Security Alert: G DATA warnt vor aktueller Dridex-Welle

Aktuell gibt es verstärkt Aktivitäten der Dridex-Malware. Diese bereits einige Jahre alte Schadsoftware macht zurzeit in Excel-Dateien die Runde, die per Mail verschickt werden. Dabei hat der Schädling es vor allem auf Passwörter und andere Nutzerdaten abgesehen.
"Wenn das Wochenende vor der Tür steht, lässt bei vielen Nutzern die Wachsamkeit deutlich nach. Das machen sich Kriminelle zunutze", sagt Tim Berghoff, Security Evangelist bei G DATA.

Bereits Mitte der Woche zeichnete sich ab, dass eine Schadsoftware mit dem Namen "Dridex" wieder verstärkt Aktivitäten zeigt. Dieser Schädling ist für G DATA kein unbeschriebenes Blatt - bereits 2015 haben wir über diese Malware berichtet. Wie damals versteckt das Schadprogramm sich auch in diesem Fall in einer Office-Datei, getarnt als Versandbestätigung. Heruntergeladen wird die eigentliche Malware über ein eingebettetes Makro, welches sich hinter der "Drucken"-Funktion verbirgt.

Gerade im Moment sollten Nutzer also verstärkt auf der Hut sein, wenn es um solche vermeintlichen Versandbestätigungen geht. G DATA-Kunden sind geschützt - sowohl die Office-Datei als auch das darin eingebettete Makro werden von allen G DATA Security-Lösungen erkannt.

Vorsicht bei unsignierten Makros

Um die Sicherheit noch weiter zu erhöhen, lohnt es sich, Makros vor allem in Firmennetzwerken global zu deaktivieren. Sind dennoch Makros an einigen Stellen unverzichtbar, sollten nur signierte Makros verwendet und zugelassen werden. Die entsprechenden Optionen finden sich in den Active Directory Gruppenrichtlinien.

Zurzeit scheinen Donnerstag und Freitag zu den beliebteren Tagen für den Versand von Schadsoftware zu gehören. Bereits in der vergangenen Woche haben Kriminelle mit Gootkit/Kronos diesen Zeitpunkt für ihre Angriffe gewählt. Bei näherer Betrachtung ergibt das Sinn: Wenn das Wochenende unmittelbar vor der Tür steht, lässt bei vielen Nutzern die Wachsamkeit nach.