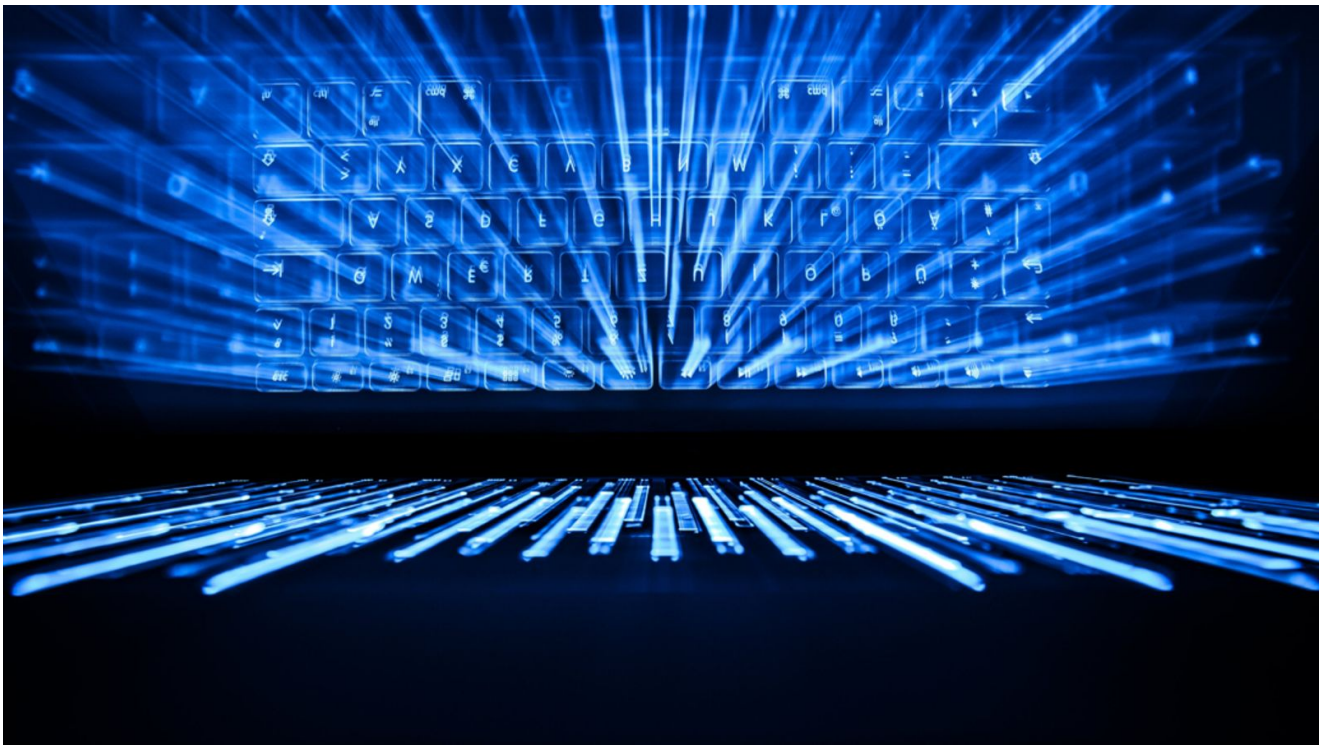
Mutmaßlicher Ransomware-Millionär identifiziert

br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ

October 28, 2021



In sozialen Netzwerken präsentiert sich Nikolay K. (Name geändert) als Händler von Kryptowährungen. Seine Accounts sind privat, doch sein Motto kann die ganze Welt lesen: "In Crypto we trust". Er vertraut Kryptowährungen wie Bitcoin – das zeigt auch ein Blick auf sein Handgelenk. Seine Uhr hat einen fünfstelligen Kaufpreis und das Bitcoin-Logo strahlt von der Mitte des Ziffernblattes. Das Instagram-Profilbild zeigt K. in einem Luxuswagen, Händchen haltend mit seiner Ehefrau. Die sozialen Netzwerke erlauben tiefe Einblicke in den Lebensstil des Mannes, der in einem Haus mit Pool in der Nähe einer südrussischen Großstadt lebt: Er verbringt Luxusurlaube in Dubai oder auf den Malediven. Eine Yacht, die er charterte, kostet 1.300 Euro – pro Tag.

