

Wie Identitätsdatendiebstahl mit Techniken der Threat Intelligence aufgespürt wird

Pascua Theus und Gina Muuss

Digitale Identitätsdaten, Konto- oder Kreditkarteninformationen sowie E-Mail-Adressen und Passwörter werden in großen Mengen von (Cyber-) Kriminellen gesammelt. In den meisten Fällen bemerken betroffene Personen nicht einmal, dass sie Opfer einer Straftat geworden sind. Je nach krimineller Aktivität erfahren sie erst sehr viel später davon, dass sich die Täter unter Verwendung ihrer persönlichen Daten bereichert haben. Die Warnung der Opfer von Identitätsdiebstahl ist entscheidend, um den durch Identitätsmissbrauch verursachten Schaden zu begrenzen.

Um den Opfern rechtzeitig proaktive Warnungen zukommen lassen, müssen die geleakten Identitätsdaten verfügbar sein. Hierzu wurde ein Verfahren entwickelt, das online Zeitungsartikel verarbeitet und entscheidet, ob diese über geleakte Identitätsdaten berichten oder nicht. So lässt sich ein Benachrichtigungsservice für Analysten erstellen, die sich dann auf die Suche nach den geleakten Daten machen können.

Im Forschungsprojekt EIDI wurde eine Methodik zur Sammlung und Analyse geleakter Identitätsdaten entwickelt, die bereits erfolgreich zur proaktiven Warnungen von Opfern genutzt wird.