"Metel"-Gruppe hinterlässt keine Spuren

Probe für Giga-Attacke? Hacker schießen Rubel ab – und keiner hat es gemerkt

Freitag, 19.02.2016
von FOCUS-Online-Redakteur Melchior Poppe

dpa/Karl-Josef Hildenbrand Hacker manipulierten im Februar 2015 den Rubelkurs (Symbolbild)

Cyberkriminelle haben die Systeme einer kasachischen Bank geknackt. Im Namen des Instituts machten sie gigantische Währungsgeschäfte, die sogar den Rubelkurs in die Knie zwangen. Geld haben sie nicht verdient. Experten sagen: Es war der Test für einen viel größeren Angriff.

Der Eingriff dauerte nur 14 Minuten. Doch er ließ den Rubelkurs so stark schwanken, dass die russische Zentralbank erschrak: Hacker sollen das Computersystem einer Regionalbank in Kasachstan gekapert und mithilfe eines Trojaners namens „Corkow“ Währungs-Transaktionen im Wert von mehr als 400 Millionen Dollar ausgeführt haben.

Als die Moskauer Börse bekräftigte, dass es keinen Fehler in ihren Systemen gegeben habe, leitete die Zentralbank Ermittlungen wegen möglicher Kursmanipulationen ein. Die Ermittler konnten jedoch keine Unregelmäßigkeiten feststellen. Kein Wunder: Die Hacker hatten Corkow befohlen, die eigenen Spuren zu verwischen, ehe sich das Virus selbst zerstörte.

Infiziert andere Rechner - auch ohne Internet

Die Zentralbank musste schließlich annehmen, dass es sich bei den Transaktionen um Fehler der Händler handelte. Erst jetzt sind Spezialisten den Hackern auf die Schliche gekommen: Im Auftrag der betroffenen Energobank aus Kasachstan untersuchte die Sicherheitsfirma Group-IB den Fall, der sich bereits im Februar 2015 ereignete. Was die Experten herausfanden, gibt Anlass zu großer Sorge.

Bei "Corkow" handelt es sich nämlich um eine Variante einer als „Metel“ bekannten Malware: Über scheinbar seriöse Webseiten, Emails oder Dateien gelangt sie auf fremde Rechner und verbreitet sich von dort aus weiter. „Hat sich das Virus erst einmal Zugang zu einem lokalen Netzwerk verschafft, ist es so schlau, dass es von

selber andere Rechner infiziert, die nicht einmal mit dem Internet verbunden sind“, erklärte der Chef der Sicherheitsabteilung von Group-IB gegenüber „Bloomberg“.

Bleibt monatelang unentdeckt

Außerdem aktualisiert sich "Metel" kontinuierlich selber, damit es von Antivirenprogrammen nicht erkannt werden kann. Die Mehrzahl aller infizierten Rechner werde regelmäßig mit Antivirenprogrammen geprüft, ohne dass diese Alarm schlagen, heißt es im Bericht von „Group-IB“. So könne das Virus sechs Monate und länger unentdeckt auf den Rechnern bleiben.

Auch die Attacke auf die Energobank war nur so möglich. Das Virus gelangte nämlich bereits im September 2014 auf deren Rechner – griff aber monatelang nicht in die Abläufe des Systems ein.

Hacker haben nichts verdient

Erst im Dezember begannen die Hacker damit, die Rechner der Bank zu manipulieren: Jedesmal, wenn die Mitarbeiter der Bank neue Programme installierten und Daten ins System gaben, taten die Eindringlinge dasselbe - mit ihren Programmen und ihren Daten. Im Februar schlossen sie die Vorbereitungen ab und griffen blitzschnell an.

Bemerkenswert ist, dass die Hacker so viel Zeit und Mühe investierten – um am Ende leer auszugehen. Zwar haben viele Händler die enormen Kursschwankungen ausgenutzt und gute Geschäfte gemacht, während die Energobank lokalen Medien zufolge mehr als drei Millionen Dollar verlor. Doch die Hacker haben nichts verdient.

Metel-Virus bereits auf 250.000 Rechnern

Group-IB vermutet deshalb, dass es sich bei der Attacke lediglich um einen Test handelte. Der eigentliche Angriff steht wohl noch aus, und er dürfte viel drastischere Folgen haben. Denn bei "Corkow" handelt es sich um eine Variante des "Metel"-Virus. Dieses habe sich weltweit bereits auf 250.000 Rechnern eingenistet.

Auch 100 überwiegend große Banken seien betroffen, berichtet Group-IB weiter und warnt: „Wir können vorhersagen, dass es in naher Zukunft ähnliche Attacken gegen Finanzinstitute in Russland, in der EU, im Nahen Osten, Asien und den USA geben wird.“

Geheimdienste haben nichts mit Angriffen zu tun

Einen Angriff, bei dem die Hacker Geld verdienten, gab es bereits: Im August 2015 wurde "Metel" für einen Beutezug an russischen Geldautomaten eingesetzt. Die Hacker konnten die Auszahlungen rückabwickeln, so dass die verwendeten Bankkarten zunächst nicht belastet wurden. „Die Kriminellen fuhren nachts in russischen Städten herum und leerten Geldautomaten unterschiedlicher Banken“, berichtet die Sicherheitsfirma Kaspersky.

Group-IB zufolge handelt es sich bei der "Metel"-Gruppe um russischsprachige Cyberkriminelle. „Es gibt keine Hinweise darauf, dass Geheimdienste etwas mit dem Angriff zu tun haben könnten“, heißt es im Bericht.

„Werden sich nicht auf russischen Raum beschränken“

Stattdessen sind offenbar Verbrecher am Werk, die früher oder später auch in anderen Ländern zuschlagen werden. „Es besteht Grund zur Annahme, dass die Gruppe sich nicht nur auf den russischen Raum beschränken wird“, warnt Kaspersky. Alle Banken sollten deshalb ihre Netzwerke auf "Metel"-Viren überprüfen.