



E-Spionagegruppe OceanLotus greift gezielt Regierungsbehörden an - ESET-Forscher erklären die neuesten Techniken der Spionagegruppe

ESET-Forscher haben die neuesten Methoden der Spionagegruppe OceanLotus (auch bekannt als APT32 und APT-C-00) aufgedeckt. Derzeit nutzen die Angreifer eine bekannte Sicherheitslücke in Microsoft Office aus (CVE-2017-11882) und erlangen über ein schädliches .rtf-Dokument Zugriff auf die Systeme. Zudem hat die Gruppe einen Weg gefunden, Schadprogramme einzuschleusen, dabei jedoch kaum Spuren zu hinterlassen. Die Angreifer vereinen dabei eine grosse Bandbreite von Techniken und verbessern diese kontinuierlich, um unentdeckt zu bleiben. Aktuelle Analysen der ESET-Forscher zeigen, dass OceanLotus weiterhin gezielt Regierungen und Behörden in Südostasien attackieren.

"OceanLotus ist weiterhin sehr aktiv und entwickelt sich kontinuierlich weiter", erklärt Thomas Uhlemann, ESET Security Specialist. "Die Gruppe verfeinert ihre Techniken, damit gezielte Angriffe noch erfolgreicher durchgeführt werden können. Daher gehen wir davon aus, dass wir von OceanLotus in den nächsten Monaten noch einiges hören werden."

zefis.ch - info@zefis.ch

portals powered and hosted by proswiss.ch

Jena (pts) 21.03.2019

Ausgedruckt am 19.04.2024 - Seite 1/1