Ransomware sperrt die Computer der Opfer oder verschlüsselt ihre Daten und verlangt Lösegeld für deren Freigabe.

Europol, die niederländische Polizei, Intel Security und Kaspersky Lab starteten die Initiative „No More Ransom“.

Tool gegen Internet-Erpresser

„No more Ransom“: Ein neues Tool mit mehr als 160.000 Schlüsseln unterstützt Opfer von digitaler Erpressung bei der Wiederherstellung ihrer Daten.

Die niederländische Polizei, Europol, *Intel Security* und *Kaspersky Lab* starteten im Juli 2016 eine Initiative mit dem Namen „No More Ransom“: Ein Onlineportal, das die Öffentlichkeit über Ransomware-Gefahren informiert und Opfer bei der Wiederherstellung ihrer Daten unterstützt, ohne dass sie Lösegeld an Cyber-Kriminelle zahlen müssen.

Ransomware sperrt die Computer der Opfer oder verschlüsselt ihre Daten und verlangt im Anschluss eine Lösegeldsumme, damit die Kontrolle über betroffene Geräte und Daten wieder erlangt werden kann. Ransomware ist für die EU-Strafverfolgungsbehörden eine der derzeit größten Bedrohungen: In fast zwei Drittel der EU-Mitgliedstaaten erfolgen Ermittlungen aufgrund dieser Art der Malware-Attacke. Die Zielobjekte sind oftmals persönliche Geräte, aber auch Unternehmen und sogar staatliche Netzwerke. Die Anzahl der Opfer wächst bedrohlich: Laut *Kaspersky Lab* stieg die Zahl der von Krypto-Malware attackierten Nutzer zwischen den Jahren 2015 und 2016 um 550 Prozent an, von 131.000 auf 718.000.

Onlineportal. Auf *www.nomoreransom.org* finden Opfer Informationen, was Ransomware ist, wie die Schädlinge funktionieren und wie man sich dagegen schützen kann. Bei einer Infizierung ist die Wahrscheinlichkeit groß, dass die Daten für immer verloren sind. Das Erlernen einer bewussten Internetnutzung, bei der eine Reihe einfacher Cyber-Sicherheitstipps berücksichtigt werden, kann eine Infektion vermeiden. Das Projekt bietet Nutzern Tools, die ihnen bei der Wiederherstellung der Daten nach einer erfolgten Verschlüsselung helfen können. Zum Start beinhaltet die Seite vier Entschlüsselungstools für verschiedene Malware-Arten, beispielsweise ein im Juni 2016 entwickeltes Tool für eine Version von „Shade“ – einen Ransomware-Trojaner, der Ende 2014 auftauchte. Der Schädling wird über schadhafte Webseiten und infizierte E-Mail-Anhänge verbreitet. Ist er auf einem Nutzersystem gelandet, verschlüsselt „Shade“ Dateien, die auf dem Rechner gespeichert sind, und erstellt eine „txt.-Datei“, die eine Lösegeldforderung und eine Anleitung der Cyber-Kriminellen enthält, was zur Wiedererlangung der persönlichen Daten zu tun ist.

Lösegeld. „Das größte Problem hinsichtlich Krypto-Malware ist heutzutage, dass Nutzer, bei denen wertvolle Daten gesperrt wurden, bereitwillig den Cyber-Kriminellen Geld bezahlen, damit sie die Daten wieder bekommen. Das fördert die Untergrundökonomie“, sagt Jornt van der Wiel, Security-Researcher bei *Kaspersky Lab*. Opfer von Ransomware sollten das geforderte Lösegeld niemals zahlen. Es gibt keine Gewährleistung dafür, dass Opfer nach der Zahlung wieder Zugang zu den verschlüsselten Daten erhalten. Laut Ermittlern des Bundeskriminalamts Österreich sei bei vielen Klein- und Mittelunternehmen, die von Ransomware betroffen sind, die Wiederherstellung von Daten oft eine Frage der Existenz. Das Problem sei, dass diese Betriebe keine eigene IT-Abteilung haben, sondern IT-Angelegenheiten von einem Mitarbeiter „mitbetreut“ werden. Sie sind auf einen solchen Fall oft nicht vorbereitet.

„Seit einigen Jahren hat sich Ransomware zu einer der drängendsten Sorgen für die EU-Strafverfolgungsbehörden entwickelt. Ein Problem, das Bürger und Wirtschaft sowie Computer und mobile Geräte betrifft“, sagt Wil van Gemert, Deputy Director Operations bei Europol. „Initiativen wie das No-More-Ransom-Projekt zeigen, dass der richtige Weg über geteilte Expertise und gebündelten Kräfte im erfolgreichen Kampf gegen Cyberkriminalität zu gehen ist. Wir erwarten, vielen Menschen dabei helfen zu können, die Kontrolle über ihre Daten wieder zu erlangen und die Bevölkerung aufzuklären, wie sie die eigenen Geräte frei von Malware halten.“

Das Anzeigen von Ransomware-Delikten ist wichtig, um den Behörden dabei zu helfen, ein möglichst komplettes Bild zu bekommen und reagieren zu können. Die „No More Ransom“-Webseite bietet den Opfern die Möglichkeit, kriminelle Delikte anzuzeigen, indem sie direkt von der Übersichtsseite von Europol *(www.europol.europa.eu/content/report-cybercrime)* zu den nationalen Behörden weitergeleitet werden.

FOTOS: MARZIA COSENZA/EUROPÄISCHE UNION, KASPERSKY LAB