BKA befragt Schlüsselfigur im Fall Emotet

By Hakan Tanriverdi und Maximilian Zierer, BR

Published: 2021-06-10 · Archived: 2026-04-05 16:40:10 UTC

Exklusiv

Schadsoftware Emotet BKA befragt Schlüsselfigur

Stand: 10.06.2021 • 06:10 Uhr

Emotet galt als "König der Schadsoftware" - bis deutsche Ermittler das Botnetz zerschlugen. Recherchen von *BR* und "Zeit" zeigen jetzt neue Details zu einer mutmaßlichen Schlüsselfigur, die auch im Fokus des BKA steht.

Ende Januar dieses Jahres: Die ukrainische Polizei bricht mit einem Stemmeisen eine Wohnungstür auf. Sie ist auf der Suche nach Beweisen im Fall der Schadsoftware Emotet. In einem Youtube-Video ist zu sehen, wie Beamte einen heruntergekommenen Plattenbau in der Stadt Charkiw stürmen.

Ich bin damit einverstanden, dass mir Inhalte von YouTube angezeigt werden.

In der Wohnung: keine hochgesicherten Serverräume, sondern aufgeschraubte Computer, herumliegende Festplatten und mehrere alte Handys. Von dieser heruntergekommenen Bude aus soll das Schadprogramm Emotet administriert worden sein.

Die Schadsoftware hatte in den vergangenen Jahren das Geschäftsmodell der Cyberkriminalität revolutioniert. Über clever gefälschte E-Mails verbreitete sich das Programm automatisiert auf bis zu anderthalb Millionen Rechner weltweit, wie das US-Justizministerium mitteilte. Hatte Emotet einen Rechner übernommen, konnten

Hacker die Systeme lahmlegen, Ausspähprogramme installieren oder Daten verschlüsseln, um Geld zu erpressen. Der Schaden weltweit: hunderte Millionen Dollar.

Beschuldigter streitet Vorwürfe ab

Bislang war unklar, wem die durchsuchte Wohnung gehört: Nach Informationen von *BR* und "Zeit" handelt es sich bei dem Beschuldigten um den 48-jährigen Ukrainer Petro Ponomarenko *(Name geändert*). Von seiner Wohnung aus soll er nach Ansicht des Bundeskriminalamtes (BKA) das Netzwerk hinter Emotet administriert haben.

Reportern von *BR* und "Zeit" ist es gelungen, mit Ponomarenko zu kommunizieren. Über seinen Anwalt bestreitet er die Vorwürfe der Ermittler. "Die haben gesagt, dass von den Servern eine gefährliche Erpressungssoftware gesteuert wird. Das wusste ich einfach nicht."

Nur ein paar Computer vom Flohmarkt?

Er habe Server gewartet, für ein paar seiner Stammkunden. Die hätten ihm monatlich 40 bis 80 Dollar pro Maschine gezahlt. Anderen Kunden habe er geholfen, neue Programme zu installieren oder Daten zwischen Rechnern hin- und herzuschieben. Seine Computer habe er auf dem Flohmarkt gekauft, mit ihnen verdiene er sein Geld. Das brauche er vor allem für sein herzkrankes Kind.

Die Reporter folgten Ponomarenkos Fährte in sozialen Netzwerken, wo sich der mutmaßliche Emotet-Administrator mit Sonnenbrille und braunen Locken zeigt. Schon seit seiner Jugend in den 1990er-Jahren beschäftigte er sich offenbar mit Computern. Er verbrachte Zeit in einem russischsprachigen Forum für das Betriebssystem Linux und programmierte in seiner Freizeit Level für das Computerspiel Doom II. Später studierte er in Charkiw Computertechnik. In Internetforen bot er seine Dienste als Administrator an.

Spuren zu einem Forum für Cyberkriminalität

Doch es finden sich auch andere Spuren von Ponomarenko im Internet: Zum Beispiel nutzte er offenbar eine seiner E-Mail-Adressen in einem russischsprachigen Forum für Cyberkriminalität. In solchen Foren bieten Programmierer und Hacker gegen Geld ihre Dienste an, um Straftaten zu verüben. Crime-as-a-service, also Straftaten als Dienstleistung nennen Ermittler diese Form der Cyberkriminalität. Ponomarenkos Anwalt spricht von "Seiten für Spezialisten", wo Meinungen ausgetauscht und Kontakte geknüpft werden. Sein Mandant habe keine kriminelle Ausrichtung.

Zu laufenden Ermittlungen wollen sich deutsche Behörden nicht äußern. Die Ermittler des BKA gehen nach Informationen von *BR* und "Zeit" aber davon aus, dass die Kerngruppe hinter Emotet Ponomarenko für die Instandhaltung des Botnetzes angeworben hat. Botnetze sind Zusammenschlüsse von meist heimlich infizierten Rechnern, die Cyberkriminelle aus der Ferne steuern. Für den Aufbau dieser technischen Infrastruktur werden Administratoren eingesetzt.

"Haben es mit absoluten Profis zu tun"

Ponomarenko soll Anweisungen von einer Person aus Russland entgegengenommen und mutmaßlich direkt mit der Kerngruppe von Emotet kommuniziert haben. Wer Emotet entwickelt und damit große Summen verdient hat,

ist allerdings weiterhin unklar.

Linda Bertram, Staatsanwältin der Zentralstelle für die Bekämpfung der Internetkriminalität (ZIT), spricht von einem "wirklichen Geschäftsmodell", das hinter Emotet stecke: "Wir haben es mit absoluten Profis zu tun, die letzten Endes auch durch die Dauer, in der sie dieses Botnetz aufrechterhalten und vor den Strafverfolgungsbehörden zunächst geheim halten konnten, nochmal unterstrichen haben, mit welcher Akribie und Professionalität sie da eigentlich vorgegangen sind."

Emotet-Beschuldigter fünf Stunden im Verhör

Ponomarenko ist für die Ermittler des BKA eine Schlüsselfigur: Zum ersten Mal konnten sie eine konkrete Person nach den Hintergründen zu Emotet befragen. Fünf Stunden lang habe das erste Verhör gedauert, sagt Ponomarenko: Gefragt wurde nach den Servern und wer Zugriff auf diese hatte. Außerdem wollten die Ermittler wissen, wer ihn beauftragt und wer die Software zur Steuerung des Botnetzes programmiert habe.

Die Liste der Betroffenen von Emotet alleine in Deutschland ist lang: Der Maschinenhersteller Krauss-Maffei ist darunter, das Kammergericht Berlin und ein Klinikum bei München.

Wohl Zehntausende Opfer allein in Deutschland

Der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm, bezeichnet Emotet im Interview mit *BR* und "Zeit" als "König der Schadsoftware": "Emotet war eine fortschrittliche Schadsoftware, die technologisch neue Maßstäbe gesetzt hat. Früher war das so, dass das sehr hochspezialisierte Angriffe waren und die wurden durch Emotet massentauglich." Das BSI geht von mehreren Zehntausend Betroffenen allein in Deutschland aus.

BSI-Präsident Schönbohm erwartet weitere Attacken nach dem Emotet-Vorbild.

Heute gilt das Emotet-Netzwerk als zerschlagen. Doch für BSI-Präsident Schönbohm ist es nur eine "Frage der Zeit", bis Cyberkriminelle nachrücken, um die Lücke zu füllen. "Das dauert nicht zu lange, bis wieder ein Nachfolger nach oben kommt. Der König ist tot, es lebe der König. Das gilt auch hier."
