Inhalt

Angeblich wurde jetzt eine 64-BIT Version des Trojaners gefunden. Dies schreibt sich die Firma F-Secure auf die Fahne. F-Secure soll dann einen MD5 Hashwert (eine Art Prüfsumme, mit der sich eine Datei erkennen lässt) an Mitarbeiter der Firma Kaspersky weiter geleitet haben. Diese hätten dann wiederum in ihrer Datenbank den Schädling ausmachen und schließlich analysieren können. Soweit so gut!

Siehe:
http://www.gulli.com/news/17361-kaspersky-analysiert-zweite-staatstrojaner-version-update-2011-10-18

Das Analyseergebnis *

Was ist neu? *

Jetzt aber zum eher fraglichen Analyseergebnis bzw. unsauberen Ergebnis. In der 64-BIT Version habe man entdeckt, dass nicht nur ein paar Browser, sondern auch andere Programme, wie Messenger überwacht werden. Lesen Sie sich im Blogbeitrag „**Der 64-Bit Anti-Bundestrojaner**“ den Abschnitt „**Warum wir sicher sind, die 64-BIT Version zu finden, so es sie gibt?**“ durch. Dort finden Sie bei der Analyse der 32-BIT Version genau diese angeblich nur in der 64-BIT Version vorhandenen Programme im Punkt 6 aufgelistet. Es sieht also nicht nach neuen Ergebnissen, sondern eher nach unsauberer Arbeit aus?!

Interessant *

Interessant ist in der Tat die Erwähnung des Zertifikats. Hier müssten sich doch unglaublich interessante Erkenntnisse gewinnen lassen. Wer ist der Besitzer des Zertifikates, wer ist der Aussteller! Leider schweigt man sich genau über diesen Punkt

aus. Oder hat man ein s.g. self-signed Zertifikat eingesetzt und den Rechner in den „Testsigning“ Modus versetzt und das verschleiert? Ich wüsste das gerne!

Einschub: Ein reguläres Zertifikat muss bei einer autorisierten Instanz beantragt werden. Dabei wird, festen Regeln folgend, nach eindeutiger Feststellung der Identität des Antragstellers ein Zertifikat ausgestellt. Dieses Zertifikat wird mit einem anderen Zertifikat unterzeichnet. Ein solches Zertifikat benötigt man unter 64 BIT Betriebssystemen, um einen Treiber zu installieren. Dabei enthält der Treiber die digitale Signatur, die mit dem Zertifikat erstellt wurde. Man kann dann aus der Datei selbst die Zertifikatdetails wie „Name des Signaturgebers“ auslesen. Wenn man Treiber entwickelt und diese testen möchte, muss man die Treiber zuvor immer signieren. Es gibt anscheinend Entwickler, die kein echtes Zertifikat besitzen. Für diese Gruppe hat Microsoft eine Boot-Option geschaffen, mit der man Treiber auch mit „unechten“ Zertifikaten signieren kann. Man nennt solche Zertifikate self-signed (*selbst signiert*). Hier fehlt also die übergeordnete Instanz, die mit der eigenen digitalen Signatur wieder für die Korrektheit aller Angaben im Zertifikat steht. Solche self-signed Zertifikate kann jeder selbst erzeugen und dabei beliebige Angaben machen. Auf einem regulären 64-BIT System laufen diese Treiber aber nicht. Erst dann, wenn man den Rechner in den s.g. Testsigning Modus versetzt, funktioniert es. Dazu muss man in der Kommandozeile den Boot Editor bcdedit mit den Parametern -set TESTSIGNING ON aufrufen. Die Konsequenz ist allerdings, dass, je nach Betriebssystem mehr oder weniger deutlich, auf dem Desktop angezeigt wird, dass sich der Rechner im Testmodus befindet.

Fazit *

Bisher sieht es so aus, als wäre ich bei der Analyse und mit meinen Vermutungen genau auf der richtigen Spur gewesen. Auch die saubere Analyse der 32-BIT Version hat dazu geführt, dass die in der neuen Version des Anti-Bundestrojaners (32+64 BIT) eingesetzte Mustererkennung damit dann auch sicher die 64-BIT Versionen findet.