RATs auf dem Vormarsch: aktuelle Malware-Analyse von SophosLabs

SophosLabs haben sich in ihrem aktuellsten Report mit dem faszinierenden Fall der RATicate-Malwaregruppe beschäftigt. Dieser Fall sticht deshalb so heraus, weil er die jüngste Operation und Entwicklung einer Gruppe von Cyberkriminellen aufdeckt, die anscheinend ihre geldgierigen Finger in einer Reihe von Malware-Fällen haben.

Tatsächlich haben diese Gauner eine Vielzahl von Unternehmen in zahlreichen Industriezweigen zumindest in Europa, im Nahen Osten und in Asien angegriffen. RAT ist die Abkürzung für Remote Access Trojan, eine Art von Malware, die darauf abzielt, den Nutzer-Computer so einzurichten, dass Cyberkriminelle ihm abtrünnige Befehle über das Internet senden können.

Bei eine RAT-Infektion kann der Computer angewiesen werden, eine Reihe von Aktivitäten durchzuführen. Dazu gehören u.a. eine Rückmeldung mit einer detaillierten Bestandsaufnahme des Computers, einschließlich installierter Software, Konnektivität und Geschwindigkeit des Netzwerks sowie Konfigurationseinstellungen und Lizenzcodes. Auch das Durchforsten der Dateien nach sogenannten „Trophäendaten“, die es wert sind, gestohlen zu werden, gehört ins Portfolio. Darüber hinaus ist auch die Überwachung der Tastatureingaben und des Netzwerkverkehrs, in der Hoffnung, Passwörter und Token zur Netzwerkauthentifizierung zu extrahieren, möglich

RATs können für eine Vielzahl anderer Zwecke eingesetzt werden. Weitere Details dieser perfiden Malware sind hier zu finden.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de