Sathurbot: Botnet greift WordPress-Seiten an - Trojaner verbreitet sich über File-Sharing-Seiten

Kostenlose Filme und Software: Damit lockt der Trojaner Sathurbot Nutzer, um ihre Rechner zu infizieren und mit einem wachsenden Botnet WordPress-Webseiten anzugreifen. Der europäische Security-Software-Hersteller ESET hat Sathurbot analysiert und stellt die Ergebnisse in einem ausführlichen Bericht vor.

Gezielter Angriff auf WordPress-Webseiten

Sathurbot hat es auf Webseiten abgesehen die das Content Management System WordPress verwenden. Mit mehr als 5.000 grundlegenden generischen Wörtern versucht die Malware, Anmeldeinformationen für WordPress-Webseiten zu erstellen. Verschiedene Bots im Sathurbot-Botnet probieren unterschiedliche Anmeldeinformationen auf der gleichen Website aus. Jeder Bot versucht aber nur einen einzigen Login pro Seite und wechselt danach zur nächsten. Dieses Verhalten stellt sicher, dass ein Bot nicht anhand seiner IP-Adresse erkannt und für zukünftige Versuche gesperrt wird.

Sathurbot verbreitet sich über File-Sharing-Seiten, auf denen Nutzer Torrents für angeblich kostenlose Filme und Dateien herunterladen. Die Torrent-Datei dient Sathurbot als Transfermedium: Sobald ein Nutzer die Datei ausführt, kapert der Trojaner den Rechner und stellt eine Verbindung zu einem Command and Control (C&C)-Server her, sodass der Computer in das Botnet integriert wird.

So schützen sich Nutzer gegen Sathurbot

Nutzer, die von Sathurbot betroffen sind, können mit einem Drittanbieter-Dateimanager die bösartige .DLL entlarven, mit dem Taskmanager explorer.exe und/oder rundll32.exe terminieren und die betreffende .DLL löschen. Danach muss der Computer neu gestartet werden. Um einer Infektion des Rechners mit Sathurbot vorzubeugen, sollten Nutzer keine Dateien ausführen, deren Ursprung nicht einwandfrei geklärt ist. Ausserdem sollten sie keine Software von File-Sharing-Seiten beziehen.