



Fragen und Antworten der Kaspersky Labs GmbH zum Thema „Bundestrojaner“

Gibt es bald Antivirensoftware mit staatlich verordneter Hintertür? Wie würden Sie reagieren, wenn Sie per Gesetz gezwungen werden, Lücken/Schwachstellen in Ihrem Programm zu nennen? Könnte die Regierung ein Gesetz erlassen, welches Kaspersky Labs verbietet den "Bundestrojaner" zu erkennen?

Sollte die Regierung ein solches Gesetz erlassen wollen, würde dies sicherlich wie jede Gesetzesänderung von der Presse öffentlich begleitet. Wir gehen davon aus, dass der öffentliche Druck so groß wäre, dass ein solches Gesetz nicht zustande käme.

Im Übrigen ist es schwer zu sagen, ob ein Bundestrojaner tatsächlich wirksam wäre, denn wir denken, dass Kriminelle, die etwas zu verbergen haben, durchaus in der Lage sind, sich vor solchen Trojanern zu schützen. Darüber hinaus könnte ein Krimineller diese Art von Spionageprogrammen auch leicht mittels mehrerer PCs umgehen - einen mit Zugang ins Internet und einen ohne. Dateien könnten auf dem Offline-PC verschlüsselt, per USB-Stick auf den mit dem Internet verbundenen übertragen und von dort aus verschickt werden. Selbst wenn zig Spionageprogramme auf dem mit dem Netz verbundenen PC installiert wären, würden diese die Verschlüsselung nicht aufheben können. Dasselbe würde bei eingehenden Nachrichten passieren: Datei kommt verschlüsselt an, per USB-Stick auf den abgeschirmten Rechner, entschlüsseln, verarbeiten.

Welche Gefahr sieht Kaspersky Lab in dem Versuch, einen "Bundestrojaner" zu entwickeln?

Es würde sich hierbei um einen massiven Eingriff in die gesamte IT-Sicherheitsindustrie handeln, der aus unserer Sicht nicht vorstell- und durchführbar wäre. Die Produkte der Hersteller würden nämlich für den Kunden abgewertet, was hieße, dass der Staat sich massiv in die wirtschaftlichen Belange der Unternehmen einmischen würde.

Andere Länder wie China oder die USA haben solche Programme bereits eingesetzt. Gibt es bald die "guten" und die "bösen" Spionageprogramme? Wie will man diese unterscheiden?

Wir wollen und werden sie nicht unterscheiden. Ein Trojaner zeigt auf dem Rechner ein bestimmtes Verhalten - ob er jetzt staatlich oder nicht-staatlich ist. Unsere Produkte analysieren dieses Verhalten und unterbinden es, wenn es ihnen gefährlich vorkommt. Ein "gutes" Spionageprogramm gibt es nicht. Das widerspricht der Natur der Sache.





Würde Ihr Programm einen sogenannten "Bundestrojaner" erkennen?

Der Staat hätte natürlich beim Einsatz eines Trojaners mehr Möglichkeiten, als sie einem Virenautoren zur Verfügung stehen. So bestünde bei einer Zusammenarbeit mit Providern die Möglichkeit, sich in den Datenverkehr einzuklinken und Dateien quasi "on the fly" mit einem Trojaner zu infizieren, bevor sie beim Anwender ankommen. Der Anwender lädt also eine - eigentlich "saubere" Datei von einem Rechner - erhält aber die präparierte Variante.

Dennoch müsste aber auch ein Bundestrojaner letztlich mit den gleichen Methoden arbeiten wie die Spyware von Malwareschreibern - und würde damit mit sehr hoher Wahrscheinlichkeit von unseren proaktiven Schutzmaßnahmen (Code-Heuristik, verhaltensbasierte Heuristik etc.) als potentiell gefährlich gemeldet. Nach Einschicken des verdächtigen Programms in unser Labor würde entsprechend eine Klassifizierung als Trojaner inkl. Signaturerstellung folgen.

Würde ihn das Programm abwehren und blockieren?

Generell können wir natürlich keine Erkennungsgarantien für Programme abgeben, die bislang noch niemand gesehen hat. Letztlich müsste aber auch ein "Bundestrojaner" mit den gleichen Mitteln arbeiten wie herkömmliche Spyware, so dass er von unserer Software höchst wahrscheinlich erkannt werden würde. Wenn unsere Software ein Programm als Trojaner erkennt, wird sie verhindern, dass es Daten nach außen sendet.

Wären Sie bereit, mit Behörden bei Online-Durchsuchungen zusammenzuarbeiten und mögliche Lücken im System zu nennen?

Es würde sich hierbei um einen massiven Eingriff in die gesamte IT-Sicherheitsindustrie handeln, der aus unserer Sicht nicht vorstell- und durchführbar wäre. Die Produkte der Hersteller würden nämlich für den Kunden abgewertet, was hieße, dass der Staat sich massiv in die wirtschaftlichen Belange der Unternehmen einmischen würde.

Gab es bereits entsprechende Anfragen von Seiten der Behörden?

Bislang gab es keine Kontaktaufnahme seitens staatlicher Stellen.





Was sind die Kriterien für eine Software, damit diese vom Virens scanner als Trojaner erkannt wird?

Entweder die Software wurde nach einer Analyse in unserem Labor als Trojaner klassifiziert (und eine entsprechende Signatur zur Erkennung veröffentlicht), oder aber unsere proaktiven Schutzmaßnahmen (Code-Heuristik, verhaltensbasierte Heuristik etc.) stufen ein Programm als potentiell gefährlich ein.

Falls die Software der Bundesregierung nicht den Kriterien eines Trojaners entspricht, würde die Software trotzdem erkannt werden, um den Kunden zu schützen?

Wenn sich eine Software nicht wie ein Trojaner/Virus/Wurm/Rootkit etc. verhält, gibt es natürlich auch keinen Grund sie entsprechend einzustufen, denn dann wäre sie harmlos.

Wäre es möglich, dass die Regierung sich einer schon vorhandenen Trojaner-Software bedient und diese nur leicht modifiziert, damit sie nicht mehr erkannt wird?

Möglich ist alles - letztlich wäre dies aber nur Spekulation. Darüber hinaus würden jedoch auch Modifikationen mit sehr hoher Wahrscheinlichkeit erkannt werden.

Wurde bereits verdächtige Software gefunden die auf einen Beta-Test eines Bundestrojaners hinweist?

Nein - und es ist auch unwahrscheinlich, dass es einen Betatest im großen Maßstab geben würde.

