linksunten.indymedia.org

14. Juni 2010

Wie das BKA Trojaner FUD macht

von Roland Ionas Bialke

Durch private Sicherheitsdienste für Computersysteme fällt es dem Bundeskriminalamt schwer, relativ nicht detektierbare Spionagesoftware zu entwickeln bzw. zu verwenden. An dieser Stelle will ich darum ein Beispiel nennen, wie das BKA vorgehen kann, um ihre Spionagesoftware "unsichtbar" zu machen.

In der Szenesprache wird das Spionagesoftware-relativ-nicht-detektierbar-machen "stealthen" genannt. Mit den gängigsten Antivirenprogrammen wird überprüft, ob z.B. ein Trojaner für die meisten gängigen Antivirenprogramme unsichtbar ist. Das könnt Ihr auch ganz einfach machen. Marktführerin in Deutschland ist hierfür die Homepage http://www.virustotal.com/de . Dort könnt Ihr Eure Dateien hochladen und überprüfen, ob ca. 40 der gängigsten Antivirenprogramme Eure Dateien als Schadsoftware erkennen. Wird dort keine Schadsoftware erkannt, obwohl Ihr absichtlich einen Trojaner hochgeladen habt, dann wird in der Szene davon gesprochen, dass der Trojaner "full undetectet" (FUD) ist. Erkennen nur einige Antivirenprdogramme den Trojaner, jedoch das Antivirenprogramm des zu infizierenden Computers ist bekannt und dieses Antivirenprogramm erkennt den Trojaner nicht, dann wird nur noch von "undetected" (UD) gesprochen.

Private Sicherheitsdienste für Computersysteme, also z.B. kommerzielle Antivirenprogramme, tauschen sich jedoch aus und werten zudem analysierte Dateien aus. Wird eine Datei auf http://www.virustotal.com/de oder ähnlichen Homepages hochgeladen und nicht als Schadsoftware erkannt, so wird diese mit Netzwerkanalyseprogrammen (Szenesprache: "Sniffer") untersucht. Sollte zuvor ein hochgeladener Trojaner nicht als Schadsoftware erkannt, so werden schliesslich die Bewegungen dieser Software per Reverse Engineering analysiert. Es wird geschaut, was sich wie auf dem Computer bewegt. Bei ungewünschten Verhaltensweisen und Inhalten der Dateien (Was unerwünscht ist, definiert der private Sicherheitsdienst - Chemische Synthesedarstellungen wurden von solchen Programmen auch schon als Schadsoftware benannt!) wird markiert. Die Analysen werden untereinander ausgetauscht bzw. Dienstleisterinnen wie die Homepage http://www.virustotal.com/de verkaufen Ihre Dateien zum Analysieren an die privaten Sicherheitsdienste weiter und kaufen selbst die analysierten Dateien auf. Wenn Ihr also nach einigen Tagen nochmal einen Trojaner hochladet, der zuvor FUD war, so wird dieser nun von guten Antivirenprogrammen als Schadsoftware erkannt. Und genau das ist ein Problem, was Behörden wie das Bundeskriminalamt haben.

Gäbe es also "einen Bundestrojaner", dann wären deren RATs (RAT = der Teil vom Troyaner, der auf den zu infizierenden Computer gebracht werden muss) schon nach kürzester Zeit als Schadsoftware bekannt. Darum müssen für jeden Computer individuell die RATs angepasst werden. Und eine Operation mit den individuellen RATs wäre (im für das Bundeskriminalamt schlechtesten Fall) nur kurzzeitig möglich.

Mit Reverse Engineering zu unsichtbaren Trojanern

Eine Möglichkeit RATs individuell FUD zu machen ist das "hexen". Hexen ist eine Form des Stealthen und hat nichts mit Zauberei zu tun. Hexen ist eine Methode des Reverse Engineering. Die privaten

Sicherheistdienste markieren nämlich bestimmte Abschnitte, die auf Schadprogramme hinweisen. Und diese "Markierungen" werden beim Hexen herausgefunden und in den RATs verändert.

Um hexen zu können, wird ein Hexeditor gebraucht. Hexeditoren wandeln die jeweilige Computersprache in binäre Sprache um. Die binäre Sprache ist die wirkliche Sprache der Computer und besteht, wie der Name schon sagt, aus "Nullen und Einsen" bzw. aus "an und aus". Wenn das Bundeskriminalamt nun den binären Code eines als Trojaner detektieren RATs haben, dann weiss das BKA, dass darin irgendwo der markierte Teil zu finden ist. Und nun wird es einfach: Das Bundeskriminalamt (und auch jeder andere Mensch) kann nun den binären Code einfach in zwei gleiche Teile teilen, und diese wieder in eine ausführbare Datei umwandeln. Beide Teile können nun wieder auf http://www.virustotal.com/de oder ähnlichen Homepages hochgeladen werden. Der markierte Teil wird des Codes wird nur in einem dieser beiden Teile stehen und somit wird nur ein Teil des ursprünglichen RATs als Schadsoftware erkannt. Der erkannte Teil wird einfach wieder als Binärcode in der Mitte durchgeschitten, wieder in ausführbare Dateien umgewandelt und wieder auf Schadsoftware überprüft. Wieder wird nur ein Teil dieser beiden Viertel als Schadsoftware erkannt. Und wieder wird der erkannte Teil des binären Codes in der Mitte getrennt und die Teile nach Schadsoftware gescannt. Das geschieht so lange, bis nur noch ein ganz kleiner binärer Codeschnipsel übrigbleibt - Die von den Antivirenprogrammen markierte Stelle des Trojaners. Diese markierte Stelle wird dann verändert und schliesslich alle Teile wieder zusammengefügt. Dann wird überprüft, ob die ganze Datei nicht mehr als Schadsoftware erkannt werden (manchmal gibt es zwei Markierungen und eine Markierung wurde beim Teilen in der Mitte zerschnitten) und ob die veränderte Datei überhaupt noch funktionsfähig ist. Im Idealfall hätte das Bundeskriminalamt nun das RAT FUD gehext.

Letztendlich schützt jedoch nur das Erlernen der Handhabung und der Gebrauch eines Sniffers vor Schadsoftware! In der Vergangenheit wurden z.B. soganannte "Sandboxes" (virtuelle Computersysteme) für die sichere Ausführung von mit Schadsoftware befallenden Dateien empfohlen. Ich kenne jedoch die Entwicklungsgeschichte von kommerziellen Trojanern und weiss daher, dass eine Programm-Generation weiter das Problem "Sandbox" einfach umgangen wurde, indem die Funktion der Sandboxes einfach ausgeschaltet wurde, dem Computer aber eine einwandfreie Funktion vorgegaukelt wurde. Kaum etwas ist sicher!

Ein paar Namen bekannter Trojaner: Bitfrost, Poison Ivy, CIA, Shark - All diese Programme sind als Troaner extrem bekannt und werden als Schadsoftware angezeigt. Aus Sicherheitsgründen sollte sich das BKA diese Programme nur von den Herstellerseiten runterladen.

Originaltext