Schlag gegen international agierendes Netzwerk von Cyber-Kriminellen

LKA NRW

06. März 2023 | 14:51

Schlag gegen international agierendes Netzwerk von Cyber-Kriminellen

Drahtzieher identifiziert – Durchsuchungsbeschlüsse in Deutschland und der Ukraine vollstreckt.

PLZ

40221

Landeskriminalamt NRW

Landeskriminalamt NRW

In Zusammenarbeit mit Europol, dem Federal Bureau of Investigation (FBI), der niederländischen und der ukrainischen Polizei, ist den Spezialisten der Polizei NRW unter Führung des Landeskriminalamtes Nordrhein-Westfalen (LKA NRW) ein Schlag gegen ein international agierendes Netzwerk von Internetkriminellen gelungen. Unter Leitung der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) durchsuchten die Ermittler letzten Dienstag zeitgleich mehrere Objekte in Deutschland und der Ukraine.

Seit Juni 2020 sind die Cybercrime-Spezialisten des LKA NRW den international agierenden Cyber-Kriminellen auf der Spur. Die eigens eingerichtete Ermittlungskommission (EK) "Parker" konnte nun die Drahtzieher sowie weitere Mitglieder der Ransomware-Gruppierung "DoppelSpider"/"DoppelPaymer" identifizieren und im Rahmen einer gezielten Aktion zeitgleich Durchsuchungsbeschlüsse in Deutschland und der Ukraine vollstrecken.

Die kriminelle Gruppe, die sich auch "Indrik Spider" oder "Doppel Spider" nennt, ist in Deutschland unter anderem für die Erpressung der Universitätsklinik Düsseldorf, die Cyberattacken gegen die Funke Mediengruppe und weiterer namhafter Unternehmen im Jahr 2020 verantwortlich.

Durch die Ermittlungskommission "Parker" des LKA NRW zusammen mit der ZAC NRW werden zentral die Ermittlungen für alle bundesweiten Fälle geführt sowie die Ermittlungen gegen die Gruppierung zusammen mit Europol weltweit koordinierend geleitet.

Die Vorwürfe lauten insbesondere auf gewerbsmäßige, digitale Erpressung und Computersabotage. Mit einer Schadsoftware, sogenannter Ransomware (BitPaymer, DoppelPaymer, PayOrGrief, Entropy) verschafften sich die Täter digitalen Zugang zu den Rechnern der betroffenen Unternehmen, griffen Daten ab und drohten anschließend mit der missbräuchlichen Nutzung, verbunden mit Geldforderungen. So wurden weltweit von über 600 Geschädigten teils bis zu zweistellige Millionenbeträge erpresst. Der erste bekannt gewordene Angriff dieser Art richtete sich im Mai 2017 gegen das Gesundheitswesen des Vereinigten Königreiches (UK). Es folgten weltweit weitere Cyberattacken auf die digitale Infrastruktur verschiedenster Firmen und Institutionen.

Bei einer Aktion am Dienstag, 28.02.2023, durchsuchte die EK "Parker" mehrere Objekte in NRW, während zeitgleich Ermittler in der Ukraine gegen identifizierte Angehörige des Netzwerkes vorgingen. Darüber hinaus erließ die ZAC NRW Haftbefehle gegen mutmaßliche Drahtzieher der kriminellen Gruppierung mit Bezügen nach Russland. Mit Haftbefehlen suchen die Strafverfolgungsbehörden nun weltweit nach zunächst drei Verdächtigen.

Igor Olegovich Turashev steht im Verdacht, eine wesentliche Rolle, bei Cyberattacken auf deutsche Unternehmen gespielt zu haben. Der Gesuchte fungierte als Administrator der für die Angriffe genutzten IT-Infrastruktur und Malware.

Irina Zemlianikina zeichnet nach derzeitigen Ermittlungen ebenfalls mitverantwortlich für mehreren Cyberattacken auf deutsche Unternehmen. Sie administrierte insbesondere die genutzten Chat- und Leakingseiten, die für die Kommunikation der Täter mit ihren Opfern und zur Veröffentlichung gestohlener Daten dienten. Sie versendete auch E-Mails mit Malware im Anhang, um so Systeme mit Verschlüsselungssoftware zu infizieren.

