Sophos X-Ops: Quakbot lebt und bleibt gefährlich

Sophos X-Ops hat eine neue Variante der Qakbot-Malware entdeckt und analysiert. Erstmals traten diese Fälle Mitte Dezember auf und sie zeigen, dass sich die Qakbot-Malware trotz der erfolgreichen Zerschlagung der Botnet-Infrastruktur durch die Strafverfolgungsbehörden im vergangenen August weiterentwickelt hat. Dabei setzen die Angreifer noch bessere Methoden ein, ihre Spuren zu verwischen.

Die von Sophos X-Ops analysierten Fälle zeigen, dass die Cyberkriminellen gezielte Anstrengungen unternommen haben, um die Verschlüsselung der Malware zu verstärken. Für Verteidiger ist es dadurch schwieriger geworden, den schädlichen Code zu analysieren. Außerdem verschlüsseln die Angreifer jetzt die gesamte Kommunikation zwischen der Malware und dem Kontrollserver mit einer stärkeren Methode als in früheren Versionen. Die Malware hat auch eine zuvor entfernte Funktion wieder eingeführt, die verhindert, dass sie in einer virtuellen Umgebung oder Sandbox ausgeführt wird.

Erst wenn die Schöpfer des Bots strafrechtlich belangt sind, könnte Quakbot enden
„Die Zerschlagung der Qakbot-Botnet-Infrastruktur war ein Sieg, aber die Schöpfer des Bots sind weiterhin aktiv," kommentiert Andrew Brandt, Principal Researcher von Sophos X-Ops die jüngsten Qakbot-Vorfälle. „Cyberkriminelle, die Zugang zum ursprünglichen Qakbot-Quellcode haben, experimentieren mit neuen Varianten und testen diese im realen Einsatz.

Eine der bemerkenswertesten Änderungen betrifft den Verschlüsselungsalgorithmus, den der Bot verwendet, um die im Bot fest einkodierten Standardkonfigurationen zu verbergen. Dies macht es für Analysten noch schwieriger, die Funktionsweise der Malware zu erkennen. Die Angreifer stellen auch zuvor veraltete Funktionen wie die Erkennung virtueller Maschinen (VM) wieder her und testen sie in diesen neuen Versionen.

Es ist sehr wahrscheinlich, dass die Entwicklung von Qakbot weitergeht, bis seine Schöpfer strafrechtlich verfolgt werden. Die gute Nachricht ist, dass diese neuen Qakbot-Varianten mit zuvor erstellten Signaturen von einer Endpoint-Detection-Software leicht zu erkennen sind.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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