HESSEN
GENERALSTAATSANWALTSCHAFT FRANKFURT AM MAIN
ZIT

Bundeskriminalamt

PRESSEMITTEILUNG

der Generalstaatsanwaltschaft Frankfurt am Main -ZIT-
und des Bundeskriminalamtes

27.01.2021

Infrastruktur der Emotet-Schadsoftware zerschlagen

Deutschland initiiert „Takedown“ im Rahmen international koordinierter Maßnahmen – Schadsoftware auf zahlreichen Opfersystemen für die Täter unbrauchbar gemacht

Die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – und das Bundeskriminalamt (BKA) haben am gestrigen Dienstag im Rahmen einer international konzertierten Aktion mit Strafverfolgungsbehörden aus den Niederlanden, der Ukraine, Litauen, Frankreich sowie England, Kanada und den USA die Infrastruktur der Schadsoftware Emotet mit Unterstützung von Europol und Eurojust übernommen und zerschlagen.

Emotet galt als derzeit gefährlichste Schadsoftware weltweit und hat auch in Deutschland neben Computern zehntausender Privatpersonen eine hohe Anzahl von IT-Systemen von Unternehmen, Behörden und Institutionen infiziert, wie beispielsweise die des Klinikums Fürth, des Kammergerichts Berlin, der Bundesanstalt für Immobilienaufgaben (BImA) oder der Stadt Frankfurt am Main. Emotet besaß als sogenannter „Downloader“ die Funktion, unbemerkt ein Opfersystem zu infizieren und weitere Schadsoftware nachzuladen, etwa zur Manipulation des Online-Bankings, zum Ausspähen von gespeicherten Passwörtern oder zur Verschlüsselung des Systems für Erpressungen. Die Nutzung dieses durch die Täter geschaffenen „Botnetzes“ wurde zusammen mit der Nachladefunktion von beliebiger Schadsoftware in der „Underground Economy“ gegen Entgelt angeboten. Deshalb kann das kriminelle Geschäftsmodell von Emotet als „Malware-as-a-Service“ bezeichnet werden. Es bot weiteren Kriminellen die Grundlage für zielgerichtete Cyber-Angriffe. Alleine in Deutschland ist durch Infektionen mit der Malware Emotet oder durch nachgeladene Schadsoftware ein Schaden in Höhe von mindestens 14,5 Millionen Euro verursacht worden.

Die Ermittlungen von ZIT und BKA gegen die Betreiber der Schadsoftware Emotet und des Emotet-Botnetzes wegen des Verdachts des gemeinschaftlichen gewerbsmäßigen Computerbetruges und anderer Straftaten werden seit August 2018 geführt.

Im Rahmen dieses Ermittlungsverfahrens wurden zunächst in Deutschland verschiedene Server identifiziert, mit denen die Schadsoftware verteilt und die Opfersysteme mittels verschlüsselter Kommunikation kontrolliert und gesteuert werden. Umfangreiche Analysen der ermittelten Daten führten zu der Identifizierung weiterer Server in mehreren europäischen Staaten. So konnten

Pressesprecher ZIT | Dr. Benjamin Krause | Zeil 42, 60313 Frankfurt am Main | +49 611 3265-8708 | presse@gsta.justiz.hessen.de
BKA-Pressestelle | Jens Beismann | Thaerstraße 11, 65193 Wiesbaden | +49 611 55-13083 | pressestelle@bka.bund.de

im Wege der internationalen Rechtshilfe weitere Daten erlangt und die Emotet-Infrastruktur durch Beamte des BKA und der internationalen Partnerdienststellen immer weiter aufgedeckt werden.

Da sich die auf diese Weise identifizierten Bestandteile der Emotet-Infrastruktur in mehreren Ländern befinden, sind die gestrigen Maßnahmen zum „Takedown“ auf Initiative von ZIT und BKA in enger Kooperation mit den betroffenen internationalen Strafverfolgungsbehörden durchgeführt worden. Beamte des BKA sowie Staatsanwälte der ZIT haben dabei in Deutschland bisher bereits 17 Server beschlagnahmt. Daneben sind auf Ersuchen der deutschen Strafverfolgungsbehörden auch in den Niederlanden, in Litauen und in der Ukraine im Rahmen von internationalen Rechtshilfemaßnahmen weitere Server beschlagnahmt worden.

Durch dieses von Europol und Eurojust koordinierte Vorgehen ist es nicht nur gelungen, den Zugriff der Täter auf die Emotet-Infrastruktur zu unterbinden. Auch umfangreiche Beweismittel wurden gesichert. Zudem konnte im Rahmen der Rechtshilfemaßnahmen in der Ukraine bei einem der mutmaßlichen Betreiber die Kontrolle über die Emotet-Infrastruktur übernommen werden.

Durch die Übernahme der Kontrolle über die Emotet-Infrastruktur war es möglich, die Schadsoftware auf betroffenen deutschen Opfersystemen für die Täter unbrauchbar zu machen. Um den Tätern jegliche Möglichkeit zu nehmen, die Kontrolle zurück zu erlangen, wurde die Schadsoftware auf den Opfersystemen in Quarantäne verschoben und die Kommunikationsparameter der Schadsoftware so angepasst, dass die Opfersysteme ausschließlich zu einer zur Beweissicherung eingerichteten Infrastruktur kommunizieren können. Die dabei erlangten Informationen über die Opfersysteme wie z.B. öffentliche IP-Adressen werden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelt.

Das BSI benachrichtigt die für die übermittelten IP-Adressen zuständigen Netzbetreiber in Deutschland. Provider werden gebeten, ihre betroffenen Kunden entsprechend zu informieren. Weiterhin stellt das BSI Informationen zur Bereinigung betroffener Systeme zur Verfügung.

Für ZIT und BKA stellt das Zerschlagen der Emotet-Infrastruktur einen bedeutenden Schlag gegen die international organisierte Internetkriminalität und zugleich eine wesentliche Verbesserung der Cybersicherheit in Deutschland dar.

Weitere Informationen für Medienvertreter und Interessierte finden Sie auf der Webseite des Bundeskriminalamtes unter:

https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

Einladung für Pressevertreter:

Für O-Töne stehen die ZIT und das BKA heute zwischen 14:00 und 17:00 Uhr zur Verfügung.

Aufgrund der aktuellen Einschränkungen durch die Corona-Lage steht Ihnen der Pressesprecher der **Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) - Dr. Benjamin Krause** für Einzeltermine im Außenbereich der ZIT, Konrad-Adenauer-Straße 15, 60313 Frankfurt am Main, zur Verfügung. Bitte vereinbaren Sie einen Termin über die Pressestelle der ZIT:

Tel.: +49 611 3265-8708
E-Mail: presse@gsta.justiz.hessen.de

Aufgrund der aktuellen Einschränkungen durch die Corona-Lage steht Ihnen der **Präsident des Bundeskriminalamts Holger Münch** in diesem Zeitraum für O-Töne über Skype zur Verfügung. Bitte vereinbaren Sie einen Termin über die Pressestelle des BKA:

Tel: +49 611 55-13083
E-Mail: pressestelle@bka.bund.de

Ein Videostatement von Herrn Münch finden Sie auf der Webseite des BKA. Die Videodatei können Medienvertreter bei Bedarf über die Pressestelle des BKA auch aus mehreren Perspektiven für die Berichterstattung erhalten.