Vier Drahtzieher, allesamt russische Staatsbürger, wurden letzte Woche festgenommen und 27 Server abgeschaltet. Foto: LW-Archiv

Schlüsselfiguren einer Hackergruppe verhaftet

Sie erpressten Privatpersonen und Unternehmen, auch in Luxemburg. Jetzt klickten die Handschellen

Im November 2023 hatte die Gruppe eine Firma in Hobscheid attackiert und im Darknet erklärt, verschiedene Arten von Daten erlangt zu haben, darunter Rechnungen, Quittungen, Arbeitsverträge und eine beträchtliche Menge an vertraulichen Informationen. Die Hacker nannten sich 8Base. Ihr Geschäftsmodell: Computer blockieren, Daten stehlen, erpressen.

Jetzt klickten die Handschellen. Wie Europol am Dienstag mitteilt, sind in einer internationalen Operation gegen Cyberkriminalität, an der vergangene Woche mehrere Länder beteiligt waren, die vier Schlüsselfiguren der Hackergruppe festgenommen worden. Es handelte sich laut Europol um „eine der aktivsten Ransomware-Gruppen des Jahres 2024".

„Diese Personen, allesamt russische Staatsbürger, werden verdächtigt, eine Variante der Phobos-Ransomware eingesetzt zu haben, um von Opfern in ganz Europa und darüber hinaus hochwertige Zahlungen zu erpressen", führt die europäische Polizeibehörde mit Sitz in Den Haag aus.

Mit Ransomware wird eine Form der digitalen Erpressung bezeichnet, bei der Hacker die Daten von Privatpersonen, Unternehmen oder Institutionen verschlüsseln, den Zugriff auf ihre Geräte oder Dateien blockieren, und dann Geld für die Freigabe verlangen. Für die Entschlüsselung und Rückgabe der Daten forderten die Hacker ein Lösegeld meist im sechs- oder siebenstelligen Bereich.

Mehr als 400 Unternehmen im Visier der Kriminellen

Europol teilte außerdem mit, dass 27 Server, die mit dem kriminellen Netzwerk in Verbindung standen, abgeschaltet wurden.

Die Operation folgte auf eine Reihe von Verhaftungen gegen die Phobos-Gruppierung, betonte Europol und erwähnte insbesondere die Festnahme eines Phobos-Administrators in Südkorea im Juni 2024, der im November desselben Jahres an die USA ausgeliefert wurde. Ein anderer wurde bereits 2023 in Italien aufgrund eines französischen Haftbefehls verhaftet.

Dank der Operation der letzten Woche, an der 14 Länder beteiligt waren, konnten die Behörden mehr als 400 Unternehmen weltweit vor laufenden oder drohenden Ransomware-Angriffen warnen, fügt Europol hinzu.

> *Dank der Operation konnten die Behörden mehr als 400 Unternehmen weltweit vor laufenden oder drohenden Ransomware-Angriffen warnen.*

Die Ransomware Phobos, die erstmals im Dezember 2018 entdeckt wurde, wurde laut Europol häufig für Angriffe auf kleine und mittlere Unternehmen oder Organisationen verwendet, denen es oft an Cybersicherheitsabwehr mangelt. Unter Ausnutzung der Infrastruktur von Phobos entwickelte 8Base eine eigene Variante der Ransomware und nutzte deren Verschlüsselungs- und Verteilungsmechanismen für eine maximale Wirkung.

„Die 8Base-Gruppe war besonders aggressiv in ihren doppelten Erpressungstaktiken, indem sie nicht nur die Daten der Opfer verschlüsselte, sondern auch damit drohte, die gestohlenen Informationen zu veröffentlichen, wenn nicht ein Lösegeld gezahlt wird", so Europol. *AFP/MeM*