

Java-Malware kopiert Passwörter und ermöglicht Fernsteuerung

Bochum (Deutschland), 16. Juni 2020

Eine in Java entwickelte neu entdeckte Malware kann Zugangsdaten kopieren, den Rechner des Opfers fernsteuern und weitere Kommandos ausführen. Die integrierte Ransomware-Komponente ist derzeit noch nicht voll funktionsfähig.

Analysten von G DATA CyberDefense warnen vor einer neuen Malware, die in Java entwickelt wurde. Ist die Malware auf einem System aktiv, können Kriminelle Passwörter aus Browsern und dem E-Mail-Programm auslesen. Da die Schadsoftware über eine Remote-Access-Funktion (RAT) verfügt, kann ein Angreifer außerdem aus der Ferne die Kontrolle über das infizierte System übernehmen. Dazu wird das Remote Desktop Protokoll (RDP) genutzt - eine modifizierte Version des Tools "rdpwrap" (<https://github.com/stascorp/rdpwrap>) wird dazu im Hintergrund heruntergeladen. In der modifizierten Version sind versteckte RDP-Zugänge möglich.



Zudem verfügt die Malware über eine - derzeit noch - rudimentäre Ransomware-Komponente. Hier findet aber bislang keine Verschlüsselung statt, sondern lediglich eine Umbenennung der Dateien. Da Malware oft kontinuierlich weiterentwickelt wird, könnte sich das in künftigen Versionen aber ändern.

„Die aktuelle Malware ist ungewöhnlich, wir haben schon länger keine neue Java-Schadsoftware mehr gesehen“, sagt Karsten Hahn, Virus Analyst bei G DATA CyberDefense. „Bei der von uns analysierten Schadsoftware sehen wir bereits versuchte Infektionen bei unseren Kunden.“

Mit dem vorliegenden Infektionsweg ist die Schadsoftware nicht ohne Java lauffähig. Es ist davon auszugehen, dass derjenige, der die Software geschrieben hat, experimentiert hat. Es ist jedoch bereits eine Funktion vorhanden, die die Java-Laufzeitumgebung direkt vor Infektion mit der Java-Malware herunterlädt und installiert. Wer bereits eine Version der Java Runtime Environment (JRE) auf dem Rechner installiert hat, ist für eine Infektion verwundbar.

RDP-Zugänge sind traditionell ein beliebtes Mittel von Kriminellen, um auf Systeme in Firmennetzen Zugriff zu erhalten. Firmen wiederum nutzen RDP-Zugänge für Wartungsarbeiten und teilweise für die Remote-Arbeit. Innerhalb eines Unternehmensnetzes sollte also sorgfältig darauf geachtet werden,

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Pressemitteilung

RDP-Traffic genau im Auge zu behalten, um Auffälligkeiten sofort bemerken zu können.

Weitere technische Details und Grafiken finden Sie im englischsprachigen [Techblog-Artikel](#) unseres Analysten Karsten Hahn.



G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299