Finanziert wird der luxuriöse Lebensstil mutmaßlich durch Erpressungsgeld – gezahlt von Unternehmen und Behörden, die Opfer von Hackerangriffen geworden sind. Nach Informationen des Bayerischen Rundfunks und Zeit Online haben deutsche Ermittlungsbehörden Nikolay K. seit Monaten im Visier. Ermittler von Bundeskriminalamt (BKA) und LKA Baden-Württemberg halten den Mann für einen der Drahtzieher hinter der berüchtigten Schadsoftware REvil und deren mutmaßlichem Vorgänger Gandcrab.

US-Finanzministerium: Schaden in Milliardenhöhe

Mit sogenannter Ransomware lassen sich binnen Minuten auch große Firmen-Netzwerke verschlüsseln und Unternehmen erpressen. Wie groß das Phänomen mittlerweile ist, zeigt eine Zahl des US-Finanzministeriums: Demnach haben kriminelle Hacker dank Ransomware binnen weniger Jahre mindestens fünf Milliarden Dollar erbeutet. Die Gruppe REvil ist bekannt dafür, fantastisch hohe Forderungen zu stellen, um Daten wieder zu entschlüsseln: 70 Millionen US-Dollar beträgt der bisherige Rekord.

Zum Artikel: "Die skrupellosen Cyberkriminellen von 'REvil'"

REvil ist wie ein Franchise-Unternehmen organisiert: Entwickler lizenzieren die Software und geben sie an sogenannte Affiliates weiter, die eigentlichen Hacker, die in Unternehmensnetze eindringen und Lösegeld erpressen. Die müssen dafür einen Teil des Gewinns abgeben. Welche Rolle Nikolay K. genau gespielt haben soll, ist unklar – aus Ermittlerkreisen ist jedoch zu hören, dass er "zweifelsfrei" der Kerngruppe von REvil angehören soll und damit wohl bei jedem Hackerangriff mitverdiente.

Ermittler verfolgen Bitcoin-Zahlungen

Der Haftbefehl ist nach Informationen von BR und Zeit Online vorbereitet, monatelange Ermittlungsarbeit ist in ihn geflossen. Das LKA Baden-Württemberg kam Nikolay K. über Bitcoin-Zahlungen auf die Spur. Im Frühjahr 2019 erstattete ein Software-Entwickler in der Nähe von Stuttgart Anzeige. Die Hacker waren an die Zugangsdaten eines Mitarbeiters gekommen und konnten so in die Systeme einiger Kunden eindringen.

Zu diesen gehörten auch die Staatstheater Stuttgart. Fünf Tage lang war dort der E-Mail-Verkehr lahmgelegt, statt Online-Tickets erhielten Zuschauer mit Kugelschreiber beschriebene Ersatzkarten. Um die Daten zu entschlüsseln, sollen die Staatstheater Medienberichten zufolge 15.000 Euro in einer Digitalwährung gezahlt haben. Beim LKA Baden-Württemberg wurde im Anschluss an diesen Angriff eine Ermittlungsgruppe gegründet. Sie trägt den Namen "Krabbe" – damals waren die Hacker bekannt unter dem Namen Gandcrab. Ermittler und IT-Sicherheitsexperten gehen davon aus, dass hinter REvil und Gandcrab dieselben Kriminellen stecken.

Gespräche auf höchster politischer Ebene

IT-Sicherheitsexperten halten es für naheliegend, dass viele Ransomware-Gruppen in Russland sitzen. Im Juni drohte US-Präsident Joe Biden seinem russischen Amtskollegen Wladimir Putin mit Konsequenzen, sollte dieser nicht gegen jene Hackerbanden vorgehen, die von Russland aus operieren. Auch die Bundesregierung spricht die Frage von Cyberbedrohungen regelmäßig gegenüber der russischen Regierung an, heißt es aus dem Auswärtigen Amt. Doch konkrete Tatverdächtige zu ermitteln, gilt als äußerst schwierig. Genau das haben die deutschen Ermittler im Fall Nikolay K. nun offenbar geschafft.

