NACHRICHTEN
Österreich
22. Mai 2025

US klagt Russen wegen Führung eines globalen Cyberkriminellen Netzwerks

Ein US-Bundesanklage beschuldigt einen Russen, ein globales Cyberkriminalitätsnetzwerk geleitet zu haben, das weltweit Millionen Schäden verursacht hat. Die US-Behörden arbeiten daran, gestohlenes Krypto zurückzugeben.

Ein US-amerikanisches Bundesgericht hat am Donnerstag eine Anklage gegen einen Russen veröffentlicht, der beschuldigt wird, eine globale Cyberkriminellenvereinigung geleitet zu haben. Diese Bande hat weltweit Schäden in Höhe von Hunderten Millionen Dollar verursacht.

Umfang der Cyberkriminalität

Die Ermittlungen zeigen, dass die Gruppe Menschen in den USA und verschiedenen Wirtschaftssektoren ins Visier nahm. Dies

reichte von einer Zahnarztpraxis in Los Angeles bis hin zu einem Musikunternehmen in Tennessee.

Wiedergutmachung für die Opfer

Im Rahmen der Anklage kündigte das US-Justizministerium an, dass es daran arbeite, mehr als 24 Millionen Dollar in Kryptowährungen, die dem Russen angeblich gestohlen und vom Ministerium beschlagnahmt wurden, an die Opfer zurückzugeben.

US-amerikanische Maßnahmen gegen Cyberkriminalität

Dies ist Teil einer jahrelangen US-Strafverfolgung, die darauf abzielt, es Russland-basierten Kriminellen zu erschweren, amerikanische Anbieter kritischer Infrastruktur mit Ransomware-Angriffen zu erpressen und zu stören. Am Mittwoch gab das Justizministerium bekannt, dass es die Computersysteme hinter einem weiteren aufsehenerregenden Hacking-Tool beschlagnahmt hat, dessen Drahtzieher ebenfalls in Russland vermutet wird.

Russland und die Auslieferung von Kriminellen

Die USA und Russland haben keinen Auslieferungsvertrag, und das Kremlin zeigt sich zurückhaltend, wenn es darum geht, Hacker auf russischem Boden zu verfolgen, solange sie keine russischen Organisationen angreifen, so US-Beamte.

Die Rolle von Rustam Gallyamov

Der am Donnerstag angeklagte Rustam Rafailevich Gallyamov, ein 48-jähriger aus Moskau, wird beschuldigt, im Jahr 2008 eine bösartige Software namens Qakbot entwickelt zu haben, die

genutzt wurde, um Hunderttausende von Computern in den USA und weltweit zu infizieren. Diese Malware wurde in schädlichen Ransomware-Angriffen auf Gesundheitsbehörden und staatliche Stellen eingesetzt, berichten die Staatsanwälte.

Ransomware und finanzieller Gewinn

Gallyamov erhielt häufig einen Anteil an den Erlösen aus Ransomware-Angriffen, die andere Hacker unter Verwendung von Qakbot durchführten. Für den Ransomware-Angriff auf das Musikunternehmen in Tennessee erhielt er über 300.000 Dollar, so die Anklage.

Reaktionen und weitere Maßnahmen

CNN hat die russische Botschaft in Washington D.C. um einen Kommentar zu den Vorwürfen gebeten. Die Anklage bietet einen Einblick in den widerstandsfähigen Werdegang eines mutmaßlichen Cyberkriminellen. Im Jahr 2023 dismantierten das FBI und europäische Strafverfolgungsbehörden ein riesiges Netzwerk von mit Qakbot infizierten Computern und beschlagnahmten Millionen von Dollar, die den Hackern gehörten.

Versteckte Methoden der Cyberkriminellen

Nach dieser Zerschlagung suchte Gallyamov offenbar nach neuen Wegen, um seine bösartige Software Cyberkriminellen anzubieten, die Ransomware-Angriffe durchführten. Er und seine Komplizen sollen damit begonnen haben, Unternehmen mit Spam zu bombardieren und sich als IT-Support auszugeben, um das Problem zu beheben, so die Anklage.

Belohnungen für Informationen

Das Außenministerium bot 2023 eine Belohnung von 10 Millionen Dollar für Informationen über die Hintermänner von

Qakbot an. Es ist unklar, ob vertrauliche Hinweise zu Gallyamovs Anklage führten. In einigen Fällen werden Anklagen veröffentlicht, wenn nicht sicher ist, ob ein Angeklagter in ein Land reist, das mit den USA keinen Auslieferungsvertrag hat.

Die Verbindungen zu Ransomware-Gruppen

Zu den Hauptkunden von Gallyamov gehörte offenbar die Ransomware-Gang Conti, die in einem kurzen Zeitraum von vier Monaten im Jahr 2021 mindestens 25 Millionen Dollar aus einer Reihe von Angriffen erzielt hat, so die Krypto-Tracking-Firma Elliptic. Diese Gang setzte Gallyamovs Hacking-Tool in Angriffen auf ein Fertigungsunternehmen in Wisconsin und ein Technologieunternehmen in Nebraska im Herbst 2021 ein.

Die Auswirkungen des Ukraine-Konflikts

Die letzte Erwähnung der Conti-Ransomware-Gruppe in der Anklage datiert aus Ende Januar 2022. Ein Monat später startete Russland seine umfassende Invasion in die Ukraine, und ein ukrainischer Hacker **leakte eine Fülle von Daten** über Conti als Vergeltung für dessen Unterstützung der russischen Regierung. Dies zwang das kriminelle Netzwerk zur Neugründung, doch Gallyamov wandte sich offenbar anderen Kunden zu.

Details