwachungssoftware infizieren kann.*

1. Eine Software, die einen Remote-access-Zugriff („Fernzugriff“ oder auch Ernwartungszugriff) auf einen Rechner ermöglicht, muss also vorher dort installiert worden sein. Das

kann nur unter ganz speziellen und klar definierten Bedingungen geschehen, *nicht* aber, wenn das „Opfer“ sich vernünftig und sicherheitsbewusst verhält. Das gilt auch für Punkt 2. Die Firma behauptet selbst auch nichts anderes.

3. „Präparierte“ USB-Sticks können nicht automatisch etwas auf einem Rechner installieren. Der Besitzer des Rechners muss das (fahrlässig) erlaubt haben oder sich nicht sicherheitbewusst verhalten.

4. Wir haben auch schon die Sina-Box. So what?

Wer in derartigen Artikel verschweigt, dass es auch möglich ist, sich vor Spionage-Software zu schützen, wer behauptet, diese könne ohne (fahrlässiges) Wollen des Nutzers installiert werden, ist ein Dummschwätzer|Wichtigtuer und verbeitet nur Panik im Sinne der Geheimdienste („man kann nichts tun – sie sind eh schon drin“). And period.