Netz-Recherchen erhärten Verdacht

Auch Reportern von BR und Zeit Online ist es gelungen, Spuren zu folgen, die Nikolay K. im Netz hinterlassen hat. So finden sich etwa Fotos aus seiner Jugend, noch ohne teure Uhren und Designerkleidung. "Wenn man sich die Klamotten anschaut, dann sieht man allein daran schon seinen Aufstieg", wie es einer der Ermittler kommentiert.

Außerdem finden sich Anhaltspunkte, dass K. Geld erhalten hat, das direkt aus Ransomware-Vorfällen stammen soll. Wer etwa seinen Instagram-Nutzernamen in Suchmaschinen eingibt, landet zuerst bei einer E-Mail-Adresse. Mit dieser wurden mehr als 60 Webseiten angemeldet, teilweise mit authentischen Kontaktinformationen, etwa Handynummern. Das geht aus einer Datenbank der IT-Sicherheitsfirma Domaintools hervor. Eine dieser Handynummern ist mit einem Telegram-Account verknüpft, der sich angeblich auf den Handel mit Kryptowährungen spezialisiert hat. Auf eine dort angegebene Bitcoin-Adresse wurden Zahlungen im Wert von knapp 400.000 Euro transferiert. Diese Zahlungen stammen wahrscheinlich aus Ransomware-Vorfällen, wie es ein Experte erklärt, der sich auf das Auswerten von Bitcoin-Zahlungen spezialisiert hat. Ein weiterer geht davon aus, dass K. das Geld von jemandem bekommen hat, der für verschiedene Ransomware-Gruppen arbeitet, möglicherweise ein Affiliate. Zu diesen Gruppen gehört unter anderem REvil.

LKA äußert sich nicht zu laufenden Ermittlungen

Offiziell wollen weder das BKA noch das LKA Baden-Württemberg laufende Ermittlungen kommentieren. Die zuständige Staatsanwaltschaft Stuttgart wollte sich über ein halbes Jahr lang und auf mehrfache telefonische Nachfrage, nicht äußern. Nur so viel: Die Ermittlungen dauerten an.

Doch manche Ermittler vertreten die Ansicht, dass man deutlicher über diesen Ermittlungserfolg reden müsse: "Wenn wir jemanden hätten, der diese Summen bei einem Bankraub erbeutet, dann gäbe es viel mehr Druck. Aber die Gefahr wird nicht verstanden", sagt einer von ihnen. Außerdem werde durch öffentliche Berichterstattung klar, wie erfolgreich deutsche Behörden arbeiten können. Dass man sowohl über talentiertes Personal verfüge als auch über die technischen Mittel.

Urlaub in der Türkei

Dennoch ist Nikolay K. weiter auf freiem Fuß – denn deutsche Ermittlungsbehörden könnten ihn nur dann festnehmen, wenn er Russland verlässt und in ein Land reist, das nach Deutschland ausliefert. Eine Gelegenheit dafür hätte es nach Recherchen von BR und Zeit Online im vergangenen Jahr gegeben: Mit Freunden und seiner Ehefrau verbrachte der Mann seinen Sommerurlaub an der türkischen Mittelmeerküste. Zu einem Auslieferungsantrag kam es jedoch nicht. Die Gründe sind unklar.

Seit durch einen Bericht der Nachrichtenagentur Reuters Mitte Oktober bekannt wurde, dass es internationalen Ermittlern gelungen ist, die Infrastruktur der Hacker zu kapern, dürften diese extrem vorsichtig sein.

Ob Nikolay K. Bescheid weiß, dass er seit Monaten im Fokus von Ermittlungen steht, ist offen. Eine Anfrage ließ K. unbeantwortet. Solange er nicht rechtskräftig verurteilt ist, gilt die Unschuldsvermutung. Auf Instagram finden sich jedenfalls auch aus diesem Sommer Urlaubsfotos aus der Türkei. Doch die Ehefrau reiste offenbar alleine – Nikolay K. blieb dieses Mal wohl in Russland.

"Hier ist Bayern": Der BR24 Newsletter informiert Sie immer montags bis freitags zum Feierabend über das Wichtigste vom Tag auf einen Blick – kompakt und direkt in Ihrem privaten Postfach. Hier geht's zur Anmeldung!