Die Hackergruppe LockBit, die sich auf Datendiebstahl mit Lösegeldforderungen spezialisiert hat, wurde von einer gemeinsamen Operation von zehn Ländern, darunter Frankreich, ins Visier genommen. Zwei Mitglieder wurden festgenommen und zahlreiche Daten beschlagnahmt.

Ein schwerer Schlag für eine der gefährlichsten Hackerbanden der Welt. Die Gruppe LockBit, die für mehrere hundert groß angelegte Hackerangriffe in Frankreich und weltweit verantwortlich ist, war am Montag, den 19. Februar, Ziel einer internationalen Polizeiaktion, bei der mehrere Websites der Gruppe im Dark Web beschlagnahmt wurden.

> Lockbit ransomware groups website has been seized by EUROPOL.
> pic.twitter.com/Z4UTRy25z6
>
> — vx-underground (@vxunderground) February 19, 2024

Die Operation, die von Ermittlern aus mehreren Ländern, darunter auch Frankreich, durchgeführt wurde, führte zur Festnahme von zwei Mitgliedern der Hackerbande und zur Beschaffung zahlreicher Daten.

Die aktivste Hackergruppe der Welt
LockBit ist eine russischsprachige Hackergruppe, die mehrere Generationen der gleichnamigen Ransomware (oder „Lösegeld-Software“) entwickelt hat. Mit dieser Malware werden Daten auf Geräten in einem Netzwerk verschlüsselt, sodass sie nicht mehr lesbar sind, es sei denn, man verfügt über einen speziellen Code – den LockBit nur gegen ein Lösegeld liefert. Wenn das Opfer nicht zahlt, drohen die Hacker damit, die Daten zu veröffentlichen oder weiterzuverkaufen.

Im November 2022 hatten die USA behauptet, dass die LockBit-Ransomware die „aktivste und zerstörerischste Variante der Welt“ sei. Allein in den USA hat die Gruppe seit 2020 mehr als 1.700 Angriffe durchgeführt, bei denen insgesamt fast 91 Millionen US-Dollar Lösegeld erpresst wurden, wie eine US-Behörde berichtete. Im Gegensatz zu anderen Gruppen hat sich LockBit zu einem echten Unternehmen entwickelt, das seine Dienste gegen eine prozentuale Beteiligung an Auftraggeber und andere Hacker verkauft.

In Frankreich war LockBit laut der Pariser Staatsanwaltschaft an über 200 Angriffen beteiligt, z. B. gegen das Krankenhaus von Corbeil-Essonnes (Departement Essonne) im Oktober 2022, um eine Million Dollar Lösegeld zu fordern. Ausserdem gegen La Poste Mobile im Juli desselben Jahres oder gegen die Gruppe Voyageurs du monde im Juni 2023. Eine seiner

Ransomware, die auch von anderen Gruppen verwendet wird, könnte bei dem Cyberangriff auf das Krankenhaus in Armentières (Nordfrankreich) am 10. Februar 2024 zum Einsatz gekommen sein, wie Valéry Rieß-Marchive, Chefredakteur der Fachseite LeMagIT, auf X erklärt.

Etwa zwanzig der Gruppe bekannte Websites im Dark Web wurden in der Nacht von Montag auf Dienstag, den 20. Februar offline geschaltet und beschlagnahmt, wie das auf Cybersicherheit spezialisierte Konto vx-underground auf dem sozialen Netzwerk X berichtet. Das LockBit-Team bestätigte die Beschlagnahmung seiner Seiten durch das FBI, wie die spezialisierte Website Zataz berichtet.

Die Webseiten wurden alle durch die gleiche englischsprachige Nachricht ersetzt, in der erklärt wird, dass „diese Seite nun unter polizeilicher Kontrolle steht“. Die Beschlagnahme wurde durch die gemeinsame Aktion von Ermittlern in 10 Ländern ermöglicht, die an der „Operation Cronos“ beteiligt sind, darunter die USA, Großbritannien oder auch Frankreich, Deutschland und Japan.

> The NCA reveals details of an international disruption campaign targeting the world’s most harmful cyber crime group, Lockbit.
>
> Watch our video and read on to learn more about Lockbit and why this is a huge step in our collective fight against cyber crime. pic.twitter.com/m00VFWkR9Z
>
> — National Crime Agency (NCA) (@NCA_UK) February 20, 2024

In einer am Dienstagmittag veröffentlichten Erklärung veröffentlichte Europol, es habe „die kriminellen Operationen von LockBit auf allen Ebenen gestört und ihre Kapazität und Glaubwürdigkeit schwer beschädigt“. Die internationale Polizeiorganisation spricht von einer „monatelangen Operation“, bei der 34 Server in mehreren Ländern abgeschaltet wurden.

Die britischen Behörden erklärten in einer Pressemitteilung, dass sie den Quellcode der LockBit-Plattform sowie zahlreiche Informationen über die Fähigkeiten der Gruppe erhalten hätten. Man habe auch die Kontrolle über die Umgebung übernommen, in der die LockBit-Mitglieder ihre Angriffe durchführen, sowie über die „Wand der Schande“, auf der die Hacker unter anderem die Namen ihrer Opfer veröffentlichen.

Zwei „Akteure“ der Gruppe wurden „auf Ersuchen der französischen Justizbehörden“ festgenommen, so Europol, das darauf hinweist, dass auch zwei internationale Haftbefehle

und fünf Anklagen von den französischen und US-amerikanischen Behörden ausgesprochen wurden. Mehr als 200 Kryptowährungs-Wallets, die mit LockBit in Verbindung stehen, wurden laut Europol eingefroren.

Um den Opfern von LockBit zu helfen, haben die Behörden der an der Operation beteiligten Länder auch Entschlüsselungstools zur Verfügung gestellt, mit denen die durch die Angriffe beschädigten Daten wiederhergestellt werden können. Diese sind kostenlos auf dem Portal No More Ransom erhältlich.

Die Beschlagnahmung der LockBit-Seiten ist ein schwerer Schlag für die Operationen der Gruppe. Diese beschlagnahmten Server und Webseiten dienten dazu, die Namen der Opfer anzuzeigen, Lösegeld zu fordern, aber auch gestohlene Daten zu veröffentlichen. Die Daten, die die Behörden zur Entschlüsselung der beschädigten Seiten erhalten haben, verringern natürlich ebenfalls die Auswirkungen der LockBit-Angriffe.

Es wurden offensichtlich aber nicht alle Server beschlagnahmt, auf einem seiner Kommunikationskanäle behauptet LockBit, Ersatzserver zu besitzen, die von der Operation nicht betroffen seien.

> Lockbit ransomware group has issued a message to individuals on Tox.
>
> "ФБР уебали сервера через PHP, резервные сервера без PHP не тронуты"
>
> "The FBI fucked up servers using PHP, backup servers without PHP are not touched"
>
> — vx-underground (@vxunderground) February 19, 2024