Igor Garshin (alternativ: Garschin) steht im Verdacht, durch Ausspähen, Infiltrieren sowie die finale Verschlüsselung von Daten, einer der Hauptverantwortlichen für die Cyber-Angriffe nicht zuletzt auch auf deutsche Unternehmen zu sein.

"Das Verfahren zeigt, dass Cybercrime internationale Kriminalität ist - und zwar auf Seiten der Täter wie der Opfer. Täter greifen weltweit Infrastrukturen an, um Lösegelder für Daten zu erpressen." bewertet Markus Hartmann, Leiter der ZAC NRW, den aktuellen Ermittlungsstand. "Der jetzige Ermittlungserfolg zeigt aber auch, dass wir als Strafverfolger international handlungsfähig sind."

An den Ermittlungen und den operativen Maßnahmen sind neben Europol und dem FBI auch die High-Tech Crime Unit der niederländischen Polizei und die Polizei in der Ukraine entscheidend beteiligt. Die Ermittlungskommission "Parker", angesiedelt bei der Abteilung "Cybercrime" des LKA NRW führt ihre Ermittlungen in guter Zusammenarbeit mit Sicherheitsbehörden weltweit fort im Kampf gegen Internetkriminalität.

Leiter des Dezernats 42 der Abteilung für "Cybercrime"-Ermittlungen, Kriminaldirektor Dirk Kunze konstatiert: "Das Internet ist kein rechtsfreier Raum. Die Polizei NRW und das LKA NRW stellen sich - weltweit vernetzt - wirkungsvoll dem internationalen Kampf gegen diese Verbrechen." Die Polizei NRW habe dabei aber insbesondere bei der Wirtschaft immer noch mit Befürchtungen und Vorurteilen zu kämpfen, stellt Kunze fest. "Wir helfen den Unternehmen im Rahmen unserer Aufgaben und der Gefahrenabwehr bei der Bewältigung der Angriffe und unterstützen dabei, die Ausbreitung der Schäden zu verringern. Eine nicht angezeigte Straftat schützt jedoch die Täter und hat in der Wahrnehmung nicht stattgefunden."

Der Direktor des LKA Ingo Wünsch begleitete die operativen Maßnahmen seiner EK "Parker" in der vergangenen Woche eng. Neben der großen Anerkennung für die in seinem Haus geleistete Ermittlungsarbeit und die Zusammenarbeit mit Sicherheitsbehörden weltweit stellt er fest: "Täter können sich sicher sein, dass die Bekämpfung dieser Kriminalität nicht an den Grenzen aufhört, sondern grenzüberschreitend - eben - international erfolgt." Aber auch Ermittlungserfolge ändern nichts an der immer noch anhaltenden Gefahr durch Cyberangriffe. Wünsch: "Firmen, Institutionen und Behörden müssen ihre digitale Welt schützen, das bedeutet nicht nur faktisch begreif- und angreifbare Zugangstore und -türen sichern, sondern auch digitale Tore und Türen!"

Mit Unterstützung des BKA und Europol sucht die Polizei nun nach den oben genannten Verdächtigen im Rahmen einer weltweiten Öffentlichkeitsfahndung.

Turashev https://polizei.nrw/fahndung/100196
Zemlianikina https://polizei.nrw/fahndung/100197
Garshin https://polizei.nrw/fahndung/100198

Europol hat die Cyber-Kriminellen auf ihre "Europe's most wanted" - Liste gesetzt
https://eumostwanted.eu/de

Für weitere Informationen zum Thema Cyber-Ermittlungen besuchen Sie gern folgende Seiten: https://lka.polizei.nrw/artikel/lagebild-cybercrime
https://www.justiz.nrw.de/JM/schwerpunkte/zac/

Bild

Pressekonferenz EK Parker

LKA NRW