Gestohlene FTP-Zugangsdaten

Im Rahmen der Analyse eines Botnetzes durch ein CERT wurde eine Liste mit mehreren zehntausend gestohlenen FTP-Zugangsdaten gefunden. Die Zugangsdaten wurden vermutlich auf mit Schadprogrammen infizierten PCs ausgespäht, von denen auf die FTP-Accounts zugegriffen wurde. In den meisten Fällen handelt es sich um FTP-Accounts für die Administration von Websites.

Die Zugangsdaten werden offenbar aktuell aktiv von den Tätern missbraucht, um Skripte zur Verbreitung von Schadprogrammen über ein Angler Exploit Kit in die mit den FTP-Accounts verbundenen Websites einzuschleusen.

Der CERT-Bund hat eine Liste der in Deutschland gehosteten betroffenen FTP-Accounts erhalten. Nachfolgend senden wir Ihnen eine Liste betroffener Accounts in Ihrem Netzbereich. Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen einzuleiten bzw. Ihre Kunden zu informieren.

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/gestohlene-ftp-zugangsdaten/