FAST DETECT

SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK

CASE STUDY

AUSWERTUNG RELEVANTER KOMMUNIKATIONSSPUREN EINES FINANZAGENTEN

DIE AUSGANGSSITUATION

Einer Person wurde vorgeworfen, als Finanzagent agiert und Unbekannten im entgeltlichen Auftrag sein Konto zur Verfügung gestellt zu haben. Über dieses Konto wurden Geldbeträge transferiert, um deren Geldflüsse zu verschleiern.

Um den oder die Auftraggeber zu identifizieren, wurde FAST-DETECT mit der IT-forensischen Auswertung von sichergestellten Computern und Mobiltelefonen des Finanzagenten beauftragt.

DIE RAHMENBEDINGUNGEN

Das Konto des Finanzagenten wurde durch die Bank gesperrt bevor die Computer und Handys des Beschuldigten durch die Polizei sichergestellt werden konnten.

Zwischen der Sperrung des Kontos und der Hausdurchsuchung wurde sämtliche Kommunikation auf den Endgeräten des Beschuldigten gelöscht. Bei der Sichtung der aktiven Dateisysteme konnten demnach keine E-Mails, Chatprotokolle oder sonstige fallrelevanten Daten festgestellt werden.

DAS VORGEHEN VON FAST-DETECT

1. Durch die Analyse der ungenutzten Speicherbereiche aller sichergestellten Geräte wurde festgestellt, dass diese zur Kommunikation mit den Auftraggebern genutzt worden waren.

ZEITAUFWAND

BEWEISMITTEL	AUSWERTUNGSUMFANG
Computer 1	Komplett (Genutzter und ungenutzter Speicherbereich)
Laptop 1	Komplett (Genutzter und ungenutzter Speicherbereich)
Handy 1	Genutzter Speicherbereich
Handy 2	Genutzter Speicherbereich

Zeitaufwand für die Auswertung inklusive Gutachtenerstellung: 42 Std.

ZUSAMMENFASSUNG

Tatbestand: Geldwäsche

Kunde: Staatsanwaltschaft

Auftrag: IT-forensische Auswertung von sichergestellten Computern und Mobiltelefonen eines Finanzagenten.

Vorgehen: Analyse von Kommunikationsspuren im gelöschten Speicherbereich der Geräte zur Identifikation von Auftraggebern.

Befund: Rekonstruktion von ca. 99% der gesamten Kommunikation mit dem Auftraggeber aus dem ungenutzten Speicherbereich. Identifikation von mehreren E-Mail-Adressen und Facebook-/ Skypekonten der Auftraggeber.

Ergebnis: Aufnahme von Folgeermittlungen gegen weitere Personen durch die Auswertung der von FAST-DETECT ermittelten Konten.

2. Mit Hilfe spezieller Techniken wurden Skype- und Facebook-Nachrichten aus dem gelöschten Speicherbereich wiederhergestellt.
3. Durch die Auswertung dieser Nachrichten konnten zwei Kommunikationspartner identifiziert werden, die dem Verdächtigen Anweisungen erteilten.
4. FAST-DETECT identifizierte zwei weitere E-Mail-Adressen der Auftraggeber sowie ein Facebook-Profil, das bei der Anwerbung von Finanzagenten als Lockvogel genutzt wurde.
5. Mit Hilfe der E-Mail-Adressen wurden weitere Informationen aus den ungenutzten Speicherbereichen identifiziert:
   - E-Mails waren über einen Webmailer verschickt und empfangen worden.
   - Da der Auftraggeber ausschließlich in englischer Sprache kommunizierte, wurde vom Beschuldigten das Übersetzungsprogramm Google Translate genutzt.
   - Durch Rekonstruktion aus Fragmenten der Internethistorie und Internetcache-Dateien konnten eine Vielzahl der von Google Translate übersetzten Nachrichten und einige E-Mails des Webmailers wiederhergestellt werden.
6. Die wiederhergestellten Nachrichten wurden chronologisch sortiert, von Duplikaten befreit und aggregiert aufbereitet.

DER BEFUND

Folgende Informationen wurden von FAST-DETECT rekonstruiert:

- 250 Skype-Nachrichten
- 150 Facebook-Nachrichten
- 100 Nachrichten aus der Internethistorie (die per Google Translate übersetzt worden waren)
- 10 relevante E-Mails (aus dem nicht genutzten Speicherbereich)

Da die wiederhergestellte Kommunikation so gut wie keine inhaltlichen Brüche aufwies, konnte davon ausgegangen werden, dass über 99% der gesamten Kommunikation mit den Auftraggebern sichergestellt worden waren.

Aus der ausgewerteten Kommunikation wurde folgendes Vorgehen der Auftraggeber ersichtlich:

- Die Anwerbung von Finanzagenten erfolgte über ein Facebook-Profil eines fiktiven asiatischen Models, das angeblich einen deutschen Mann suchte.
- Nahm ein Interessent Kontakt auf, wurde versucht eine Fernbeziehung aufzubauen. Die zum Teil in Englisch geführte Kommunikation fand größtenteils über Nachrichten statt.
- Nach einem gewissen Zeitraum teilte das angebliche „Model“ dem potentiellen Finanzagenten mit, dass er durch Weiterleiten bestimmter Geldsummen ihre Familie unterstützen könne. Der „Anwalt“ des „Models“ bescheinigte gleichzeitig die Seriosität und Legalität dieser Transaktionen.

FABIAN UNUCKA
Sachverständiger für IT-Forensik

fabian.unucka@fast-detect.de

DAS ERGEBNIS

Anhand der identifizierten Facebook-Profile, E-Mail-Adressen und Telefonnummern konnten die Auftraggeber durch FAST-DETECT identifiziert und Folgeermittlungen gegen weitere Personen angestoßen werden.

IDENTIFIZIERTE KOMMUNIKATIONSSTRUKTUR

EINGESETZTE TECHNIKEN UND VORGEHENSWEISEN

SPEZIELLE SOFTWARE

FAST-DETECT besitzt eine umfassende Auswahl an kommerzieller und selbstentwickelter IT-Forensik-Software, um beispielsweise gelöschte Kommunikationsdaten aus ungenutzten Speicherbereichen wiederherzustellen bzw. zu rekonstruieren.

TEILAUTOMATISIERTE AUSWERTUNG

FAST-DETECT hat ein forensisch sicheres Vorgehen für teilautomatisierte Auswertungen entwickelt, deren Ergebnisse bei Bedarf mit in die Untersuchungen einfließen.

DETAILLIERTE AUSWERTUNG UND PRÄSENTATION

FAST-DETECT legt höchsten Wert auf eine optimale Präsentation des Befunds. Mit Hilfe verschiedener Visualisierungsprogramme werden auch komplexe Zusammenhänge genau und verständlich wiedergegeben.

FAST-DETECT GmbH

Inselkammerstraße 12
82008 Unterhaching
Tel +49 89 204040-0
Fax +49 89 204040-299
Mail info@fast-detect.de
Web www.fast-detect.de

10/2018