

Sicherheitswarnung: Aktuelle NetWire-Kampagne wird über Excel-Tabellen verbreitet

G DATA Virus-Analysten entdecken neue Angriffswelle

Bochum (Deutschland), 13. Mai 2020

Die Security-Analysten von G DATA CyberDefense warnen vor einer aktuellen Angriffswelle mit dem Remote Access Trojaner (RAT) NetWire. Dazu versenden die Angreifer Spam-Mails mit infizierten Excel-Dokumenten. Einmal im System, übernehmen Cyberkriminelle die administrative Kontrolle des Rechners. Die Angreifer haben dann Zugriff auf persönliche Daten und können Passwörter auslesen. G DATA Kunden sind vor den Angriffen geschützt.



Seit kurzem ist der Remote Access Trojaner (RAT) NetWire sehr aktiv und greift Windows-Systeme an. Die Schadsoftware ist in der Cybercrime-Szene weit verbreitet und bereits seit längerem aktiv.

„Anwender sollten bei E-Mails mit Excel-Dokumenten im Anhang höchste Vorsicht walten lassen“, rät Karsten Hahn, Virus Analyst bei G DATA CyberDefense. „Zurzeit nutzen Kriminelle diesen Weg, um den Remote Access Trojaner NetWire zu verbreiten. Wird die Datei geöffnet, aktiviert sich PowerShell und lädt über paste.ee zwei Dateien nach. Eine der Dateien ist eine .NET DLL, welche die zweite Datei, NetWire, mittels Process Injection ausführt. Die Kriminellen können den infizierten Rechner anschließend mit NetWire aus der Ferne steuern und ausspähen. Anwender sind gut vor der NetWire-Kampagne geschützt, wenn sie eine Antiviren-Software installiert haben und regelmäßig aktuelle Updates einspielen. Unsere Technologien Beast und DeepRay erkennen die Malware. Falls PowerShell auf einem Rechner nicht nötig ist, sollte es deaktiviert werden.“

Das macht ein RAT

Mit Remote Access Trojanern (RAT) wie NetWire übernehmen Cyberkriminelle die vollständige administrative Übernahme und Steuerung des infizierten Windows-Computers. Nutzer bemerken davon nichts, sodass das RATs unentdeckt seine schädlichen Funktionen ausführen kann. So spähen die Angreifer beispielsweise persönliche Informationen sowie Passwörter aus oder löschen Dateien. Die so erbeuteten Informationen, zum Beispiel Zugänge zu Onlinebankkonten oder Shops, lassen sich gewinnbringend in speziellen Untergrundmärkten verkaufen.

Für das initiale Laden von NetWire wird ein Powershell-Skript verwendet. Powershell ist Bestandteil von Microsoft Windows und wird von vielen IT-

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

Abteilungen eingesetzt, um bestimmte Vorgänge zu automatisieren. Powershell ist an sich also eine legitime Applikation. Sofern Powershell nicht ausdrücklich auf dem System benötigt wird, sollte es deaktiviert werden – die entsprechende Option findet sich in den Windows-Features.



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