Der Krake analysiert

Anfang des Monats erlangte das Kraken-Botnetz aufgrund seiner vermuteten Größe einige Aufmerksamkeit. Sicherheitsforscher haben die Bots des Netzes jetzt genauer analysiert.

Das Kraken-Botnetz erlangte auf der RSA-Sicherheitskonferenz einige Aufmerksamkeit aufgrund seiner Größe – es soll rund 400.000 Drohnen umfassen. Bislang werde das Botnetz zumeist zum Spam-Versand eingesetzt – die üblichen Spam-Mails für Online-Apotheken, Penisverlängerungen, Online-Casinos oder Kredite, hieß es Anfang April. Diverse Sicherheitsunternehmen haben mittlerweile die Bot-Software analysiert; sie haben jetzt die Algorithmen etwa zur Erstellung der zufälligen Domain-Namen für die Command-and-Control-Server (C&C) oder zur Ver- und Entschlüsselung der Kommunikation nachprogrammiert und stellen sie sogar zum Download zur Verfügung.

McAfee beobachtet bei den Kraken-Drohnen eine zunehmend ausgefeiltere Verschleierung. Während die älteren Varianten des Schädlings noch über den UDP-Port 447 mit anderen Drohnen kommuniziert haben, nutzen die neuen Versionen beliebige UDP-Ports sowie die TCP-Ports 80 und 443 zur Kommunikation. Dadurch können die Drohnen häufiger in Unternehmen anzutreffende Schutzmaßnahmen umgehen, bei denen etwa nur die Ports für HTTP- und HTTPS-Verkehr freigeschaltet sind.

Michael Hale Ligh und Greg Sinclair haben mittels Reverse Engineering den Verschlüsselunsgalgorithmus des C&C-Verkehrs analysiert. Sie erläutern das Paket-Format in einem Blog-Eintrag und stellen sogar Quellcode zum Download bereit, der die Ver- und Entschlüsselung in C++ nachbildet. Ein Analyse-Modul für Wireshark wollen die beiden ebenfalls veröffentlichen, bislang bieten sie jedoch nur ein Kommandozeilen-Werkzeug zur Analyse von mitgeschnittenem Botnet-Traffic an.

Die Kraken-Drohnen suchen unter zufällig erzeugten Domain-Namen nach ihrem C&C-Server. Die Forscher von PCTools haben den Algorithmus untersucht, mit dem die Drohnen diese Domain-Namen erstellen, und darauf aufbauend ebenfalls eine Variante in C++ programmiert, die interessierte Nutzer herunterladen können.

Durch die Analyse-Ergebnisse ist es einfacher, neue Varianten des Kraken-Bots abzugreifen und die Erkennungsroutinen und -Signaturen der Antivrenlösungen anzupassen. Vielleicht gelingt es aber auch, das Botnetz empfindlich zu stören – das haben Forscher um Thorsten Holz von der Universität Mannheim bereits mit dem Sturm-Wurm-Botnetz demonstriert.