Medieninformation

Landeskriminalamt Sachsen

Ihr Ansprechpartner
Kay Anders

Durchwahl
Telefon +49 351 855 2010
Telefax +49 351 855 2095

kommunikation.lka@
polizei.sachsen.de*

23.10.2023

Internationale Operation gegen die Ransomware-Gruppe Ragnar Locker

Exekutivmaßnahmen in elf Ländern

In der Woche vom 16. bis 20. Oktober 2023 haben Strafverfolgungsbehörden aus elf Ländern einer der gefährlichsten Cybercrime-Gruppierungen der letzten Jahre einen schweren Schlag versetzt.

Diese auf internationaler Ebene von Europol und Eurojust koordinierte Aktion richtete sich gegen die Ransomware-Gruppe Ragnar Locker, die für zahlreiche aufsehenerregende Angriffe auf IT-Systeme von Unternehmen und kritischen Infrastrukturen weltweit verantwortlich sein soll (siehe auch die Presseveröffentlichungen von Europol und Eurojust vom 20. Oktober 2023).

Wesentliche Teile der Infrastruktur der Ransomware wurden in Deutschland und den Niederlanden beschlagnahmt. Die zugehörigen Server der Webseiten im Darknet konnten in Schweden lokalisiert und sichergestellt werden.

Diese internationale Operation ist das Ergebnis komplexer Ermittlungen, die von der französischen Nationalgendarmerie gemeinsam mit Strafverfolgungsbehörden aus der Tschechischen Republik, Deutschland, Italien, Japan, Lettland, den Niederlanden, Spanien, Schweden, der Ukraine und den Vereinigten Staaten von Amerika durchgeführt wurden.

In Deutschland beteiligt sich das Landeskriminalamt Sachsen seit April 2021 im Auftrag der Staatsanwaltschaft Leipzig an den Ermittlungen. In enger Zusammenarbeit mit dem Bundeskriminalamt konnte die Abschaltung und Sicherstellung mehrerer Server in Deutschland und Schweden sowie die Schaltung eines Sperrbanners auf den Webseiten der Tätergruppierung erfolgreich umgesetzt werden.

Die Gruppierung ist seit Dezember 2019 aktiv. Der Name Ragnar Locker ist gleichzeitig der Name einer Ransomware, welche die Gruppe entwickelt und

Hausanschrift:
Landeskriminalamt Sachsen
Neuländer Straße 60
01129 Dresden

www.lka.sachsen.de

betrieben hat. Diese Ransomware-Variante zielte auf Geräte mit Microsoft Windows-Betriebssystemen ab.

Die Ragnar Locker-Gruppe hat sich durch Angriffe auf kritische Infrastrukturen auf der ganzen Welt einen Namen gemacht. In Deutschland gab es neun geschädigte Unternehmen bzw. Organisationen – zwei davon in Sachsen.

Es entstand im Bundesgebiet ein Schaden von mindestens 760.000 Euro. Die bekannten Forderungen der Täter für Entschlüsselungstools sowie für die Nichtfreigabe der gestohlenen sensiblen Daten betrugen insgesamt 6.300.000 Euro.

Ausgehend von einem hier bearbeiteten Fall übernahm das Landeskriminalamt Sachsen im November 2022 die zentralen Ermittlungen für alle in der Bundesrepublik registrierten Fälle und damit einhergehend den intensiven Austausch mit den internationalen Behörden und die Durchführung von zahlreichen Ermittlungsmaßnahmen. In Bezug auf die in Deutschland geführten Verfahren ist eine Identifizierung von Tatverdächtigen bislang nicht gelungen. Die Ermittlungen, die wegen des Tatverdachts der Erpressung in Tateinheit mit Ausspähen von Daten und Computersabotage geführt werden, dauern an.

Wie können sich Behörden und Unternehmen vor Ransomware schützen?

• Orientieren Sie sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Grundschutz)

• Aktualisieren Sie regelmäßig Ihre Software zur Schließung von Sicherheitslücken

• Achten Sie auf funktionierende Backupsysteme und eine bedarfsorientierte Rechtevergabe

• Halten Sie eine Notfallplanung mit umfassender Beschreibung der Vorgehensweise und Systemwiederherstellung im Falle einer Ransomware-Infektion vor

• Nehmen Sie die Betreuung von professionellen IT-Dienstleistern in Anspruch

• Schulen und sensibilisieren Sie Ihre Mitarbeiter regelmäßig

• Die Kombination mehrerer dieser Maßnahmen kann dazu beitragen, das Risiko zu minimieren und die Auswirkungen zu begrenzen

Welche Präventionsmöglichkeiten habe ich als Privatperson?

• Teilen Sie persönliche Daten nur sehr begrenzt öffentlich mit, achten Sie auf Ihre Social-Media-Einstellungen

• Verwenden Sie unterschiedliche komplexe Passwörter für Ihre verschiedenen Online-Zugänge

• Richten Sie eine sogenannte Zweifaktorauthentifizierung zu Ihren Online-Zugängen ein, sofern dies möglich ist

Abbildung: Sperrbanner auf der Leakpage der Ransomware Ragnar Locker

Medien:
Dokument: Internationale Operation gegen die Ransomware-Gruppe Ragnar Locker - Exekutivmaßnahmen in elf Ländern
Foto: Sperrbanner auf der Leakpage der Ransomware Ragnar Locker