RheinlandPfalz
GENERALSTAATSANWALTSCHAFT
KOBLENZ

Bundeskriminalamt

PRESSEMITTEILUNG

der Generalstaatsanwaltschaft Koblenz – LZC -
und des Bundeskriminalamtes

10.04.2024

Illegaler Online-Service „AegisTools.pw“ abgeschaltet

Mutmaßlicher Betreiber identifiziert +++ Plattform ermöglichte Verschleierung von Schadsoftware sowie Diebstahl von Zugangsdaten

Die Generalstaatsanwaltschaft Koblenz – Landeszentralstelle Cybercrime (LZC) – und das Bundeskriminalamt (BKA) haben am 09.04.2024 den illegalen Online-Service „AegisTools.pw“ abgeschaltet. Gegen einen deutschen Staatsbürger besteht der Verdacht des gewerbsmäßigen Betreibens einer kriminellen Handelsplattform im Internet. In diesem Zusammenhang erfolgten Durchsuchungsmaßnahmen am Wohnobjekt des mutmaßlichen Betreibers in Speyer, Rheinland-Pfalz. Dabei wurden zahlreiche Beweismittel sichergestellt, darunter mehrere PCs und Laptops, verschiedene Datenträger und Mobiltelefone.

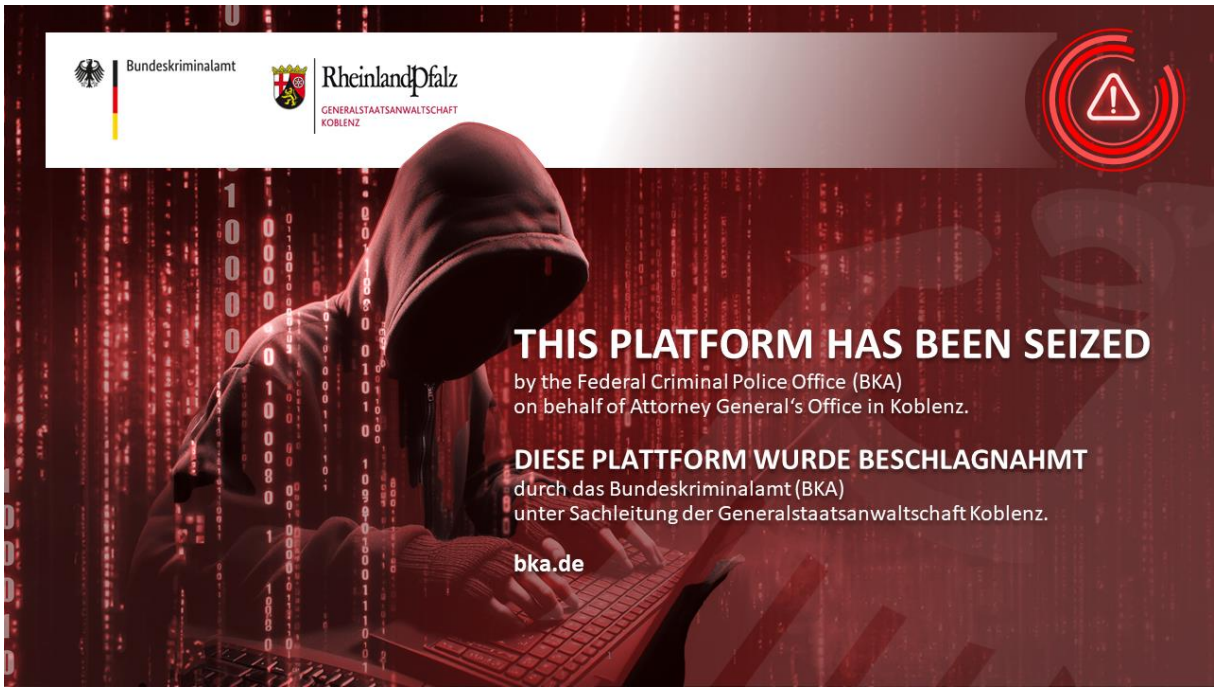
Bei „AegisTools.pw“ handelt es sich um eine in der Underground-Economy seit 2020 bekannte Plattform, die in erster Linie Counter-Antivirus- und Crypting-Dienste bereitstellte – zwei aus phänomenologischer Sicht wichtige Säulen innerhalb des Cybercrime-as-a-Service-Modells. Sie ermöglichte, Schadsoftware so zu tarnen, dass diese von den gängigen Antivirenprogrammen nicht erkannt werden konnte. „Aegis Tools.pw“ bot unmittelbar auf der Plattform auch Tests zur Überprüfung der Wirksamkeit der Kryptierung an. Weiterhin wurde eine Software für die unerlaubte Erlangung von Nutzer-Passwort-Zugangsdaten angeboten. „AegisTools.pw“ selbst hingegen verlangte von ihren Nutzern keine klassische Registrierung und konnte nahezu anonym verwendet werden. Die polizeilichen Auswertungen deuten darauf hin, dass die Plattform in der Vergangenheit weltweit von über 1.000 Usern für deren cyberkriminelle Aktivitäten in Anspruch genommen wurde. Sämtliche Dienstleistungen konnten mit Kryptowährungen bezahlt werden.

Die Abschaltung von „AegisTools.pw“ und die Identifizierung des mutmaßlichen Betreibers erfolgten unter Beteiligung von nationalen und internationalen Partnern - darunter das US-amerikanische FBI, das Western District of North Carolina (WDNC) US Attorney’s Office, die Computer Crime and Intellectual Property Section des US Department of Justice sowie die rheinland-pfälzische Polizei – und sind ein weiterer Schlag gegen spezialisierte Cybercrime-Akteure in der Underground Economy.

Pressesprecher LZC | Dr. Jörg Angerer | Deinhardpassage 1, 56058 Koblenz | +49 261 1307 30864 | pressestelle.genstako@gnstako.j.rlp.de

BKA-Pressestelle | Nina Lehmann | Marie-Curie-Straße 1, 65189 Wiesbaden | +49 611 55-13083 | pressestelle@bka.bund.de

Auf der Webseite der Plattform wurde das nachfolgende Sicherstellungsbanner veröffentlicht:



Weitere Auskünfte können derzeit nicht erteilt werden.