



G DATA

# Whitepaper 2008

Fehlalarm 2.0 – Funktionsweise von Rogue-AntiSpyware  
Werner Klier, Virus Research G DATA Security Lab

Die internationale Cybermafia überrollt ahnungslose PC-Anwender zur Zeit mit unzähligen Varianten vorgeblicher Anti-Spyware-Programme. Besonders hinterhältig: Die durch die gefälschte Anti-Spyware „aufgedeckte“ Infektion des Systems ist Teil einer ausgeklügelten Inszenierung. Am Ende machen die Angreifer gleich in mehrfacher Hinsicht satte Beute.

Die Experten der G DATA Security Labs verzeichneten während der letzten Wochen einen explosionsartigen Anstieg sogenannter „Rogue Antispyware“. Hat jemand dafür eine griffige Übersetzung. Dabei handelt es sich um Software, die vorgibt, auf dem System des Opfers zahlreiche Malware-Infektionen gefunden zu haben und diese auch gleich entfernen zu können.

Messungen von G DATA zufolge sind allein für die Malware-Familie „Trojan-Downloader.Fraud-Load“, die für die Mehrheit der „Rogue Antispyware“-Vorfälle verantwortlich zeichnet, bis heute weit über 1000 verschiedene Varianten aufgetaucht. Der Angriff folgt dabei stets dem gleichen Schema:

Beim Besuch einer unter der Kontrolle des Angreifers stehenden Webseite erhält das Opfer die Meldung, dass sein System möglicherweise infiziert sei. In den meisten Fällen erfolgt bereits in diesem Moment tatsächlich eine Infektion des Rechners, welche die gefälschte Abwehrsoftware auf dem Rechner installiert. Anschließend gibt die Software vor, einen Komplettscan des Systems durchzuführen, welcher in aller Regel damit endet, dass unzählige „Infektionen“ festgestellt werden. Das Ergebnis des angeblichen „Scans“ steht dabei von Anfang an fest, da die gemeldeten Dateien kurz vorher durch die angebliche Abwehrsoftware selbst angelegt werden, wodurch immer Infektionen gefunden werden, selbst wenn das System de facto „sauber“ ist.

### Screenshot des Schwindel-Scanners Antimalware Guard



Im nächsten Schritt wird der verunsicherte Anwender aufgefordert, eine „Vollversion“ der Software zu erwerben oder die Software zu „registrieren“, da die aufgefundenen Infektionen angeblich erst dann überhaupt entfernt werden können. Dazu wird das Opfer auf eine Webseite gelockt, die den Anschein erwecken soll, dass es sich bei der angeblichen Sicherheitssoftware um ein seriöses Produkt handelt. Die Aufmachung derartiger Webseiten ist dabei durchaus als professionell zu bezeichnen und dient dennoch ausschließlich dem Zweck, dem Opfer persönliche Daten bis hin zur Kreditkartennummer zu entlocken. Durch das geschickte einleitende Ablenkungsmanöver haben die Cyber-Gangster dabei leichtes Spiel.

### Screenshot: Registrierungsseite von Antimalware Guard



Neben der angetäuschten Infektion, die über die Zwischenstation der ebenfalls angetäuschten Abwehrsoftware zur Herausgabe persönlicher Informationen führen soll, bringen viele Varianten quasi „im Huckepack“ reale Infektionen mit, die durch die gefälschte Sicherheitssoftware natürlich nicht erkannt werden, dabei das System des Opfers aber tatsächlich um echte Schadsoftware unterschiedlichster Machart bereichern und ihn obendrein gar zum Zombie machen und in ein Botnetz integrieren.

Um ihr schmutziges Geschäft möglichst lang und unbehelligt betreiben zu können, registrieren die Angreifer unzählige Domains unter professionell anmutenden Namen, auf denen die zugehörigen Produktseiten hinterlegt werden. Dabei werden die jeweiligen Namen in unterschiedlichsten Schreibweisen registriert. Grund: Wird ein Domainname durch Strafverfolgungsbehörden stillgelegt, wird er einfach durch einen ähnlich klingenden ersetzt, das hinterhältige Spiel beginnt erneut und kann fast endlos wiederholt werden.



G DATA empfiehlt allen Anwendern den Einsatz etablierter Virenschutzlösungen. Da die aktuell massenhaft auftretenden Vorfälle angeblicher Schutzsoftware in der Mehrzahl auf sog. Drive-by-Infektionen setzen, bei denen über Sicherheitslücken in den gängigen Internet-Browsern Systeme infiziert werden können, ohne dass dies von klassischen Wächtermechanismen bemerkt wird, sollte zum Schutz des Systems ein http-Filter eingesetzt werden, der die ankommenden Daten bereits vor Erreichen des Browsers überprüft und im Falle von Schadsoftware direkt blockt.

Darüberhinaus sollten Betriebssystem und Browser immer auf dem aktuellsten Updatestand gehalten werden.

Aktive Inhalte im Browser lassen sich beispielsweise durch den Einsatz spezieller Toolbars oder Webfilter-Komponenten deaktivieren.