Neue Bedrohungen für das Betriebssystem Linux

27.04.2016, 17:08 | IT, New Media & Software

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

Logo Dr.Web

Backdoor-Trojaner, die Remote-Befehle ausführen können, sind ein wichtiges Thema in der IT-Sicherheitsszene. Insbesondere dann, wenn diese auf das Betriebssystem Linux abzielen. Denn dieses wird auch gerne von größeren Unternehmen, Regierungen, der Verwaltung oder anderen Organisationen eingesetzt. Im April 2016 haben die Virenanalysten von Doctor Web gleich mehrere gefährliche Trojaner mit Fernzugriffsfunktionen entdeckt. Dazu gehören Linux.BackDoor.Xudp.1, Linux.BackDoor.Xudp.2 und Linux.BackDoor.Xudp.3.

Das erste Glied in der Infizierungskette ist eine ELF-Datei. Sobald sie heruntergeladen wurde, wird der Nutzer beim Starten der Applikation nach Root-Rechten gefragt. Werden diese gewährt, installiert sich zunächst der darin verborgene Linux.Downloader.77. Dieser ist in der Lage, Angriffe, die auf dem Versenden von UDP-Paketen beruhen, durchzuführen oder selbständig andere Malware herunterzuladen.

Verschachtelte Trojaner ebnen Weg für Mehrfachinfektionen:
Daneben lädt der Trojaner vom Server der Cyber-Kriminellen ein weiteres Skript (Linux.Downloader.116) herunter und startet es. Dieses dient zum Download des Linux.BackDoor.Xudp.1, speichert ihn als /lib/.socket1 oder /lib/.loves ab, platziert ihn im Autostart-Verzeichnis /etc/ als rc.local und stellt das automatische Starten des Schädlings im Cron-Zeitplan sicher. Darüber hinaus wird der Inhalt von iptables geleert. Nachdem Linux.BackDoor.Xudp.1 gestartet wurde, entschlüsselt er seine Konfigurationsdaten und übermittelt Informationen vom infizierten Endgerät an den Server der Cyber-Kriminellen.
Danach startet er drei unabhängige Protokolle. Erster Schritt über HTTP: der Trojaner versendet eine Nachricht, dass er gestartet wurde und erhält einen Schlüssel zur Kodierung von Nachrichten, Serverdaten und Portnummern. Anschließend sendet Linux.BackDoor.Xudp.1 in einem definierten Zeitintervall Anfragen für mögliche Befehle an den Server. Dieser Algorithmus dient wahrscheinlich zum Update des Schädlings. Alle eingehenden Befehle sind verschlüsselt und können nur durch einen speziellen Algorithmus des Trojaners entschlüsselt werden. Im zweiten Schritt erwartet Linux.BackDoor.Xudp.1 Befehle via UDP vom Server. Im dritten Schritt versendet der Schädling schließlich Nachrichten an den Server, dass er immer noch aktiv ist.

Unter den Befehlen, die Linux.BackDoor.Xudp.1 ausführen kann, sind u.a. das ständige Versenden von Anfragen, DDoS-Angriffe und willkürliche Aktionen auf einem infizierten PC. Linux.BackDoor.Xudp.1 ist unter anderem auch in der Lage, Ports im definierten Bereich von IP-Adressen zu scannen oder Dateien auf Befehl zu starten. Außerdem haben die Virenanalysten von Doctor Web herausgefunden, dass dieser Trojaner ständig verbessert und upgedatet wird.

Die Trojaner Linux.BackDoor.Xudp.2 und Linux.BackDoor.Xudp.3 sind verbesserte Versionen von Linux.BackDoor.Xudp.1, die sich u.a. durch Namen, den Umfang von versendeten Daten und auszuführenden Befehlen unterscheiden.

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: 901367 • Views: 128 (Stand: 06.06.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/901367/Neue-Bedrohungen-fuer-das-Betriebssystem-Linux.html