Online-Bankräuber erweitern mit DanaBot-Upgrade ihr Arsenal - Einer der gefährlichsten Banking-Trojaner geht in die nächste Entwicklungsstufe

Nach neuesten Erkenntnissen der ESET-Malware-Analysten mutiert DanaBot zur neuen Allzweckwaffe der eCrime-Szene. Neben Emotet zählt der seit 2018 aktive Computerschädling zu den aggressivsten Banking-Trojanern. Er ist für eine Vielzahl erfolgreicher Angriffe gegen Privatanwender und Unternehmen verantwortlich. Wie bei kaum einem anderen Schadprogramm investieren kriminelle Programmierer bei DanaBot viele Ressourcen, um im hohen Tempo neue Versionen zu verteilen. Das jetzt von ESET entdeckte Update von Ende Januar 2019 beinhaltet u.a. eine neue Architektur. Die Kommunikation zwischen dem befallenen Opfer-PC und den dahinterliegenden Command & Control Servern erfolgt nun mehrfach verschlüsselt (AES und RSA). Eine Nachverfolgung der Datenströme und die Enttarnung der Täter wird dadurch immens erschwert.

Wo sind die Online-Bankräuber aktiv?

Die Opfer der seit vergangenem Jahr laufenden DanaBot-Kampagne befinden sich weltweit. Beginnend in Australien hat der Trojaner hauptsächlich Computernutzer in Polen, Italien, Deutschland, Ã–sterreich, Ukraine und den USA ins Visier genommen. Gerade die europäischen Versionen verfügen über zusätzliche Features mit neuen Plugins und Spam-Versand-Möglichkeiten.

Was ist neu?

Das neue Kommunikationsprotokoll wird derzeit in zwei Szenarien verteilt: Als Update rollen die Täter die modifizierte Verision automatisiert an bereits infizierte DanaBot-Opfer. Eine zweite und leider immer noch äusserst erfolgreiche Verbreitungsvariante ist der Versand von SPAM mit schädlichen Dateianhängen. Diese tarnen sich unter anderem als vermeintliche Rechnungen, Shopping-Angebote, Bankinformationen oder Bestellbestätigungen. Letzterer Verbreitungsweg wird aktuell verstärkt in Polen eingesetzt.

Eine weitere Ã„nderung des Trojaners betrifft die Vorgehensweise. In der älteren Variante hat eine Downloader-Komponente erst das Hauptmodul aus dem Netz nachgeladen, welches dann wiederum die Plugins und Konfigurationen herunterlud. Die neue Version registriert einen sogenannten Loader als Betriebssystemdienst, welcher dann das Hauptmodul zusammen mit den Plugins und Konfigurationen nachlädt.

Dynamische eCrime-Reaktionen

"Wir haben im letzten Jahr beobachtet, dass die Täter DanaBot innerhalb kürzester Zeit weltweit verbreiten konnten. Neben der Qualität und der permanenten Malware-Produktpflege zeigt das vor allem eines: Die Gruppierung, die hinter DanaBot steckt, muss über professionelle und leistungsfähige eCrime-Strukturen verfügen", so Thomas Uhlemann, ESET Security Specialist. Die bisher von der weltweiten IT-Security-Community veröffentlichten Erkenntnisse über DanaBot blieben nach Einschätzung des Experten nicht ohne Reaktion. "Offenbar haben die Autoren hinter DanaBot diese Veröffentlichungen dazu benutzt, die Struktur des Schädlings der Kampagne entsprechend hochdynamisch anzupassen, um Erkennungen, etwa auf Netzwerkebene, zu entgehen."

Weitere Informationen und IoC finden Sie auf WeLiveSecurity: