Inhalt

1. Anti-Bundestrojaner als Wegbereiter für Verbrechen
2. Anti-Bundestrojaner reine Publicity
3. Anti-Bundestrojaner ist nutzlos

Heute möchte ich mich einem Thema widmen, welches ebenfalls Bestandteil der Vorgänge rund um den Bundetrojaner ist. Obwohl wir nahezu ausschließlich positive Kritik für unser Engagement im Zusammenhang mit dem Bundestrojaner erhalten, darf nicht verschwiegen werden, dass es auch sehr kritische Stimmen zu unserem Anti-Bundestrojaner gibt. Im Wesentlichen hat man es mit den folgenden drei Arten der Kritik zu tun.

1. Sie sind mit Ihrem Anti-Bundestrojaner Wegbereiter für Verbrechen und behindern den legitimen Einsatz der Überwachungssoftware
2. Sie haben den Anti-Bundestrojaner doch nur veröffentlicht, um Publicity zu machen.
3. Anti-Bundestrojaner ist doch völlig nutzlos, weil bereits minimale Änderungen am Bundestrojaner genügen, um ArchiCrypt auszutricksen.

Anti-Bundestrojaner als Wegbereiter für Verbrechen *

Das ist nicht unsere Intention und, im Gegensatz zu Alfred Nobel mit seinem Dynamit, können wir uns auch ziemlich sicher sein, dass wir in der Realität auch kein Wegbereiter sind.

Was haben wir gemacht?

Wir haben eine ganz konkrete Version des Bundestrojaners analysiert und ein technisches Werkzeug geschaffen, mit dem man diese Version inkl. etwaiger Varianten entlarven kann. Diese bestimmte Version des Anti-Bundestrojaners verstößt gegen geltendes Recht und ist damit nicht geeignet, im Rahmen von Ermittlungen, verwertbares Beweismaterial zu liefern. Über diesen Umstand ist man sich bis in höchste Politikerkreise inzwischen einig.

Welche Folgen hat das?

Der Einsatz des unzulässigen Überwachungstrojaners ist damit gestoppt. Die

Öffentlichkeit hat ihre Aufmerksamkeit auf dieses Thema gerichtet und die Politiker zum Handeln gezwungen. Es wird einen Neuanfang geben, bei dem darauf geachtet wird, dass die gesetzlichen Vorgaben der Quellen Telekommunikationsüberwachung strikt eingehalten werden. An dieser Stelle wird dann auch der Anti-Bundestrojaner digital zu Grabe getragen, er hat dann quasi seinen Zweck erfüllt.

Anti-Bundestrojaner reine Publicity *

Tja, was soll man einem solchen Vorwurf entgegenbringen. Ich wundere mich gelegentlich über bestimmte Ansichten. Nur wundern, sonst nichts! Aber will man jemandem zum Vorwurf machen, dass er in einer Tageszeitung erwähnt wird, weil er bei einem Unfall Erste Hilfe geleistet hat oder Zivilcourage gezeigt hat? Ich würde das nicht tun, wäre doch eine Art Neid, oder? Schließlich schreiben wir die Artikel nicht selbst, sondern sie werden geschrieben. Wenn dabei unser Name fällt, freue ich mich, denn wir nehmen die Publicity natürlich trotzdem gerne mit! Schließlich sind wir auch nicht Microsoft!

Anti-Bundestrojaner ist nutzlos *

Während mir die Kritikpunkte oben per E-Mail und Telefon zukamen, kann ich mich bei diesem Punkt auf einen Blog-Beitrag beziehen und meine konkrete Antwort mit anfügen:

Der Blog-Beitrag…

Inhaltslos ist der Beitrag keinesfalls, er hat einen durchaus wahren Kern! Man sieht aber, wie komplex das Thema ist und wie schnell man dabei ist, Dinge falsch zu interpretieren.

Meine konkrete Antwort auf den Beitrag:

> „Hallo Christian,
>
> zunächst einmal freue ich mich, in Dir einen Gefährten im Kampf um

