Presse

Niedersachsen

Staatsanwaltschaft Verden
Die Leitende Oberstaatsanwältin
– Pressestelle –

ZENTRALE KRIMINALINSPEKTION
LÜNEBURG

01.12.2016

AVALANCHE, eine der weltweit größten Infrastrukturen zum Einsatz von Botnetzen wurde in internationaler Zusammenarbeit aufgedeckt und analysiert.

Polizei und Staatsanwaltschaft zerschlagen Strukturen für massenhafte Angriffe auf Online-Banking-Kunden und verhaften maßgebliche Führungsmitglieder einer kriminellen Vereinigung

(gemeinsame Presseinformation der Zentralen Kriminalinspektion Lüneburg und der Staatsanwaltschaft Verden)

Verden (Aller), Lüneburg. Am gestrigen Tage konnten in einer international koordinierten Aktion mutmaßliche Führungsmitglieder einer kriminellen Vereinigung verhaftet werden. Durch die gleichzeitig erfolgte Beschlagnahme von 39 Servern und mehreren hunderttausend Domains wurde den Tatverdächtigen allein in Deutschland die Kontrolle über mehr als 50.000 Opfer-Computer entzogen.

Nach über vier Jahren intensiver Ermittlungsarbeit der Cybercrime-Spezialisten der Zentralen Kriminalinspektion Lüneburg und der Staatsanwaltschaft Verden und in Zusammenarbeit mit dem amerikanischen FBI, dem United States Attorney's Office for the Western District of Pennsylvania, dem Department of Justice sowie den Sicherheitsbehörden von 39 europäischen und außereuropäischen Staaten war es möglich geworden, die wohl weltweit größte Infrastruktur zum Betrieb von Botnetzen aufzudecken und zu analysieren. Bis zum gegenwärtigen Zeitpunkt konnten allein auf der Führungsebene 16 Beschuldigte identifiziert werden. Gegen 7 Tatverdächtige hat das Amtsgericht Verden Haftbefehle wegen Bildung einer kriminellen Vereinigung, banden- und gewerbsmäßigen Computerbetruges und anderer Straftaten erlassen.

Mit der strukturierten Zusammenlegung von mehreren Botnetzen war es den Tätern gelungen, Bankkunden, die ihre Geschäfte online erledigten, um durchschnittlich mehr als 5.000 EUR zu schädigen. Mindestens seit 2009 nutzten die Täter die weltweit vernetzte Botnetz-Infrastruktur „AVALANCHE“ für Phishing- und Spamkampagnen. Pro Woche wurden mehr als eine Million Spammails mit schädigendem Anhang oder Link versandt. Durch Öffnen des Anhangs oder Anklicken des Links wurde das nunmehr infizierte Computer-System Teil des Botnetzes. Auf diese Weise wurden durch die Täter zeitgleich mehr als 50.000 Opfer-PCs kontrolliert und ausspioniert. Aufgrund der hier vorliegenden Anzeigen kann die Schadenssumme derzeit auf ca. 6 MioEUR aus 1.336 Taten beziffert werden. Der

tatsächliche Schaden dürfte auch in Deutschland weitaus höher liegen, während die genannten Zahlen sowieso nur die Angriffe gegen Opfer in Deutschland wiedergeben.

Begonnen hatten die Ermittlungen allerdings vor vier Jahren, als massenhaft sog. Ransomware verbreitet wurde, mit der private und geschäftliche Nutzer von PCs und PC-Netzwerken erpresst wurden, Geld zu zahlen. Während die Ermittler mit der Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) in Bonn hinter die enormen Dimensionen der Botnetzinfrastuktur „AVALANCHE" kamen, wechselten die Tatverdächtigen nicht nur die Geschäftsfelder, sondern auch die Server und die Länder von denen aus sie agierten. Derzeit liegt der Schwerpunkt darin, Online-Banking-Kunden zu schädigen. "Die Tücke einer ausgefeilten Botnetz-Infrastruktur liegt darin, dass allein das Abschalten eines einzelnen Botnetzes nicht ausreicht, um die kriminellen Angriffe zu unterbinden", teilte der Leiter der Zentralstelle für Cybercrime der Staatsanwaltschaft Verden, Oberstaatsanwalt Frank Lange mit. "Die Aufgaben der entdeckten und unschädlich gemachten Server werden schlagartig von den Servern der anderen Botnetze übernommen, bis ein neues weiteres Botnetz aufgebaut wird". Durch die Analyse der Strukturen von AVALANCHE und die Identifizierung der einzelnen Server auf Führungsebene wurde der Grundstein für die gestrige Zerschlagung der Infrastruktur gelegt. Unterstützt durch die europäischen Behörden EUROJUST und EUROPOL erfolgten zeitgleich in 10 Ländern der Welt Durchsuchungen, Beschlagnahmen von Servern und Domains sowie Festnahmen aufgrund bestehender Haftbefehle. Die identifizierten Tatverdächtigen kommen aus 10 verschiedenen Ländern. In einzelnen Fällen wird es nicht möglich sein, die Beschuldigten in Deutschland vor Gericht zu stellen, weil entsprechende Auslieferungsabkommen fehlen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilt dazu folgendes mit:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt nach einem Amtshilfeersuchen die ZKI Lüneburg sowie die StA Verden bei der Analyse der Botnetzinfrastruktur AVALANCHE und der verwendeten Schadsoftware. Das Nationale Cyber-Abwehrzentrum koordiniert aktuell BSI-seitig die Zerschlagung der Botnetzinfrastruktur. Die Analysen haben ergeben, dass rund 20 verschiedene Botnetze diese Infrastruktur nutzen, um u.a. Spam- und Phishing-E-Mails zu versenden, Ransomware zu verbreiten und die Nutzer von Online-Banking-Angeboten zu betrügen.

Im Rahmen der Zerschlagung werden nun sogenannte Sinkhole-Server eingesetzt, mit deren Hilfe betroffene Kunden gewarnt werden können. Dies erfolgt durch die Internetserviceprovider auf Basis der BSI-Analyse. Bereits im laufenden Ermittlungsverfahren wurde zur Warnung der Nutzer das Providerinformationssystem (PI) aufgebaut. Hierbei werden durch das BSI Mitteilungen über infizierte Systeme an die Provider übermittelt. Seit 2014 wurden so bereits mehr als 4,5 Millionen Meldungen an die deutschen Provider und über diese an die Kunden gesendet.

Die Zerschlagung der Botnetzinfrastruktur ist allerdings nur ein erster Schritt. Die Schadprogramme auf den infizierten Rechnern werden dadurch nicht gelöscht. Dies muss durch die Nutzer selbst erfolgen. Die betroffenen Bürgerinnen und Bürger werden über ihre Provider informiert. Ihnen wird dringend empfohlen, ihre Rechner auf eine Infektion mit

Schadprogrammen zu überprüfen. Nähere Informationen dazu erhalten Sie unter www.bsi-fuer-buerger.de/botnetz.

Kontakt:

Lutz Gaebel
Pressesprecher
Staatsanwaltschaft Verden
Die Leitende Oberstaatsanwältin
- Pressestelle -
Johanniswall 8
27283 Verden (Aller)

Tel: +49-4231-18-436 (am 01.12.2016 nicht erreichbar)
Mobil: +49-151-59087764
Fax: +49-4231-18-887
E-Mail: lutz.gaebel@justiz.niedersachsen.de