Freistaat
SACHSEN

Medieninformation

Polizeidirektion Leipzig

Ihr Ansprechpartner
Olaf Hoppe

Durchwahl
Telefon +49 341 966 44400
Telefax +49 341 966 43185

medien.pd-l@
polizei.sachsen.de*

09.01.2023

Gemeinsame Medieninformation der Polizeidirektion Leipzig und der Staatsanwaltschaft Leipzig Nr. 15|23

Bekämpfung des bandenmäßigen Computerbetruges – Festnahme in Bonn

Erstellerinnen: Jana Friedrich und Dorothea Benndorf

Ort: Bonn

Zeit: 05.01.2023, 06:00 Uhr

Am 5. Januar 2023 führte die Leipziger Kriminalpolizei in Zusammenarbeit mit der Kriminalpolizeiinspektion Bonn im Auftrag der Staatsanwaltschaft Leipzig im Stadtgebiet von Bonn umfangreiche Maßnahmen zur Aufklärung von Straftaten in Zusammenhang mit sogenannten »falschen Sparkassenmitarbeitern« durch. Dabei wurden auf Grundlage entsprechender richterlicher Beschlüsse auch drei Wohn- bzw. Geschäftsräume sowie mehrere Fahrzeuge durchsucht und umfangreiche Beweismittel sichergestellt. So wurden unter anderem eine zweistellige Zahl von Smartphones, ein Computer, verschiedene Dokumente sowie mehr als 53.000 Euro Bargeld beschlagnahmt. Ein 24-jähriger Beschuldigter (deutsch), der die Taten koordiniert haben soll, wurde auf Grundlage eines bereits zuvor durch die Staatanwaltschaft Leipzig beantragten und durch den zuständigen Ermittlungsrichter des Amtsgerichts Leipzig erlassenen Haftbefehls festgenommen und befindet sich nunmehr in Untersuchungshaft.

Dem 24-Jährigen Beschuldigten und weiteren, zum Teil noch unbekannten Mittätern, liegt zur Last, sich unter Verwendung gefälschter E-Mails oder SMS-Nachrichten von den Geschädigten die Kunden- und Zugangsdaten für das Online-Banking der jeweiligen Hausbank erschlichen und diese in der Folge zur Begehung von Straftaten verwendet zu haben (sog. »Phishing«). Die so erlangten Daten nutzten die Tatverdächtigen, um die Geschädigten telefonisch zu kontaktieren, sich als ein Mitarbeiter der

Hausanschrift:
Polizeidirektion Leipzig
Dimitroffstraße 1
04107 Leipzig

https://www.polizei.sachsen.de/de/pdl.htm

* Kein Zugang für verschlüsselte elektronische Dokumente. Zugang für qualifiziert elektronisch signierte Dokumente nur unter den auf www.lsf.sachsen.de/eSignatur.html vermerkten Voraussetzungen.

jeweiligen Hausbank auszugeben und mittels geschickter Gesprächsführung einen Notfall vorzutäuschen, der die Freigabe eines Bankauftrages über das Smartphone des Geschädigten erforderlich machte. Das betrügerische Vorgehen der Gruppierung hatte unter anderem deshalb Erfolg, weil diese die vorab erlangten Kundendaten, darunter Wohnort, Telefonnummer und Geburtstag, in die Gesprächsführung integrierte und die Verwendung der Rufnummer der jeweiligen Hausbank vortäuschte, um dem Anliegen eine besondere Glaubhaftigkeit zu verleihen. In dem Glauben, tatsächlich mit einem Mitarbeiter der jeweiligen Hausbank zu sprechen, führten die Geschädigten das geforderte TAN-Verfahren aus. Diese Freigabe nutzten die Tatverdächtigen, um auf präparierten Smartphones eine virtuelle Debitkarte (Zahlungsdienst ApplePay) einzurichten, mit der in der Folge insbesondere Bargeld, Gutscheinkarten und hochwertige Elektronikartikel erworben wurden.

Im Zuge umfangreicher und akribischer Ermittlungen von Kriminalpolizei und Staatsanwaltschaft ergaben sich Erkenntnisse dahingehend, dass hohe Geldbeträge regelmäßig in nordrhein-westfälischen Großstädten ausgecasht wurden, indem die Tatverdächtigen dort mit ihren Smartphone-Geldkarten an Tankstellen und in Geschäften bezahlten. Weitere Ermittlungsmaßnahmen ergaben dann, dass die Gruppierung um den 24-Jährigen von Bonn aus agierte, was Grundlage für die Maßnahmen am vergangenen Donnerstag war.

Die Ermittlungen unter anderem wegen des Tatverdachts des banden- und gewerbsmäßigen Computerbetruges dauern an. Der bislang festgestellte Gesamtschaden beträgt rund 26.000 Euro, wobei sich dieser im Verlauf der weiteren Ermittlungen noch erweitern kann.

Anlässlich dessen ergehen seitens der Ermittlungsbehörden folgende Hinweise:

Jeder Kontoinhaber kann sich durch Aufmerksamkeit bei der Nutzung seines ihm vertrauten Online-Banking-Portals und Beachtung der Sicherheitshinweise seines Kreditinstitutes vor unkontrollierten Abhebungen an Geldautomaten und Bezahlvorgängen an elektronischen Kassen schützen. E-Mails und SMS, die vermeintlich von der Hausbank stammen, sind Fälschungen und dienen der Erschleichung der Kundendaten. Fallen Sie nicht fahrlässig auf Täteranrufe rein, die Sie nach persönlichen Zugangsdaten für Ihr Online-Banking-Verfahren und/oder TAN-Nummern fragen. Es handelt sich dabei stets um Betrüger! Informieren Sie umgehend die Polizei.