PRESSEMITTEILUNG

Hacker-Gruppe will kein Geld, sondern Propaganda

Berlin, 13. November 2024 – Die Deutsche Cyber-Sicherheitsorganisation (DCSO) hat die Cyberangriffe auf Websites in Südkorea vergangene Woche mit einer neuartigen Hacker-Gruppe in Verbindung gebracht. Diese will kein Geld erpressen. Stattdessen setzt sie auf Propaganda für den russischen Angriffskrieg in der Ukraine. Entsprechend hat sie auch schon deutsche Seiten ins Visier genommen.

Anfang November meldete das Verteidigungsministerium Südkoreas, dass ein DDoS-Angriff seine Website lahmgelegt hatte. Anschließend wurden ähnliche Attacken auf weitere Internetseiten der Regierung und anderer Organisationen des Landes bekannt. Schon die ersten Vermutungen sahen einen Zusammenhang mit der kurz zuvor veröffentlichten Drohung der Regierung Südkoreas, Waffen an die Ukraine zu liefern. Hintergrund dieser Ankündigung war die Einbindung nordkoreanischer Truppen durch Russland.

Den ursprünglichen Verdacht, dass Nordkorea für die Cyberangriffe verantwortlich sei, konnte jedoch die DCSO entkräften. Im Rahmen ihrer weltweiten Überwachung der Sicherheitslage stellte sie eine starke Aktivität der russischen Hacker-Gruppe NoName057(16) auf südkoreanische Seiten fest. Parallel veröffentlichte diese Gruppe auch ein entsprechendes Bekennerschreiben.

Ungewöhnlich an NoName057(16) ist, dass es den Hackern nicht um Geld oder Daten geht. Stattdessen möchten sie Unterstützer der Ukraine beeinträchtigen und gleichzeitig die russische Propaganda verbreiten. Ihr Ziel ist eine möglichst breite Berichterstattung in den Medien. Dies gelingt einerseits durch bekannte Opfer wie Regierungen oder große Unternehmen, andererseits mit einer unangenehmen Störung für viele Menschen, etwa das Lahmlegen des Ticketverkaufs für öffentliche Verkehrsmittel. Der rein finanzielle Schaden für die Betroffenen bleibt dabei oft gering.

Aufgrund der geringen Einnahmen und der wohl fehlenden Finanzierung durch die russische Regierung nutzt die Gruppe einen ungewöhnlichen Ansatz, den sie DDoSia nennt: Um möglichst viele Teilnehmer für die DDoS-Angriffe zu rekrutieren, kann sich jeder Russland-Unterstützer auf sein privates Endgerät einen Client installieren. Dieser steht für Windows, Linux und Android bereit. Da NoName057(16) auf Telegram bereits über 80.000 Mitglieder hat, erreichen die durch Crowdsourcing verstärkten DDoS-Angriffe ein Volumen, das auch gut geschützte Websites überlasten kann. Besonders aktive Nutzer erhalten sogar Belohnungen in Kryptowährung. Doch Vorsicht: In Deutschland ist die bewusste Teilnahme an DDoS-Angriffen strafbar, selbst wenn sie als Protestaktion gedacht ist.

Deutschland ebenfalls im Fokus

Auch deutsche Seiten waren in der Vergangenheit bereits von der seit März 2022 aktiven Gruppe betroffen. So griff NoName057(16) unter anderem Internetseiten der Bundesregierung, von Rheinmetall und mehreren Banken an. Mit jeder neuen Aktion zur Unterstützung der Ukraine besteht somit die Gefahr einer weiteren DDoS-Attacke.

Da die Gruppe ihren zentralen Server, über den alle Befehle laufen, immer wieder ändert, lässt sie sich von außen kaum zerschlagen. So sollten sich deutsche Betreiber von Websites und Online-Services gründlich auf DDoS-Attacken vorbereiten. Dazu stehen verschiedene Anti-DDoS-Lösungen bereit, um auch großvolumige Angriffe abzuwehren.

Über die DCSO
Die DCSO Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) bietet innovative Cybersecurity-Services für die deutsche Wirtschaft und einen geschützten und herstellerneutralen Raum zum Austausch und der Zusammenarbeit in allen Fragen der Cybersicherheit. Unter dem Dach der DCSO tauschen sich Unternehmen nicht nur untereinander, sondern auch mit Behörden und Forschungsinstituten über Cybersicherheitsgefahren aus. Die gewonnenen Erkenntnisse fließen in effektive Strategien und Lösungen für Prävention, Reaktion sowie Abwehr und sorgen so für mehr Sicherheit für Unternehmen, Wirtschaft und Gesellschaft.

Das in Berlin ansässige Unternehmen mit Fokus auf den deutschen Mittelstand und Großunternehmen, stellt Managed Security Services in den Bereichen Bedrohungsidentifikation (Threat Intelligence), Monitoring und Detektion (Threat Detection & Hunting) sowie Hilfe zur Vorfallsbehandlung (Incident Response) zur Verfügung. Daneben unterstützt die DCSO auch mit Beratungsleistungen bei der Bewertung geeigneter Sicherheitstechnologien, der eigenen Cybersicherheit und der von Dienstleistern sowie beim Aufbau resilienter Business- und Informationssicherheitsprozesse.

Mit dem Ziel den Bedrohungen durch global organisierte Cyberkriminalität und staatlich gelenkte Wirtschaftsspionage entgegenzuwirken, wurde die DCSO 2015 von Allianz SE, BASF SE, Bayer AG und Volkswagen AG für die deutschen Wirtschaft gegründet.

Unternehmensdaten:

- Gründung: 2015
- Gesellschafter: Allianz SE, BASF SE, Bayer AG und Volkswagen AG
- Geschäftsführung: Dr. Andreas Rohr, Dominic Coxinho
- Mitarbeiter:innen: 113

Mehr unter: www.DCSO.de

Pressekontakt:

Jonas Bedau
Marketing Manager
DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22, 10829 Berlin
Mobil: +49 (0) 151 18274803
jonas.bedau@dcso.de

Fink & Fuchs AG
Matthias Thews
Telefon +49 (0) 611-74131-918
dcso-presse@finkfuchs.de