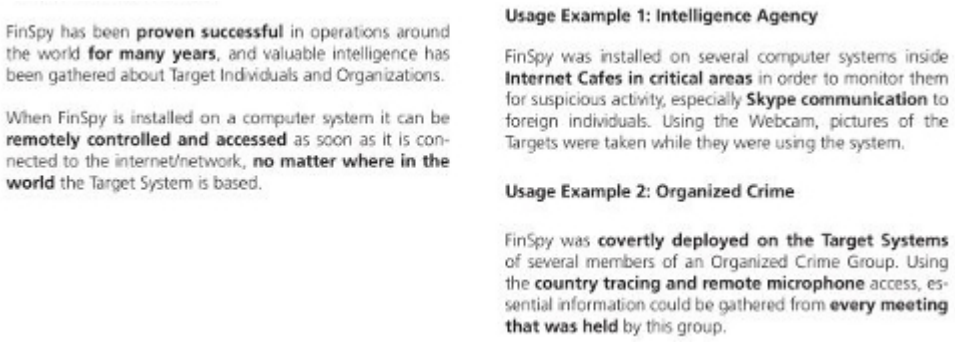
Cyberdurchsuchung, die 894ste



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.

Manchmal habe ich bei den offenbar hingeschlampten Meldungen von Heise, insbesondere von Stefan Krempl, den Eindruck, hier werde haarscharf an einer Verschwörungstheorie vorbeigeschrieben.

Es ist eindeutig eine urbane Legende, wenn man suggeriert, irgendein Cyberpolizist säße irgendwo vor dem Monitor und "hackte" sich irgendwo in einen privaten Rechner. So etwas zu können behauptet noch nicht einmal FinSpy.

Auch Wikipedia faselt sinnfrei herum: "handelt es sich um einen Trojaner, da die Spionagefunktionen in einer harmlos aussehenden Hülle eingeschmuggelt werden." (Die Diskussionsseite ist gesperrt – vermutlich nicht zufällig.)

"Harmlos aussehende Hülle"? Geht es ein bisschen konkreter? Nein, weil das Blödsinn ist! Man kann trojanische Pferde (so heißt das und nicht "Trojaner") nur auf einem "fremden" Rechner implementieren, wenn man entweder den physischen Zugriff hat und der Rechner ungesichert ist oder wenn man per USB-Stick Software installieren kann, und das alles nur unter ganz bestimmten Bedingungen. Alles andere ist Voodoo und ein Hoax der allerfeinsten Sorte.

Wenn man sich die Passagen bei Wikipedia zur Quellen-Telekommunikationsüberwachung (was für ein Wort!) genauer anschaut, wird auch sofort klar, dass es sich weitgehend um heiße Luft handelt.

“Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen”, schreibt der CCC in seiner Analyse. “Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde.” Quod erat demonstrandum. Nur wie ich oben schrieb.

In einem Internet-Cafe ginge das natürlich, falls ein Richter das anordnete. Übrigens habe ich Linux. Und man müsste schon an meinem Stangenschloss hinter der Wohnungstür vorbei und einbrechen, um an meine Rechner zu kommen. Per USB geht bei mir auch nichts, meine BIOSSE (heißt das so?) verbieten das. Keylogger funktionieren bei Ubuntu oder XFCE auch nicht oder ich würde es merken.

Aber noch mal für Krempl zum Mitschreiben: Gefährder sitzen ausschließlich und immer an demselben Platz in immer demselben Internetcafe und nutzen ausschließlich Windows.