Freiheit und Grundrechte gefunden zu haben. Als Autor des Anti-Bundestrojaners bin ich auf Deinen Blog- Beitrag aufmerksam gemacht worden. Du hast nicht ganz unrecht mit Deiner Aussage, dass bestimmte Tools (*im Wesentlichen Antivieren-Programme; AV-Programme*) im Zusammenhang mit dem Bundestrojaner (BT) sehr hilflos sind bzw. komplett hilflos waren. Aber was die konkrete Kritik am Anti-Bundestrojaner angeht, liegst Du falsch. Heise kritisiert zu Recht in erster Linie Cloud-basierte Lösungen, die eine Prüfsumme für einen Schädling berechnen (*meist mit MD5 oder SHA*) und in einer Datenbank ablegen. Lokal wird dann auf Deinem Rechner für jede Datei ebenfalls dieser Prüfwert (*Hashwert genannt*) berechnet und zum Server gesendet. Wird der Hashwert in der Serverdatenbank gefunden, hat man einen Schädling, sonst nicht. Jetzt ist es in der Tat so, dass alleine die Änderung eines einzelnen BIT-Wertes den gesamten Hashwert ändert. Heise hat hier im MZ Header einfach ein großes O in DOS in ein kleines O umgeändert. Obwohl die Datei natürlich weiterhin schädlich ist, wird sie nicht mehr als Trojaner erkannt. Mit diesem Problem schlagen sich auch viele AV-Programme herum, die lokal arbeiten.

Was meinen Anti-Bundestrojaner angeht, habe ich aber einen völlig anderen Ansatz gewählt. Ich habe die Binärdateien des Trojaners installiert und im laufenden Betrieb analysiert (*richtig analysiert und nicht nur einen Hashwert berechnet*). Dabei habe ich mir genau angesehen, wie der Trojaner arbeitet. Was richtet der Treiber für ein Geräteobjekt ein, wie kann man sich über die Windows API mit ihm verbinden, wo verewigt er sich im Dateisystem, wie trägt er sich in die Registry ein, welche Methoden werden in der DLL aufgerufen, an welche Prozesse hängt sich der Trojaner etc. Du kannst das alles in meinem Blog (http://blog.archicrypt.de) nachlesen. Es gibt zur Analyse auch ein PDF Dokument (http://www.archicrypt.com/files/Warum_wir_den_64_BIT_Bundestrojaner_finden.pdf) Herausgekommen sind Merkmale, die ich s.g. Kernmerkmale genannt habe. D.h.: Die Eigenschaften sind so speziell, dass es bereits genügt, wenn nur eines in einem System auftritt, um mit hoher Sicherheit zu sagen, ob sich der Bundestrojaner auf dem Rechner befindet. Da müsste der aktuelle Bundestrojaner komplett umgearbeitet werden, damit die Heuristik in meinem Anti-Bundestrojaner nicht mehr anschlägt.

Das von mir verwendete Verfahren ist sehr zeitaufwendig und kann so in einem normalen AV-Programm nicht eingesetzt werden. Das System wäre kaum mehr nutzbar. Für diesen speziellen Fall ist diese Methode jedoch extrem gut geeignet. Wenn Du Lust und Laune hast, kannst Du ja eine virtuelle Maschine mit zum Beispiel Windows XP aufsetzen, die Binärdateien, die Du beim CCC laden kannst, manuell installieren (*etwas Know-how ist nötig, da der eigentliche Installer nicht verfügbar ist*) und das Anti-Bundestrojaner Tool darauf loslassen. Ändere etwas im Trojaner, passe aber auf, dass Du den Trojaner nicht kaputt machst, sprich im ausführbaren Code etwas änderst, und versuche es erneut. Du müsstest nahezu alles ändern, sprich einen neuen Trojaner schreiben, um das Tool auszutricksen.

Aber damit habe ich genau das genannt, womit ich Dir eingangs Recht gegeben habe. Wenn mir jetzt jemand einen Auftrag gäbe (ich würde ihn aus moralischen Gründen ablehnen) einen neuen Bundestrojaner zu schreiben, bekäme ich sehr viel Geld dafür und könnte mir den Aufwand leisten, alles komplett neu zu schreiben. Ich kann mir dann alle aktuellen AV-Programme kaufen und natürlich den Anti – Bundestrojaner kostenlos laden. Jetzt schreibe ich so lange an meinem Bundestrojaner, bis kein Gegenmittel mehr wirkt und bin am Ziel. Der Schreiber der Abhörsoftware ist also immer einen Schritt voraus. Das gilt übrigens auch für jeden Virus und jeden Trojaner. Mir ging es mit meinem Anti-Bundestrojaner rein darum, etwas gegen den aktuell im Umlauf befindlichen BT in all seinen Varianten zu unternehmen, da er im Grundsatz gegen die Quellen TKÜ (*also geltende Gesetze*) verstößt. Nicht darum, den Ermittlungsbehörden für alle Zeiten einen Strich durch die Rechnung zu machen.

Ach ja, Informatiker nennen solche Verfahren nicht „Running-Gag“ sondern

heuristischen Ansatz

Würde mich freuen, wenn DU meinen Beitrag auch veröffentlichst!“