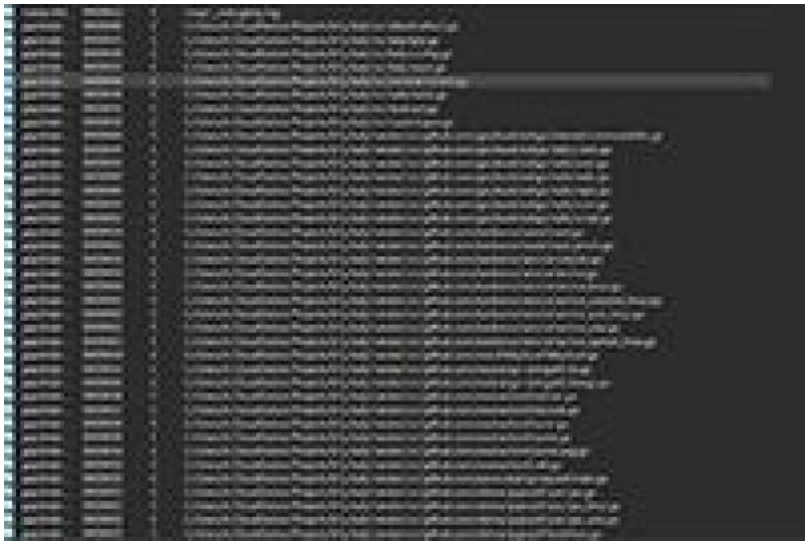
Entdeckung eines in Google GO geschriebenen Linux-Trojaners

25.08.2016, 13:11 | IT, New Media & Software

Pressemitteilung von: *Doctor Web Deutschland GmbH*
Presseagentur: *WE Communications*



Linux.Lady.1

Die Sicherheitsanalysten von Doctor Web haben einen neuen Linux-Trojaner entdeckt, der Mining-Malware für Kryptowährungen auf dem infizierten PC startet. Der Trojaner ist in Googles Programmiersprache GO geschrieben, was ihn so außergewöhnlich macht.

Der Trojaner Linux.Lady.1 ist in der Lage, externe IP-Adressen von infizierten Rechnern zu bestimmen, Rechner gezielt anzugreifen sowie Mining-Malware für Kryptowährungen herunterzuladen und zu starten. Linux.Lady.1 ist in Googles Programmiersprache Go geschrieben, was für einen Trojaner dieser Art eine Seltenheit darstellt und ihn schwieriger auffindbar macht. In seiner Architektur nutzt er vielfältige Bibliotheken, die auf GitHub verfügbar sind.

Nach dem Start von Linux.Lady.1 übermittelt er die Versionsdaten des installierten Betriebssystems Linux, die Anzahl der Prozessoren und gestarteten Prozesse an den Remote-Server der Cyber-Kriminellen. Von diesem Server erhält der Trojaner eine Konfigurationsdatei, durch die eine Mining-Malware für Kryptowährungen installiert und gestartet wird. Auf diese Weise werden die geminten Gelder auf das Konto der Angreifer transferiert.

Über spezielle Webseiten bestimmt Linux.Lady.1 eine externe IP-Adresse um andere Rechner gezielt anzugreifen. Der Trojaner versucht zunächst eine Verbindung zum Port herzustellen und greift dann auf den Redis (remote dictionary server) zu. Bei fehlerhafter Konfiguration durch den Systemadministrator - also wenn kein Passwort eingerichtet ist - gelingt dieser Versuch. Nach erfolgreicher Verbindung schreibt der Trojaner im cron eines Remote-Rechners ein Skript ein, welches von Dr.Web Antivirus als Linux.DownLoader.196 erkannt wird. Dieses Skript lädt dann Linux.Lady.1 herunter und installiert ihn auf dem infizierten Rechner. Anschließend fügt der Trojaner einen neuen Schlüssel zum Verbindungsaufbau via SSH in die Liste der autorisierten Schlüssel ein.

Die Antivirensoftware von Doctor Web entdeckt und löscht Linux.Lady.1 und Linux.DownLoader.196. Sie stellen daher keine Gefahr für Benutzer von Dr.Web dar.

Portrait

Das russische Unternehmen Doctor Web Ltd. ist einer der führenden Hersteller von Anti-Virus- und Anti-Spam-Lösungen mit Hauptsitz in Moskau. Das Doctor Web Team entwickelt seit 1992 Anti-Malware-Lösungen und beschäftigt weltweit 400 Mitarbeiter, davon 200 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Das Unternehmen legt großen Wert auf die effektive Beseitigung von Kundenproblemen und bietet schnelle Antworten auf akute Virengefahren. Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Frankfurt vertrieben. Zu den nationalen und internationalen Kunden zählen neben privaten Anwendern namhafte börsennotierte Unternehmen wie die russische Zentralbank, JSC Russian Railways, Gazprom oder Arcelor Mittal sowie Bildungseinrichtungen und öffentliche Auftraggeber wie das russische Verteidigungsministerium.

News-ID: 915890 • Views: 212 (Stand: 30.04.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/915890/Entdeckung-eines-in-Google-GO-geschriebenen-Linux-Trojaners.html